



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

Informe de Gestión de Seguridad Cibernética

CSIRT - SEPTIEMBRE 2020

Santiago, 05 de octubre de 2020



Índice

1. Resumen Ejecutivo	3
2. Alcances del Informe	4
3. Tipos de Tickets	5
4. Tipos de Ticket Públicos y Privados.....	7
5. Estado de Ticket Procesados en el Presente Mes.....	8
6. Procedencia de Generación de Tickets.....	9
7. Fuentes de Origen Externo de Tickets	10
8. Boletines con resúmenes de alertas y vulnerabilidades del mes.....	10
9. Síntesis de informes y trabajos de investigación	12

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 Tickets	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
Tabla 8 - Gestión de cambios.....	14

1. Resumen Ejecutivo

El presente informe contiene un resumen de la totalidad de los tickets procesados en el mes de septiembre de 2020. El documento muestra la composición de los tickets desagregados por categorías que corresponden al tipo de vulnerabilidad de las incidencias que originaron los tickets.

El informe también da cuenta del porcentaje de tickets que fueron cerrados con éxito en el curso del mes de septiembre y también muestra la proporción de aquellos que quedan por terminar.

Asimismo, en este documento se muestra por categorías los tipos de tickets que se reportan para notificar a las instituciones públicas o privadas.

Este reporte mensual muestra, además, el origen o procedencia de la información que procesa CSIRT –si es interna o externa- y presenta en términos porcentuales el peso relativo que cada una de estas fuentes tiene dentro de la demanda de trabajo que se recibió durante el mes.

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

Finalmente, se presenta información proveniente de la plataforma MISP¹ que contiene la cantidad de posibles IoCs² o –Índices de Compromiso- que se hayan detectado. Esta información es relevante para CSIRT dado que se utiliza como punto de partida para validar correlaciones con todas nuestras plataformas de análisis. En el informe se expone una tabla donde se puede enumerar la cantidad de IoCs detectados en el presente mes, los cuales se presentan diferenciados en base a direcciones IP³ o a URL⁴.

¹ MISP es una sigla en idioma inglés que significa Malware Information Sharing Platform o “Plataforma para compartir información de Malware y amenazas”.

² IOC es una sigla en idioma inglés que significa “Índice de compromiso”, y se refiere a la descripción de un incidente de ciberseguridad, actividad y/o artefacto malicioso mediante patrones.

³ IP es una sigla en idioma inglés que significa “Internet Protocol” y corresponde a un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, smartphone).

⁴ Es una sigla en idioma inglés que significa Uniform Resource Locator o “Localizador Uniforme de Recursos”. Se trata de la secuencia de caracteres que sigue un estándar y que permite denominar recursos dentro del entorno de Internet para que puedan ser localizados. Los documentos de texto, las fotografías y los audios, entre otros tipos de contenidos digitales, tienen un URL cuando se publican en Internet. Estos localizadores permiten crear hipervínculos. De esta forma, el URL, por lo tanto, es el conjunto de caracteres que posibilita la asignación de una dirección exclusiva a un recurso que se encuentra disponible en el espacio virtual. En otras palabras, el URL es una dirección de Internet que, al ser encontrada y visualizada por un navegador, muestra un recurso de información al usuario.

2. Alcances del Informe

La información que se muestra en el presente informe proviene de la gestión de CSIRT en el marco del proceso de notificación a entidades, instituciones y/o organismos afectados. Esa información se produce como consecuencia de las actividades desarrolladas por el equipo 24/7 en un período de tiempo mensual. A continuación, se enumera resumidamente esas actividades:

- Gestión de tickets generados, efectuando seguimiento y validando las acciones que se tomaron con el ticket enviado al organismo gubernamental afectado.
- Reporte de vulnerabilidades de aquellos tickets precedentes una vez validado que la falla de seguridad se encuentre aún presente.
- Generación de análisis y reporte de vulnerabilidades detectadas dentro de la RCE⁵ (falta cifrado, CMS obsoletos, credenciales recuperadas, servidores desactualizados, puertos expuestos, Phishing, deface, etc...).
- 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 -6.200 sitios aproximadamente- los cuales corresponden a portales gubernamentales, a los que se ha validado su estatus utilizando las plataformas Splunk, Pingdom y PRTG.
- Monitoreo de los dispositivos de las instituciones que se encuentran conectadas dentro de la RCE.
- Generación de ticket para notificar a la entidad y/o organismo afectado, ante la identificación de cualquier eventualidad sucedida con los dispositivos y sitios que se encuentran dentro del alcance de monitoreo de CSIRT.

⁵ RCE significa Red de Conectividad del Estado

3. Tipos de Tickets

En la siguiente tabla se expone las categorías, o tipos de tickets, que son generados por el equipo CSIRT. La información se presenta ordenada, de mayor a menor, respecto a la cantidad de tickets que se generó por cada tipo de ticket. Más abajo se muestra un gráfico que refleja esta misma información, pero como una distribución en términos porcentuales de lo que representa la participación de cada tipo de ticket dentro del total de la demanda de trabajo que recibe y procesa CSIRT.

N°	Tipos de ticket	Código	Cantidad
1	Fraude	8F00	256
2	Recopilación de Información	3R00	198
3	Vulnerabilidad	9V00	142
4	Información de seguridad de contenidos	7S00	91
5	Operaciones Ciberseguridad CSIRT	19OC	69
6	Código Malicioso	2C00	56
7	Disponibilidad	6D00	38
8	Contenido Abusivo	1A00	11
9	Intrusión	5I00	1
10	Intentos de Intrusión	4I00	1
TOTAL			863

Tabla 1 - Total Tipos de Tickets



Ilustración 1 - Tipos de tickets

En la siguiente tabla se muestran la tendencia y los cambios en el ranking que experimentan los tipos de tickets generados por CSIRT en el mes de septiembre, respecto del mes anterior.

Como se aprecia en la tabla, los tickets de las categorías vulnerabilidad, disponibilidad y contenido abusivo, experimentan una tendencia creciente al comparar ambos períodos, mientras que los tickets de las otras siete restantes categorías decrecen en el mismo espacio de tiempo en que se realiza la comparación.

Al comparar el ranking de ambos períodos se puede observar que los tipos de alertas que suben de posición corresponden a las categorías de operación de ciberseguridad y vulnerabilidad, descendiendo operaciones de ciberseguridad y las restantes categorías mantienen sus posiciones en el ranking.

El resto de las categorías mantienen sus posiciones en los rankings de ambos períodos.

Agosto		Septiembre		Tendencia	Variación
1	Fraude	1	Fraude	▼	→
2	Recopilación de Información	2	Recopilación de Información	▼	→
3	Operaciones Ciberseguridad CSIRT	3	Vulnerabilidad	▲	▲
4	Vulnerabilidad	4	Información de seguridad de contenidos	▼	▲
5	Información de seguridad de contenidos	5	Operaciones Ciberseguridad CSIRT	▼	▼
6	Código Malicioso	6	Código Malicioso	▼	→
7	Disponibilidad	7	Disponibilidad	▲	→
8	Contenido Abusivo	8	Contenido Abusivo	▲	→
9	Intrusión	9	Intrusión	▼	→
10	Intentos de Intrusión	10	Intentos de Intrusión	▼	→

Tabla 2 - Ranking de Alertas Recibidas

4. Tipos de Ticket Públicos y Privados

En la siguiente tabla se presenta el desgregado de los tickets que fueron reportados a instituciones públicas o privadas.

Tickets	Privado	Público	Total
Fraude	236	20	256
Recopilación de Información	196	2	198
Vulnerabilidad	1	141	142
Información de seguridad de contenidos	84	7	91
Operaciones Ciberseguridad CSIRT	53	16	69
Código Malicioso	4	52	56
Disponibilidad	0	38	38
Intentos de Intrusión	8	3	11
Intrusión	0	1	1
Contenido Abusivo	0	1	1
Total	582	281	863

Tabla 3 - Tickets a Instituciones Públicas y Privadas

En el siguiente gráfico expone el porcentaje de participación que tiene cada destino de los tickets que son enviados a instituciones públicas o privadas.

Tickets a Instituciones Públicas y privadas

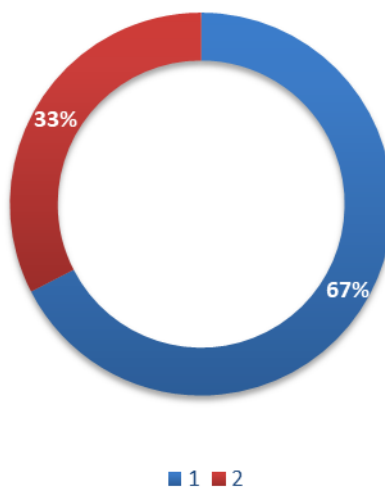


Ilustración 2 - Tickets a Instituciones Públicas (1) y Privadas (2)

5. Estado de Ticket Procesados en el Presente Mes

En la siguiente tabla y gráfico de distribución se muestra el estado de los tickets procesados en el mes de septiembre de 2020. Como se puede apreciar la cantidad de tickets abiertos o generados en el período son un total de 863 unidades. De este total, 402 tickets fueron cerrados, lo que representa un 47% de eficacia, mientras que 461 tickets (53%) siguen en desarrollo para terminar de ser procesados en los períodos siguientes.

Total Estado ticket	Suma total
En desarrollo	461
Cerrados	402
Total general	863

Tabla 4 - Total Estado de Ticket

Total Estado de Tickets

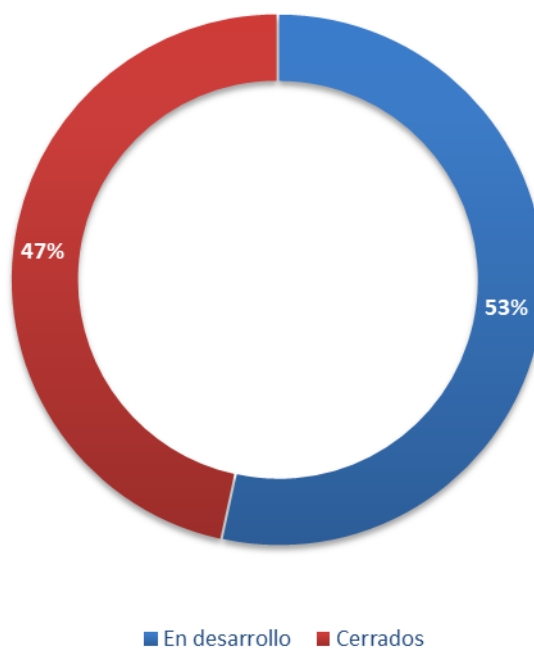


Ilustración 3 - Total Estado de Tickets

6. Procedencia de Generación de Tickets

En la siguiente tabla se presenta la composición -del origen de los tickets- que procesó CSIRT para el desarrollo de su labor durante el mes de septiembre de 2020.

Como se aprecia en la tabla los tickets se pueden originar tanto internamente, como externamente. Los tickets de origen internos son todos aquellos que fueron generados por sistemas propios del Ministerio del Interior y Seguridad Pública, mediante el software que utiliza CSIRT -que también considera los sensores que dan aviso o reportan- desde otros servicios públicos o de las FF.AA.

Por otro lado, los tickets de origen externo son todos aquellos que provienen de proveedores que tienen contrato y que se generan a través de 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	271
Servicios Externos	592
Total Fuentes de Tickets	863

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

Como se puede observar en el siguiente gráfico, un 31% de la demanda de trabajo que recibe CSIRT en el pasado mes de septiembre tiene un origen interno, mientras que el 69% restante proviene de fuentes externas.

Tipos de Servicios

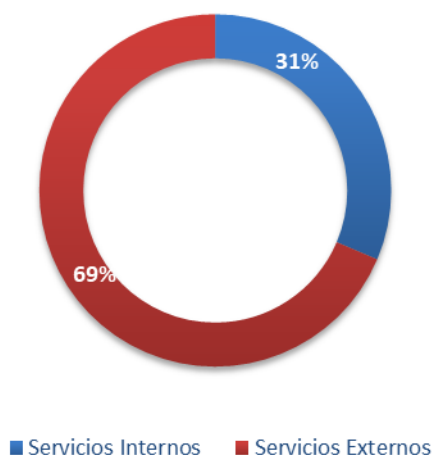


Ilustración 4 - Distribución Porcentual de Origen de Tickets

7. Fuentes de Origen Externo de Tickets

En la siguiente tabla se presenta información que da cuenta de las fuentes externas que dieron origen a tickets de esa procedencia durante el pasado mes de septiembre.

Fuentes de Origen Externo de Tickets	Cantidad de Tickets
Tickets generados por información entregada por empresas privadas sin convenio de ciberseguridad	582
Tickets generados por información entregada por empresas privadas con convenio de ciberseguridad	0
Tickets generados por privados vía formulario web	69
Tickets generados por privados vía email	0
Tickets generados por privados vía call center	0
Tickets generados por información de otros CSIRT internacionales	0
Total	651

Tabla 6 - Fuentes de Origen Externo de Tickets

En septiembre de 2020, el siguiente gráfico de distribución muestra que el porcentaje mayor de tickets externos son generados por reportes entregados por “Empresas privadas que no prestan servicio al CSIRT”, con un 89% de participación. En segundo lugar, se ubican aquellos tickets que provienen de “de privados vía formulario web” con un 11% de contribución.



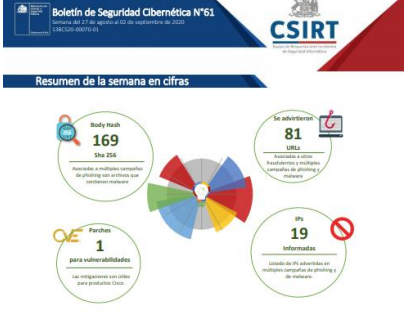
Ilustración 5 - Tipos de servicios externos

8. Boletines con resúmenes de alertas y vulnerabilidades del mes

Los enlaces que se comparten a continuación, corresponden a los boletines semanales publicados durante el mes de septiembre que contienen el resúmenes de actividades realizadas por el CSIRT y que fueron publicadas en el sitio web www.csirt.gob.cl

Boletín de Ciberseguridad n°61

<https://www.csirt.gob.cl/estadisticas/boletin-de-ciberseguridad-n61/>



Resumen de la semana en cifras

- Body Hash**: 169 (Sitio 256) - Asociado a múltiples campañas de phishing con enlaces que contienen malware
- Se advirtieron**: 81 URL - Asociado a sitios fraudulentos y múltiples campañas de phishing y malware
- Parches**: 1 para vulnerabilidades - Las investigaciones con sitios para productos Cisco
- IPs**: 19 Informadas - Sitios de IP advertidos en múltiples campañas de phishing y de malware

Contenido

Sitios Fraudulentos	2
Phishing	11
Vulnerabilidades	1
Indicadores de Compromiso	14
Recomendaciones y Buenas Prácticas	14
Investigación	24
Muro de la Fama	25

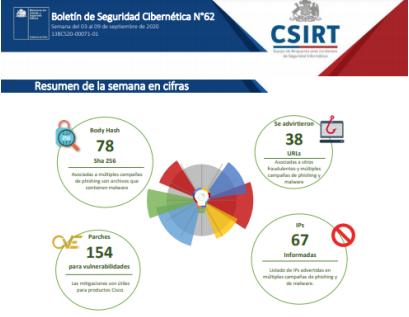
Sitios fraudulentos

Ministerio del Interior y Seguridad Pública | Página 2 de 25

<https://www.csirt.gob.cl> | (562) 2488 3850 | @cungob | <https://www.linkedin.com/company/csirt-gob>

Boletín de Ciberseguridad n°62

<https://www.csirt.gob.cl/estadisticas/boletin-de-ciberseguridad-n62/>



Resumen de la semana en cifras

- Body Hash**: 78 (Sitio 256) - Asociado a múltiples campañas de phishing con enlaces que contienen malware
- Se advirtieron**: 38 URL - Asociado a sitios fraudulentos y múltiples campañas de phishing y malware
- Parches**: 154 para vulnerabilidades - Las investigaciones con sitios para productos Cisco
- IPs**: 67 Informadas - Sitios de IP advertidos en múltiples campañas de phishing y de malware

Contenido

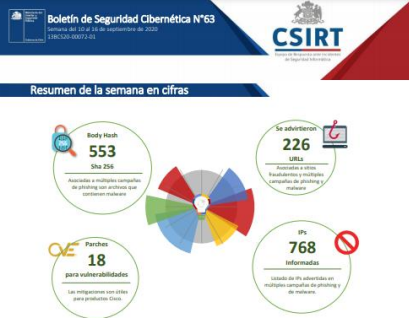
Sitios Fraudulentos	3
Phishing	13
Vulnerabilidades	14
Indicadores de Compromiso	19
Recomendaciones y Buenas Prácticas	22
Actualidad	23
Muro de la Fama	24

Ministerio del Interior y Seguridad Pública | Página 2 de 24

<https://www.csirt.gob.cl> | (562) 2488 3850 | @cungob | <https://www.linkedin.com/company/csirt-gob>

Boletín de Ciberseguridad n°63

<https://www.csirt.gob.cl/estadisticas/boletin-de-ciberseguridad-n63/>



Resumen de la semana en cifras

- Body Hash**: 553 (Sitio 256) - Asociado a múltiples campañas de phishing con enlaces que contienen malware
- Se advirtieron**: 226 URL - Asociado a sitios fraudulentos y múltiples campañas de phishing y malware
- Parches**: 18 para vulnerabilidades - Las investigaciones con sitios para productos Cisco
- IPs**: 768 Informadas - Sitios de IP advertidos en múltiples campañas de phishing y de malware

Contenido

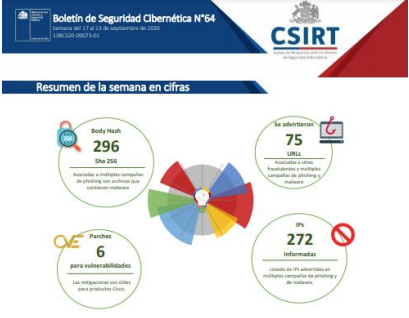
Sitios Fraudulentos	3
Phishing	15
Vulnerabilidades	17
Indicadores de Compromiso	19
Recomendaciones y Buenas Prácticas	42
Investigación	43
Muro de la Fama	44

Ministerio del Interior y Seguridad Pública | Página 2 de 44

<https://www.csirt.gob.cl> | (562) 2488 3850 | @cungob | <https://www.linkedin.com/company/csirt-gob>

Boletín de Ciberseguridad n°64

<https://www.csirt.gob.cl/estadisticas/boletin-de-ciberseguridad-n64/>



Resumen de la semana en cifras

- Body Hash**: 296 (Sitio 256) - Asociado a múltiples campañas de phishing con enlaces que contienen malware
- Se advirtieron**: 75 URL - Asociado a sitios fraudulentos y múltiples campañas de phishing y malware
- Parches**: 6 para vulnerabilidades - Las investigaciones con sitios para productos Cisco
- IPs**: 272 Informadas - Sitios de IP advertidos en múltiples campañas de phishing y de malware

Contenido

Sitios Fraudulentos	3
Ingeniería Social	9
Vulnerabilidades	10
Indicadores de Compromiso	11
Recomendaciones y Buenas Prácticas	22
Muro de la Fama	23

Ministerio del Interior y Seguridad Pública | Página 2 de 33

<https://www.csirt.gob.cl> | (562) 2488 3850 | @cungob | <https://www.linkedin.com/company/csirt-gob>

9. Síntesis de informes y trabajos de investigación

Los enlaces que se comparten a continuación, corresponden a los informes e investigaciones publicadas por CSIRT durante el mes de septiembre y que están disponibles en el sitio web <https://www.csirt.gob.cl/reportes/>

Sistemas Legacy	Defacement. El grafiti digital
https://www.csirt.gob.cl/reportes/an2-2020-16/	https://www.csirt.gob.cl/reportes/an2-2020-17/
	

10. Síntesis de gestión sobre concientización y buenas prácticas

Los enlaces que se comparten a continuación, corresponden a campaña de concientización y buenas prácticas publicadas por CSIRT durante el mes de septiembre y que están disponibles en el sitio web <https://www.csirt.gob.cl/recomendaciones/>

Sexting: riesgo online para menores	Cyber Day Seguro
https://www.csirt.gob.cl/recomendaciones/sexting-un-riesgo-online-para-nuestros-hijos/	https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-un-cyber-day-seguro/
 <p>SEXTING un riesgo on-line para nuestros hijos</p> <p>¿QUÉ ES EL SEXTING? Enviar fotos, mensajes o videos con contenido sexual explícito o sugerente se conoce como sexting, una práctica que se realiza a través de los distintos medios electrónicos, como celulares, webcam, correos electrónicos u otros.</p> <p>¿POR QUÉ LOS JÓVENES COMPARTEN FOTOS ÍNTIMAS?</p> <ul style="list-style-type: none"> • Aprobación social. • Autoestima. • Presión entre los mismos adolescentes. • Percepción de que pueden controlar donde terminan las imágenes. 	 <p>CIBERCONSEJOS PARA UN CYBERDAY SEGURO #Cybercl</p> <ol style="list-style-type: none"> SI RECIBES UN CORREO inesperado con enlaces o archivos adjuntos sobre una oferta especial, descártalo, podría tratarse de una estafa de phishing. SI BUSCAS una buena oferta, hazlo directamente en los sitios web oficiales de las tiendas comerciales. <p>CYBERDATO: Más de 100 millones de visitas se esperan para el Cyber Day en 2020 Verifica todas las webs oficiales en www.cyber.cl</p>

Revista Cibersucesos 3
<https://www.csirt.gob.cl/recomendaciones/revista-cibersucesos-n3/>



CIBER SUCESOS
Investigación, Tendencia y Concientización

EMPRENDEDORES Y DESARROLLOS INNOVADORES EN CIBERSEGURIDAD
No sólo se trata de buenas ideas

Cooperación Internacional
Tendencia Digital
Comunidad Hackers
Legal

11. Gestión de Cambios

Versión cambios	Fecha emisión	Autor cambios	Referencia, sección o capítulo modificado	Motivo de modificación
V 1.0	02/10/2020	Carlos Silva C.	Datos Iniciales.	Entrega de datos filtrados.
V 1.0	05/10/2020	Carlos Silva C.	Creación Informe.	Preparación Informe. Ajuste de formato.
V 1.0	05/10/2020	Katherina Canales	Aprobación.	Aprobación datos.
V 1.0	05/10/2020	Carlos Landeros	Aprobado	Aprobado

Tabla 7 - Gestión de cambios