

Publican Política Nacional de Ciberseguridad 2023 – 2028

El lunes 04 de diciembre, se publicó en el Diario Oficial el Decreto N°164/2023, del Ministerio del Interior y Seguridad Pública que aprueba la Política Nacional de Ciberseguridad que regirá durante el período 2023 – 2028, reemplazando a la Política anterior, publicada el día 28 de enero del 2017, que rigió entre ese mismo año y 2022.

La nueva Política se dicta con el propósito de guiar las actuaciones del Estado en el ámbito de la ciberseguridad, estableciendo un plan de acción, metas y objetivos con el fin de abordar los múltiples desafíos y obstáculos que enfrenta el país en este campo. Estos desafíos incluyen el incremento de delitos cibernéticos, la vulnerabilidad de la infraestructura y otros problemas relevantes en el ciberespacio.

Las novedades e innovaciones que contiene la nueva Política, en comparación con la anterior, dicen relación con: (i) las medidas específicas para abordar los objetivos principales; (ii) la inclusión de dimensiones transversales; y (iii) la relación con otros objetivos nacionales.

Objetivos particulares de la Política

Para abordar las problemáticas nacionales señaladas en relación con la ciberseguridad, la nueva Política aborda cinco objetivos principales: a) infraestructura resiliente; b) derechos de las personas; c) cultura de ciberseguridad; d) coordinación nacional e internacional; y e) fomento a la industria e investigación científica. Tales objetivos no difieren de los enumerados por la anterior Política de Ciberseguridad, pero sí tienen innovaciones, específicamente con respecto a las medidas particulares para abordar cada objetivo, las que se señalan a continuación.

****1) Infraestructura resiliente****

La Política busca fortalecer los elementos técnicos, físicos y lógicos del

ciberspacio, para lo cual considera indispensable:

- Impulsar la tramitación del proyecto de ley marco sobre ciberseguridad e infraestructura crítica de la información, que crea la Agencia Nacional de Ciberseguridad.
- Fortalecer el análisis de la información de red en el ciberespacio, a través de la inversión en investigación científica aplicada.

****2) Derechos de las personas****

La Política busca que todas las personas puedan hacer uso de internet para sus distintos fines, en un entorno de equidad, inclusión, justicia y protección a la diversidad. Para lo cual estima necesario:

- Fortalecer el marco normativo sobre protección de datos personales, a través de la aprobación e implementación del proyecto de ley respectivo.
- Generar instancias de capacitación para los funcionarios públicos en hábitos y medidas básicas de seguridad digital.
- Prevenir la comisión de delitos informáticos.
- Identificar y corregir inequidades en el acceso y uso del ciberespacio producidas por la falta de conocimiento de seguridad digital.

****3) Cultura de ciberseguridad****

La Política busca desarrollar una cultura de ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales, para tal efecto, se estima necesario:

- Diseñar e implementar un plan de concientización nacional sobre ciberseguridad y privacidad.
- Generar e implementar un plan matriz de introducción y mejora en la educación en ciberhigiene y ciberseguridad para el sistema de enseñanza entre sus niveles básico a medio.
- Fomentar una cultura de evaluación y gestión del riesgo en las organizaciones.
- Promover la investigación científica aplicada en ciberseguridad para resolver los futuros problemas que enfrente el país.

****4) Coordinación nacional e internacional****

La Política impulsa la colaboración entre organismos públicos y privados junto con otros sectores gubernamentales y la industria, en conjunto con la futura

autoridad nacional de ciberseguridad. Con este fin, la política subraya la importancia de:

- Generar instancias de colaboración y cooperación entre organizaciones públicas y privadas en diversos ámbitos.
- Establecer relaciones de cooperación con instituciones de ciberseguridad de países avanzados en el área.
- Promover activamente la ciberdiplomacia.
- Coordinar la política internacional en materia de ciberseguridad.

5) Fomento de la industria y la investigación científica

Finalmente, la Política promueve el desarrollo de una industria de ciberseguridad, a través de:

- La focalización de la investigación aplicada respecto de aquellos problemas en ciberseguridad.
- La generación de incentivos para el emprendimiento tecnológico en ciberseguridad.
- La revisión de mecanismos de contratación de servicios de ciberseguridad por parte del Estado.
- La promoción de productos y servicios de empresas locales en ciberseguridad a nivel nacional e internacional.
- El fomento a la integración e inclusión de una transversalización de género en el desarrollo del ecosistema de ciberseguridad.

****Dimensiones transversales****

Un elemento nuevo en relación con la política anterior es el establecimiento de cuatro dimensiones transversales, que se deben considerar en todas las iniciativas de protección y promoción de los derechos de las personas:

- Equidad de género
- Protección de la infancia
- Protección al adulto mayor
- Protección del medio ambiente

****Relación con otros objetivos nacionales****

La nueva Política, a su vez, considera otras tres políticas que se han dictado por parte del ejecutivo, para abordar objetivos de carácter nacional: a) Política de ciberdefensa; b) Política Nacional de Inteligencia Artificial; y c)

Política Nacional contra el crimen organizado.

La Política de Ciberseguridad señala estar en estrecha armonía con estas últimas, en particular, por centrarse en la planificación y regulación de las tecnologías en general, donde la ciberseguridad encuentra gran relevancia.

Autores: Guillermo Carey; José Ignacio Mercado