

INFORME DE GESTIÓN MENSUAL NOVIEMBRE 2022



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

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 **noviembre** 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

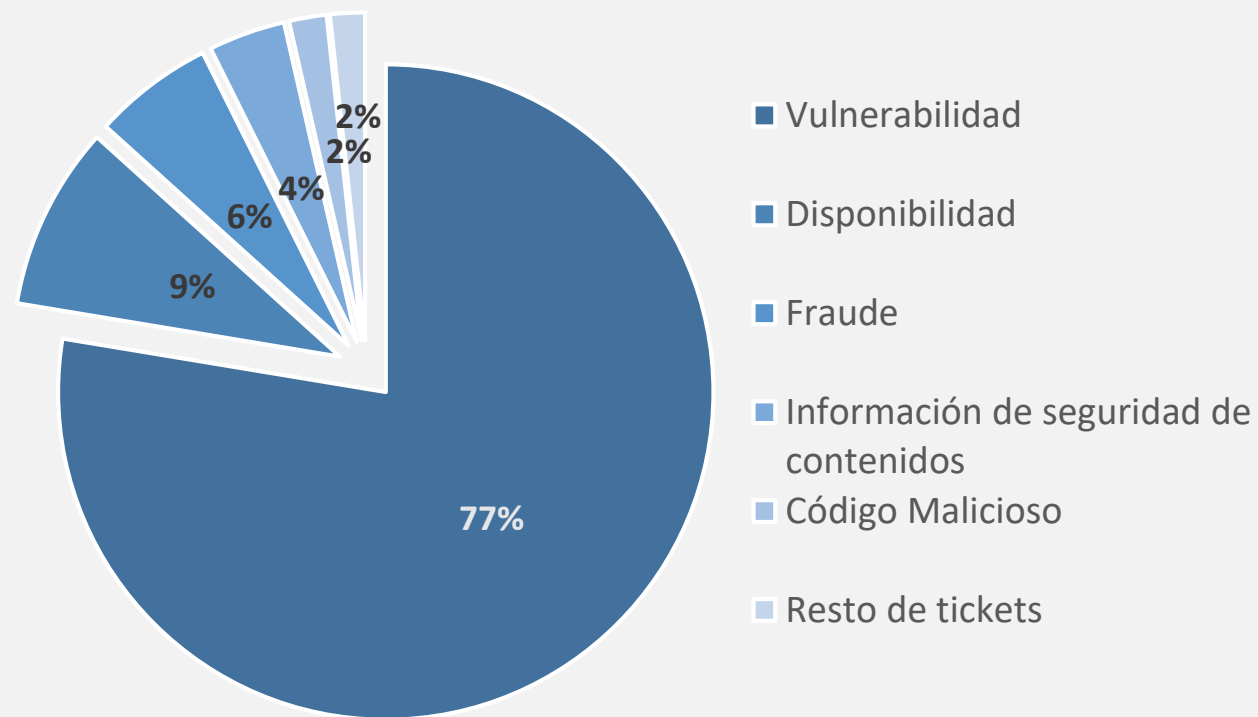
Ante las diversas amenazas y peligros que abundan en el ciberespacio, el CSIRT de Gobierno notifica a instituciones públicas y privadas de aquellos riesgos que considera más probables de afectar a sus sistemas. Es así como este mes generamos **2.269** tickets, un **6%** menos que en el período precedente. Estos tickets responden a las siguientes categorías, definidas según el tipo de incidente de seguridad informática al que corresponden, y ordenadas según su frecuencia.



TIPO DE INCIDENTE

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

Por lo anterior, 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. Por esto, adquirimos el compromiso de alertar de situaciones o incidentes riesgosos que se detectan en organizaciones privadas.

Tickets	Privado	Público	Total
Vulnerabilidad	93	1.668	1.761
Disponibilidad	11	196	206
Fraude	120	15	135
Información de seguridad de contenidos	83	3	86
Código Malicioso	35	7	42
Otros	21	13	34
Intentos de Intrusión	2	1	3
Contenido Abusivo	1	-	1
Intrusión	-	1	1
Recopilación de Información	-	-	-
Total	366	1.904	2.269

Públicas

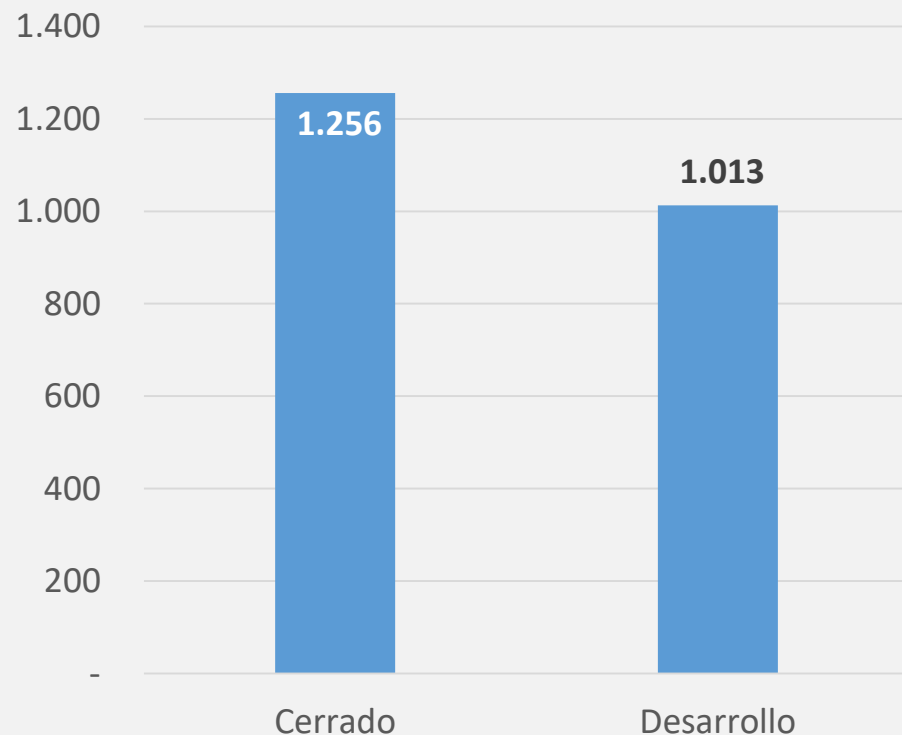
84%

Privadas

16%

PROCESAMIENTO DE TICKETS

Este mes, el **55%** de los tickets generados en el período logró ser cerrado exitosamente (contra un 66% el mes anterior), mientras el resto seguirá siendo procesado en **diciembre**.



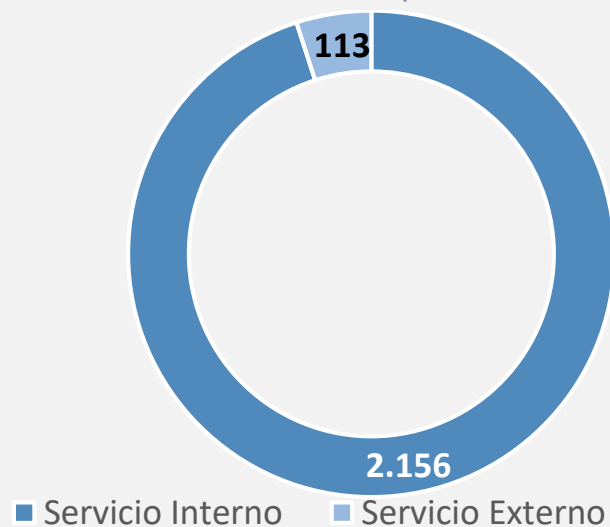
Recordamos lo esencial de obtener retroalimentación de las gestiones que se realizan en función del hallazgo encontrado.

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

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

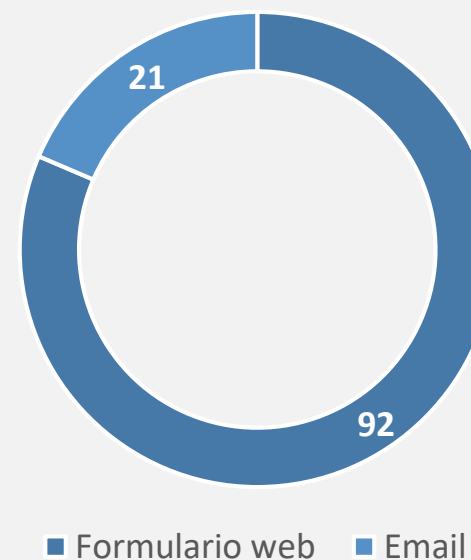
PROCEDENCIA DE TICKETS

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



Fono
CSIRT:
1510

Por otro lado, los tickets de origen externo (un **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 (**98%** de los tickets externos), alerta desde otros CSIRT internacionales, o por correos electrónicos de empresas privadas.



BOLETINES DE SEGURIDAD CIBERNÉTICA, NOVIEMBRE 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.

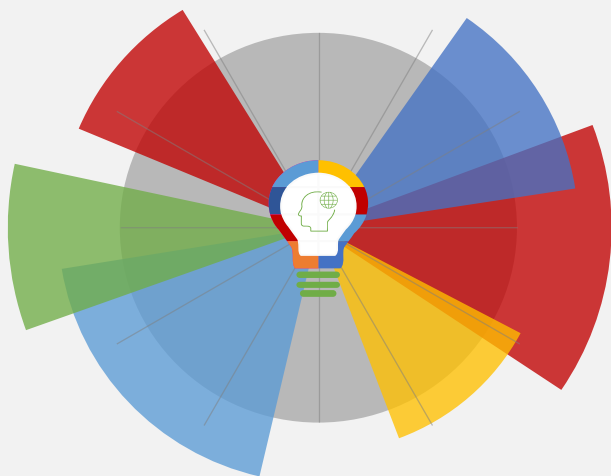
Boletín de Seguridad Cibernética n°174 - 28 de oct. al 3 de nov.: <https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-174/>

Boletín de Seguridad Cibernética n°175 - 4 al 10 de nov. : <https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-175/>

Boletín de Seguridad Cibernética n°176 - 11 al 17 de nov.: <https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-176/>

Boletín de Seguridad Cibernética n°177 - 18 al 24 de nov.: <https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-177/>

Boletín de Seguridad Cibernética n°178 - 25 de nov. Al 1 de dic.: <https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-178/>



Indicadores	B 174	B 175	B176	B177	B178
CVE	3	81	44	3	1
IP	3	10	16	25	17
Hash	12	65	19	0	7
URL	4	17	33	32	25

CAMPAÑAS DE CONCIENTIZACION

Ciberconsejos | Los secretos de la deep y la dark web

<https://www.csirt.gob.cl/recomendaciones/ciberconsejos-deep-dark-web/>

Ciberdiccionario Volumen 22

<https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-22/>

Más ciberconsejos en el Mes de la Ciberseguridad

<https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-personas-mayores/>



#ciberconsejos
Los secretos de la deep y la dark web

Cuidado con lo que puedes encontrar en la dark web
Su contenido es muchas veces ilegal, como pornografía infantil, drogas, armas, cuentas hackeadas, datos personales, malware y piratería, entre otros.

No todo es malo en la dark web, ya que también sirve para que periodistas y activistas en regímenes autoritarios puedan evitar la censura y el encarcelamiento.



Ciberdiccionario

1. ADWARE:
Tipo de software diseñado para mostrar anuncios publicitarios a quienes navegan por Internet o utilizan una app. Pueden ser legítimos o creados con fines maliciosos. En este último caso, el objetivo es obtener información privada del usuario, robar sus contraseñas o infecta su equipo con programas maliciosos



Ciberconsejos para evitar estafas en personas mayores

ESTUDIO "RADIOGRAFÍA DIGITAL EN PERSONAS MAYORES"

De acuerdo a este estudio, 1 de cada 3 personas mayores ha sido víctima de estafas digitales, principalmente, con tarjetas y cuentas bancarias.



Fuente: Estudio Radiografía Digital en Personas Mayores* elaborado por VTR y Criteria.

CAMPAÑAS DE CONCIENTIZACION

Ciberdiccionario Volumen 23

<https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-23/>

Ciberconsejos para protegerse de la violencia de género en línea

<https://www.csirt.gob.cl/recomendaciones/ciberconsejos-violencia-de-genero-2/>

Ciberconsejos para una pyme más segura

<https://www.csirt.gob.cl/recomendaciones/ciberconsejos-pymes-2022/>



Ciber diccionario

Ataque a la cadena de suministro: Se trata de una amenaza en la que los actores maliciosos infectan a un proveedor tecnológico con el objetivo de comprometer, a través de éste, a sus clientes y usuarios. Esto, al introducir código malicioso en el software del proveedor, y aprovechar la confianza que tienen en éste sus clientes.



Ciber diccionario

1. COPIA DE SEGURIDAD O BACKUP:

Proceso que consiste en duplicar los archivos o datos que se guardan en los dispositivos (computador, smartphone, etc.), con el fin de poder recuperarlos en caso de pérdida o un incidente.

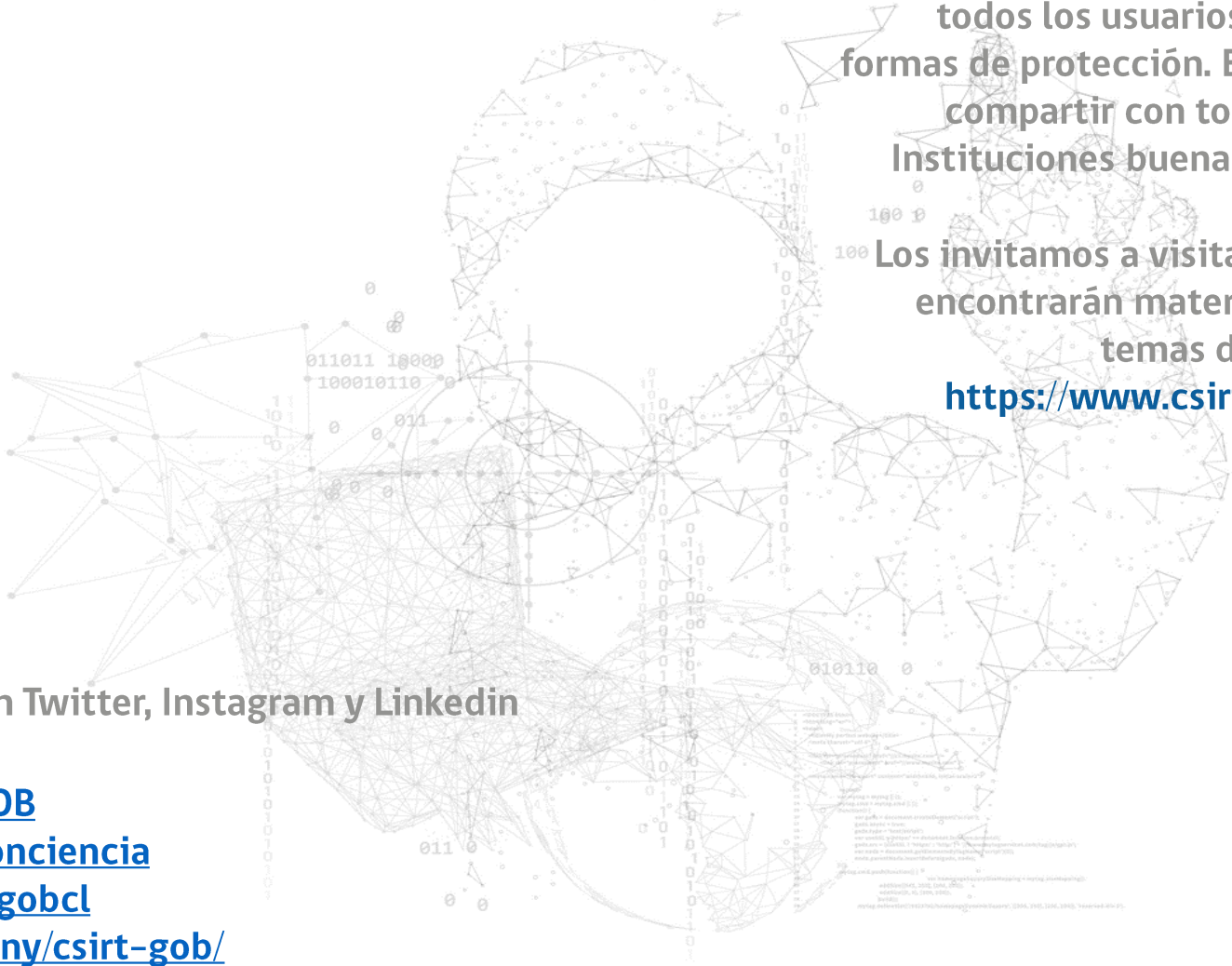


Seis #ciberconsejos para una pyme más segura

1. Capacitar sobre los riesgos cibernéticos

Las personas **somos el eslabón más débil** en ciberseguridad. Por eso, es clave que estemos al día con los riesgos de internet y **realicemos capacitaciones periódicas** en temas como identificación de phishing, detección de fraudes y creación de contraseñas robustas a **todos los trabajadores** de tu empresa, sin importar su rango.





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/