Ciberseguridad

Desafíos Legislativos

KENNETH PUGH
SENADOR REGIÓN VALPARAÍSO

La Sociedad Digital Segura

Estamos transitando hacia un “Sociedad Digital”

Dependeremos cada vez mas de sistemas digitales

Necesitaremos cada vez mas conectividad digital

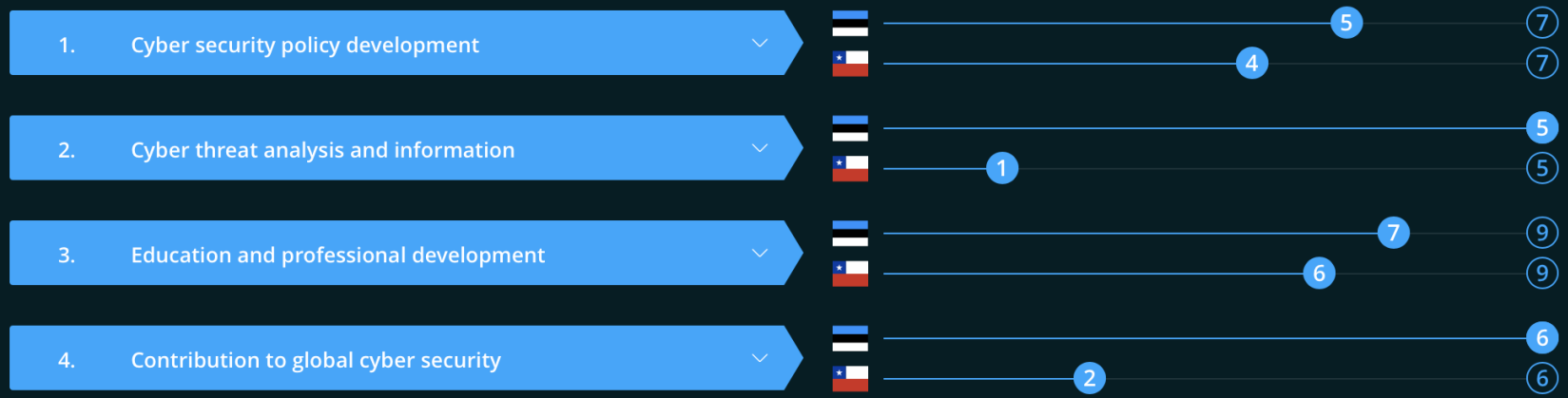
¿ Sabemos si esta nueva Sociedad será segura ?

¿ Qué haremos para contribuir a su seguridad ?

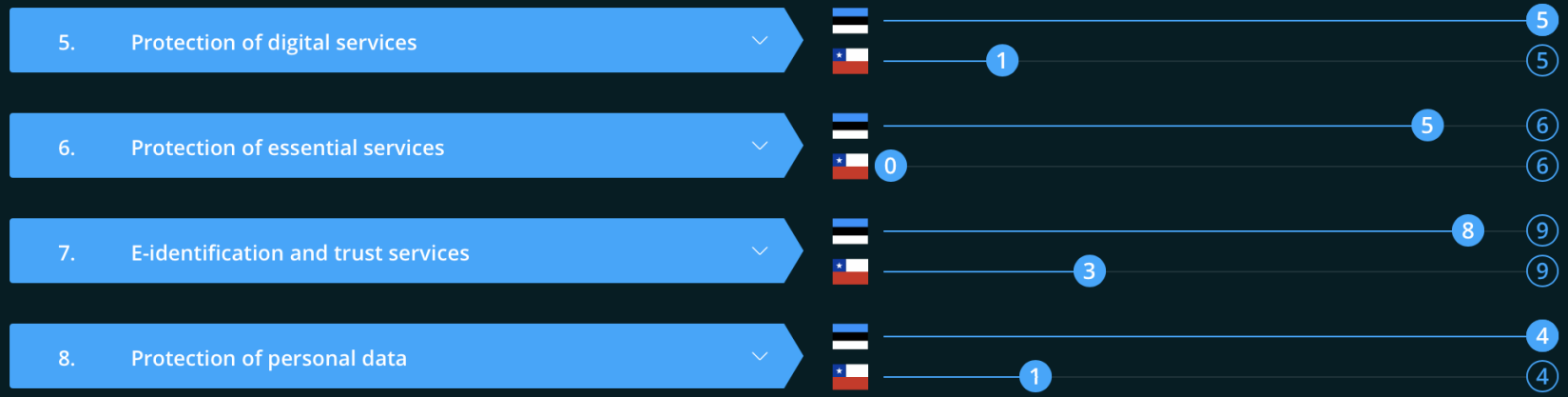
Rank	Country	National Cyber Security Index	Digital development	Difference
3.	Estonia	81.82	79.27	2.55
52.	Chile	38.96	65.71	-26.75

SOCIEDAD DIGITAL SEGURA

GENERAL CYBER SECURITY INDICATORS



BASELINE CYBER SECURITY INDICATORS



https://ncsi.ega.ee/

RIESGOS GLOBALES 2018

FORO ECONÓMICO MUNDIAL 2018

2 de 4 Riesgos

ESTE ES EL ESCENARIO:

EL RIESGO ES MUY ALTO

DONDE ESTÁBAMOS

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
More rights for more people

BID

REPORTE

Chile

El Ministerio del I
el Secretario Gen
Subsecretaría de
los principales o
establecen la polít
nivel gubernam
mitido una estra
bernética, la
stituciones guber
raestructura gube
seguridad actua
rtinentes regula
ulnerabilidades
cional. El Estado
gestión de crisis y
redundancia.

ramas de las
mparten respo
bernética e info
uctura central d
ncipales desafío
ortalecimiento
cidentes: el CS
cionamiento de
dentes para los
está institucion
cional para abor

ile ha establecido un marco jurídico global
ra hacer frente a los delitos cibernéticos. El
ecreto Supremo n° 1299 describe las normas y
efine los roles para el manejo de la delincuencia
bernética, la Ley n° 19.223 introduce los delitos
nformáticos al Código Penal y la Ley n° 19.628
obre 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

ptales para abordarlos.

POBLACIÓN TOTAL DEL PAÍS	17.762.647
Abonos a teléfonos celulares	23.683.351
Personas con acceso a Internet	12.789.105

Penetración de Internet

72%

62

CIBERSEGURIDAD

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Global Cyber Security Capacity Centre

y privacidad. Desde 2005, ha participado en trabajos de investigación con otros profesionales, como psicólogos, sociólogos, economistas, politólogos, abogados, criminólogos y filósofos, entre otros. Creese tiene experiencia en filosofía, matemáticas y ciencias de la computación y ha trabajado profesionalmente en organizaciones comerciales, gubernamentales y académicas. Antes de incorporarse a Oxford en octubre de 2011, fue Profesora y Directora de Seguridad Electrónica del Laboratorio Digital Internacional de la Universidad de Warwick. Creese se vinculó a Warwick en 2007 después de haber trabajado 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

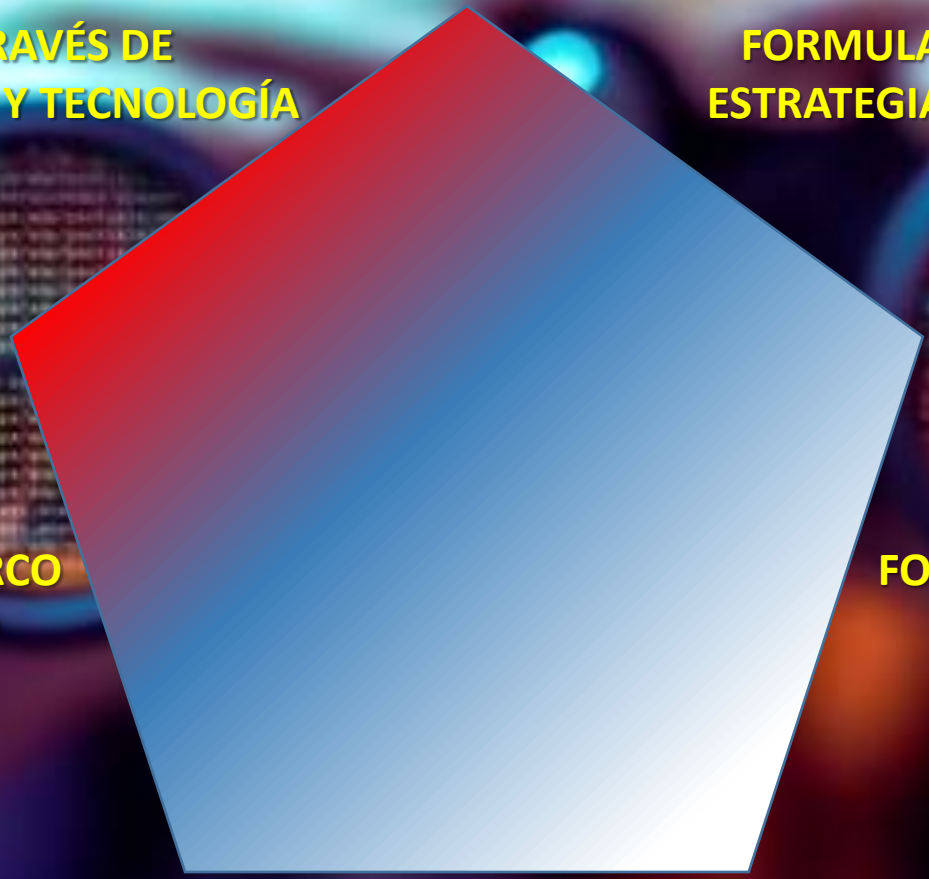
OEA

HACIA DONDE VAMOS

MODELO DE MADUREZ 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

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Global Cyber Security Capacity Centre

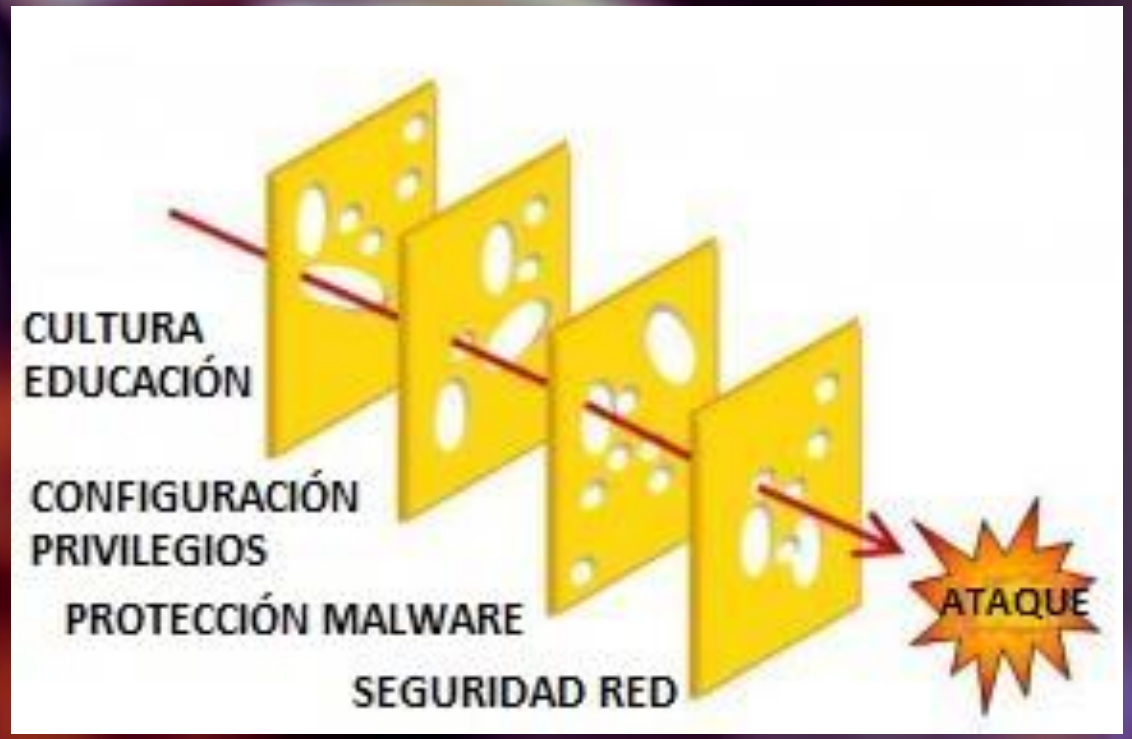
MODELO DE MADUREZ PARA NACIONES CMM

Ciberseguridad es sinónimo de “Cambio Constante”

¿ Como la hacemos para ir EVOLUCIONANDO con la Ciencia y la Tecnología, a la par de la Inovacción, sin tener que estar REACCIONANDO ?

LIDERAR EL CAMBIO – ADAPTÁNDONOS RÁPIDAMENTE

TEORÍA DE SEGURIDAD: “QUESO SUIZO”



10 Steps To Cyber Security

CESG

Defining and communicating your Board's Information Risk Management Regime is central to your organisation's overall cyber security strategy. CESG recommend you review this regime - together with the nine associated security areas described below - in order to protect your business against the majority of cyber threats.

User Education and Awareness

Produce user security policies covering acceptable and secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

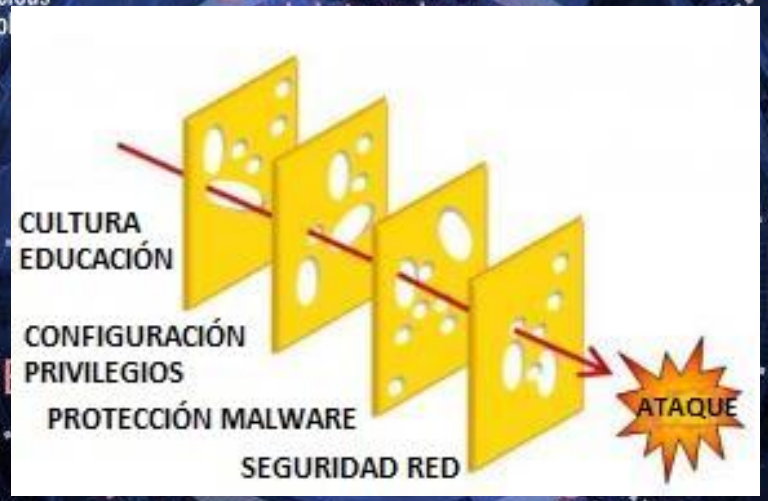
Home and Mobile Working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest.

Network Security

Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security contro

Establish an effective governance structure



Secure Configuration

Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.

Malware Protection

Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.

Removable Media Controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing on to the corporate system.

policies.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activity that could indicate an attack.

Managing User Privileges

Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident Management

Establish an incident response and disaster recover capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

Department for Business Innovation & Skills | CPNI Centre for the Protection of National Infrastructure | Cabinet Office

National Cyber Security Centre

a part of GCHQ

https://www.ncsc.gov.uk/

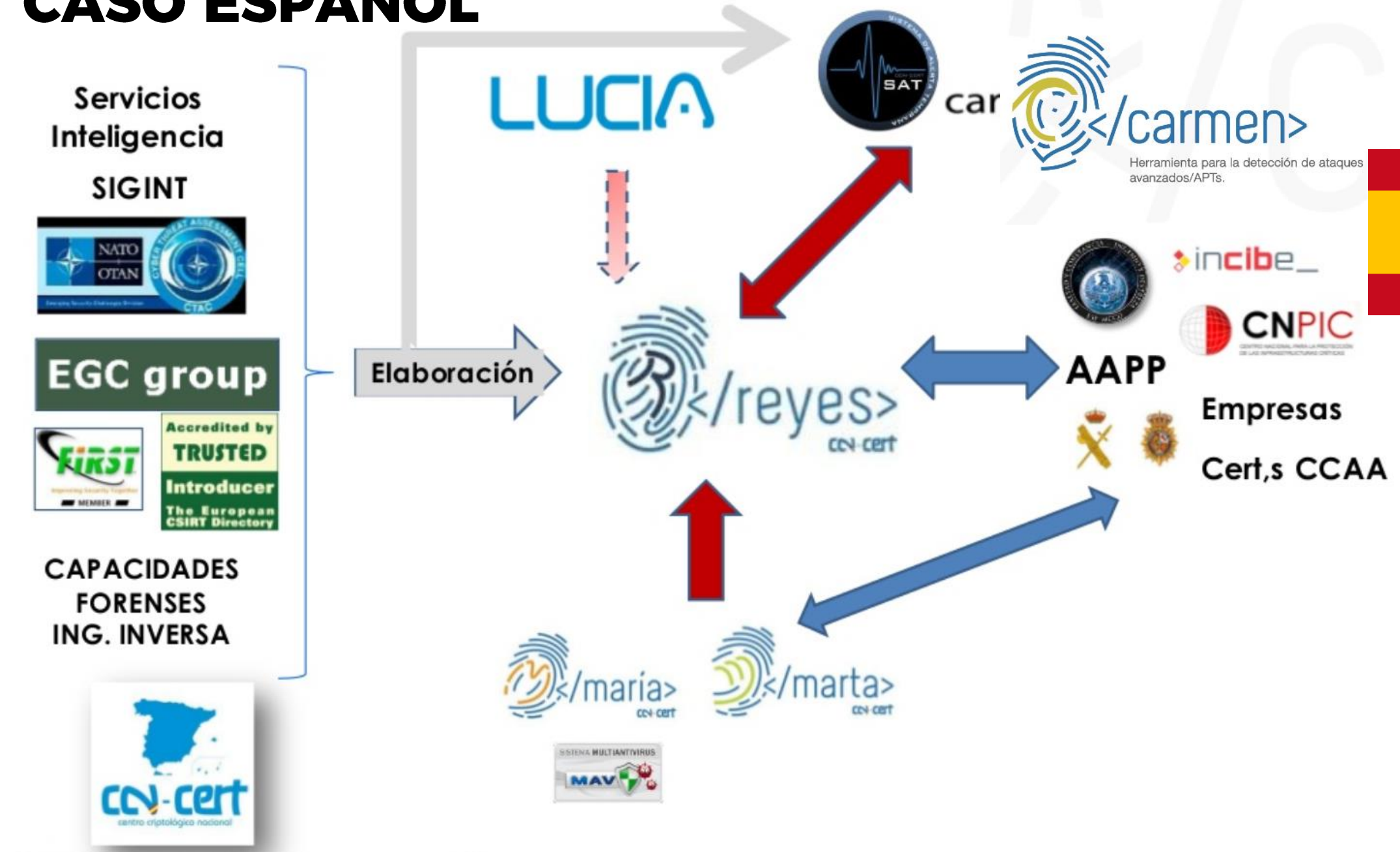
Ciberseguridad es sinónimo de “Confianza”

“seguir mejorando para minimizar el riesgo”, reducir el número de incidentes y conseguir que los clientes puedan seguir disfrutando de sus servicios.

Gestión del Riesgo de la Información y del Control Digital

REYES (REpositorio común Y ESTructurado de amenazas y código dañino)

CASO ESPAÑOL



CNPIC
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD

http://www.cnpic.es/

CARABINEROS - PDI

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*. 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 permiten que la creación continúe. «Nosotros somos entusiastas de la tecnología. La amamos y, como la conocemos, encontramos sus 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*.

11%

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

stidas a su aire

Encima tienen que seguir la moda ni contentar a nadie con su *look*. Aquí vale todo, tanto que podríamos estar en el mundo de *Friki*s: no están sujetos a dictaduras de corbatas o convencionalismos. ¿Quién si no iba a pensar que Telefónica incluyese en su Comité de Dirección a un tipo de pelos largos, gorro de lana y que se desestresa en monopatín? 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%.»

BRECHA DE GÉNERO

REVISTA COSMOPOLITAN SEPTIEMBRE 2018

CIBERSEGURIDAD

2017

CIBERDEFENSA

DIARIO OFICIAL
DE LA REPUBLICA DE CHILE
Ministerio del Interior y Seguridad Pública

I SECCIÓN

LEYES, REGLAMENTOS, DECRETOS Y RESOLUCIONES DE ORDEN GENERAL

Núm. 42.003 | Viernes 9 de Marzo de 2018 | Página 1 de 6

Normas Generales

CVE 1363153

MINISTERIO DE DEFENSA NACIONAL

APRUEBA POLÍTICA DE CIBERDEFENSA

2018

Núm. 3.- Santiago, 9 de noviembre de 2017.

Vistos:

1. Las facultades establecidas en el artículo 32, número 6° de la Constitución Política de la República de Chile;
2. La Ley N° 20.424, Orgánica del Ministerio de Defensa Nacional;
3. Lo preceptuado en el decreto supremo N° 248, de 29 de noviembre de 2010, que aprueba reglamento orgánico y de funcionamiento del Ministerio de Defensa Nacional;
4. Lo establecido en el decreto supremo N° 533/2015, de 27 de abril de 2015, que crea el Comité Interministerial sobre Ciberseguridad;
5. Lo ordenado en el Instructivo Presidencial N° 1/2017, de 27 de abril de 2017, que aprueba e instruye la implementación de la Política Nacional de Ciberseguridad;
6. Lo establecido en la Orden Ministerial N° 2, de 9 de octubre de 2015, del Ministro de Defensa Nacional, que dispone iniciar el proceso de elaboración de una Política de Defensa en materias de ciberespacio;
7. Lo propuesto por la Subsecretaría de Defensa, y;

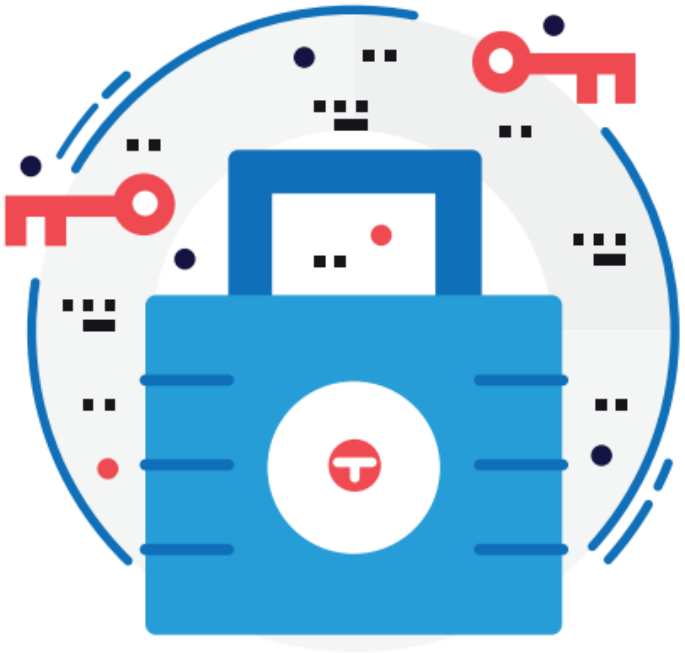
Considerando:

1. Que la ley N° 20.424 establece que le corresponderá al Ministro de Defensa Nacional proponer a la Presidenta de la República la política de defensa nacional y la documentación de la planificación primaria de la Defensa Nacional;
2. Que la ley N° 20.424 establece que le corresponderá al Subsecretario de Defensa sugerir al Ministro de Defensa Nacional la política de defensa nacional y la planificación primaria de la defensa nacional, así como su actualización y explicitación periódica;
3. Que atendido el desarrollo tecnológico y la creciente incorporación de tecnologías de la información y las comunicaciones en los procesos cotidianos y críticos de la Defensa Nacional, resulta necesario adaptar y actualizar las disposiciones de la política de defensa y los contenidos de la planificación vigente, adecuándolas a este nuevo contexto para una mejor seguridad y defensa nacional;
4. Que el creciente uso de tecnologías de la información y las comunicaciones suponen el surgimiento de nuevos riesgos y amenazas para la seguridad del país, sus habitantes y sus infraestructuras, los cuales deben ser abordados de manera integral;
5. Que, para ello, se aprobó e instruyó la implementación de la Política Nacional de Ciberseguridad, que tiene por objeto esencial resguardar la seguridad de las personas y de sus derechos en el ciberespacio y plantea además cinco objetivos estratégicos de largo plazo, destinados a abordar los múltiples desafíos que enfrenta nuestro país, y un conjunto de medidas de política pública;
6. Que una de las medidas urgentes de la Política Nacional de Ciberseguridad consiste en el establecimiento de una Política de Ciberdefensa que fije los objetivos a ser cumplidos gradualmente hasta el año 2022 por las instituciones de la Defensa Nacional en este ámbito;
7. Que el presente instrumento configura la respuesta del Estado de Chile a los nuevos riesgos y amenazas que el ciberespacio genera para las capacidades de la Defensa Nacional, las cuales incluyen, entre otros elementos, la información, infraestructura y operaciones de defensa;
8. Que, asimismo, esta política forma parte de la Política de Defensa y, por tanto, sostiene los mismos principios básicos que tienen plena expresión en el ciberespacio: el respeto del

LA ARQUITECTURA PARA UN SISTEMA NACIONAL

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, con copia a 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.**

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.

Desafíos Legislativos

LEY DE PROTECCIÓN DE DATOS PERSONALES

LEY DE PROTECCIÓN INFRAESTRUCTURA CRÍTICA INFORMACIÓN

MES CHILENO DE LA CIBERSEGURIDAD (OCTUBRE)

MES DE LA CIBERSEGURIDAD

October is

National Cyber Security Awareness Month

OCTOBER

EUROPEAN CYBER SECURITY MONTH

Online security requires your participation

Este año, el Departamento de Seguridad Interior (DHS) desarrolló la campaña "Stop. Think. Connect".

Esta será desarrollada con distintos objetivos durante 5 semanas:

Semana 1: Pasos simples para mantenerse seguro en línea

Semana 2: La seguridad informática en el lugar de trabajo es cosa de todos

Semana 3: Predicciones actuales para Internet del futuro

Semana 4: Internet te necesita: piensa en seguir una carrera relacionada con la seguridad informática

Semana 5: Protegiendo la infraestructura crítica de los ciberataques

Cada semana está dedicada a un tema distinto:

- 1ª semana — 2-6 octubre: Ciberseguridad en el lugar de trabajo.
- 2ª semana — 9-13 octubre: Gobernanza, privacidad y protección de datos
- 3ª semana — 16-20 octubre: Ciberseguridad en el hogar
- 4ª semana — 23-27 octubre: Competencias en materia de ciberseguridad

EUROPEAN CYBER SECURITY MONTH

5th Anniversary

MOIS EUROPÉEN DE LA CYBERSÉCURITÉ

Du 1er au 31 octobre 2017

#TousSecNum

CASO ESPAÑOL

EJERCICIOS INTERNACIONALES

#CyberEx18, una iniciativa de la OEA (Organización de los Estados Americanos), INCIBE (Instituto Nacional de Ciberseguridad de España) y CNPIC (Centro Nacional de Protección de Infraestructuras y Ciberseguridad)

El campeonato ha contado con 300 participantes, de 35 países, repartidos en 75 equipos, de los cuales el 42% eran del sector privado; un 32% del sector público, un 10% académico y un 8% militar.

EJERCICIOS NACIONALES

EJERCICIOS INTERNACIONALES

CyberEx 2018

https://www.ccdcoe.org/

CCDCOE

NATO Cooperative Cyber Defence Centre of Excellence
Tallinn, Estonia

LOCKED SHIELDS

EJERCICIOS CIBERSEGURIDAD

MES DE LA CIBERSEGURIDAD

ALIANZA CHILENA DE CIBERSEGURIDAD

Asociación de Aseguradores de Chile

Asociación Chilena de Empresas de Tecnología de Información (ACTI)

Cámara Chilena Norteamericana de Comercio (AmCham Chile)

Cámara de Comercio de Santiago (CCS)

Colegio de Ingenieros de Chile

Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile

Fundación País Digital

Instituto Chileno de Derecho y Tecnologías

Universidad Tecnológica de Chile Inacap

30 de Mayo 2018

Ley Octubre “Mes Nacional de la Ciberseguridad”

Tramitación

Sesión/Leg.	Fecha	Subetapa	Etapa	Ver Documentos
	09/05/2018	Ingreso de proyecto .	Primer trámite constitucional / Senado	Mensaje/Moción
15 / 366	15/05/2018	Cuenta de proyecto . Pasa a Comisión de Defensa Nacional	Primer trámite constitucional / Senado	
	29/05/2018	Primer informe de comisión de Defensa Nacional.	Primer trámite constitucional / Senado	Informe
20 / 366	30/05/2018	Cuenta de primer informe de comisión .	Primer trámite constitucional / Senado	
20 / 366	30/05/2018	Discusión general . Aprobado en general y particular a la vez	Primer trámite constitucional / Senado	Diario Votación
	30/05/2018	Oficio de ley a Cámara Revisora .	Primer trámite constitucional / Senado	Oficio
29 / 366	31/05/2018	Cuenta de proyecto . Pasa a Comisión de Defensa Nacional	Segundo trámite constitucional / C.Diputados	
	21/08/2018	Primer informe de comisión de Defensa Nacional.	Segundo trámite constitucional / C.Diputados	Informe
62 / 366	22/08/2018	Cuenta de primer informe de comisión .	Segundo trámite constitucional / C.Diputados	
69 / 366	06/09/2018	Discusión general . Aprobado en general y particular sin modificaciones .	Segundo trámite constitucional / C.Diputados	Diario
	06/09/2018	Oficio aprobación sin modificaciones a Cámara de Origen .	Segundo trámite constitucional / C.Diputados	Oficio
51 / 366	11/09/2018	Cuenta oficio aprobación sin modificaciones de C. Revisora .	Trámite finalización en Cámara de Origen / Senado	
	11/09/2018	Oficio de ley al Ejecutivo .	Trámite finalización en Cámara de Origen / Senado	Oficio

Declara el mes de Octubre de cada año, como el mes nacional de la Ciberseguridad, con el fin de promoverla y realizar ejercicios nacionales de ciberseguridad".

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.".

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.

LEY 21.113

LANZAMIENTO – 1 OCTUBRE 2018

LANZAMIENTO – 1 OCTUBRE 2018

PDI

nacap

CASO ESPAÑOL – LEON (DESCENTRALIZADO)

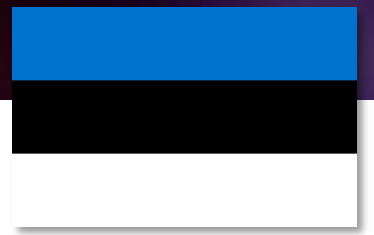
INCIBE
INSITITUTO CIBERSEGURIDAD ESPAÑOL

MINISTERIO ECONOMIA

certsi_
CERT DE SEGURIDAD E INDUSTRIA

CNPIC
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD

CASO ESTONIA



Cybersecurity Act[1]

Passed 09.05.2018

Chapter 1
GENERAL PROVISIONS

§ 1. Subject matter and scope of Act

(1) This Act provides for the requirements for the maintenance of network and information systems essential for the functioning of society and state and local authorities' network and information systems, liability and supervision as well as the bases for the prevention and resolution of cyber incidents.

(2) This Act is not applied to the processing of state secrets and classified information of foreign states or to the maintenance of processing systems for such information.

(3) This Act is not applied to digital service providers which employ on average fewer than 50 persons during a financial year and whose annual balance sheet total or annual turnover does not exceed 10 million euros, taking into account the definitions of micro and small enterprises in European Commission Recommendation 2003/361/EC concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.05.2003, pp. 36–41).

(4) If the requirements for the maintenance of network and information systems are provided by an international agreement or another act, this Act is applied with the specifications arising from the international agreement or other act.

CASO ESPAÑOL

BOLETÍN OFICIAL DEL ESTADO
Núm. 218 Sábado 8 de septiembre de 2018 Sec. I. Pág. 87675

I. DISPOSICIONES GENERALES

JEFATURA DEL ESTADO

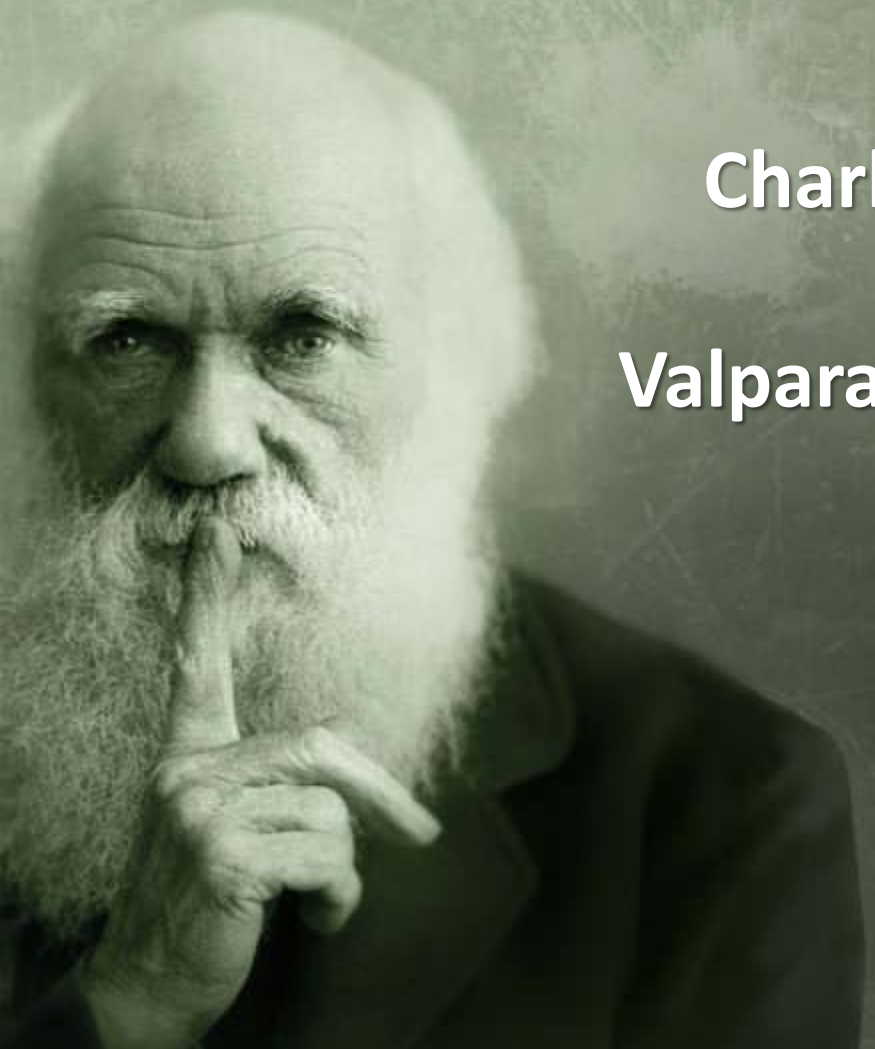
12257 *Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.*

I

La evolución de las tecnologías de la información y de la comunicación, especialmente con el desarrollo de Internet, ha hecho que las redes y sistemas de información desempeñen actualmente un papel crucial en nuestra sociedad, siendo su fiabilidad y seguridad aspectos esenciales para el desarrollo normal de las actividades económicas y sociales.

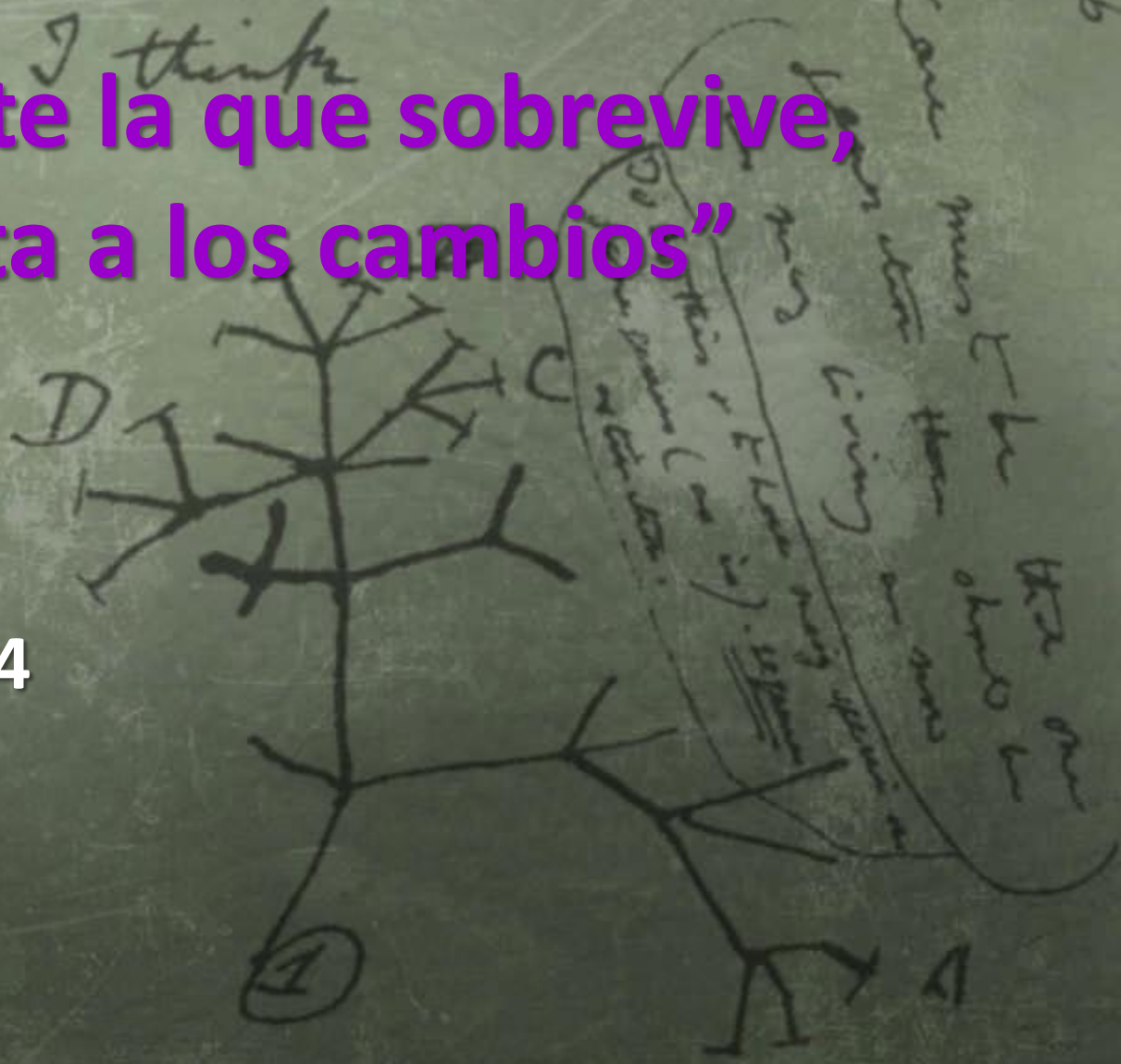
Por ello, los incidentes que, al afectar a las redes y sistemas de información, alteran

“No es la especia mas fuerte la que sobrevive, sino, la que mejor se adapta a los cambios”



Charles Darwin

Valparaíso: Julio 1834



Ciberseguridad

Desafíos Legislativos

KENNETH PUGH
SENADOR REGIÓN VALPARAÍSO