Reporte de Resultados Segunda Consulta Ciudadana Virtual sobre Ciberseguridad

Comité Interministerial de Ciberseguridad

PNCS2-D9-20230520

Este documento es responsabilidad de la Coordinación Nacional de Ciberseguridad (CNC), en la Subsecretaría del Interior.

Este documento debe ser visualizado en línea en la URL bit.ly/pncs2-d3, o escaneando el código QR; una versión en papel podría estar desactualizada.

Índice de contenidos

1. Contexto

Nuestro país se encuentra finalizando la Segunda Política Nacional de Ciberseguridad para el período 2023-2028. En el marco de este proceso participativo y abierto, el Comité Interministerial sobre Ciberseguridad realizó una consulta final sobre los objetivos propuestos en el documento.

Este reporte presenta los resultados de la consulta. En la sección 2 se presentan las preguntas realizadas, y la sección 3 contiene un breve resumen de las respuestas recibidas. En todas las secciones que presentan gráficos, se indica la cantidad de personas que respondieron cada pregunta en el mismo gráfico.

2. Preguntas realizadas

La consulta contiene 8 preguntas de selección múltiple. En cada una de ellas se presentó un resumen del texto de los objetivos de la política, respecto a los cuales los participantes debían expresar su conformidad sobre la redacción del texto, mediante un sí o un no. Adicionalmente, se habilitó la posibilidad de entregar comentarios a cada punto consultado.

La consulta fue comenzada por 235 personas, y fue terminada por 138 personas (un 58,7%), entre el 8 de mayo de 2023 a las 18:03, y el 19 de mayo a las 16:11. El tiempo promedio de respuesta fue de 4 minutos y 16 segundos.

En la siguiente tabla se indican las preguntas en el mismo orden en el que fueron realizadas.

#	Pregunta
01	En términos generales, ¿qué tan importante es la ciberseguridad para nuestro país?: *Alternativas:* ☐ Muy importante ☐ Importante ☐ Tiene el mismo nivel de importancia que otros temas ☐ Poco importante ☐ Nada importante
02	¿Está usted de acuerdo con el texto en la sección 1.2 de la propuesta, bajo el título "Los desafíos en ciberseguridad para nuestro país"? Un resumen del texto: "Los principales problemas que enfrentamos hoy en materia de ciberseguridad en nuestro país son: ➔ La falta de conciencia de las personas y las organizaciones sobre la importancia de la ciberseguridad. ➔ La falta de especialistas en ciberseguridad. ➔ La falta de resiliencia de nuestras organizaciones e infraestructura. ➔ La falta de sofisticación de nuestra demanda por ciberseguridad." *Alternativas:* ☐ Sí ☐ No Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres): [ ]

#	Pregunta
03	¿Está usted de acuerdo con el texto en la sección 1.3 de la propuesta, bajo el título "Los cinco objetivos de la Política Nacional de Ciberseguridad"? Un resumen del texto: "Para enfrentar los problemas y los desafíos anteriores, la nueva Política Nacional de Ciberseguridad contiene cinco objetivos fundamentales: ● Infraestructura resiliente ● Derechos de las personas ● Cultura de ciberseguridad ● Coordinación nacional e internacional ● Fomento a la industria" *Alternativas:* ☐ Sí ☐ No Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres):

#	Pregunta
04	¿Está usted de acuerdo con el texto propuesto para el primer objetivo de la Política ("Infraestructura resiliente"), en la sección 2.1 de la propuesta? *Un resumen del texto: "El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad y de desastres socioambientales, bajo una perspectiva de gestión de riesgos. Para ello, es necesario avanzar en el fortalecimiento de los elementos técnicos físicos y lógicos de nuestro ciberespacio, incluida nuestra creciente red de dispositivos conectados a Internet (Internet-of-Things, o IoT).* Para avanzar en este objetivo, es necesario: 1. Crear una Agencia Nacional de Ciberseguridad. 2. Crear el Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional) 3. Fortalecer la resiliencia de nuestros servicios esenciales frente a incidentes de ciberseguridad. 4. Fortalecer la resiliencia física de la red en Chile. 5. Fortalecer el monitoreo y análisis de la información de red en el ciberespacio nacional, a través de la inversión en investigación científica aplicada." *Alternativas:* ☐ Sí ☐ No Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres): [ ]

#	Pregunta
05	¿Está usted de acuerdo con el texto propuesto para el segundo objetivo de la Política ("Derechos de las personas"), en la sección 2.2 de la propuesta? Un resumen del texto: "El Estado protegerá y promoverá la protección de los derechos de las personas en Internet, a través del fortalecimiento de la institucionalidad existente en materias de ciberseguridad; y de la generación, adopción, y promoción de los mecanismos y las herramientas tecnológicas suficientes para que cada persona pueda integrarse a la sociedad y desarrollarse y expresarse plenamente, otorgando especial protección a mujeres, niñas, niños, jóvenes, personas de la tercera edad y disidencias sexogenéricas. Cada persona podrá hacer uso de Internet para comunicarse, trabajar, estudiar, y desarrollarse en lo personal, familiar y social en un entorno de equidad, inclusión, justicia y protección a la diversidad. Para avanzar en este objetivo, es necesario: 1. Fortalecer el marco normativo de protección a los datos personales y de ciberseguridad. 2. Generar instancias de capacitación para todos los funcionarios públicos en y en hábitos y medidas básicas de seguridad digital. 3. Generar medidas de acción positiva para favorecer y fortalecer la incorporación de la mujer en todo el quehacer de protección de nuestro ciberespacio. 4. Proteger y prevenir la comisión de delitos informáticos que afectan a las personas, sus derechos y su patrimonio. 5. Identificar y corregir inequidades en el acceso y uso del ciberespacio." *Alternativas:* ☐ Sí ☐ No Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres): [ ]
06	¿Está usted de acuerdo con el texto propuesto para el tercer objetivo de la Política ("Cultura de ciberseguridad"), en la sección 2.3 de la propuesta? Un resumen del texto: *"Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas, responsabilidad en el manejo de tecnologías digitales, y promoción y garantía de los derechos de las personas. La protección de todos nosotros va en directa relación con la capacidad de cada uno de protegerse. Necesitamos generar nociones de higiene digital en todas las personas de nuestro*

#	Pregunta
	país, de forma que cada persona sea capaz de cuidar por sí misma su identidad digital y su información. Para avanzar en este objetivo, es necesario: 1. Diseñar e implementar un plan de concienciación nacional sobre ciberseguridad y privacidad. 2. Generar e implementar un plan matriz de introducción y mejora de la educación en higiene digital y ciberseguridad para el sistema de enseñanza básica, media científico-humanista y media técnico-profesional. 3. Fomentar una cultura de evaluación y gestión del riesgo, tanto en organizaciones públicas como privadas. 4. Fomentar la investigación científica aplicada en ciberseguridad, para resolver problemas que nuestro país tendrá en los próximos años a raíz del uso e implementación de tecnologías con aplicaciones insospechadas." *Alternativas:* ☐ Sí ☐ No Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres): [ ]

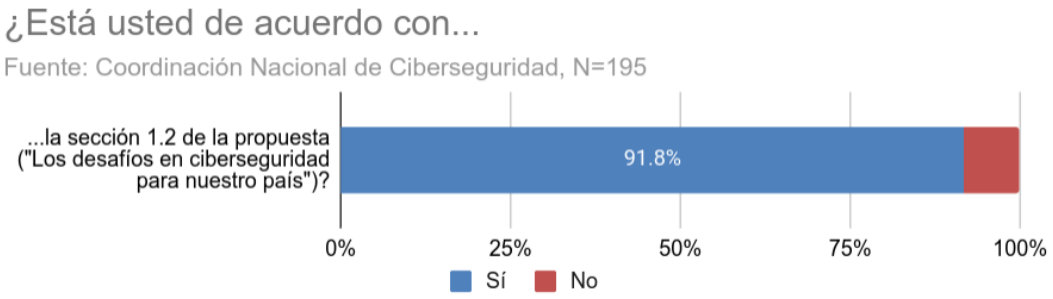
#	Pregunta
07	¿Está usted de acuerdo con el texto propuesto para el cuarto objetivo de la Política ("Coordinación nacional e internacional"), en la sección 2.4 de la propuesta? Un resumen del texto: *"Los organismos públicos y privados deben establecer instancias de cooperación con el resto del sector público, de la industria, o de la autoridad nacional de ciberseguridad, con el propósito de comunicar y difundir sus esfuerzos en ciberseguridad, evitar la duplicación de trabajo y pérdida de recursos, y hacer eficientes los esfuerzos en ciberseguridad. Tenemos que coordinar mejor nuestros esfuerzos e intencionarlos hacia la consecución de estos objetivos de política pública."* *En el aspecto internacional, el Estado debe coordinarse y trabajar con países, organismos, instituciones, y otros actores internacionales, para permitir a nuestro país enfrentar de mejor manera las actividades maliciosas e incidentes en el ciberespacio, y contribuir de esa forma a fortalecer su liderazgo regional en ciberseguridad.* Para avanzar en este objetivo, es necesario: 1. Generar instancias de colaboración entre organizaciones públicas y privadas en educación, infraestructura, protección de derechos, fomento a la industria, y otras áreas relacionadas con la ciberseguridad. 2. Establecer relaciones de cooperación con instituciones de ciberseguridad de países avanzados. 3. Aumentar la participación en instancias multilaterales, particularmente en el ámbito de las Naciones Unidas y la Organización de los Estados Americanos. 4. Promover activamente la ciberdiplomacia." *Alternativas:* ☐ Sí ☐ No Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres): [ ]

#	Pregunta
08	¿Está usted de acuerdo con el texto propuesto para el quinto objetivo de la Política ("Fomento a la industria"), en la sección 2.5 de la propuesta? Un resumen del texto: "El país promoverá el desarrollo de una industria de la ciberseguridad, que proteja a las personas y las organizaciones y que sirva a sus objetivos estratégicos. Este fomento se implementará a través de estímulos y fondos dirigidos a la oferta de servicios y productos en ciberseguridad, pero también a través de la generación de una demanda más sofisticada en ciberseguridad, de forma que nuestra industria pueda proteger de mejor forma a las personas y organizaciones, y servir mejor a los intereses del país. Para avanzar en este objetivo, es necesario: 1. Crear institutos de investigación científica aplicada y transferencia tecnológica en materias de ciberseguridad 2. Generar incentivos para el emprendimiento tecnológico en ciberseguridad 3. Revisión de los mecanismos de contratación de servicios de ciberseguridad por parte del Estado 4. Promocionar los productos y servicios de las empresas locales en ciberseguridad a nivel nacional y en el extranjero" *Alternativas:* ☐ Sí ☐ No Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres): [ ]

3. Resultados obtenidos

Nivel de acuerdo con el texto “los desafíos en ciberseguridad”

En el siguiente gráfico se muestra el nivel de acuerdo con la sección 1.2 de la propuesta de Política, consultado en la pregunta 2.



A continuación se incluyen las sugerencias de mejora al texto, sin filtrar ni editar, en orden alfabético:

Respuesta	Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres):
No	- Es un diagnóstico de debilidades, no de problemas. - Primera afirmación es sobre la falta de conciencia, responsabilizando primero a los usuarios.
Sí	3 y 4 están demás. Educar es la clave; a escolares, en finanzas electrónicas y seguridad informática. Una ley no resuelve el problema y la ignorancia nos expone al delito en forma reiterada.
Sí	5. Ausencia de leyes adecuadas y actualizadas que regulen la protección de las personas e infraestructura crítica.
Sí	5. La falta de coordinación internacional en materias de ciberseguridad
Sí	5. La falta de normativa y de un esquema nacional de ciberseguridad
Sí	Además de considerar integración público privada en temas de ciberseguridad.
No	Agregaría 5. La falta de regulaciones sobre el ámbito de ciberseguridad. 6. Falta de resiliencia entre las políticas regulatorias de ciberseguridad que

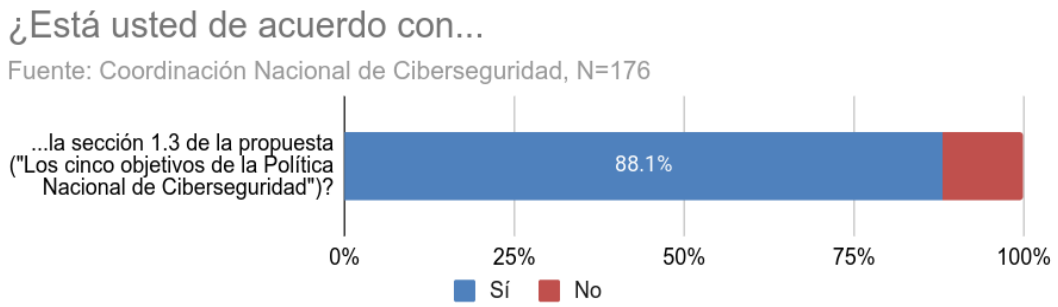
Respuesta	Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres):
	rigen los distintos organismos
Sí	Agregaría que la falta de conocimiento en el impacto económico, político y social de los efectos adversos en materia de ciberseguridad.
Sí	considerar que dada la falta de profesionales se tenga que partir con gente con experiencia empirica mas que teorica sobre la disciplina
Sí	cultura por la ciberseguridad
Sí	El trabajo colaborativo entre entidades y organismo fiscalizador independiente y competente que proteja a las personas
Sí	En general no hay especialización en áreas técnicas, solo diplomados debería haber un tipo de academia a nivel de estado dependiente de una agencia de ciberseguridad
Sí	Esto es importante no solo para la seguridad y tranquilidad de cada individuo, también para que hayan menos disrupciones que se traducen en pérdidas tanto a nivel de empresas como a nivel país
Sí	Falta compromiso de las autoridades sectoriales, como Ministros, Subsecretarios, Directores, etc, Ya que ellos son los dan fuerza a la medidas implementadas en cada servicio.
Sí	falta de conciencia de la alta dirección en el sector público de gobernanza tanto en ciber como en prevención de delitos, integridad, sostenibilidad, control interno, gestión de riesgos, etc
Sí	Falta de coordinación regional.
Sí	Falta de inversión en seguridad de la información, incorporar a los planes de estudios desde prebásica en adelante iniciativas educativas al respecto
Sí	Falta de leyes y normativas.
Sí	Falta de reglamentación y canales de denuncia, por fraudes telefónicos, sitios maliciosos, etc.
Sí	falta de sanciones por el no cumplimiento de medidas de ciberseguridad
Sí	Falta educación sobre lo que es la Ciberseguridad, a nivel escolar, desde enseñanza básica, porque ha analfabetismo digital, inclusive para familias y adultos mayores.
Sí	Falta establecimiento de "responsabilidades" y "protección del bien público". Salvo situaciones extremas, todo termina dando lo mismo

Respuesta	Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres):
No	Falta recursos, nuevo equipamiento, capacitación, modernización y mejor personal
Sí	Falta una entidad que fiscalice a sector publico y privado que cuente con las protecciones mínimas para el resguardo de datos privados (Ente regulador)
Sí	Faltan directrices y equipos de apoyo transversal, para las distintas verticales de las infr. crítica. Lo mismo para pequeñas y medianas empresas que no tienen capacidad de inversión (subsidios)
Sí	gobernanza de ciberseguridad y el ciber espacio como una dimensión estratégica al igual que aire, mar y tierra
No	Hay un elemento vinculado a la prioridad que se le da a la ciberseguridad. Sigue siendo un tema muy de nicho y técnico que dificulta la concientización y por tanto la priorización como temática.
Sí	Ignorancia de la autoridades respecto a lo que significa ciberseguridad
Sí	Ignorancia en la contratación de personal calificado. Piden que uno tenga varios millones de pesos en certificaciones porque no saben qué buscar o medir.
Sí	Iniciar con la educación en la ciberseguridad de temprana edad, mejorar las asignaturas en las universidades en el ámbito de la ciberseguridad.
No	La ciberseguridad invisibiliza la importancia de la de privacidad de datos. En particular, qué información pueden las empresas recolectar, almacenar y comercializar sobre las personas.
No	la falta de conocimientos, debido que las empresas y profesionales son mediocres.
Sí	La falta de incorporación de la ciberseguridad en alguna asignatura de la educación secundaria y terciaria
Sí	la falta de interes y conocimiento de las partes interesadas, jefes y directivos, ya sea entidad publica o privada
Sí	La falta de persecución de los delitos de ciberseguridad.
Sí	La falta de presupuesto para iniciativas debe estar al mismo nivel que el gasto operacional.
Sí	La falta de retención de talento (sale más conveniente ir a trabajar afuera)

Respuesta	Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres):
No	La falta de un organismo especialista centralizado encargado de velar por la seguridad del estado. ej: NSA de EE.UU.
Sí	La falta de una cultura de ciberhigiene.
Sí	La oferta académica en pregrado, la visión de las instituciones educacionales, la inclusion de ramos en las carreras "cercanas" a tecnologías de la informacion
No	Lo que falta son compromisos con fechas y Políticas de Estado
Sí	Mayor difusión
Sí	N/A
No	No creo que falte nada de eso, pero si falta un organismo nacional a cargo del tema
No	No faltan especialista eso es un mito, hay muchos colegas cesante y en eso me incluyo, hago cursos, diplomado y saco certificiones pero de nada sirve
No	No queda claro el concepto de resiliencia.
No	No solo faltan profesionales o conciencia al nivel de personas, sino que no hay politicas concretas ni presupuesto ni proyectos de publico conocimiento asociados a la ciberseguridad.
Sí	Reorganizar el tema
Sí	Riesgo de sobretegulqcion
Sí	Se requiere tener un área transversal llamada CiberRiesgo, quien obligue a las instituciones a proteger sus sistemas.
No	Se vulneración de confidencialidad y datos personales para ser contactados en campañas políticas, publicitarias, ofrecer seguros, etc. No se sanciona el vulnerar nuestros datos personales.
Sí	Sin #LiderazgoDigital no hay cultura en ciberseguridad ni verdadera transformación digital.
No	Son puros cuentos np mas

Nivel de acuerdo con el texto “los cinco objetivos de la Política”

En el siguiente gráfico se muestra el nivel de acuerdo con la sección 1.3 de la propuesta de Política, consultado en la pregunta 3.



A continuación se incluyen las sugerencias de mejora al texto, sin filtrar ni editar, en orden alfabético:

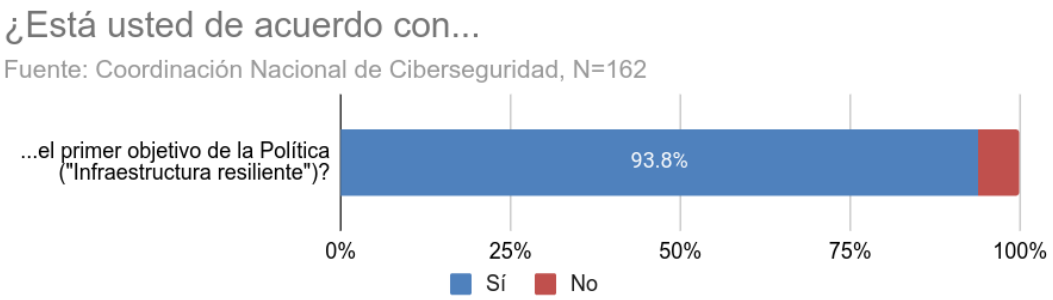
Respuesta	Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres):
No	" 2. Protección de las personas "
No	3.Cultura y educación en Materias de Ciberseguridad
No	Agregaría temas como, Generar o adoptar un estándar de seguridad de la información en el sector público.
Sí	Ante un ciberataque que sufra una empresa privada, este obligada a comunicar respecto al caso de forma precisa y oportuna a clientes y y organismos interesados que puedan verse afectados
Sí	Concientizar a las autoridades sectoriales
Sí	Creo que falta indicar la actualización de normas y leyes, para que pueda ser implementada por el poder judicial y endurecer penas, en aquellos casos que se detecte identidad de los ciberdelincuentes.
No	Creo que no se alinean con los desafíos, al menos no con el de talento ciber. Tampoco es tan claro que significa fomento a la Industria.
Sí	Creo que sería bueno añadir un elemento de "Obligaciones empresariales", el cual determine procedimientos que notificación de ataques o brechas de seguridad de cada compañía.

Respuesta	Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres):
Sí	Cuando se habla de cultura en ciberseguridad debemos tratar también educación en seguridad de la información en el sistema formal de educación privado y publico
No	Deberían plantearse como objetivos más concretos. Con un verbo claro.
Sí	Definición de principios guías de ciberseguridad para usuarios y empresas como marco referente, que estandaricen las medidas de protección mínimas a aplicar.
No	Derechos de las personas es un tema muy ancho para quedar restricto a una debate sobre ciberseguridad.
No	derechos y responsabilidades de las personas
Sí	diria cultura de ciberseguridad y privacidad de datos personales
Sí	Educación temprana en ciberseguridad (colegios), Política de gestión de datos personales tipo RGPD europeo.
No	Educación, inglés, espacios de prueba
Sí	En 2.2.3 agregar al final de la frase: ", y asegurar que las personas de todas las identidades de género tengan las mismas oportunidades y apoyo."
Sí	En el objetivo 3, se repite la protección de los derechos de las personas. Deberían destacar de forma más explícita las responsabilidades y deberes de las personas en contribuir a la ciberseguridad.
Sí	explicitar mejor la diferencia entre derechos y cultura
Sí	Falta educación y apoyo en educación en temas de ciberseguridad. Implementación junto con universidades e institutos en creación de carreras en e área.
Sí	Falto coordinación de las instituciones por áreas en temas de incidentes y amenazas
Sí	fiscalización a las instituciones publicas, para corroborar la aplicación de la PNCS y sus leyes asociadas.
No	Fomentar la educación en finanzas electrónica y seguridad informática. Luego sancionar los delitos informáticos. La ciberseguridad debe ser cultural y no sólo legal
Sí	fomento a la industria de ciberseguridad (especificar)
Sí	Fortalecer la educación y desarrollar contenidos para abordar los nuevos le guajes. Fortalecer contenidos integrales , porque el individuo es un todo y

Respuesta	Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres):
	funciona en redes.
No	Habilitar y potenciar el #LiderazgoDigital para construir una cultura de ciberseguridad. (la cultura es una consecuencia del trabajo de líderes, los cuales fomentan y lideren el cambio cultural)
Sí	Hay que considerar en el tema de Infraestructura resiliente los controles de acceso a las soluciones cloud. Las solcuiones cloud no ofrecen seguridad 100% sino más bien compartida.
Sí	identificar trabajo conjunto en temas de la UAF, Protección de datos personales, Sostenibilidad, Gestión de riesgos, Control Interno, etc
No	Inclusión de Ciberseguridad+Redes+Programación básica en el colegio. EDUCACIÓN!!!
Sí	La capacitación de las policías y ffaa
No	Le falta un cronograma con fechas y metas, en donde especifique claramente la Ejecución y no buenas intenciones.
No	Los objetivos deben presentarse en función al estado deseado, no en términos abstractos y meramente descriptivos.
Sí	Mas exigencias de seguridad al sector privado "fomento de la industria" agregaría establecer normativas básicas
Sí	N/A
No	No me interesa
No	No se aprecia concordancia entre los principales problemas y los objetivos enunciados
No	Porque es mentira en todo este periodo no se ha logrado nada de esto, solo se ha tramitado y no hay seguridad de la información y de nuestros datos
Sí	preferir de ser posible centros de datos en centros de datos en suelo nacional
Sí	Sanciones ejemplares para uso o usurpación de identidad
Sí	Sólo que el punto 2 DEBE ser Derechos y Deberes de las personas e instituciones
No	Tienen un orden de prioridad? Si es así, N° 1 cultura, siguiendo con derechos de las personas.
Sí	Transparencia en la gestión

Nivel de acuerdo con objetivo 1: Infraestructura resiliente

En el siguiente gráfico se muestra el nivel de acuerdo con el primer objetivo de la propuesta de Política, consultado en la pregunta 4.



A continuación se incluyen las sugerencias de mejora al texto, sin filtrar ni editar, en orden alfabético:

Respuesta	Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres):
Sí	"... bajo una perspectiva de gestión de riesgos y de constante reconocimiento de la superficie de amenazas."
Sí	Además, se requiere la implementación de estándares de seguridad sólidos y la actualización constante de nuestras defensas para adaptarse a las nuevas amenazas y desafíos en constante evolución.
Sí	Ampliar las atribuciones de CSIRT para regular a privados con relación estatal.
Sí	Asignar responsabilidades a los csirt sectoriales en temas de ciberseguridad.
Sí	Considerar capacitación a todo nivel, no sólo a los TI, a los Directivos. Considerar apoyar a las instituciones con RRHH especializado. Más cargos desplegados, no sólo al interior de los Ministerios.
Sí	Constate capacitación y preparación para los distintos equipos de trabajo en las TICs
Sí	Crear leyes que castiguen el delito de ataques
Sí	crear normas que obliguen a los privados a invertir en seguridad de la

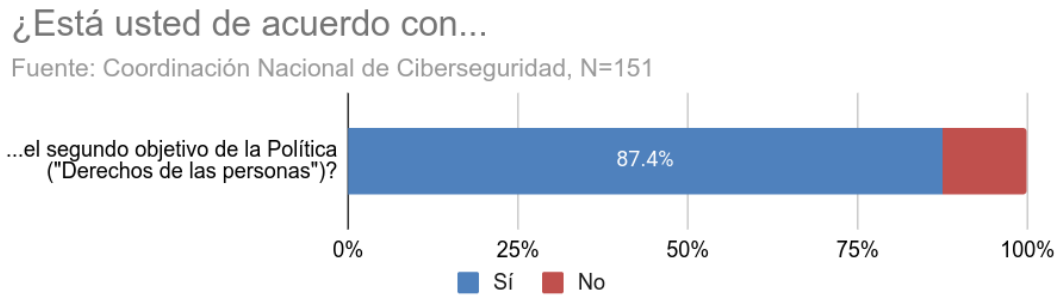
Respuesta	Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres):
	información y ciberseguridad, como así informar de brechas que sufrieran en ambos aspectos a la agencia del punto 1.
Sí	Crear un ente que genere respuesta pero también la inteligencia de amenaza, saber medir cómo debo abordar los espacios de acuerdo a los niveles de exposición que tenemos
Sí	Crear una red de CSIRTs sectoriales: Sector Financiero, Minería, Educación, etc... Inversión no solamente en investigación pero también en innovación en ciberseguridad.
No	Creo debiera estar bajo el alero de la ANI/ ANID, para poder usar eficientemente los recursos ya disponibles
Sí	Creo que debe haber una especial preocupación del punto número 5
Sí	Creo que establecer y explicitar la colaboración como objetivo posibilita mucha de las acciones que se están proponiendo en el documento y sus objetivos.
Sí	el nro 5 sobra el "a través de", ya que para monitorear y analizar se debe efectuar una serie de medidas y la inversión en investigación científica aplicada es muy indirecta
Sí	En el 4, añadiría la resiliencia "lógica" además de la física; no obstante podría subentenderse del 3. También lo extendería no solo a la red sino que a servicios escenciales para la red y la sociedad
Sí	Establecer mecanismos que permita compartir especialmente indicadores de compromiso de manera temprana.
Sí	Falta el verbo coordinar, el monitoreo es caro y si se detectan riesgos deben ser compartidos y coordinadas acciones de prevención o mitigación, ya existe un csirt pero no coordina ni apoya
Sí	fortalecer desde la infancia la conciencia de la ciberseguridad
Sí	Fortalecer fiscalías en cibercrimen
Sí	Fortalecer la formación técnica del personal encargado de la infraestructura publica, mediante un plan de capacitación permanente.
Sí	Fundamental que la Agencia Nacional de Ciberseguridad tenga autonomía del poder ejecutivo.
Sí	Generar un esquema que establezca los requisitos mínimos según

Respuesta	Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres):
	sector
No	Incentivar y Desarrollar una industria de Ciberseguridad nacional, privada, capaz de entregar soluciones robustas como israel
Sí	infraestructura no se alinea con lo que actualmente contiene el proyecto de ley, que eliminó esta palabra y ocupa otras nomenclaturas. Debiese incluirse el talento y la retención del mismo
Sí	Investigación de las universidades y a través de anid investigación en la materia
No	IR foco a soluciones on promise, hoy % clave de empresas tienen nube. Más que una agencia se deben tener regulaciones que las empresas deben cumplir. ejemplo en salud en HIPAA. o la iso 27001, 22301
Sí	La ANI debe ser con gente experta y no con cupos politicos
No	Le faltan fechas, indicar cobertura, capacidad técnica instalada y objetivos a Cumplir con fechas. Del decir al hacer aquí hay mucha distancia.
Sí	Legislar en sanciones
No	leyeron la iso? o esto es solo para el papel?, porque ya hay un csirt, la insfraestructura critica por defecto debe ser resilente. entonces se explica con manzanas?
Sí	Me parece bien el texto, no le haría cambios.
Sí	N/A
No	Ninguma sigan asi no mas
No	No se entiende "red" de qué: "Fortalecer la resiliencia física de la red en Chile." No es sólo la red (si fuese la de telecomunicaciones). Son los "activos" si quieren hablar de gestión del riesgo.
No	No se hace cargo especificamente de la privacidad de datos
Sí	Organismo fiscalizador e independiente que asegure derechos
Sí	Pero falta especificar equipos a nivel regional. No centralizado solamente.
Sí	Que sean independientes del Ministerio del interior.
Sí	Resiliencia debe anticiparse a cambios e innovar. No sólo incidentes y desastres sino evolución tecnológica y social. Pto2 destacar los CSIRT Sectoriales y de cada organización.

Respuesta	Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres):
No	Sólo el 5 el resto NO sirve. Hay que invertir en tecnología y permitir a los organismos técnicos del estado el cruce de datos comerciales, como lo hacen el SII, Fonasa y otros.
Sí	Una Ley que obligue a las empresas contar con algun nivel de madurez en la gestion de ciberseguridad
Sí	y capacitar a los privados
Sí	y la infraestructura del país también, puentes, suministro de agua, electricidad, etc.

Nivel de acuerdo con objetivo 2: Derechos de las personas

En el siguiente gráfico se muestra el nivel de acuerdo con el segundo objetivo de la propuesta de Política, consultado en la pregunta 5.



A continuación se incluyen las sugerencias de mejora al texto, sin filtrar ni editar, en orden alfabético:

Respuesta	Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres):
Sí	¿Corresponde hablar de "disidencias sexogenéricas"? ¿No basta con "diversidad sexual"?
Sí	"otorgando especial protección a mujeres, niñas, niños, jóvenes, personas de la tercera edad y disidencias sexogenéricas" es perjuicio para quienes no

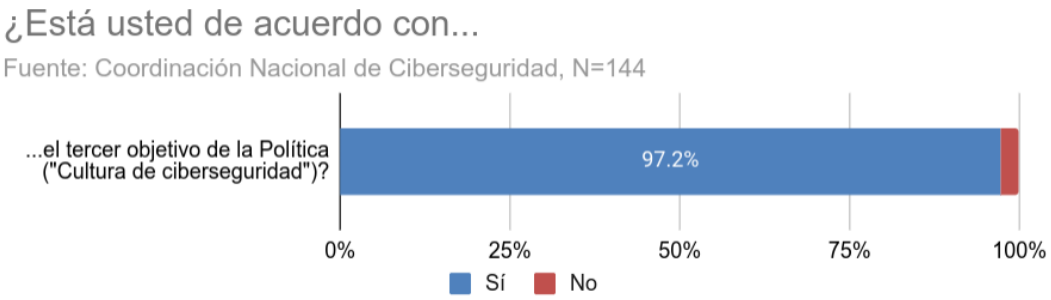
Respuesta	Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres):
	están, en esta redacción, incluidos.
No	1 sí. 2, la educación digital y en seguridad informática debe ser transversal y desde la escolaridad, no sólo a los empleados públicos. 3, otra estupidez que segrega aún más. 4 sí. 5, imposible.
Sí	2 no lo restringas a públicos. Así como se desarrolló una política de concientizacion de uso de cinturones de seguridad, necesitamos una para la ciberseguridad
No	Cero
Sí	como mantener internet como un espacio seguro, como se protege de los ciber delincuentes
Sí	Creo que el primer objetivo es conocer el estado del arte en estas materias y luego promover un plan sectorial de implementación de medidas.
No	de que sirve esto, si al final las empresas se pasan las DB, asi como todo ya es publico con nombre y rut, volante o maleta?... no se quien autorizo eso..
Sí	Debería haber una declaración de derechos y deberes, se piensa que el estado regula estás cosas
Sí	derecho a no ver publicidad y contenido dañino para menores de edad (NNA), para promover una educación libre de ese contenido.
Sí	Derechos y deberes, personas e instituciones, 1) sumar CIP; 2) y 3) para todas las personas (indep sexo, raza, etnia); 4) .. empresas...
Sí	Educación en materia de protección de datos personales y conductas riesgosas en el uso de redes informáticas en la educación primaria, secundaria, técnica y universitaria
No	El incluir a la "mujer" creo que esta de mas... es una persona igual que todos y tiene los mismos derechos que un hombre, se debería optar mas por la meritocracia que el favoritismo.
Sí	el obj 3 es muy forzado, la inclusión en este caso no es un tema de sexo, es de educación y cultura, nivel socioeconómico, ubicación geográfica, etc. que son transversales a los sexos.
Sí	El párrafo 2 comenta sólo capacitar al sector público, y creo qué hay que abordar la sensibilización a nivel pais, llegar al sector privado y todo ciudadano que tenga acceso a estas capacitaciónes.
No	El punto 1 no debería incluir "y de ciberseguridad". Esto confunde el

Respuesta	Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres):
	propósito de ese punto.
No	el punto 2, no debe discriminar, ya que el sector privado, por ser privado no significa que no necesiten capacitación o que tenga los recursos como las pymes
Sí	En el punto 3, agregar: y asegurar que las personas de todas las identidades de género tengan las mismas oportunidades y apoyo.
Sí	en la frase "Generar instancias de capacitación para todos los funcionarios públicos en y en hábitos" falta algo, dice "en y en hábitos"
Sí	En relación al punto cuatro generar espacios y obligaciones para que los ISP puedan cumplir con lo mandato por ley para preservar información que permita esclarecer una delito.
Sí	Estas acciones deben tener difusión y seguimiento no sólo por género
Sí	falta contratar empresas expertas para que realice asesoría al Estado y puedan revisar las falencia que tiene, ademas de cambiar personas del Estado no solo capacitarlas hay que cambiarlas
Sí	Generar instancia de participación público-privadas
Sí	Generar las condiciones en la formación de los profesores para enseñar la ciberseguridad de forma temprana en los colegios, para generar una cultura nacional fuerte en el tema.
Sí	hábitos y medidas básicas en ciberseguridad, los reemplazaría por el concepto de ciberhigiene, el cual debemos posicionar.
No	Identificar y corregir inequidades de acceso al ciberespacio, no es algo que pueda ver el estado entendiendo que los isp son en su mayoría privados.
No	la capacitación debería ser para todas las personas, no solo empleados publicos
Sí	La N°3 está pobremente redactada. "La mujer" en singular y referencia a "todo el quehacer de protección..." requieren de edición, comunican pobremente. La 5 parece fuera de lugar.
Sí	La protección debe ser igual para todos, no con mayor protección a ciertas partes de la sociedad. Todos tenemos los mismos derechos.
No	Las capacitaciones no debieran ser solo para empleados públicos, en Chile la mayoría no somos empleados del sector público sino que del privado, por ende la invitación debiera ser abierta

Respuesta	Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres):
Sí	Limitar quien va a las capacitaciones es contraproducente, dado que la ciberseguridad nacional la hacemos todos en el país. MAKE CYBERSECURITY OPEN SOURCE
No	Los funcionarios públicos debiesen ser contratados teniendo en mente las exigencias de ciberseguridad, no formar a aquellos que por años no han tenido el interés de hacerlo.
No	Me tiene aburrido meter temas de género en temas transversales a la sociedad, falta que tengan agua y luz para distintos generos (asi de ridículo suena)
Sí	N/A
No	Nada es infalible, habrá casos en que se filtren datos personales ¿las empresas/organizaciones o funcionarios serán los últimos responsables? y los delitos deben tener sanciones altas
Sí	No se entiende el énfasis por la mujer y no por los NNA. Una política basa en protección de derechos debería ya superar la protección de datos y pensar en otro tipo de regulaciones x ej la IA.
Sí	No solo funcionarios públicos. Una mirada más amplia. Reconocer el rol del sector privado
Sí	nuevamente falta en la educación formal iniciativas de educación en la protección de datos personales a nivel de comunidad educativa: alumnos, docentes y apoderados
Sí	Plan de concientización nacional sobre ciberseguridad iniciando por escuelas
Sí	Promover la "alfabetizacion digital" a todos los sectores de la sociedad
No	que sucede con las personas neurodivergentes?
Sí	Realizar minicursos de ciberseguridad obligatorios para los funcionarios cada cierto tiempo
Sí	se debe incluir la privacidad de los datos personales
Sí	Siempre mantener alternativas reales y no tecnológicas para quienes opten por el no el uso de la tecnología
No	Sugerencia de hacer el debate de privacidad y porteccion de datos personales en un momento distinto del debate sobre ciberseguridad

Nivel de acuerdo con objetivo 3: Cultura de ciberseguridad

En el siguiente gráfico se muestra el nivel de acuerdo con el tercer objetivo de la propuesta de Política, consultado en la pregunta 6.



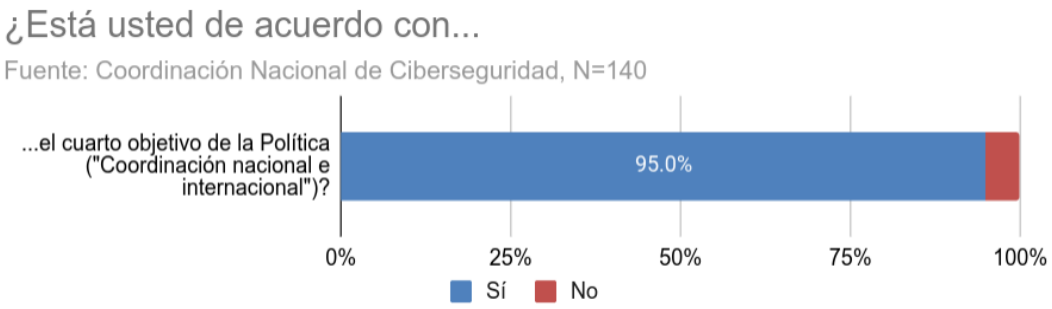
A continuación se incluyen las sugerencias de mejora al texto, sin filtrar ni editar, en orden alfabético:

Respuesta	Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres):
Sí	Reemplazar higiene digital por ciberhigiene; complementar con la difusión de buenas practicas en materia de ciberseguridad
Sí	"Este programa se enfocará especialmente en [...]" No veo cómo les pueda jugar a favor políticamente este texto. Esos grupos tienen más oportunidades de sufrir ataques, eso sí.
Sí	1er parrafo: Esta cultura deberá ser inclusiva y accesible, asegurando que individuos de todas las edades y niveles de habilidad digital puedan entender y adoptar comportamientos seguros en línea
No	3 Fomentar una cultura de evaluación y gestión del riesgo QUE INCLUYA CIBERSEGURIDAD, tanto en organizaciones públicas como privadas.
Sí	Algunas instituciones publicas, el RRHH de TI es muy escaso. Y la gestión de riesgo pasa a ser apagar incendios. No hay suficiente inversión en TI para renovar o invertir en seguridad.
Sí	Asegurar que sea agnóstica a la contingencia política e influencia en los pensamientos de ideologías
Sí	Asignar recursos y tecnología para educar a todos y monitorear la red. NO crear nuevos servicios públicos al servicio de los políticos de turno.
No	cultura parte desde la niñes,

Respuesta	Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres):
Sí	el obj 4 es más investigación, desarrollo e innovación tecnológica, más que científica
Sí	El plan debe ser curriculum obligatorio en las escuelas.
Sí	El plan en materia de privacidad debiese ser coordinado con las entidades que correspondan.
Sí	El texto requiere de edición para que sea más neutro en términos de género "todOs nosotrOs" - "cada unO"
No	en el punto 2: Me parece que en los entornos universitarios también se debe trabajar
Sí	Especialmente incluir en la malla educacional un ramo o taller sobre ciberseguridad desde temprana edad.
Sí	Fomentar la innovación en ciberseguridad (no solamente la investigación), a través de proyectos CORFO específicos.
Sí	Hay una brecha en la educación, con un modelo atrasado, se debería trabajar eso primero
Sí	idem al anterior. Es necesario evaluar y luego diseñar e implementar los planes. En términos de optimización hay diferencias.
Sí	incluir en la oferta académica a temprana edad educación en tecnologías y ciberseguridad.
Sí	Incluir talleres de Ciberseguridad en el currículo escolar medio- mayor y superior
Sí	Integrar noción de gestión y normalización de "Competencias digitales y de ciberseguridad"
Sí	Inyectar presupuestos a empresas emergentes para aumentar oferta en el mercado
Sí	Me parece bien el texto.
Sí	N/A
Sí	Partir en los colegios con temas, ramos en la U. Hoy hay Riesgo info de los ministros, diputados y senadores..curso especial
Sí	pero ingresar recursos y capacitacion
No	punto 2 hay un nivel generacional y acceso a internet importante, no es solo por tipo de enseñanza
Sí	Quita seriedad de la política incluir disidencias sexogenéricas. No tienen ninguna desventaja frente al resto de la sociedad en materia de ciberseguridad. Sería mejor incluir zonas rurales.
Sí	Un plan de concientización de la privacidad de nuestros datos personales

Nivel de acuerdo con objetivo 4: Coordinación nacional e internacional

En el siguiente gráfico se muestra el nivel de acuerdo con el cuarto objetivo de la propuesta de Política, consultado en la pregunta 7.



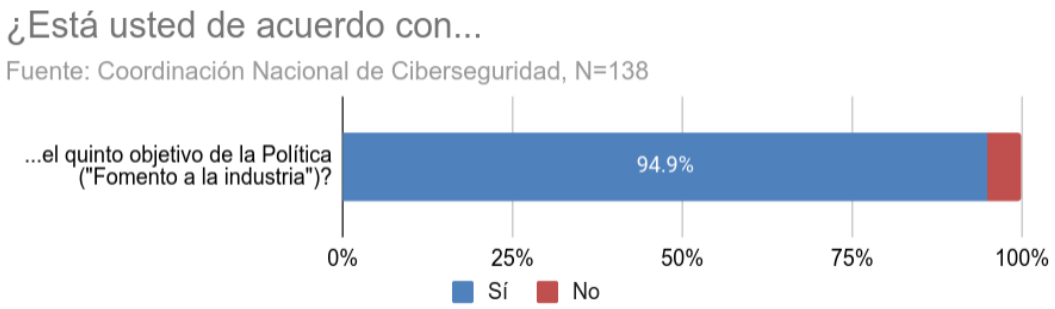
A continuación se incluyen las sugerencias de mejora al texto, sin filtrar ni editar, en orden alfabético:

Respuesta	Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres):
Sí	.- 2) "eliminar" lo de países avanzados y dejarlo "abierto". .- Velar por la "consistencia" de los marcos normativos desarrollados (Caso trágico, el sector eléctrico nacional)
No	"Coordinación nacional" es toda la política, no es necesaria aquí. Falta prevenir conflictos en el ciberespacio. La "ciberdiplomacia" requiere más contexto (quizás lo tiene en otra parte).
Sí	abrir la legislación para perseguir los ciber-delitos internacionalmente
Sí	Asegurar que en la supervigilancia no se pierdan libertades y derechos
Sí	considerar organizaciones del asia pacifico y europa tambien
Sí	Creación de comité Nacional
Sí	Cuidando celosamente la privacidad y dignidad de las personas.
No	debe generarse una entidad coordinadora publico privada que canalice las instancias de colaboración en vez de tener iniciativas dispersas. la ciberdiplomacia es un concepto englobado en el punto 3,
Sí	En general se debe generar más participación con países aliados, en cómo

Respuesta	Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres):
	desarrollar e implementar tecnologías de seguridad
Sí	Establecer un centro de inteligencia publica de ciberseguridad. (OSINT)
Sí	falta mencionar rol de sociedad civil organizada
Sí	Incentivar la creación de una instancia de cooperación en el ámbito de la OEA siguiendo el modelo de la ENISA europea.
Sí	Incorporar la debida diligencia con la responsabilidad que se tiene referente a enfrentar los nuevos desafios, las incidencias y tener la forma de responder
No	Intercambio de información con organismos técnicos y de seguridad ya se hace. el resto es politiquería no más.
Sí	la ciberseguridad es una sola, tenemos que estar coordinados con otros paises para enfrentar la ciberdelincuencia
Sí	La cooperación es un medio para lograr objetivos y no un objetivo en si misma
Sí	Muy bien, la idea es avanzar en paralelo en Latinoamérica y el mundo.
Sí	N/A
Sí	Punto 4 agregar: ... y fomentar el desarrollo de acuerdos y tratados internacionales que refuercen la ciberseguridad y el respeto a los derechos humanos en el ciberespacio."
No	Se debe aclarar que toda coordinación internacional debe pasar por el Ministerio de Relaciones Exteriores. El punto 4 restringe la dimensión internacional de la ciberseguridad a solo un aspecto.
Sí	Se debiese crear un consejo asesor sobre diplomacia pública digital.
Sí	Todo debe ser con expertos y no cupos politicos
Sí	ya existen acuerdos, lo malo es que chile hace las cosas a la chilena, ejempli iso, chile saca su version chilean way nch----

Nivel de acuerdo con objetivo 5: Fomento a la industria

En el siguiente gráfico se muestra el nivel de acuerdo con el quinto objetivo de la propuesta de Política, consultado en la pregunta 8.



A continuación se incluyen las sugerencias de mejora al texto, sin filtrar ni editar, en orden alfabético:

Respuesta	Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres):
Sí	2.- ... no sólo tecnológico.. sino de servicios, modelos, metodologías
No	Agregar "privacidad" en cada uno de los 4 puntos. Esto es un tema aparte de "ciberseguridad"
Sí	Añadiría cierta orientación del sistema normativo para que confluya la productividad de la mano con el respeto a la privacidad y, en general, a la ciberseguridad.
Sí	benefios tribitarios para emrpresas que creen soluciones. Paquetes de becas para integración, cursos con empresas eeuu. Exigir una linea base al estado
Sí	Capacitar activamente a emprendimientos en ciberseguridad
Sí	Cómo pais no hay una industria en el área solo vendedores de tecnología, se debería fomentar a las empresas de desarrollo a entrar en el campo
Sí	Crear el Instituto Nacional de Ciberseguridad Inciber. Generar certificaciones de software y de empresas en ciberseguridad según el modelo de la ANSSI en Francia.
Sí	Crear sellos de ciberseguridad para Empresas de prestación de servicios TI
No	El estado debe promover la manufactura que es la que mueve al país. La ciberseguridad es un "must" y no se promueve: se utiliza porque es necesario.
Sí	en el punto 1 creo que es mas rápido robustecer a la academia actual que crear nuevos entes
No	Esto debiera dejarse a la libre empresa
Sí	evitar el humo y los reportes de alto nivel
Sí	evitar sobre proteccionismo, buscar especialización en cluster temáticos. Por ejemplo ciberseguridad en la mineria

Respuesta	Si tiene sugerencias de mejora para el texto, por favor indíquelas acá (máximo 200 caracteres):
Sí	Excelente
Sí	Falta más articulación entre investigación académica y emprendimiento - en el fondo cómo articulamos 1 y 2. La N°3 no se entiende bien en este contexto.
Sí	Fomentar e integrar a la, sociedad civil organizada. Facilitar acceso a la información a fundaciones.
No	La creación de institutos de investigación es inncesaria, se deben potenciar las UES y CFT. Se debe promover el usos de soluciones nacionales, dando beneficio tributario a los usuarios.
Sí	Me parece bien el texto, inclusivo.
Sí	N/A
Sí	No, creo que no hay cultura ni objetivos.
No	objetivos versus medios se siguen mezclando. La industria de ciberseguridad sirviendo "objetivos estratégicos o protegiendo personas y organizaciones no es claro
Sí	Que el estado de Chile cree un fondo de becas para la educación y capacitación en Ciberseguridad
Sí	Reglas claras y controles que eviten la concentración de poder

4. Conclusiones

En general, el grado de acuerdo con los textos propuestos es alto. En la mayor parte de ellos, el grado de acuerdo es superior al 90%. El nivel más bajo de acuerdo se dio con el texto propuesto para el objetivo 2, “Derechos de las personas”.

Con la finalidad de comprender las sugerencias de mejora del texto recibidas, se generó un “diccionario” (*codebook*) con el que se clasificaron los comentarios en diez categorías arbitrarias. Luego de acordar un diccionario, tres analistas categorizaron cada comentario. El proceso no fue realizado independientemente pero sí de forma consensuada.

El siguiente fue el diccionario acordado:

- **Coordinación:** Relativo a la necesidad de generar instancias entre organizaciones para gestionar temas específicos.
- **Cultura:** Referente a la generación de conocimientos, ideas y costumbres que sería necesario adquirir.
- **Derechos de las personas:** Toda aquella referencia a las garantías y libertades de la población.
- **Educación:** Abarcando la temática desde el nivel preescolar hasta el universitario.
- **Especialización:** Entendiéndose como una mayor necesidad de mejorar las capacidades de los profesionales.
- **Gestión del riesgo:** En vinculación a la administración del riesgo y su mitigación.
- **Gobernanza:** Menciones a la necesidad de que las autoridades se involucren en temas específicos de la vinculación entre Estado, sociedad civil y sector privado.
- **I+D:** Toda mención relativa a investigación y desarrollo.
- **Inversión:** Referencias sobre algún requerimiento de mayor financiamiento.
- **Regulación:** Comprendiendo toda remisión a ámbitos normativos y legales.

Cada comentario recibido fue clasificado en una o más categorías. La tabla siguiente indica el número de menciones por categoría, y la proporción de comentarios que mencionaron dicha categoría. La tabla está ordenada de mayor a menor número de menciones. Dado que cada comentario puede haber sido categorizado en más de una categoría, la cantidad de menciones suma más que un 100%.

Categoría	Número de menciones	Proporción de menciones sobre total de comentarios
Regulación	65	34.9%
Educación	34	18.3%
Especialización	28	15.1%
Coordinación	18	9.7%

Categoría	Número de menciones	Proporción de menciones sobre total de comentarios
Inversión	16	8.6%
Derechos de las personas	15	8.1%
I+D	10	5.4%
Cultura	9	4.8%
Género	9	4.8%
Gestión del riesgo	7	3.8%
Gobernanza	6	3.2%
Canales de denuncias	1	0.5%
Total	**186**	

Lo anterior puede ser presentado de forma visual a través de una nube de palabras:

En general, puede interpretarse de lo anterior que un 34,9% de los participantes de la consulta quieren contar con una mayor regulación en ciberseguridad, por sobre lo incluido en la política; un 18,3% sobre educación, y un 15,1% sobre especialización. En consecuencia, el texto se modificó para enfatizar especialmente estos temas, y se incluirán medidas pertinentes en el plan de acción de la Política.