Evolución del ecosistema de ciberseguridad en Chile

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Ciberseguridad al alero de una agencia: “análisis del nuevo marco normativo”

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

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, 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 y digitalización 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.


Ministerio del Interior y Seguridad Pública
Gobierno de Chile

CSIRT

Evolución del ecosistema de **ciberseguridad en Chile**

Ejemplos en el mundo de Ciberataques

MUNDO La Tercera AM Mundo

Pegasus: el software espía de firma israelí usado contra periodistas, políticos y activistas

Varios medios de comunicación recibieron una lista de hasta 50.000 números de teléfono que se cree que fueron identificados como pertenecientes a personas de interés por los

GIZMODO

Oil Giant Shell Hacked Thanks to Accellion System

By Lucas Ropek | 3/23/21 3:45PM | Comments (4) | Alerts

Hackers Say They Stole 250GB of Documents From DC Police

By Lucas Ropek | 4/27/21 9:20AM | Comments (23) | Alerts

MUNDO EE.UU. Biden

Biden acusa a Rusia de querer interferir en elecciones de 2022 y advierte que ciberataques podrían provocar guerra verdadera

"Miren lo que está haciendo ya Rusia con las elecciones de 2022 y la desinformación. Es una violación pura y simple de nuestra soberanía", dijo el mandatario estadounidense durante una visita a

Presidente Joe Biden durante su visita a la Oficina de la Dirección de cerca de Washington. Foto: Reuters

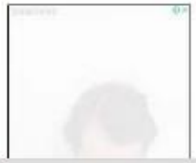
Los ciberataques al sector energético de todo el mundo aumentan alrededor de un 41% en solo los primeros seis meses de 2019

Sector energético es el segundo mercado más atacado por el cibercrimen

EL PAÍS INTERNACIONAL

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



BBC NEWS | México

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

EL PAÍS TECNOLOGÍA

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

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

CSIRT

Evolución del ecosistema de **ciberseguridad en Chile**

Ejemplos en Chile de Ciberataques

Agrosuper y Ariztía sufrieron fraude informático

11/01/2018 por Willian 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 sintieron 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 hicieron llegar 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 siderúrgica CAP: dejan mensaje extorsivo para cobrar por "rescate" del sistema

Por Jorge Molina Sandoval

Gobierno alerta sobre ciberataque a empresa proveedora de grandes hospitales

NACIONAL Alerta Datos

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.

Hackers atacaron base de datos de Cencosud y piden rescate

El ataque es atribuido al ransomware Egregor.

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

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, ...ido social), han ...e en torno al 35%.

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.

SECCIONES CNN CHILE

Detienen a presunto autor de hackeo a página de Gobierno Digital

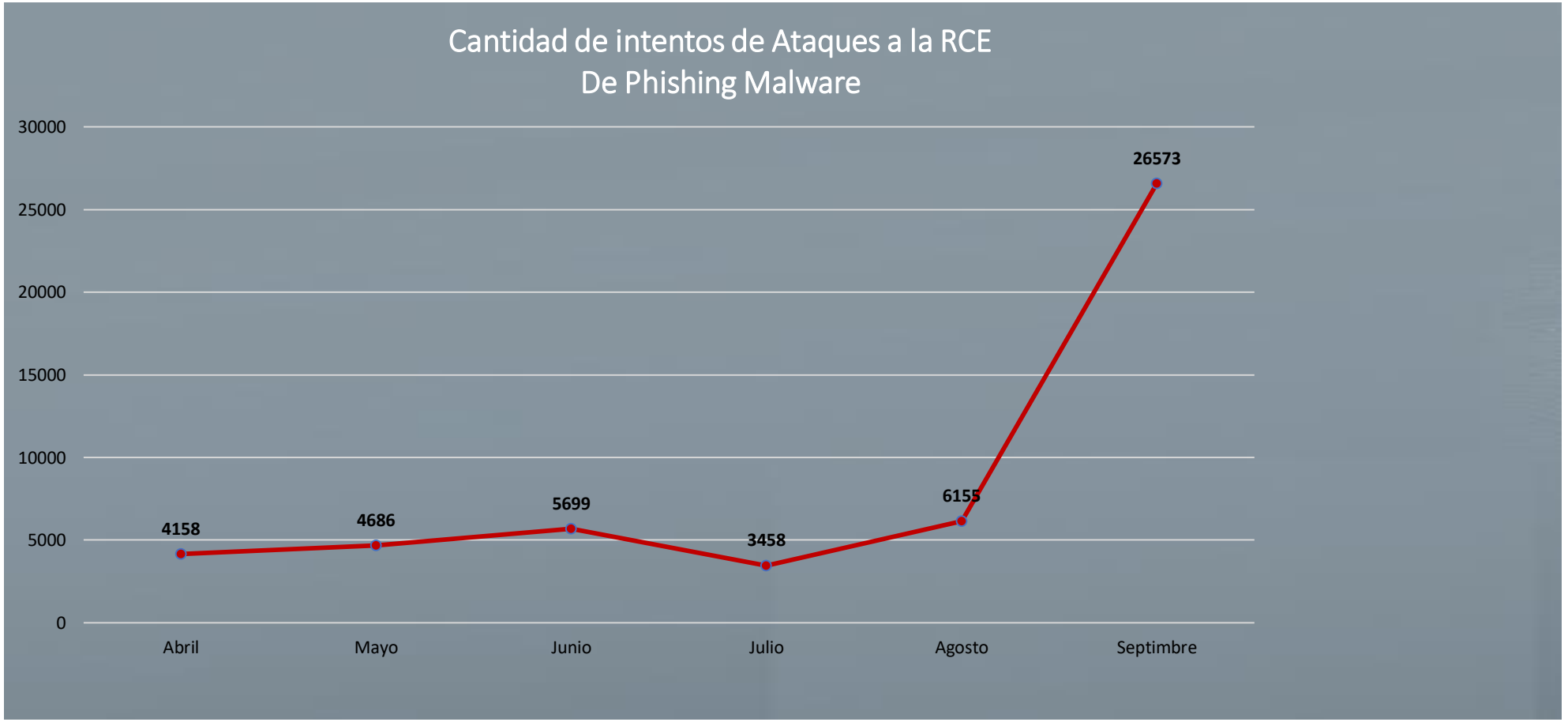
21-10-2020 19:13 / El hombre será puesto a disposición de la justicia el jueves por el delito sabotaje informático. Al respecto, el ministro Cristián Monckeberg sostuvo que "valoramos la rápida acción de la Fiscalía y la PDI que ha permitido la detención".

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Evolución del ecosistema de **ciberseguridad en Chile**

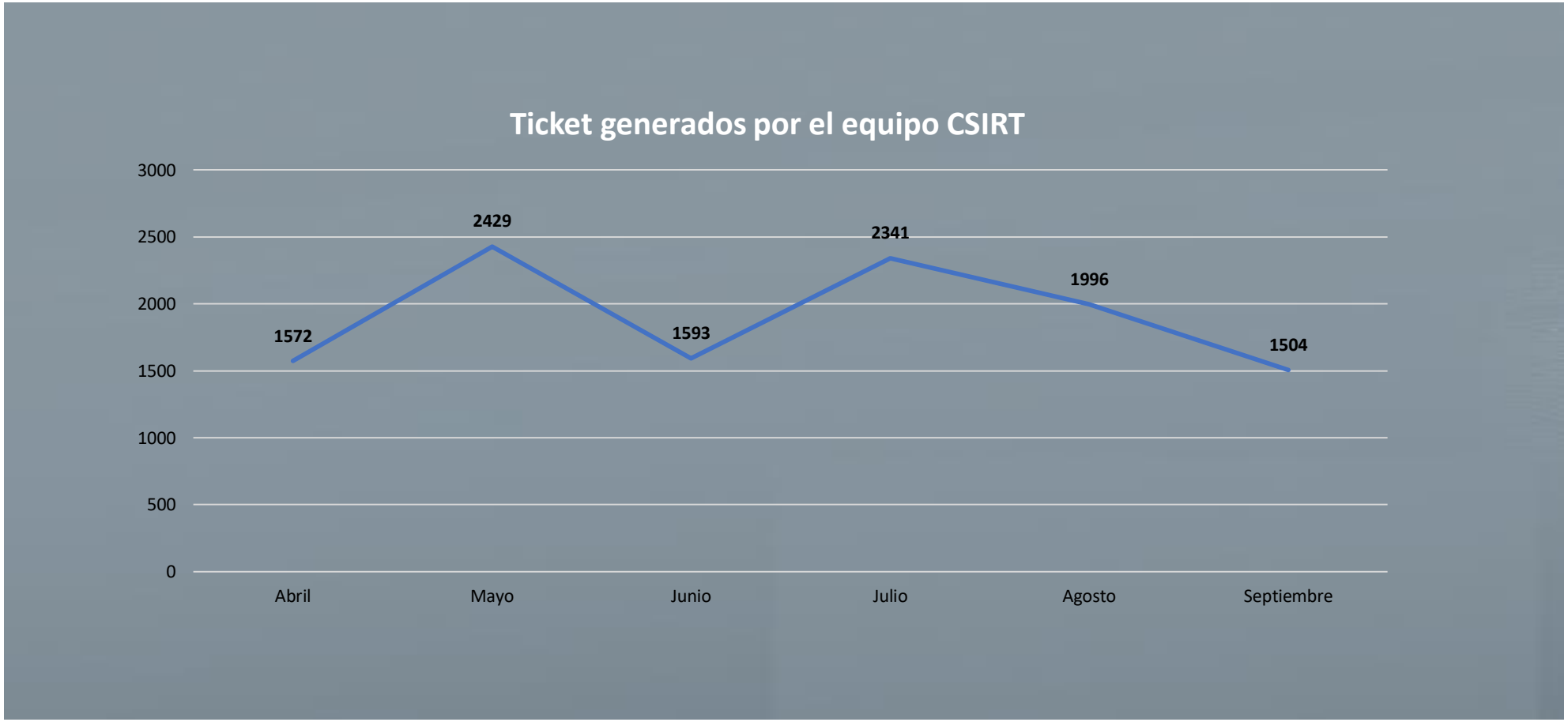
Crecimiento exponencial de los ataques



Este tráfico es ocasionado por conexiones procedentes de direcciones IPs comprometidas con algún tipo de malware que implementa capacidad de instalar motor SMTP propio lo cual se emplea para difundir spam, virus, ataques de diccionario, denegación de servicio (DoS), mensajes a destinatarios no existentes. La mayor parte de las soluciones de seguridad en el correo electrónico no tienen en cuenta este tráfico indeseado a través del puerto 25 que es aceptado, analizado y rechazado

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Crecimiento exponencial de los ataques



Los ticket generados por el equipo CSIRT, se agrupan según la matriz de clasificación de incidentes de ENISA, (Agencia de la Unión Europea para la Ciberseguridad) en 10 categorías relacionadas a incidentes de seguridad informática y acciones preventivas y operacionales, programadas de las instituciones que resultan en la interrupción parcial de un servicio.

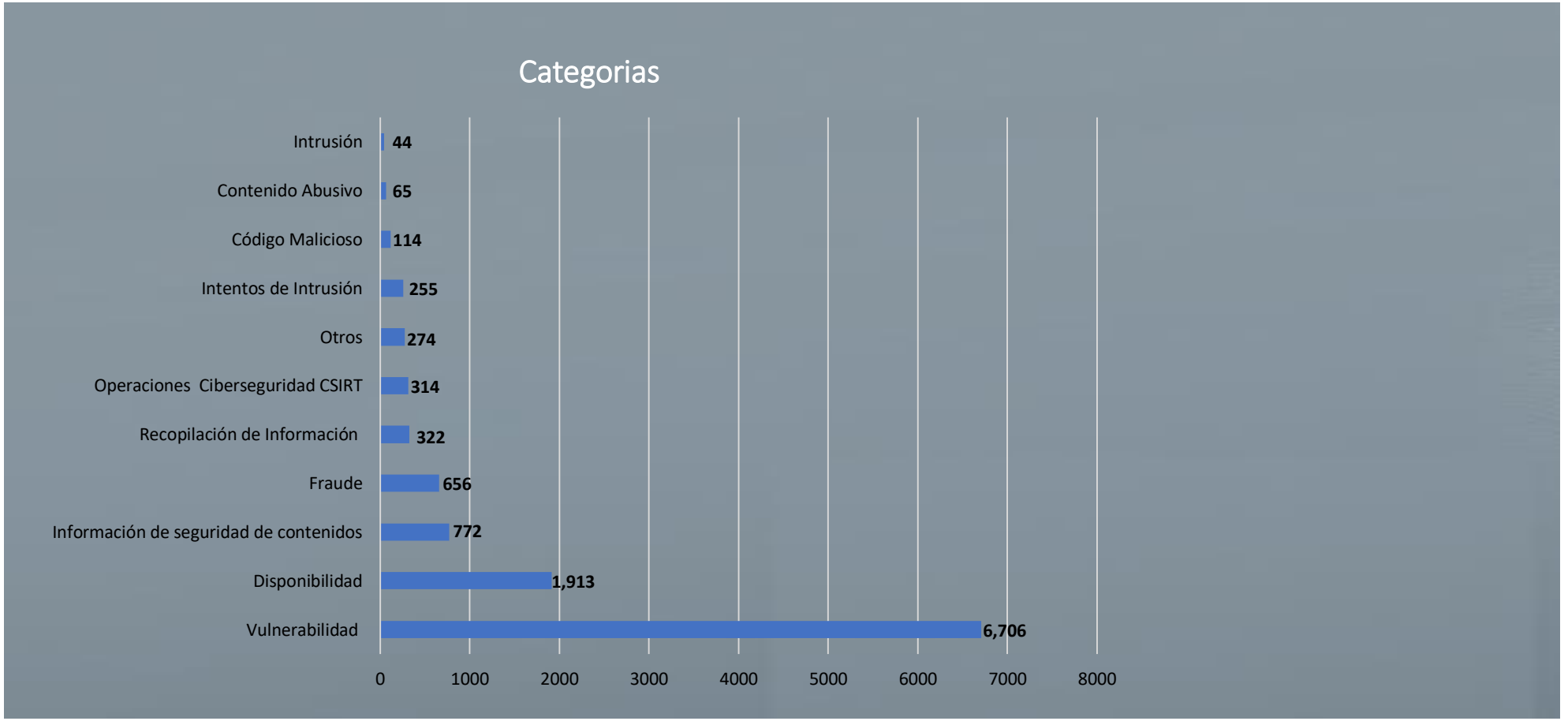
CSIRT

Evolución del ecosistema de **ciberseguridad en Chile**

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Evolución del ecosistema de **ciberseguridad en Chile**

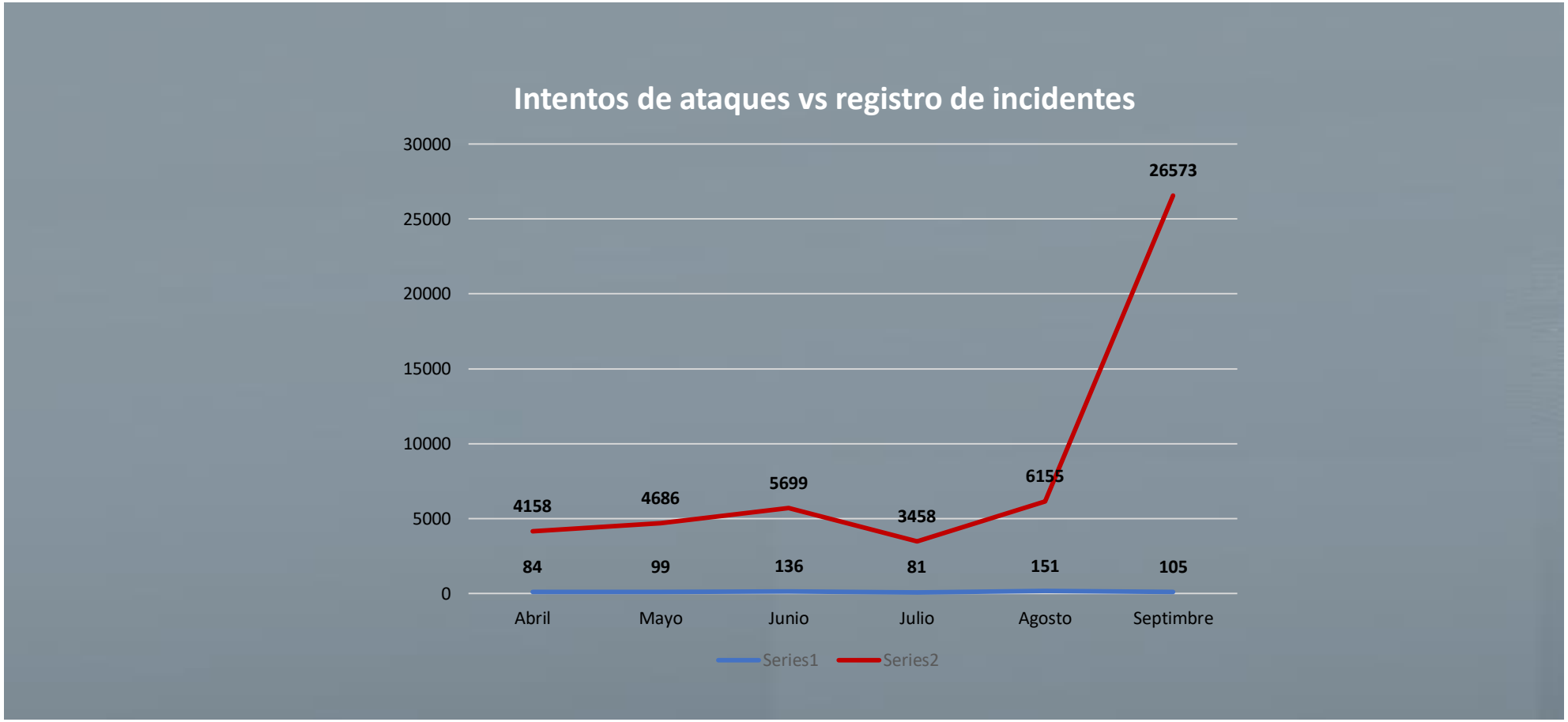
Crecimiento exponencial de los ataques



Entre abril y septiembre de 2021, CSIRT proceso 11.435 ticket agrupados correspondientemente en las 10 categorías que recomienda ENISA para incidentes de seguridad.

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Crecimiento exponencial de los ataques



El siguiente gráfico representa el comparativo entre los intentos de ataque mediante envió de Phishing con adjuntos maliciosos catalogados como malware y los incidentes reportados por CSIRT bajo la categoría de fraude.

CSIRT

Evolución del ecosistema de **ciberseguridad en Chile**

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

CSIRT

Evolución del ecosistema de **ciberseguridad en Chile**

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

¿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

2.-Para proteger el Estado

Es necesario promover el resguardo de las redes y sistemas informáticos del sector público y privado, 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

Contenido Central de la Norma

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Contenido central de la norma

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

Basados en Experiencia Internacional

- Considerando que tenemos desde el 2018 en adelante MoU de Cooperación en Ciberseguridad con potenciales mundiales en este ámbito(Estonia, UK, Israel, España, Colombia, OEA); nos hemos basado en los modelos más exitosos de implementación para crear una Institución a cargo de la Ciberseguridad, como a su vez la regulación y operación de la Infraestructura Crítica de la Información; considerando la realidad país, las ventajas y desventajas prácticas de cada referencia.

- Israel: modelo de coordinación concentrado en una Institución. Directorio/Consejo de apoyo técnico como político, red de interconexión y cooperación entre CSIRT al interior del país.
- España: no directa coordinación/muchos actores distintos. Buen modelo de funciones, (CCN-Cert, CNPIC, OCC, INCIBE).
- EEUU: Modelo de clasificación de Infraestructura Crítica de la Información y protección de esta.
- Colombia: Coordinación rápida y eficaz a través de C4.
- Entre otros.

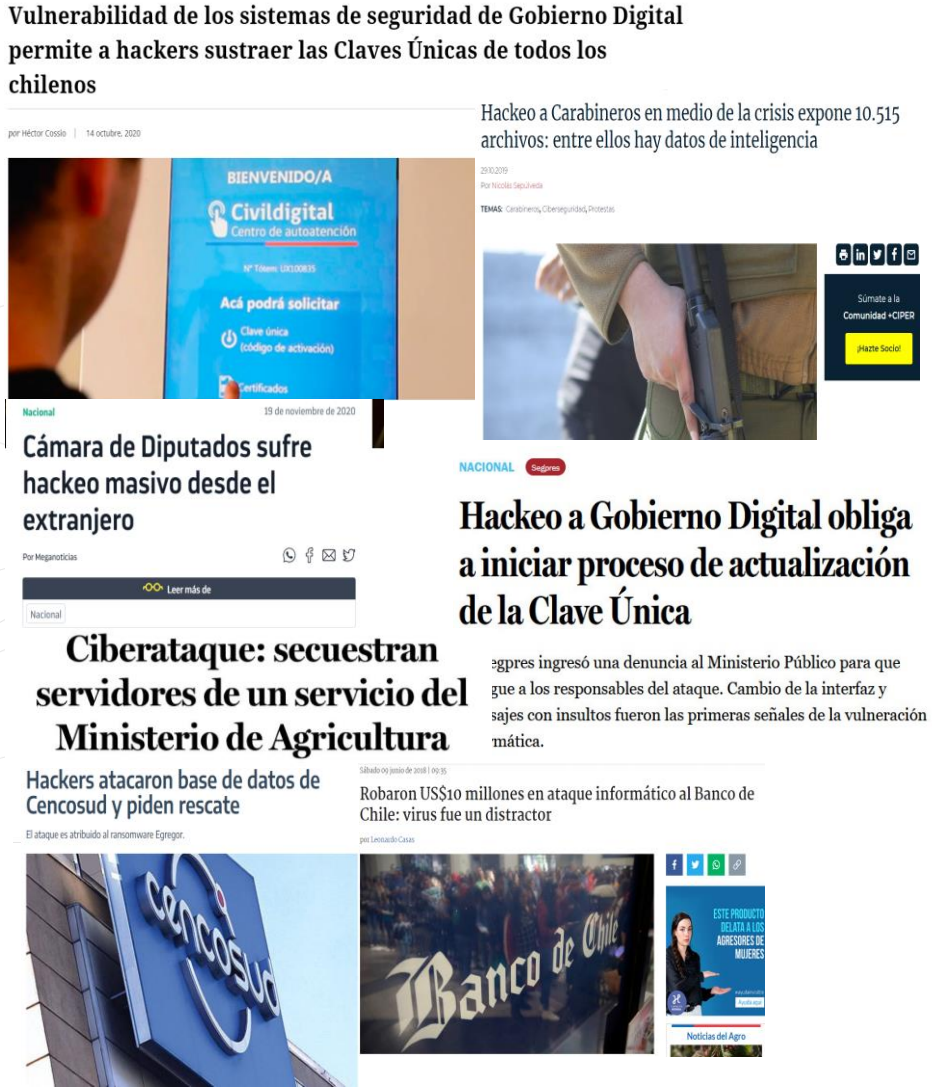
Objeto y ámbito de aplicación

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.

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.**



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.

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.

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

<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.

Institucionalidad

c.- Consejo Técnico de la Agencia Nacional de Ciberseguridad: se crea un consejo de expertos que tendrá como objeto asesorar y apoyar técnicamente a la Agencia en el análisis y revisión periódica de las políticas públicas propias de su ámbito de competencia, como la proposición al Director Nacional de la Agencia de los sectores, rubros, instituciones, instalaciones, redes, sistemas , plataformas, servicios entre otros para ser considerados como Infraestructura Crítica de la Información.

Estará formado por un funcionario de la Agencia y y cuatro consejeros designados por el Presidente de la República, entre personas de destacada labor en el ámbito de la ciberseguridad.

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Institucionalidad

<u>d. Equipo Nacional de Respuesta a Incidentes de Seguridad Informáticos:</u>

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.

CSIRT

Evolución del ecosistema de **ciberseguridad en Chile**

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Institucionalidad

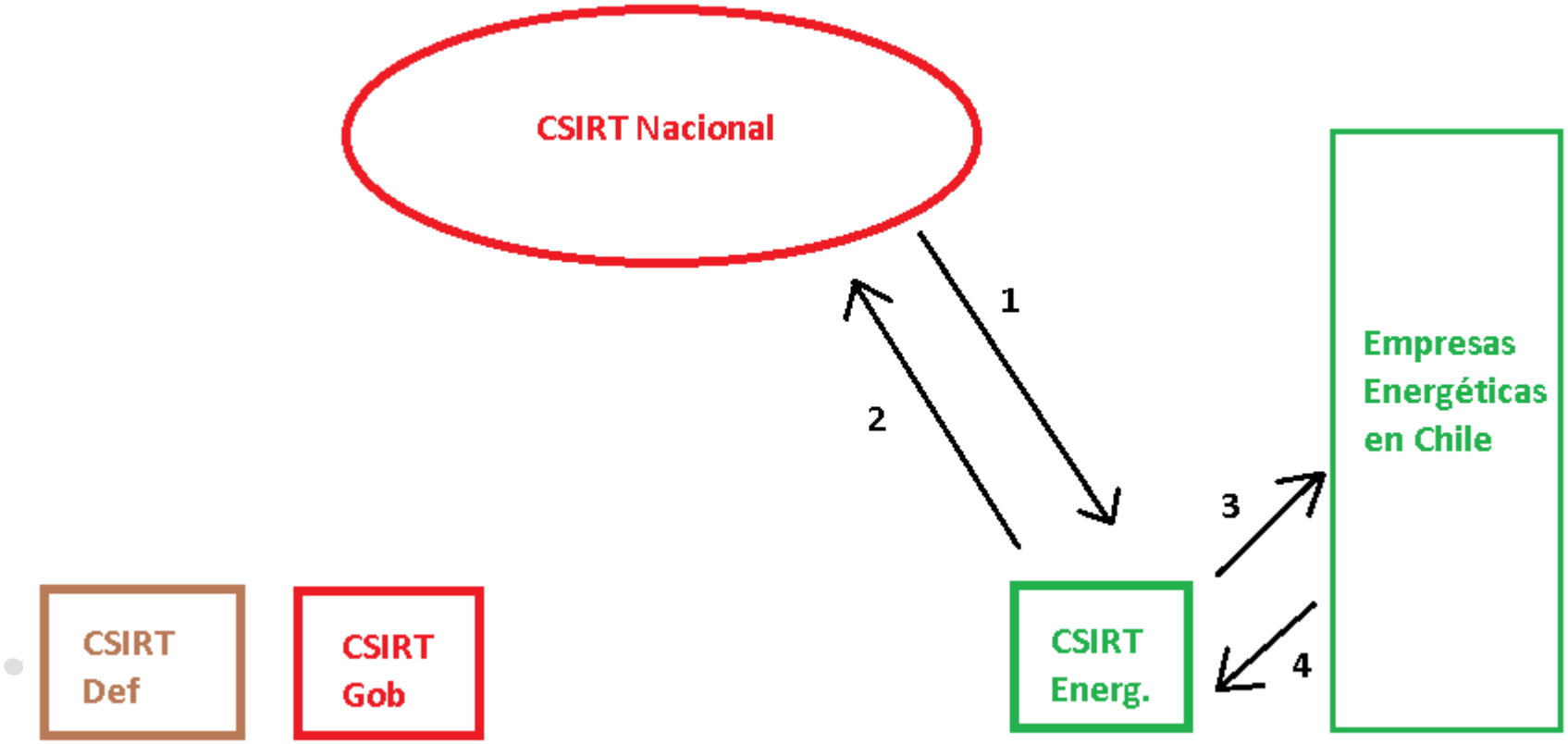
e. Equipos de Respuesta a Incidentes de Seguridad Informáticos Sectoriales:

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.

Modelo de Interconexión y Cooperación



1: Comunicación de avisos, alarmas y amenazas propias, del sector en sí, de otros sectores nacionales o bien internacionales a un CSIRT Sectorial (Anonimizado)
2: Comunicación de reportes, tickets y casos para ser informados al CSIRT Nacional (Anonimizado)
3.- Comunicación propia que genera un CSIRT Sectorial o bien recibida del CSIRT Nacional o bien recibida de una empresa del sector para ser difundida en todo el sector energético de Chile.(Anonimizado)
4.-Comunicación que reporta una empresa energética en Chile a su CSIRT Sectorial.

CSIRT

Evolución del ecosistema de **ciberseguridad en Chile**

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

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.10.28 15:44:36 -03'00'

Evolución del ecosistema de ciberseguridad en Chile

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática