



Informe de gestión de Seguridad Cibernética

Febrero 2022



011011
100010

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

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



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 enero	6
3.4. Procedencia de tickets	6
4. Boletines de Seguridad Cibernética del mes	7



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 definidas¹ 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	11000	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

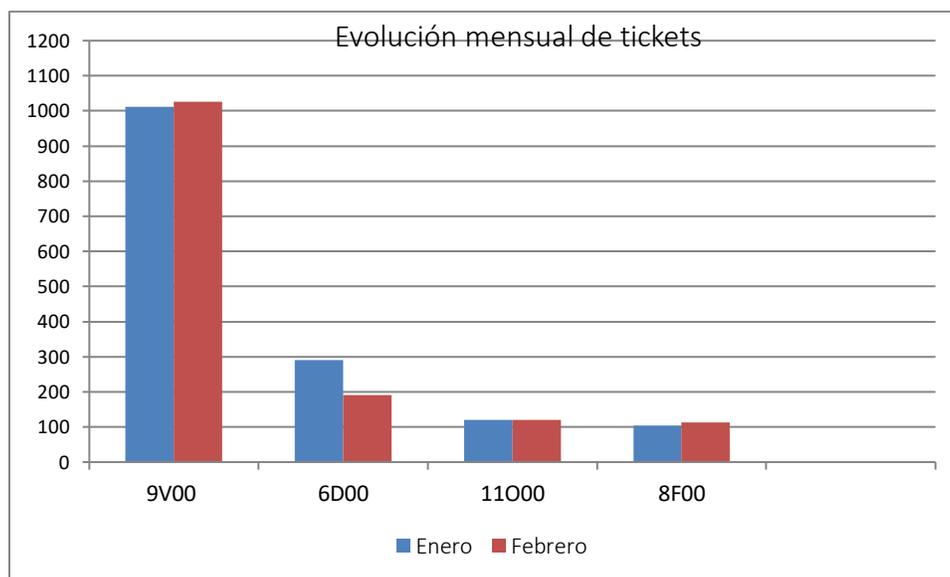


Imagen 2.- Distribución mensual de tickets por tipo.

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.

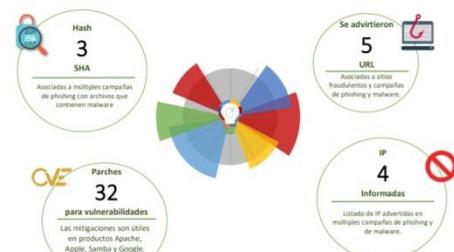
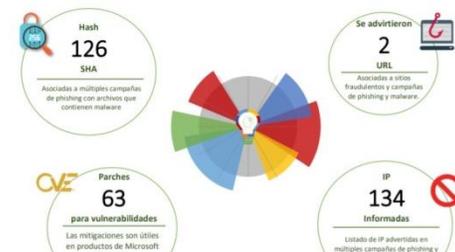
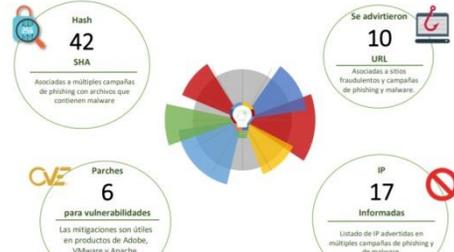
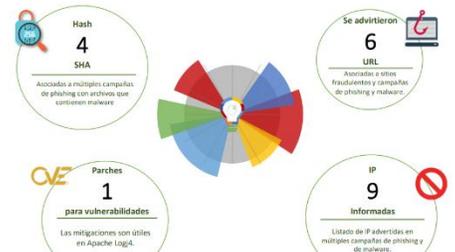
Por otro lado, los tickets de origen externo (11%) provienen de proveedores vinculados al CSIRT vía contractual o que se generan a través de reportes ciudadanos a través nuestro call center y por formulario web, alerta desde otros CSIRT internacionales, o por correos electrónicos de empresas privadas.

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.

<p>Boletín de Seguridad Cibernética n°135 https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n135/</p> <p>La semana en cifras</p>  <p>Hash 3 SHA Asociadas a múltiples campañas de phishing con archivos que contienen malware.</p> <p>Se advirtieron 5 URL Asociadas a sitios fraudulentos y campañas de phishing y malware.</p> <p>Parches 32 para vulnerabilidades Las mitigaciones son útiles en productos Apache, Apple, Samba y Google.</p> <p>IP 4 Informadas Listado de IP advertidas en múltiples campañas de phishing y de malware.</p> <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°136 https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n136/</p> <p>La semana en cifras</p>  <p>Hash 126 SHA Asociadas a múltiples campañas de phishing con archivos que contienen malware.</p> <p>Se advirtieron 2 URL Asociadas a sitios fraudulentos y campañas de phishing y malware.</p> <p>Parches 63 para vulnerabilidades Las mitigaciones son útiles en productos de Microsoft y Adobe.</p> <p>IP 134 Informadas Listado de IP advertidas en múltiples campañas de phishing y de malware.</p> <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°137 https://www.csirt.gob.cl/media/2022/02/13BCS22-000146-01.pdf</p> <p>La semana en cifras</p>  <p>Hash 42 SHA Asociadas a múltiples campañas de phishing con archivos que contienen malware.</p> <p>Se advirtieron 10 URL Asociadas a sitios fraudulentos y campañas de phishing y malware.</p> <p>Parches 6 para vulnerabilidades Las mitigaciones son útiles en productos de Adobe, VMware y Apache.</p> <p>IP 17 Informadas Listado de IP advertidas en múltiples campañas de phishing y de malware.</p> <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°138 https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n134</p> <p>Boletín de Seguridad Cibernética N°130 Semana del 3 al 9 de diciembre de 2021 13BCS21-00139-01</p>  <p>La semana en cifras</p>  <p>Hash 4 SHA Asociadas a múltiples campañas de phishing con archivos que contienen malware.</p> <p>Se advirtieron 6 URL Asociadas a sitios fraudulentos y campañas de phishing y malware.</p> <p>Parches 1 para vulnerabilidades Las mitigaciones son útiles en Apache Log4j.</p> <p>IP 9 Informadas Listado de IP advertidas en múltiples campañas de phishing y de malware.</p>



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 https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-protger-dispositivos-iot/	Ciberconsejos para una navegación segura https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-una-navegacion-segura/
 <p>CIBERCONSEJOS PARA PROTEGER TUS DISPOSITIVOS IoT</p> <p>Peligros del IoT</p> <ul style="list-style-type: none"> Infcción con malware: Sus consecuencias pueden ser múltiples: robo de datos personales o sensibles, pérdida del control del equipo, encriptación de archivos, entre otras amenazas. Robos: Toda la información que recopilan los IoT es atractiva para los cibercriminales: conocer nuestros movimientos, almacenar contraseñas, documentos de identidad, datos de tarjetas de crédito, etc. 	 <p>CIBERCONSEJOS PARA UNA NAVEGACIÓN MÁS SEGURA</p> <p>Para navegar seguro en redes sociales:</p> <ol style="list-style-type: none"> Nunca publiques datos personales como nombres, rut u otros, ya que pueden ser utilizados para descifrar contraseñas o suplantar identidad. Configura tu perfil en modo privado y acepta sólo a personas que realmente conoces. Cuidado con el envío de fotografías o videos. Otras personas pueden acceder a ellas y utilizarlas para extorsionar.



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/>

Ministerio del Interior y Seguridad Pública



CIBERCONSEJOS PARA UN TELETRABAJO MÁS SEGURO

SI TRABAJAS DESDE TU CASA O EN LA OFICINA:

- 1.- **CUIDADO** con correos electrónicos o llamados falsos.
- 2.- **SÉ CRÍTICO** con la información que recibes.
- 3.- **ACTUALIZA** el antivirus, softwares y sistemas operativos de tu computador.
- 4.- **EVITA** conectarte a internet desde una Wi-Fi pública a la red institucional.



Ministerio del Interior y Seguridad Pública



Ciberconsejos para una convivencia digital sana entre niños y jóvenes

¿A qué se exponen los niños y jóvenes en redes sociales?

1. **Cyberbullying:** Abuso, acoso o humillación constante entre escolares por medio de las redes sociales.
2. **Acceso a contenido inapropiado:** Los sitios a veces muestran comentarios o imágenes maliciosos, agresivos, violentos o sexuales.
3. **Sextorsión:** Chantaje en el que se amenaza a la víctima con la difusión de imágenes, videos o mensajes de contenido sexual propios.



Ciberconsejos para lograr comunidades educativas más seguras

<https://www.csirt.gob.cl/recomendaciones/ciberconsejos-comunidades-educativas/>

Ministerio del Interior y Seguridad Pública



CIBERCONSEJOS para comunidades educativas más seguras

Escuelas y universidades son atractivas para delincuentes

Acceso no autorizado a plataformas escolares: Delincuentes pueden robar identidades, realizar declaraciones de impuestos falsas, generar pagos a terceros, alterar el registro de los alumnos y secuestrar sitios web o cuentas de redes sociales, entre otros riesgos.

- 1.

Phishing y ransomware: Con listas de correos de alumnos o funcionarios pueden enviar emails, SMS o WhatsApp haciéndose pasar por el colegio y robar datos personales o convencer a sus víctimas de descargar programas maliciosos, como los que posibilitan el ransomware (cifrado de su PC para exigir un rescate).

- 2.

