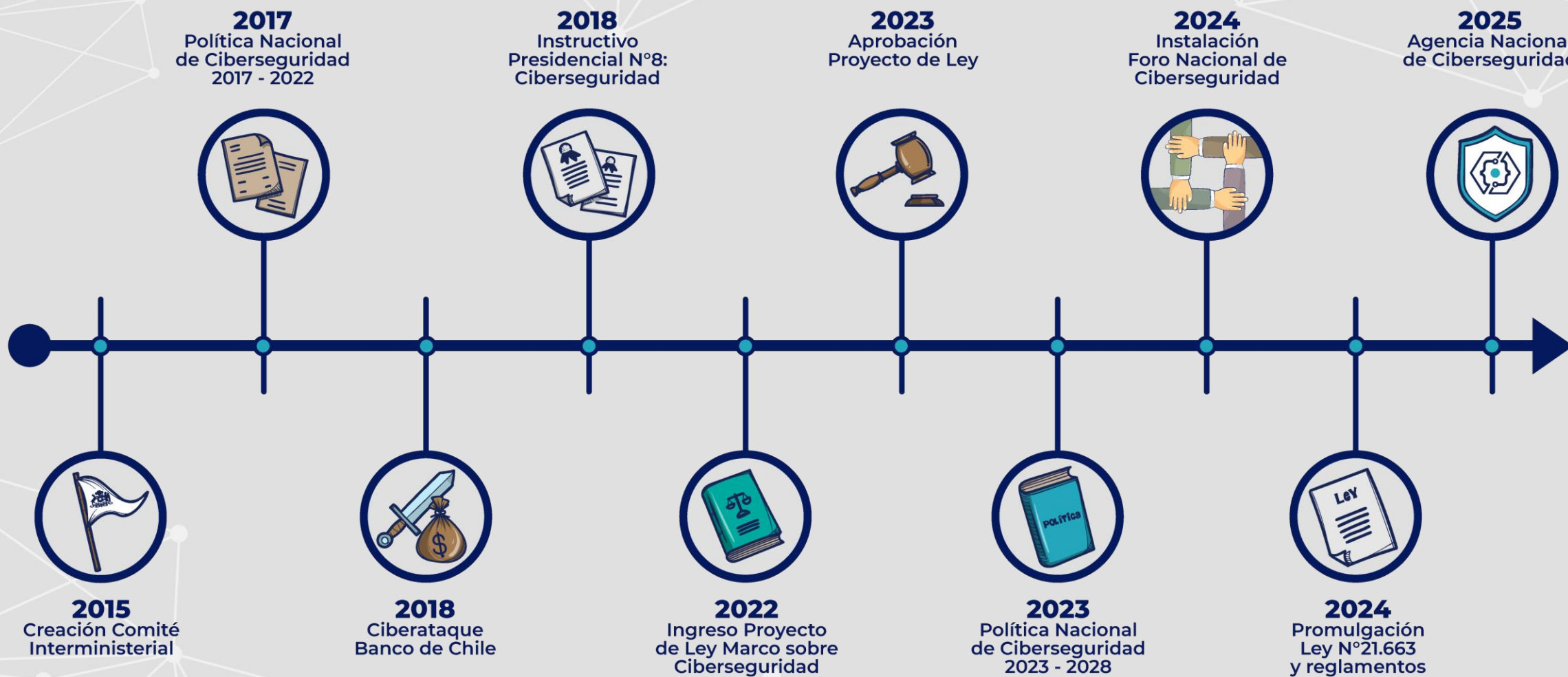




CIBERSEGURIDAD EN CHILE ESTRATEGIA E IMPLEMENTACIÓN

Dr. Daniel Álvarez Valenzuela
Director Nacional



The background of the image is a dark blue gradient. It features a network diagram composed of numerous small, light blue dots (nodes) connected by thin, light blue lines (edges). These nodes and lines are primarily concentrated in the top-left and bottom-right corners, creating a sense of connectivity and digital infrastructure. The central area of the image is a solid dark blue, providing a high-contrast background for the white text.

AGENCIA NACIONAL DE CIBERSEGURIDAD

Agencia Nacional de Ciberseguridad



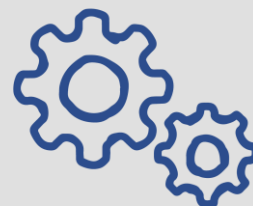
Servicio público de carácter técnico y especializado, funcionalmente descentralizado y dotado de personalidad jurídica y patrimonio propio.



Asesorar al Presidente de la República en materias propias de ciberseguridad



Colaborar en la protección de los intereses nacionales en el ciberespacio



Previene, gestiona y responde a ciberataques e incidentes de ciberseguridad de impacto significativo



Velar por la protección, promoción y respeto al derecho a la seguridad informática



Norma, supervisa, fiscaliza y sanciona al sector público y privado en materia de ciberseguridad



SISTEMA DE NOTIFICACIÓN DE INCIDENTES

Servicios esenciales son:



- Ministerios
- Delegaciones presidenciales regionales y provinciales
- Gobiernos regionales
- Municipalidades
- Fuerzas Armadas
- Fuerzas de Orden y Seguridad Pública
- Empresas públicas creadas por ley
- Coordinador Eléctrico Nacional
- Órganos y servicios públicos creados para el cumplimiento de la función administrativa.
- Empresas del Estado y sociedades con participación accionaria superior al 50% o mayoría en el directorio.

Servicios esenciales son:



- Generación
- Transmisión
- Distribución eléctrica



- Transporte
- Almacenamiento
- Distribución de combustible

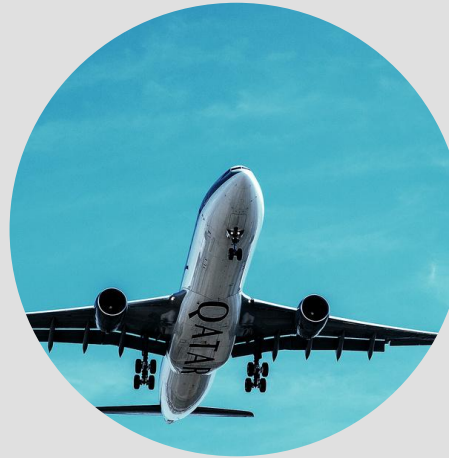


- Suministro de agua potable
- Saneamiento

Servicios esenciales son:



- Servicio de telecomunicaciones
- Servicios digitales
- Servicios de infraestructura digital
- Servicios de tecnología de la información gestionada por terceros



- Transporte Terrestre
- Transporte aéreo
- Transporte ferroviario
- Transporte marítimo
- Operación de la infraestructura respectiva



- Banca
- Servicios financieros
- Medios de pago

Servicios esenciales son:



- Prestación institucional de salud:
Hospitales, clínicas, consultorios y centros médicos
- Producción y/o investigación de productos farmacéuticos.
- Administración de prestaciones de seguridad social.
- Servicios postales
- Servicios de mensajería

¿Qué se debe reportar?

Se considera un incidente de ciberseguridad de efecto significativo, cuando pueda:

- Interrumpir la continuidad de un servicio esencial.
- Afectar la integridad física o la salud de las personas.
- Afectar la integridad o confidencialidad de activos informáticos, o la disponibilidad de alguna red o sistema informático.
- Utilizar o ingresar sin autorización a redes o sistemas informáticos.
- Afectar sistemas informáticos que contengan datos personales.





PROCEDIMIENTO DE CALIFICACIÓN DE OPERADORES DE IMPORTANCIA VITAL





OBLIGACIONES OIV

Obligaciones Operadores Importancia Vital

	Servicios Esenciales	Operador de Importancia Vital
Deberes Generales	X	X
Deber de Reportar	X	X
Sistema de Gestión de Seguridad de la Información		X
Registro de las acciones ejecutadas SGSI		X
Planes de continuidad operacional y ciberseguridad		X
Revisión, ejercicios, simulacros y análisis de las redes.		X
Adoptar medidas necesarias para reducir el impacto.		X
Informar a los potenciales afectados		X
Contar con programas de capacitación, formación y educación continua		X
Designar un delegado de ciberseguridad		X



anci.gob.cl