Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Informe de gestión de Seguridad Cibernética

01 de octubre 2021

Índice

Índice de Ilustraciones

Índice de Tablas

1. Resumen Ejecutivo

El presente informe contiene un resumen de la totalidad de los tickets procesados en el mes de septiembre de 2021. El documento muestra la composición de los tickets desagregados por categorías que corresponden al tipo de vulnerabilidad de las incidencias que originaron los tickets.

El informe también da cuenta del porcentaje de tickets que fueron cerrados con éxito en el curso del mes de septiembre y también muestra la proporción de aquellos que quedan por terminar.

Asimismo, en este documento se muestra por categorías los tipos de tickets que se reportan para notificar a las instituciones públicas o privadas.

Este reporte mensual muestra, además, el origen o procedencia de la información que procesa CSIRT –si es interna o externa- y presenta en términos porcentuales el peso relativo que cada una de estas fuentes tiene dentro de la demanda de trabajo que se recibió durante el mes.

Adicionalmente, también se entrega un desagregado con el detalle que permite conocer la participación –en cantidades y en términos porcentuales- de las diversas fuentes externas que componen la actual generación de tickets desde ese origen de procedencia.

Finalmente, se presenta información proveniente de la plataforma MISP[1] que contiene la cantidad de posibles IoCs[2] o –Índices de Compromiso- que se hayan detectado. Esta información es relevante para CSIRT dado que se utiliza como punto de partida para validar correlaciones con todas nuestras plataformas de análisis. En el informe se expone una tabla donde se puede enumerar la cantidad de IoCs detectados en el presente mes, los cuales se presentan diferenciados en base a direcciones IP[3] o a URL[4].

[1] MISP es una sigla en idioma inglés que significa Malware Information Sharing Platform o "Plataforma para compartir información de Malware y amenazas".
[2] IOC es una sigla en idioma inglés que significa "Índice de compromiso", y se refiere a la descripción de un incidente de ciberseguridad, actividad y/o artefacto malicioso mediante patrones.
[3] IP es una sigla en idioma inglés que significa "Internet Protocol" y corresponde a un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, smartphone).
[4] Es una sigla en idioma inglés que significa Uniform Resource Locator o "Localizador Uniforme de Recursos". Se trata de la secuencia de caracteres que sigue un estándar y que permite denominar recursos dentro del entorno de Internet para que puedan ser localizados. Los documentos de texto, las fotografías y los audios, entre otros tipos de contenidos digitales, tienen un URL cuando se publican en Internet. Estos localizadores permiten crear hipervínculos. De esta forma, el URL, por lo tanto, es el conjunto de caracteres que posibilita la asignación de una dirección exclusiva a un recurso que se encuentra disponible en el espacio virtual. En otras palabras, el URL es una dirección de Internet que, al ser encontrada y visualizada por un navegador, muestra un recurso de información al usuario.

2. Alcances del Informe

La información que se muestra en el presente informe proviene de la gestión de CSIRT en el marco del proceso de notificación a entidades, instituciones y/u organismos afectados. Esa información se produce como consecuencia de las actividades desarrolladas por el equipo 24/7 en un período de tiempo mensual. A continuación, se enumera resumidamente esas actividades:

- Gestión de tickets generados, efectuando seguimiento y validando las acciones que se tomaron con el ticket enviado al organismo gubernamental afectado.

- Reporte de vulnerabilidades de aquellos tickets precedentes una vez validado que la falla de seguridad se encuentre aún presente.

- Generación de análisis y reporte de vulnerabilidades detectadas dentro de la RCE[5] (falta cifrado, CMS obsoletos, credenciales recuperadas, servidores desactualizados, puertos expuestos, Phishing, deface, etc…).

- Seguimiento a los tickets reportados (contacto mediante llamada telefónica y/o correo electrónico) para validar qué acciones ha tomado la entidad reportada con la información de la vulnerabilidad detectada.

- Análisis y monitoreo de un listado de 4.200 sitios aproximadamente- los cuales corresponden a portales gubernamentales, a los que se ha validado su estatus utilizando las plataformas Splunk, Pingdom y PRTG.

- Monitoreo de los dispositivos de las instituciones que se encuentran conectadas dentro de la RCE.

- Generación de ticket para notificar a la entidad y/u organismo afectado, ante la identificación de cualquier eventualidad sucedida con los dispositivos y sitios que se encuentran dentro del alcance de monitoreo de CSIRT.

[5] RCE significa Red de Conectividad del Estado

3. Tipos de Tickets

En la siguiente tabla se expone las categorías, o tipos de tickets, que son generados por el equipo CSIRT. La información se presenta ordenada, de mayor a menor, respecto a la cantidad de tickets que se generó por cada tipología. Los cuales 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. Más abajo se muestra un gráfico que refleja esta misma información, pero como una distribución en términos porcentuales de lo que representa la participación de cada tipo de ticket dentro del total de la demanda de trabajo que recibe y procesa CSIRT.

N°	Tipos de ticket	Código	Total
1	Vulnerabilidad	9V00	753
2	Disponibilidad	6D00	391
3	Información de seguridad de contenidos	7S00	149
4	Fraude	8F00	105
5	Otros	11O00	86
6	Código Malicioso	2C00	15
7	Contenido Abusivo	1A00	2
8	Intrusión	5I00	1
9	Recopilación de Información	3R00	1
10	Intentos de Intrusión	4I00	1
Total			**1504**

Tabla 1 - Total Tipos de Tickets

Ilustración 1 - Tipos de tickets

En la siguiente tabla se muestran la tendencia y los cambios en el ranking que experimentan los tipos de tickets generados por CSIRT en el mes de septiembre, respecto a agosto de 2021.

Como se aprecia en la tabla, los tickets de las categorías de vulnerabilidades, disponibilidad, contenido abusivo, intrusión, recopilación de información e intentos de intrusión presentan una tendencia a la baja (hay menos números de tickets), mientras que tres categorías experimentan una tendencia creciente al comparar el mes de septiembre con el pasado mes de agosto.

N°	Agosto	Septiembre	Tendencia	Variante
1	Vulnerabilidad	Vulnerabilidad	▼	➡
2	Disponibilidad	Disponibilidad	▼	➡
3	Fraude	Información de seguridad de contenidos	▲	⬆
4	Información de seguridad de contenidos	Fraude	▼	⬇
5	Otros	Otros	▲	➡
6	Contenido Abusivo	Código Malicioso	▲	⬆
7	Código Malicioso	Contenido Abusivo	▼	⬇
8	Intrusión	Intrusión	▼	➡
9	Recopilación de Información	Recopilación de Información	▼	➡
10	Intentos de Intrusión	Intentos de Intrusión	▼	➡

Tabla 2 - Ranking de Alertas Recibidas

4. Tipos de Ticket Públicos y Privados

En la siguiente tabla se presenta el desagregado de los tickets que fueron reportados a instituciones públicas o privadas, por las distintas categorías presentadas.

Tickets	Privado	Público	Total
Vulnerabilidad	32	721	753
Disponibilidad	30	361	391
Información de seguridad de contenidos	125	24	149
Fraude	91	14	105
Otros	42	44	86
Código Malicioso	10	5	15
Contenido Abusivo	1	1	2
Intrusión	0	1	1
Recopilación de Información	0	1	1
Intentos de Intrusión	1	0	1
Total	**332**	**1172**	**1504**

Tabla 3 - Tickets a Instituciones Públicas y Privadas

En el siguiente gráfico expone el porcentaje de participación que tiene cada destino de los tickets que son enviados a instituciones públicas o privadas.

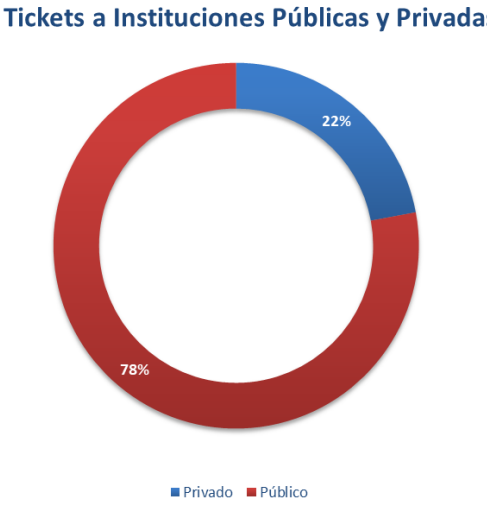


Ilustración 2— Tickets a Instituciones Públicas y Privadas

5. Estado de Ticket Procesados en el Presente Mes

En la siguiente tabla y gráfico de distribución se muestra el estado de los tickets procesados en el mes de septiembre de 2021. Como se puede apreciar la cantidad de tickets abiertos o generados en el período son un total de 1504 unidades. De este total, 837 tickets fueron cerrados exitosamente, lo que representa un 56% de eficacia, mientras que 667 tickets 44% siguen en desarrollo para terminar de ser procesados en el período siguiente.

Total estado Ticket	Total
En desarrollo	667
Cerrados	837
Total general	**1504**

Tabla 4 - Total Estado de Ticket

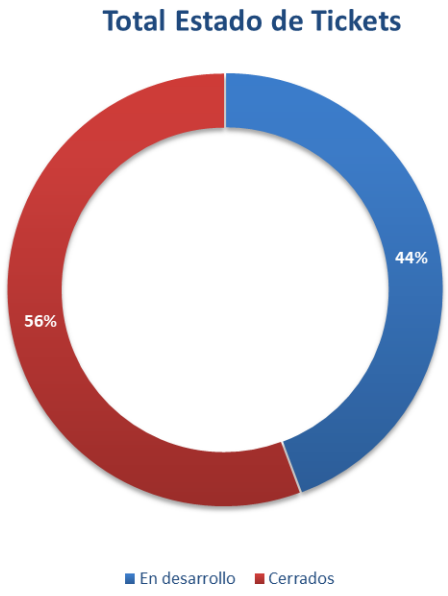


Ilustración 3 - Total Estado de Tickets

6. Procedencia de Generación de Tickets

En la siguiente tabla se presenta la composición -del origen de los tickets- que procesó CSIRT para el desarrollo de su labor durante el mes de septiembre de 2021.

Como se aprecia en la tabla, los tickets se pueden originar tanto interna como externamente.

Los tickets de origen internos son todos aquellos que fueron generados por sistemas propios del Ministerio del Interior y Seguridad Pública, mediante el software que utiliza CSIRT -que también considera los sensores que dan aviso o reportan- desde otros servicios públicos o de las FF.AA.

Por otro lado, los tickets de origen externo son todos aquellos que provienen de proveedores vinculados a CSIRT vía contractual o que se generan a través de call center, por formulario web, por medio de otros CSIRT internacionales, o por correos electrónicos de empresas privadas.

Tipo de Fuente	Cantidad de Tickets
Servicios Internos	1322
Servicios Externos	182
Total Fuentes de Tickets	**1504**

Tabla 5 - Fuentes de Servicios (Interna y/o Externa)

Como se puede observar en el siguiente gráfico, un 88% de la demanda de trabajo que recibió CSIRT en el pasado mes de septiembre tiene un origen interno, mientras que el 12% restante proviene de fuentes externas.

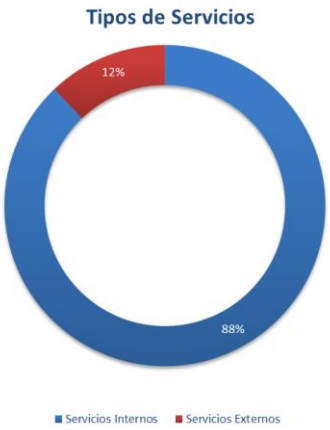


Ilustración 4- Distribución Porcentual de Origen de Tickets

7. Fuentes de Origen Externo de Tickets

En la siguiente tabla se presenta información que da cuenta de las fuentes externas que dieron origen a tickets de esa procedencia durante septiembre de 2021.

Fuentes de Origen Externo de Tickets	Cantidad de Tickets
Generados por privados vía formulario web	110
Generados por privados vía email	53
Generados por privados vía call center	19
Total	**182**

Tabla 6 - Fuentes de Origen Externo de Tickets

El siguiente gráfico de distribución muestra que en septiembre de 2021 el porcentaje mayor de tickets externos son generados por aquellos tickets que provienen de "de privados vía formulario web", con un 60,5% de participación. En segundo lugar, se ubican aquellos tickets que provienen de "de privados vía email" con un 29,1% de contribución.

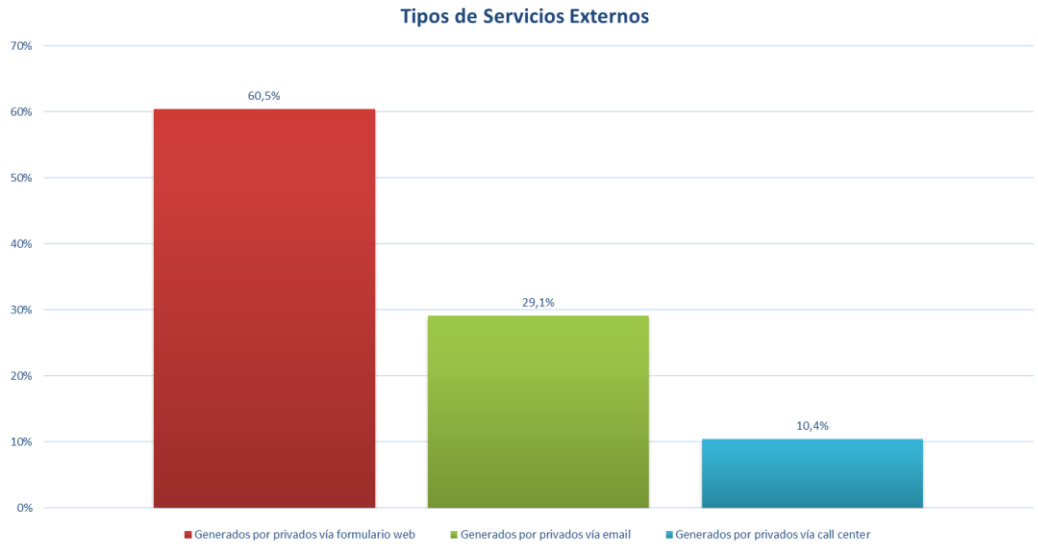
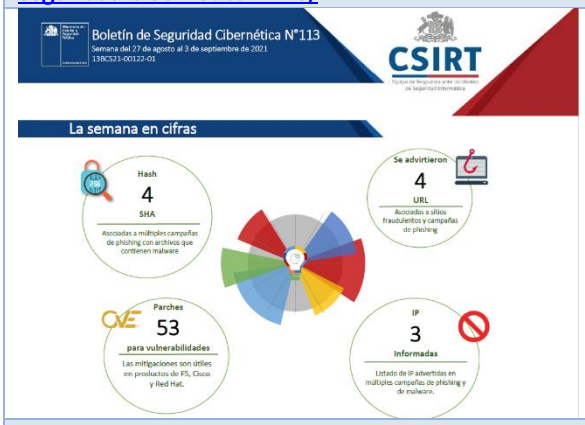
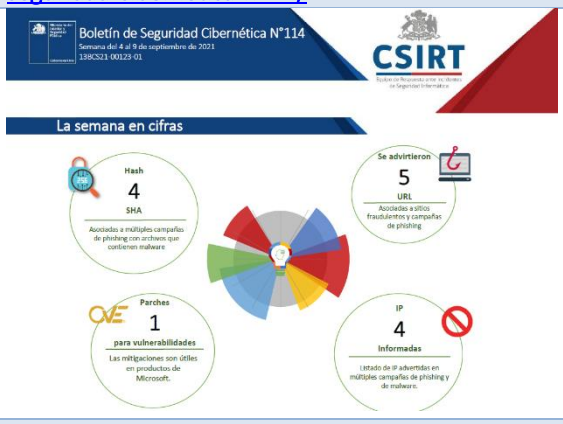
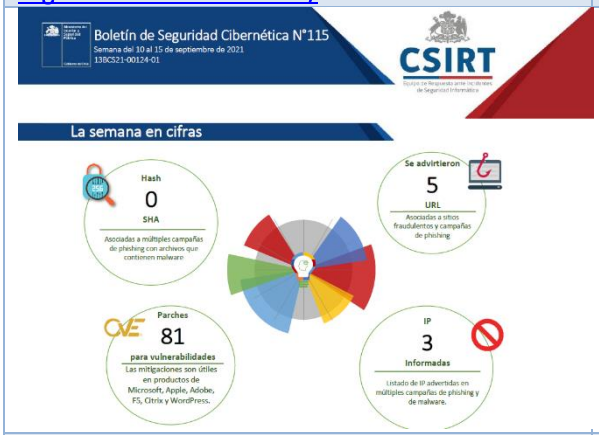
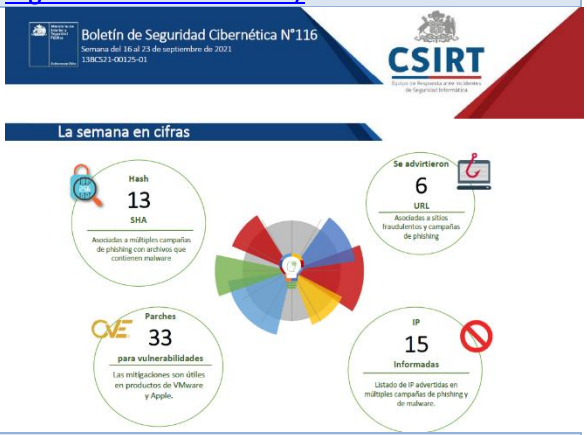
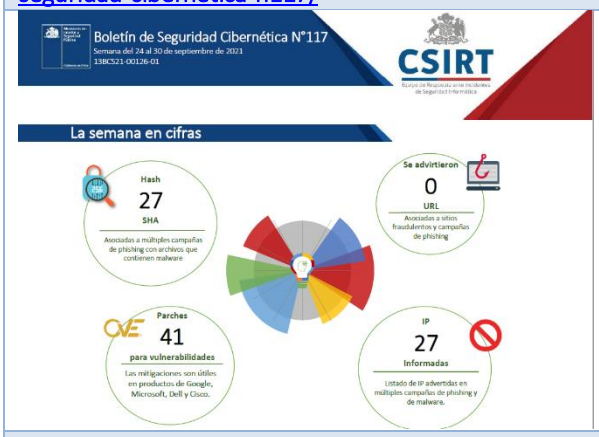


Ilustración 5- Tipos de servicios externo

8. Boletines con resúmenes de alertas y vulnerabilidades del mes

Los enlaces que se comparten a continuación corresponden a los boletines semanales publicados durante septiembre, los que contienen el resumen de actividades realizadas por el CSIRT de Gobierno y que fueron publicadas en el sitio web www.csirt.gob.cl.

Boletín de Seguridad Cibernética n°113	Boletín de Seguridad Cibernética n°114
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n113/	https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n114/
	
Boletín de Seguridad Cibernética n°115	Boletín de Seguridad Cibernética n°116
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n115/	https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n116/
	

Boletín de Seguridad Cibernética n°117	
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n117/	
	

9. Síntesis de gestión sobre concientización y buenas prácticas

Los enlaces que se comparten a continuación, corresponden a campaña de concientización y buenas prácticas publicadas por CSIRT de Gobierno durante el mes de septiembre y que están disponibles en el sitio web https://www.csirt.gob.cl/recomendaciones/

CiberSucesos No. 12 Ciberseguridad Industrial	Ciberconsejos | Egosurfing: el saludable hábito de buscarse en internet
https://www.csirt.gob.cl/recomendaciones/cibersucesos-no-12-ciberseguridad-industrial/	https://www.csirt.gob.cl/recomendaciones/ciberconsejos-egosurfing/
	

Ciberconsejos para evitar los peligros del Malvertising	Ciberconsejos | El riesgo que suponen los keyloggers, espías que pueden infectar nuestros dispositivos
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-evitar-los-peligros-del-malvertising/	https://www.csirt.gob.cl/recomendaciones/ciberconsejos-el-riesgo-que-suponen-los-keyloggers-espias-que-pueden-infectar-nuestros-dispositivos/
	

Actualidad

Exitoso Segundo Simposio de Ciberseguridad para Funcionarios Públicos, realizado por el CSIRT de Gobierno, congrega a casi mil inscritos

El Segundo Simposio para Funcionarios Públicos, efectuado el 28 de septiembre y realizado íntegramente por funcionarios del CSIRT de Gobierno, dependiente del Ministerio del Interior, logró superar con creces los números de registros de su primera versión, llegando a los casi mil inscritos.

Pueden leer los detalles y descargar las presentaciones en www.csirt.gob.cl/noticias/exitoso-segundo-simposio-funcionarios.

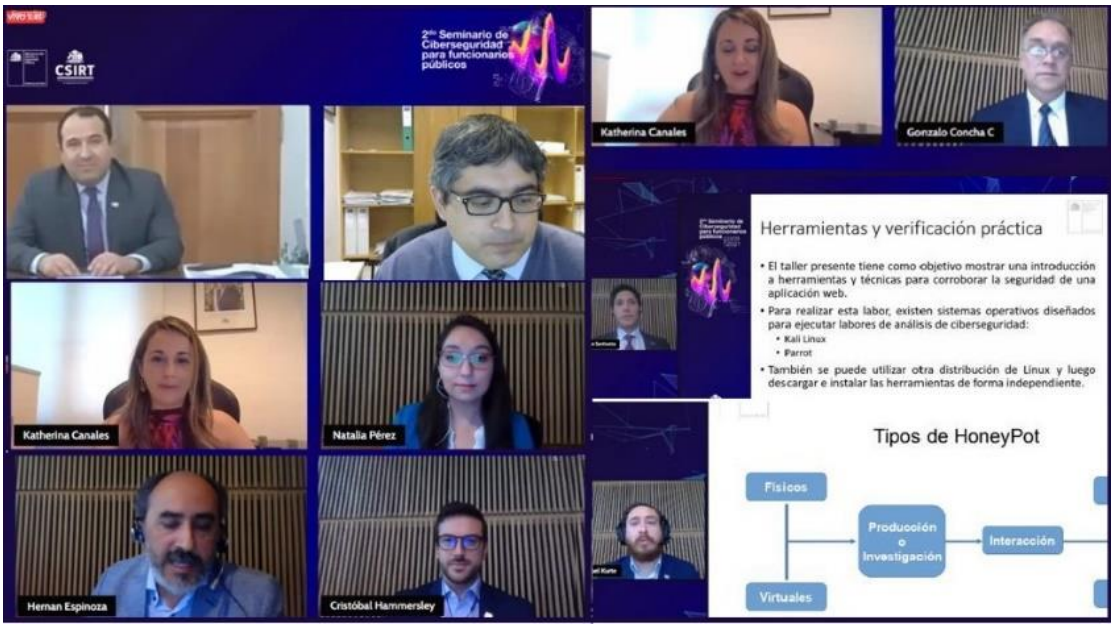
Como en su primera versión, la bienvenida estuvo a cargo del Subsecretario del Interior, desde el Palacio de La Moneda. Las charlas y talleres realizadas por los funcionarios fueron las siguientes.

CHARLAS

- Ciberseguridad en el Estado, análisis del nuevo marco normativo: Carlos Landeros, Director del CSIRT de Gobierno.
- Seguridad en sitios web: Natalia Perez, Analista CSIRT.
- Controles para mitigar amenazas en ciberseguridad: Gonzalo Concha, Analista CSIRT
- Revocación de nombres de dominio: Cristóbal Hammersley, Asesor CSIRT.

TALLERES

- Usando un SIEM (opensource): Wazuh: Hernan Espinoza, Analista CSIRT.
- Usando un Honeypot (opensource): Miguel Kurte, Analista CSIRT.
- Seguridad en sitios web, herramientas y verificación práctica: Juan Sanhueza, Analista CSIRT.



Claves de la jornada

- Se registraron para participar casi 1.000 encargados de ciberseguridad de reparticiones del Estado, empresas públicas y organizaciones privadas que tienen convenio con el CSIRT de Gobierno, contra 680 el año pasado.
- Las charlas y talleres son realizadas íntegramente por expertos pertenecientes al CSIRT de Gobierno, por lo que además de su conocimiento técnico comparten su experiencia en la práctica, monitoreando el ciberespacio nacional
- Para servir a un público lo más amplio posible, sin importar restricciones presupuestarias, los talleres utilizaron herramientas de código abierto, con uso libre, gratuito y adaptable.
- Para elegir los temas a tratar se encuestó a los encargados de ciberseguridad de los servicios públicos con los que trabaja el CSIRT de Gobierno, con tal de responder a necesidades concretas de la administración pública en materia de ciberseguridad.
- Se transmitió durante 8 horas a través de Zoom y Linkedin Live.

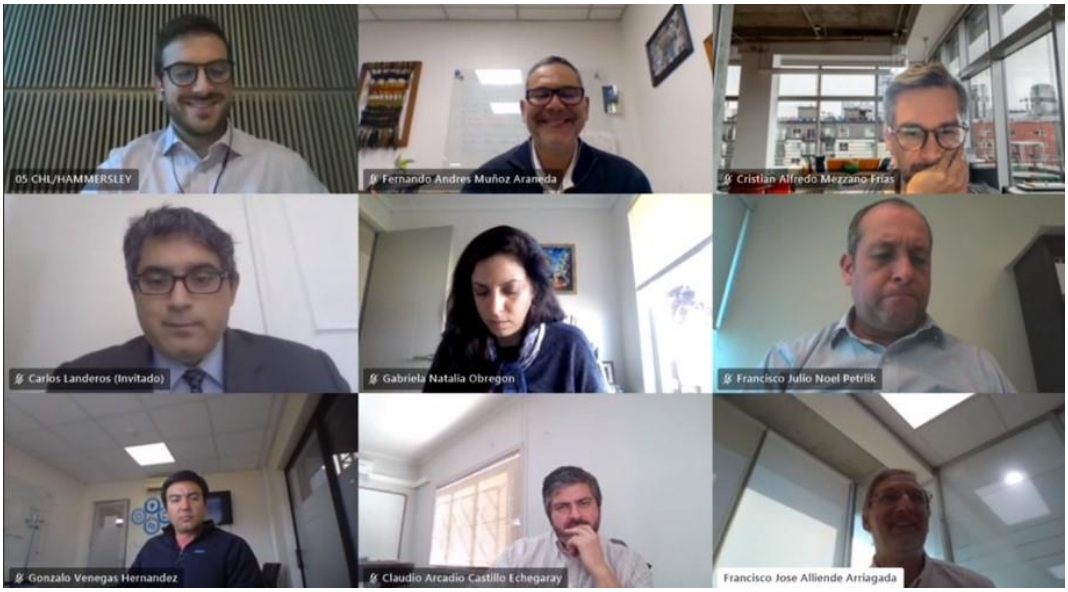
Gobierno presenta proyecto de ley para crear el Ministerio de Seguridad Pública, que incorpora a la futura Agencia Nacional de Ciberseguridad

El Presidente de la República, Sebastián Piñera, acompañado de los Ministros del Interior y Seguridad Pública, Rodrigo Delgado, y de Justicia y Derechos Humanos, Hernán Larraín, presentó el proyecto de ley que busca crear el Ministerio de Seguridad Pública. A la ceremonia también asistieron el General Director de Carabineros, Ricardo Yáñez, y el Director General de la Policía de Investigaciones (PDI), Sergio Muñoz, y los subsecretarios del Interior, Juan Francisco Galli, y de Prevención del Delito, María José Gómez.

El proyecto pone bajo dependencia jerárquica de este nuevo ministerio a Carabineros y la PDI, además de la futura Agencia Nacional de Ciberseguridad. Con él, además, colaborará la Agencia Nacional de Inteligencia (ANI), cuando se trate de materias de seguridad pública. Todas estas instituciones deben funcionar como un sistema de seguridad pública, explicó el Presidente.

Más detalle de la presentación y del proyecto de ley: https://www.csirt.gob.cl/noticias/gobierno-presenta-proyecto-de-ley-para-crear-el-ministerio-de-seguridad-publica/.

La Ciberseguridad Industrial fue el foco de una productiva presentación realizada por el CSIRT de Gobierno ante gerencia del grupo Saesa



En el marco del trabajo de colaboración público-privada del CSIRT de Gobierno, nuestra institución realizó una presentación a miembros de la alta gerencia del Grupo Saesa, empresa que es parte de la asociación Empresas Eléctricas, la que a su vez mantiene un convenio con el CSIRT.

Comenzó el evento el director nacional del CSIRT de Gobierno, Carlos Landeros, quien realizó su presentación titulada «Ciberseguridad desde la primera línea», que trataba, entre otras cosas, sobre las diferencias de la ciberseguridad cuando se trata de procesos industriales, debido a la convergencia entre las tecnologías de la información (IT) y las tecnologías operacionales (OT).

El director nacional también detalló las implicancias del proyecto de Ley Marco de Ciberseguridad (que también crea la Agencia Nacional de Ciberseguridad). Siguió luego la presentación de Cristóbal Hammersley, asesor jurídico del CSIRT de Gobierno, quien habló del trabajo realizado por la institución para implementar normas sectoriales de ciberseguridad.

Más detalles de lo presentado: csirt.gob.cl/noticias/la-ciberseguridad-industrial-fue-el-foco-de-una-productiva-presentacion-realizada-por-el-csirt-de-gobierno-ante-gerencia-del-grupo-saesa/.

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.10.04 09:48:16 -03'00'