AVANCES Y DESFÍOS DIGITALES 2024

Kenneth Pugh
Senador por Valparaíso

RIESGOS GLOBALES

FORO ECONÓMICO MUNDIAL

2018 CIBERATAQUES

2 de 4 Riesgos

EL RIESGO ES MUY ALTO

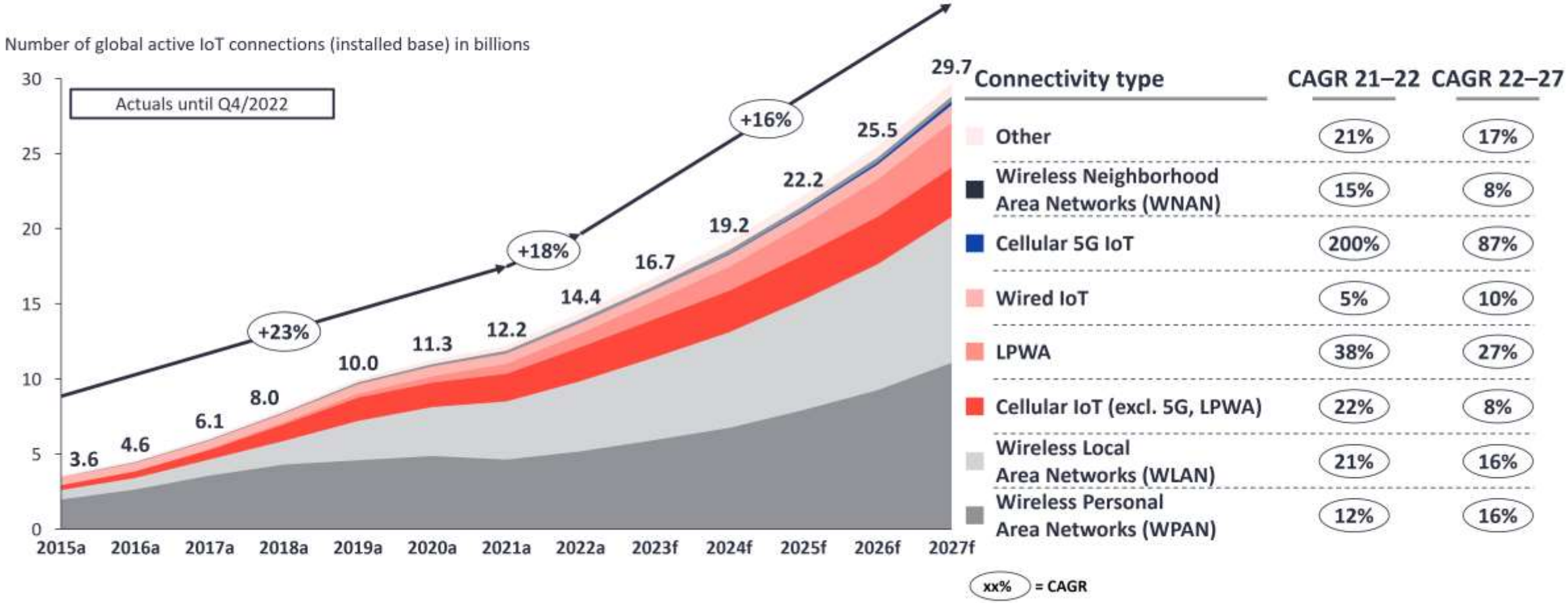
2021

FALLAS DE CIBERSEGURIDAD

AUMENTO DEL RIESGO

LOS RIESGOS PARA LAS PERSONAS Y LOS PROCESOS CRÍTICOS AUMENTAN EXPONENCIALMENTE EN EL CIBERESPACIO

Global IoT market forecast (in billions of connected IoT devices)



Note: IoT connections do not include any computers, laptops, fixed phones, cellphones, or consumers tablets. Counted are active nodes/devices or gateways that concentrate the end-sensors, not every sensor/actuator. Simple one-directional communications technology not considered (e.g., RFID, NFC). Wired includes ethernet and fieldbuses (e.g., connected industrial PLCs or I/O modules); Cellular includes 2G, 3G, 4G, 5G; LPWA includes unlicensed and licensed low-power networks; WPAN includes Bluetooth, Zigbee, Z-Wave or similar; WLAN includes Wi-Fi and related protocols; WNAN includes non-short-range mesh, such as Wi-SUN; Other includes satellite and unclassified proprietary networks with any range.


REPUBLICA DE CHILE
SENADO
Data Breach
Cyber Attack
Protection Failed
System Safety Compromised

Ucrania denuncia que Rusia está usando bombas de vacío, prohibidas por la **Convención de Ginebra**

2022

REPUBLICA DE CHILE

IA

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

CONTRATO DIGITAL

CIBERESPACIO

CIBERSEGURIDAD

FÍSICO

DIGITAL

DESINFORMACIÓN

PROTECCION DATOS PERSONALES

PROTECCIÓN DE LAS I.C.I.

"CONFIANZA DIGITAL"

INTEROPERABILIDAD

IDENTIDAD DIGITAL

Proveer la certeza jurídica de los actos digitales del Estado y de las Personas (naturales y jurídicas) y de los Dispositivos conectados a la red.

PÚBLICO

I.A.

PRIVADO

TRANSFORMACIÓN DIGITAL

LEY 21.180

INTERNET
CRIPTOGRAFÍA
TELECOMUNICACIONES (5G)
IOT
BIG DATA
SERVICIOS CLOUD
MACHINE LEARNING
ROBOTICA AVANZADA
INTELIGENCIA ARTIFICIAL

CONVERGENCIA DIGITAL

Sistema Nacional de ciberseguridad

2018 2019 2020 2021 2022 2023

PNCS

MES

LIBROS

POLÍTICA NACIONAL DE CIBERSEGURIDAD

1) Infraestructura resiliente

•Impulsar la tramitación del proyecto de ley marco sobre ciberseguridad e infraestructura crítica de la información, que crea la Agencia Nacional de Ciberseguridad.

PNCS

•Fortalecer el análisis de la información de red en el ciberespacio.

2) Derechos de las personas

•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.

POLÍTICA NACIONAL DE CIBERSEGURIDAD

3) Cultura de ciberseguridad

•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.

PNCS

•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

•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.

POLÍTICA NACIONAL DE CIBERSEGURIDAD

5) Fomento de la industria y la investigación científica

•La focalización de la investigación aplicada respecto de aquellos problemas en ciberseguridad.

PNCS

•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.

ESTRATEGIA CHILE DIGITAL 2035

CAPÍTULO 6

ESTRATEGIA CHILE DIGITAL 2035

Figura II.1
Estrategia Chile Digital

CAPÍTULO 6

Fuente: Comisión de Transportes y Telecomunicaciones del Senado, Comisión Económica para América Latina y el Caribe (CEPAL), Chile Telcos y Asociación Chilena de infraestructura digital.

ESTRATEGIA CHILE DIGITAL 2035

Senadora/Senator
XIMENA ORDENES N.

Senador/Senator
KENNETH PUGH O.

PRÓLOGO

La Senadora Ximena Ordenes y el Senador Kenneth Pugh, miembros de la Comisión "Desafíos del Futuro, Ciencia, Tecnología e Innovación", tienen el agrado de presentar la Estrategia de Ciberseguridad que forma parte de "CHILE DIGITAL 2035" presentada el pasado 19 de mayo, con el apoyo de la CEPAL, la academia y la sociedad civil organizada.

FOREWORD

Senators Ximena Ordenes and Kenneth Pugh, members of the Committee "Challenges of the Future, Science, Technology, and Innovation" of the Chilean Senate are pleased to present the Cybersecurity Strategy part of "CHILE DIGITAL 2035" issued last May 19, with the support of ECLAC, academia and organized civil society.

MODELO DE MADUREZ DE CIBERCAPACIDADES PARA NACIONES (CMM)

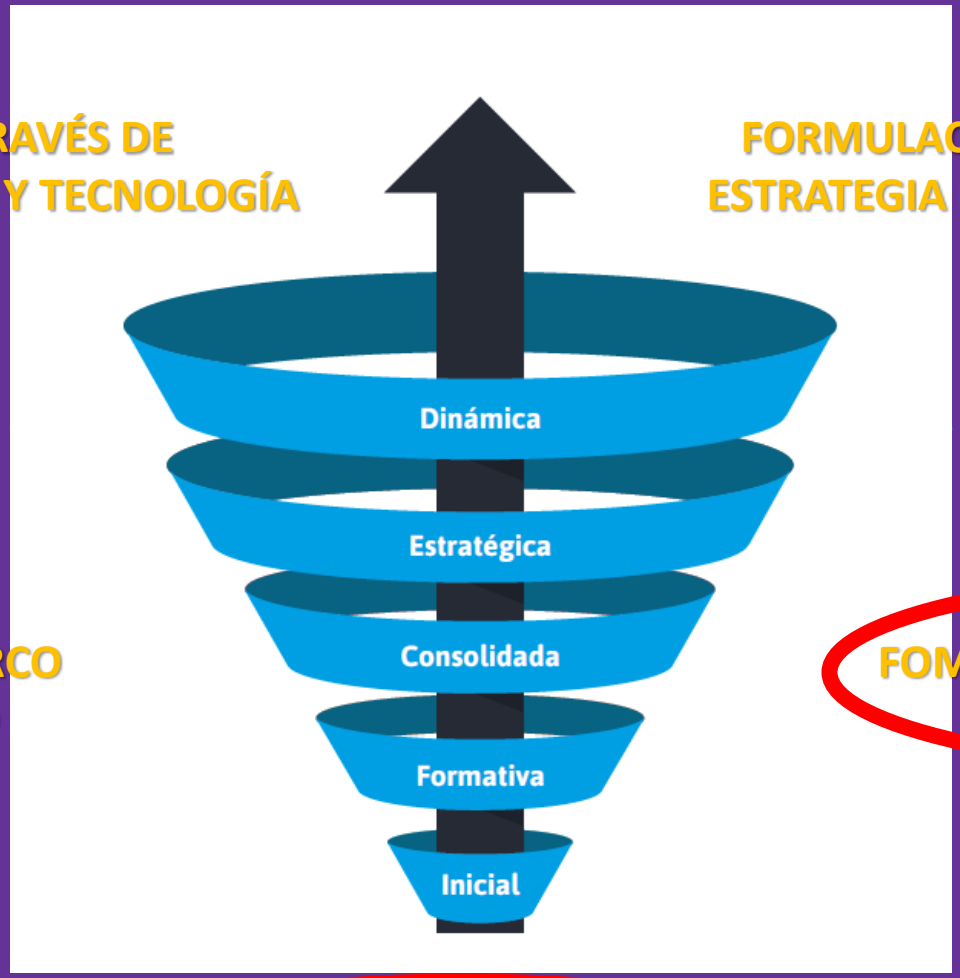
2016

2020

MODELO DE MADUREZ DE CIBERCAPACIDADES PARA NACIONES (CMM)

GESTIÓN DEL RIESGO A TRAVÉS DE ESTÁNDARES, ORGANIZACIONES Y TECNOLOGÍA

FORMULACIÓN DE POLÍTICA Y ESTRATEGIA DE CIBERSEGURIDAD



PROMULGACIÓN DE UN MARCO JURÍDICO Y REGULATORIO DE CIBERSEGURIDAD

FOMENTO EN LA SOCIEDAD DE UNA CULTURA RESPONSABLE EN CIBERSEGURIDAD

DESARROLLO DE CONOCIMIENTO EN CIBERSEGURIDAD

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Global Cyber Security Capacity Centre

2016

2020

Indicadores: Chile

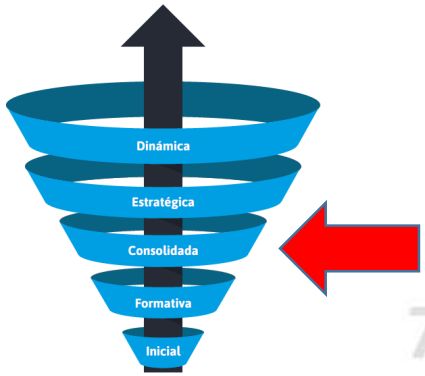
D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
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 Cultura Cibernética y Sociedad

	2016	2020
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		

EDICIÓN 2021



BID

CONOCIMIENTO

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

	2016	2020
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		

3.1

3.2

3.3

D5 Estándares, Organizaciones y Tecnologías

	2016	2020
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

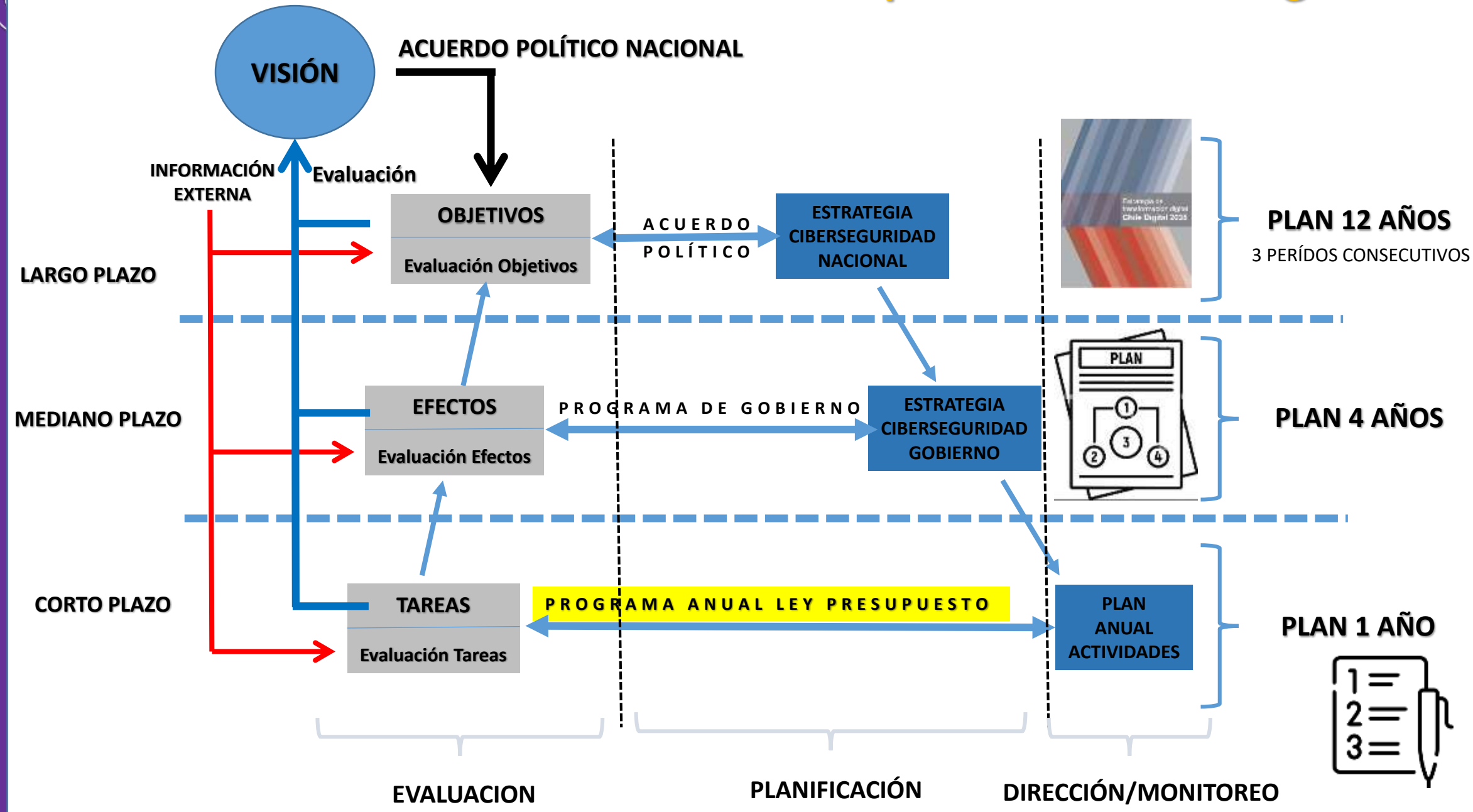
Aspects

- **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.

METAS 2035 EN CIBERSEGURIDAD

- Creación del Instituto Nacional de Ciberseguridad y del Centro de Capacidades de Ciberseguridad de Iberoamérica al 2023
- Creación de las nuevas agencias nacionales de Protección de Datos Personales y de Ciberseguridad y Protección de Infraestructura Críticas de la Información al 2025
- Creación de la totalidad de los CSIRT sectoriales y COC Nacional al 2030
- Inversión del gasto en I+D+i de Ciberseguridad como porcentaje del PIB en un 0,1% al 2025 y en 0,2% al 2030
- Formación de 10.000 profesionales certificados en Ciberseguridad al 2035, donde al menos el 30% de ellos sean mujeres.

Modelo de Planificación de Capacidades Ciberseguridad



Sistema Nacional de ciberseguridad

Agencia Nacional de Ciberseguridad

Organismo Público

ANCI

Agencia Nacional de Protección de Datos Autónoma

Autoridad Pública Autónoma

Instituto Nacional de Ciberseguridad

Organismo Descentralizado Público/Privado

Entidad Pública

Centro de Protección de Infraestructura Crítica

MARCO JURÍDICO DE LA CIBERSEGURIDAD

OCTUBRE

LEY MES CIBERSEGURIDAD

21.113

NOVIEMBRE

MES II.CC.

CULTURA CIBERSEGURIDAD

MES CHILENO DE LA CIBERSEGURIDAD

GDPR

LEY PROTECCIÓN DE DATOS PERSONALES

PROTECCION DE DATOS PERSONALES

LEY MARCO CIBERSEGURIDAD

GOBERNANZA CIBERSEGURIDAD

COORDINACIÓN CSIRTS

TD 21.180

PROTECCION DE INFRAESTRCTURA CRÍTICA INFORMACIÓN

NIS2

LEY PROTECCIÓN DE INFRAESTRUCTURA CRÍTICA

BUDAPEST

LEY DE DELITOS INFORMÁTICOS

21.459

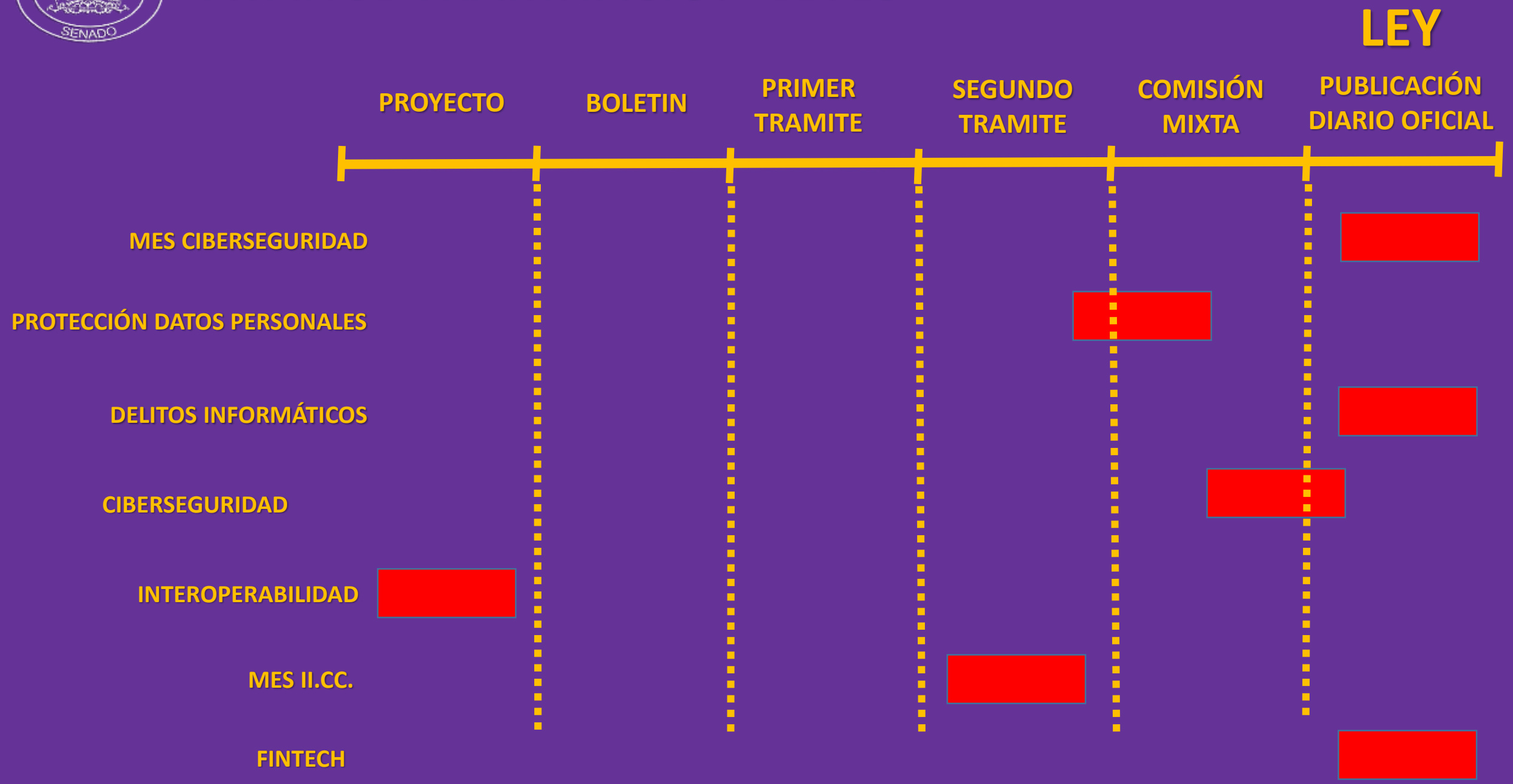
INTEROPERABILIDAD

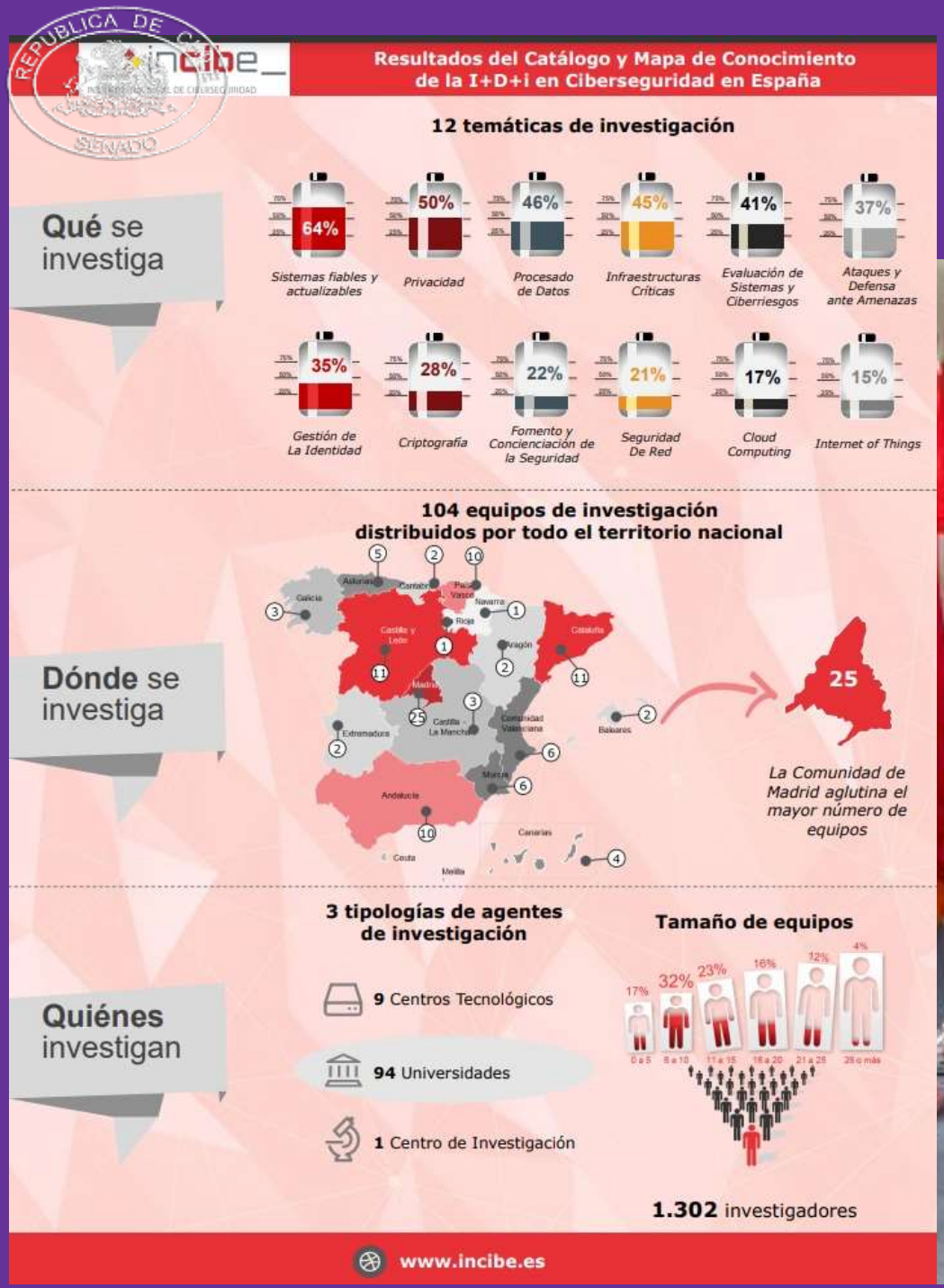
Tratados Internacionales – Leyes Nacionales

4 CAPAS

LEY GOBERNANZA INTEROPERABILIDAD

AVANCE TRAMITACIÓN LEYES




incibe_
Resultados del Catálogo y Mapa de Conocimiento de la I+D+i en Ciberseguridad en España
Qué se investiga
12 temáticas de investigación
64% Sistemas fiables y actualizables
50% Privacidad
46% Procesado de Datos
45% Infraestructuras Críticas
41% Evaluación de Sistemas y Ciberriesgos
37% Ataques y Defensa ante Amenazas
35% Gestión de La Identidad
28% Criptografía
22% Fomento y Concienciación de la Seguridad
21% Seguridad De Red
17% Cloud Computing
15% Internet of Things
Dónde se investiga
104 equipos de investigación distribuidos por todo el territorio nacional
25
La Comunidad de Madrid aglutina el mayor número de equipos
Quiénes investigan
3 tipologías de agentes de investigación
9 Centros Tecnológicos
94 Universidades
1 Centro de Investigación
Tamaño de equipos
17% 32% 23% 16% 12% 4%
1.302 investigadores
www.incibe.es


INCIBE
19 Octubre 2021
LEÓN

Stories

LAS GUARDIANAS DEL CIBERESPACIO

NOS ACERCAMOS A LAS 'HACKERS', PROFESIONALES QUE QUIEREN CAMBIAR EL MUNDO ENTRANDO EN AGUJEROS DE LA RED QUE SÓLO ELLAS SABEN ENCONTRAR. CONÓCELAS.

TEXTO: LULA GÓMEZ

Y si quieren destruir el mundo ni son personajes asociales y excéntricos, ocultos tras una sudadera y que viven encerrados en un sótano. Esta es la imagen que el cine nos ha dado de los *hackers*, pero es sólo esa: una imagen. El programador norteamericano Eric Raymond, gurú en este tema, cree incluso que tú podrías ser una de ellos. Y bajo él, si piensas que el mundo está lleno de conflictos fascinantes que esperan una solución efectiva, si crees que ningún problema tendría que resolverse dos veces, y que el aburrimiento y el trabajo rutinario son tus enemigos, respondes al perfil perfecto para dedicarte a este oficio. Otras dos virtudes imprescindibles son que compartas la idea de que la libertad es sagrada y de que además de tener buena voluntad hay que ser competente. De hecho, por concepto, y en su inmensa mayoría, se trata de expertos en seguridad informática que trabajan de forma colaborativa para arreglar los fallos de los diferentes *softwares*. Lo hacen, como en cualquier otro ámbito, por dinero. Lo que sí es común a todos estos hackers es que son personas muy intuitivas y fascinadas por ir más allá.

El término *hacker* nació en el MIT, el prestigioso Institute of Technology de Massachusetts, y tomó fuerza con el nacimiento de los movimientos de software libre (gratis y con código abierto), que permiten que la creación sea común. «Nosotros somos entusiastas de la tecnología. La amamos y, como la conocemos, encontramos ese pequeño fallo. En eso trabajamos», afirma María Isabel Rojo, *hacker* o *arquitecta de seguridad*, la forma políticamente correcta de referirse a ellas. Se deleitan investigando y probando en muchas cosas diferentes a parte de lo que saben hacer en internet. El color del sombrero que llevan, metafóricamente hablando, es lo que distingue si tipo o tipa que te roba las claves de la tarjeta de crédito de quienes trabajan por la ciberseguridad. Los que entre ellos dicen portarlo blanco son profesionales que trabajan para empresas o instituciones. Su misión: evitar que los malos, los del sombrero negro (también conocidos como *crackers*), entren por ejemplo en el Ministerio de Defensa y airees sus secretos. En medio estarían los grises. Estos no pretenderían tumbar el sistema de comunicación de un aeropuerto para causar el caos, pero sí esperarían algún beneficio a cambio si encuentran una brecha en su seguridad.

Aquí no hay paro

Su información –y ellos lo saben– resulta muy valiosa para los gobiernos, servicios de inteligencia, fuerzas armadas o grandes empresas. Por eso este peculiar oficio no conoce el desempleo. «Lo nuestro no es una profesión de futuro, lo es del presente», afirma Yaiza Rubio, la primera *hacker* española en participar en DefCON y BlackHat, algo así como las olimpiadas más importantes de estos friendlies del ciberespacio. Se celebran una vez al año, ambas en Las Vegas, Estados Unidos. Y es que, de alguna forma, la comunidad *hacker* se mueve en el personal. En esa reunión, por lo menos, el trabajo de María Isabel Rojo, que todas las semanas recibe ofertas de empleo a través de su fanfiedlin. Esta curtida ingeniera cuenta que vive inmersa en las tecnologías dos años antes de que estas sean realidad. Inteligencia artificial (máquinas que piensan), internet de las cosas (por ejemplo, una nevera conectada a la red y programada para comprar los batidos que te gustan cuando coges el último del frigorífico); o blockchain (la tecnología que hace posible las criptomonedas) son los conceptos que más repite María Isabel. Y apunta otro aspecto interesante: ella y sus colegas son las profesionales mejor pagadas en el sector de las tecnologías de la información. Su sueldo anual oscila entre los 75.000 o 115.000 euros brutos anuales, señalan diversas consultoras. No sólo no hay paro, sino que se calcula que hacen falta unos seis millones de *hackers*.

...stidas a su aire

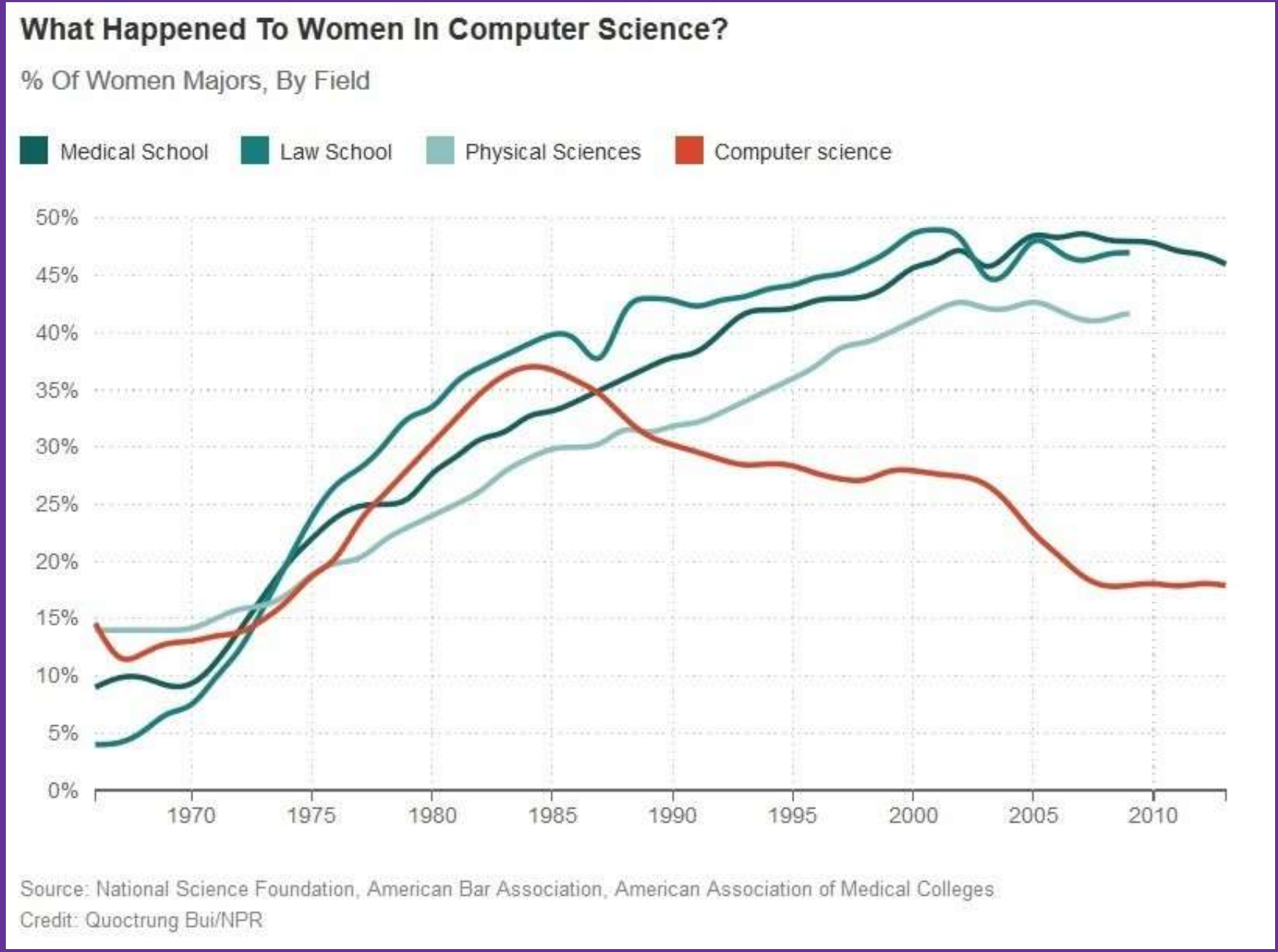
...Tienen que seguir la moda ...adie con su look. Aquí vale todo, ...podríamos estar en el mundo de ...rífico: no están sujetos a dictadu... cochatas o convencionalismos. ...ién si no iba a pensar que Telefónica ...cluyese en su Comité de Dirección ...o pasado a un tipo de pelos largos, ...de luna y que se desestresa en mono...ón? Es Chema Alonso, de 42 años, el ...de Yaiza. Eso sí, si hubiese que hac... un retrato robot de la profesión, sin ...a, habría que pintar a un hombr... como en otras secciones del m... tecnológico, el de la seguridad inf...ática todavía hoy se conjuga en ...sculino. «En Estados Unid... Europa sólo somos el 11%.»

11%
ES EL PORCENTAJE DE MUJERES QUE TRABAJAN EN ESTE SECTOR EN ESTADOS UNIDOS Y EUROPA

BRECHA DE GÉNERO

REVISTA COSMOPOLITAN SEPTIEMBRE 2018

BRECHA DE GÉNERO DE MUJERES EN TIC



@kpughsenador

DIARIO OFICIAL – 1 OCTUBRE 2018

MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA

LEY NÚM. 21.113

DECLARA EL MES DE OCTUBRE COMO EL MES NACIONAL DE LA CIBERSEGURIDAD

Teniendo presente que el H. Congreso Nacional ha dado su aprobación al proyecto de ley originado en moción de los Honorables senadores señores Kenneth Pugh Olavarría, Pedro Araya Guerrero, Carlos Bianchi Chelech, Álvaro Elizalde Soto y Víctor Pérez Varela,

Proyecto de ley:

"**Artículo único**.- Declárase el mes de octubre de cada año como el "Mes Nacional de la Ciberseguridad", con el fin de promoverla y realizar ejercicios nacionales relacionados con ella.".

1 2

Y por cuanto he tenido a bien aprobarlo y sancionarlo; por tanto promúlguese y llévese a efecto como Ley de la República.

Santiago, 24 de septiembre de 2018.- SEBASTIÁN PIÑERA ECHENIQUE, Presidente de la República.- Andrés Chadwick Piñera, Ministro del Interior y Seguridad Pública.

Lo que transcribo a Ud. para su conocimiento.- Saluda Atte. a Ud., Rodrigo Ubilla Mackenney, Subsecretario del Interior.

OCTUBRE MES NACIONAL CIBERSEGURIDAD

1

SEMINARIOS – TALLERES - CONGRESOS

OCTUBRE MES NACIONAL CIBERSEGURIDAD

EJERCICIOS NACIONALES

PDI
POLICÍA DE INVESTIGACIONES DE CHILE

Universidad Andrés Bello

1° Ejercicios de Ci
19 Octubre

CTF

Jueces


David Ruete

Lidia Herrera

Xavier Bonnaire


Nicolás Contador


Carlos Betancourtt

Arquitecto CTF


Oliver Tessini

CTF - Green	
Categoría	Básicos
Capacidad	6 Equipos (5 integrantes)
Formato	Competencia Grupal
WS	Kali 2018.3a
Sala	INF 216

2

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA
EX UMBRA IN SOLEM

DEPARTAMENTO DE INFORMÁTICA

CTF CAMPO DE MARTE

octubre
29

09:00 A
19:00 HRS.

TRANSMISIÓN POR CANAL DE YouTube
MES DE LA CIBERSEGURIDAD


PRESENTA
NICOLÁS VALENZUELA
Senior Security Consultant
Dreamlab Technologies


CONDUCE
CESAR SOTO
Security Consultant
Dreamlab Technologies

DREAMLAB
TECHNOLOGIES

MESA DE CIBERSEGURIDAD SENADO 2023

MESA DE CIBERSEGURIDAD SENADO 2023

FORO NACIONAL DE CIBERSEGURIDAD

al futuro como una verdadera República Digital Cibersegura.

Tomando como base el capítulo de Ciberseguridad del documento Chile 2035, la mesa se organizó en 7 sub-mesas, las cuales se completaron según el interés personal de cada uno, y que fueron cada una dirigidas por un chair y un cochair

→01
Ciberseguridad y Políticas Públicas, a cargo de la **Dra. Carolina Sancho** y **Pelayo Covarrubias, Mag.**

→02
Desarrollo de Talento Ciber, a cargo del **Dr. Xavier Bonaire,** y **Tania Yovanovic.**

→03
Investigación Avanzada en Ciberseguridad, a cargo de la **Dra. Romina Torres** y **Dr. Pedro Pablo Pinacho.**

→04
Tecnologías Emergentes, a cargo del **Dr. Rodrigo Alfaro** y **Dra. Luz Cardona, Mag.**

10

→06
Desinformación en Línea, a cargo del **Dr. Jorge Gatica** y **Félix Staicu, MsSc.**

→07
Interoperabilidad e Identidad Digital, a cargo de **Francisco Méndez, Mag.,** y **Carla Illanes, Mag.**

→08
Foro Nacional de Ciberseguridad

forociber.cl

11

https://obtienearchivo.bcn.cl/obtienearchivo?id=documentos/10221.1/89176/1/Construyendo_la_Ciberseguridad_en_Chile.pdf

ABRIL – JULIO - OCTUBRE

Foro Nacional de Ciberseguridad

forociber.cl


forociber.cl

ENERO 2024

1) LEY MARCO CIBERSEGURIDAD

2) LEY PROTECCION DATOS PERSONALES

3) NUEVA “SECRETARIA GOBIENO DIGITAL” (HACIENDA)

LEY MARCO CIBERSEGURIDAD

Principio de control de daños: frente a un ciberataque o a un incidente de ciberseguridad siempre se deberá actuar coordinada y diligentemente, y adoptar las medidas necesarias para evitar la escalada del ciberataque o del incidente de ciberseguridad y su posible propagación a otros sistemas informáticos.

Principio de cooperación con la autoridad: para resolver los incidentes de ciberseguridad se deberá prestar la cooperación debida con la autoridad competente y, si es necesario, cooperar entre diversos sectores, teniendo en cuenta la interconexión y la interdependencia de los sistemas y servicios.

Principio de coordinación: La Agencia y las autoridades sectoriales deberán cumplir sus cometidos coordinadamente, propender a la unidad de acción y evitar la duplicación o interferencia de funciones.

Principio de seguridad en el ciberespacio: es deber del Estado resguardar la seguridad en el ciberespacio. El Estado velará porque todas las personas puedan participar de un ciberespacio seguro, por lo que otorgará especial protección a las redes y sistemas informáticos que contengan información de aquellos grupos de personas que suelen ser en mayor medida objeto de ciberataques.

LEY MARCO CIBERSEGURIDAD

Principio de respuesta responsable: la aplicación de medidas para responder a incidentes de ciberseguridad o ciberataques en ningún caso podrá significar la realización o el apoyo a operaciones ofensivas.

Principio de seguridad informática: toda persona tiene derecho a adoptar las medidas técnicas de seguridad informática que considere necesarias, incluyendo el cifrado.

Principio de racionalidad: las medidas para la gestión de incidentes de ciberseguridad, las obligaciones de ciberseguridad y el 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.

Principio de seguridad y privacidad por defecto y desde el diseño: los sistemas informáticos, aplicaciones y tecnologías de la información deben diseñarse, implementarse y gestionarse teniendo en cuenta la seguridad y la privacidad de los datos personales que procesan.

LEY MARCO CIBERSEGURIDAD

Artículo 33. De la reserva de información. Se considerarán secretos y de circulación restringida, para todos los efectos legales, los antecedentes, datos, informaciones y registros que obren en poder de la Agencia, de los CSIRT, sean Nacional, de Defensa o que pertenezcan a organismos de la Administración del Estado, o de su personal, cualquiera que sea su cargo o la naturaleza de su vinculación jurídica con éstos. Asimismo, tendrán dicho carácter aquellos otros antecedentes respecto de los cuales el personal de tales organismos del Estado tome conocimiento en el desempeño de sus funciones o con ocasión de éstas.

Adicionalmente, serán considerada como información secreta o reservada, la siguiente:

i. Las matrices de riesgos de ciberseguridad.

ii. Los planes de continuidad operacional y planes ante desastres.

iii. Los planes de acción y mitigación de riesgos de ciberseguridad.

OCTUBRE MES NACIONAL CIBERSEGURIDAD

Artículo 48. Comité Interministerial sobre Ciberseguridad. Créase el Comité Interministerial sobre Ciberseguridad, en adelante el Comité, que tendrá por objeto asesorar al Presidente de la República en materias de ciberseguridad relevantes para el funcionamiento del país.

Artículo 49. De los integrantes del Comité. El Comité estará integrado por los siguientes miembros permanentes:

a) Por el Subsecretario del Interior o quien éste designe.
b) Por el Subsecretario de Defensa o quien éste designe.
c) Por el Subsecretario de Relaciones Exteriores o quien éste designe.
d) Por el Subsecretario General de la Presidencia o quien éste designe.
e) Por el Subsecretario de Telecomunicaciones o quien éste designe.
f) Por el Subsecretario de Hacienda o quien éste designe.
g) Por el Subsecretario de Ciencia, Tecnología, Conocimiento e Innovación o quien éste designe.
h) Por el Director o Directora Nacional de la Agencia Nacional de Inteligencia.
i) Por el Director o Directora Nacional de la Agencia Nacional de Ciberseguridad, quien lo presidirá.

22 ENERO 2023

GOBIERNO CONSTITUYE MESA PARA ELABORACIÓN DE PROYECTO DE LEY SOBRE GOBERNANZA DE DATOS

TRENDTIC | 23 enero, 2024 at 08:50

Santiago, 23 de enero de 2023 – Este lunes 22 se realizó la primera reunión de mesa de trabajo para la elaboración del proyecto de ley sobre gobernanza de datos, instancia comprometida por el Gobierno, tras la aprobación de la Ley Marco de Ciberseguridad.

Participaron en la reunión la Ministra del Interior y Seguridad Pública del Gobierno, Carolina Tohá, el Ministro de Secretaría General de la Presidencia, Álvaro Elizalde, la Ministra de Ciencia, Tecnología, Conocimiento e Innovación, Aisén Etcheverry, la Subsecretaria de Hacienda, Heidi Berner, el Presidente del Senado, Juan Antonio Coloma, los Senadores, Kenneth Pugh y Ximena Ordenes, el Jefe de la División de Gobierno Digital, José Inostroza y el Coordinador Nacional de Ciberseguridad, Daniel Álvarez.

Cabe destacar que entre los objetivos planteados para la mesa de trabajo están:

- Armonizar dispersión regulatoria en materia de interoperabilidad e intercambio de datos.
- Habilitar el intercambio de datos más allá de la Administración del Estado
- Dotar de un marco común a las nuevas instituciones relacionadas con datos: Agencia de Ciberseguridad, Agencia de Protección de Datos y Secretaría de Gobierno Digital.
- Agilizar la implementación de la Ley de Transformación Digital del Estado

AVANCES Y DESFÍOS DIGITALES 2024

Kenneth Pugh
Senador por Valparaíso