Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Informe de gestión de Seguridad Cibernética

Marzo 2022

Índice

1.- Introducción

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

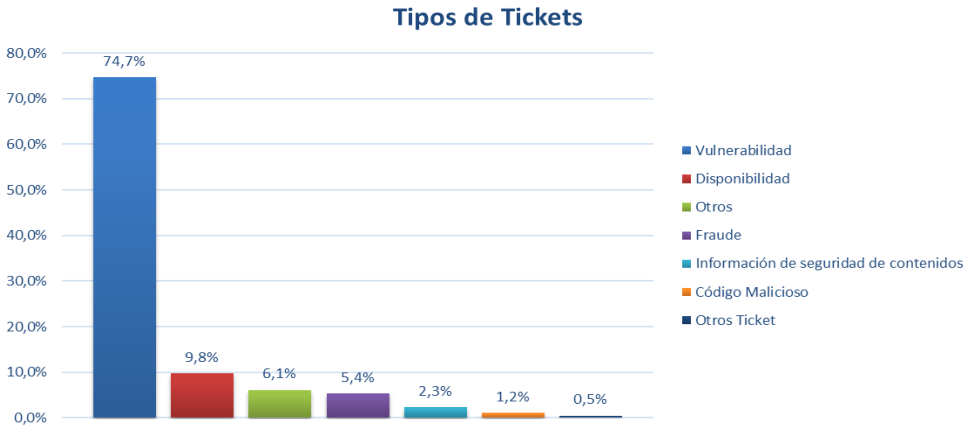
3. Resumen mensual de tickets y tipos de incidentes reportados

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 marzo generamos 2.492 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	Marzo 2022
1	Vulnerabilidad	9V00	1864
2	Disponibilidad	6D00	245
3	Otros	11O00	153
4	Fraude	8F00	132
5	Información de seguridad de contenidos	7S00	58
6	Código Malicioso	2C00	29
7	Contenido Abusivo	1A00	9
8	Intentos de Intrusión	4I00	2
9	Intrusión	5I00	0
10	Recopilación de Información	3R00	0
Total			**2.492**

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

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



2.- Distribución tipos de tickets.

[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

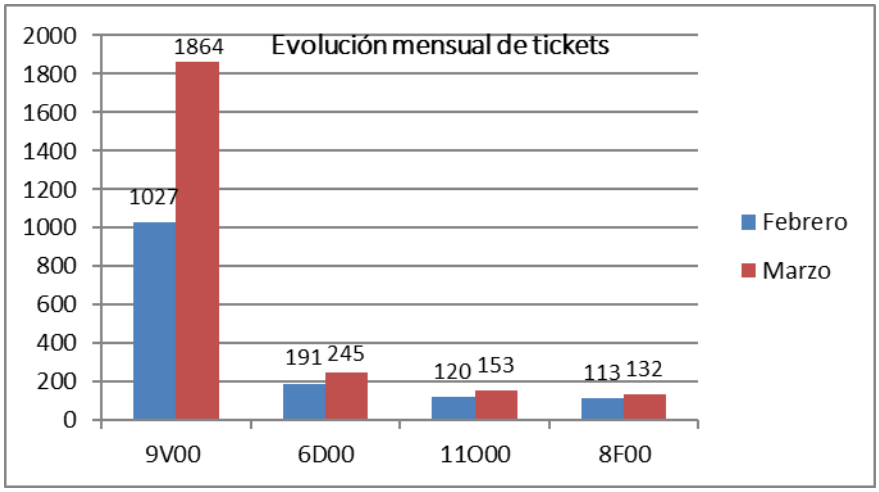


Imagen 33.- Distribución mensual de tickets por tipo.

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	152	1.712	1.864
Disponibilidad	21	224	245
Otros	111	42	153
Fraude	106	26	132
Información de seguridad de contenidos	51	7	58
Código malicioso	24	5	29
Contenido abusivo	5	4	9
Intentos de Intrusión	0	2	2
Intrusión	0	0	0
Recopilación de Información	0	0	0
Total	**472**	**2.022**	**2.492**

3.3. Estado de procesamiento de tickets durante marzo

En marzo, un 56% de los tickets generados en el período logró ser cerrada exitosamente, mientras el resto seguirá siendo procesado en abril.

Total estado Ticket	Total
En desarrollo	1.092
Cerrados	1.400
Total general	**2.492**

3.4. Procedencia de tickets

Los tickets que procesa el CSIRT de Gobierno se pueden originar tanto interna como externamente. Aquellos de origen interno (90,5% en marzo) 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 (9,5%) 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	2.259
Servicios Externos	233
Total Fuentes de Tickets	**2.492**

4. Boletines de Seguridad Cibernética del mes

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

Boletín de Seguridad Cibernética n°139:
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n139/

Boletín de Seguridad Cibernética n°140:
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n140/

Boletín de Seguridad Cibernética n°141:
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-141/

Boletín de Seguridad Cibernética n°142:
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-142/

5. Campañas de concientización durante marzo 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/.

Las campañas publicadas durante marzo fueron:

Ciberconsejos para proteger a tus hijos en redes sociales: Ya comenzó el año escolar y muchos padres, emocionados por el primer día de clases, publican fotografías de sus hijos para guardar esos lindos recuerdos. En los ciberconsejos que entrega el CSIRT cada semana, hablamos sobre lo que nunca debes publicar para cuidar y resguardar la seguridad de los niños y niñas.

Más detalles en:
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-proteger-a-tus-hijos-en-redes-sociales/

Ciberconsejos para estar más protegidas en el mundo virtual: El 8 de marzo se conmemora un nuevo Día Internacional de la Mujer, y debido a que internet es una de las vías por las cuales muchas mujeres son víctimas cada día de violencia de género, queremos aprovechar esta efeméride para recordar algunos de los principales riesgos al desenvolverse en la red, y algunas conductas seguras que es recomendable adoptar para reducirlos.

Más detalles en: https://www.csirt.gob.cl/recomendaciones/dia-internacional-de-la-mujer-ciberconsejos-para-estar-mas-protegidas-en-el-mundo-virtual/

Ciberconsejos para protegerse del ciberacoso: En el Día Contra el Ciberacoso, el CSIRT de Gobierno junto con la Fundación Katy Summer se unieron para concientizar y educar a los padres y menores sobre cómo protegerse y apoyar a las víctimas del ciberbullying.

Más detalles en:
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-protegerse-del-ciberacoso/

¿Cómo identificar un phishing?: Para realizar estos fraudes, los delincuentes requieren solo armar una página web y correos electrónicos o mensajes de texto para producir el engaño. Por eso, los mensajes fraudulentos son incesantes y, pese a que los bancos, el CSIRT de Gobierno y otras instituciones trabajamos permanentemente para advertir de ellos y bloquearlos, es indispensable que como usuarios estemos atentos a estos intentos de engaño y sepamos cómo no caer en ellos.

Más detalles en: https://www.csirt.gob.cl/recomendaciones/ciberguia-como-identificar-un-phishing/

Estafas y malware relacionados con las criptomonedas: Con el creciente interés en las denominadas criptomonedas, también han aumentado los fraudes que se apoyan en ellas. Por esto les traemos una serie de recomendaciones para evitar ser víctima de estafas con criptomonedas y criptoactivos, o que nos convirtamos en involuntarios "mineros" para los ciberdelincuentes.

Más detalles en: https://www.csirt.gob.cl/recomendaciones/ciberguia-estafas-y-malware-relacionados-con-las-criptomonedas/

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.04.04 17:09:48 -04'00'