Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Informe de gestión de Seguridad Cibernética

Febrero 2022

Índice

1.- Introducción

A continuación se resume la labor del Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) de Gobierno durante febrero 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 2022.

El contenido del siguiente informe reúne:

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

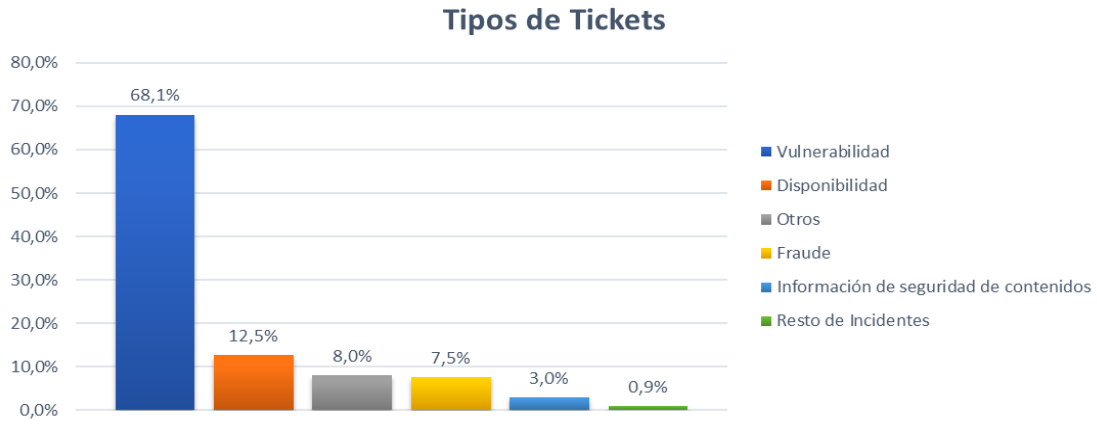
3. Resumen mensual de tickets y tipos de incidentes reportados

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 en febrero generamos 1.509 tickets, los que corresponden a distintas categorías definidas[1] según el tipo de incidente de seguridad informática al que corresponden, y ordenadas a continuación según su frecuencia:

N°	Tipos de Tickets	Código	Febrero 2022
1	Vulnerabilidad	9V00	1027
2	Disponibilidad	6D00	191
3	Otros	11O00	120
4	Fraude	8F00	113
5	Información de seguridad de contenidos	7S00	45
6	Código Malicioso	2C00	10
7	Intentos de Intrusión	4I00	2
8	Contenido Abusivo	1A00	1
9	Intrusión	5I00	0
10	Recopilación de Información	3R00	0
Total			1509

Imagen 1.- Distribución de tickets reportados durante febrero por tipo.

Respecto de la categoría “Vulnerabilidad”, recordamos lo esencial de realizar las actualizaciones de nuestros programas 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.



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

3.1. Distribución mensual de tickets según tipo de incidente reportado

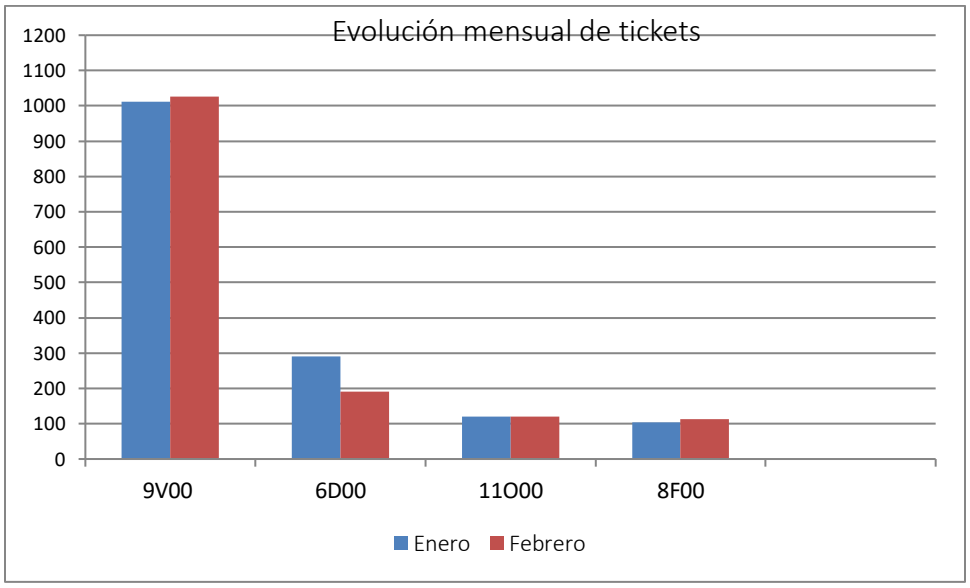


Imagen 2.- Distribución mensual de tickets por tipo.

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 también alertar de situaciones o incidentes riesgosos que se detectan en organizaciones privadas. Es así como de 19% tickets totales corresponde al sector privado.

Tickets	Privado	Público	Total
Vulnerabilidad	54	973	1027
Disponibilidad	13	178	191
Otros	86	34	120
Fraude	80	33	113
Información de seguridad de contenidos	38	7	45
Código malicioso	10	0	10
Intentos de intrusión	0	2	2
Contenido abusivo	0	1	1

Intrusión	0	0	0
Recopilación de Información	0	0	0
Total	**281**	**1228**	**1509**

3.3. Estado de procesamiento de tickets durante enero

En febrero, el 52% de los tickets generados en el período logró ser cerrada exitosamente, mientras el resto seguirá siendo procesado en febrero.

Total estado Ticket	Total
En desarrollo	711
Cerrados	786
Total general	**1509**

3.4. Procedencia de tickets

Los tickets que procesa el CSIRT de Gobierno se pueden originar tanto interna como externamente. Aquellos de origen interno (89% en febrero) 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 (11%) provienen de proveedores vinculados al CSIRT vía contractual o que se generan a través de reportes ciudadanos a través 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	1339
Servicios Externos	170
Total Fuentes de Tickets	**1509**

4. Boletines de Seguridad Cibernética del mes

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

Boletín de Seguridad Cibernética n°135	Boletín de Seguridad Cibernética n°136
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n135/	https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n136/
	
Boletín de Seguridad Cibernética n°137	**Boletín de Seguridad Cibernética n°138**
https://www.csirt.gob.cl/media/2022/02/13BCS22-000146-01.pdf	https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n134
	

5. Campañas de concientización durante febrero 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 para proteger tus dispositivos IoT	Ciberconsejos para una navegación segura
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-proteger-dispositivos-iot/	https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-una-navegacion-segura/
	

Ciberconsejos para un teletrabajo más seguro	Cómo lograr una mejor Convivencia Digital para nuestros niños
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-un-teletrabajo-mas-seguro/	https://www.csirt.gob.cl/recomendaciones/ciberconsejos-convivencia-digital/
	
Ciberconsejos para lograr comunidades educativas más seguras	
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-comunidades-educativas/	
	

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.03.24 10:54:31 -03'00'