



Índice

| | |
|--|----|
| 1. Resumen Ejecutivo | 3 |
| 2. Alcances del Informe | 4 |
| 3. Tipos de Tickets | 5 |
| 4. Tipos de Tickets Públicos y Privados..... | 7 |
| 5. Estado de Ticket Procesados en el Presente Mes..... | 8 |
| 6. Procedencia de Generación de Tickets | 9 |
| 7. Fuentes de Tickets Externos | 10 |
| 8. Boletines con resúmenes de alertas y vulnerabilidades del mes | 11 |
| 9. Síntesis de gestión sobre concientización y buenas prácticas | 12 |
| Actualidad..... | 14 |

Índice de Ilustraciones

| | |
|--|----|
| Ilustración 1 - Tipos de tickets..... | 5 |
| Ilustración 2 - Tickets a Instituciones Públicas y Privadas..... | 7 |
| Ilustración 3- Total Estado de Tickets | 8 |
| Ilustración 4- Distribución porcentual de origen de ticket..... | 9 |
| Ilustración 5- Tipos de servicios externos..... | 10 |

Índice de Tablas

| | |
|---|----|
| Tabla 1 - Total Tipos de Tickets | 5 |
| Tabla 2 - Ranking de Alertas Recibidas | 6 |
| Tabla 3 - Tickets a Instituciones Públicas y Privadas | 7 |
| Tabla 4 - Total Estado de Ticket | 8 |
| Tabla 5 - Fuentes de Servicios (Interna y/o Externa) | 9 |
| Tabla 6 - Fuentes de Origen Externo de Tickets..... | 10 |



1. Resumen Ejecutivo

El presente informe contiene un resumen de la totalidad de los tickets procesados en el mes de noviembre de 2021, entregando además la composición de los tickets desagregados por categorías, correspondientes al tipo de vulnerabilidad de las incidencias que originaron los tickets.

Este trabajo también da cuenta del porcentaje de tickets que fueron cerrados con éxito en el curso de noviembre y la proporción que queda por terminar, junto con las categorías de tickets que se reportan a las instituciones públicas o privadas.

Asimismo, se detalla el origen o procedencia de la información que procesa el CSIRT de Gobierno – si es interna o externa- y presenta el peso relativo que cada una de estas fuentes tiene dentro de la demanda de trabajo que se recibió durante el mes.

Finalmente, se entrega un desagregado que permite conocer la participación –en cantidades y términos porcentuales- de las diversas fuentes externas que componen la actual generación de tickets desde ese origen de procedencia.



2. Alcances del Informe

La presente información proviene de la gestión del CSIRT de Gobierno, en el marco del proceso de notificación a entidades, instituciones y organismos afectados, resultado a su vez de las actividades desarrolladas por nuestro equipo 24/7 durante un mes, como las siguientes:

- Gestión y seguimiento de los tickets generados, validando las acciones que se tomaron con el ticket enviado al organismo gubernamental afectado.
- Reporte de vulnerabilidades de aquellos tickets, una vez validado que la falla de seguridad siga presente.
- Generación de análisis y reporte de las vulnerabilidades detectadas dentro de la RCE¹ (falta de cifrado, CMS obsoletos, credenciales recuperadas, servidores desactualizados, puertos expuestos, phishing, defacement, entre otros).
- Seguimiento a los tickets reportados (contacto mediante llamada telefónica y/o correo electrónico) para validar qué acciones ha tomado la entidad reportada con la información de la vulnerabilidad detectada.
- Análisis y monitoreo de un listado de alrededor de 4.200 sitios gubernamentales, utilizando las plataformas Splunk, Pingdom y PRTG.
- Monitoreo de los dispositivos de las instituciones de la RCE.
- Generación de tickets para notificar a los organismos afectados ante la identificación de cualquier eventualidad en los dispositivos y sitios dentro del alcance de monitoreo del CSIRT.

¹ RCE: Red de Conectividad del Estado



3. Tipos de Tickets

En la siguiente tabla se expone las categorías de tickets, generados por el CSIRT de Gobierno. Estas tipologías son definidas según la matriz de clasificación de incidentes de la ENISA (Agencia de la Unión Europea para la Ciberseguridad) en 10 categorías relacionadas a incidentes de seguridad informática y acciones preventivas y operacionales, programadas de las instituciones que resultan en la interrupción parcial de un servicio.

El gráfico bajo la tabla muestra la misma información, pero como una distribución en términos porcentuales.

| Nº | Tipos de ticket | Código | Total |
|--------------|--|--------|-------------|
| 1 | Vulnerabilidad | 9V00 | 1288 |
| 2 | Disponibilidad | 6D00 | 337 |
| 3 | Información de seguridad de contenidos | 7S00 | 167 |
| 4 | Fraude | 8F00 | 118 |
| 5 | Otros | 11O00 | 106 |
| 6 | Código Malicioso | 2C00 | 16 |
| 7 | Recopilación de Información | 3R00 | 3 |
| 8 | Contenido Abusivo | 1A00 | 1 |
| 9 | Intrusión | 5I00 | 0 |
| 10 | Intentos de Intrusión | 4I00 | 0 |
| Total | | | 2036 |

Tabla 1 - Total Tipos de Tickets

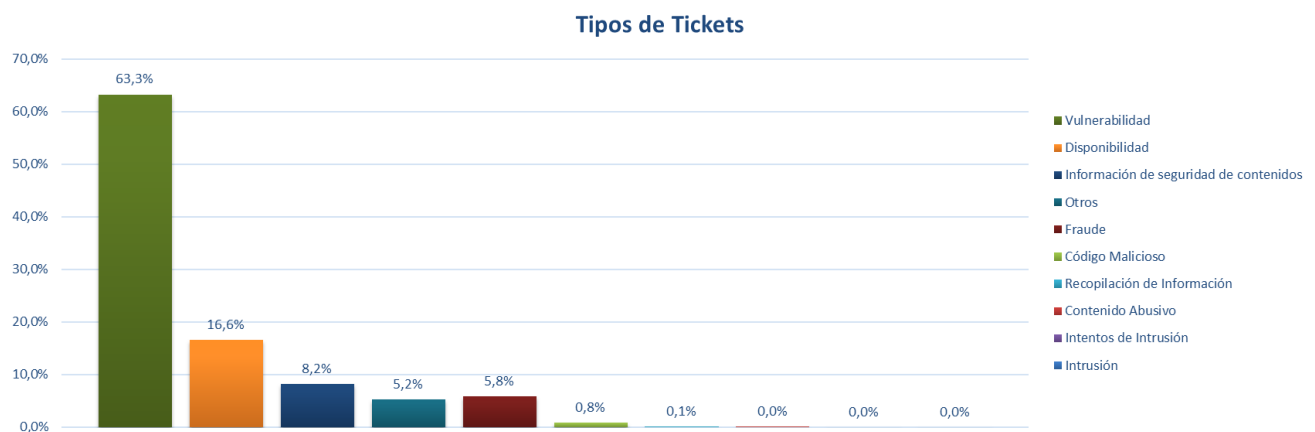


Ilustración 1 - Tipos de tickets



La siguiente tabla muestra los cambios en el ranking que experimentan los tipos de tickets generados por el CSIRT de Gobierno en noviembre, en comparación con el mes anterior.

| Nº | Septiembre | Octubre | Tendencia | Variante |
|----|--|--|-----------|----------|
| 1 | Vulnerabilidad | Vulnerabilidad | → | ↑ |
| 2 | Disponibilidad | Disponibilidad | → | ↓ |
| 3 | Información de seguridad de contenidos | Información de seguridad de contenidos | → | ↑ |
| 4 | Otros | Fraude | ▲ | ↑ |
| 5 | Fraude | Otros | ▼ | ↓ |
| 6 | Código Malicioso | Código Malicioso | → | ↑ |
| 7 | Recopilación de Información | Recopilación de Información | → | ↑ |
| 8 | Intentos de Intrusión | Contenido Abusivo | ▲ | → |
| 9 | Contenido Abusivo | Intrusión | ▼ | ↓ |
| 10 | Intrusión | Intentos de Intrusión | ▼ | ↓ |

Tabla 2 - Ranking de Alertas Recibidas



4. Tipos de Tickets Públicos y Privados

Número de tickets de noviembre, según fueron reportados a instituciones públicas o privadas, ordenados según las categorías presentadas anteriormente.

| Tickets | Privado | Público | Total |
|--|------------|-------------|-------------|
| Vulnerabilidad | 95 | 1193 | 1288 |
| Disponibilidad | 20 | 317 | 337 |
| Información de seguridad de contenidos | 145 | 22 | 167 |
| Fraude | 110 | 8 | 118 |
| Otros | 61 | 45 | 106 |
| Código Malicioso | 14 | 2 | 16 |
| Recopilación de Información | 3 | 0 | 3 |
| Contenido Abusivo | 1 | 0 | 1 |
| Intrusión | 0 | 0 | 0 |
| Intentos de Intrusión | 0 | 0 | 0 |
| Total | 449 | 1587 | 2036 |

Tabla 3 - Tickets a Instituciones Públicas y Privadas

El siguiente gráfico expone el porcentaje de tickets enviados a instituciones públicas o privadas.

Tickets a Instituciones Públicas y Privadas

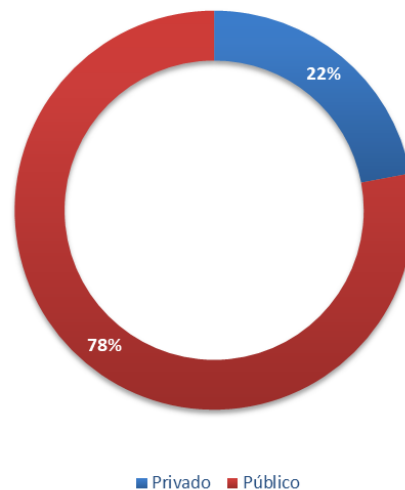


Ilustración 2— Tickets a Instituciones Públicas y Privadas



5. Estado de Ticket Procesados en el Presente Mes

La siguiente tabla y gráfico de distribución muestra el estado de los tickets procesados en noviembre de 2021. De un total de 2.036 tickets, 1.325 fueron cerrados exitosamente, lo que representa un 65% de eficacia, mientras que 711 tickets (35%) siguen en desarrollo para terminar de ser procesados en el período siguiente.

| Total estado Ticket | Total |
|----------------------|-------------|
| En desarrollo | 711 |
| Cerrados | 1325 |
| Total general | 2036 |

Tabla 4 - Total Estado de Ticket

Total Estado de Tickets

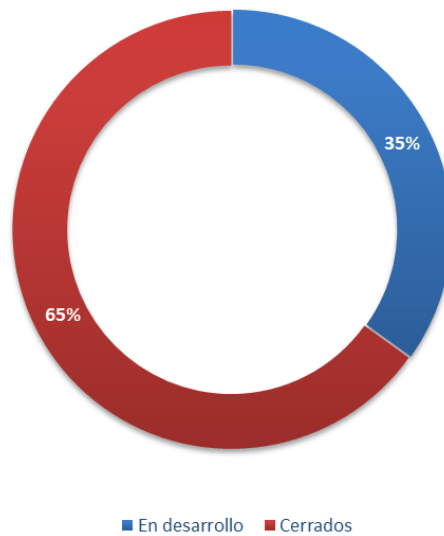


Ilustración 3 - Total Estado de Tickets



6. Procedencia de Generación de Tickets

En la siguiente tabla se presenta la composición -del origen de los tickets (interna o externa)- que procesó el CSIRT de Gobierno durante el mes de noviembre de 2021.

Los tickets de origen interno son aquellos generados por sistemas propios del Ministerio del Interior y Seguridad Pública, mediante el software que utiliza el CSIRT -que también considera los sensores que dan aviso o reportan- desde otros servicios públicos o las Fuerzas Armadas.

Por otro lado, los tickets externos son los provenientes de proveedores vinculados al CSIRT vía contractual o que se generan a través de nuestro call center, por formulario web, por medio de otros CSIRT internacionales o por correos electrónicos de empresas privadas.

| Tipo de Fuente | Cantidad de Tickets |
|---------------------------------|---------------------|
| Servicios Internos | 1866 |
| Servicios Externos | 170 |
| Total Fuentes de Tickets | 2036 |

Tabla 5 - Fuentes de Servicios (Interna y/o Externa)

Un 92% de la demanda de trabajo que recibió CSIRT en el pasado mes de noviembre tiene un origen interno, mientras que el 8% restante proviene de fuentes externas.

Tipos de Servicios

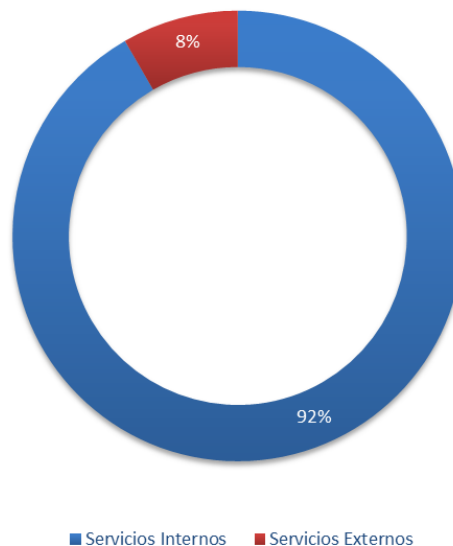


Ilustración 4- Distribución Porcentual de Origen de Tickets



7. Fuentes de Tickets Externos

En la siguiente tabla se da cuenta de las fuentes externas que dieron origen a tickets en noviembre de 2021.

| Fuentes de Origen Externo de Tickets | Cantidad de Tickets |
|--------------------------------------|---------------------|
| Generados vía Formulario web | 104 |
| Generados vía Email | 48 |
| Generados vía Call center | 12 |
| Generados vía Internacionales | 4 |
| Generados vía Redes sociales | 1 |
| Generados vía Proveedor de servicio | 1 |
| Total | 170 |

Tabla 6 - Fuentes de Origen Externo de Tickets

En noviembre de 2021, el porcentaje mayor de tickets externos fueron generados vía formulario web, con un 61,2% de participación. En segundo lugar, aquellos vía email” con un 28,2%.

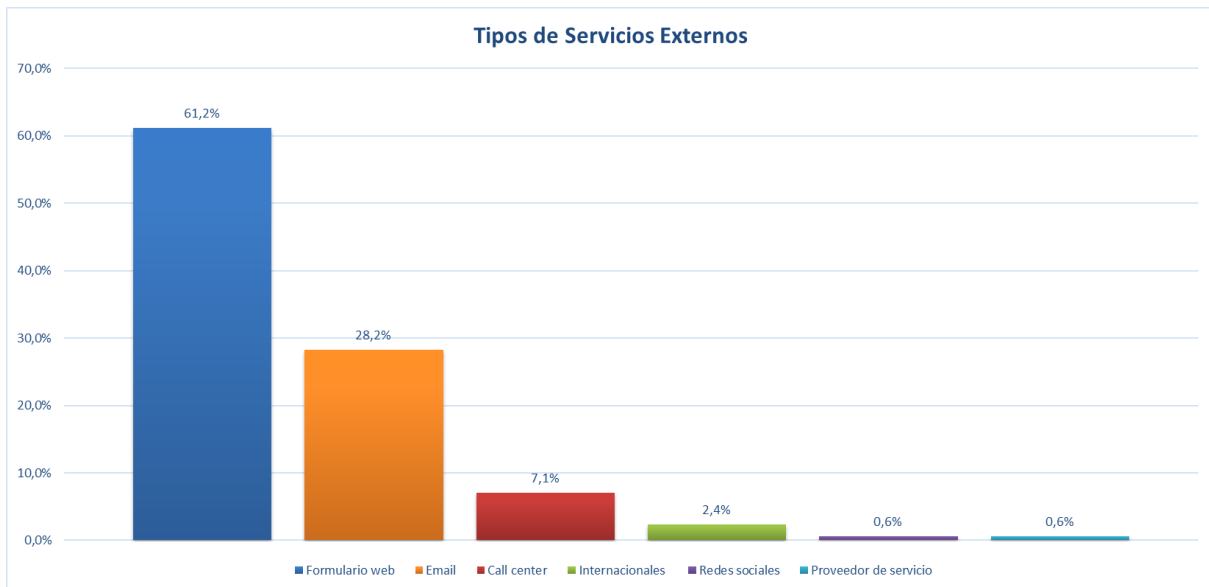

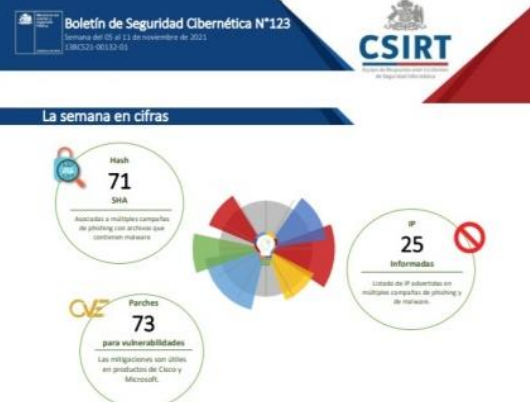




Ilustración 5- Tipos de servicios externo



8. Boletines con resúmenes de alertas y vulnerabilidades del mes





Los enlaces que se comparten a continuación, corresponden a los boletines semanales publicados durante noviembre, que contienen el resumen de las actividades realizadas por el CSIRT de Gobierno, y que fueron publicados semanalmente en el sitio web www.csirt.gob.cl.

| Boletín de Ciberseguridad n°122 | Boletín de Ciberseguridad n°123 |
|--|--|
| https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n122/ | https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n123-2/ |
|  <p>Boletín de Seguridad Cibernética N°122 Semana del 22 al 28 de noviembre de 2021 [SANC21-00133-01]</p> <p>La semana en cifras</p> <ul style="list-style-type: none"> Hash SHA: 34. Asociados a múltiples campañas de phishing con archivos que contienen malware. Se advirtieron URL: 10. Asociados a otros fraudulentos y campañas de phishing y malware. Parches para vulnerabilidades: 228. Las investigaciones son útiles en productos de Red Hat, Discourse, Apple y Adobe. IP Informadas: 16. Estado de IP advertidas en múltiples campañas de phishing y de malware. <p><small>*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web www.csirt.gob.cl.</small></p> |  <p>Boletín de Seguridad Cibernética N°123 Semana del 01 al 07 de noviembre de 2021 [SANC21-00133-01]</p> <p>La semana en cifras</p> <ul style="list-style-type: none"> Hash SHA: 71. Asociados a múltiples campañas de phishing con archivos que contienen malware. Se advirtieron IP Informadas: 25. Estado de IP advertidas en múltiples campañas de phishing y de malware. Parches para vulnerabilidades: 73. Las investigaciones son útiles en productos de Cisco y Microsoft. <p><small>*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web www.csirt.gob.cl.</small></p> |
| Boletín de Ciberseguridad n°124 | Boletín de Ciberseguridad n°125 |
| https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n124/ | https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n125/ |
|  <p>Boletín de Seguridad Cibernética N°124 Semana del 12 al 18 de noviembre de 2021 [SANC21-00133-01]</p> <p>La semana en cifras</p> <ul style="list-style-type: none"> Hash SHA: 42. Asociados a múltiples campañas de phishing con archivos que contienen malware. Se advirtieron URL: 9. Asociados a otros fraudulentos y campañas de phishing y malware. Parches para vulnerabilidades: 22. Las investigaciones son útiles en productos de Citrix, Palo Alto, Intel y Google. IP Informadas: 20. Estado de IP advertidas en múltiples campañas de phishing y de malware. <p><small>*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web www.csirt.gob.cl.</small></p> |  <p>Boletín de Seguridad Cibernética N°125 Semana del 23 al 29 de noviembre de 2021 [SANC21-00134-01]</p> <p>La semana en cifras</p> <ul style="list-style-type: none"> Hash SHA: 46. Asociados a múltiples campañas de phishing con archivos que contienen malware. Se advirtieron URL: 3. Asociados a otros fraudulentos y campañas de phishing y malware. Parches para vulnerabilidades: 20. Las investigaciones son útiles en productos de Microsoft. IP Informadas: 25. Estado de IP advertidas en múltiples campañas de phishing y de malware. <p><small>*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web www.csirt.gob.cl.</small></p> |



9. Síntesis de gestión sobre concientización y buenas prácticas

Los siguientes enlaces corresponden a las campañas de concientización y buenas prácticas publicadas por CSIRT durante noviembre, disponibles en [csirt.gob.cl/recomendaciones](https://www.csirt.gob.cl/recomendaciones).

| | |
|---|---|
| <p>Kits de herramientas para mejorar la ciberseguridad de las pymes</p> <p>https://www.csirt.gob.cl/recomendaciones/ciberguia-para-las-pymes/</p>  | <p>CiberSucesos ESPECIAL Mes de la Ciberseguridad</p> <p>https://www.csirt.gob.cl/recomendaciones/cibersucesos-especial-mes-ciberseguridad/</p>  |
| <p>Ciberconsejos: Cómo cuidarnos de las fake news en estas elecciones</p> <p>https://www.csirt.gob.cl/recomendaciones/ciberconsejos-fake-news-elecciones2021/</p>  | <p>Ciberconsejos para protegernos de la violencia de género en línea</p> <p>https://www.csirt.gob.cl/recomendaciones/ciberconsejos-violencia-de-genero/</p>  |



| Ciberconsejos para prevenir estafas en la plataforma de streaming Twitch | Ciberconsejos para comprar con seguridad este Black Friday |
|---|---|
| https://www.csirt.gob.cl/recomendaciones/ciberconsejos-twitch/ | https://www.csirt.gob.cl/recomendaciones/ciberconsejos-black-friday-2021/ |
|  |  |

Ciberconsejos para evitar caer en estafas esta Navidad

<https://www.csirt.gob.cl/recomendaciones/ciberconsejos-navidad-2021/>





Actualidad

CSIRT informa de nueva campaña con el malware Emotet y comparte IoC para monitoreo

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, informó a fines de noviembre de la detección de una nueva campaña de malware a través de correos electrónicos, enfocada en difundir el peligroso programa Emotet. Para revisar todos los detalles e indicadores de compromiso (IoC) útiles para reducir la efectividad de esta campaña maliciosa, se sugiere revisar el siguiente informe: <https://www.csirt.gob.cl/noticias/emotet-2021-ioc/>.

Emotet es considerado altamente peligroso, ya que no es fácil de identificar y es de rápida propagación. Por esto, el CSIRT de Gobierno recomienda estar alertas y reforzar las medidas de seguridad de cada de las instituciones. Para ello, sugerimos:

- Mantener actualizados los sistemas operativos, navegadores y complementos, además de sistemas antivirus y antimalware.
- Aumentar las medidas de seguridad de los programas antispam o poner en cuarentena los archivos .zip que incluyan una contraseña, con tal de realizar una revisión preventiva.
- Educar a los funcionarios para que no descarguen archivos ni ingresen a enlaces de correo de remitente desconocido. Se recomienda compartir esta campaña a sus trabajadores: [csirt.gob.cl/media/2021/04/CSIRT-de-Gobierno-Campa%C3%B1a-Emotet-1.pdf](https://www.csirt.gob.cl/media/2021/04/CSIRT-de-Gobierno-Campa%C3%B1a-Emotet-1.pdf).

Solicitamos informar al CSIRT de Gobierno si detectan este tipo de correos electrónicos o si sufren una afectación de los sistemas para apoyar cualquier incidente.

Características de esta nueva campaña

Estas nuevas apariciones de Emotet tienen un comportamiento diferente al de ocasiones anteriores. Así, para que malware no sea detectado por programas de ciberseguridad, el atacante adjunta a su correo electrónico un archivo .zip, junto a la contraseña para descomprimirlo. Hecho esto, el usuario encontrará un archivo .doc, el que a su vez incorpora un script ofuscado.

Si el usuario ejecuta este documento, el script comienza a buscar en internet sitios donde se ha alojado previamente un archivo DLL malicioso para su descarga, infectando el equipo. También se ha detectado Emotet en archivos de Excel (.xlsm), o directamente en enlaces de descarga.