



Informe de gestión de Seguridad Cibernética

Junio 2022



011011
100010

1	00001	0
	00 10 1	0
	10100	1
	000 0	
	11010 1	

```

1 1
2 1
3 1
4 1
5 1
6 1
7 1
8 1
9 1
10 1
11 1
12 1
13 1
14 1
15 1
16 1
17 1
18 1
19 1
20 1
21 1
22 1
23 1
24 1
25 1
26 1
27 1
28 1
29 1
30 1
31 1
32 1
33 1
34 1
35 1
36 1
37 1
38 1
39 1
40 1
41 1
42 1
43 1
44 1
45 1
46 1
47 1
48 1
49 1
50 1
51 1
52 1
53 1
54 1
55 1
56 1
57 1
58 1
59 1
60 1
61 1
62 1
63 1
64 1
65 1
66 1
67 1
68 1
69 1
70 1
71 1
72 1
73 1
74 1
75 1
76 1
77 1
78 1
79 1
80 1
81 1
82 1
83 1
84 1
85 1
86 1
87 1
88 1
89 1
90 1
91 1
92 1
93 1
94 1
95 1
96 1
97 1
98 1
99 1
100 1

```





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 junio	6
3.4. Procedencia de tickets.....	6
4. Boletines de Seguridad Cibernética del mes	7
5. Campañas de concientización durante junio 2022	8



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, definidas¹ 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.

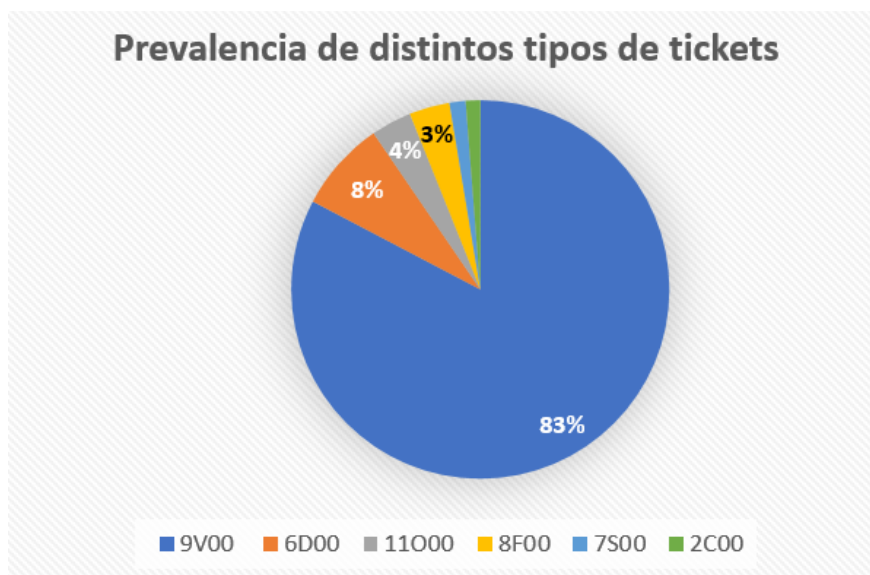


Imagen 2.- Prevalencia de tickets reportados durante el mes por tipo.

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

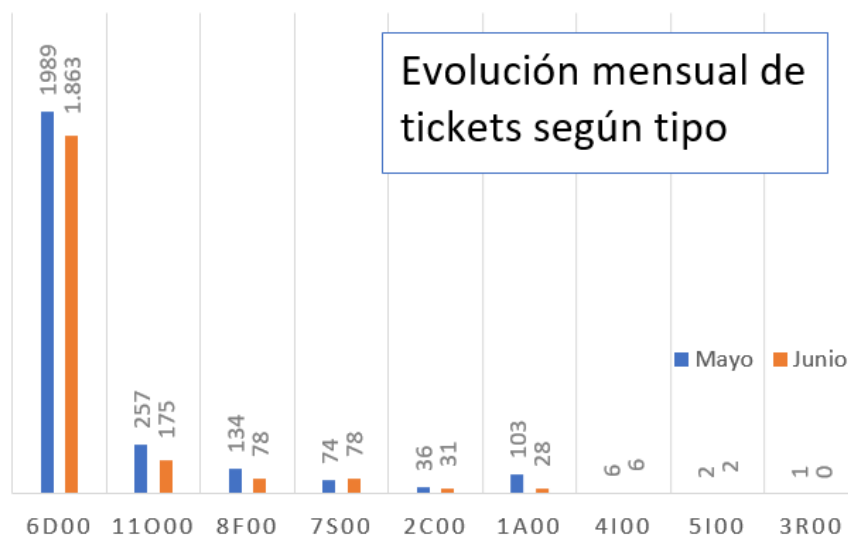


Imagen 3.- Distribución mensual de tickets por tipo.

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 https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-153/	Boletín de Seguridad Cibernética n°154 https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-154/
 <p>Boletín de Seguridad Cibernética N°153 Semana del 3 al 9 de junio de 2022 138CS22-00165-01</p> <p>La semana en cifras</p> <ul style="list-style-type: none"> 53 Parches para vulnerabilidades Sus mitigaciones son útiles en productos de Atlasian, Ubuntu y Android (Google). 8 Hash Asociados a múltiples campañas de phishing con archivos que contienen malware. 8 Se advirtieron URL Asociadas a sitios fraudulentos y campañas de phishing y malware. 10 IP Informadas Listado de IP advertidas en múltiples campañas de phishing y de malware. <p><small>*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web https://www.csirt.gob.cl</small></p>	 <p>Boletín de Seguridad Cibernética N°154 Semana del 10 al 16 de junio de 2022 138CS22-00165-01 TLP: BLANCO (la información puede ser distribuida sin restricciones, sujeta a controles de copyright)</p> <p>La semana en cifras</p> <ul style="list-style-type: none"> 121 Parches para vulnerabilidades Sus mitigaciones son útiles en productos de Drupal, Microsoft, Adobe, Cisco y Google. 4 Se advirtieron URL Asociadas a sitios fraudulentos y campañas de phishing y malware. 4 IP Informadas Listado de IP advertidas en múltiples campañas de phishing y de malware.
Boletín de Seguridad Cibernética n°155 https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-155/	Boletín de Seguridad Cibernética n°156 https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-156/
 <p>Boletín de Seguridad Cibernética N°155 Semana del 17 al 23 de junio de 2022 138CS22-00164-01 TLP: BLANCO (la información puede ser distribuida sin restricciones, sujeta a controles de copyright)</p> <p>La semana en cifras</p> <ul style="list-style-type: none"> 44 Parches para vulnerabilidades Sus mitigaciones son útiles en productos de Zimbra, Citrix, Siemens, Splunk, Cisco, SAP y Google. 14 Hash Asociados a múltiples campañas de phishing con archivos que contienen malware. 21 Se advirtieron URL Asociadas a sitios fraudulentos y campañas de phishing y malware. 7 IP Informadas Listado de IP advertidas en múltiples campañas de phishing y de malware. 	 <p>Boletín de Seguridad Cibernética N°156 Semana del 24 al 30 de junio de 2022 138CS22-00165-01 TLP: BLANCO (la información puede ser distribuida sin restricciones, sujeta a controles de copyright)</p> <p>La semana en cifras</p> <ul style="list-style-type: none"> 57 Parches para vulnerabilidades Mitigaciones son útiles en productos Drupal, Microsoft, Adobe, Cisco, Emerson, Honeywell, Bendly Nevada, Siemens, Motorola, Dvtron, Phoenix Contact, Telego, ITXT y Google. 24 Hash SHA Asociados a múltiples campañas de phishing con archivos que contienen malware. 8 Se advirtieron URL Asociadas a sitios fraudulentos y campañas de phishing y malware. 70 IP Informadas Listado de IP advertidas en múltiples campañas de phishing y de malware.



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 csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-7/	Ciberconsejos para un uso más seguro de TikTok csirt.gob.cl/recomendaciones/ciberconsejos-tiktok/
 <p>CSIRT Ciberdiccionario Equipo de Respuesta ante Incidentes de Seguridad Informática</p> <p>Análisis forense: Investigación hecha por profesionales de ciberseguridad durante o después de un ciberataque o incidente, con tal de saber qué ocurrió, si los sistemas siguen infectados, y evitar que un ataque vuelva a tener éxito. Es importante conservar las evidencias de posibles delitos de cara a su persecución legal.</p>	 <p>CSIRT CIBERCONSEJOS PARA USAR DE FORMA SEGURA TIKTOK Equipo de Respuesta ante Incidentes de Seguridad Informática</p> <p>Riesgos de TikTok</p> <ul style="list-style-type: none">● Sobre exposición de la imagen del menor o de información familiar● Contenido inapropiado● Grooming: Acoso y abuso sexual en línea● Ciberacoso● Retos virales peligrosos● Accede a los datos para funcionar como contactos, localización, micrófono y cámara.



<p>Ciberconsejos Control Parental csirt.gob.cl/recomendaciones/ciberconsejos-control-parental/</p> <p>#ciberconsejos</p> <p>Herramientas de Control Parental</p> <p>Son apps y configuraciones que permiten a los padres:</p> <ul style="list-style-type: none"> • Administrar, filtrar o restringir el acceso a sitios o contenido en Internet de niños, niñas y adolescentes (NNA). • Llevar un registro de las actividades que realizan en dispositivos y plataformas de juegos o de streaming. 	<p>Ciberdiccionario Volumen 8 csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-8/</p> <p>Ciberdiccionario</p> <p>Credenciales: Elementos que emplea el usuario para ingresar a un sistema o sitio web que exige identificación. Usualmente se refiere a usuario y contraseña, comprende otras claves, tokens o combinaciones de autenticación si las hubiera.</p> 
<p>¿En qué consisten las Actualizaciones de Seguridad?</p> <p>csirt.gob.cl/recomendaciones/actualizacion/</p>	<p>Ciberconsejos ¿Qué capacidades debe tener nuestra organización para enfrentar un ciberataque?</p> <p>csirt.gob.cl/recomendaciones/capacidades-ciberataque/</p>
<p>¿QUÉ SON LAS ACTUALIZACIONES?</p> <p>Es una modificación que realizan los desarrolladores y fabricantes de los sistemas operativos, aplicaciones, navegadores web, etc., para solucionar las fallas de seguridad o también para mejorar la funcionalidad del programa o dispositivo.</p> 	<p>SI ENFRENTA UN CIBERATAQUE, SU EQUIPO DEBE TENER LAS SIGUIENTES CAPACIDADES</p> 



<p>Ciberconsejos Cómo protegernos contra los stealers</p>	<p>Ciberdiccionario Volumen 9</p>
<p>csirt.gob.cl/recomendaciones/ciberconsejos-stealers/</p>	<p>csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-9/</p>
 <p>#ciberconsejos</p> <p>STEALERS</p> <p>¿Cómo se propagan?</p> <ul style="list-style-type: none"> •Phishing (falsos enlaces que parecen inofensivos) •Archivos Word, Excel, PDF, RAR o ZIP, adjuntos en email. •Enlaces en la descripción de videos de YouTube •Falsos sitios de descarga de software. 	 <p>Ciberdiccionario</p> <p>Día cero (Zero day): Vulnerabilidades recién oficialmente divulgadas por los responsables del software o entidades de seguridad, siendo hasta entonces solo conocidas por actores maliciosos. Son muy peligrosas porque en un principio no se cuenta con parches para contrarrestarlas.</p>
<p>Ciberconsejos 5 formas de protección para una pyme cibersegura</p>	
<p>csirt.gob.cl/recomendaciones/pyme-cibersegura/</p>	
 <p>5 FORMAS DE PROTECCIÓN PARA UNA PYME CIBERSEGURA</p> <p>Para disminuir la probabilidad de que una pyme sea víctima de un ciberataque, entregamos cinco formas básicas de protección:</p> <p>1. ANTIMALWARE/ANTIVIRUS Y FIREWALL</p> <p>Para tener una infraestructura tecnológica más segura, se recomienda implementar un antivirus y un firewall regularmente actualizados. Sin embargo, de ninguna manera son suficientes para proteger completamente tu pyme.</p>	