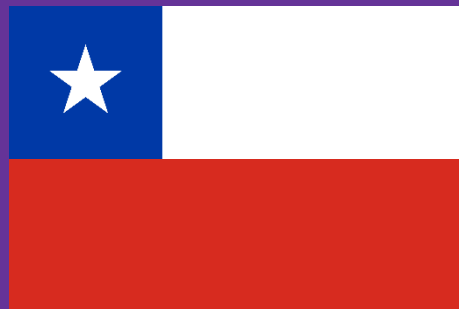




AVANCE FOROCIBER



8 JULIO 2024

1 abril 2024


TV

SENADO

INSTALACIÓN DEL FORO NACIONAL DE CIBERSEGURIDAD





www.forociber.cl



Instalación del
**FORO NACIONAL
DE CIBERSEGURIDAD**

SALÓN DE HONOR - CONGRESO NACIONAL SEDE SANTIAGO
LUNES 01 DE ABRIL / 10:00 a 12:00 HORAS

Exponen:

- **Daniel Álvarez**
Coordinador Nacional de Ciberseguridad
- **Juan Luis Núñez**
Fundación País Digital
- **Paulo Manzato**
CLOUDFLARE

Transmisión por: tv.senado.cl

1 abril 2024

Foro Nacional
de Ciberseguridad

Foro Nacional
de Ciberseguridad





Hito
2024

A
GO

26 Marzo

LEY MARCO DE
CIBERSEGURIDAD

8 Abril



Evento Iberoamericano de Ciberseguridad en Panamá destaca ley marco de Chile

El senador Kenneth Pugh fue invitado a las Jornadas STIC de Ciberseguridad, por el Gobierno de España a través de la Secretaria de Estado Esperanza Casteleiro, organizado por el CNI-CCN y apoyado por la OEA y el BID. El encuentro se ha convertido en uno de los más importantes del continente y, por primera vez, contó con paneles especializados de legisladores.

15 de abril de 2024

11 abril 2024



Trámite del Proyecto

Título del Proyecto:

Establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.

Conocido como:

Ley Marco sobre Ciberseguridad e infraestructura crítica de la información

Etapa en que se encuentra:

- Tramitación terminada ()
- /

Fecha de Ingreso:

Martes 15 de Marzo, 2022

Boletín: 14847-06

[Ver Boletín](#)

Artículos relacionados

Evento Iberoamericano de Ciberseguridad en Panamá destaca ley





ESTRATEGIA CHILE DIGITAL 2035

SENADO
CEPAL
19 MAYO 2022

Estrategia de
Transformación digital
Chile Digital 2035



Instrumento regional
de la Unión Europea para
América Latina y el Caribe



CAPÍTULO 6

ESTRATEGIA DE TRANSFORMACIÓN DIGITAL
DIGITAL TRANSFORMATION STRATEGY

CHILE DIGITAL
2035

CIBERSEGURIDAD/CYBERSECURITY

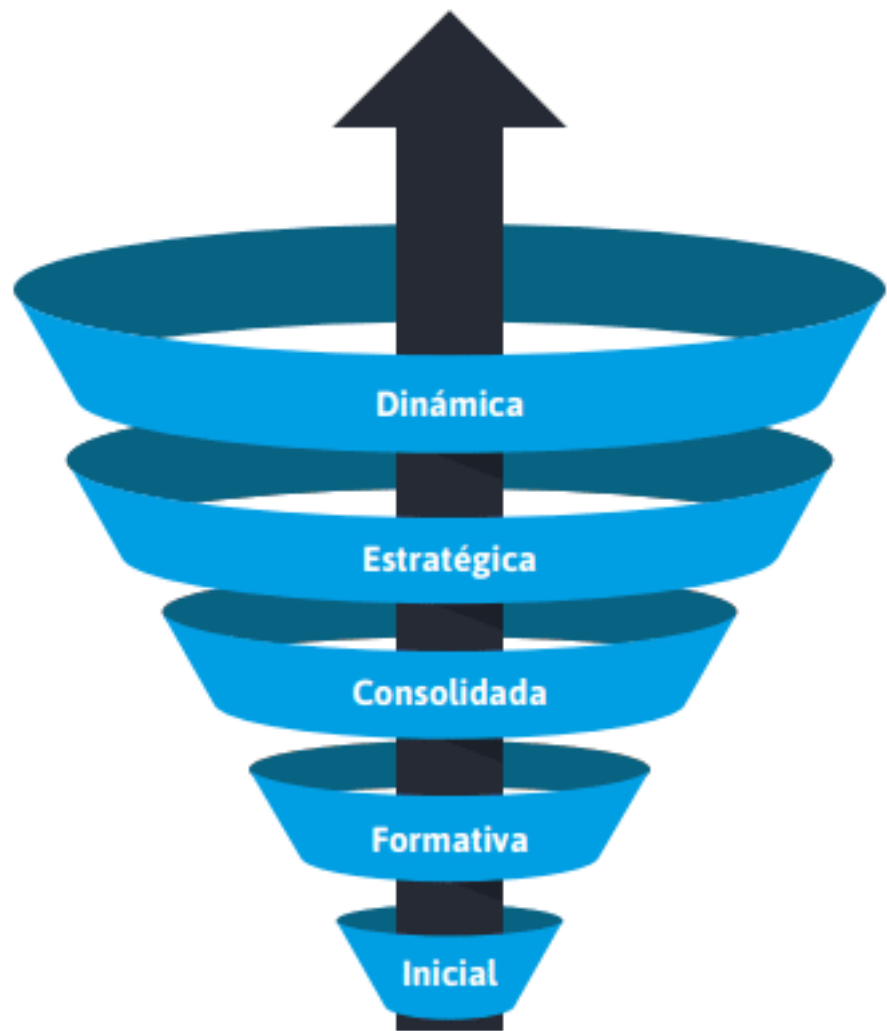


Gráfico 1: Las cinco etapas de madurez de la capacidad de ciberseguridad



Gráfico 2: Las cinco dimensiones del CMM

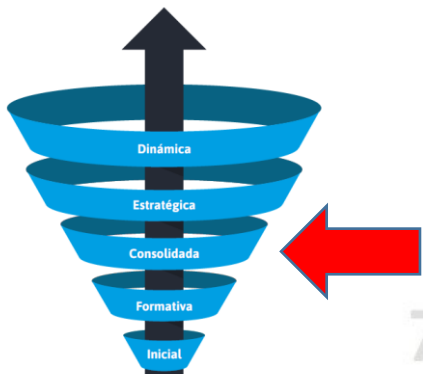


2016

D1	2016	2020
Política y Estrategia de Seguridad Cibernética		
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia	██████	████████
Organización	██████	████████
Contenido	██████	████████
1-2 Respuesta a Incidentes		
Identificación de Incidentes	██████	████████
Organización	██████	████████
Coordinación	██████	████████
Modo de Operación	██████	████████
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación	██████	████████
Organización	██████	████████
Gestión de Riesgos y Respuesta	██████	████████
1-4 Manejo de Crisis		
Manejo de Crisis	██████	████████
1-5 Defensa Cibernética		
Estrategia	██████	████████
Organización	██████	████████
Coordinación	██████	████████
Redundancia de Comunicaciones		
Redundancia de Comunicaciones	██████	████████

D2	2016	2020
Cultura Cibernética y Sociedad		
2-1 Mentalidad de Seguridad Cibernética		
Gobierno	██████	████████
Sector Privado	██████	████████
Usuarios	██████	████████
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario	██████	████████
Confianza del Usuario en los Servicios de Gobierno Electrónico	██████	████████
Confianza del Usuario en los Servicios de Comercio Electrónico	██████	████████
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea	██████	████████
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia	██████	████████
2-5 Medios y Redes Sociales		
Medios y Redes Sociales	██████	████████

2020



EDICIÓN 2021



Cybersecurity Capacity Maturity Model for Nations (CMM) Global Cyber Security Capacity Centre 2021 EDITION

CONOCIMIENTO

D3	2016	2020
Formación, Capacitación y Habilidades de Seguridad Cibernética		
3-1 Sensibilización		
Programas de Sensibilización	██████	████████
Sensibilización Ejecutiva	██████	████████
3-2 Marco para la Formación		
Provisión	██████	████████
Administración	██████	████████
3-3 Marco para la Capacitación Profesional		
Provisión	██████	████████
Apropiación	██████	████████

D5	2016	2020
Estándares, Organizaciones y Tecnologías		
5-1 Cumplimiento de los Estándares		
Estándares de Seguridad de las TIC	██████	████████
Estándares en Adquisiciones	██████	████████
Estándares en el Desarrollo de Software	██████	████████
5-2 Resiliencia de la Infraestructura de Internet		
Resiliencia de la Infraestructura de Internet	██████	████████
5-3 Calidad del Software		
Calidad del Software	██████	████████

Factor

D 3.4: Cybersecurity Research and Innovation

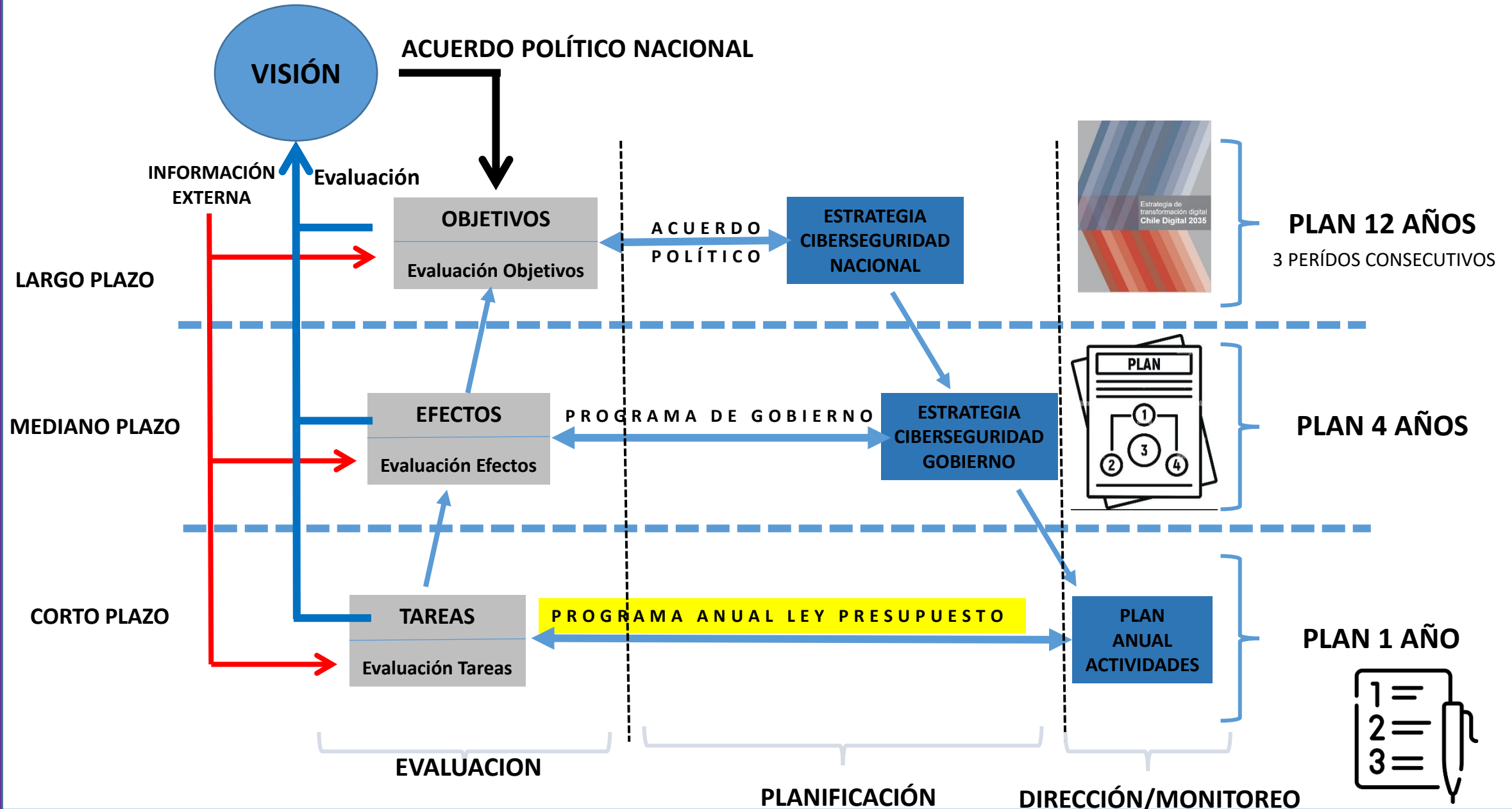
This Factor addresses the emphasis placed on cybersecurity research and innovation to address technological, societal and business challenges and to advance the building of cybersecurity knowledge and capabilities in the country.

> Navigate to Factor

Aspects

- **Cybersecurity Research and Development:** this Aspect investigates the existence of a research and innovation culture in the country, one that is related to a national list of current and completed projects, financial support, incentives and usable research outputs.

Modelo de Planificación de Capacidades Ciberseguridad





DIRECTIVA NIS2 (EU) 2022/2555

Sectors covered by the NIS Directive 2016



Transport



Banking



Financial markets



Drinking water



Digital infrastructure



Energy



Health sector

Extended scope for the NIS2 Directive 2023



Postal and courier services



Manufacture of certain critical products



Waste water and waste management



Public administration



Space



Research



Digital services



Food production, processing & distribution



Providers of public electronic communications networks or services



Manufacture, production and distribution of chemicals



Digital service providers

NIS2 art 16.



Cada 18 meses

<https://www.nis-2-directive.com/>

18 Oct 2024



PRINCIPIOS



Marcela Pallero



Chile: Principios rectores de la Ley Marco de Ciberseguridad Ley 21663, publicada el 8 de abril de 2024.



01

Control de daños: Acciones para minimizar y contener los impactos.

02

Cooperación con la autoridad: para resolver los incidentes de ciberseguridad.

03

Coordinación: entre agencias intervinientes cada una en su área de intervención.

04

Seguridad en el ciberespacio: El Estado otorgará protección a las redes y sistemas informáticos



05

Respuesta Responsable: La respuesta ante incidentes no significará la realización o el apoyo a operaciones ofensivas.



06

Seguridad informática: Toda persona tiene derecho a adoptar las medidas técnicas de seguridad informática, incluyendo el cifrado.



07

Racionalidad: las medidas en materia de ciberseguridad y ejercicio de las facultades de la Agencia deberán ser necesarias y proporcionales al grado de exposición a los riesgos, y al eventual impacto social y económico.



08

Seguridad y privacidad por defecto y desde el diseño



https://twitter.com/Marce_I_P/status/1777846466330923205



CIBERESPACIO (TI-OT)





RELACIONES



C.M.C.

ANCI



C.I.C.



CSIRT
NACIONAL



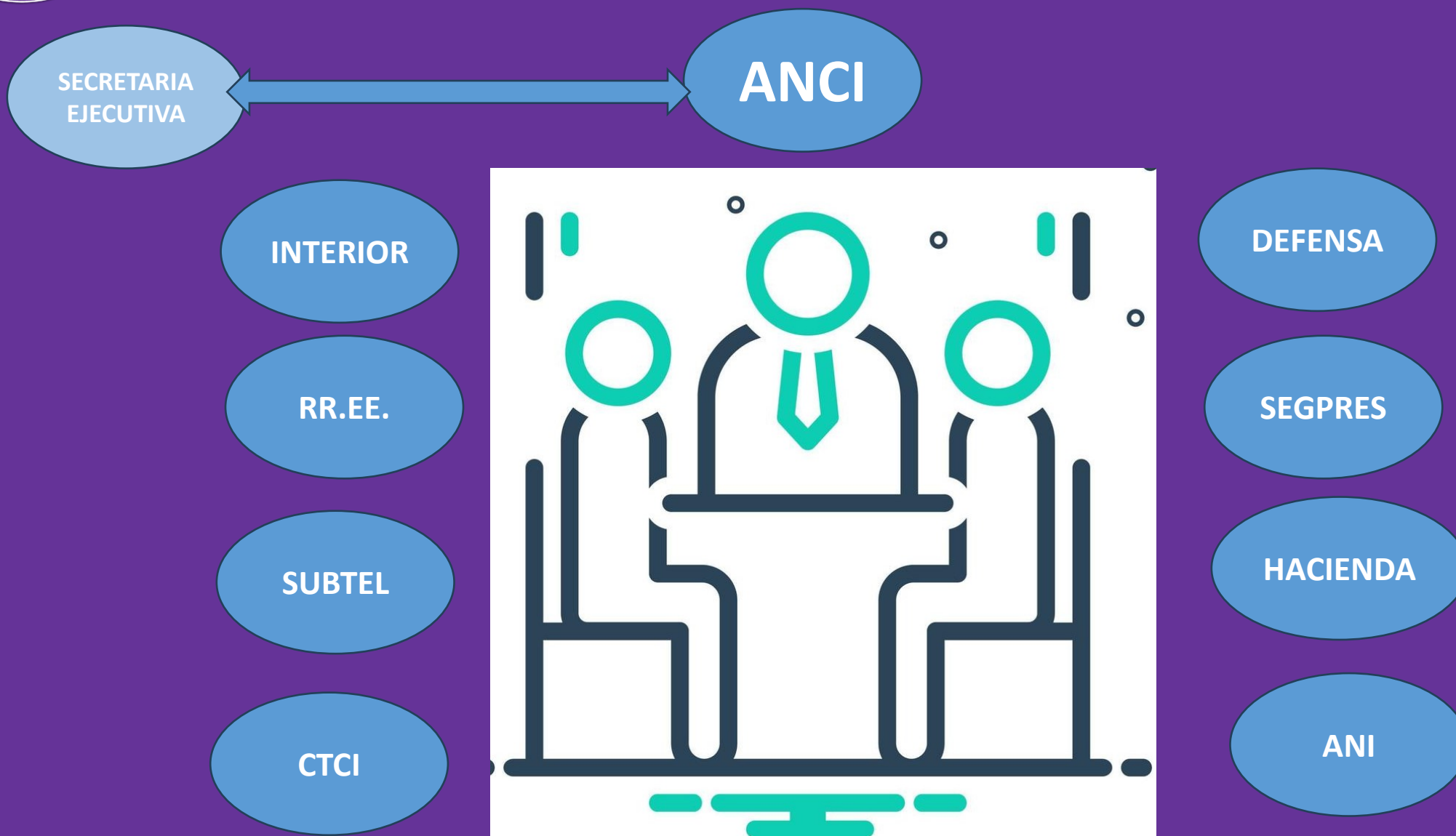
CSIRT
DEFENSA

RCSE





COMITÉ INTERMINISTERIAL CIBERSEGURIDAD



SUBSECRETARIOS Y JEFE SERVICIO



CONSEJO MULTISECTORIAL SOBRE CIBERSEGURIDAD

ANCI

INDUSTRIA

ACADEM 1

S. CIVIL 1



COMERCIO

ACADEM 2

S. CIVIL 2

Por 6 AÑOS
1 Renovación
Cada 3 años 3

Asesorar y formular recomendaciones a la Agencia en el análisis y revisión periódica de la situación de ciberseguridad del país, en el estudio de las amenazas existentes y potenciales en el ámbito de ciberseguridad, y proponer medidas para abordarlas.



Data Breach

Cyber Attack

Protection Failed

Data Leak Detected

System Safety Compromised

PAPÉL

DARON
ACEMOGLU

“EL IMPACTO
DE LA INTELIGENCIA
ARTIFICIAL SERÁ
UNA MEZCLA
DE LA IMPRENTA,
LA MÁQUINA
DE VAPOR Y LA
BOMBA ATÓMICA”

El catedrático del MIT
revisa la lucha milenaria
de la humanidad para
controlar la tecnología en
Poder y progreso' (Deusto).
“La industria tecnológica
quiere que nos sintamos
impotentes ante la
inteligencia artificial para
evitar que la regulemos”
Por Gonzalo Suárez (Madrid)

IA



“EL IMPACTO
DE LA INTELIGENCIA
ARTIFICIAL SERÁ
UNA MEZCLA
DE LA IMPRENTA,
LA MÁQUINA
DE VAPOR Y LA
BOMBA ATÓMICA”



452 Registrados
81 En proceso registro

Ley Marco de Ciberseguridad fue publicada en Diario Oficial

“Este hito legislativo marca el inicio de la construcción de nuestra nueva edificación digital”, valoró el Senador Kenneth Pugh.

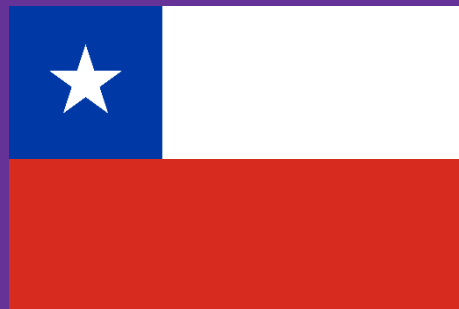
[Ver más](#)



*“Las organizaciones que sobrevivirán al gigantesco cambio digital, social y político no son necesariamente ni las mas grandes ni las más inteligentes, sino aquellas que aprendan a **adaptarse más rápidamente**”*



AVANCE FOROCIBER



8 JULIO 2024