

INFORME DE GESTIÓN MENSUAL AGOSTO 2022



ACERCA DE ESTE INFORME

En el siguiente documento resumimos la labor del Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) de Gobierno, dependiente del Ministerio del Interior y Seguridad Pública.

Es la gestión realizada durante agosto de 2022, que comprende 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.

TIPO DE INCIDENTE

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 **2.474** tickets, un **17,4% más** que en julio. Estos tickets de agosto corresponden a las siguientes categorías, definidas según el tipo de incidente de seguridad informática al que corresponden, y ordenadas según su frecuencia.



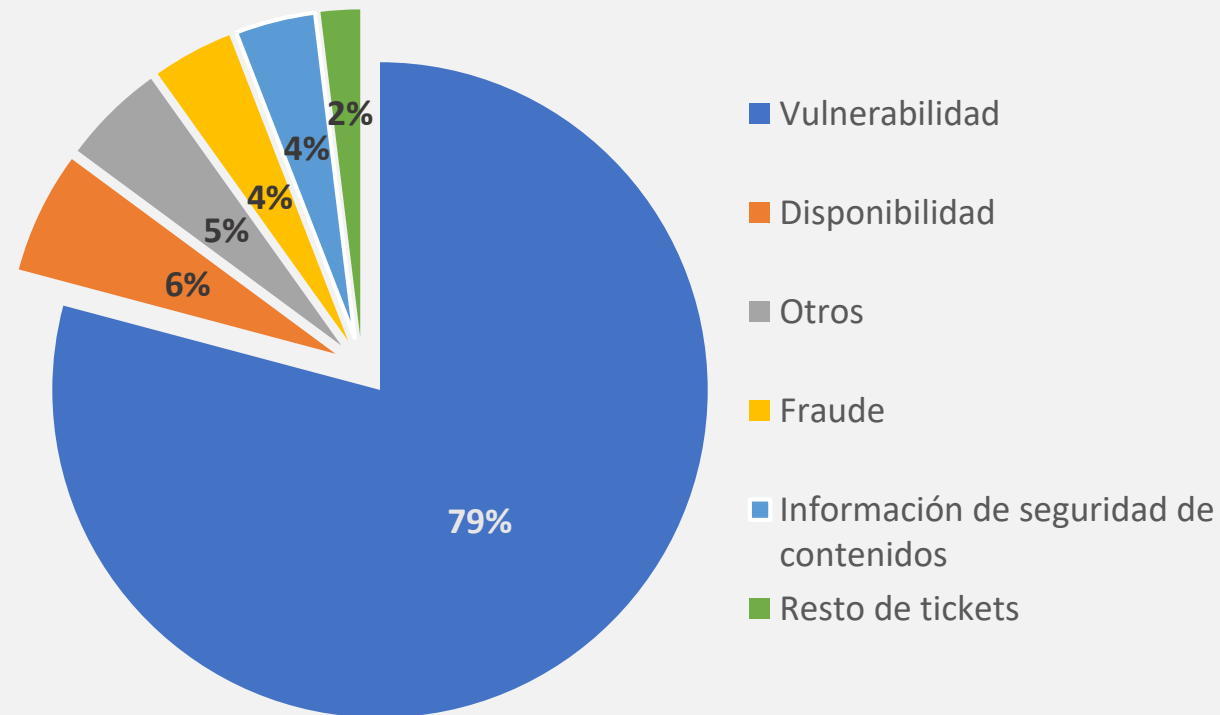
Estos tickets los ordenamos en categorías definidas por ENISA (Agencia de Ciberseguridad de la Unión Europea) según el tipo de incidente de seguridad informática al que corresponden.

Más información sobre esta clasificación:
<https://www.csirt.gob.cl/matriz-clasificacion-incidentes>

TIPO DE INCIDENTE

La enorme mayoría de los incidentes corresponde a la categoría **Vulnerabilidad**

El CSIRT de Gobierno reitera su llamado a actualizar cuánto antes sea posible sus software, ya que así se parchan dichas vulnerabilidades, que corresponden a deficiencias de seguridad, las que pueden ser explotadas por ciberdelincuentes.



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.

Tickets	Privado	Público	Total
Vulnerabilidad	164	1794	1958
Disponibilidad	4	144	148
Otros	109	15	124
Fraude	91	7	98
Información de seguridad de contenidos	91	7	98
Código Malicioso	18	27	45
Contenido Abusivo	0	2	2
Intentos de Intrusión	0	1	1
Intrusión	0	0	0
Recopilación de Información	0	0	0
Total	477	1.997	2.474

Públicas

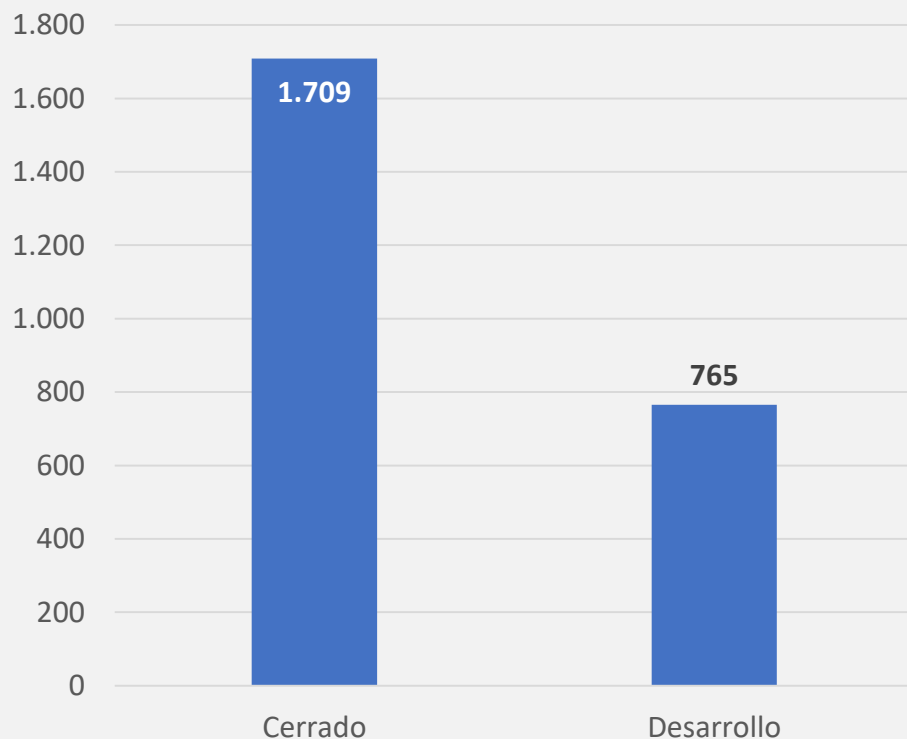
80%

Privadas

20%

PROCESAMIENTO DE TICKETS

Este mes, el 69% de los tickets generados en el período logró ser cerrada exitosamente (contra un 54,8% en julio), mientras el resto seguirá siendo procesado en agosto.



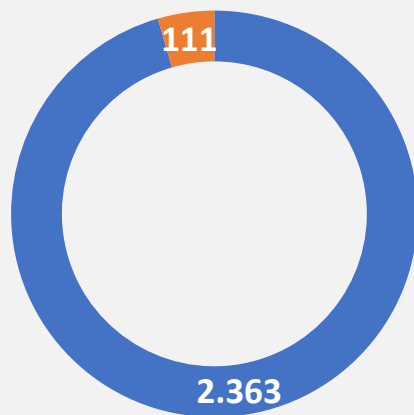
Recordamos lo esencial de obtener retroalimentación de las gestiones que se realizan en función del hallazgo encontrado.

Los invitamos a seguir cerrando brechas de seguridad para tener un Estado más ciberseguro

<https://www.csirt.gob.cl>

PROCEDENCIA DE TICKETS

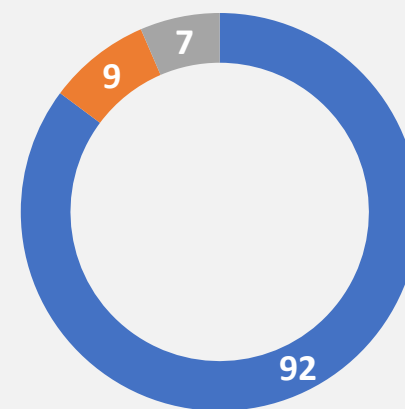
Los tickets que procesa el CSIRT de Gobierno se pueden originar tanto interna como externamente. Aquellos de origen interno que corresponde al **95,5%**, fueron generados por sistemas propios del Ministerio del Interior y Seguridad Pública, mediante software utilizado por el CSIRT.



■ Servicio Interno ■ Servicio Externo

Fono
CSIRT:
1510

Por otro lado, los tickets de origen externo (un **4,5%**), se originan por colaboradores vinculados al CSIRT vía contractual o se generan a través de reportes ciudadanos a través nuestro call center y por formulario web (85% de tickets externos), alerta desde otros CSIRT internacionales, o por correos electrónicos de empresas privadas.



■ Formulario web ■ Email ■ Call center

BOLETINES DE SEGURIDAD CIBERNÉTICA, AGOSTO 2022

Aquí pueden revisar los boletines que comparte el CSIRT de Gobierno cada semana, con las principales alertas, vulnerabilidades y campañas que realizamos en el período.

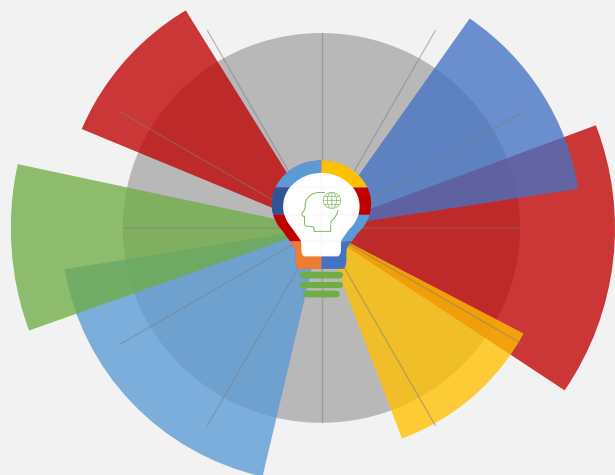
Boletín de Seguridad Cibernética n°161 – 29 de julio al 4 de agosto: <https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-161>

Boletín de Seguridad Cibernética n°162 – 5 al 11 de agosto: <https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-162>

Boletín de Seguridad Cibernética n°163 – 12 al 18 de agosto: <https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-163>

Boletín de Seguridad Cibernética n°164 – 19 al 25 de agosto: <https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-164>

Boletín de Seguridad Cibernética n°165 – 26 de agosto al 1 de sept.: <https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-165>



Indicadores	Boletín 161	Boletín 162	Boletín 163	Boletín 164	Boletín 165
CVE	47	152	21	4	22
IP	1	12	4	8	0
Hash	0	23	20	21	12
URL	5	15	8	12	0

CAMPAÑAS DE CONCIENTIZACION

Cuídate de las fake news con los
consejos del CSIRT de Gobierno

<https://www.csirt.gob.cl/recomendaciones/fake-news-2022/>

Ciberguía | Mediación Parental

<https://www.csirt.gob.cl/recomendaciones/ciberguia-mediacion-parental/>

Ciberdiccionario Volumen 13

<https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-13/>

Ministerio del Interior y
Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes
de Seguridad Informática

**CIBERCONSEJOS DE SEGURIDAD
PARA EVITAR FAKE NEWS**
En tiempo de elecciones

**¿QUÉ SON LAS
FAKE NEWS?**

Literalmente "noticias falsas",
son una forma de desinformación,
hechos o datos falsos que son
difundidos como verdaderos con
la intención de engañar a la
población. En tiempos de elecciones
se multiplican, buscando
influir en la intención de voto de
las personas con mentiras.

**Ciberguía de
Mediación Parental
2022**

18+

Consejos de **uso responsable**
de internet para la familia

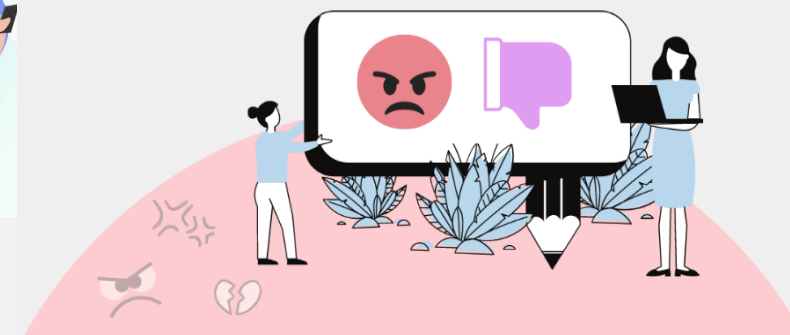
CSIRT
Equipo de Respuesta ante Incidentes
de Seguridad Informática



Ciber diccionario

1.HATER:

Personas que esparcen comentarios y comportamientos negativos y de odio por redes sociales hacia todo aquello que detestan.



CAMPAÑAS DE CONCIENTIZACION

Juegos conectados | ¿Qué son y cómo jugar seguros?

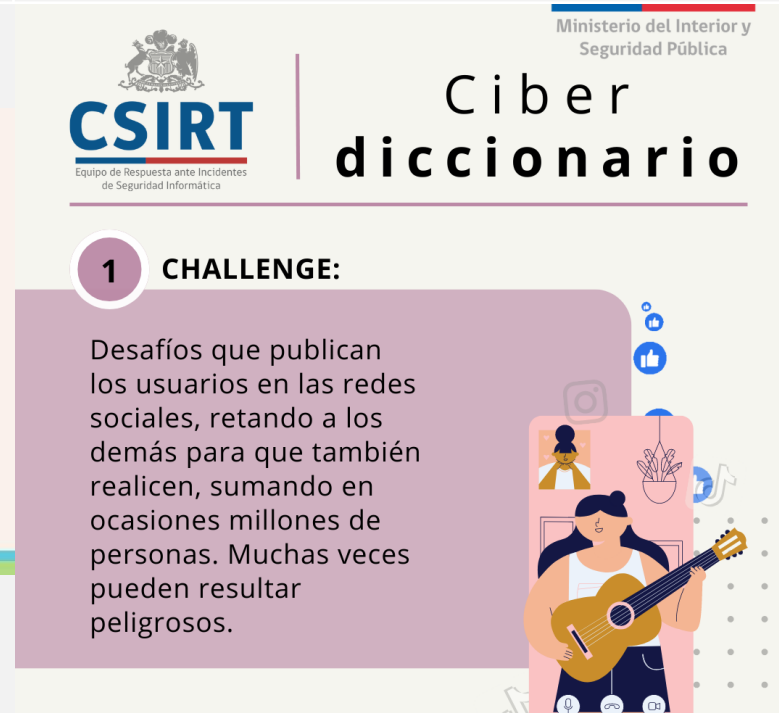
www.csirt.gob.cl/recomendaciones/juegos-conectados-que-son-y-como-jugar-seguros/

Ciberguía familiar | Hábitos para navegar Internet

www.csirt.gob.cl/recomendaciones/ciberguia-familiar-habitos-para-navegar-internet/

Ciberdiccionario Volumen 14

<https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-14/>



CAMPAÑAS DE CONCIENTIZACION

Ciberdiccionario Volumen 15

<https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-15/>

Ciberconsejos en el Día Mundial del Gamer

www.csirt.gob.cl/recomendaciones/ciberconsejos-en-el-dia-mundial-del-gamer/

Ciberconsejos para descargar apps seguras

www.csirt.gob.cl/recomendaciones/ciberconsejos-para-descargar-apps-seguras/



Ciberdiccionario

Honeypot: En ciberseguridad, es un activo diseñado para atraer ataques y así poder analizar el accionar de los ciberdelincuentes y conocer las debilidades de nuestros sistemas. Su nombre viene del atractivo que representa un frasco con miel para todo tipo de insectos y animales.



Ciberconsejos en el Día Mundial del Gamer

¿Qué es un gamer?

Persona que se dedica a los videojuegos varias horas a la semana, juega con destreza o participan de torneos, muchas veces compartiendo su pasión en plataformas de streaming. A veces el término se limita solo a quienes juegan de forma profesional.



Ciberconsejos para descargar apps seguras

¿Y qué pasa con las app del Gobierno?

Solo se descargan de las tiendas oficiales. ¡Evita caer en estafas!



CAMPAÑAS DE CONCIENTIZACION

Ciberdiccionario Volumen 16

<https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-16/>

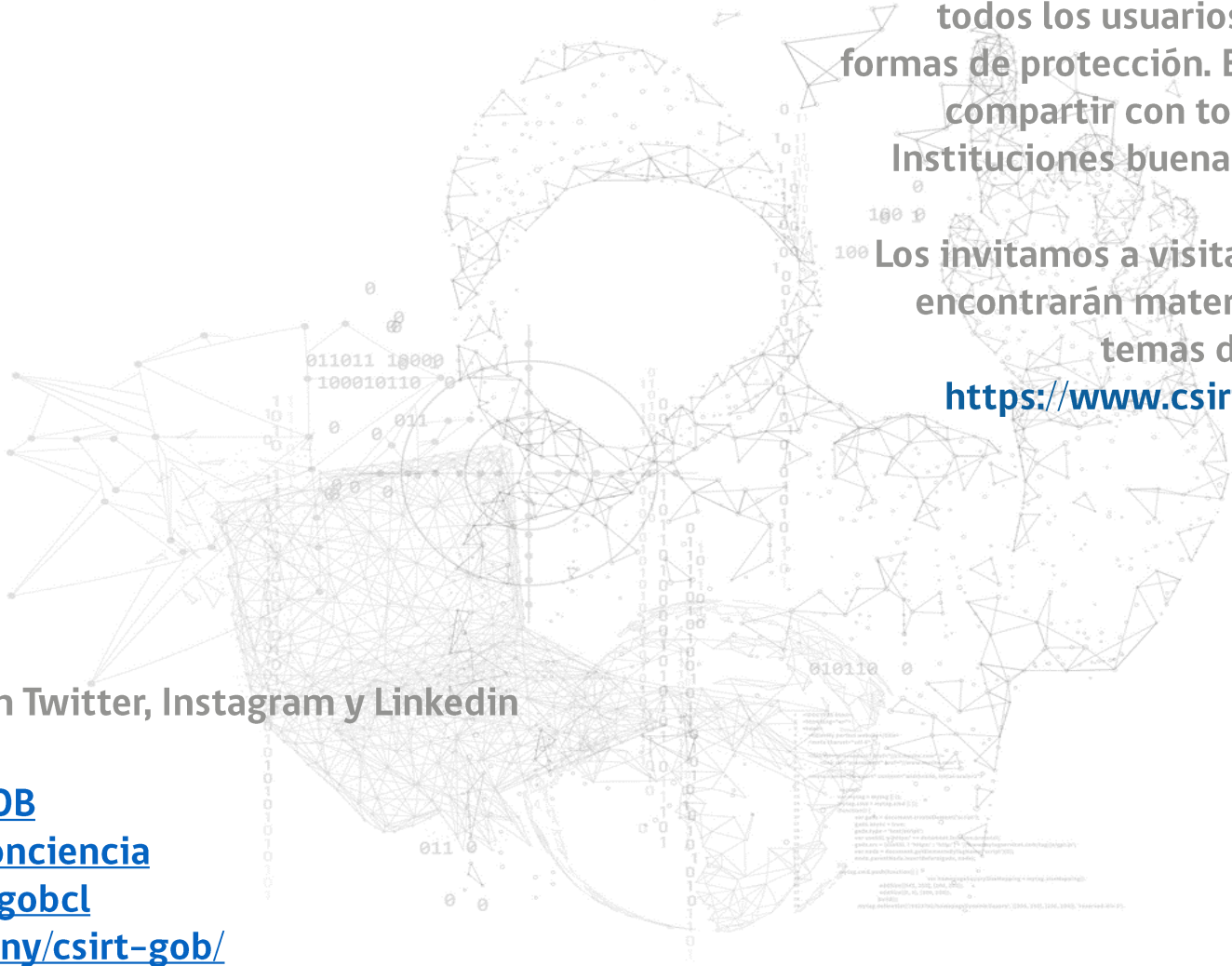


Ciber diccionario

Máquina virtual (virtual machine o VM):

Recurso que se comporta como un computador tradicional, pero no cuenta con su propio hardware, existiendo solo como código. Así, se pueden tener varias VM (llamadas "guests") en una misma máquina física (o "host"), usando, por ejemplo, distintos sistemas operativos.





Para prevenir una amenaza, es fundamental que todos los usuarios conozcan los riesgos y las formas de protección. El CSIRT de Gobierno recomienda compartir con todos los trabajadores de las Instituciones buenas prácticas de ciberseguridad.

Los invitamos a visitar el sitio web del CSIRT, donde encontrarán material educativo sobre diversos temas de ciberseguridad.

<https://www.csirt.gob.cl/recomendaciones/>

Síguenos también en Twitter, Instagram y LinkedIn

twitter.com/CSIRTOGOB

twitter.com/CSIRTConciencia

instagram.com/csirtgobcl

linkedin.com/company/csirt-gob/