

2^{do} Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09
2021

011011 10000
100010110 0

0 0

1
00001 0
00 10 1
10100
000 0 1
11010 1

10110 1
0 0001

000 000110 0011

```
1 <script src=
2 <script src=
3 <script src=
4 <script src=
5 <script src=
6 <script src=
7 <script src=
8 <script src=
9 <script src=
10 <script src=
11 <script src=
12 <script src=
13 <script src=
14 <script src=
15 <script src=
16 <script src=
17 <script src=
18 <script src=
19 <script src=
20 <script src=
21 <script src=
22 <script src=
23 <script src=
24 <script src=
25 <script src=
26 <script src=
27 <script src=
28 <script src=
29 <script src=
30 <script src=
31 <script src=
32 <script src=
33 <script src=
34 <script src=
35 <script src=
36 <script src=
37 <script src=
38 <script src=
39 <script src=
40 <script src=
41 <script src=
42 <script src=
43 <script src=
44 <script src=
45 <script src=
46 <script src=
47 <script src=
48 <script src=
49 <script src=
50 <script src=
51 <script src=
52 <script src=
53 <script src=
54 <script src=
55 <script src=
56 <script src=
57 <script src=
58 <script src=
59 <script src=
60 <script src=
61 <script src=
62 <script src=
63 <script src=
64 <script src=
65 <script src=
66 <script src=
67 <script src=
68 <script src=
69 <script src=
70 <script src=
71 <script src=
72 <script src=
73 <script src=
74 <script src=
75 <script src=
76 <script src=
77 <script src=
78 <script src=
79 <script src=
80 <script src=
81 <script src=
82 <script src=
83 <script src=
84 <script src=
85 <script src=
86 <script src=
87 <script src=
88 <script src=
89 <script src=
90 <script src=
91 <script src=
92 <script src=
93 <script src=
94 <script src=
95 <script src=
96 <script src=
97 <script src=
98 <script src=
99 <script src=
100 <script src=
```



2do Seminario de
Ciberseguridad
para funcionarios
públicos



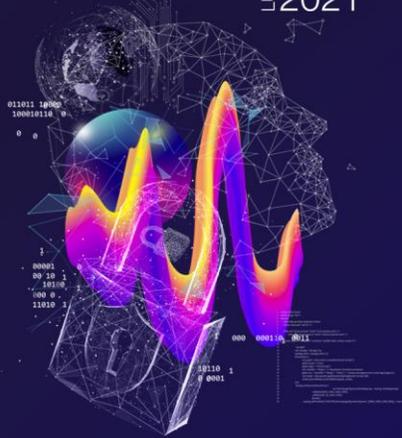
“Ciberseguridad en el Estado: análisis del nuevo marco normativo”

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

MARTES 28/09
2021

Ejemplos en el mundo de Ciberataques

NEWS

Ataques cibernéticos en la industria marítima habrían subido 900% en los últimos tres años

Los ataques cibernéticos a los sistemas de tecnología marítima (TTC) en la industria marítima han aumentado en un 900% en los últimos tres años, según un informe de Trend Micro, una empresa especializada en soluciones para la ciberseguridad a escala de sector.

De acuerdo a la compañía, en cada un de los últimos tres años se han reportado 50 ataques cibernéticos a un monto de \$120 en 2018 y más de \$150 en el año pasado.

Trend Micro

Ciberataque iraní dañó seis instalaciones del sistema hídrico de Israel

24 de mayo de 2021 - Seguridad

Lo más reciente

Fueron para nuevas elecciones: 10 de mayo de 2021 y los ataques de 2020

Un ciberataque en Libia parece ser un pretexto por parte de Irán de diciembre de 2020

Sector energético es el segundo mercado más atacado por el cibercrimen

Artículos Recientes

- Navegación a través del Caribe y como...
- En el 2020 ¿asímató o ¿reabundó?
- 2021, año de Planes de Contingencia...
- Importancia de Administrar para las Organizaciones
- 10 años con el primer ataque a los Clientes...

EE.UU. declara estado de emergencia tras un ciberataque a la mayor red de oleoductos del país

Desde el 20 de mayo de 2021

Supuestos 'hackers' norcoreanos atacan a AstraZeneca, uno de los fabricantes de la vacuna contra la covid

Los datos relacionados se hicieron públicos por intermediarios en Lactancia y WhatsApp para abordar el problema de la seguridad con datos de trabajo, según Francia.

Brasil investiga ciberataque en tribunal superior

November 5, 2020

SAO PAULO (AP) — La policía federal de Brasil abrió el jueves una investigación en torno al hackeo en las computadoras de uno de los tribunales superiores del país.

El presidente del Tribunal Superior de Brasil, Humberto Martins, dijo que se han suspendido todas las sesiones hasta que los expertos garanticen que están a salvo de los ciberataques. El tribunal ha realizado sus sesiones por internet desde el comienzo de la pandemia de COVID-19.

Click to copy

RELATED TOPICS

Noticias

Los ciberataques al sector energético de todo el mundo aumentan alrededor de un 41% en solo los primeros seis meses de 2019

Lo más reciente

Ciberataque a un hospital alemán en tiempos de pandemia

La muerte de una paciente en Alemania tras un ataque informático a un centro médico es el último episodio de una tendencia que corre el riesgo de agudizarse con la covid-19

EL PAIS INTERNACIONAL

Ejemplos en Chile de Ciberataques

Agrosuper y Ariztía sufrieron fraude informático

10/07/2020 por **Ulises Sepúlveda**
Hace pocos días se conoció la noticia de un nuevo ciberataque que vulneró la seguridad informática de empresas en Chile. Esta vez se afectó a **Ariztía** y **Agrosuper**, dos de las más grandes productoras y comercializadoras de alimentos. Ariztía y Agrosuper. Ambas enviaron un comunicado de sus respectivos sitios web, alertando de la situación e invitando a sus clientes a cancelar sus compras en línea.

De acuerdo a información recopilada en el **Sistema Financiero**, los atacantes hicieron llegar correo electrónico a los administradores de estas empresas, logrando así que información privilegiada, como por ejemplo el formato tipo de crédito y documentos que utilizan para comunicarse (trabaja con sus clientes, así como las credenciales para acceder a los sistemas de clientes, con sus datos e información de contacto.

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

Si bien hasta ahora no se ha reportado robo de dinero, las 430 sucursales de la estatal amanecieron cerradas, aunque en el día reabrieron 24. El banco presentó una querrela por sabotaje informático, y la CMF se instaló en las dependencias de la entidad. Esperan reabrir el resto de las sucursales durante la semana.

Martín Morales - 7 SEP 2020 12:21 AM

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 en Latin America de Fortinet, herramienta que detecta 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 cibernética durante la primera mitad del 2020.

Chile fue objetivo de **625 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.

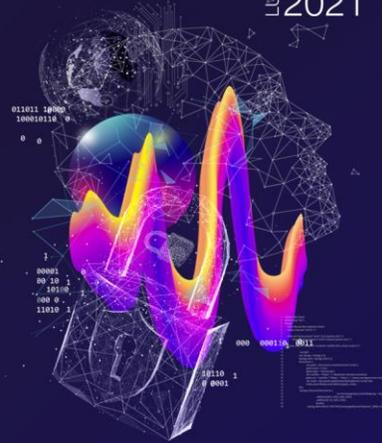
Hackers atacaron base de datos de Cencosud y piden rescate



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.

COMPARTIDOS: f t G+ P

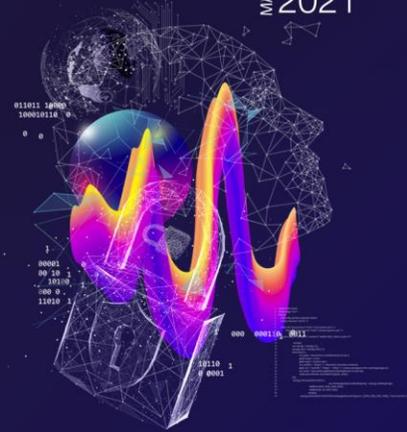
Un reciente estudio realizado por la empresa dedicada a la investigación de la seguridad en Internet Fortinet arrojó que, durante los últimos meses (post estallido social), han aumentando los ciberataques en Chile en torno al 35%.



¿Por qué se requiere una iniciativa legislativa?

2^{do} Seminario de
Ciberseguridad
para funcionarios
públicos

MARTES 28/09
2021



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.

¿Por qué se requiere una iniciativa legislativa?

5. Para gestionar los riesgos del ciberespacio

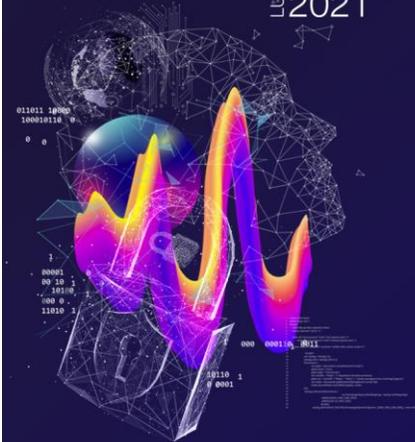
Es necesario considerar el desarrollo de procesos de análisis y gestión de riesgos que permitan identificar las vulnerabilidades, amenazas y riesgos implícitos en el uso, procesamiento, almacenamiento y transmisión de la información, junto a la generación de las capacidades para la prevención y la recuperación 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

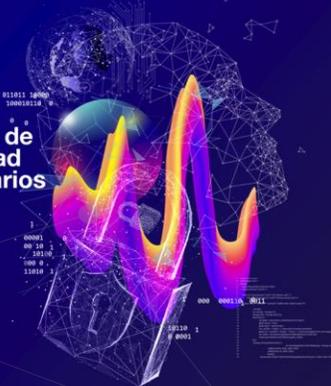
Con la presentación del Proyecto de Ley, se da cumplimiento a las medidas N°1 y 4 de la Política Nacional de Ciberseguridad



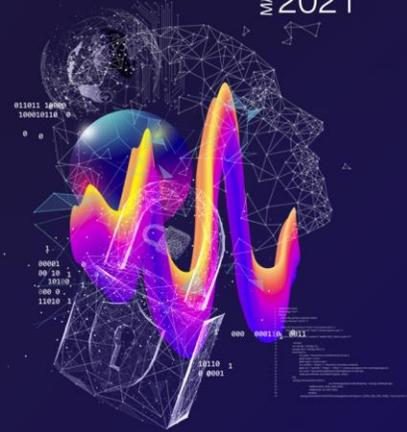


CSIRT
Equipo de Respuesta ante Incidentes
de Seguridad Informática

2^{do} Seminario de
Ciberseguridad
para funcionarios
públicos

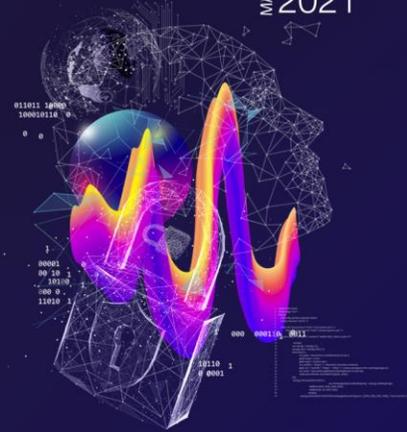


“Contenido central de
la norma”



Contenido central de la norma





Objeto y ámbito de aplicación

1. **Objeto:** Establecer la institucionalidad, principios y el marco general que structure, 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.

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.

Vulnerabilidad de los sistemas de seguridad de Gobierno Digital permite a hackers sustraer las Claves Únicas de todos los chilenos

por Héctor Cossío | 14 octubre, 2020



Hackeo a Carabineros en medio de la crisis expone 10.515 archivos: entre ellos hay datos de inteligencia

29/10/2019
Por Nicolás Sepúlveda
TEMAS: Ciberseguridad, Protección



Cámara de Diputados sufre hackeo masivo desde el extranjero

Por Meganoticias
Leer más de

Ciberataque: secuestran servidores de un servicio del Ministerio de Agricultura

Hackers atacaron base de datos de Cencosud y piden rescate

El ataque es atribuido al ransomware Egregor.

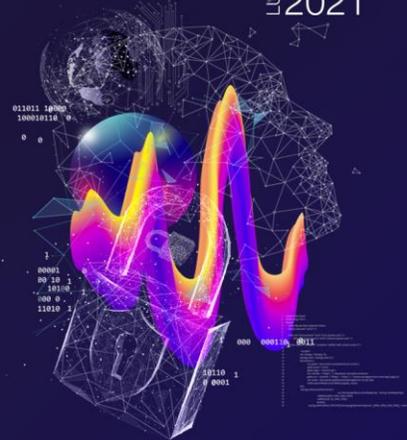


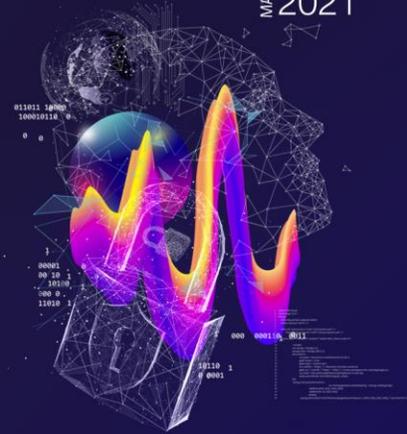
Hackeo a Gobierno Digital obliga a iniciar proceso de actualización de la Clave Única

agres ingresó una denuncia al Ministerio Público para que que a los responsables del ataque. Cambio de la interfaz y sajes con insultos fueron las primeras señales de la vulneración mática.

Sábado 09 junio de 2018 | 09:35
Robaron US\$10 millones en ataque informático al Banco de Chile: virus fue un distractor

por Leonardo Casas





Determinación de la ICI

a. Mecanismo de clasificación de infraestructuras como críticas:

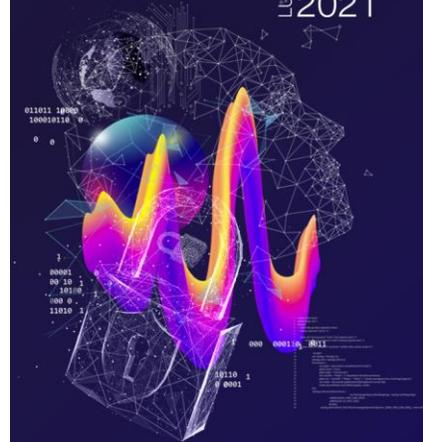
Establece un mecanismo formal en virtud del cual se determinará que sectores rubros o instituciones, que, en virtud de sus instalaciones, redes, sistemas, servicios, equipos físicos y de tecnología de la información, que tendrán la calidad de infraestructura crítica de la información.

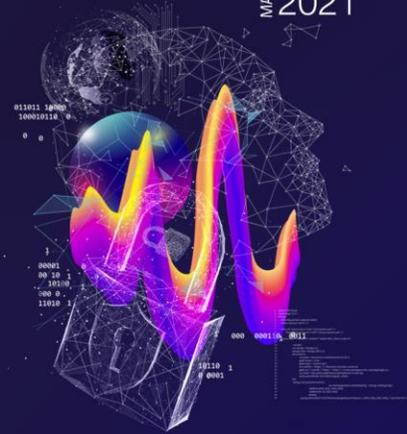
Dicho mecanismo consiste en un Decreto Supremo dictado por el Ministerio del Interior y Seguridad Pública, el que teniendo en consideración factores tales como la gravedad del impacto de una interrupción o mal funcionamiento del servicio, las pérdidas económicas asociadas, la afectación relevante al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

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.





Institucionalidad

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.

Institucionalidad

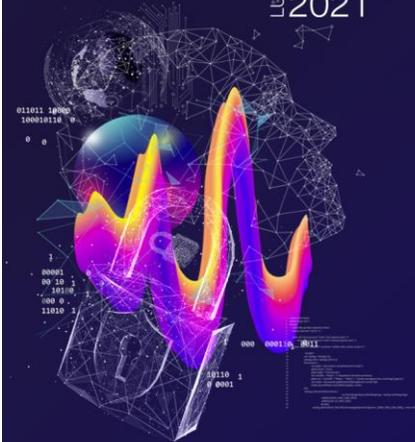
b. Comité Interministerial de Ciberseguridad:

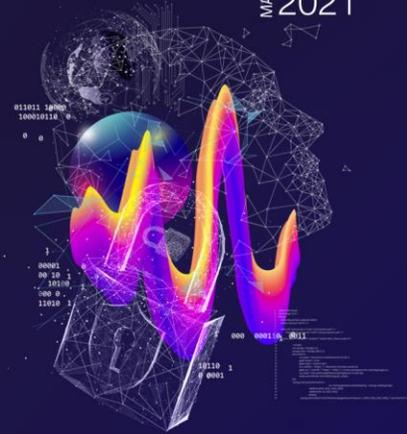
Se crea el Comité Interministerial de Ciberseguridad, cuya función será asesorar y apoyar a la Agencia en la coordinación estratégica nacional en materias de ciberseguridad, relevantes para el funcionamiento de la Administración Pública y Servicios Esenciales, constituyendo una instancia de información,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

2^{do} Seminario de
Ciberseguridad
para funcionarios
públicos

LUNES 23/09
2021





Institucionalidad

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.

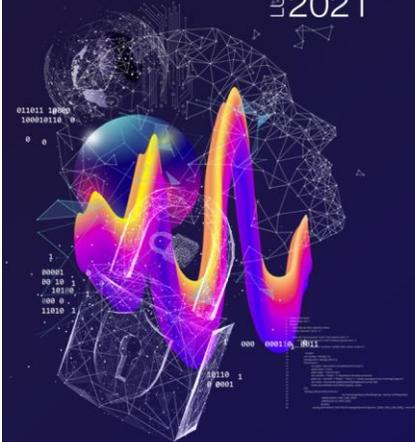
Institucionalidad

d. Equipos de Respuesta a Incidentes Informáticos Sectoriales:

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.

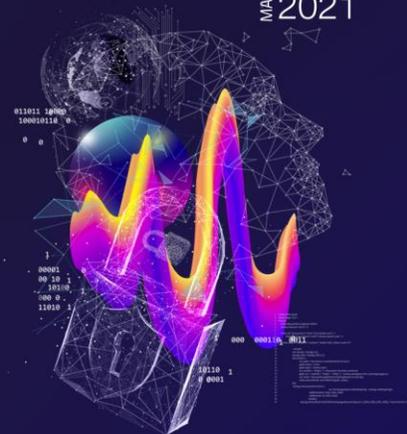
Entre sus principales funciones se encuentran las siguientes:

- 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.



2^{do} Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09
2021



Funciones

Órganos del Estado

Privados regulados Considerados Críticos

Privados No regulados y Organismo autónomos Considerados Críticos

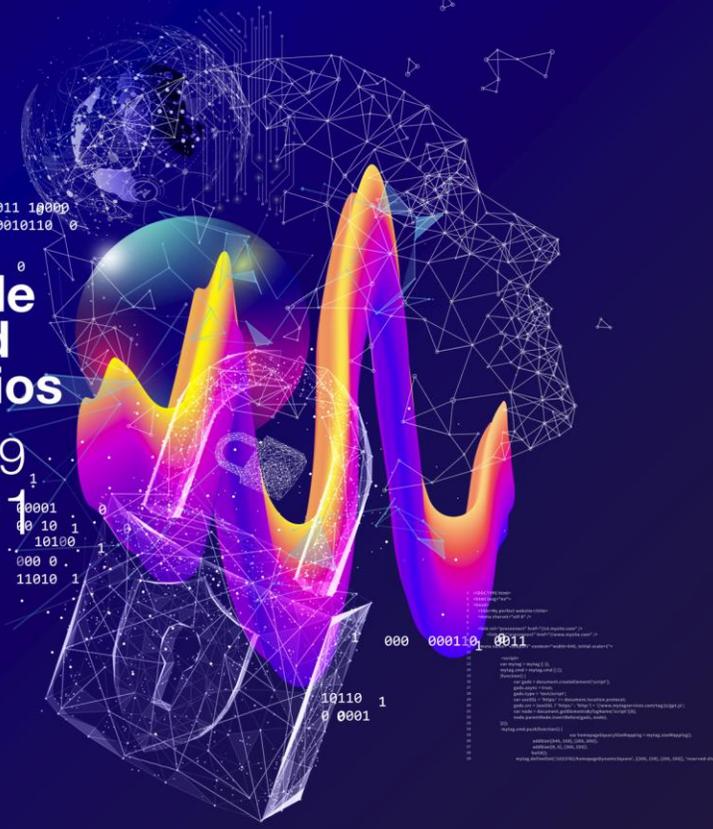
Privados No Considerados Críticos y Ciudadanía

	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 del Interior 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 Interna General 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 sancionatoria	
Protección	Proteger y gestionar incidentes de ciberseguridad 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



2^{do} Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09
2021

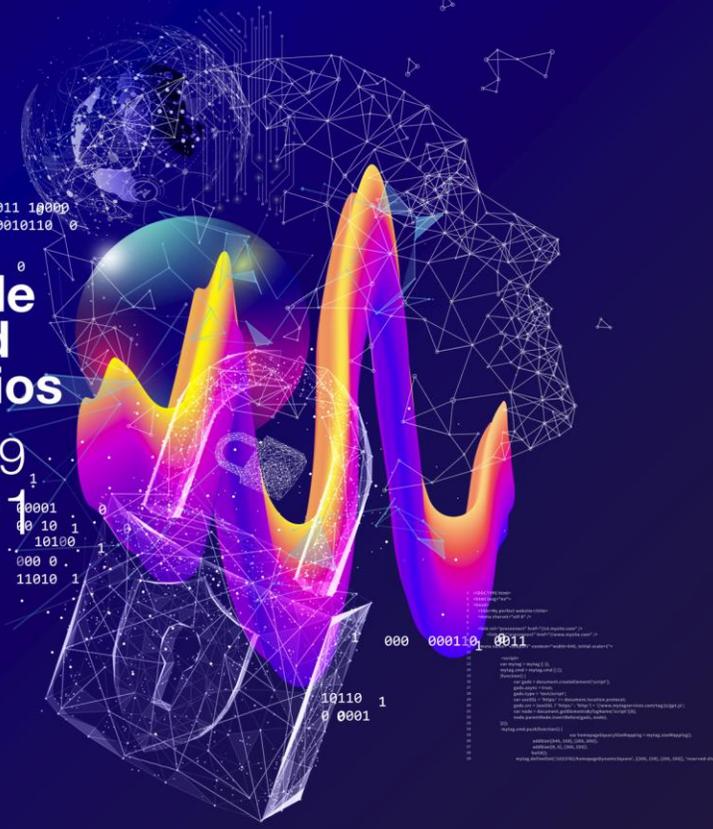


CSIRT
<https://www.csirt.gob.cl/>

Teatinos 92 piso 6
Santiago, Chile

2^{do} Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09
2021



CSIRT
<https://www.csirt.gov.cl/>

Teatinos 92 piso 6
Santiago, Chile