

# El Ecosistema de la Transformación Digital en el Estado

Chile hacia una  
República Digital



Por la Razón o la Fuerza  
de los DATOS



@kpughsenador

Kenneth Pugh  
Senador por Valparaíso

US\$ 12



AIoT  
Sipeed MAix

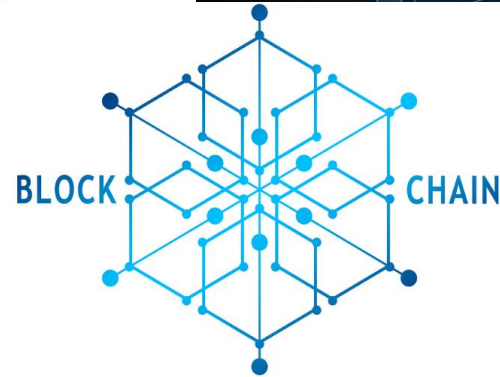


**Sabiduría**  
Evaluación e internalización del conocimiento

**Conocimiento**  
Aplicación mental de los datos y la información

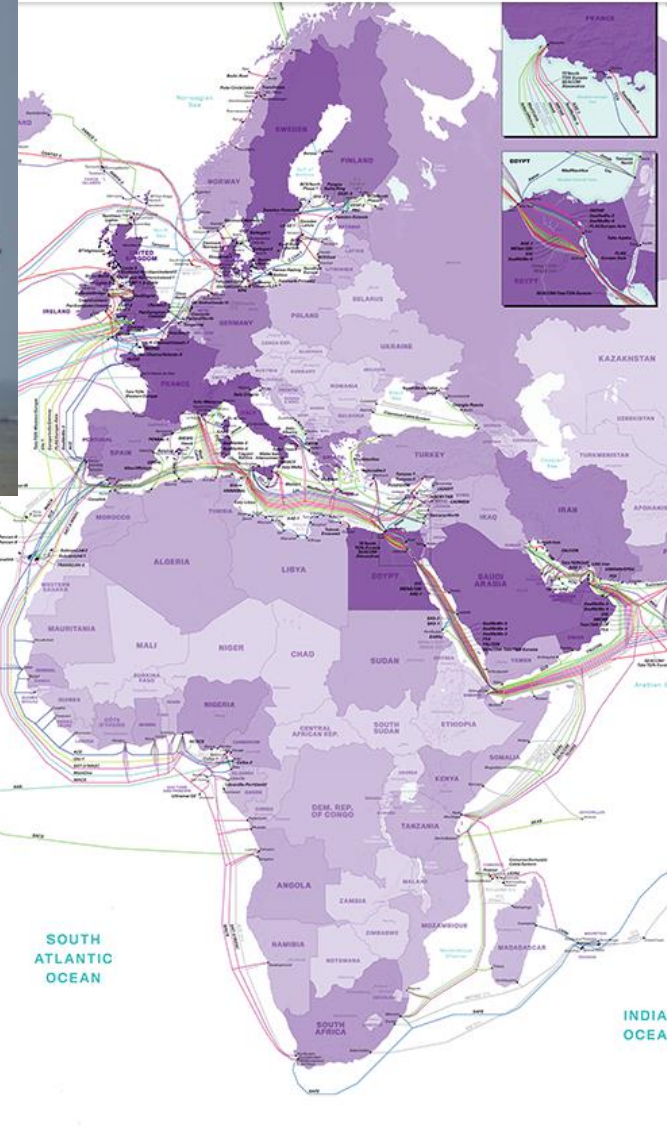
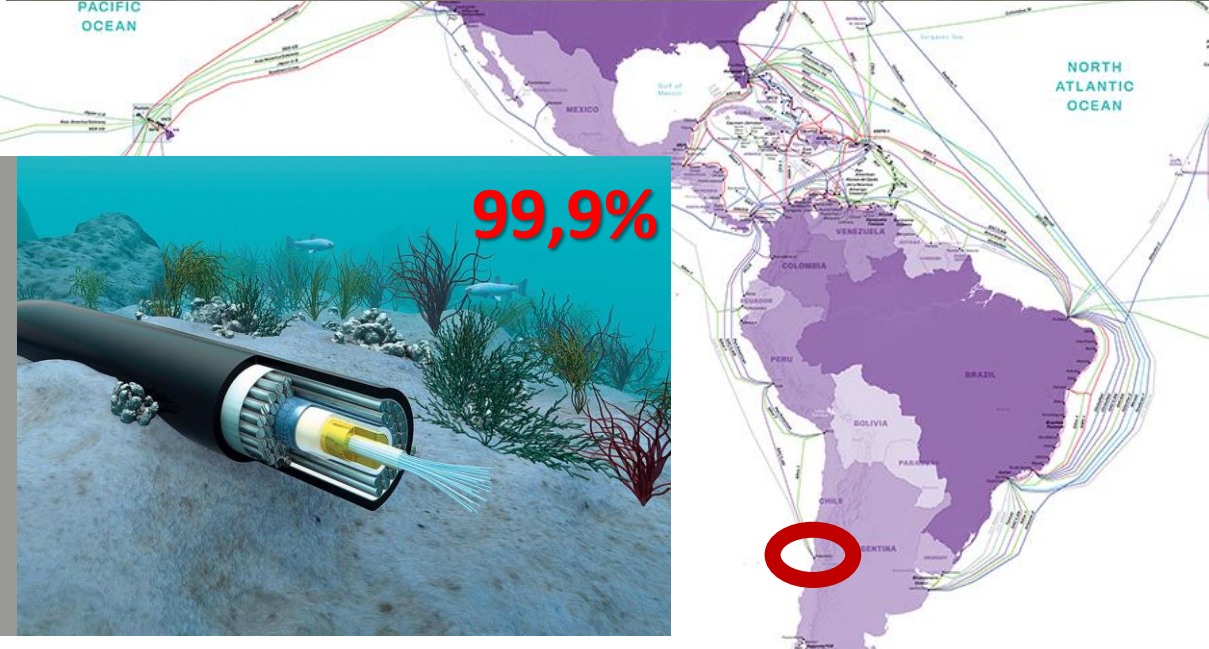
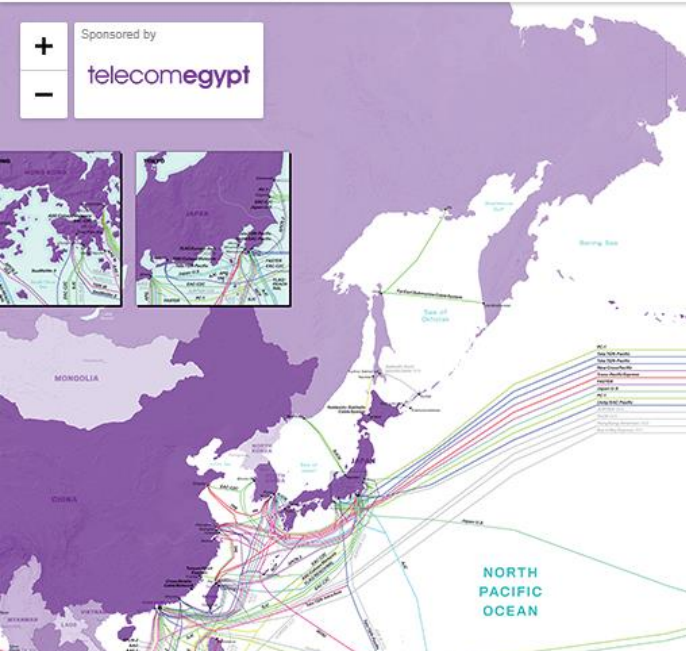
**Información**  
Datos procesados para ser útiles

**Datos**  
Elementos discontinuos que representan hechos



Fuente: Hey, J.: The Data, Information, Knowledge, Wisdom Chain: The Metaphorical Link

Sponsored by  
telecomegypt



# MODELO DE GLOBALIZACION DEL MUNDO

# CABLE "CURIE" de Google de SAN FRANCISCO a VALPARAÍSO



ABRIL  
2019

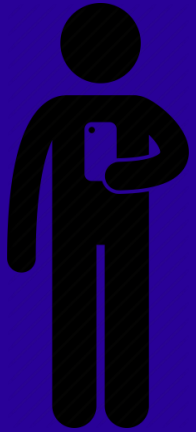
GLORIA  
HUTT

JAYNE  
STOWELL

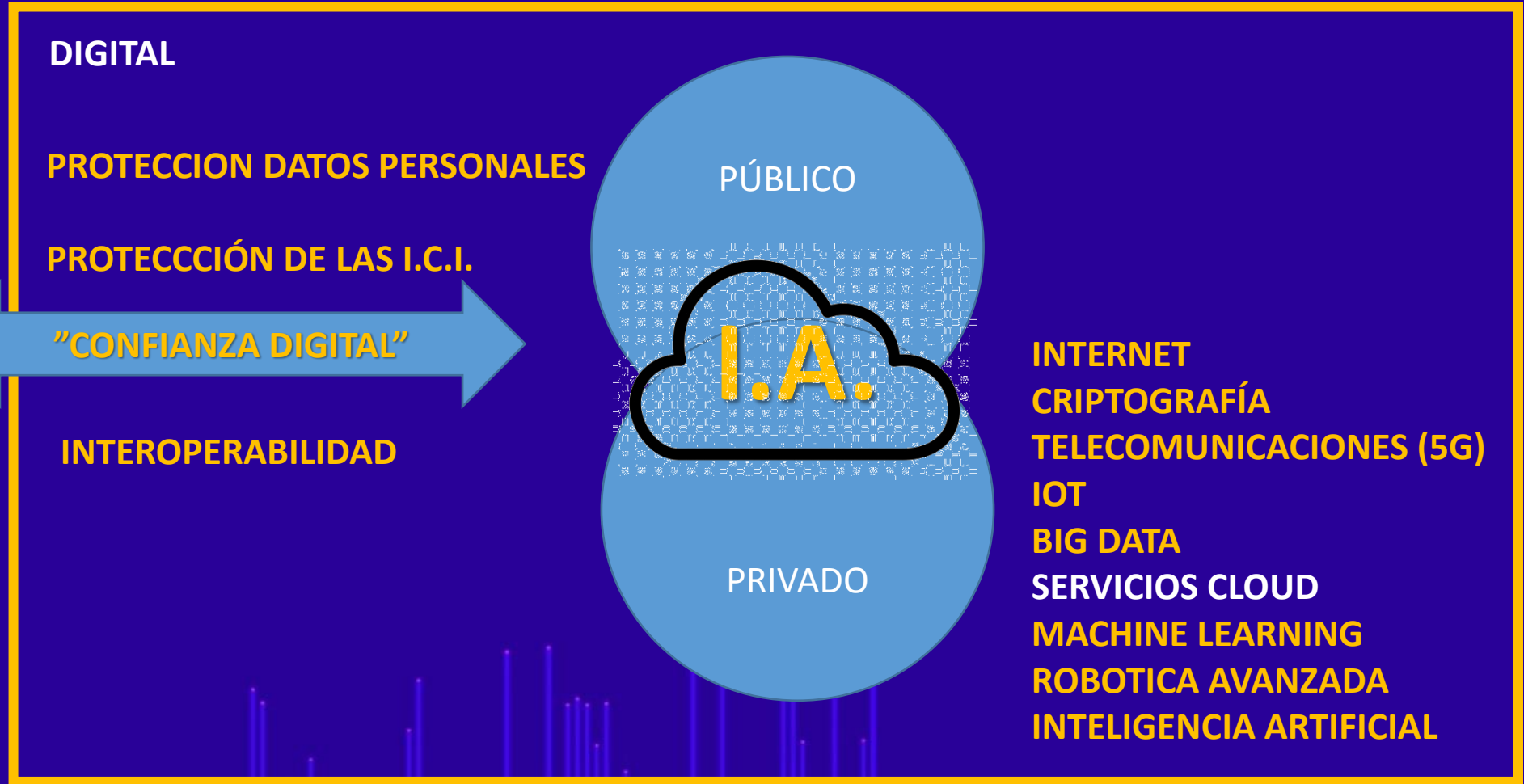
KENNETH  
PUGH

# CONTRATO DIGITAL

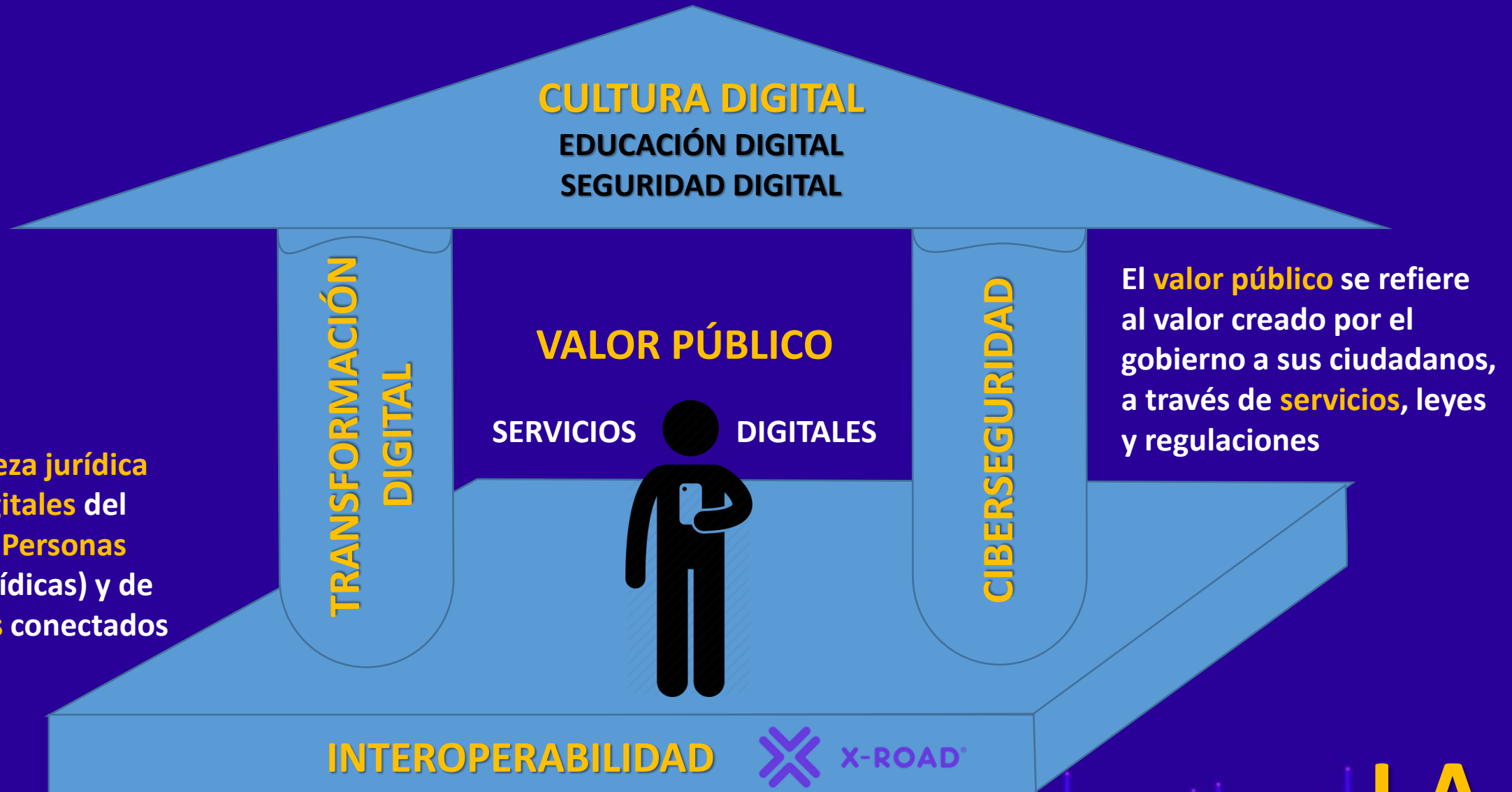
FÍSICO



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.



# ARQUITECTURA “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.

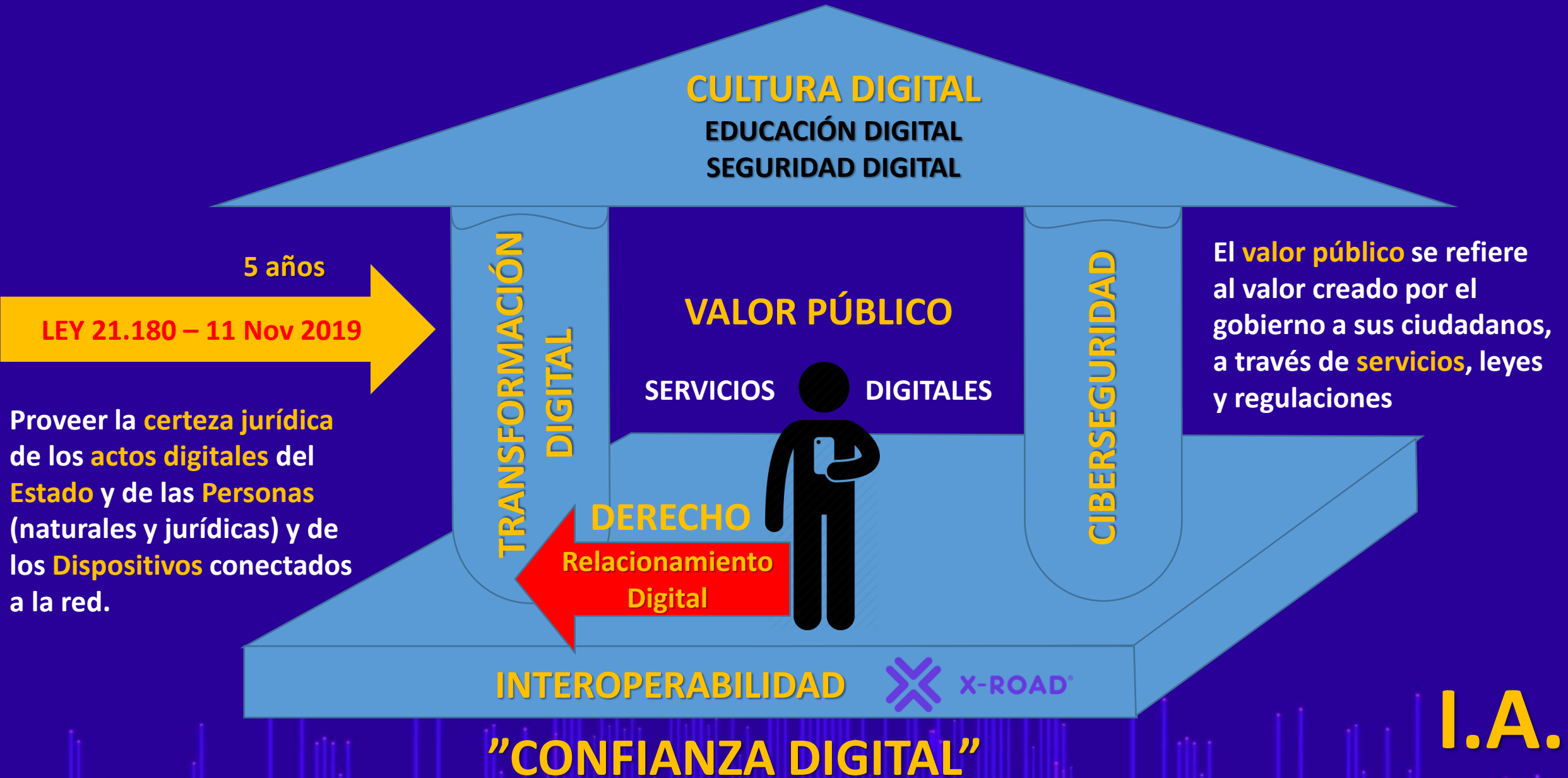
El **valor público** se refiere al valor creado por el gobierno a sus ciudadanos, a través de **servicios**, leyes y regulaciones

INTEROPERABILIDAD  X-ROAD

“CONFIANZA DIGITAL”

I.A.

# ARQUITECTURA "REPÚBLICA 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.

CULTURA DIGITAL

EDUCACIÓN DIGITAL  
SEGURIDAD DIGITAL

TRANSFORMACIÓN  
DIGITAL

VALOR PÚBLICO

SERVICIOS DIGITALES



DERECHO

Relacionamento  
Digital

CIBERSEGURIDAD

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

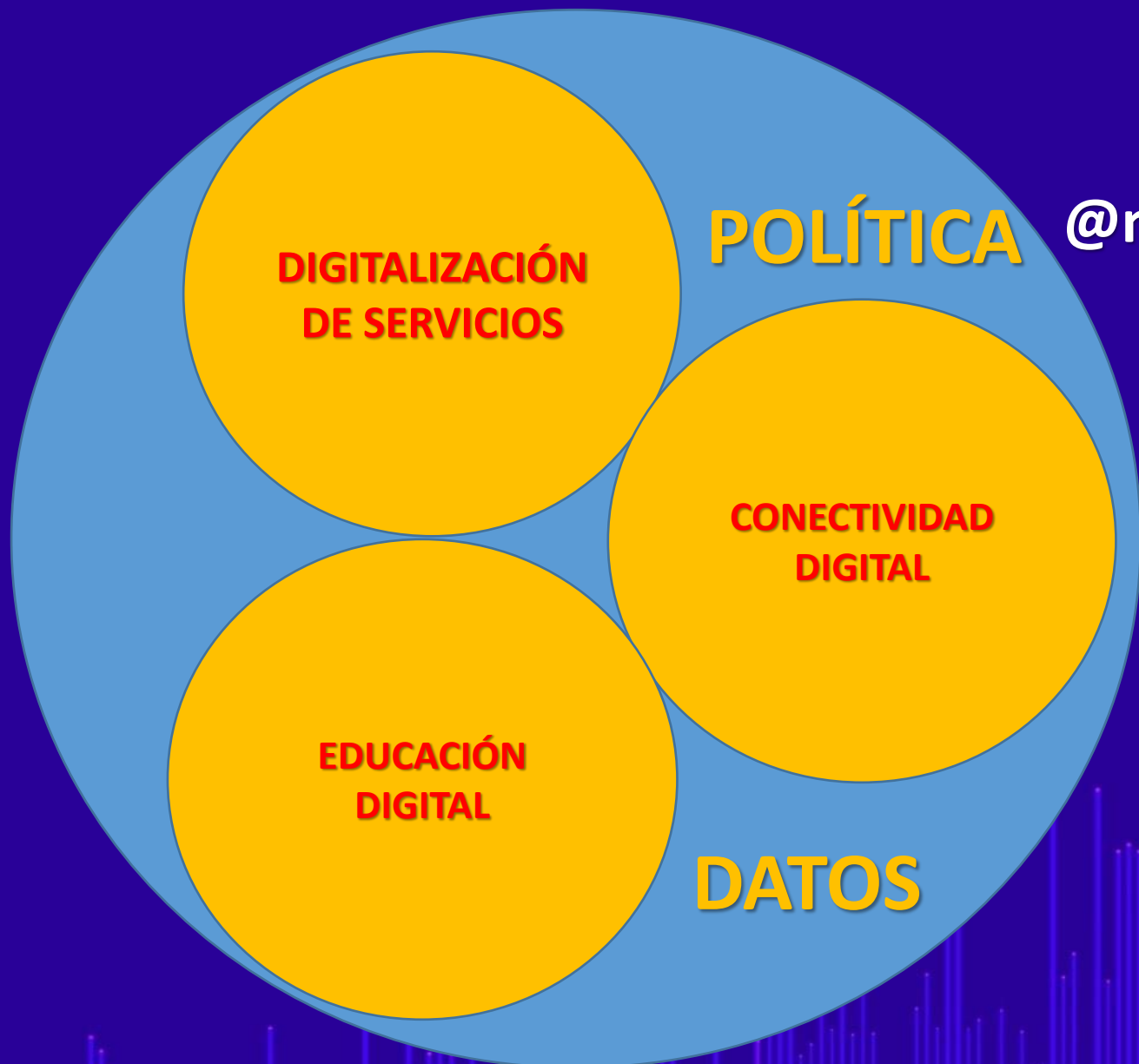
INTEROPERABILIDAD



"CONFIANZA DIGITAL"

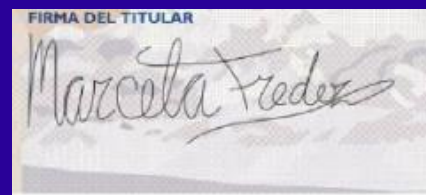
I.A.

# TRANSFORMACIÓN DIGITAL EN EL ESTADO



@marcela\_chile.cl

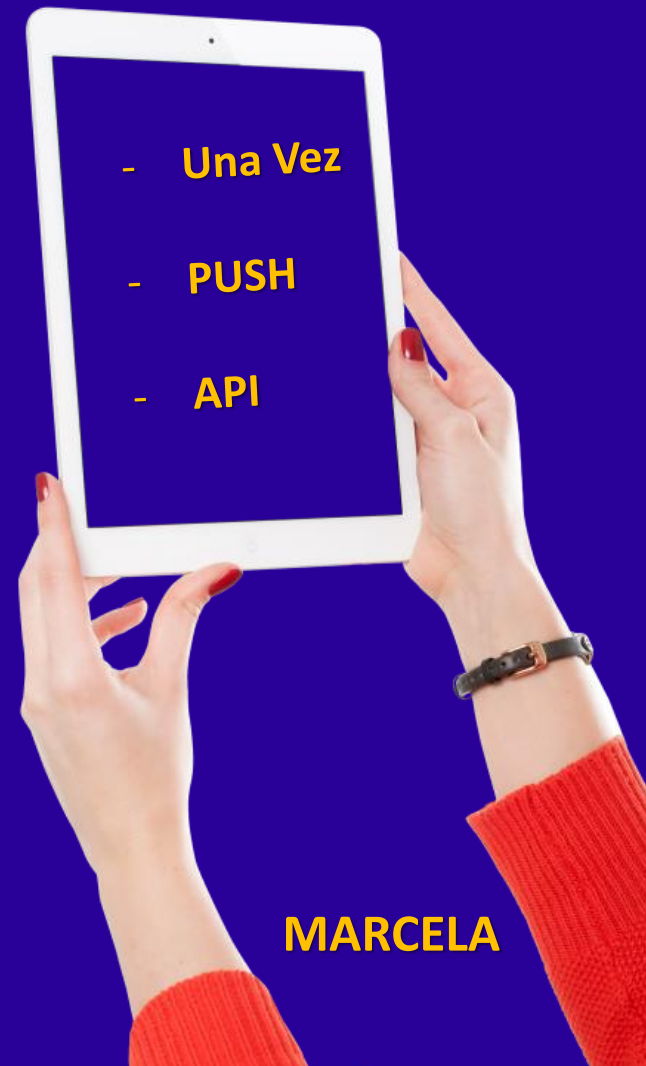
Domicilio Digit@l



Firm@ Digit@l



Identid@d Digit@l



MARCELA



Rank	Country	National Cyber Security Index	Digital development	Difference
3.	Estonia	81.82	79.27	2.55
52.	Chile	38.96	65.71	-26.75
3.	Estonia	90.91	79.27	11.64
36.	Chile	59.74	65.71	-5.97

Ciberseguridad

Transform. Digital

No se puede realizar  
la Transformación Digital  
sin Ciberseguridad

**BASELINE CYBER SECURITY INDICATORS**

5.	Protection of digital services <b>Infra. Crítica Inform.</b>	5	1
8.	Protection of personal data <b>Datos Personales</b>	4	1

SOCIEDAD  
DIGITAL  
SEGURA



<https://ncsi.ega.ee/>

ESTONIA





2018 CIBERATAQUES

2 de 4 Riesgos

EL RIESGO ES MUY ALTO

2021 FALLAS DE CIBERSEGURIDAD

# REPORTE CIBERSEGURIDAD OEA - 2016

OBSERVATORIO DE LA CIBERSEGURIDAD EN AMÉRICA LATINA Y EL CARIBE

## Ciberseguridad

### ¿Estamos preparados en América Latina y el Caribe?

Informe Ciberseguridad 2016

www.observatoriociberseguridad.com

Organization of American States  
Mejorando vidas

## Chile

Política y estrategia

Cultura y sociedad

Educación

Marcos legales

Tecnología

El Ministerio del Interior y Seguridad Pública, el Secretario General de la Presidencia y la Subsecretaría de Telecomunicaciones son los principales organismos nacionales que establecen la política de seguridad cibernética a nivel gubernamental. Si bien el país no ha emitido una estrategia nacional de seguridad cibernética, la sensibilización entre las instituciones gubernamentales es generalizada. La infraestructura gubernamental presenta tecnología de seguridad actualizada y las partes interesadas pertinentes regularmente analizan los activos vulnerabilidades de la Infraestructura Crítica nacional. El Estado también coordina la planeación de gestión de crisis y ha puesto en marcha medidas de redundancia.

Las ramas de las Fuerzas Armadas de Chile comparten responsabilidades de defensa cibernética e información pero no tienen una estructura central de mando y control. Uno de los principales desafíos de Chile de cara al futuro es el fortalecimiento de su capacidad de respuesta ante incidentes: el CSIRT-CL que se encuentra en funcionamiento desde 2004 ofrece respuesta a incidentes para los sitios web del gobierno pero no está institucionalizado formalmente a nivel nacional para abordar todo tipo de violaciones.

Chile ha establecido un marco jurídico global para hacer frente a los delitos cibernéticos. El Decreto Supremo n° 1299 describe las normas y define los roles para el manejo de la delincuencia cibernética, la Ley n° 19.223 introduce los delitos informáticos al Código Penal y la Ley n° 19.628 cubre la privacidad y protección de datos. Aunque el sector privado no está obligado por ley a divulgar las violaciones, el gobierno trabaja en estrecha colaboración con las empresas para informar y responder a incidentes cibernéticos. De acuerdo con las autoridades de Chile, la suplantación y piratería de contenidos son frecuentes. El Departamento de Criminales (O) de los Carib de Chile, Llev forense digiti han detenido cibernéticos tribunales tie manejar evid

La mentalid inconsistente para crear co inició la ca educar a los seguro de Int campaña, lla los ciudadanos comercio ele derechos col de Chile ofre cibernética y cursos en tin Comparativ, vuelto cada de seguridad planes para e

POBLACIÓN TOTAL DEL PAÍS	17.762.647	Penetración de Internet	72%
Abonos a teléfonos celulares	23.683.351		
Personas con acceso a Internet	12.789.105		

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Global Cyber Security Capacity Centre

con QinetiQ. En Warwick, su puesto más reciente fue como Directora de Programas Estratégicos para la División de Gestión de Confianza de la Información. Sus publicaciones recientes incluyen trabajos sobre temas de detección de amenazas internas, analítica visual de ataque cibernético, predicción de la propagación del riesgo cibernético, atribución de identidad en espacios físicos y cibernéticos, privacidad personal de cara a datos grandes, vulnerabilidad de las identidades en contextos de redes sociales, métricas de confiabilidad de los datos de origen abierto y la mejor manera de comunicar el riesgo cibernético.

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Global Cyber Security Capacity Centre

Universidad de Oxford  
https://www.cybersecurity.ox.ac.uk  
enquiries@cybersecurity.ox.ac.uk

42

# 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

**C.M.M.**

PROMULGACIÓN DE UN MARCO JURÍDICO Y REGULATORIO DE CIBERSEGURIDAD

FOMENTO EN LA SOCIEDAD DE UNA CULTURA RESPONSABLE EN CIBERSEGURIDAD

DESARROLLO DE CONOCIMIENTO EN CIBERSEGURIDAD



Global Cyber Security Capacity Centre



**SEPTIEMBRE  
2018**



**Global  
Cyber Security  
Capacity Centre**



**OCSC**  
Oceania Cyber Security Centre  
Australia - Victoria



**MODELO DE MADUREZ  
PARA NACIONES  
CMM**

2016

2020



www.observatoriociberseguridad.com

# CIBERSEGURIDAD

RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE

Reporte Ciberseguridad 2020

BID Mejorando vidas

OEA Más derechos para más gente

# Chile

Metric	2017 Value
Habitantes (Ref: Banco Mundial*)	18.470.439
Abonos a teléfonos celulares (Ref: ITU**)	23.013.147
Personas con acceso a Internet	15.206.248
Porcentaje de penetración de Internet (Ref: ITU**)	82%

74



2016

2020



# LOS "PUERTOS 5G"

94% COMERCIO EXTERIOR



5G  
100 Time Faster  
Speed: 20Gbps  
Download UltraHD Movie in 10 Seconds



**Concurso Público 5G**  
Banda 26 GHz



ALIANZA CHILENA DE CIBERSEGURIDAD

FORMACIÓN EJECUTIVA DF

CLUB CIBERSEGURIDAD

PRIMER ENCUENTRO DIGITAL 4 DE SEPTIEMBRE / 9:00 HRS.

CIBERSEGURIDAD INDUSTRIAL Y CORPORATIVA  
**DESAFÍOS PENDIENTES PARA LA INDUSTRIA 4.0**

**MODERADORA:**  
**Alejandra Moya**  
Directora Alianza Chilena de Ciberseguridad.

**EXPOSITOR:**  
**Cyril Delaere**  
Gerente de Servicios de Ciberseguridad en Entel Ocean.

**EXPOSITORA:**  
**Soledad Bastias**  
Directora Corporativa de Ciberseguridad IT/ OT.

**EXPOSITOR:**  
**Juan Francisco Galli**  
Subsecretario del Interior.

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



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



Si 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 características 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. Un poco, como en cualquier otro oficio, delinquen. Lo que sí es común a estos técnicos es que son personas 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 desarrollo de los movimientos de software libre (gratis y con código abierto), que permitieron que la creación continúe. «Nosotros somos entusiastas de la tecnología. La amamos y, como la conocemos, encontramos los pequeños fallos. En eso trabajamos», afirma María Isabel Rojo, hacker o arquitecta 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.

## Estadas a su aire

Encima, tienen que seguir la moda ni contentarse con su look. Aquí vale todo, tanto que podríamos estar en el mundo de *Travis*: no están sujetos a dictaduras de corbatas o convencionalismos. También si no iba a pensar que Telefónica se incluyese en su Comité de Dirección el año pasado a un tipo de pelos largos, gesto de lana y que se desestresara en mono azulín? Es Chema Alonso, de 42 años, el jefe de Yaiza. Eso sí, si hubiese que hacer un retrato robot de la profesión, sin duda, habría que pintar a un hombre. Como en otras secciones del mundo tecnológico, el de la seguridad informática todavía hoy se conjuga en masculino. «En Estados Unidos y 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

# ARQUITECTURA DE CIBERSEGURIDAD



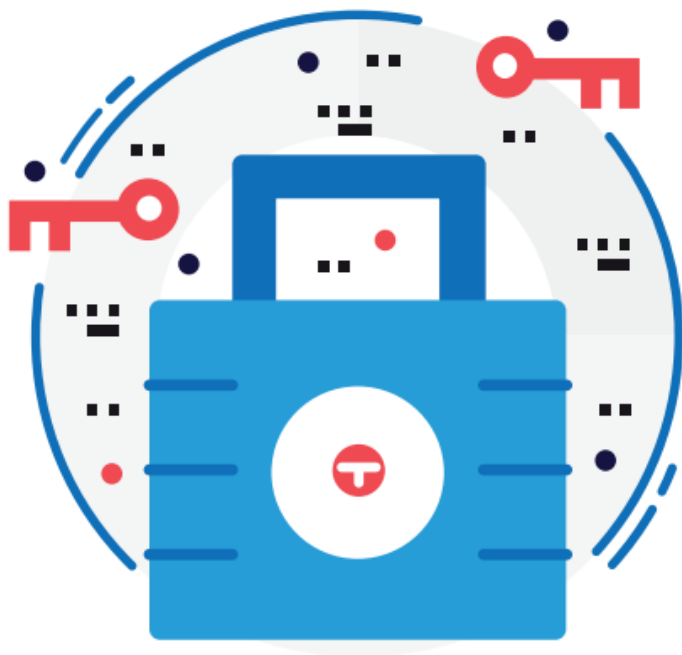
Proyecto de ley de  
Delitos informáticos



# DELITOS INFORMÁTICOS



# Instructivo Presidencial de Ciberseguridad



## 1-Encargado de Ciberseguridad por Servicio

Cada Jefe de Servicio deberá designar a un encargado de ciberseguridad y a un subrogante en un plazo máximo de 10 días hábiles contados desde el lanzamiento del instructivo. Estos nombres deben ser informados al correo [csirt@interior.gob.cl](mailto:csirt@interior.gob.cl), con copia a [ciberseguridad@digital.gob.cl](mailto:ciberseguridad@digital.gob.cl)

## 2-Aplicación y Actualización de Normativa Técnica

Gobierno Digital entregará una nueva normativa técnica actualizada en materia de ciberseguridad, documentos electrónicos, protección de las redes y seguridad de la información, junto al reforzamiento del DS 83 y una guía técnica actualizada del PMG de seguridad de la información.

### 3-Medidas Internas de Ciberseguridad

Cada Jefe de Servicio, en un plazo máximo de 60 días hábiles contados desde el lanzamiento del instructivo, deberá presentar una evaluación de riesgo de ciberseguridad, un análisis del estado de vulnerabilidades, medidas actualmente adoptadas y un plan de acción de corto plazo.

### 4-Revisión de Redes, Sistemas y Plataformas Digitales

Los órganos de la Administración del Estado que cuenten con infraestructura crítica deberán enviar un informe que analice su política interna en materia de ciberseguridad, en el plazo de 30 días corridos desde que sea requerido por el Centro de Coordinación de Entidades de Gobierno.

### 5-Vigilancia y Análisis de Infraestructura

El Centro de Coordinación de Entidades de Gobierno verificará el cumplimiento de las normas y estándares de ciberseguridad vigentes, definirá un esquema de monitoreo en forma continuada y en un trabajo coordinado con cada Jefe de Servicio de la Administración del Estado.

### 6-Reporte Obligatorio de Incidentes

Los órganos de la Administración del Estado deberán reportar la totalidad de incidentes de ciberseguridad que se presenten, tan pronto tomen conocimiento de los mismos, se informará al Centro de Coordinación de Entidades de Gobierno, vía correo electrónico al [csirt@interior.gob.cl](mailto:csirt@interior.gob.cl).

### 7-Respuestas de Incidentes Informáticos

Ante un incidente de ciberseguridad, independientemente de las acciones propias de cada Institución, el Centro de Coordinación de Entidades de Gobierno deberá disponer las acciones que aseguren la continuidad del funcionamiento de las redes y plataformas de los diversos servicios públicos.

### 8-Gobernanza transitoria de Ciberseguridad

Se nombrará a un Coordinador del Sistema Nacional de Ciberseguridad, dependiente del Ministerio del Interior y Seguridad Pública, quien articulará el plan de acción para la implementación de la Política Nacional de Ciberseguridad, la cual contempla la creación de centros de respuesta ante incidencias informáticas.

## 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 llévase 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 Ubaldo Mackenney, Subsecretario del Interior.





## Sesión Especial Mes de La Ciberseguridad

“Hacia una República Digital”



### JUEVES 1 DE OCTUBRE

DESDE LAS 10:00 HRS.

#### Intervienen



**Adriana Muñoz**

Presidenta del Senado de la República de Chile



**Kenneth Pugh**

Senador de la República de Chile



**Felipe Harboe**

Senador de la República de Chile



**Rosa Díaz**

Directora General INCIBE España



**Chema Alonso**

Hacker profesional CDCO de Telefónica

Puedes seguir la sesión vía streaming en los siguientes links:



<https://tv.senado.cl/>



<https://bit.ly/3iZ9rgo>

1



Senador Sr. Kenneth Pugh

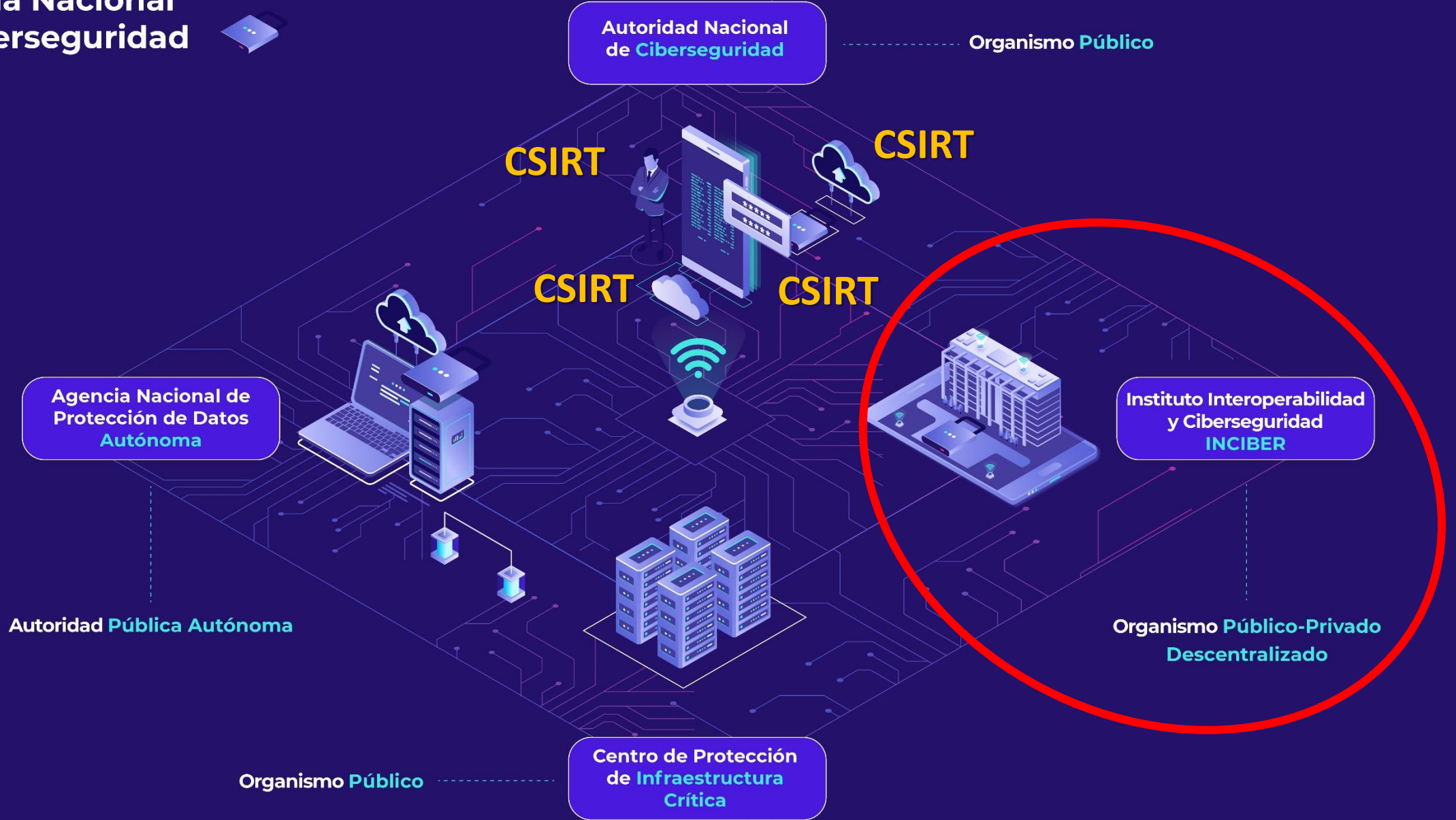


Sr. Eugene Kaspersky





# Sistema Nacional de ciberseguridad



## MISIÓN

La **MISIÓN** del **INCIBER®** es trabajar para afianzar la confianza digital, elevar la ciberseguridad y contribuir al desarrollo de una nueva industria de ciberseguridad, apoyando la transformación digital de manera que se impulse el uso seguro del ciberespacio Chileno.

## VISIÓN





# FIRMA MOU CON INCIBE



La Fundación Inciber "Instituto Nacional de Ciberseguridad de Chile" en formación, es una fundación público-privada sin fines de lucro que tiene por objeto la gestión, generación, asesoramiento, promoción y difusión de proyectos tecnológicos en el marco de la Sociedad de la Información. Entre de sus objetivos está la I&D+i, colaboración, capacitación, promoción y concienciación en materias de Ciberseguridad para los sectores públicos, privados y académicos

Con este documento, INCIBE manifiesta su compromiso para el desarrollo de los mecanismos de colaboración oportunos en el medio y largo plazo entre ambas instituciones, la disposición a contraer futuros acuerdos de colaboración técnica y profesional, y la eventual firma de un "Memorándum de Entendimiento" para la definición y desarrollo de esta colaboración.

Atentamente,

Rosa Díaz Moles  
Directora General INCIBE



**MEMORANDUM OF UNDERSTANDING  
ON COOPERATION IN CYBERSECURITY  
BETWEEN  
THE GOVERNMENT OF THE REPUBLIC OF CHILE  
AND  
THE GOVERNMENT OF THE REPUBLIC OF ESTONIA**

The Government of the Republic of Chile and the Government of the Republic of Estonia, hereinafter referred to as “the Participants”;

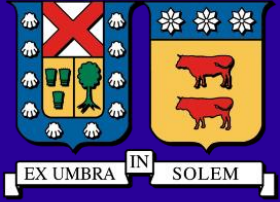
**ACKNOWLEDGING** the importance of cyberspace and its positive impact on the economic and social development of countries, as well as the increasing use by the States of information and communication technologies (ICT), networks, information systems and related technology, integrated to the Internet global network;

**CONSIDERING** that...



**16 Enero 2020**





## INTEROPERABILIDAD



## CIBERSEGURIDAD

## Proyecto busca convertir a Valparaíso en la primera región con interoperabilidad digital



**\$ 400 millones**  
ES EL COSTO ESTIMADO DEL PROYECTO PILOTO DE FEDEFruta

**PRUEBA DICIEMBRE 2020**

meses se puso en marcha smart valpo, proyecto que tiene como piedra angular la implementación de una plataforma de interoperabilidad para intercambiar información entre las organizaciones y avanzar en transformación digital. La iniciativa, impulsada por el senador de Valparaíso Kenneth Pugh y cinco asociaciones gremiales, como la construcción, comercio y frutícola, busca establecer un estándar de interoperabilidad basado en una plataforma tecnológica. "Aspiramos a ser la primera región inteligente y

■ La iniciativa Smart Valpo busca registrar la trazabilidad de las exportaciones chilenas con blockchain. En noviembre de este año realizarán un piloto con Fedefruta.

el proceso de las inversiones de infraestructura, tanto del Gobierno Central, Gobierno Regional o privados. Pugh señala que el objetivo es que se "suban", de manera encriptada, para que los proyectos estén integrados y se pueda hacer su trazabilidad. "Esto permitirá confianza digital, no hay espacio para la corrupción", sostiene.

**Pilotos**  
Una vez que la plataforma esté operativa, planean realizar dos pilotos vinculados a los proyectos

ES-13. Pontificia Universidad Católica de Valparaíso



Universidad de Playa Ancha



Inacap  
UNIVERSIDAD TECNOLÓGICA DE CHILE  
INSTITUTO PROFESIONAL  
CENTRO DE FORMACIÓN TÉCNICA



Duoc UC



Valparaíso



14 Hectáreas  
US\$ 23,7 millones

26 Ghz

PARQUE PRUEBAS CIBER E INTELIGENCIA ARTIFICIAL

26 Ghz



Concurso Público 5G  
Banda 26 GHz



inciber

Valparaíso  
Capital de la  
Ciberseguridad  
del Pacífico Sur

[www.inciber.cl](http://www.inciber.cl)







**OFICINAS**



**CENTRO  
PRUEBAS  
CIBER I.A.**



**POLICIAL**



**DEFENSA**



**CITA**  
IDEAS DESDE EL MAR



# ECOSISTEMA CIBERSEGURIDAD



**PDI**

**UNAB**

**SENADO**

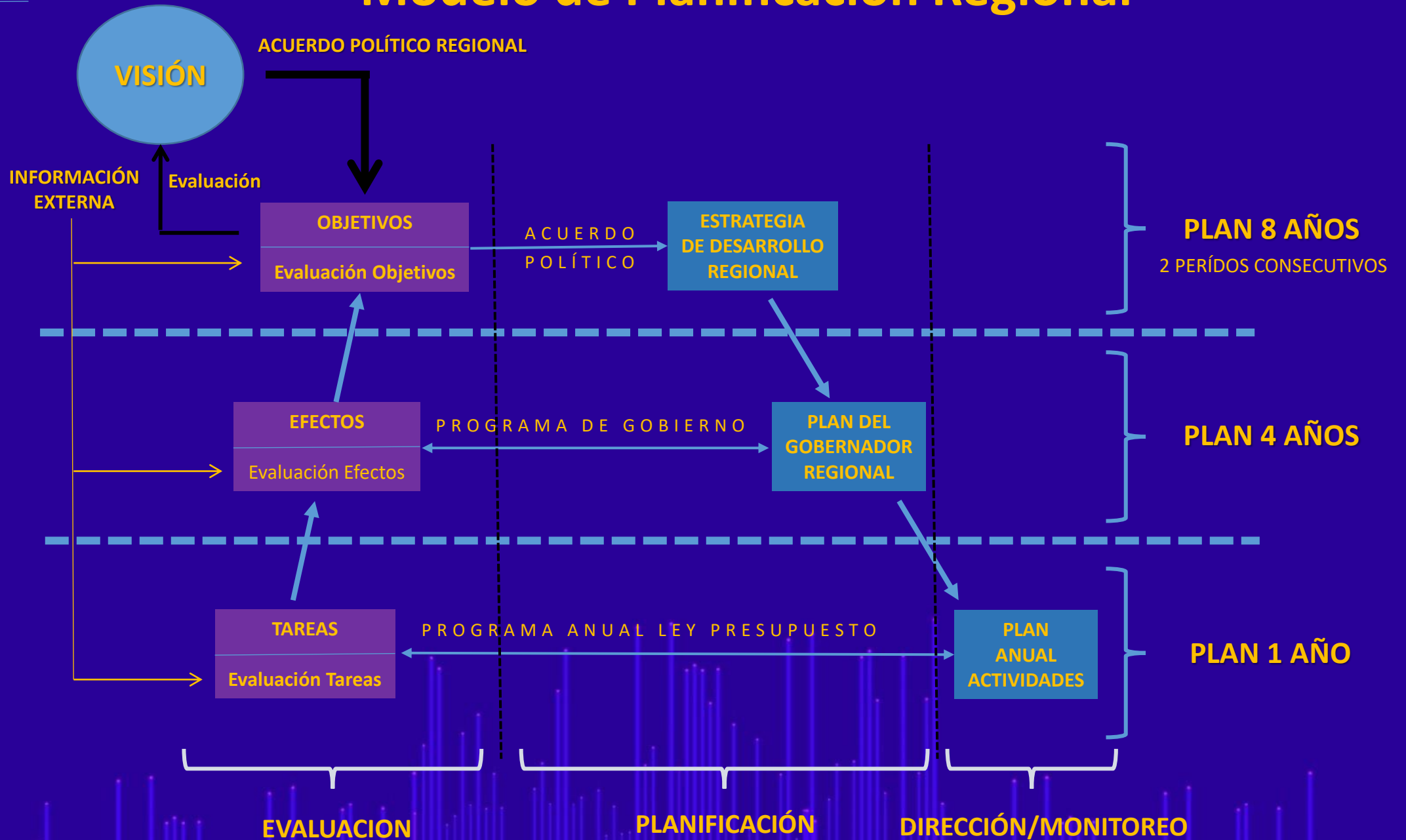
**USM**

**ARMADA**

**CORFO**

**SISDEF**

# Modelo de Planificación Regional



# Modelo de Financiamiento Regional

**INVERSIONES  
GOBIERNO  
CENTRAL  
(SECTORIALES)**

**INVERSIONES  
GOBIERNO  
REGIONAL  
(CORE)**

**INVERSIONES  
PRIVADAS**

QUÉ PASA

Antropología

Isla de Pascua

...

## Las lecciones de la Isla de Pascua para la futura colonización de Marte

Un estudio explora cómo los complejos patrones comunitarios en Rapa Nui ayudaron a la gente a sobrevivir desde su asentamiento en los siglos XII al XIII hasta el contacto con los europeos, un aislamiento que podría ayudar a entender cómo los astronautas en Marte podrían asentarse en el planeta.

Europa Press 13 MAY 2021 09:45 AM



**EXCEPCIÓN CONSTITUCIONAL (Art 126 bis)**

**GLOSA ESPECIAL (Glosa Insular)**

**LEY DE CONTROL MIGRATORIO (Ley 21.070)**

**MODELO DE CARGA (Consejo Local)**

**DESPLIEGE 5G Y FIBRA ÓPTICA SUBMARINA**

# COMISIÓN DESAFÍOS DEL FUTURO DEL SENADO

Zoom Reunión

Kenneth Pugh... Julio Cámara David Bravo María Paz Her... Senador Girar... Nicolas Luco

Grabando



REPUBLICA DE CHILE  
SENADO

José Inostroza

Cancelar silenciar ahora Detener video

Participantes 35 Chat Compartir pantalla Reacciones

Salir

Escribe aquí para buscar

15:31 25-01-2021



**OEA**  
**Laboratorio Ciberseguridad para Parlamentarios**  
**Consejo Innovación Ciberseguridad - CIC**



**PARLAMENTO ANDINO**  
**Marco normativo para el fortalecimiento de**  
**la ciberseguridad en la región andina**



**SENADO CHILE**  
**Comisión de Ciencia, Tecnología y**  
**Desafíos del Futuro**

# El Ecosistema de la Transformación Digital en el Estado

Chile hacia una  
República Digital



Por la Razón o la Fuerza  
de los DATOS



@kpughsenador

Kenneth Pugh  
Senador por Valparaíso