Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Informe de gestión de Seguridad Cibernética

01 de marzo 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 febrero 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 febrero 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 -6.200 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	921
2	Recopilación de Información	3R00	324
3	Información de seguridad de contenidos	7S00	124
4	Código Malicioso	2C00	106
5	Operaciones Ciberseguridad CSIRT	19OC	68
6	Fraude	8F00	65
7	Disponibilidad	6D00	44
8	Intrusión	5I00	21
9	Contenido Abusivo	1A00	16
10	Intentos de Intrusión	4I00	2
	Total		**1691**

Tabla 1 - Total Tipos de Tickets

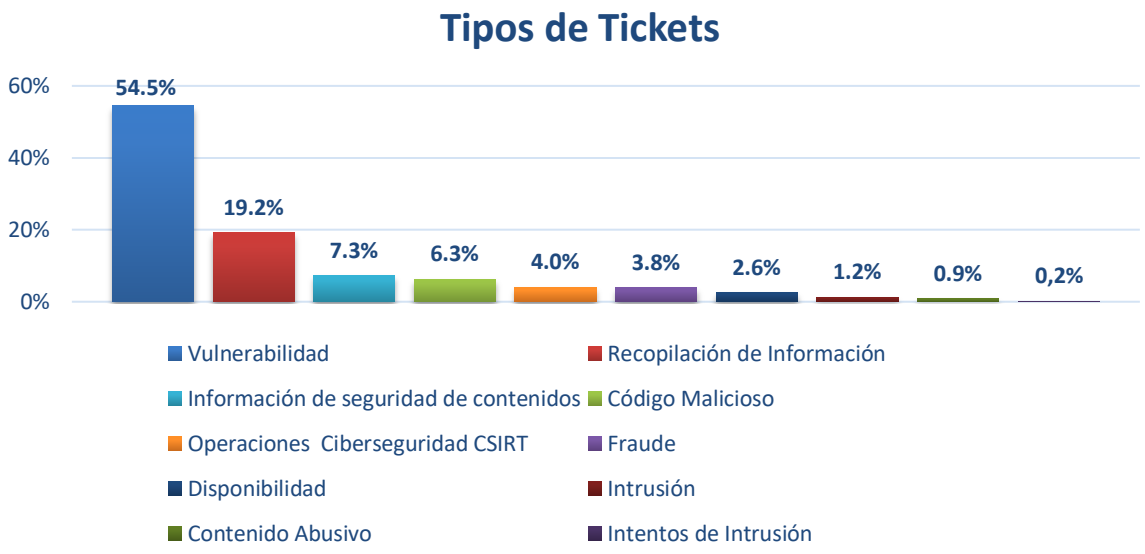


Ilustración 1 - Tipos de tickets

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 febrero, respecto a enero de 2020.

Como se aprecia en la tabla, los tickets de las categorías de, información de seguridad de contenidos fraude, operaciones de ciberseguridad CSIRT, código malicioso, contenido abusivo e intentos de intrusión decrecen en su tendencia (hay menos números de tickets), mientras que vulnerabilidades, recopilación de información y disponibilidad experimentan una tendencia creciente al comparar el mes de enero con el pasado mes de febrero, en el caso de intrusión, se mantiene su tendencia
.

	Enero		Febrero	Tendencia	Variante
1	Recopilación de Información	1	Vulnerabilidad	▲	⬆
2	Vulnerabilidad	2	Recopilación de Información	▲	⬇
3	Información de seguridad de contenidos	3	Información de seguridad de contenidos	▼	➡
4	Código Malicioso	4	Código Malicioso	▼	➡
5	Operaciones Ciberseguridad Csirt	5	Operaciones Ciberseguridad CSIRT	▼	➡
6	Fraude	6	Fraude	▼	➡
7	Contenido Abusivo	7	Disponibilidad	▲	⬆
8	Intrusión	8	Intrusión	➡	➡
9	Intentos de Intrusión	9	Contenido Abusivo	▼	⬇
10	Disponibilidad	10	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.

Ticket	Privado	Público	Total
Vulnerabilidad	47	874	921
Recopilación de Información	65	259	324
Información de seguridad de contenidos	104	20	124
Código Malicioso	9	97	106
Operaciones Ciberseguridad CSIRT	53	15	68
Fraude	42	23	65
Disponibilidad	7	37	44
Intrusión	2	19	21
Contenido Abusivo	1	15	16
Intentos de Intrusión	0	2	2
Total	330	1361	1691

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.

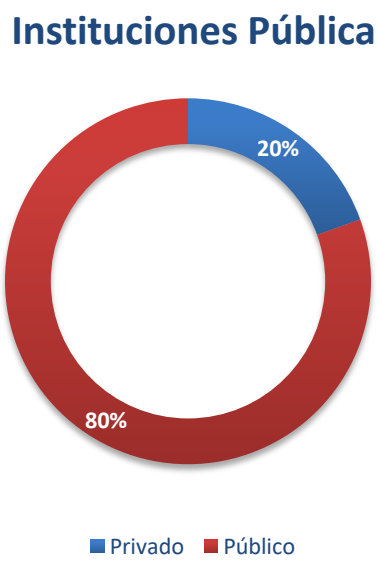


Ilustración 2 - Tickets a Instituciones Públicas y Privadas

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 febrero de 2021. Como se puede apreciar la cantidad de tickets abiertos o generados en el período son un total de 1.691 unidades. De este total, 883 tickets fueron cerrados exitosamente, lo que representa un 52% de eficacia, mientras que 808 tickets (48%) siguen en desarrollo para terminar de ser procesados en el período siguiente.

Total estado Ticket	Total
En desarrollo	808
Cerrados	883
Total general	1691

Tabla 4 - Total Estado de Ticket

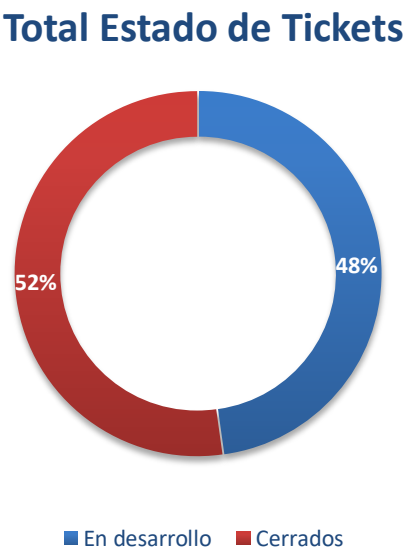


Ilustración 3 - Total Estado de Tickets

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 febrero 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	1307
Servicios Externos	384
Total Fuentes de Tickets	1691

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

Como se puede observar en el siguiente gráfico, un 77% de la demanda de trabajo que recibió CSIRT en el pasado mes de febrero tiene un origen interno, mientras que el 23% restante proviene de fuentes externas.

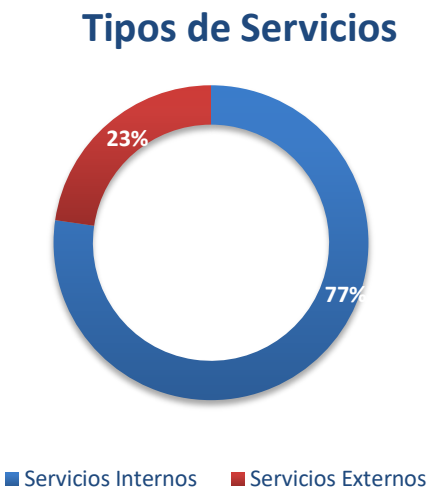


Ilustración 4 - Distribución Porcentual de Origen de Tickets

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 febrero de 2021.

Fuentes de Origen Externo de Tickets	Cantidad de Tickets
Tickets generados por información entregada por empresas privadas sin convenio de ciberseguridad	242
Tickets generados por información entregada por empresas privadas con convenio de ciberseguridad	0
Tickets generados por privados vía formulario web	99
Tickets generados por privados vía email	43
Tickets generados por privados vía call center	0
Tickets generados por información de otros CSIRT internacionales	0
Total	**384**

Tabla 6 - Fuentes de Origen Externo de Tickets

El siguiente gráfico de distribución muestra que en febrero de 2021 el porcentaje mayor de tickets externos son generados por reportes entregados por "Empresas privadas sin convenio de ciberseguridad CSIRT", con un 63% de participación. En segundo lugar, se ubican aquellos tickets que provienen de "de privados vía formulario web" con un 26% de contribución.

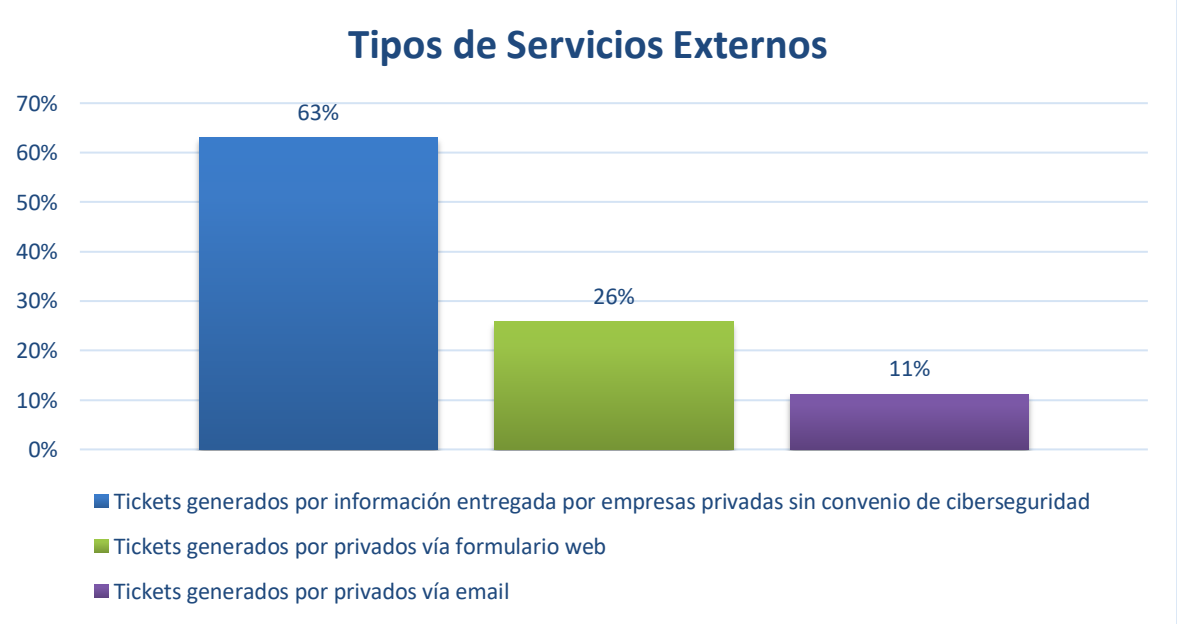


Ilustración 5 - Tipos de servicios externos

8. Boletines con resúmenes de alertas y vulnerabilidades del mes

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

Boletín de Seguridad Cibernética n°83	Boletín de Seguridad Cibernética n° 84
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n83/	https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n84/
	
Boletín de Seguridad Cibernética n°85	**Boletín de Seguridad Cibernética n°86**
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n85/	https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n86/
	

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 durante el mes de febrero y que están disponibles en el sitio web https://www.csirt.gob.cl/recomendaciones/

Día Internacional de Internet Segura: Ciberconsejos para navegar por internet	Ciberconsejos para una conexión a redes Wifi públicas más segura
https://www.csirt.gob.cl/recomendaciones/dia-internacional-de-internet-segura-ciberconsejos-para-navegar-por-internet/	https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-una-conexion-a-redes-wifi-publicas-mas-segura/
	
Vuelta a clases segura | Cibersucesos no. 7	**Ciberconsejos de verano para navegar seguros en redes sociales**
https://www.csirt.gob.cl/recomendaciones/cibersucesos-no-7/	https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-evitar-ser-victimas-del-spoofing/
	

Ciberconsejos para el uso seguro de los videojuegos
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-el-uso-seguro-de-los-videojuegos/

10. Actualidad

Cibersucesos no. 7

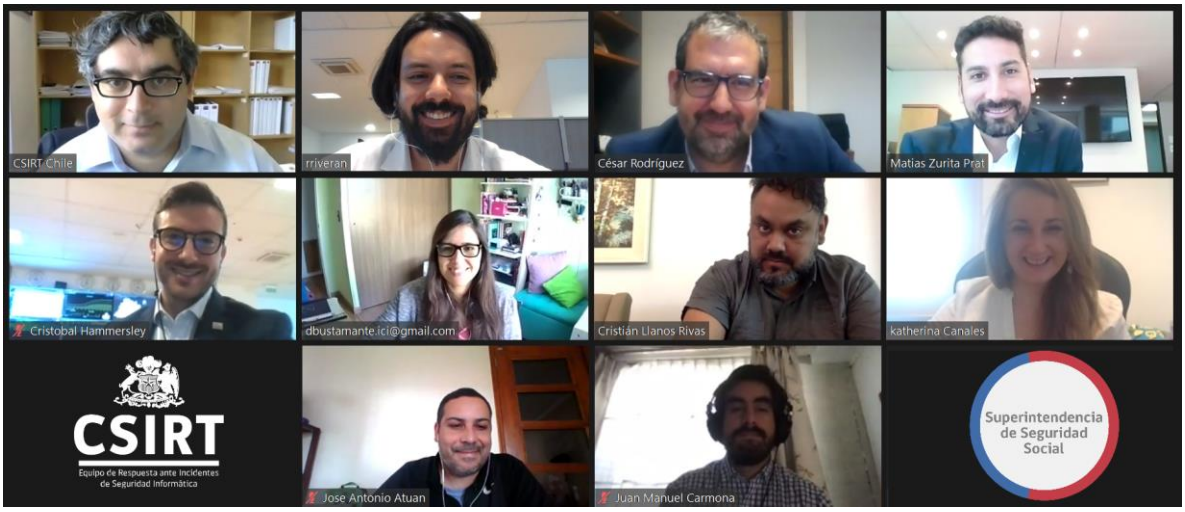
Promover una vuelta a clases virtual segura es el eje de esta séptima edición de Cibersucesos, que lanzamos hoy como CSIRT de Gobierno. Así, como tema principal ofrecemos un decálogo de convivencia en las redes sociales, dirigido a los jóvenes, para que sepan qué hacer al enfrentarse al lado oscuro de la interacción digital, como el ciberbullying, la exposición a contenido violento y perturbador, la sextorsión y la violación de su privacidad.

En la misma línea, compartimos los pasos a seguir para que los niños tengan la mayor seguridad al conectarse para recibir sus clases de forma virtual, tendencia que continúa desde el año pasado a causa de la pandemia, y que se ha visto posibilitada en muchos casos gracias a los esfuerzos del Gobierno para proveer de computadores y conexión de internet a estudiantes vulnerables a lo largo del país. Colombia es la nación que comparte su ejemplo en la sección Cooperación Internacional, a través de la experiencia de "En TIC confío", iniciativa destinada a concientizar a los jóvenes para adquirir hábitos saludables en internet.

En Comunidad Hacker, los creadores de la Fundación Katy Summer comparten los proyectos e iniciativas que han desarrollado para combatir el ciberacoso a los menores, en honor a su hija, Katy Winter, que murió a causa de este flagelo de la vida online que afecta a niños y adolescentes. Asimismo, nuestros expertos de la sección Legal analizan, en esta ocasión, las implicancias judiciales del ciberacoso o ciberbullying, cómo se define y su regulación (o más bien, falta de) en nuestro país.

Ver más: https://www.csirt.gob.cl/recomendaciones/cibersucesos-no-7/

CSIRT presenta a la Suseso resultados de Evaluación de Madurez en Ciberseguridad de las Cajas de Compensación



El CSIRT de Gobierno, dependiente de la Subsecretaría del Interior, presentó a la Superintendencia de Seguridad Social (Suseso) los resultados de la Evaluación de la Madurez en Ciberseguridad de las Cajas de Compensación, entidades que son fiscalizadas por la Suseso.

La correspondiente reunión, hecha de forma virtual, fue dirigida por los dos más altos cargos de las respectivas instituciones, César Rodríguez, superintendente (s) de la Suseso e intendente de Beneficios Sociales, y Carlos Landeros, director nacional del CSIRT de Gobierno.

Esta evaluación tiene como objetivo principal conocer las oportunidades de mejora, en términos de ciberseguridad, dentro de las distintas cajas de compensación. Es además la primera vez que el CSIRT evalúa la madurez de la ciberseguridad en este tipo de instituciones.

La iniciativa permite asimismo a la Suseso y el CSIRT avanzar hacia el desarrollo de una circular que fije normativas y estándares comunes entre todas las cajas de compensación, proceso que ya se encuentra en su recta final en lo relativo a las mutuales, entidades igualmente fiscalizadas por la Suseso.

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.03.01 20:16:00 -03'00'