República Digital

Chile hacia una
República Digital

La Estrategia CHILE DIGITAL 2035

Por la Razón y la Fuerza
de los DATOS

cibersenador@gmail.com

@kpughsenador

Kenneth Pugh
Senador por Valparaíso

República Digital

NUEVO CONTRATO DIGITAL

CIBERESPACIO

CIBERSEGURIDAD

FÍSICO

DIGITAL

DESINFORMACIÓN

PROTECCION DATOS PERSONALES

PROTECCCIÓN DE LAS I.C.I.

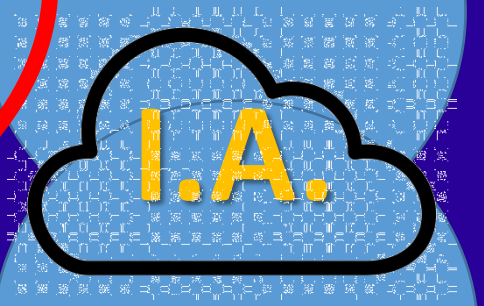
”CONFIANZA DIGITAL”

INTEROPERABILIDAD

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.

TRANSFORMACIÓN DIGITAL

PÚBLICO

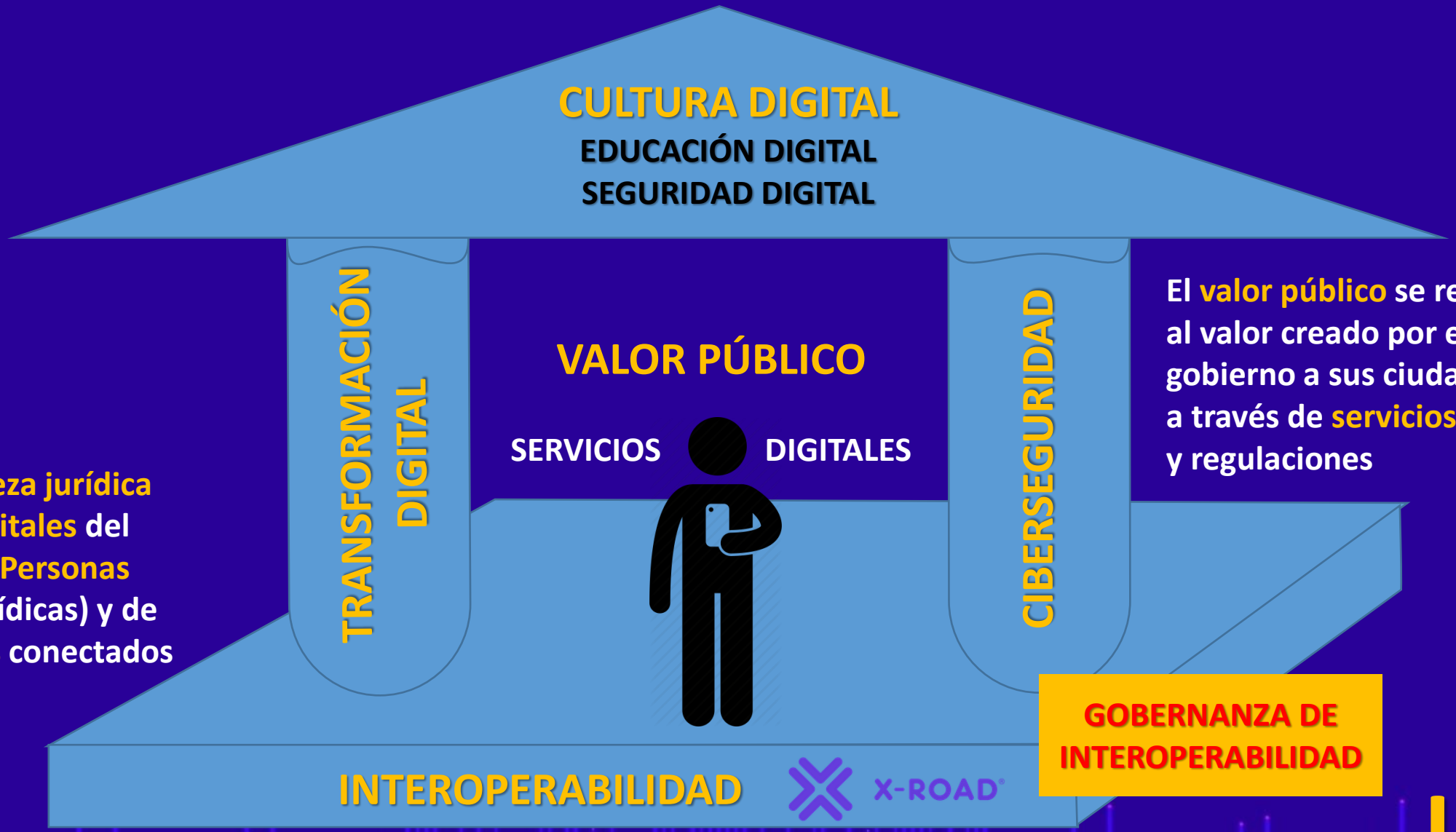


PRIVADO

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

CONVERGENCIA DIGITAL

ARQUITECTURA DE UNA "REPÚBLICA 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.

El valor público se refiere al valor creado por el gobierno a sus ciudadanos, a través de servicios, leyes y regulaciones

GOBERNANZA DE INTEROPERABILIDAD

"CONFIANZA DIGITAL"

I.A.

ARQUITECTURA "REPÚBLICA DIGITAL"

CULTURA DIGITAL
EDUCACIÓN DIGITAL
SEGURIDAD DIGITAL

5 años

LEY 21.180 – 11 Nov 2019

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.

TRANSFORMACIÓN DIGITAL

VALOR PÚBLICO

SERVICIOS DIGITALES

DERECHO
Relacionamiento Digital

CIBERSEGURIDAD

El valor público se refiere al valor creado por el gobierno a sus ciudadanos, a través de servicios, leyes y regulaciones

GOBERNANZA DE INTEROPERABILIDAD

INTEROPERABILIDAD X-ROAD

"CONFIANZA DIGITAL"

I.A.

MARCO JURÍDICO DE CIBERSEGURIDAD

OCTUBRE

LEY MES CIBERSEGURIDAD

21.113

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

PROTECCION DE INFRAESTRCTURA CRÍTICA INFORMACIÓN

LEY PROTECCIÓN DE INFRAESTRUCTURA CRÍTICA

BUDAPEST

LEY DE DELITOS INFORMÁTICOS

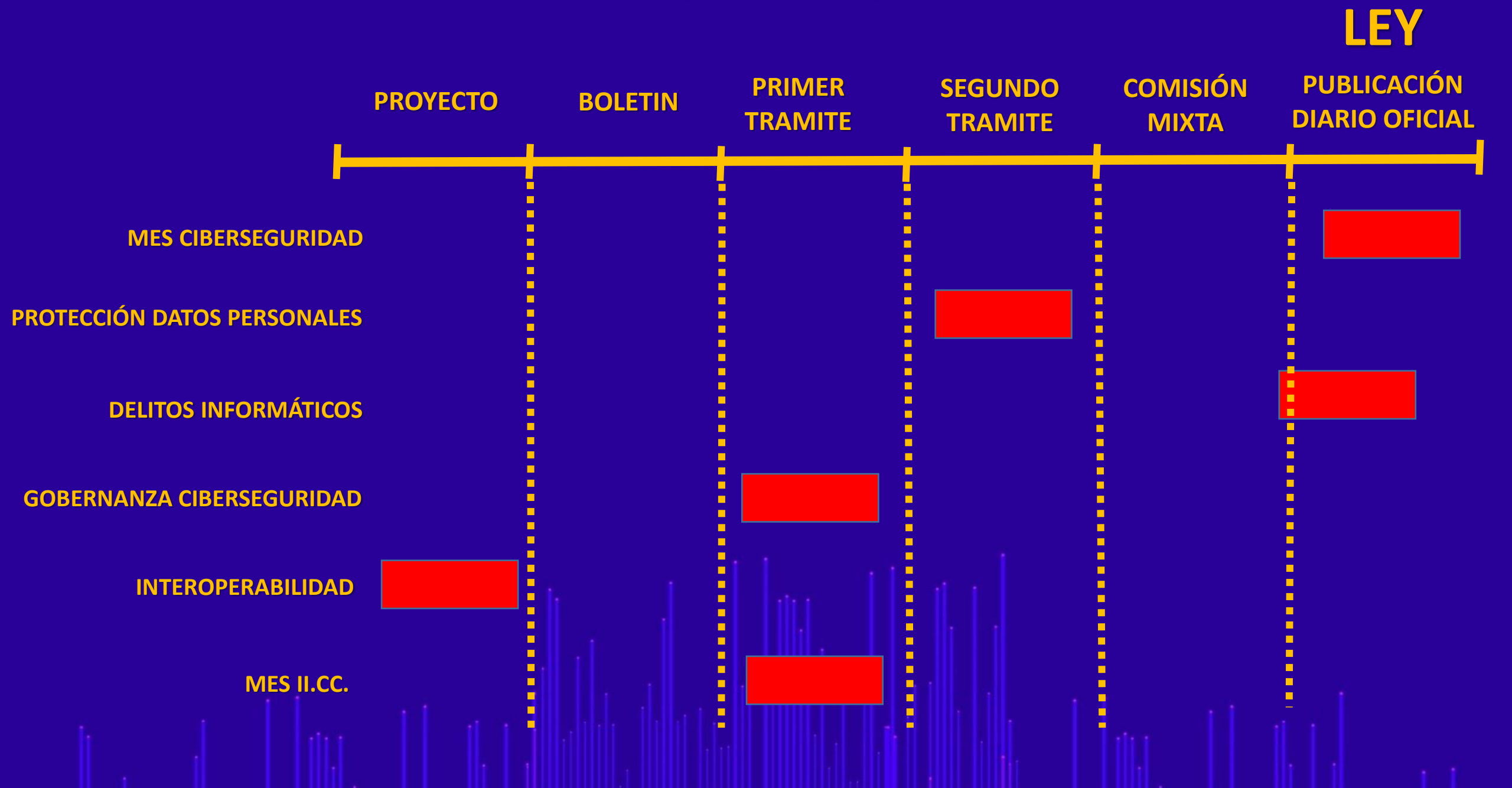
INTEROPERABILIDAD

X-ROAD

LEY GOBERNANZA INTEROPERABILIDAD

Tratados Internacionales – Leyes Nacionales

AVANCE TRAMITACIÓN LEYES CIBER



República Digital

Sistema Nacional de ciberseguridad

ANID

República Digital

LOS DESAFÍOS PARA CHILE (BRECHAS)

URBANIZACIÓN DIGITAL (conectividad)

INCLUSIÓN DIGITAL (acceso)

ALFABETIZACIÓN DIGITAL (conocimiento)

CIBERSEGURIDAD

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

Ni quieren destruir el mundo ni son personajes asociales y excéntricos, ocultos tras una capucha y que viven encerrados en un garaje. Esta es la imagen que el cine nos ha dado de los *hackers*, pero es sólo eso: ficción. El programador norteamericano Eric Raymond, gurú en este tema, cree incluso que tú podrías ser una de ellos. Según 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 perniciosos, respondes al perfil perfecto para dedicarte a este oficio. Otras dos máximas imprescindibles son que compartas la idea de que la libertad es buena y de que además de tener buena actitud 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*. U[n] pocos, como en cualquier otro [gru]po, delinquen. Lo que sí es com[ún] a estos técnicos es que son person[as] intuitivas y fascinadas por ir más a[llá].

El término *hacker* naci[ó] en el MIT, el prestigioso Institute of [T]echnology de Massachusetts, y tom[ó] fuerza con el desarrollo de los movi[mi]entos de *software* libre (gratis y [de] código abierto), que permiten [l]a creación continúe. «Nosotros so[mos] entusiastas de la tecnología. La ama[mos] y, como la conocemos, encontramos [los] pequeños fallos. En eso trabajamos», a[fir]ma María Isabel Rojo, *hacker* o *arquitect[a]* de *seguridad*, la forma políticamente correcta de referirse a ellas. Se deleitan investigando y poniendo en marcha cosas divertidas a partir de lo que saben hacer en internet. El *color del sombrero* que llevan, metafóricamente hablando, es lo que distingue al 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 aireen 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 guardianes 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 porvenir. En eso consiste, por lo menos, el trabajo de María Isabel Rojo, que todas las semanas recibe ofertas de empleo a través de su *linkedin*. Esta cotizada 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 a 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*.

11%

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

[V]estidas a su aire

[En]cima no tienen que seguir la moda ni conten[tar] a nadie con su *look*. Aquí vale todo, tan[to] que podríamos estar en el mundo de *[Fri]kis:* no están sujetos a dictadur[as] de corbatas o convencionalismos. [¿Q]uién si no iba a pensar que Telefónic[a] incluyese en su Comité de Dirección [a] un pasado a un tipo de pelos largos, g[afa]s de lana y que se desestresa en mono[pa]tín? Es Chema Alonso, de 42 años, el [je]fe de Yaiza. Eso sí, si hubiese que hac[er] un retrato robot de la profesión, sin d[uda], habría que pintar a un hombr[e]. Como en otras secciones del mu[ndo] tecnológico, el de la seguridad inf[orm]ática todavía hoy se conjuga en [m]asculino. «En Estados Unid[os] y Europa sólo somos el 11%.»

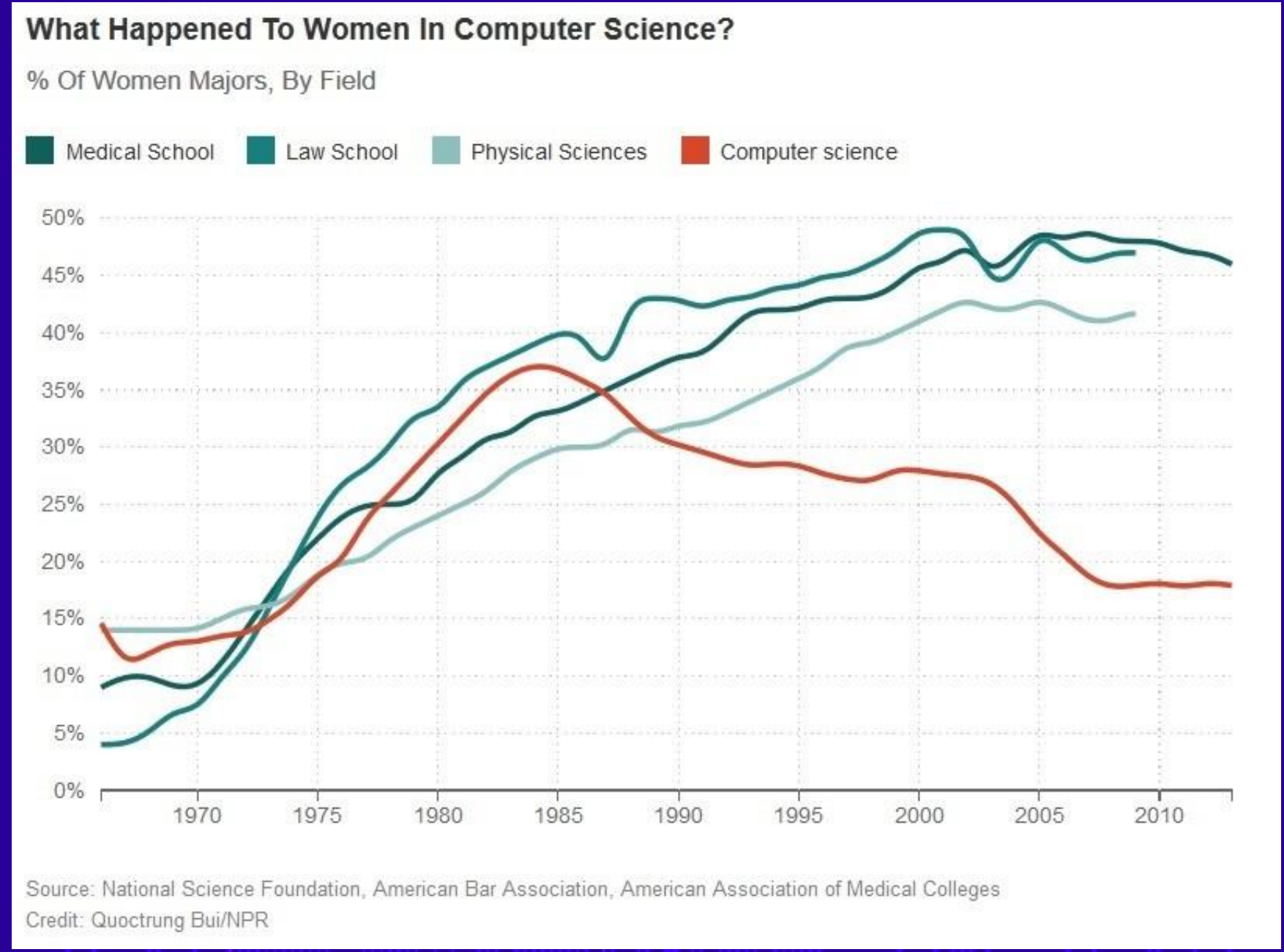
República Digital

BRECHA DE GÉNERO

REVISTA COSMOPOLITAN SEPTIEMBRE 2018

República Digital

BRECHA DE GÉNERO DE MUJERES EN TIC



@kpughsenador

República Digital

LANZAMIENTO JUEVES 19 MAYO 2022

Estrategia de Transformación digital

Chile Digital 2035

OBJETIVOS

Estrategia Chile Digital

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.

METAS: INFRAESTRUCTURA DIGITAL HABILITANTE

En este marco se propone:

- La cobertura de 5G deberá alcanzar el 90% de la población en 2025, el 98% en 2030 y 100% al 2035.
- Los hogares pasados por FTTH deberá alcanzar el 65% en 2025, el 70% en 2030 y el 85% en 2035.

En calidad de banda ancha:

- La velocidad promedio redes fijas deberá alcanzar los 160 Mbps para 2025, los 400 Mbps para 2030 y los 900 Mbps para 2035.
- La velocidad promedio redes móviles deberá alcanzar los 60 Mbps para 2025, los 180 Mbps para 2030 y los 500 Mbps para 2035.
- Las redes de ultra alta velocidad en el Estado (velocidades superiores a 400 Mbps) deberá alcanzar el 100% de las dependencias en 2030 y 1 Gbps al 2035.

En penetración:

- La penetración móvil – usuarios únicos (% población) deberá alcanzar el 80% para 2025, el 90% para 2030 y el 98% para 2035.
- La penetración fija (% hogares) deberá alcanzar el 85% para 2025, el 90% para 2030 y el 95% para 2035.

METAS: DESARROLLO DE HABILIDADES DIGITALES

En este marco se propone:

- Al menos igualar el promedio de la OCDE al 2035 en el desarrollo de habilidades digitales básicas y avanzadas.
- Establecer un plan nacional de reconversión de la fuerza laboral cuyos trabajos desaparecieron por la transformación digital al 2025.
- Incrementar la cantidad de profesionales en disciplinas en ciencia, tecnología, ingeniería y matemáticas (STEM) al menos igualar niveles promedio de los países de la OCDE.

METAS: DERECHOS DIGITALES

En este marco se propone:

- Establecer carta de derechos digitales al 2025
- Plan de educación de derechos digitales al 2025
- Ley de protección de datos personales al 2023
- Estrategia Nacional de datos abiertos al 2024
- Actualización de ley de Firma electrónica e identidad digital a 2025

METAS: DIGITALIZACIÓN DE LA ECONOMIA

En este marco se propone:

- Adoptar herramientas de comercio electrónico, especialmente en las pymes, para que en el 2025 el 35% de todas las empresas hayan adoptado este tipo de herramienta, 50% el 2030 y 70% el 2035.

- Porcentaje de start ups por año en inteligencia artificial, análisis de datos, robótica y ciberseguridad: 2025 el 5%, 2030 el 10% y 15% para 2035.
- La capacitación de pymes en el uso de herramientas digitales avanzadas para alcanzar un total de 10.000 empresas capacitadas por año hasta el 2035.
- El gasto de I+D como porcentaje del PIB alcance el 1% en 2025, 2% en 2030 y el 2,5% en 2035.
- Incrementar el financiamiento para emprendimientos de base tecnológica (startups) que permita duplicar el gasto per cápita anual hacia 2035. Pasar de 186$US per cápita en 2020 a 450$US per cápita en 2035.
- Duplicar el monto de financiamiento de inversiones ángeles hacia 2035. Pasar de un 0,17% a 0,28% en % PIB.

República Digital

METAS: DIGITALIZACIÓN DEL ESTADO

En este marco se propone:

- Al 2025, el 95% de trámites a nivel nacional se pueden realizar en línea y a partir del 2030 el 100%.
- Todas las instituciones cuentan con mecanismos digitales de participación ciudadana.
- El 100% de los ciudadanos cuentan con clave única en 2025.
- Elaborar una política nacional de datos al 2025.

METAS: CIBERSEGURIDAD

En este marco se propone:

- 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.
- Alcanzar el 2035 una "Madurez en Ciberseguridad" cercana al Estado 5 o "Dinámico" para una nación, de acuerdo con el CMM de la Universidad de Oxford, en todos los Factores con al menos evaluación Estado 4 y medido de forma externa.

METAS: GOBERNANZA

Se propone:

- Contar con un sistema de monitoreo de la Estrategia digital con indicadores de impacto y resultado.
- Reforma del ente regulador en materia de telecomunicaciones.

Modelo de Planificación de Capacidades Ciberseguridad

VISIÓN

ACUERDO POLÍTICO NACIONAL

INFORMACIÓN EXTERNA

Evaluación

LARGO PLAZO

OBJETIVOS

Evaluación Objetivos

ACUERDO POLÍTICO

ESTRATEGIA CIBERSEGURIDAD NACIONAL

PLAN 12 AÑOS

3 PERÍDOS CONSECUTIVOS

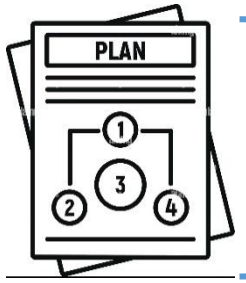
MEDIANO PLAZO

EFECTOS

Evaluación Efectos

PROGRAMA DE GOBIERNO

ESTRATEGIA CIBERSEGURIDAD GOBIERNO



PLAN 4 AÑOS

CORTO PLAZO

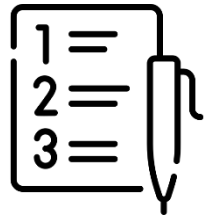
TAREAS

Evaluación Tareas

PROGRAMA ANUAL LEY PRESUPUESTO

PLAN ANUAL ACTIVIDADES

PLAN 1 AÑO



EVALUACION

PLANIFICACIÓN

DIRECCIÓN/MONITOREO

República Digital

Chile hacia una
República Digital

La Estrategia CHILE DIGITAL 2035

Por la Razón y la Fuerza
de los DATOS

cibersenador@gmail.com

@kpughsenador

Kenneth Pugh
Senador por Valparaíso