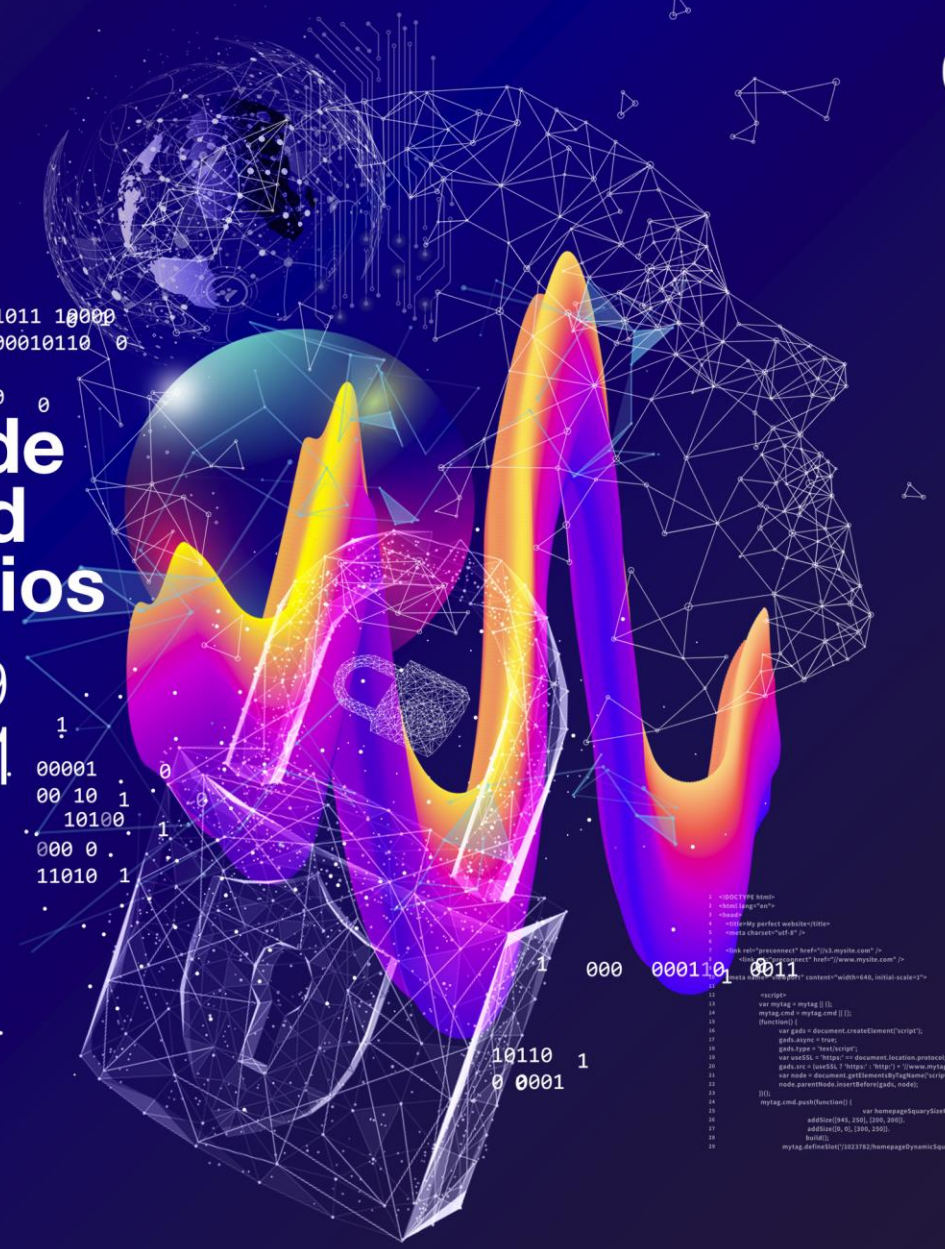
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021

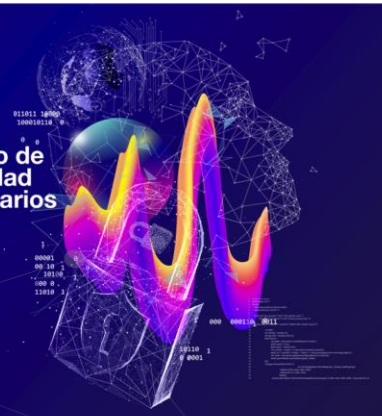


Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos



“Ciberseguridad en el Estado: análisis del nuevo marco normativo”

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

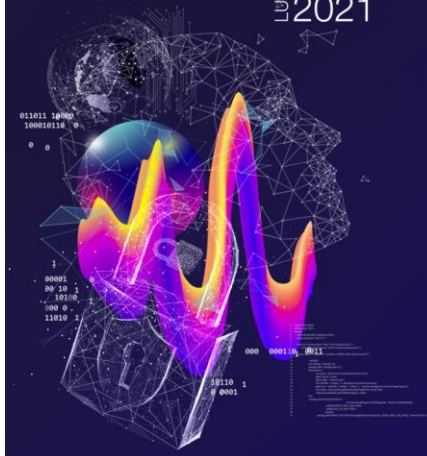
Crecimiento exponencial de los ataques

Las sociedades occidentales dependen profundamente de los sistemas informáticos para los procesos industriales, el comercio, la actividad bancaria, servicios públicos, generación y distribución de energía y agua, entre otros, los cuales además están interrelacionados.

Y por otro lado las motivaciones que ofrece el ciberespacio son muy considerables, entre ellas:

- Un ataque cibernético será siempre más simple y menos riesgoso que un ataque tradicional. Lo único que se necesita es un computador y una conexión a Internet.
- Gozan del anonimato ya que se pueden llevar a cabo ataques remotos.
- El riesgo oculto del proceso de modernización, digitalización y dependencia de proveedores supone una mayor vulnerabilidad de las infraestructuras esenciales y la consideración de la amenaza que un ataque representaría para su continuidad operacional.
- La cobertura mediática siempre será muy elevada, causando una grave preocupación entre la población y un fuerte reproche a las autoridades.

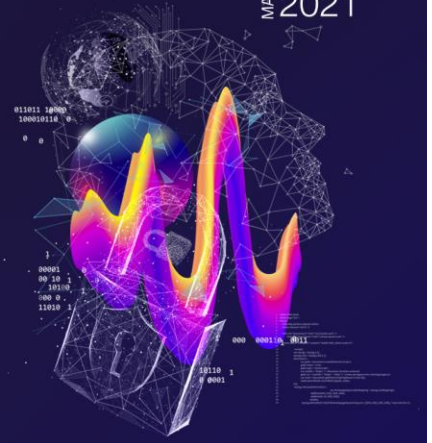
2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021



Ejemplos en el mundo de Ciberataques

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Ejemplos en Chile de Ciberataques

Agrosuper y Ariztía sufrieron fraude informático

11/01/2019 por Willars Sepúlveda

Hace pocos días se conoció la noticia de un nuevo ciberataque que volvió la seguridad informática de empresas en Chile. Esta vez las afectadas fueron 2 de las más grandes productoras y comercializadoras de alimentos. Arauco y Agrosuper. Ambas sostienen un comunicado en sus respectivos sitios web, alertando de la situación e invitando a sus clientes a canalizar sus denuncias con ellos.

De acuerdo a información consignada en el Diario Financiero, los atacantes habrían llegado correos maliciosos a los ejecutivos de estas empresas, logrando sustraer información privilegiada, como por ejemplo el formato tipo de correos y documentos que utilizan para comunicarse formalmente con sus clientes, así como las credenciales para acceder a las carteras de clientes, con sus datos e información de contacto.

Ciberataque a BancoEstado: empresa sufre inédita paralización en sucursales y presenta querella

Si bien hasta ahora no se ha reportado robo de dinero, las 410 sucursales de la estatal amanecieron cerradas, aunque en el día reabrieron 24. El banco presentó una querella por sabotaje informático, y la CMF se instaló en las dependencias de la entidad. Esperan reabrir el resto de las sucursales durante la semana.

Mariano Monsalve 2 SEP 2020 5:21 PM

Hackeo a Gobierno Digital obliga a iniciar proceso de actualización de la Clave Única

La Segpres ingresó una denuncia al Ministerio Público para que indague a los responsables del ataque. Cambio de la interfaz y mensajes con insultos fueron las primeras señales de la vulneración informática.

Ciberataque a siderúrgica CAP: dejan mensaje extorsivo para cobrar por "rescate" del sistema

Gobierno alerta sobre ciberataque a empresa proveedora de grandes hospitales

La firma ECM, que posee una plataforma para exámenes de imagenología en recintos como el Sótero del Río, dio aviso de "secuestro de datos" el jueves pasado. El sistema está en proceso de regularización y la cartera aclaró que no se vio afectada la atención o datos de pacientes.

CHILE SUFRIÓ MÁS DE 525 MILLONES DE INTENTOS DE CIBERATAQUES EN EL PRIMER SEMESTRE DEL 2020

Santiago, 02 septiembre de 2020 – Según informes de la plataforma Threat Intelligence Insider Latin America de Fortinet, herramienta que recopila y analiza incidentes de ciberseguridad en todo el mundo, la pandemia COVID-19 y los ataques de "fuerza bruta" fueron un catalizador para el aumento de la actividad cibercriminal durante la primera mitad del 2020.

Chile fue objetivo de **525 millones de intentos de ciberataque** entre enero y junio de este año, sumando el total de 15 mil millones de intentos en América Latina y el Caribe durante el mismo periodo.

Hackers atacaron base de datos de Cencosud y piden rescate

El ataque es atribuido al ransomware Egregor.

Los ataques informáticos en Chile han aumentado en torno a un 35% en los últimos meses, afectando a diversas entidades como bancos, Gobierno y AFPs.

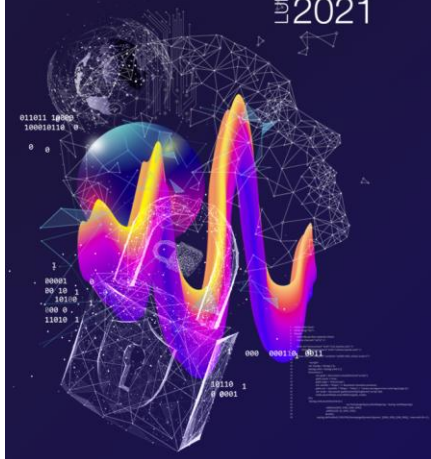
por FELIPE GARRIDO

COMPARTIDOS

Un reciente estudio realizado por la empresa dedicada a la investigación de la seguridad en Internet Fortinet arrojó que, durante los últimos meses (post estallido social), han aumentando los ciberataques en Chile en torno al 35%.

2do Seminario de Ciberseguridad para funcionarios públicos

LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

¿Por qué se requiere una iniciativa legislativa?

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

1.- Para resguardar la seguridad de las personas en el ciberespacio

Es necesario brindar a las personas un nivel de seguridad que les permita el normal desarrollo de sus actividades personales, sociales y comunitarias en el ciberespacio, junto con el ejercicio de derechos fundamentales como la libertad de expresión, el acceso a la información, la protección de la vida privada y la propiedad; incluso la vida.

2.-Para proteger el Estado

Es necesario promover el resguardo de las redes y sistemas informáticos del sector público, especialmente aquellas que son esenciales y críticos para el adecuado funcionamiento del país, velando por la continuidad operacional de ellos.

3.- Para promover la seguridad del país

Promover el resguardo de las redes y sistemas informáticos del sector privado, especialmente, aquellas que son esenciales y críticas para el adecuado funcionamiento del país, velando y asegurando por la continuidad operacional de las infraestructuras críticas de la información del país.

4.- Para prevenir la amenaza sistémica

Mejorar las instancias de comunicación, coordinación y colaboración entre instituciones, organizaciones y empresas, tanto del sector público como privado, nacionales e internacionales, con el propósito de fortalecer la confianza y entregar una respuesta común a los riesgos del ciberespacio previniendo el fenómeno de la amenaza sistémica sectorial evitando la expansión de los efectos perjudiciales de un incidente.

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

¿Por qué se requiere una iniciativa legislativa?

5. Para gestionar los riesgos del ciberespacio

Es necesario considerar el desarrollo de procesos de análisis y gestión de riesgos que permitan identificar las vulnerabilidades, amenazas y riesgos implícitos en el uso, procesamiento, almacenamiento y transmisión de la información, junto a la generación de las capacidades para la prevención y la recuperación ante incidentes de ciberseguridad que se presenten, configurando un ciberespacio estable y resiliente.

6. La ciberseguridad es clave en el proceso de transformación digital y para la IA

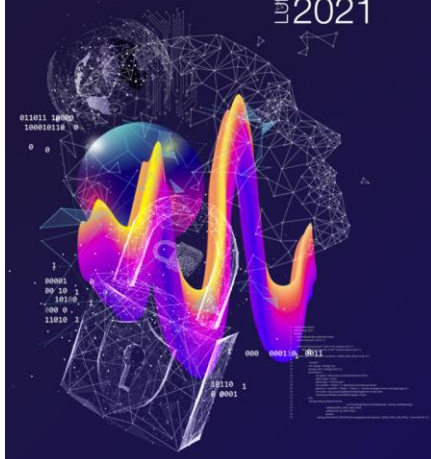
La transformación digital y la inteligencia artificial nos están aportando soluciones muy potentes, pero todo eso se puede volver en nuestra contra si no adaptamos los diferentes procesos a los actuales requerimientos de ciberseguridad. Por ello, la implementación de la transformación digital y la inteligencia artificial deben estar cimentadas en las bases de la ciberseguridad

7. Cumplimiento de la Política Nacional de Ciberseguridad

Con la presentación del Proyecto de Ley, se da cumplimiento a las medidas N°1 y 4 de la Política Nacional de Ciberseguridad

2do Seminario de Ciberseguridad para funcionarios públicos

LUNES 23/09 2021

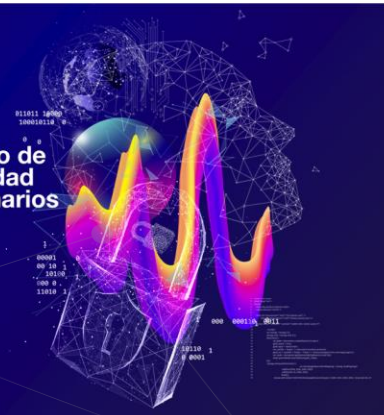


CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

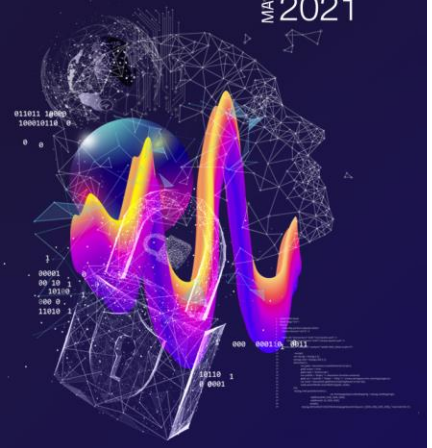
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática



2do Seminario de Ciberseguridad para funcionarios públicos

“Contenido central de la norma ”

2do Seminario de Ciberseguridad para funcionarios públicos
MARTES 28/09 2021

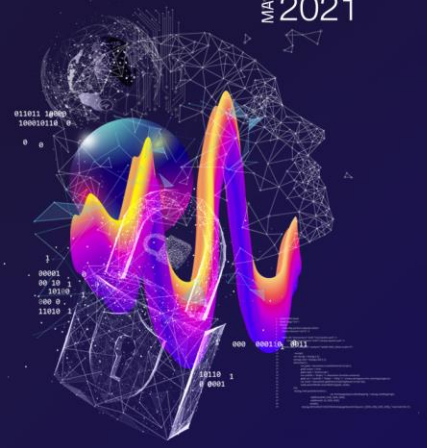


Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Contenido central de la norma

- Definiciones
- Principios
- Nuevas instituciones
- Deber de informar
- Infraestructura críticas
- Infracciones y sanciones

2do Seminario de Ciberseguridad para funcionarios públicos
MARTES 28/09 2021



Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Objeto y ámbito de aplicación

1. **Objeto**: Establecer la institucionalidad, principios y el marco general que estructure, regule y coordine la ciberseguridad a nivel nacional, así como regular la responsabilidad y deberes de los órganos de la Administración del Estado y de las instituciones privadas que se consideren como infraestructura crítica de la información. Junto a ello, tiene por objeto establecer los mecanismos de control y supervisión a los que se verán sometidos y los requisitos mínimos para prevención y resolución de incidentes de ciberseguridad.
2. **Ámbito de aplicación:** el proyecto se aplicará a los Órganos de la Administración del Estado que indica y a las instituciones privadas que sean consideradas Infraestructura Crítica de la Información, para lo cual, establece un mecanismo de clasificación y determinación de las mismas.

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

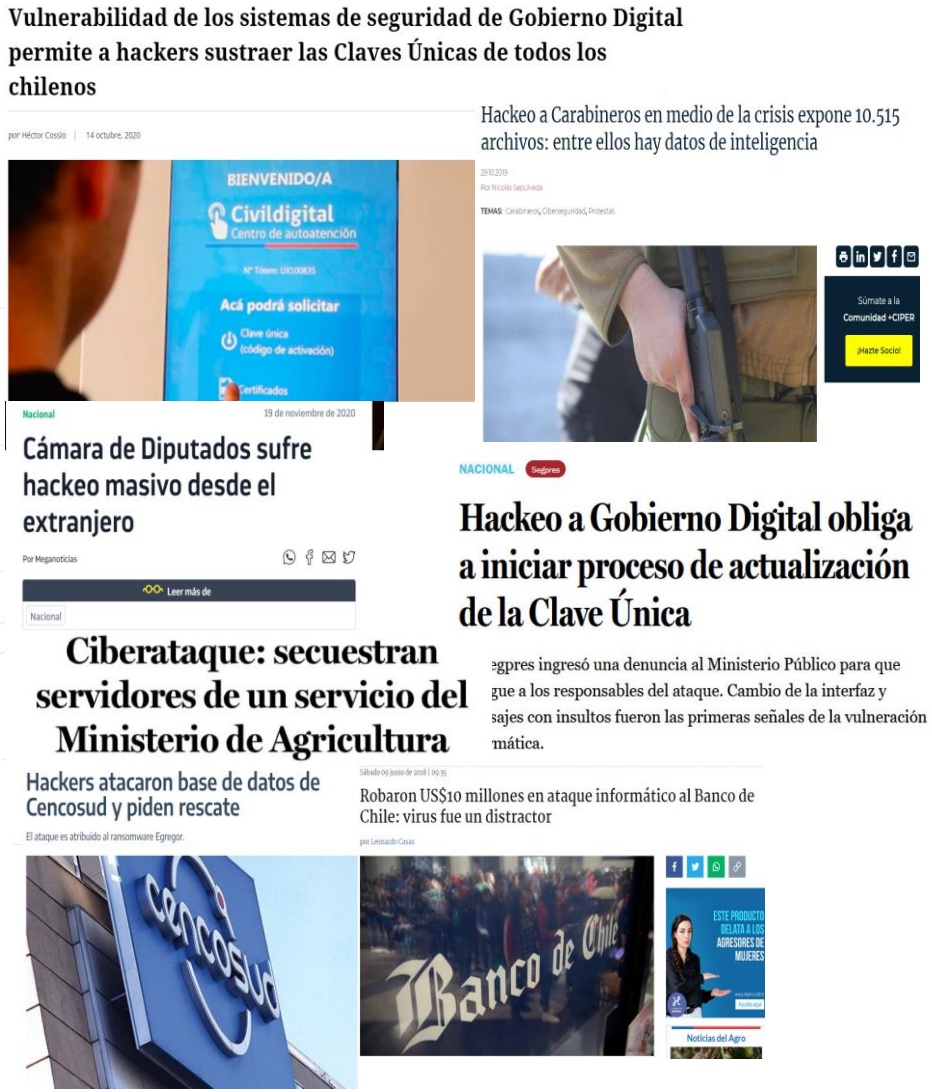
Bien jurídico protegido

"Seguridad Pública en el Ciberespacio"

- De ese modo la iniciativa buscaría Proteger los activos de la economía digital, que son datos y procesos ordinarios críticos para el país, tanto del sector público pero especialmente del sector privado considerado infraestructura crítica de la información.

- De ahí la importancia de contar con una institución centralizada que evite la duplicidad de obligaciones al sector privado y que alivie la carga regulatoria sin desproteger al país.

- Sin perjuicio de ello, dentro de bienes jurídicos tradicionales protegeríamos el **patrimonio**, **propiedad, la privacidad**, **la inviolabilidad, intimidad e incluso la vida.**



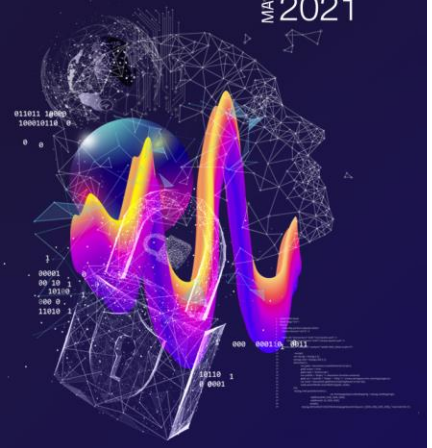
2do Seminario de Ciberseguridad para funcionarios públicos

LUNES 23/09 2021

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
MARTES 28/09 2021



Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Determinación de la ICI

a. <u>Mecanismo de clasificación de infraestructuras como críticas:</u>

Establece un mecanismo formal en virtud del cual se determinará que sectores rubros o instituciones, que, en virtud de sus instalaciones, redes, sistemas, servicios, equipos físicos y de tecnología de la información, que tendrán la calidad de infraestructura crítica de la información.

Dicho mecanismo consiste en un Decreto Supremo dictado por el Ministerio del Interior y Seguridad Pública, el que teniendo en consideración factores tales como la gravedad del impacto de una interrupción o mal funcionamiento del servicio, las pérdidas económicas asociadas, la afectación relevante al funcionamiento del Estado y sus órganos, entre otros, determinará los sectores, rubros o instituciones consideradas como críticas.

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Deberes de las infraestructuras críticas

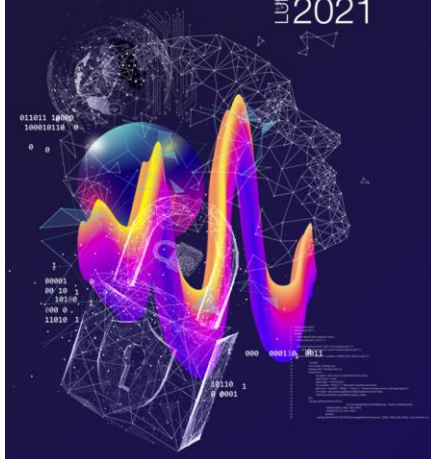
Se establecen deberes generales y especiales para las infraestructuras críticas de la información determinadas en virtud del mencionado decreto.

1) Entre los deberes generales se encuentran aplicar permanentemente las medidas de seguridad tecnológica, organizacionales, físicas e informativas necesarias para prevenir, reportar y resolver incidentes de ciberseguridad, así como las necesarias para mitigar el impacto sobre la continuidad operacional del servicio prestado.

2) Entre los deberes específicos se encuentran entre otros, el de implementar un sistema de evaluación de riesgos permanente, mantener actualizado un registro que comprenda la realización de las acciones que compongan el sistema de evaluación de riesgos, el elaborar e implementar planes de continuidad de funcionamiento y el realizar operaciones de revisión y análisis de redes, plataformas y sistemas.

2do Seminario de Ciberseguridad para funcionarios públicos

LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Institucionalidad

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

El proyecto de ley crea nueva institucionalidad y establece una nueva orgánica respecto de la gobernanza de ciberseguridad en el país. Dicha gobernanza es ejecutada por la Agencia Nacional de Ciberseguridad, el comité interministerial de ciberseguridad, el equipo nacional de respuesta a incidentes informáticos y los equipos de respuesta ante incidentes informáticos sectoriales.

a. Agencia nacional de Ciberseguridad: se crea como un servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propios, de carácter técnico y especializado, cuyo objeto será asesorar al Presidente de la República en materias propias de ciberseguridad, coordinar el actuar de las instituciones relevantes en la materia y fiscalizar las acciones de los organismos públicos y privados que sean considerados como infraestructura crítica de la información.

Ministerio del Interior y Seguridad Pública

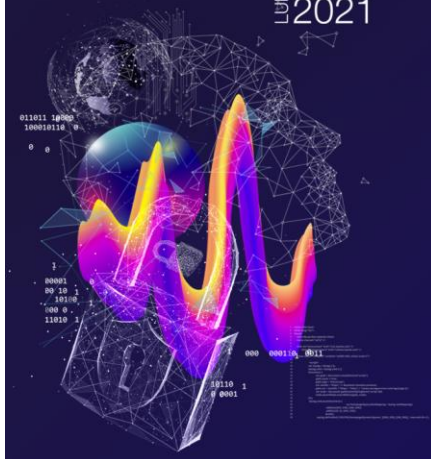
Gobierno de Chile

Institucionalidad

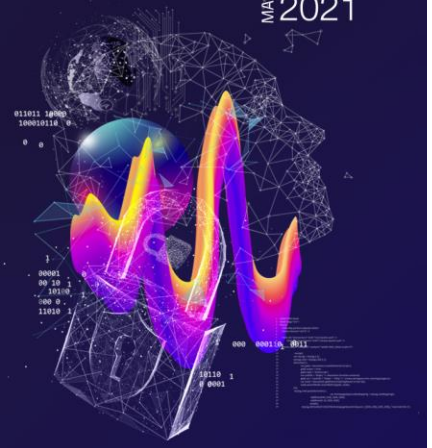
<u>b. Comité Interministerial de Ciberseguridad:</u>

Se crea el Comité Interministerial de Ciberseguridad, cuya función será asesorar y apoyar a la Agencia en la coordinación estratégica nacional en materias de ciberseguridad, relevantes para el funcionamiento de la Administración Pública y Servicios Esenciales, constituyendo una instancia de información, orientación, coordinación y acuerdo para los ministerios y servicios que lo integran.

Este estará integrado por el Director Nacional de la Agencia Nacional de Ciberseguridad, quien lo presidirá, y por los jefes de servicio por de las Subsecretarías del Interior, Defensa, Relaciones Exteriores, Justicia, Subsecretaría General de la Presidencia, Telecomunicaciones, Economía, Hacienda, Subsecretaría de Minería, Energía, Ciencia, Tecnología Conocimiento e Innovación y Dirección Nacional de la Agencia Nacional de Inteligencia.



2do Seminario de Ciberseguridad para funcionarios públicos
MARTES 28/09 2021



Institucionalidad

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

c. Equipo Nacional de Respuesta a Incidentes Informáticos:

Se establece que, para su funcionamiento, la Agencia contará con el Equipo Nacional de Respuesta ante Incidentes de Seguridad Informática o CSIRT Nacional. Institución que entre otras, tendrá las siguientes funciones:

i. Dar respuesta ante incidentes de ciberseguridad, relativos a organismos o empresas privadas no reguladas en esta materia y consideradas infraestructuras críticas de la información según esta ley.
ii. Coordinar a los CSIRT Sectoriales para intercambiar información técnica de ataques, vulnerabilidades, incidentes y brechas de ciberseguridad.
iii. Crear y administrar un sistema de entrenamiento nacional de ciberseguridad.
iv. Crear y administrar para el cumplimiento de sus funciones una red electrónica de comunicaciones segura destinada a comunicar y compartir información con los otros CSIRT Sectoriales.

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Institucionalidad

<u>d. Equipos de Respuesta a Incidentes Informáticos Sectoriales</u>:

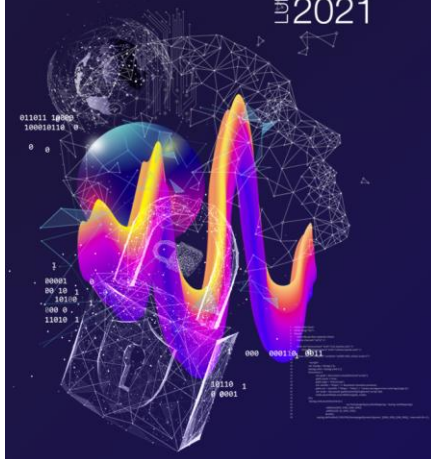
En el proyecto se faculta a los Ministerios, Subsecretarías, superintendencias y demás organismos públicos reguladores o fiscalizadores vinculados directamente con sectores regulados considerados como infraestructura crítica de la información, la creación de Equipos de Respuesta a Incidentes Informáticos. Los que tendrán por finalidad dar respuesta a vulnerabilidades e incidentes de ciberseguridad que vulneren o pongan en riesgo las redes, plataformas y sistemas informáticos de sus respectivos sectores regulados.

Entre sus principales funciones se encuentran las siguientes:

i. Dar respuesta frente a vulnerabilidades, incidentes de ciberseguridad y ciberataques que vulneren o pongan en riesgo la operación y resiliencia de los organismos considerados infraestructura crítica de la información de dicho sector regulado.
ii. Colaborar con el CSIRT Nacional, en el tratamiento de incidentes, ciberataques o vulnerabilidades de ciberseguridad de su sector.
iii. Coordinar a los equipos de respuesta que se implementen al interior del propio sector.
iv. Informar al CSIRT Nacional, a su propio sector y a alguna institución particularmente afectada del mismo, de vulnerabilidades, incidentes de ciberseguridad y ciberataques detectados o reportados en su sector, junto a sus respectivos cursos o planes de acción para subsanarlos.

2do Seminario de Ciberseguridad para funcionarios públicos

LUNES 23/09 2021

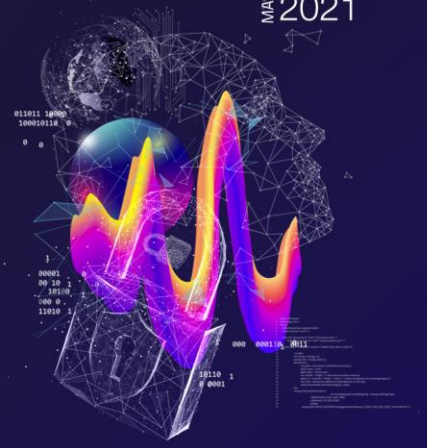


CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021



Ministerio del Interior y Seguridad Pública

Gobierno de Chile

	Funciones	Órganos del Estado	Privados regulados Considerados Críticos	Privados No regulados y Organismo autónomos Considerados Críticos	Privados No Considerados Críticos y Ciudadanía
Regulación	**Normar** los estándares técnicos mínimos de manera compartida con el ministerio sectorial.	Autoridad política (Ministerio delInterior y Seguridad Pública y Min. Segpres)	Ministerio del Interior y Seguridad Pública y regulador sectorial	Ministerio del Interior y Seguridad Pública y el organismo sectorial que tenga la facultad normativa	
	Fiscalizar y Auditar el cumplimiento de los estándares técnicos mínimos.	Consejo de Auditoría InternaGeneral de Gobierno (CAIGG)	Regulador sectorial	Organismo sectorial que tenga la facultad fiscalizadora	
	Sancionar la potestad sancionadora en caso de incumplimiento.	Por definir	Regulador sectorial	Organismo sectorial que tenga la facultad sancionatoría	
Protección	**Proteger** y gestionar incidentes de cibersguridad y fomentar el entrenamiento y creación de CSIRT sectoriales.	Agencia Nacional de Ciberseguridad	Regulador sectorial y Agencia Nacional de Ciberseguridad	Organismo sectorial y Agencia Nacional de Ciberseguridad	
Promoción de Cultura de Ciberseguridad	**Promover** la investigación y desarrollo en materia de ciberseguridad.	Agencia Nacional de Ciberseguridad	Regulador sectorial y Agencia Nacional de Ciberseguridad	Organismo sectorial y Agencia Nacional de Ciberseguridad	Agencia Nacional de Ciberseguridad
	Educar y concientizar a la ciudadanía para fomentar una cultura de ciberseguridad	Agencia Nacional de Ciberseguridad	Regulador sectorial y Agencia Nacional de Ciberseguridad	Organismo sectorial y Agencia Nacional de Ciberseguridad	Agencia Nacional de Ciberseguridad

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

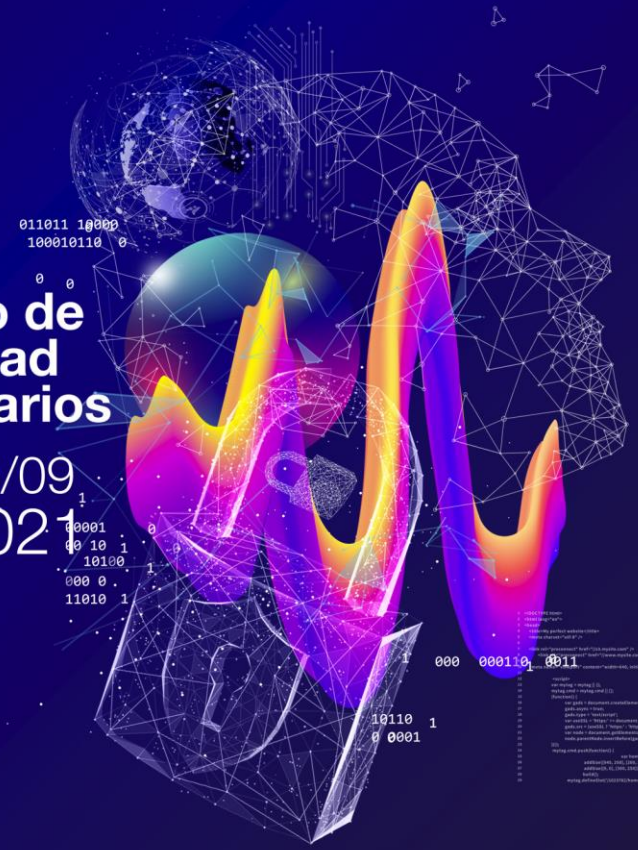
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT
https://www.csirt.gob.cl/

Teatinos 92 piso 6
Santiago, Chile

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021



Ministerio del Interior y Seguridad Pública

Gobierno de Chile

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT
https://www.csirt.gob.cl/

Teatinos 92 piso 6
Santiago, Chile