Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Informe de gestión de Seguridad Cibernética

02 de septiembre 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 agosto 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 agosto 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	1154
2	Disponibilidad	6D00	447
3	Fraude	8F00	151
4	Información de seguridad de contenidos	7S00	146
5	Otros	11O00	76
6	Contenido Abusivo	1A00	6
7	Código Malicioso	2C00	5
8	Intrusión	5I00	5
9	Recopilación de Información	3R00	3
10	Intentos de Intrusión	4I00	3
Total			**1996**

Tabla 1 - Total Tipos de Tickets

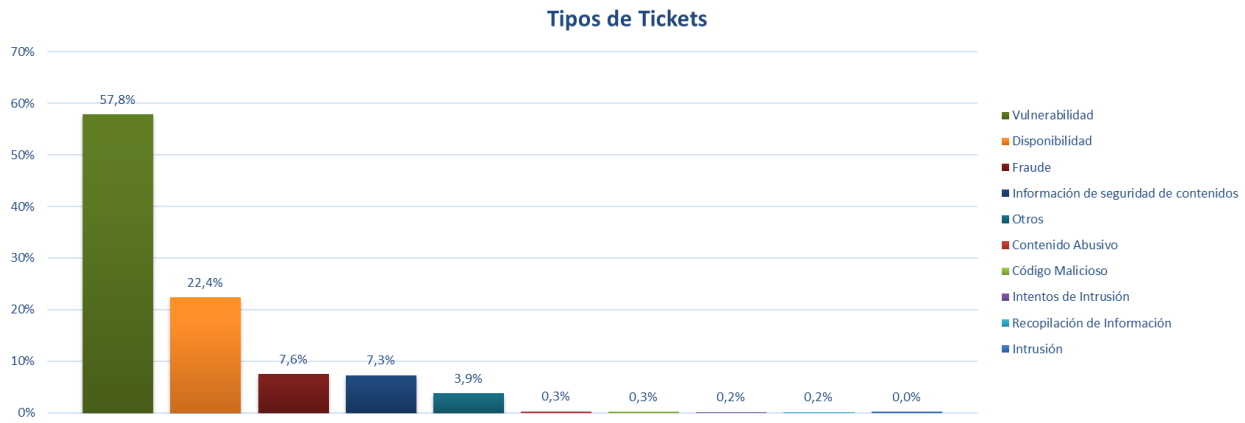


Ilustración 1 - Tipos de tickets

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 agosto, respecto a julio de 2021.

Como se aprecia en la tabla, los tickets de las categorías de vulnerabilidades (hay menos números de tickets), mientras que tres categorías experimentan una tendencia creciente al comparar el mes de agosto con el pasado mes de julio.

N°	Julio	Agosto	Tendencia	Variante
1	Vulnerabilidad	Vulnerabilidad	▼	➡
2	Disponibilidad	Disponibilidad	▲	➡
3	Información de seguridad de contenidos	Fraude	▲	⬆
4	Fraude	Información de seguridad de contenidos	▲	⬇
5	Otros	Otros	▲	➡
6	Código Malicioso	Contenido Abusivo	▲	⬆
7	Recopilación de Información	Código Malicioso	▲	⬇
8	Contenido Abusivo	Intrusión	▲	⬆
9	Intentos de Intrusión	Recopilación de Información	▲	⬇
10	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	36	1118	1154
Disponibilidad	31	416	447
Fraude	130	21	151
Información de seguridad de contenidos	121	25	146
Otros	11	65	76
Contenido Abusivo	0	6	6
Código Malicioso	4	1	5
Intrusión	3	2	5
Recopilación de Información	0	3	3
Intentos de Intrusión	0	3	3
Total	**336**	**1660**	**1996**

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.

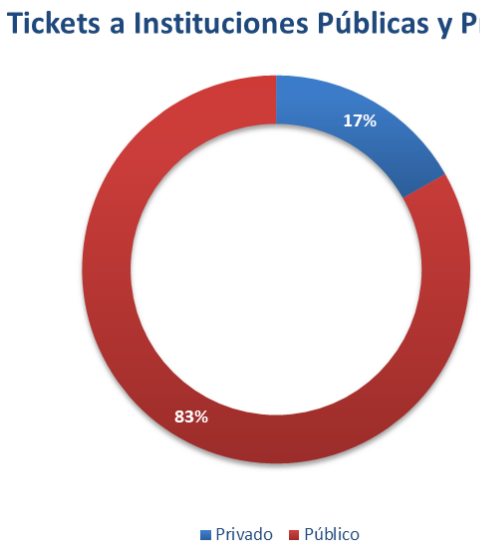


Ilustración 2–- Tickets a Instituciones Públicas y Privadas

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 agosto de 2021. Como se puede apreciar la cantidad de tickets abiertos o generados en el período son un total de 1996 unidades. De este total, 1241 tickets fueron cerrados exitosamente, lo que representa un 62% de eficacia, mientras que 755 tickets 38% siguen en desarrollo para terminar de ser procesados en el período siguiente.

Total estado Ticket	Total
En desarrollo	755
Cerrados	1241
Total general	**1996**

Tabla 4 - Total Estado de Ticket

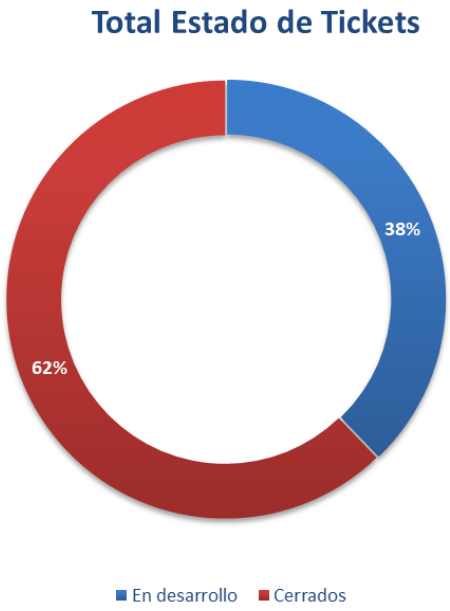


Ilustración 3 - Total Estado de Tickets

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 agosto 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	1849
Servicios Externos	147
Total Fuentes de Tickets	**1996**

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

Como se puede observar en el siguiente gráfico, un 93% de la demanda de trabajo que recibió CSIRT en el pasado mes de agosto tiene un origen interno, mientras que el 7% restante proviene de fuentes externas.

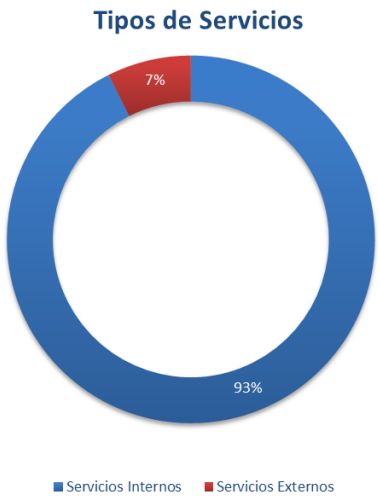


Ilustración 4- Distribución Porcentual de Origen de Tickets

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 agosto de 2021.

Fuentes de Origen Externo de Tickets	Cantidad de Tickets
Generados por información entregada por empresas privadas sin convenio de ciberseguridad	7
Generados por información entregada por empresas privadas con convenio de ciberseguridad	0
Generados por privados vía formulario web	83
Generados por privados vía email	45
Generados por privados vía call center	12
Generados por información de otros CSIRT internacionales	0
Total	**147**

Tabla 6 - Fuentes de Origen Externo de Tickets

El siguiente gráfico de distribución muestra que en agosto de 2021 el porcentaje mayor de tickets externos son generados por aquellos tickets que provienen de “de privados vía formulario web”, con un 56% de participación. En segundo lugar, se ubican aquellos tickets que provienen de “de privados vía email” con un 31% de contribución.

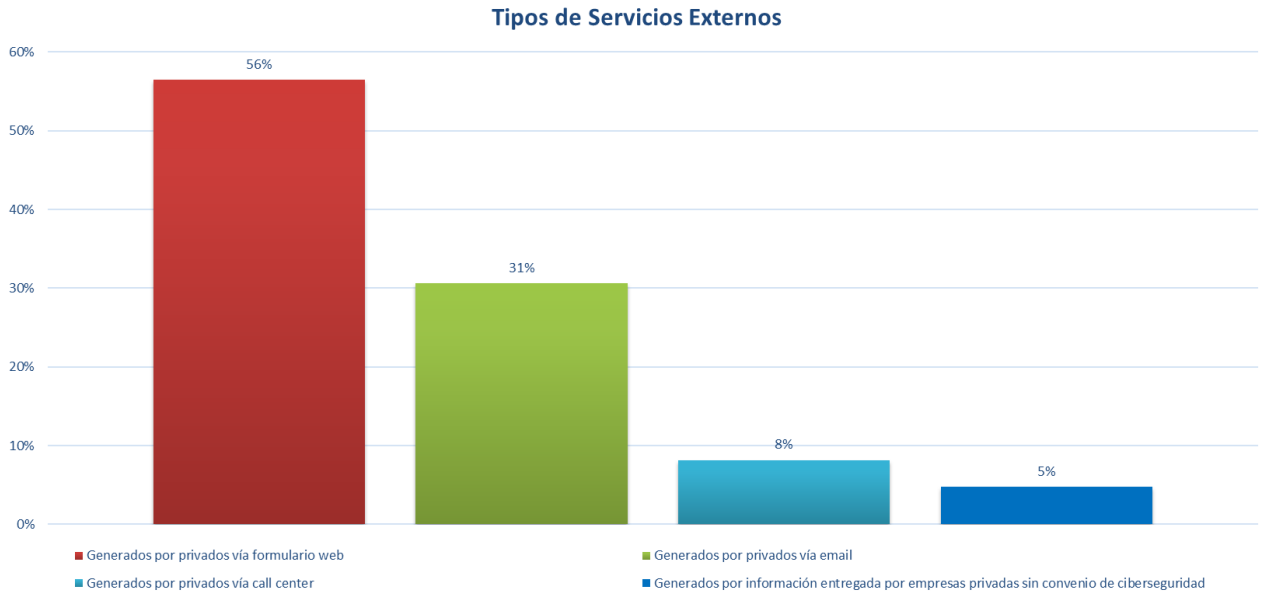
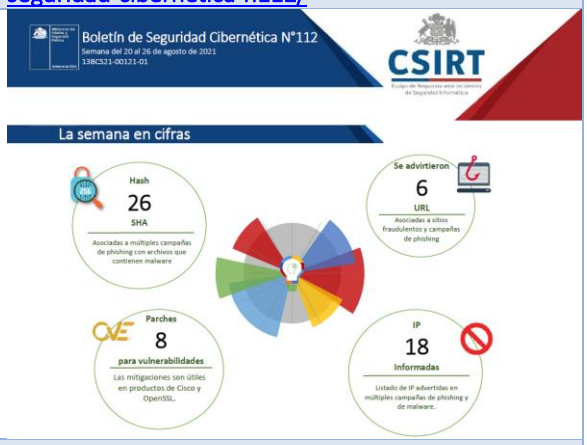


Ilustración 5- Tipos de servicios externo

8. Boletines con resúmenes de alertas y vulnerabilidades del mes

Los enlaces que se comparten a continuación corresponden a los boletines semanales publicados durante agosto, 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°109	Boletín de Seguridad Cibernética n°110
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n109/	https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n110/
	
Boletín de Seguridad Cibernética n°111	Boletín de Seguridad Cibernética n°112
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n111/	https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n112/
	

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

CiberSucesos Especial Cuentos de Ciberseguridad para Niños	Ciberconsejos | Navegación Segura para Niños, Niñas y Adolescentes
https://www.csirt.gob.cl/recomendaciones/cibersucesos-especial-cuentos-mes-del-nino/	https://www.csirt.gob.cl/recomendaciones/ciberconsejos-navegacion-segura-para-ninos-ninas-y-adolescentes/
	

Ciberguía de mediación parental | Consejos para el uso responsable de internet por parte de los niños, niñas y adolescentes	Ciberguías | Cómo Protegernos Contra el Fraude a los Emails Corporativos (BEC)
https://www.csirt.gob.cl/recomendaciones/ciberguias-consejos-de-ciberseguridad-para-el-administrador-de-zoom/	https://www.csirt.gob.cl/recomendaciones/ciberguias-como-protegernos-contra-el-fraude-a-los-emails-corporativos-bec/
	

Ciberconsejos | Cómo prevenir el secuestro de WhatsApp
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-como-prevenir-el-secuestro-de-whatsapp/

Actualidad

CSIRT de Gobierno realiza exitoso Primer Ejercicio de Simulación en Gestión de Ciberseguridad para funcionarios públicos

Este mes tuvo lugar el primer ejercicio de Simulación en Gestión de Ciberseguridad para el Estado, desarrollado en conjunto por el CSIRT de Gobierno, dependiente de la Subsecretaría del Interior, y la firma de ciberseguridad Kaspersky. La instancia reunió a 250 encargados de ciberseguridad de distintas reparticiones de la Administración Pública y de empresas que tienen convenios con el CSIRT de Gobierno.

Con el objetivo de fortalecer el rol de los encargados de ciberseguridad es que los invitamos a participar de una simulación de la respuesta ante un ciberataque, realizada de una manera lúdica, entretenida y didáctica. Así, este juego de simulación pone en práctica los conocimientos de gestión y la toma de decisiones, para poder afrontar y responder de manera efectiva y eficiente ante un ciberataque en el ámbito de la administración pública, vinculando la ciberseguridad a la reputación en la gestión de las tecnologías de información dentro del Estado.

Los tres encargados de ciberseguridad que obtuvieron los mayores puntajes fueron Andrés Camacho, de la Dirección de Presupuesto, Ítalo Foppiano, de la Universidad de Concepción y Jorge Montiel, de Metro de Santiago (en la foto de más arriba).

Tras el fin del ejercicio, tuvimos la alegría de constatar excelentes puntajes entre los participantes, estando así los 30 participantes con mejores resultados dentro de los 10 valores más altos, existiendo numerosos empates. Más orgullo aún nos causa el que el ranking fuera en su mayoría liderado por funcionarios de órganos del Estado y empresas públicas.

Más información sobre el evento y los ganadores, aquí: [https://www.csirt.gob.cl/noticias/csirt-de-gobierno-realiza-exitoso-primer-ejercicio-de-simulacion-en-gestion-de-ciberseguridad-para-funcionarios-publicos/.](https://www.csirt.gob.cl/noticias/csirt-de-gobierno-realiza-exitoso-primer-ejercicio-de-simulacion-en-gestion-de-ciberseguridad-para-funcionarios-publicos/)

1°	Andrés Camacho	Dirección de Presupuesto
2°	Ítalo Foppiano	Universidad de Concepción
3°	Jorge Montiel	Metro de Santiago
4°	Abraham Almarza	Ministerio de Bienes Nacionales
4°	Carlos Aravena	Subsecretaria de Defensa
5°	Cristián Mella	Fiscalía Nacional Económica
5°	Marcelo Rojo	Fiscalía Nacional Económica
5°	Diego Cancino	SB Pay
5°	Daniel Muñoz	Subsecretaría de Desarrollo Regional
6°	Fernando Jofré	Servicio de Evaluación Ambiental
6°	Cristián Silva	Superintendencia de Casinos de Juego
6°	Nicol Jeria	Agencia Nacional de Educación
7°	Fabián Acevedo	Subsecretaría de Energía
7°	Ariel Urrea	Junta Nacional de Auxilio Escolar y Becas
7°	Patricio Icka	SERNAGEOMIN
7°	Patricio Núñez	Superintendencia de Casinos de Juego
7°	Guillermo Meneses	Subsecretaria para Las Fuerzas Armadas
7°	Carlos Morales	Comisión para el Mercado Financiero
7°	Alejandro Figueroa	Dirección de Previsión de Carabineros
7°	Johan Palma Burrows	Econssa Chile
7°	Viterba Ordóñez	Servicio Médico Legal
7°	Tania Estrada	Instituto de Seguridad Laboral
7°	Roberto Siña	Estado Mayor Conjunto
8°	Francisco Barrera	Instituto de Salud Pública
8°	Rodrigo Ramírez	Consejo Nacional de Educación
8°	Marcelo Cancino	Servicio de Salud Ñuble
8°	Alexis Ubilla Salinas	Ministerio de Obras Públicas
8°	Rodrigo Cerda	Servicio de Evaluación Ambiental
8°	Victor Masjuan	Sixbell
8°	Alba Sepulveda	ODEPA

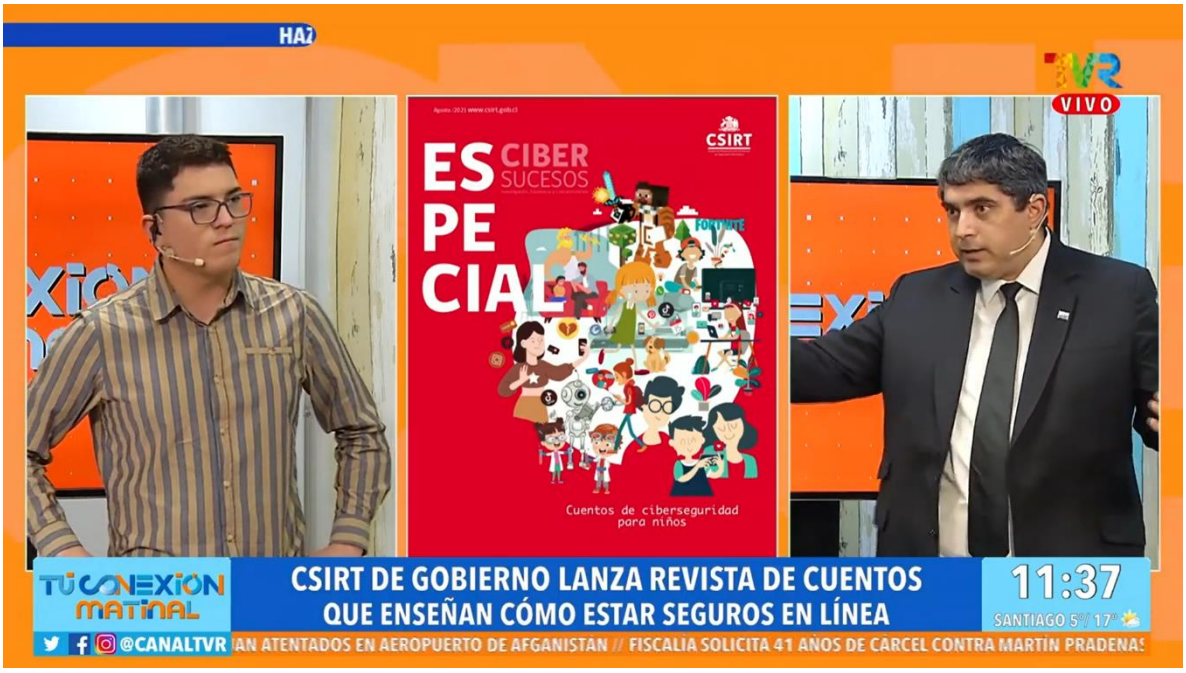
Ministerio del Interior y Subsecretaría de la Niñez lanzan junto a Entel nueva ciberguía de consejos para que los padres enfrenten junto a sus hijos las amenazas en la red

En el marco de la celebración del Día del Niño, el Ministerio del Interior, a través del CSIRT de Gobierno, el Ministerio de Desarrollo Social y Familia, a través de la Subsecretaría de la Niñez y la empresa de tecnología y telecomunicaciones Entel, a través de un alianza publico privada, presentan esta nueva “Ciberguía de Mediación Parental”, herramienta que busca entregar consejos para que padres, madres y/o tutores puedan acompañar y apoyar a niños, niñas y adolescentes en la inmersión al mundo digital, de manera informada y responsable.

“Nuestros niños necesitan del acompañamiento y la enseñanza de sus padres para usar internet, ya que necesitan conocer de los peligros que conlleva el ciberespacio y cómo protegerse”, explica el Subsecretario del Interior, Juan Francisco Galli. “Por eso creamos esta nueva ciberguía, que además de ayudar a los padres a educar a sus hijos en prácticas digitales ciberseguras, representa un nuevo ejemplo de colaboración público-privada, algo que ha estado impulsando el CSIRT de Gobierno, dependiente de esta Subsecretaría”, agregó. Más información aquí:

https://www.csirt.gob.cl/noticias/nueva-ciberguia-diadelnino2021/

Director del CSIRT de Gobierno presenta cuentos de ciberseguridad para niños en Tu Conexión Matinal de TVR



El último viernes de agosto el director nacional del CSIRT de Gobierno, Carlos Landeros, asistió a la invitación que hizo Tu Conexión Matinal del canal TVR (22 en televisión abierta, https://www.tvr.cl para su streaming en línea), para compartir con la comunidad los cuentos de ciberseguridad para niños, niñas y adolescentes que escribió el propio personal del CSIRT (y que pueden leer aquí: https://www.csirt.gob.cl/recomendaciones/cibersucesos-especial-cuentos-mes-del-nino/).

En el programa, Landeros explicó la importancia de educar a nuestros niños, niñas y adolescentes para que conozcan los riesgos de intenet y cómo evitarlos, anticipándose a los delitos y riesgos que acechan en el mundo online.

El video: https://www.youtube.com/watch?v=jNb6vLEWWbw&.

Pueden encontrar más información en csirt.gob.cl/noticias/director-del-csirt-de-gobierno-presenta-cuentos-de-ciberseguridad-para-ninos-en-tu-conexion-matinal-de-tvr/.

.

CSIRT de Gobierno abre 6° Exhibición Internacional de Seguridad Integral en panel con Senador Pugh y representantes del BID

En agosto también se realizó la sexta versión de SeguridadExpo Chile, convención que reúne especialistas de seguridad en diversos ámbitos, como la seguridad industrial, laboral y bioseguridad, prevención de incendios y riesgos naturales, y por supuesto, ciberseguridad.

Fue precisamente la ciberseguridad la que inició la jornada, con una conversación entre el Director Nacional del CSIRT de Gobierno, Carlos Landeros, y el Especialista Sectorial en Ciberseguridad del Banco Interamericano de Desarrollo (BID), Santiago Paz, moderado por el senador Kenneth Pugh, parlamentario que se ha enfocado en impulsar iniciativas de seguridad digital. El encuentro virtual contó además con las presentaciones del Subsecretario de Telecomunicaciones, Francisco Moreno, y la Representante del BID en Chile, María Florencia Attademo-Hirst.

Los detalles del evento: https://www.csirt.gob.cl/noticias/csirt-de-gobierno-abre-6-seguridadexpo/.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.09.02 19:27:59 -04'00'