



Gobierno de Reconciliación
y Unidad Nacional

El Pueblo, Presidente!



Propuesta de
**Plan de Acción de la Estrategia
en Ciberseguridad.**

INTRODUCCIÓN

- La ciberseguridad tiene un campo de aplicación transversal a todas las actividades que hacen uso de las tecnologías de la información y la comunicación en el país.
- El Plan de acción refuerza el desarrollo estratégico del país en materia de ciberseguridad, que tiene como objetivo la protección de los derechos de los ciudadanos y a la sociedad en general en el uso seguro y confiable del ciberespacio.
- El presente Plan de Acción, en concordancia con la Estrategia Nacional de Ciberseguridad, tiene un período de ejecución 2020-2025.

EJES ESTRATÉGICOS



1. FORTALECIMIENTO INSTITUCIONAL

1. Creación del Consejo Nacional de Ciberseguridad (CNC).
 2. Constituir el Órgano Administrativo y Técnico de las TICs.
 3. Creación de un equipo de respuesta a incidentes de seguridad informática (CSIRT).
 4. Establecer protocolos de cooperación, intercambio de información a nivel nacional e internacional en materia de Ciberseguridad.
- Tiempo de ejecución: Entre I y II Trimestre 2021.
 - Responsables: Presidencia, PN, EN, MINREX, TELCOR, ENATREL, UNI.

2. FORTALECIMIENTO DEL MARCO JURÍDICO

1. Actualizar el marco jurídico en materia de Ciberseguridad.
 2. Suscribir acuerdos y convenios para fortalecer la cooperación internacional en materia de Ciberseguridad.
 3. Establecer políticas, protocolos y normativas en la gestión de riesgos considerando los estándares de la industria de ciberseguridad.
- Tiempo de ejecución: II Trimestre 2021 - II Trimestre 2022.
 - Responsables: CSJ, PN, EN, MINREX, TELCOR, ENATREL, UNI, SIBOIF, MHCP, CONAMI.

3. FORMACIÓN Y CAPACITACIÓN

1. Elaborar un plan de formación en ciberseguridad en las instituciones del Estado.
 2. Establecer mecanismos de colaboración entre Estado, instituciones académicas y empresa privada para llevar a cabo capacitaciones en temas de ciberseguridad.
 3. Implementar programas de capacitación dirigido al sistema educativo nacional.
 4. Diseñar e implementar estrategias de concientización en el uso responsable y seguro de las TICs.
- Tiempo de ejecución: 2021- 2025.
 - Responsables: Consejo Nacional de Educación, CNC, CNIT (INATEC).

4. FORTALECIMIENTO TECNOLÓGICO

1. Definir e implementar las plataformas para la prevención, detección y respuesta a ciber incidentes en las instituciones del Estado.
 2. Establecer programas de apoyo especializados en investigación y desarrollo e innovación en ciberseguridad.
 3. Diseñar políticas de uso, protección y aprovechamiento de propiedad intelectual derivadas de la investigación en materia de ciberseguridad.
- Tiempo de ejecución: 2022 - 2025.
 - Responsables: CNC, Órgano Administrativo y Técnico, CSIRT-país, Entes reguladores del estado, MIFIC, CONICYT, CNIT (INATEC).

5. SEGURIDAD Y RESILIENCIA DE LOS SERVICIOS E INFRAESTRUCTURAS CRÍTICAS A NIVEL NACIONAL

1. Establecer un sistema de información para la reacción y retroalimentación de estrategias para la gestión de riesgos.
 2. Elaborar un inventario de servicios e infraestructuras críticas a nivel nacional.
 3. Realizar un análisis de amenazas, riesgos y vulnerabilidades de los servicios, sistemas de información e infraestructuras críticas del país.
 4. Crear mecanismos de procedimientos para la mitigación y restauración de los servicios e infraestructuras críticas.
- Tiempo de ejecución: 2022- 2025.
 - Responsables: Órgano Administrativo y Técnico, CSIRT- país.



Gobierno de Reconciliación
y Unidad Nacional

El Pueblo, Presidente!

CONSULTAS