Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Informe de gestión de Seguridad Cibernética

Junio 2022

Índice

1.- Introducción

En el siguiente documento resumimos la labor del Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) de Gobierno durante junio de 2022. Se compendian así los tickets que procesamos, incluyendo el detalle de los tipos de incidentes reportados y datos como el porcentaje de tickets que se reportaron al sector público y privado.

Además, este informe mensual da cuenta de las alertas sobre campañas de phishing, malware, creación de sitios fraudulentos, vulnerabilidades y ataques de fuerza bruta informados mediante los canales digitales del CSIRT de Gobierno a la ciudadanía.

Para lograr informar oportunamente y las distintas amenazas a los que están expuestas las personas, el CSIRT de Gobierno recibe la invaluable colaboración de personas e instituciones que notifican estos incidentes en cuanto los descubren. A todos ellos, les entregamos nuestros más sinceros agradecimientos. Esperamos seguir contando con su apoyo.

2.- Alcances del Informe

La información contenida en este informe proviene del proceso de notificación de incidentes de ciberseguridad del CSIRT de Gobierno, del análisis de casos, de las medidas preventivas aplicadas internamente y a terceros como parte de la misión de esta institución, y de nuestra colaboración con organismos públicos y privados. De igual forma, los datos expuestos incorporan la información pública emitida durante el mes.

El siguiente informe reúne:

- El análisis de la gestión de tickets mensual.
- La distribución de los tickets analizados durante el mes.
- El análisis de los tipos de incidentes de acuerdo con 10 variables seleccionadas.

3. Resumen mensual de tickets y tipos de incidentes reportados

Ante las diversas amenazas y peligros que abundan en el ciberespacio, el CSIRT de Gobierno notifica a instituciones públicas y privadas de aquellos riesgos que considera más probables de afectar a sus sistemas. Es así como este mes generamos **2.261 tickets**, cifra **13% menor** que la de **mayo**. Estos tickets de junio corresponden a las siguientes categorías, definidas[1] según el tipo de incidente de seguridad informática al que corresponden, y ordenadas a según su frecuencia:

N°	Tipos de ticket	Código	Total
1	Vulnerabilidad	9V00	1.863
2	Disponibilidad	6D00	175
3	Otros	11O00	78
4	Fraude	8F00	78
6	Información de seguridad de contenidos	7S00	31
5	Código Malicioso	2C00	28
7	Contenido Abusivo	1A00	6
8	Intentos de Intrusión	4I00	2
9	Intrusión	5I00	-
10	Recopilación de Información	3R00	-
Total			2.261

Imagen 1.- Distribución de tickets reportados durante el mes por tipo.

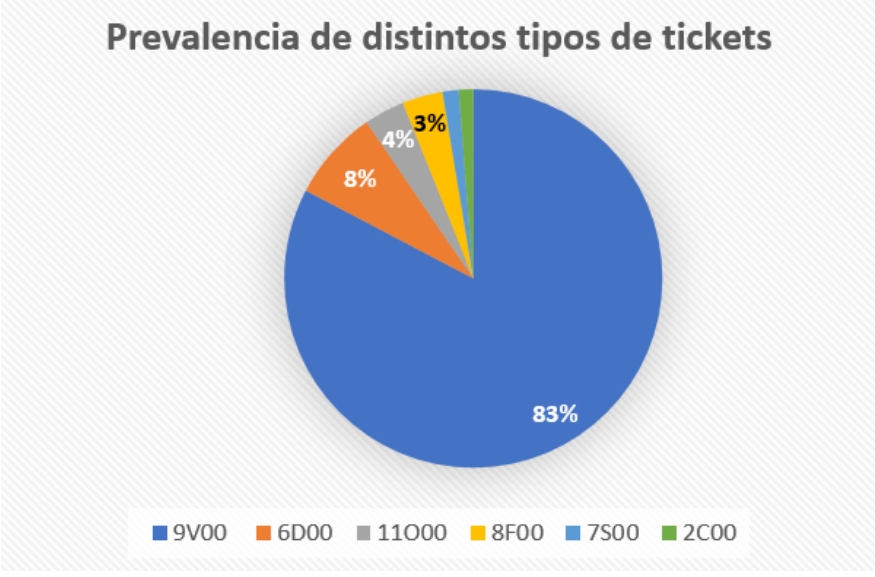


Imagen 2.- Prevalencia de tickets reportados durante el mes por tipo.

[1] Matriz de clasificación de incidentes de ENISA, Agencia de la Unión Europea para la Ciberseguridad: https://www.csirt.gob.cl/matriz-clasificacion-incidentes/

Respecto de la categoría "Vulnerabilidad" (un 83% de los tickets de junio), recordamos lo esencial de realizar las actualizaciones de nuestros programas y sistemas en cuanto están disponibles, ya que no hacerlo, en conjunto con la deficiencia de las políticas de seguridad de muchas instituciones, aumentan su exposición a ataques cibernéticos. Una fuente sobre nuevas actualizaciones a estas vulnerabilidades está en nuestra propia web: csirt.gob.cl/vulnerabilidades/.

3.1. Distribución mensual de tickets según tipo de incidente reportado

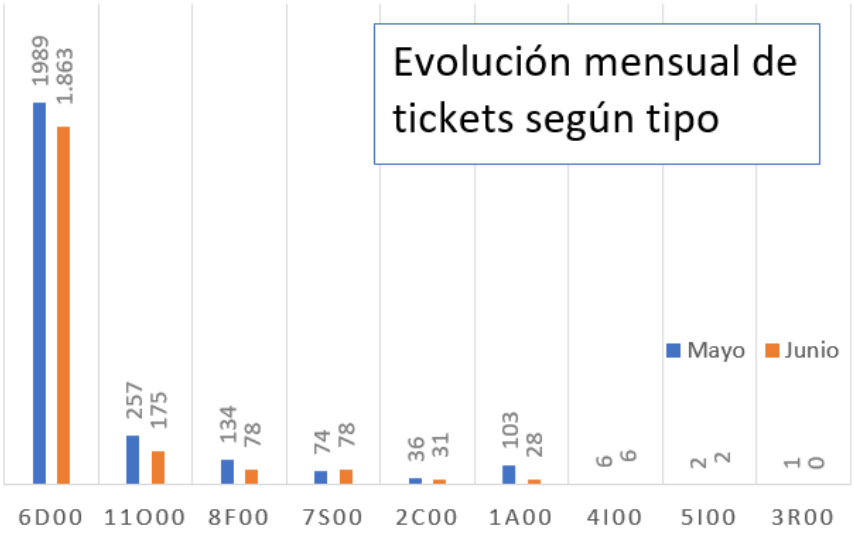


Imagen 3.- Distribución mensual de tickets por tipo.

3.2. Tickets emitidos a instituciones públicas y privadas

Nuestra vinculación con el sector privado es fundamental para contribuir a mantener un ciberespacio más seguro, además de proteger los sistemas e información de todos los chilenos. Y para lograr esa vinculación, el intercambio de información y buenas prácticas juegan un rol fundamental. Debido a lo anterior, adquirimos el compromiso de alertar de situaciones o incidentes riesgosos que se detectan en organizaciones privadas (que corresponden al **13%** de los tickets).

Tickets	Privado	Público	Total
Vulnerabilidad	113	1.750	1.863
Disponibilidad	14	161	175
Otros	64	14	78
Fraude	64	14	78
Información de seguridad de contenidos	27	4	31
Código Malicioso	21	7	28
Contenido Abusivo	1	5	6

Intentos de Intrusión	2	-	2
Intrusión	-	-	-
Recopilación de Información	-	-	-
Total	**306**	**1.955**	**2.261**

3.3. Estado de procesamiento de tickets durante junio

Este mes, el **62,7%** de los tickets generados en el período logró ser cerrada exitosamente (contra un 59% en mayo), mientras el resto seguirá siendo procesado en julio.

Total estado Ticket	Total
En desarrollo	843
Cerrados	1.418
Total general	**2.261**

3.4. Procedencia de tickets

Los tickets que procesa el CSIRT de Gobierno se pueden originar tanto interna como externamente. Aquellos de origen interno (**95% en junio**) fueron generados por sistemas propios del Ministerio del Interior y Seguridad Pública, mediante software usado por el CSIRT, que también considera los sensores que dan aviso o reportan desde otros servicios públicos y Fuerzas Armadas.

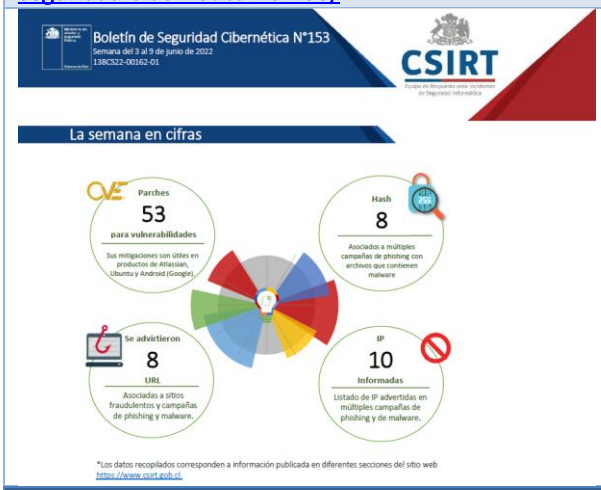
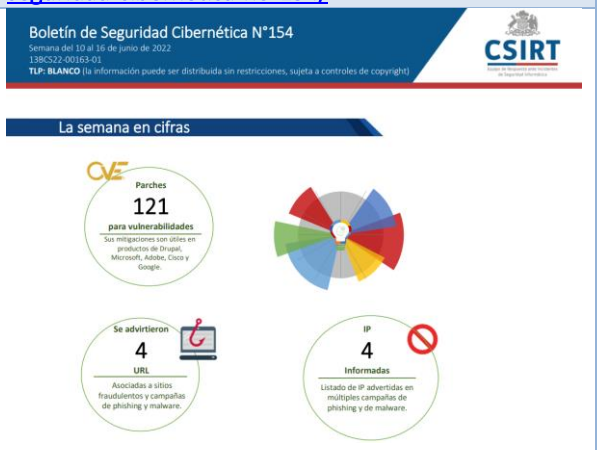
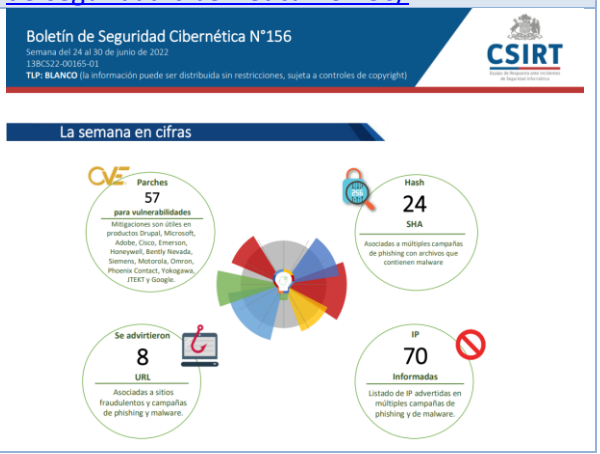
Por otro lado, los tickets de origen externo (**5%**) se originan en proveedores vinculados al CSIRT vía contractual o que se generan a través de reportes ciudadanos, via nuestro call center y por formulario web, alerta desde otros CSIRT internacionales, o por correos electrónicos de empresas privadas.

Tipo de Fuente	Cantidad de Tickets
Servicios Internos	2422
Servicios Externos	180
Total Fuentes de Tickets	**2602**

Fuentes de Origen Externo de Tickets	Cantidad de Tickets
Formulario web	85
Email	27
Call center	3
Redes sociales	0
Internacionales	0
Proveedor de servicio	0
Total	**115**

4. Boletines de Seguridad Cibernética del mes

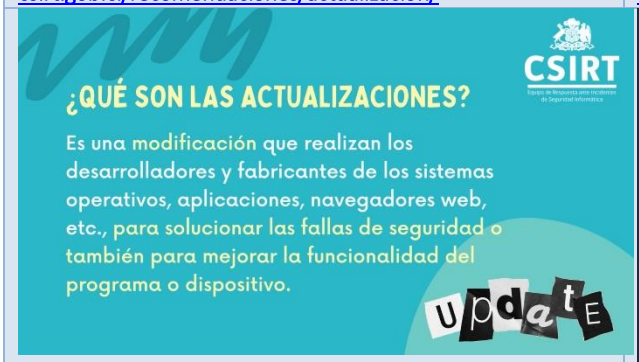
Los enlaces a continuación corresponden a los boletines semanales publicados durante junio de 2022. Cada uno resume las actividades, alertas y vulnerabilidades comunicadas por el CSIRT de Gobierno esa semana.

Boletín de Seguridad Cibernética n°153	Boletín de Seguridad Cibernética n°154
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-153/	https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-154/
	
Boletín de Seguridad Cibernética n°155	**Boletín de Seguridad Cibernética n°156**
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-155/	https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-156/
	

5. Campañas de concientización durante junio 2022

Para crear conciencia de los riesgos, amenazas y tendencias en el mundo digital, cada semana difundimos en nuestra web y las cuentas del CSIRT de Gobierno en redes sociales, campañas educativas, las que se encuentran disponibles en la sección Recomendaciones de la página web del CSIRT de Gobierno: https://www.csirt.gob.cl/recomendaciones/.

Ciberdiccionario Volumen 7	Ciberconsejos para un uso más seguro de TikTok
csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-7/	csirt.gob.cl/recomendaciones/ciberconsejos-tiktok/
	

Ciberconsejos | Control Parental	Ciberdiccionario Volumen 8
csirt.gob.cl/recomendaciones/ciberconsejos-control-parental/	csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-8/
	
¿En qué consisten las Actualizaciones de Seguridad?	**Ciberconsejos | ¿Qué capacidades debe tener nuestra organización para enfrentar un ciberataque?**
csirt.gob.cl/recomendaciones/actualizacion/	csirt.gob.cl/recomendaciones/capacidades-ciberataque/
	

Ciberconsejos | Cómo protegernos contra los stealers	Ciberdiccionario Volumen 9
csirt.gob.cl/recomendaciones/ciberconsejos-stealers/	csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-9/
	
Ciberconsejos | 5 formas de protección para una pyme cibersegura	
csirt.gob.cl/recomendaciones/pyme-cibersegura/	
	

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.07.05 11:03:59 -04'00'