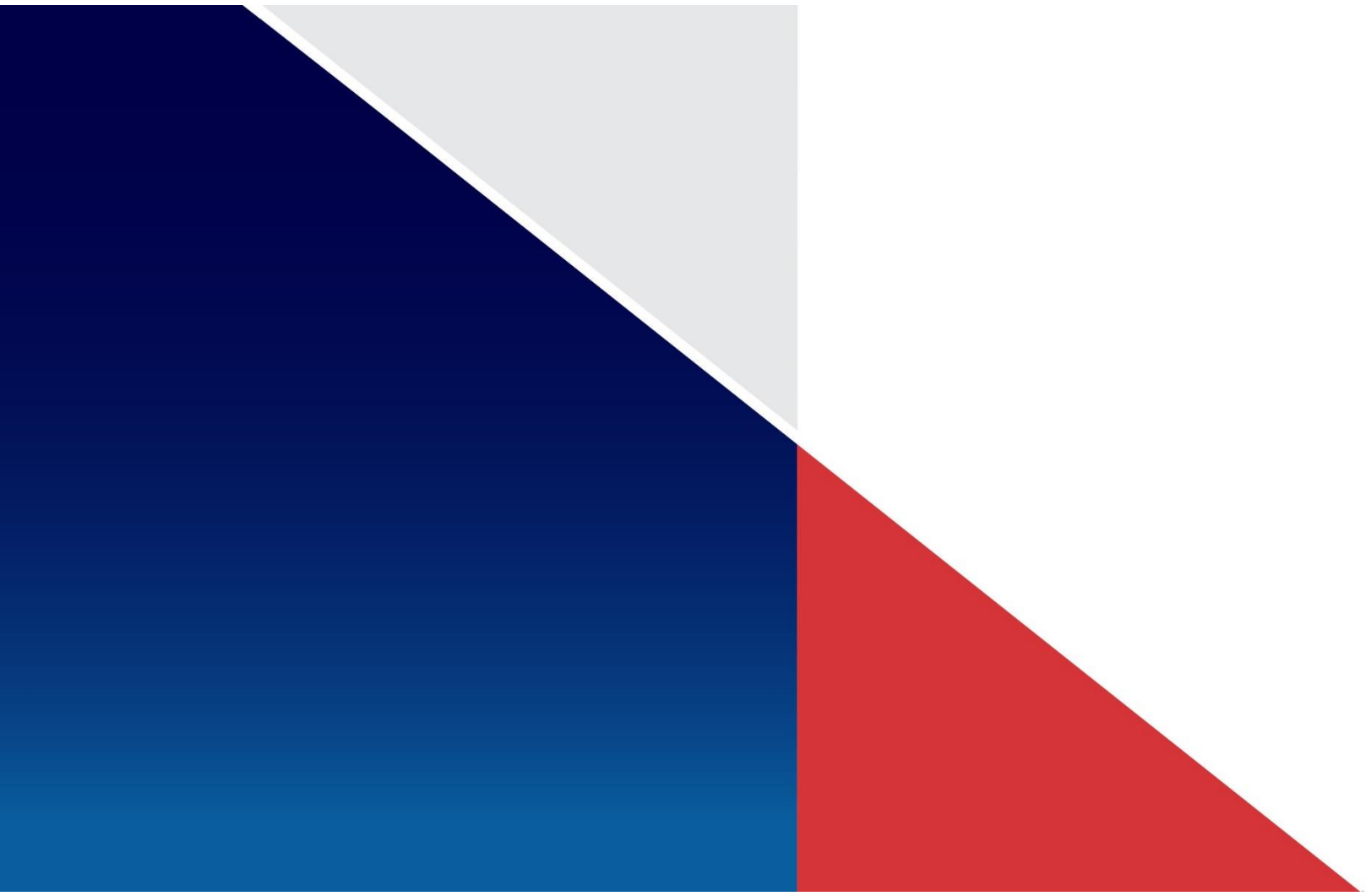
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Informe de Seguridad
“Gestión CSIRT Agosto 2019”
Ministerio del Interior y Seguridad Pública

Santiago, Agosto del 2019



Índice

Índice de Ilustraciones

Índice de Tablas

Resumen Ejecutivo

El presente informe contiene un resumen de la totalidad de los tickets procesados en el mes de agosto de 2019. 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 agosto 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 MISP[1] que contiene la cantidad de posibles IoCs[2] 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 IP[3] o a URL[4].

---

[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.

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 RCE[5] (falta cifrado, CMS obsoletos, credenciales recuperadas, servidores desactualizados, puertos expuestos, phishings, 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 -4.200 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.
- ✓ Monitoreo de los dispositivos de las gobernaciones e intendencias (WAN[6]).
- ✓ Monitoreo de los equipos y dispositivos con la plataforma Zenoss (RCE y WAN)
- ✓ 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

[6] WAN es una sigla en inglés que significa Wide Area Network, o "Red de Área Amplia" la cual corresponde a una red de computadoras que unifica varias redes locales, aunque algunos de sus miembros puedan estar en distintas locaciones físicas.

1. 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	Vulnerabilidades	9VSA	**388**
2	Phishing[7] Banco	8FPH	**164**
3	Operaciones Ciberseguridad CSIRT[8]	14IMT	**140**
4	Malware[9]	2CMV	**102**
5	Phishing Suplantación	8FPH	**79**
6	Defacement[10]	7SMN	**73**
7	Intrusión	5ICC	**7**
8	Ataque DDoS[11]	6DDS	**4**
9	Phishing Malware	8FPH	**0**
	TOTAL		**957**

Tabla 1 - Total Tipos de Tickets

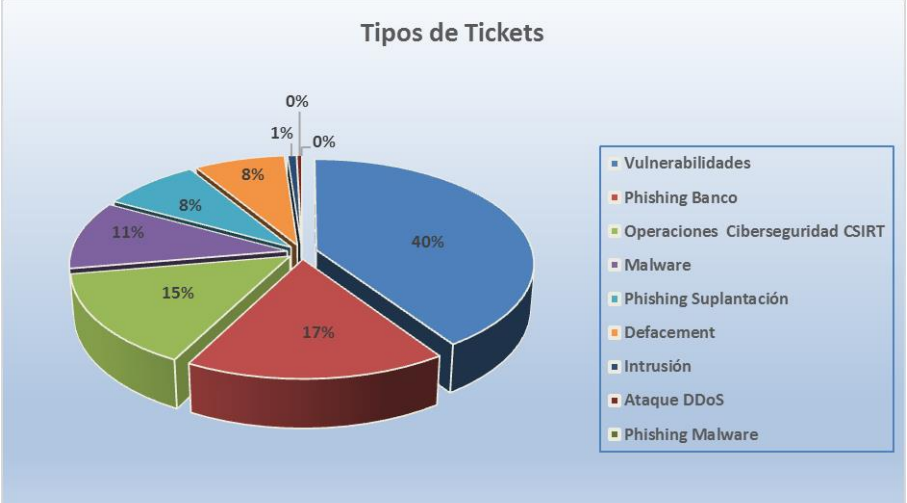


Ilustración 1 - Tipos de tickets

[7] Phishing: técnica de ingeniería social utilizada en ambientes informáticos por los delincuentes para obtener información confidencial como

nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.

[8] Aplicación de medidas de seguridad dentro de la Red de Conectividad del Estado.

[9] Malware: Amenaza o programación informática hostil.

[10] Defacement: Modificación sin autorización de una página web.

[11] DDOS: Denegación de servicio.

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 agosto, respecto del mes anterior.

Como se puede apreciar los tickets de las categorías "Vulnerabilidades, Phishing Banco, Defacement y Ataque DDoS" muestran una tendencia creciente al comparar ambos períodos, mientras que el resto de las categorías decrece en el mismo espacio de comparación, a excepción de la categoría "Phishing Suplantación" que no experimenta cambios entre ambas mediciones.

Cabe destacar que por segunda vez consecutiva las categorías de tickets de "Vulnerabilidades y Ataque DDoS" experimentan una tendencia creciente.

Al comparar el ranking de ambos períodos se puede observar que ambas mediciones presentan cambios en casi todas las posiciones, sólo las categorías de "Vulnerabilidades y Defacement" mantienen su ubicación en ambos períodos.

Los tipos de alertas que suben de posición corresponden a las categorías de "Ataque DDoS y Phishing Banco". Esta última categoría presenta una fuerte alza al subir seis posiciones en el ranking de agosto respecto a lo obtenido en el mes precedente, pasa de la octava a la segunda posición en el mes actual.

Por otro lado, las alertas que bajan en el ranking corresponden a las categorías de "Operaciones de Ciberseguridad CSIRT, Malware, Phishing Suplantación, Intrusión y Phishing Malware".

Ranking de Alertas Recibidas			
Julio 2019	**Agosto 2019**	**Tendencia**	**Cambio en el Ranking**
1.Vulnerabilidades	1.Vulnerabilidades	▲	→
2.Operaciones de Ciberseguridad CSIRT	2.Phishing Banco	▲	↑
3.Malware	3.Operaciones Ciberseguridad CSIRT	▼	↓
4.Phishing Suplantación	4.Malware	▼	↓
5.Intrusión	5.Phishing Suplantación	▶	↓
6.Defacement	6.Defacement	▲	→
7.Phishing Malware	7.Intrusión	▼	↓
8.Phishing Banco	8.Ataque DDoS	▲	↑
9.Ataque DDoS	9.Phishing Malware	▼	↓
Simbología			
Tendencia: ▼ Disminuye ; ▶ Constante ; ▲ Aumenta			
Ranking: ↓ Baja; → Igual; ↑Sube			

Tabla 2 - Ranking de Alertas Recibidas

2. Tipos de ticket públicos y/o privados

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

Tickets	Privado	Publico	Total
Vulnerabilidades	5	383	388
Phishing Banco	164	0	164
Operaciones CSIRT	22	118	140
Malware	9	93	102
Phishing Suplantación	76	3	79
Defacement	66	7	73
Intrusión	0	7	7
Ataque DDoS	1	3	4
Phishing Malware	0	0	0
TOTAL	**343**	**614**	**957**

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.

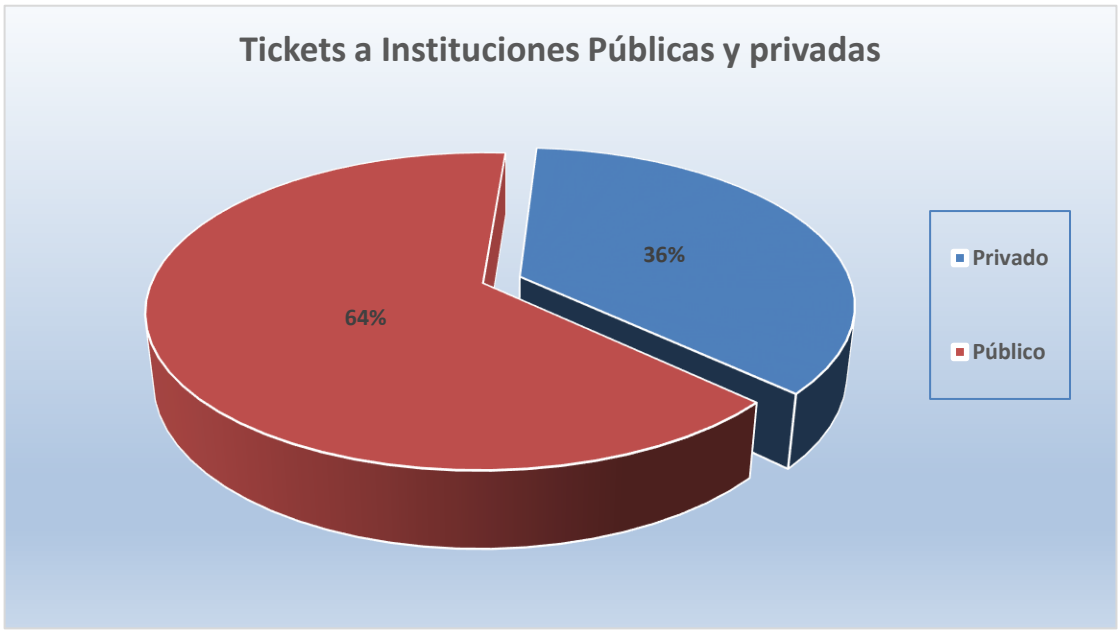


Ilustración 2 - Tickets a Instituciones Públicas y Privadas

3. 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 agosto de 2019. Como se puede apreciar la cantidad de tickets abiertos o generados en el período son un total de 957 unidades. De este total, 572 tickets fueron cerrados, lo que representa un 60% de eficacia, mientras 385 tickets (40%) siguen en desarrollo para terminar de ser procesados en los períodos siguientes.

El porcentaje de eficacia baja respecto a lo obtenido en el mes pasado, pasa de un 77% a 60% en el presente mes. Pero, al mirar la cantidad de tickets cerrados en agosto se observa que en realidad estos aumentaron en un 6% respecto a lo obtenido en el mes precedente. Por lo tanto, la disminución del porcentaje de eficacia no se explica por una baja de productividad, sino que se debe a que también aumentó la cantidad total de tickets generados en agosto en un 36% -la base de comparación es mucho mayor- y es por esta razón que se reduce el porcentaje de eficacia.

Total Estado ticket	Suma total
En desarrollo	385
Cerrados	572
Total general	**957**

Tabla 4 - Total Estado de Tickets

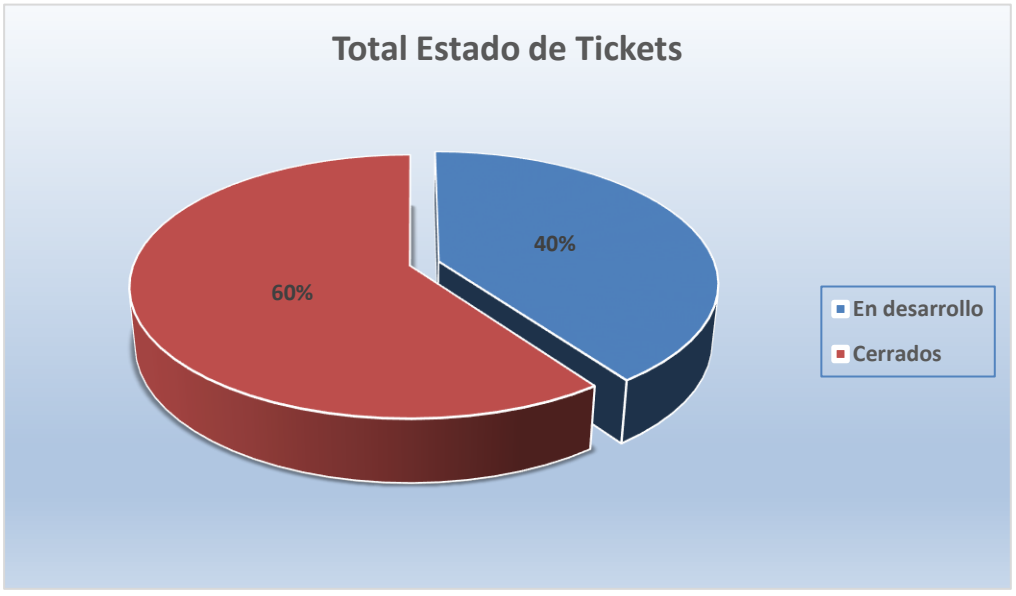


Ilustración 3 - Total Estado de Tickets

4. 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 agosto de 2019.

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, 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	679
Servicios Externos	278
Total Fuentes de Tickets	**957**

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

Como se puede observar en el siguiente gráfico, un 71% de la demanda de trabajo que recibe CSIRT en el pasado mes de agosto tiene un origen interno, mientras que el 29% restante proviene de fuentes externas

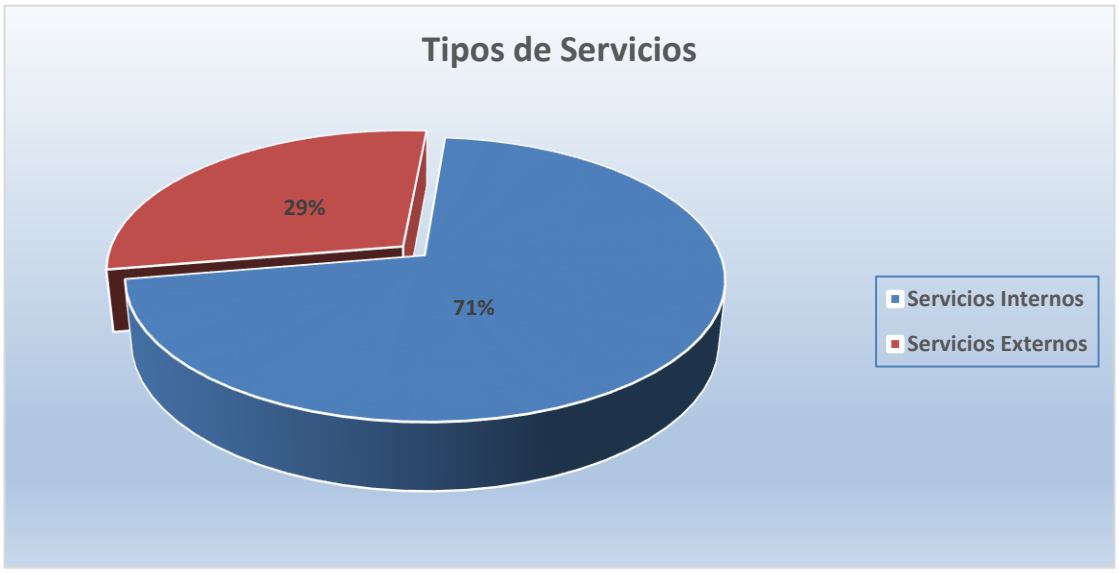


Ilustración 4 - Distribución Porcentual de Origen de Tickets

5. 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 de procedencia durante el pasado mes de agosto.

Fuentes de Origen Externo de Tickets	Cantidad de Tickets
Tickets generados por privados vía call center	0
Tickets generados por privados vía formulario web	38
Tickets generados por privados vía email	16
Tickets generados por información de otros CSIRT internacionales	0
Tickets generados por información entregada por empresas privadas que prestan servicio al CSIRT	181
Tickets generados por información entregada por empresas privadas que no prestan servicio al CSIRT	43
Total	**278**

Tabla 6 - Fuentes de Origen Externo de Tickets

En agosto de 2019, el siguiente gráfico de distribución muestra que el mayor porcentaje de tickets externos son generados por reportes entregados por "Empresas privadas con convenio de ciberseguridad", con un 65% de participación. En segundo lugar, se ubican aquellos tickets que provienen de "Empresas privadas sin convenio de ciberseguridad" con un 15% de contribución y, en tercer lugar, con un porcentaje de un 14% de incidencia, se encuentran los tickets que se originan a través de formulario web.

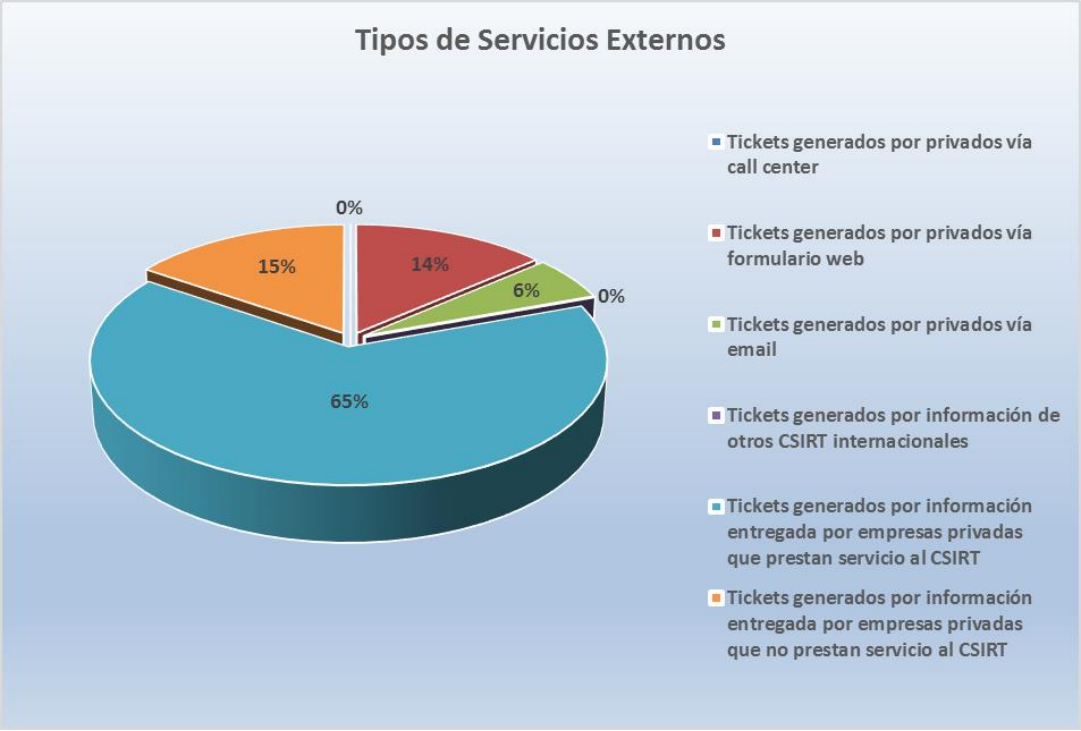


Ilustración 5 - Distribución Porcentual de Fuentes Externas de Tickets

6. Índice de Compromiso detectados en el presente mes

La siguiente tabla expone la cantidad de eventos en la plataforma MISP[12] que se han detectado en el reciente mes de Agosto. A partir de este mes también se han incluido los datos de todos los índices detectados por CSIRT que se han incorporado a su sistema de seguridad.

Mes correspondiente	Cantidad
Mayo	26
Junio	11
Julio	7
Agosto	277
Total	**321**

Tabla 7 - Eventos detectados

12 Plataforma en funcionamiento desde el 20 de abril de 2019.

7. Gestión de Cambios

Versión cambios	Fecha emisión	Autor cambios	Referencia, sección o capítulo modificado	Motivo de modificación
V 1.0	03/09/2019	Carlos Ramos B.	- Datos Iniciales.	- Entrega de datos filtrados.
V 1.0	03/09/2019	Carlos Ramos B.	- Creación Informe.	- Preparación Informe. - Ajuste de formato.
V 1.0	03/09/2019	Alejandro Palacios	- Aprobación.	- Aprobación datos.
V.2.0	05/09/2019	Carlos Landeros	- Aprobado	- Aprobado

Tabla 8 Gestión de cambios