Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Informe de gestión de Seguridad Cibernética

Mayo 2022

Índice

1.- Introducción 3
2.- Alcances del Informe 3
3. Resumen mensual de tickets y tipos de incidentes reportados 4
3.1. Distribución mensual de tickets según tipo de incidente reportado 5
3.2. Tickets emitidos a instituciones públicas y privadas 5
3.3. Estado de procesamiento de tickets durante mayo 6
3.4. Procedencia de tickets 6
4. Boletines de Seguridad Cibernética del mes 7
5. Campañas de concientización durante mayo 2022 8

1.- Introducción

En el siguiente documento resumimos la labor del Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) de Gobierno durante mayo 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 **2.602 tickets**, un **5% más que en abril**. Estos tickets de mayo 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 Tickets	Código	Mayo 2022
1	Vulnerabilidad	9V00	1989
2	Disponibilidad	6D00	257
3	Otros	11O00	134
4	Código Malicioso	2C00	103
5	Fraude	8F00	74
6	Información de seguridad de contenidos	7S00	36
7	Intentos de Intrusión	4I00	6
8	Intrusión	4I00	2
9	Recopilación de Información	5I00	1
10	Contenido Abusivo	1A00	0
Total			2602

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

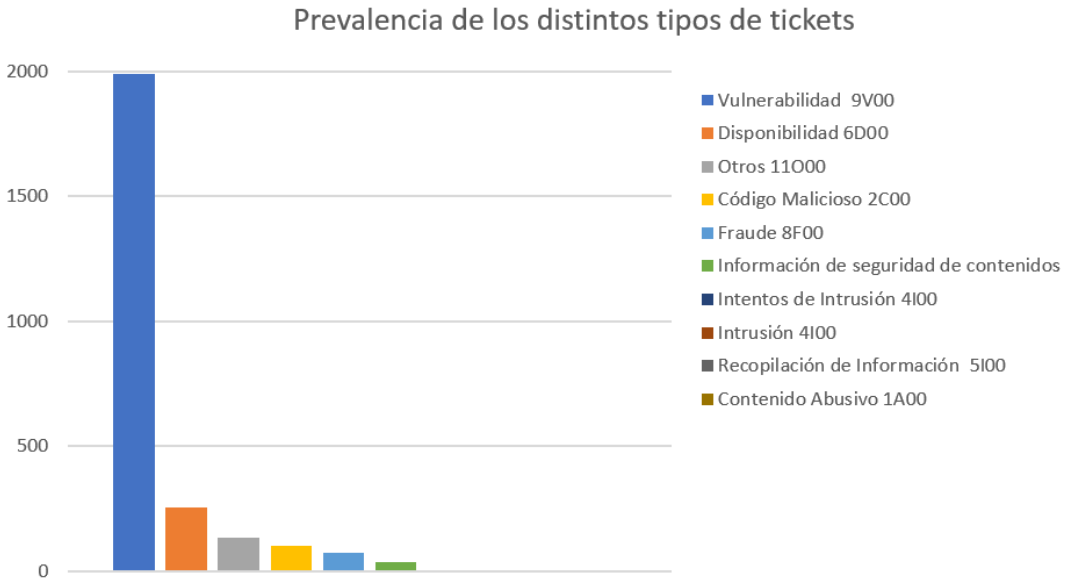


Imagen 2.- Prevalencia de tickets reportados durante el mes por tipo.

[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", 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 la ponemos disponible en nuestra propia web: https://www.csirt.gob.cl/vulnerabilidades/.

3.1. Distribución mensual de tickets según tipo de incidente reportado

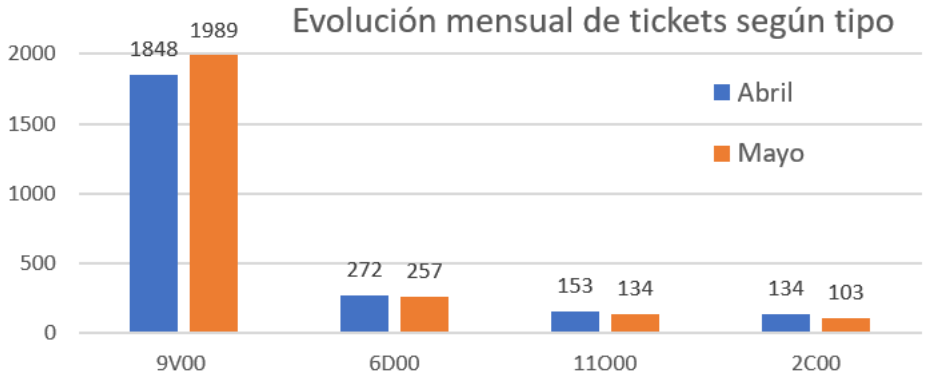


Imagen 3.- Distribución mensual de tickets por tipo.

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 **25%** de los tickets).

Tickets	Privado	Público	Total
Vulnerabilidad	199	1790	1989
Disponibilidad	20	237	257
Otros	107	27	134
Código Malicioso	88	15	103
Fraude	65	9	74
Información de seguridad de contenidos	28	8	36
Intentos de Intrusión	5	1	6
Intrusión	0	2	2
Recopilación de Información	1	0	1
Contenido Abusivo	0	0	0
Total	513	2089	2602

3.3. Estado de procesamiento de tickets durante mayo

Este mes, el **59%** de los tickets generados en el período logró ser cerrada exitosamente (contra un 51% en abril), mientras el resto seguirá siendo procesado en junio.

Total estado Ticket	Total
En desarrollo	1081
Cerrados	1521
Total general	**2602**

3.4. Procedencia de tickets

Los tickets que procesa el CSIRT de Gobierno se pueden originar tanto interna como externamente. Aquellos de origen interno (**93,1% en mayo**) fueron generados por sistemas propios del Ministerio del Interior y Seguridad Pública, mediante software utilizado por el CSIRT, que también considera los sensores que dan aviso o reportan desde otros servicios públicos y las Fuerzas Armadas.

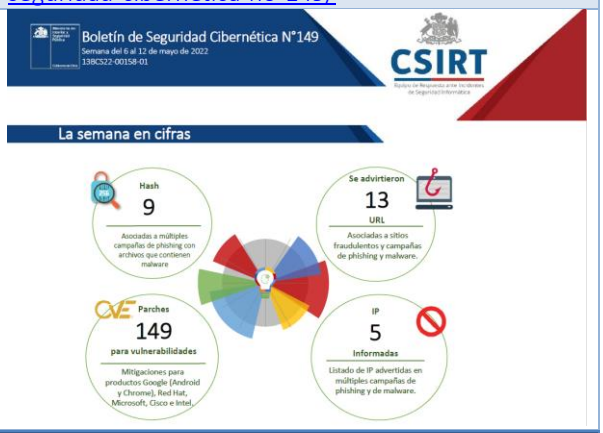
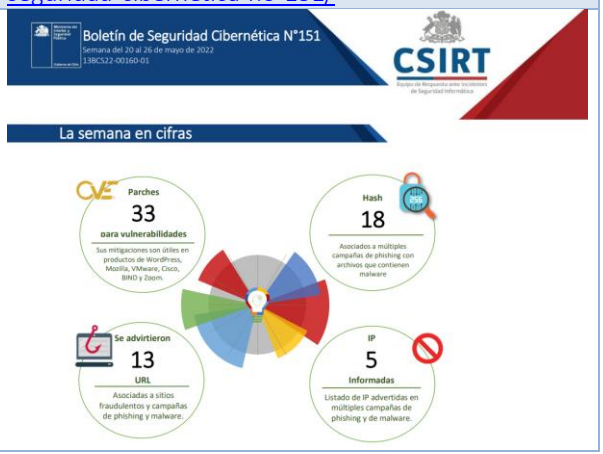
Por otro lado, los tickets de origen externo (**6,9%**) se originan en proveedores vinculados al CSIRT vía contractual o que se generan a través de reportes ciudadanos, via nuestro call center y por formulario web, alerta desde otros CSIRT internacionales, o por correos electrónicos de empresas privadas.

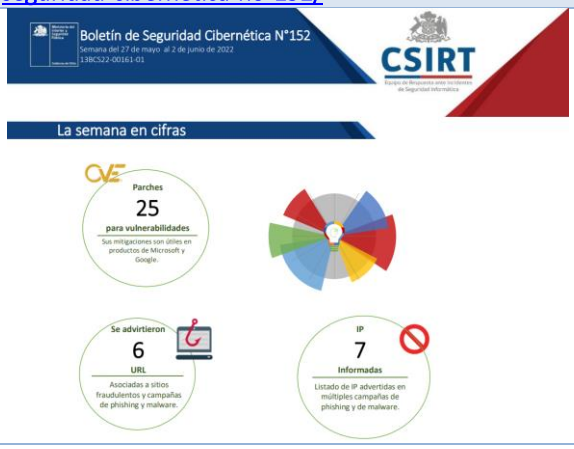
Tipo de Fuente	Cantidad de Tickets
Servicios Internos	2422
Servicios Externos	180
Total Fuentes de Tickets	**2602**

Fuentes de Origen Externo de Tickets	Cantidad de Tickets
Formulario web	127
Call center	6
Redes sociales	1
Internacionales	0
Proveedor de servicio	0
Email	46
Total	**180**

4. Boletines de Seguridad Cibernética del mes

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

Boletín de Seguridad Cibernética n°148	Boletín de Seguridad Cibernética n°149
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-148/	https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-149/
	
Boletín de Seguridad Cibernética n°150	**Boletín de Seguridad Cibernética n°151**
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-150/	https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-151/
	

Boletín de Seguridad Cibernética n°143	
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-152/	
	

5. Campañas de concientización durante mayo 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/.

Ciberconsejos | Browser In The Browser (BITB), técnica que dificulta identificar un phishing	Decálogo de Ciberseguridad
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-bitb/	https://www.csirt.gob.cl/recomendaciones/decalogo-de-ciberseguridad/
	

Ciberdiccionario Vol. IV	Ciberconsejos | ¿Cómo prevenir la escalabilidad de privilegios?
https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-4/	https://www.csirt.gob.cl/recomendaciones/ciberconsejos-escalabilidad-de-privilegios/

Ciberdiccionario Vol. V	Día Mundial de Internet: Hitos de la llegada de internet a Chile
https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-5/	https://www.csirt.gob.cl/recomendaciones/dia-mundial-de-internet/

Ciberdiccionario Vol. VI	Ciberconsejos: Vulnerabilidades informáticas
https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-6/	https://www.csirt.gob.cl/recomendaciones/ciberconsejos-vulnerabilidades/
	
Subsecretaría del Interior y Cámara de Comercio de Santiago coordinan medidas de seguridad para primer CyberDay de 2022	
https://www.csirt.gob.cl/recomendaciones/consejos-cyberday-2022/	
	

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.06.08 19:17:39 -04'00'