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

Equipo CSIRT-RCE

Santiago, junio de 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 junio 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 actual 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 e 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	Total
1	Red RCE	180
2	Vulnerabilidades	125
3	Malware	52
4	Phishing Malware	47
5	Defacement	43
6	Otros	28
7	Phishing Banco	18
8	Phishing Suplantación	4
9	Ataque DDoS	0

Tabla 1 - Total Tipos de Tickets

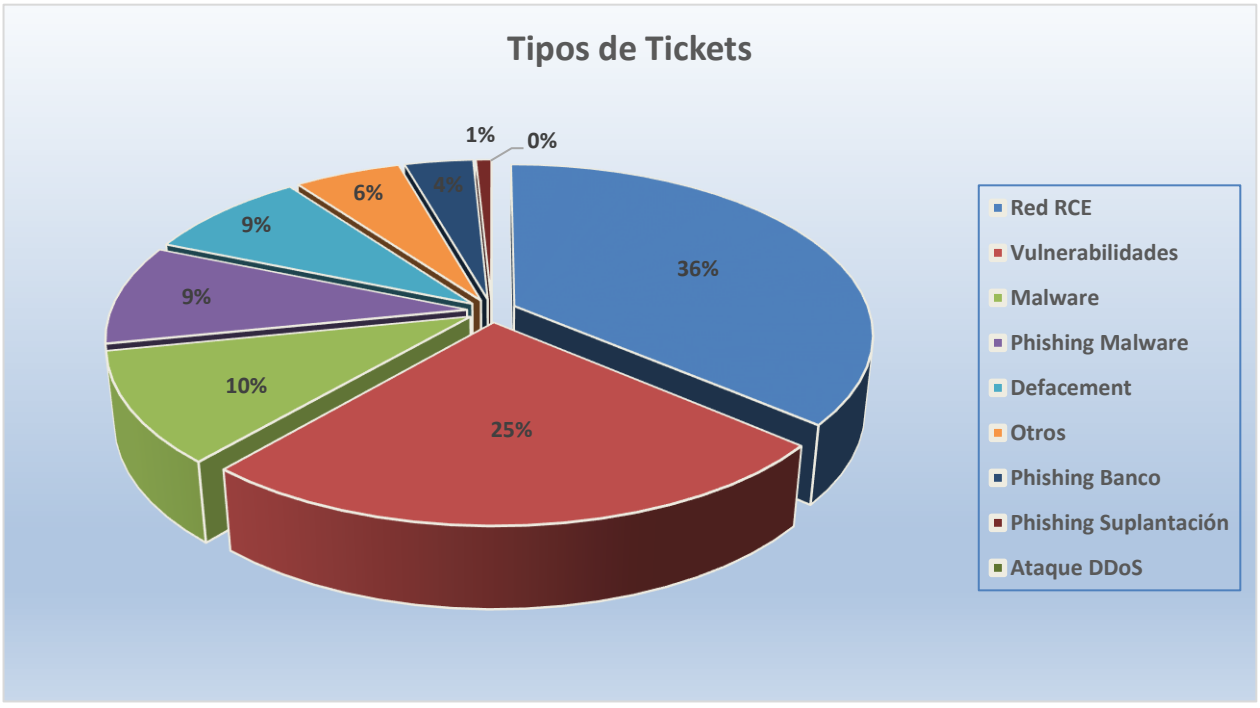

Ilustración 1 - Tipos de tickets

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 junio, respecto del mes anterior.

Como se puede apreciar los tickets de las categorías "Red RCE, Vulnerabilidades, Phishing Malware, Otros y Phishing Banco" muestran una tendencia creciente al comparar ambos períodos, mientras que el resto de las categorías decrece en el mismo espacio de comparación.

Sin embargo, cuándo se compara el ranking de los tipos de tickets generados en junio respecto de lo obtenido en el mes precedente se puede observar que ambas mediciones son relativamente estables y presentan pocas modificaciones.

Sólo cambia la categoría "Phishing Malware" que sube dos posiciones, al pasar del sexto lugar a la cuarta posición; mientras que, al mismo tiempo, los tickets de las categorías "Defacement y Otros" muestran un retroceso al bajar ambas categorías un puesto respecto del lugar obtenido en la medición anterior.

Ranking de Alertas Recibidas			
Mayo 2019	**Junio 2019**	**Tendencia**	**Cambio en el Ranking**
1.Red RCE	1.Red RCE	▲	→
2.Vulnerabilidades	2.Vulnerabilidades	▲	→
3.Malware	3.Malware	▼	→
4.Defacement	4.Phishing Malware	▲	↑
5.Otros	5.Defacement	▼	↓
6.Phishing Malware	6.Otros	▲	↓
7.Phishing Banco	7.Phishing Banco	▲	→
8.Phishing Suplantación	8.Phishing Suplantación	▼	→
9.Ataque DDoS	9.Ataque DDoS	▼	→
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
Red RCE	0	180	180
Vulnerabilidades	11	114	125
Malware	2	50	52
Phishing Malware	44	3	47
Defacement	41	2	43
Otros	1	27	28
Phishing Banco	11	7	18
Phishing Suplantación	3	1	4
Ataque DDoS	0	0	0
TOTAL	113	384	497

Tabla 3 - Tickets a Instituciones Públicas y Privadas

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

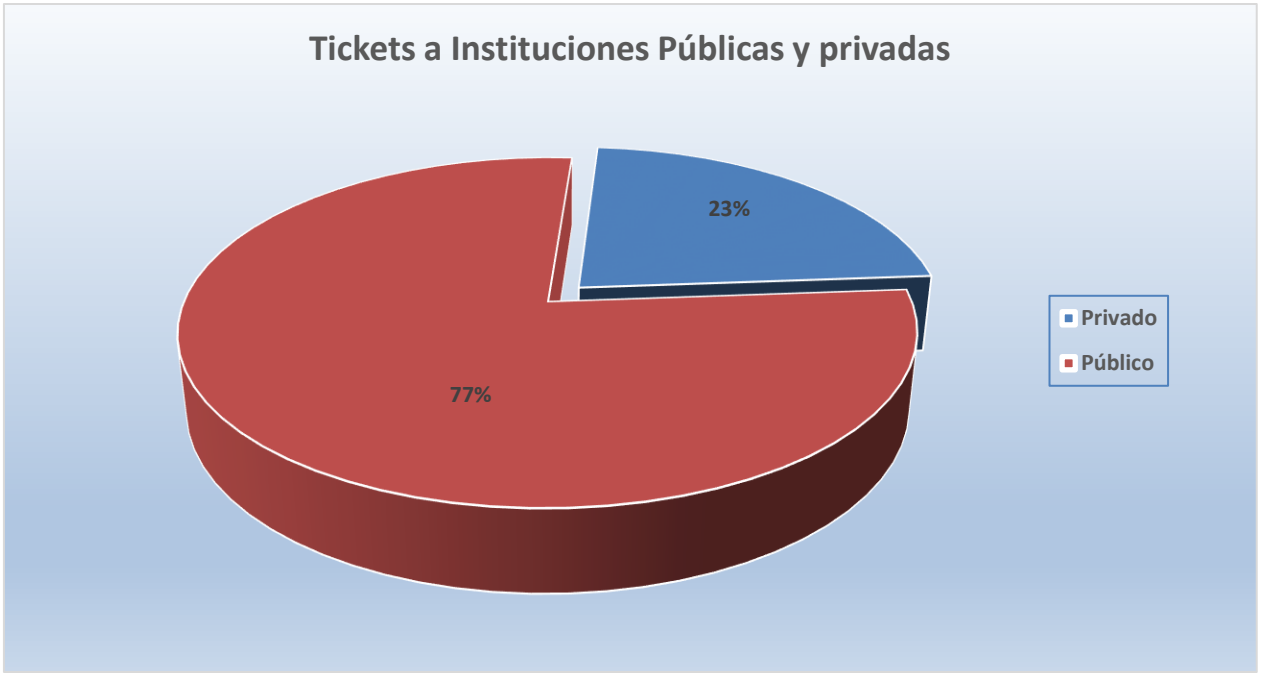

Ilustración 2 - Tickets a Instituciones Públicas y Privadas

3. Estado de ticket procesados en el presente mes

En la siguiente tabla y gráfico de torta se muestra el estado de los tickets procesados en el mes de junio de 2019. Como se puede apreciar la cantidad de tickets abiertos o generados en el período son un total de 497 unidades. De este total, 257 tickets fueron cerrados con éxito, lo que representa un 52% de eficacia, mientras 240 tickets (48%) quedaron abiertos para terminar de ser procesados en los períodos siguientes.

Total Estado ticket	Suma total
Total Abiertos	240
Total Cerrados con Éxito	257
Total general	497

Tabla 4 - Total Estado de Tickets

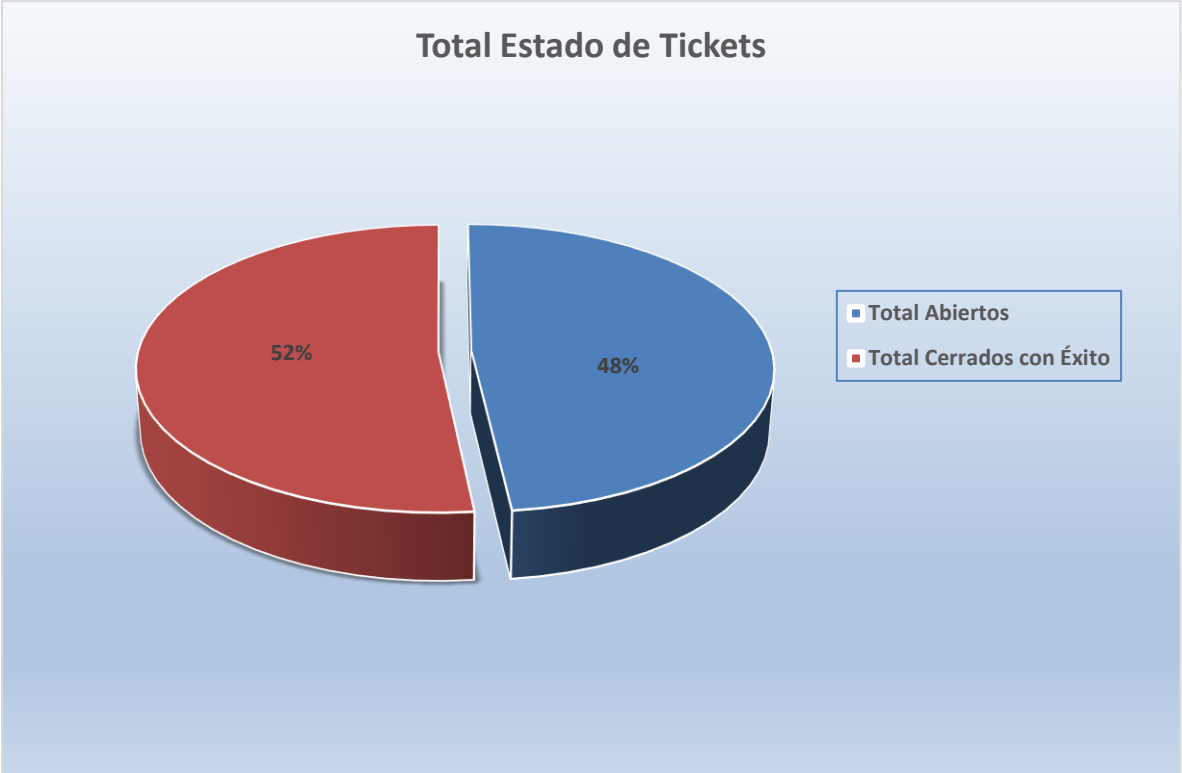

Ilustración 3 - Total Estado de Tickets

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 junio 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	332
Servicios Externos	165
Total Fuentes de Tickets	497

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

Como se puede observar en el siguiente gráfico, un 67% de la demanda de trabajo que recibe CSIRT en el pasado mes de junio tiene un origen interno, mientras que el 33% restante proviene de fuentes externas.

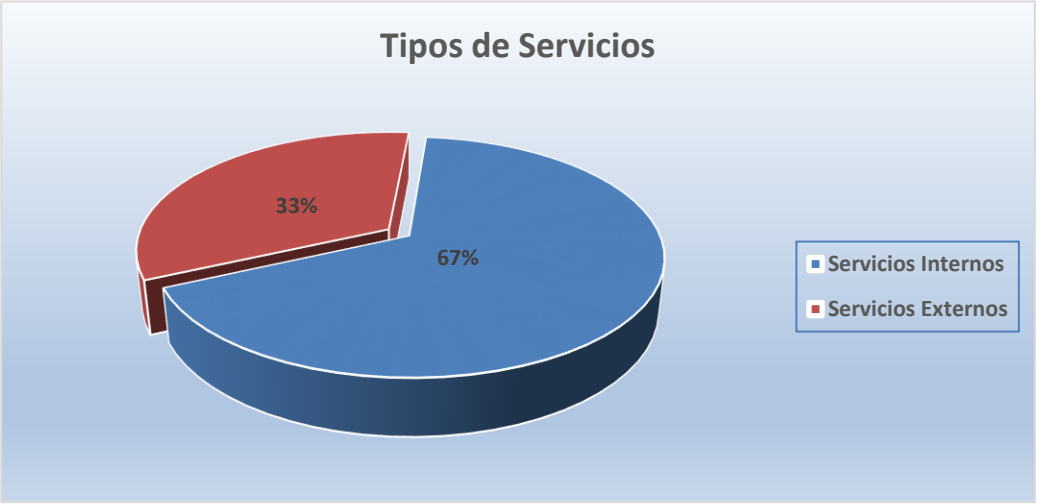

Ilustración 4 - Distribución Porcentual de Origen de Tickets

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 junio.

Fuentes de Origen Externo de Tickets	Cantidad de Tickets
Tickets generados por privados vía call center	0
Tickets generados por privados vía formulario web	11
Tickets generados por privados vía email	20
Tickets generados por información de otros CSIRT internacionales	1
Tickets generados por información entregada por empresas privadas que prestan servicio al CSIRT	91
Tickets generados por información entregada por empresas privadas sin convenio de ciberseguridad	42
Total	165

Tabla 6 - Fuentes de Origen Externo de Tickets

En junio de 2019, el siguiente gráfico de distribución muestra que el mayor porcentaje de tickets externos son generados por reportes entregados por "Empresas privadas que prestan servicio al CSIRT", con un 55% de participación. En segundo lugar, se ubican aquellos tickets que provienen de "Empresas privadas sin convenio de ciberseguridad" con un 25% de contribución y, en tercer lugar, con un porcentaje de un 12%, se encuentran los tickets que se originan a través de vía email.

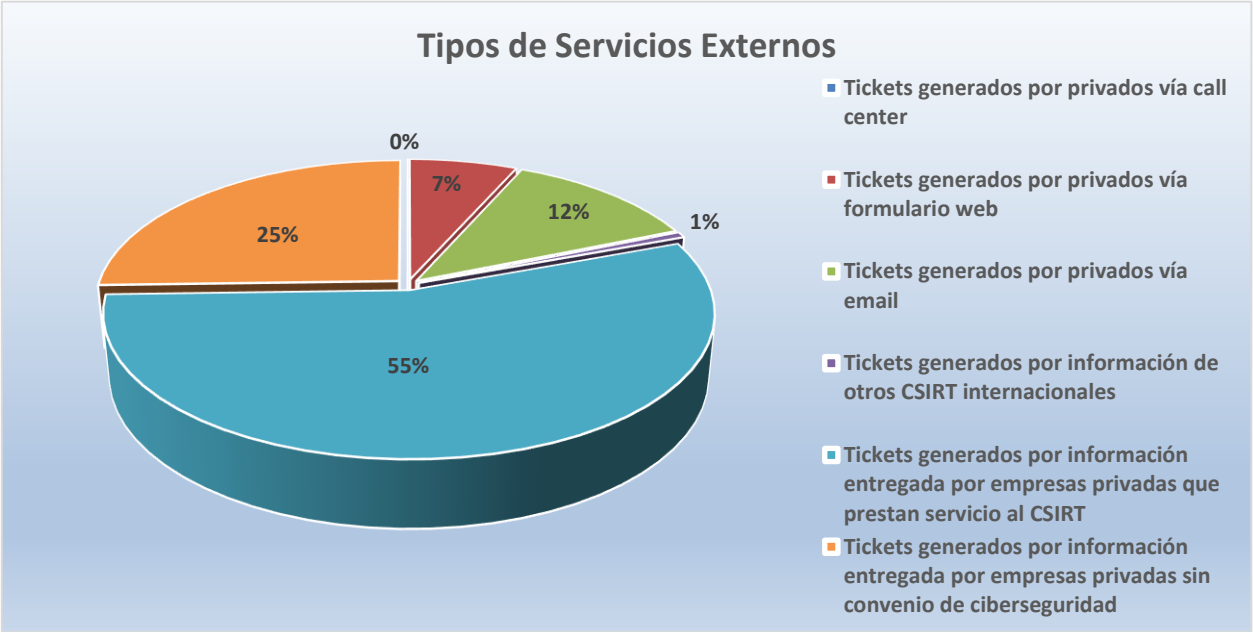

Ilustración 5 - Distribución Porcentual de Fuentes Externas de Tickets

6. Índice de Compromiso detectados en el presente mes

La siguiente tabla expone la cantidad de eventos en la plataforma MISP que se han detectado en el reciente mes de Junio (plataforma en funcionamiento el 20 de abril de 2019).

Mes correspondiente	Cantidad
Mayo	26
Junio	11
Total	37

Tabla 7 - Eventos detectados

7. Gestión de Cambios

Versión cambios	Fecha emisión	Autor cambios	Referencia, sección o capítulo modificado	Motivo de modificación
V 1.0	02/07/2019	Carlos Ramos B.	- Creación Informe.	- Preparación Informe. - Ajuste de formato.
V 1.0	02/07/2019	Carlos Ramos B.	- Datos iniciales	- Entrega de datos filtrados.
V 1.0	02/07/2019	Alejandro Palacios	- Aprobación	- Aprobación datos

Tabla 7 - Tabla gestión de cambios