Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Informe de gestión de Seguridad Cibernética

02 de agosto 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 julio 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 julio 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	1717
2	Disponibilidad	6D00	376
3	Información de seguridad de contenidos	7S00	111
4	Fraude	8F00	81
5	Otros	11O00	53
6	Código Malicioso	2C00	3
7	Recopilación de Información	3R00	0
8	Contenido Abusivo	1A00	0
9	Intentos de Intrusión	4I00	0
10	Intrusión	5I00	0
Total			**2341**

Tabla 1 - Total Tipos de Tickets

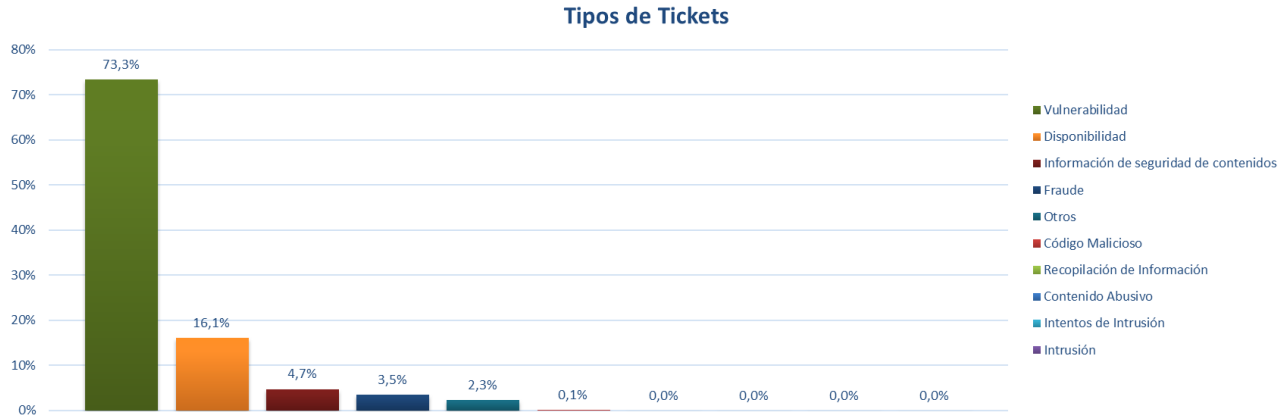


Ilustración 1 - Tipos de tickets

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 julio, respecto a junio de 2021.

Como se aprecia en la tabla, los tickets de las categorías de fraude, código malicioso, recopilación de información, contenido abusivo, decrecen en su tendencia (hay menos números de tickets), mientras que tres categorías experimentan una tendencia creciente al comparar el mes de julio con el pasado mes de junio.

N°	Junio	Julio	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	Código Malicioso	Código Malicioso	▼	➡
7	Recopilación de Información	Recopilación de Información	▼	➡
8	Contenido Abusivo	Contenido Abusivo	▼	➡
9	Intentos de Intrusión	Intentos de Intrusión	➡	➡
10	Intrusión	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	9	1708	1717
Disponibilidad	11	365	376
Información de seguridad de contenidos	97	14	111
Fraude	71	10	81
Otros	13	40	53
Código Malicioso	0	3	3
Recopilación de Información	0	0	0
Contenido Abusivo	0	0	0
Intentos de Intrusión	0	0	0
Intrusión	0	0	0
Total	**201**	**2140**	**2341**

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.

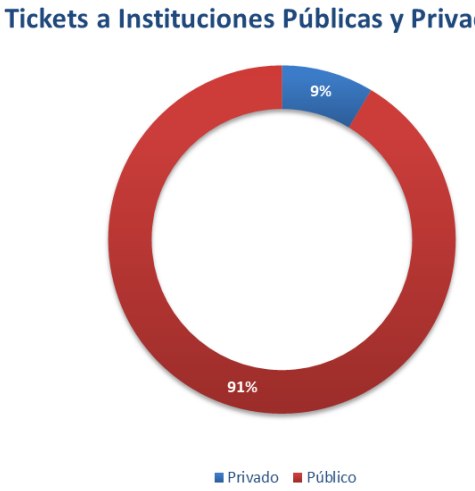


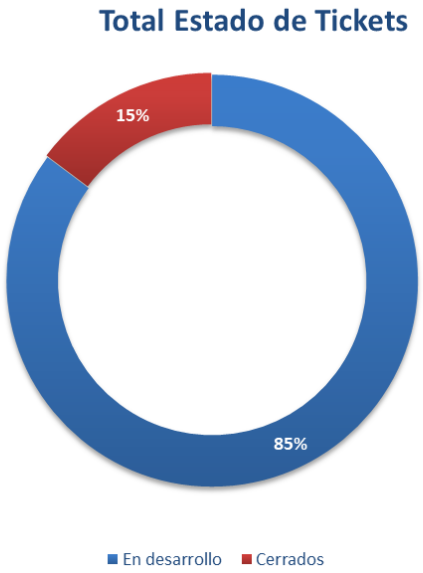
Ilustración 2–- Tickets a Instituciones Públicas y Privadas

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 julio de 2021. Como se puede apreciar la cantidad de tickets abiertos o generados en el período son un total de 2341 unidades. De este total, 346 tickets fueron cerrados exitosamente, lo que representa un 15% de eficacia, mientras que 1.995 tickets 85% siguen en desarrollo para terminar de ser procesados en el período siguiente.

Total estado Ticket	Total
En desarrollo	1995
Cerrados	346
Total general	**2341**

Tabla 4 - Total Estado de Ticket



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 julio 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	2271
Servicios Externos	70
Total Fuentes de Tickets	**2341**

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

Como se puede observar en el siguiente gráfico, un 97% de la demanda de trabajo que recibió CSIRT en el pasado mes de julio tiene un origen interno, mientras que el 3% restante proviene de fuentes externas.

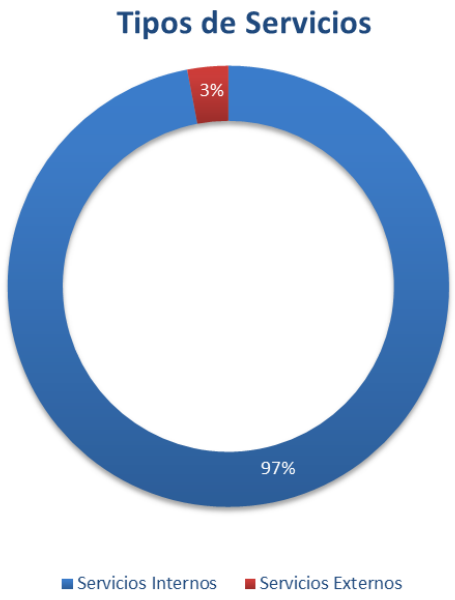


Ilustración 4- Distribución Porcentual de Origen de Tickets

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 julio de 2021.

Fuentes de Origen Externo de Tickets	Cantidad de Tickets
Generados por información entregada por empresas privadas sin convenio de ciberseguridad	4
Generados por información entregada por empresas privadas con convenio de ciberseguridad	0
Generados por privados vía formulario web	43
Generados por privados vía email	18
Generados por privados vía call center	5
Generados por información de otros CSIRT internacionales	0
Total	**70**

Tabla 6 - Fuentes de Origen Externo de Tickets

El siguiente gráfico de distribución muestra que en julio de 2021 el porcentaje mayor de tickets externos son generados por aquellos tickets que provienen de “de privados vía formulario web”, con un 61% de participación. En segundo lugar, se ubican aquellos tickets que provienen de “de privados vía email” con un 26% de contribución.

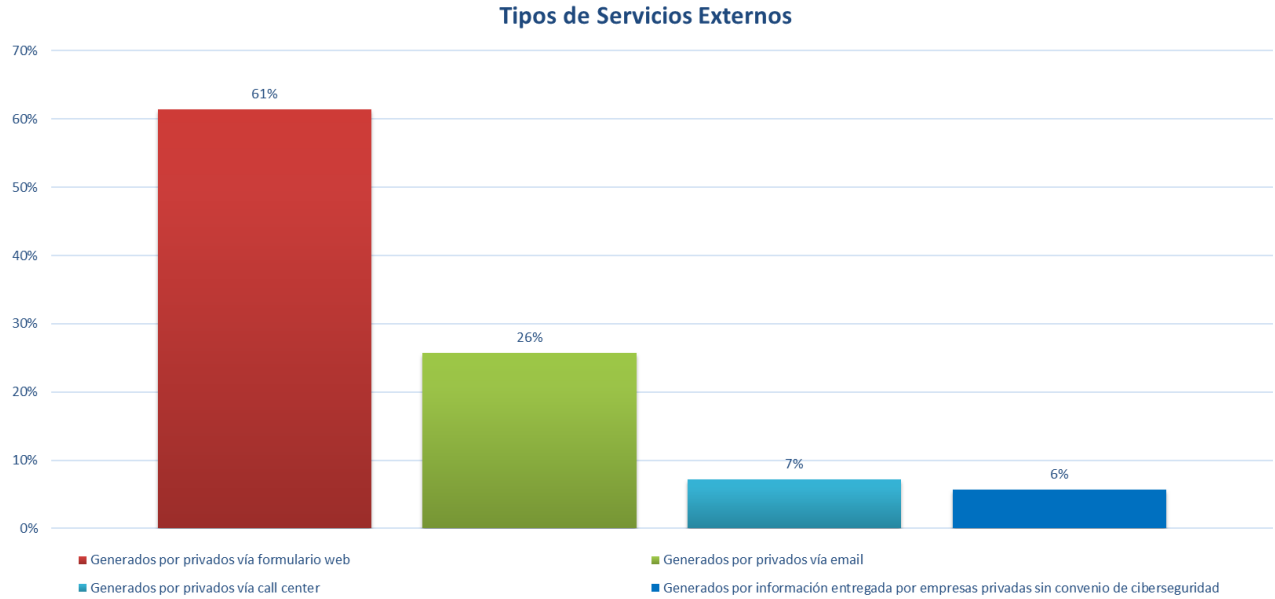
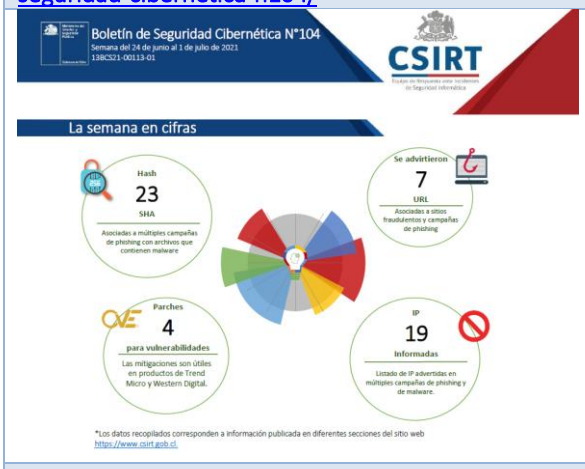
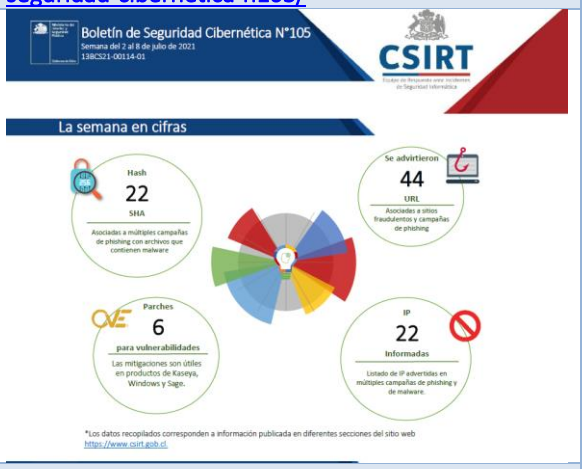
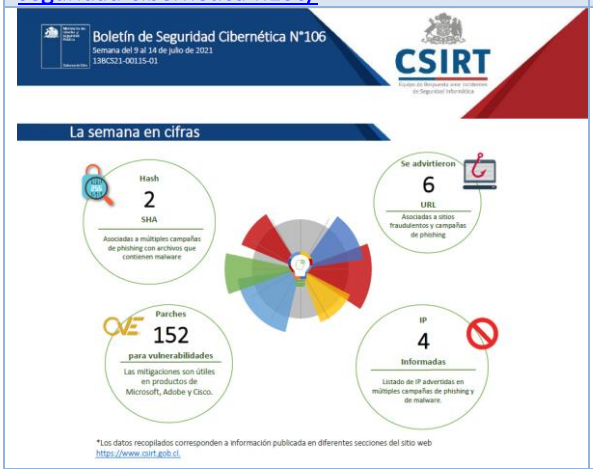
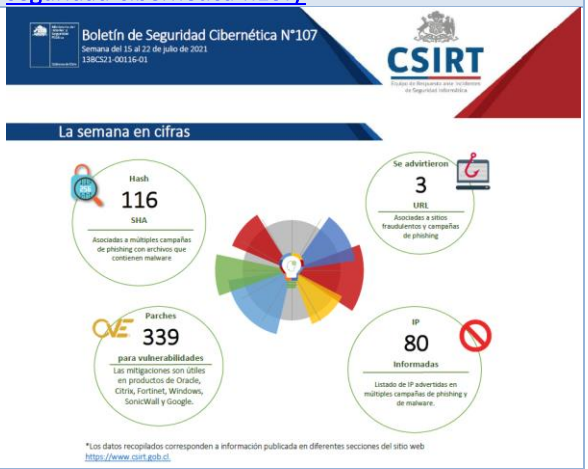


Ilustración 5- Tipos de servicios externo

8. Boletines con resúmenes de alertas y vulnerabilidades del mes

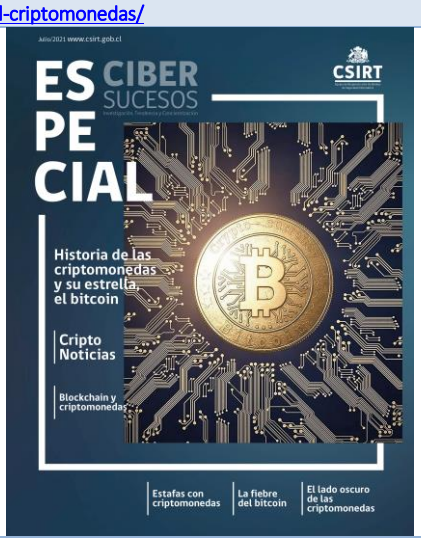
Los enlaces que se comparten a continuación corresponden a los boletines semanales publicados durante julio, los que contienen el resumen de actividades realizadas por el CSIRT de Gobierno y que fueron publicadas en el sitio web www.csirt.gob.cl.

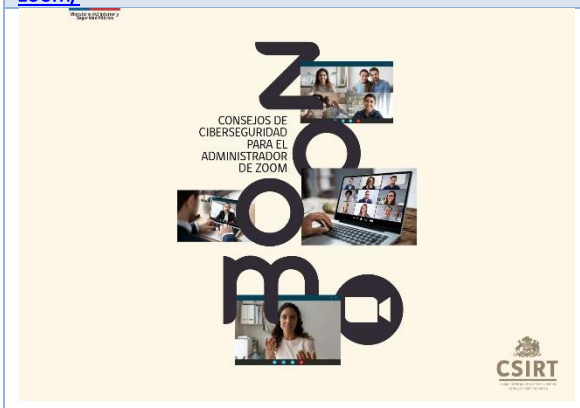
Boletín de Seguridad Cibernética n°104	Boletín de Seguridad Cibernética n°105
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n104/	https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n105/
	
Boletín de Seguridad Cibernética n°106	Boletín de Seguridad Cibernética n°107
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n106/	https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n107/
	

Boletín de Seguridad Cibernética n°108
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n108/

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 julio y que están disponibles en el sitio web https://www.csirt.gob.cl/recomendaciones/

CiberSucesos Especial Criptomonedas	Ciberconsejos | Cuida lo que compartes y evita el Descubrimiento Pasivo
https://www.csirt.gob.cl/recomendaciones/cibersucesos-especial-criptomonedas/	https://www.csirt.gob.cl/recomendaciones/ciberconsejos-cuida-lo-que-compartes-y-evita-el-descubrimiento-pasivo/
	

Ciberguías | Consejos de ciberseguridad para el administrador de Zoom	Investigación sobre Ataques a repositorios GIT
https://www.csirt.gob.cl/recomendaciones/ciberguias-consejos-de-ciberseguridad-para-el-administrador-de-zoom/	https://www.csirt.gob.cl/reportes/ataques-a-repositorios-git-caracteristicas-y-mitigacion/
	

Actualidad

Presidente Piñera envía proyecto de ley contra amenazas, coacción y hostigamiento

En una ceremonia en el Palacio de la Moneda, el Presidente de la República, Sebastián Piñera, presentó el proyecto de ley elaborado por el Gobierno para combatir de mejor forma las amenazas, el hostigamiento y la coacción.

La ceremonia contó con la participación de padres de víctimas de acoso escolar, como Evanyely Zamorano y Emanuel Pacheco, padres de Katy Summer y creadores de la fundación del mismo nombre, que lucha por combatir este tipo de hostigamiento.

Más información sobre el proyecto, aquí: https://www.csirt.gob.cl/noticias/presidente-pinera-envia-proyecto-de-ley-contra-amenazas-coaccion-y-hostigamiento-leyantiamenazas/.

Director del CSIRT de Gobierno lidera Tercera Reunión del Grupo de Trabajo sobre Medidas de Fomento de la Cooperación y Confianza en el Ciberespacio de la OEA

El Director del CSIRT del Gobierno de Chile, Carlos Landeros, dio inicio y dirigió la Tercera Reunión del Grupo de Trabajo sobre Medidas de Fomento de la Cooperación y Confianza en el Ciberespacio de la Organización de las Estados Americanos (OEA). Estuvieron presentes en la reunión, realizada de forma completamente virtual, los líderes de las instituciones nacionales y gubernamentales encargadas de la ciberseguridad de los países miembros del Grupo de Trabajo, junto a los representantes de la OEA, encabezados por la Secretaria General del Comité Interamericano Contra el Terrorismo, Alison Treppel.

Uno de los principales motivos de esta reunión fue la elección de un nuevo país líder del Grupo de Trabajo, posición que fue ejercida por Chile desde 2019, con México en la vicepresidencia. Las naciones partícipes eligieron a Isaac Morales, Coordinador de Seguridad Multidimensional en la Secretaría de Relaciones Exteriores de México como nuevo país líder, mientras Estados Unidos fue elegido para la vicepresidencia.

Más información sobre la jornada, aquí: https://csirt.gob.cl/noticias/director-del-csirt-de-gobierno-lidera-tercera-reunion-del-grupo-de-trabajo-sobre-medidas-de-fomento-de-la-cooperacion-y-confianza-en-el-ciberespacio-de-la-oea/.

Director del CSIRT de Gobierno inaugura segunda reunión de Cybersecurity Innovation Councils, organizada por la OEA y Cisco

La Organización de los Estados Americanos (OEA) y Cisco organizaron este martes la segunda reunión en Chile de los Cybersecurity Innovation Councils (CIC), espacio de discusión para la promoción de la innovación y las buenas prácticas en ciberseguridad. Teniendo un foco de ciberseguridad, el CSIRT de Gobierno no podía estar ausente, y así es como su Director Nacional, Carlos Landeros, participó del evento junto a otros actores relevantes del rubro en nuestro país, como el senador Kenneth Pugh, permanente impulsor de la ciberseguridad y la transformación digital en el Congreso; Carlos Ávila, responsable de Inteligencia Artificial del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación (un área clave en el avance de la transformación digital a todo nivel), Katherina Canales, Directora Operacional del CSIRT de Gobierno y Claudio Ortiz, gerente general en Chile de Cisco, importante empresa tecnológica que organizó la reunión junto a la OEA. Más información: https://www.csirt.gob.cl/noticias/director-del-csirt-de-gobierno-inaugurasegunda-reunion-de-cybersecurity-innovation-councils-organizada-por-la-oea-y-cisco/.

Exitosa cuarta versión del OEA Cyberwomen Challenge premia cuatro chilenas que disputarán final regional

La primera fecha de la cuarta edición del Cyberwomen Challenge, clasificatoria para la final americana tuvo lugar a principios de julio. Como cada año, mujeres de todo el país se inscribieron para participar, organizadas en equipos y compitiendo en una serie de realistas simulaciones de ataques informáticos.

Las ganadoras fueron Leticia Palazuelos, Margarita Vargas, Alejandra Rojas y Montserrat Rodríguez. Los detalles, aquí: https://www.csirt.gob.cl/noticias/exitosa-cuarta-version-del-oea-cyberwomen-challenge-premia-cuatro-chilenas-que-disputaran-final-regional/.

Katherina Canales, Mariana Cardona, Laura Alvarez y Boris Vásquez.