CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Informe de Gestión de Seguridad Cibernética

CSIRT - julio 2020

Santiago, 05 de agosto de 2020

División de Redes y Seguridad Informática
Gobierno de Chile

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

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 2020. 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/o 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/o 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 tipo de ticket. 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	Cantidad
1	Recopilación de Información	3R00	353
2	Fraude	8F00	323
3	Vulnerabilidad	9V00	299
4	Código Malicioso	2C00	129
5	Información de seguridad de contenidos	7S00	71
6	Operaciones Ciberseguridad CSIRT	19OC	65
7	Disponibilidad	6D00	28
8	Intrusión	5I00	4
9	Contenido Abusivo	1A00	2
10	Intentos de Intrusión	4I00	1
	TOTAL		1275

Tabla 1 - Total Tipos de Tickets

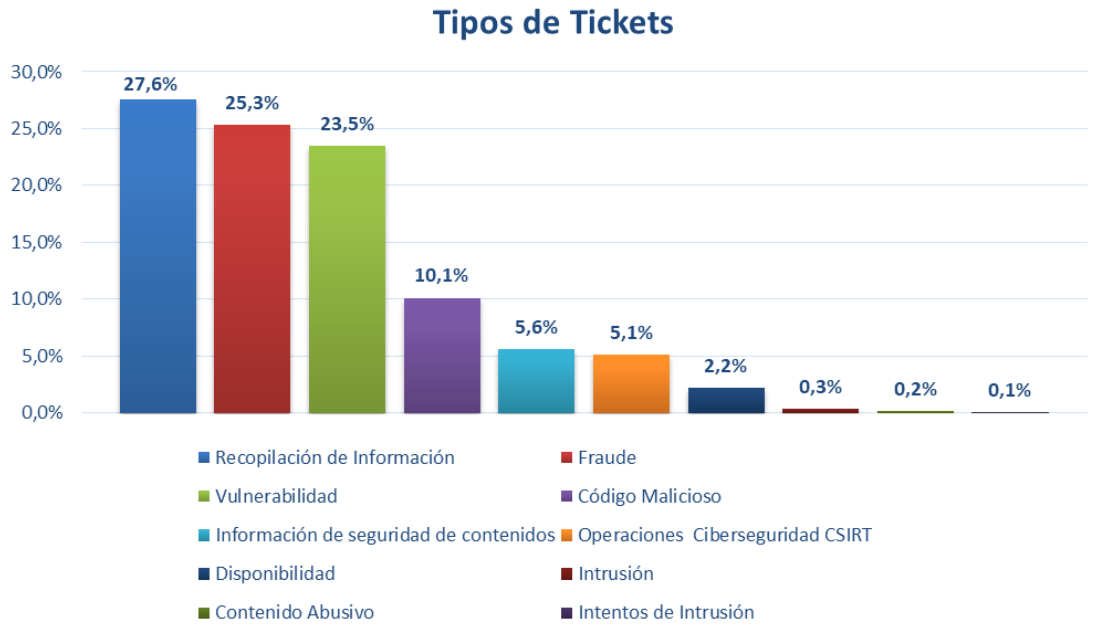


Ilustración 1 - Tipos de tickets

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 del mes anterior.

Como se aprecia en la tabla, los tickets de la categorías Fraudes, Código Malicioso, Operaciones y Disponibilidad experimentan una tendencia creciente al comparar ambos períodos, mientras que las categorías de Recopilación de información, Vulnerabilidad, Información de Seguridad de Contenidos, Contenido Abusivo e Intentos de Intrusión decrecen en el mismo espacio de comparación. La categoría Intrusión no experimentan cambios entre ambas mediciones.

Al comparar el ranking de ambos períodos se puede observar que los tipos de alertas que suben de posición corresponden a las categorías de “Recopilación de Información y Fraude”, mientras que las alertas que bajan en el ranking corresponden a las categorías de “Vulnerabilidad y Código Malicioso”.

El resto de las categorías mantienen sus posiciones en los rankings de ambos períodos.

Junio	Julio	Tendencia	Variación
1 Vulnerabilidad	1 Recopilación de Información	▼	↑
2 Recopilación de Información	2 Fraude	▲	↑
3 Código Malicioso	3 Vulnerabilidad	▼	↓
4 Fraude	4 Código Malicioso	▲	↓
5 Información de seguridad de contenidos	5 Información de seguridad de contenidos	▼	→
6 Operaciones Ciberseguridad CSIRT	6 Operaciones Ciberseguridad CSIRT	▲	→
7 Disponibilidad	7 Disponibilidad	▲	→
8 Intrusión	8 Intrusión	–	→
9 Contenido Abusivo	9 Contenido Abusivo	▼	→
10 Intentos de Intrusión	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.

Tickets	Privado	Público	Total
Vulnerabilidad	14	285	299
Recopilación de Información	0	353	353
Código Malicioso	5	124	129
Fraude	292	31	323
Información de seguridad de contenidos	5	66	71
Operaciones Ciberseguridad CSIRT	20	45	65
Disponibilidad	2	26	28
Intrusión	2	2	4
Contenido Abusivo	2	0	2
Intentos de Intrusión	0	1	1
Total	342	933	1.275

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.

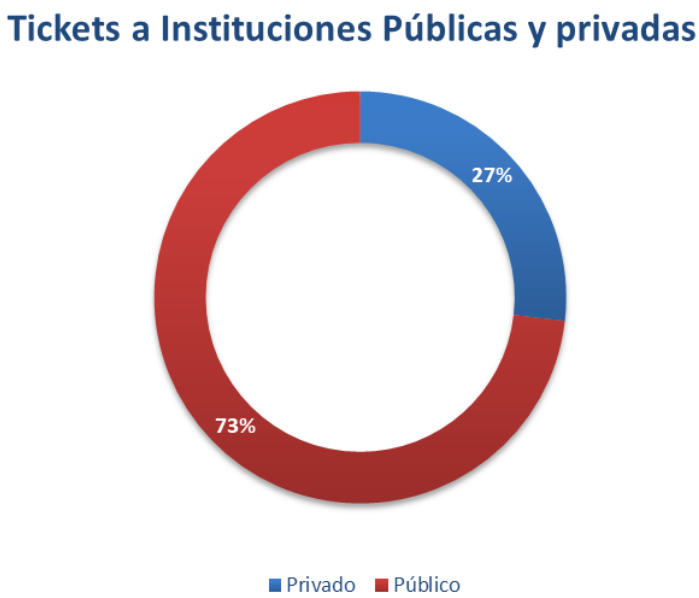


Ilustración 2 - Tickets a Instituciones Públicas y Privadas

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 2020. Como se puede apreciar la cantidad de tickets abiertos o generados en el período son un total de 1.275 unidades. De este total, 668 tickets fueron cerrados, lo que representa un 52% de eficacia, mientras que 607 tickets (48%) siguen en desarrollo para terminar de ser procesados en los períodos siguientes.

Total Estado ticket	Suma total
En desarrollo	607
Cerrados	668
Total general	**1.275**

Tabla 4 - Total Estado de Ticket

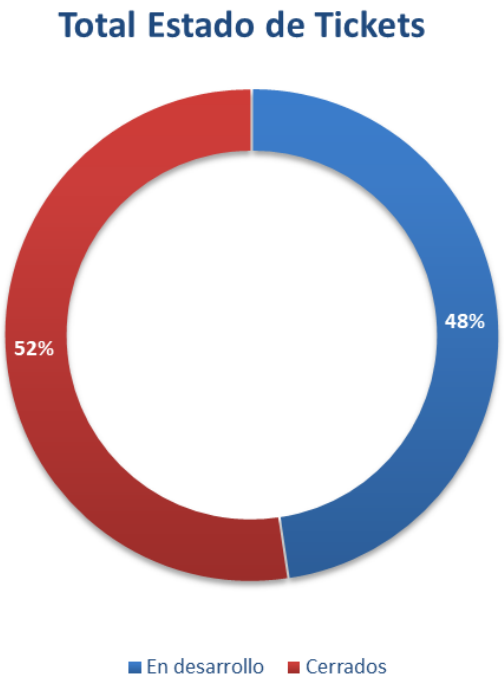


Ilustración 3 - Total Estado de Tickets

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 julio de 2020.

Como se aprecia en la tabla los tickets se pueden originar tanto internamente, 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 que tienen contrato y 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	815
Servicios Externos	460
Total Fuentes de Tickets	**1.275**

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

Como se puede observar en el siguiente gráfico, un 81% de la demanda de trabajo que recibe CSIRT en el pasado mes de julio tiene un origen interno, mientras que el 19% restante proviene de fuentes externas.

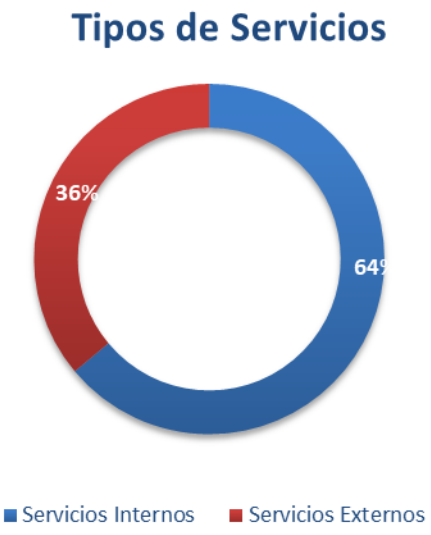


Ilustración 4 - Distribución Porcentual de Origen de Tickets

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 el pasado mes de junio.

Fuentes de Origen Externo de Tickets	Cantidad de Tickets
Tickets generados por información entregada por empresas privadas sin convenio de ciberseguridad	388
Tickets generados por información entregada por empresas privadas con convenio de ciberseguridad	0
Tickets generados por privados vía formulario web	71
Tickets generados por privados vía email	1
Tickets generados por privados vía call center	0
Tickets generados por información de otros CSIRT internacionales	0
Total	**460**

Tabla 6 - Fuentes de Origen Externo de Tickets

En julio de 2020, el siguiente gráfico de distribución muestra que el porcentaje mayor de tickets externos son generados por reportes entregados por "Empresas privadas que no prestan servicio al CSIRT", con un 84% de participación. En segundo lugar, se ubican aquellos tickets que provienen de "de privados vía formulario web" con un 15% de contribución.

Ilustración 5 - Tipos de servicios externos

8. Índice de Compromiso Detectados en el Presente Mes

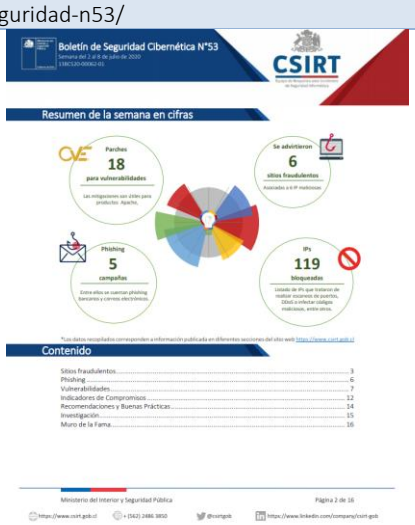
La siguiente tabla expone la cantidad de eventos en la plataforma MISP que se han detectado en el mes de julio de 2020. Los datos se muestran desde el mes de mayo de 2019 y, a partir del mes de agosto del mismo año, también se han incluido los datos de los índices que fueron detectados por CSIRT a través de su sistema de seguridad.

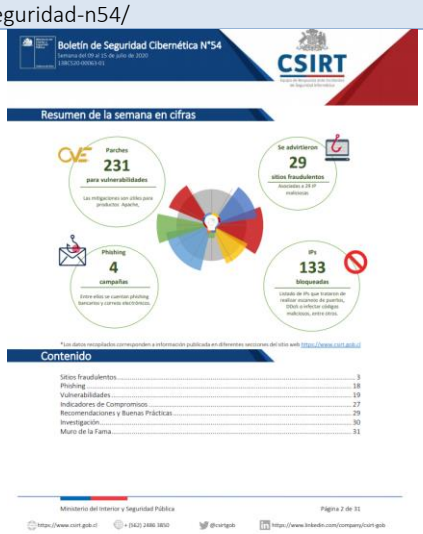
Mes correspondiente	Cantidad
Mayo	26
Junio	11
Julio	7
Agosto	277
Septiembre	791
Octubre	786
Noviembre	738
Diciembre	966
Enero	1.328
Febrero	1.138
Marzo	819
Abril	923
Mayo	727
Junio	551
Julio	492
Total	**9.580**

Tabla 7 - Índice de compromiso detectados

9. Boletines con resúmenes de alertas y vulnerabilidades del mes

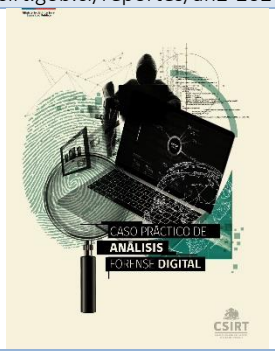
Los enlaces que se comparten a continuación, corresponden a los boletines semanales publicados durante el mes de julio que contienen el resúmenes de actividades realizadas por el CSIRT y que fueron publicadas en el sitio web www.csirt.gob.cl

Boletín de Ciberseguridad n°48	Boletín de Ciberseguridad n° 49
https://www.csirt.gob.cl/estadisticas/boletin-de-ciberseguridad-n52/	https://www.csirt.gob.cl/estadisticas/boletin-de-ciberseguridad-n53/
	

Boletín de Ciberseguridad n°50	Boletín de Ciberseguridad n° 51
https://www.csirt.gob.cl/estadisticas/boletin-de-ciberseguridad-n54/	https://www.csirt.gob.cl/estadisticas/boletin-de-ciberseguridad-n55/
	

10. Síntesis de informes y trabajos de investigación

Los enlaces que se comparten a continuación, corresponden a los informes e investigaciones publicadas por CSIRT durante el mes de julio y que están disponibles en el sitio web https://www.csirt.gob.cl/reportes/

Radiografía de las Cookies de terceros	Caso Práctico de Análisis Forense Digital
https://www.csirt.gob.cl/reportes/an2-2020-11/	https://www.csirt.gob.cl/reportes/an2-2020-12/
	

Vulnerabilidades en Cámaras IoT
https://www.csirt.gob.cl/reportes/an2-2020-13/


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

Procedimiento para denunciar suplantación de identidad en Redes Sociales	Revista Cibersucesos n°1
https://www.csirt.gob.cl/recomendaciones/procedimiento-para-denunciar-suplantacion-de-identidad-en-redes-sociales/	https://www.csirt.gob.cl/recomendaciones/revista-cibersucesos-n1/
	

Resultados Encuesta Nacional sobre el Acoso Sexual en Chile	Ciberconsejos para evitar estafas en la operación devolución de tu 10% de AFP
https://www.csirt.gob.cl/recomendaciones/resultados-encuesta-nacional-sobre-el-acoso-sexual-en-chile/	https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-evitar-estafas-en-la-operacion-devolucion-de-tu-10-de-afp/
	

Gestión de Cambios

Versión cambios	Fecha emisión	Autor cambios	Referencia, sección o capítulo modificado	Motivo de modificación
V 1.0	01/08/2020	Carlos Silva C.	Datos Iniciales.	Entrega de datos filtrados.
V 1.0	04/08/2020	Carlos Silva C.	Creación Informe.	Preparación Informe. Ajuste de formato.
V 1.0	05/08/2020	Katherina Canales	Aprobación.	Aprobación datos.
V 1.0	05/08/2020	Carlos Landeros	Aprobado	Aprobado

Tabla 8 - Gestión de cambios