

**SECURESOFT CORPORATION**

**e-Secure Consulting Group**

**REPORTE SEMANAL - SALUD**

### Preparado para:



**Fecha de elaboración:**

**${fecha\_actual}**

**El presente documento contiene información estrictamente privada y confidencial entre SECURESOFT CORPORATION**

**S.A.C. y LA POSITIVA.**

**INDICE**

[**Preparado para: 1**](#_Toc88649539)

[**I. OBJETIVO 3**](#_Toc88649540)

[**II. ALCANCES 3**](#_Toc88649541)

[**III. ESTADO DE LAS PLATAFORMAS 3**](#_Toc88649542)

[**1. FIREWALL 3**](#_Toc88649543)

[**1.1 FGTAWSLP\_MASTER – Recursos 3**](#_Toc88649544)

[**1.2 FGTAWSLP\_SLAVE – Recursos 4**](#_Toc88649545)

[**1.3 FGTINTCOT4LP\_MASTER – Recursos 4**](#_Toc88649546)

[**1.4 FGTPERCOT4LP\_MASTER– Recursos 5**](#_Toc88649547)

[**2. PROXY 5**](#_Toc88649548)

[**2.1. Proxy McAfee - proxywg01 5**](#_Toc88649549)

[**2.2. Proxy McAfee - proxywg03 6**](#_Toc88649550)

[**3. BIG IP 7**](#_Toc88649551)

[**3.1. bigipExtCOT1 - BIG IP 7**](#_Toc88649552)

[**3.2. vbigipExtCOT4 - BIG IP 8**](#_Toc88649553)

[**4. IMPERVA COT4 9**](#_Toc88649554)

[**4.1. MGT 9**](#_Toc88649555)

[**4.2. GWT 01 11**](#_Toc88649556)

[**4.3. GWT 02 13**](#_Toc88649557)

[**5. IMPERVA COT1 15**](#_Toc88649558)

[**5.1. MX02 COT1 15**](#_Toc88649559)

[**5.2. GW03 COT1 16**](#_Toc88649560)

[**IV. TICKETS REPORTADOS 17**](#_Toc88649561)

[**V. CONCLUSIONES 17**](#_Toc88649562)

# OBJETIVO

Este documento dará a conocer el estado de las plataformas de salud durante la última semana.

# ALCANCES

Este documento servirá como herramienta para verificar el estado de las plataformas y su correcto funcionamiento.

# ESTADO DE LAS PLATAFORMAS

## FIREWALL

### FGTAWSLP\_MASTER – Recursos

${graph1046}

* *Se observó un uso de CPU de* ***0%*** *durante el transcurso de la semana.*
* *Se observó un uso de Disco de* ***740 KB*** *durante el transcurso de la semana.*
* *Se observó un uso de Memoria de* ***15%*** *durante el transcurso de la semana.*

### FGTAWSLP\_SLAVE – Recursos

${graph1037}

* *No se observó un uso de CPU durante el transcurso de la semana.*
* *Se observó un uso de Disco de* ***704 KB*** *durante el transcurso de la semana.*
* *Se observó un uso de Memoria de* ***13.99%*** *durante el transcurso de la semana.*

### FGTINTCOT4LP\_MASTER – Recursos

${graph886}

* *Se observó un uso de CPU de* ***2.19%*** *durante el transcurso de la semana.*
* *No se observó un uso de Disco durante el transcurso de la semana.*
* *Se observó un uso de Memoria de* ***31.76%*** *durante el transcurso de la semana.*

### FGTPERCOT4LP\_MASTER– Recursos

${graph880}

* *Se observó un uso de CPU de* ***2.92%*** *durante el transcurso de la semana.*
* *No se observó un uso de Disco durante el transcurso de la semana.*
* *Se observó un uso de Memoria de* ***45.23%*** *durante el transcurso de la semana.*

## PROXY

### Proxy McAfee - proxywg01

* **Recursos**

${graph1011}

* *Se observó un uso de CPU de* ***1.28%*** *durante el transcurso de la semana.*
* *Se observó un uso de Memoria de* ***31.05%*** *durante el transcurso de la semana.*
* **Concurrencias**

${graph868}

* *Se observó* ***1.87******K*** *conexiones durante el transcurso de la semana.*

### Proxy McAfee - proxywg03

* **Recursos**

${graph1012}

* *Se observó un uso de CPU de* ***0.46%*** *durante el transcurso de la semana.*
* *Se observó un uso de Memoria de* ***8%*** *durante el transcurso de la semana.*
* **Conexiones concurrentes**

${graph864}

* *Se observó* ***979.99 k*** *conexiones durante el transcurso de la semana.*

## BIG IP

### vbigipExtCOT1 - BIG IP

* **Recursos**

${graph944}

* *Se observó un uso de Disco de* ***24%*** *durante el transcurso de la semana.*
* *Se observó un uso de Memoria de* ***4%*** *durante el transcurso de la semana.*
* *Se observó un uso de CPU del* ***7.98%*** *durante el transcurso de la semana.*
* **Conexiones concurrentes**

${graph946}

* *Se observó* ***260.02*** *k conexiones durante el transcurso de la semana.*

### vbigipExtCOT4 - BIG IP

* **Recursos**

${graph981}

* *Se observó un uso de Disco del* ***24%*** *durante el transcurso de la semana.*
* *Se observó un uso de Memoria de* ***4%*** *durante el transcurso de la semana.*
* *Se observó un uso de CPU de* ***10.14%*** *durante el transcurso de la semana.*
* **Conexiones concurrentes**

${graph983}

* *Se observó* ***582.34 k*** *conexiones durante el transcurso de la semana.*

## IMPERVA COT4

### MGT

* **Recursos**

${graph1020}

* *Se observó un uso de CPU del* ***2.45%*** *durante el transcurso de la semana.*
* *Se observó un uso de Memoria de* ***93.82%*** *durante el transcurso de la semana.*
* *Se observó un uso de Disco de* ***61.38%*** *durante el transcurso de la semana.*
* **Conexiones concurrentes**

${graph1021}

* *Se observó* ***66.23 k*** *conexiones durante el transcurso de la semana.*
* **Throughput**

${graph1033}

* *La interfaz* ***eth0*** *tuvo un promedio de* ***1.48 kbps*** *de tráfico entrante durante el último día.*
* *La interfaz* ***eth0*** *tuvo un promedio de* ***196.2 Kbps*** *de tráfico saliente durante el último día.*
* *La interfaz* ***eth1*** *no se visualiza tráfico entrante.*
* *La interfaz* ***eth1*** *no se visualiza tráfico saliente.*
* *La interfaz* ***Io*** *tuvo un promedio de* ***7.09 Mbps*** *de tráfico entrante durante el último día.*
* *La interfaz* ***Io*** *tuvo un promedio de* ***7.09 Mbps*** *de tráfico saliente durante el último día.*

### GWT 01

* **Recursos**

${graph1022}

* *Se observó un uso de CPU del* ***0.12%*** *durante el transcurso de la semana.*
* *Se observó un uso de Memoria de* ***74.83%*** *durante el transcurso de la semana.*
* *Se observó un uso de Disco de* ***36.44%*** *durante el transcurso de la semana.*
* **Conexiones concurrentes**

${graph1023}

* *Se observó* ***0.01 k*** *conexiones durante el transcurso de la semana.*
* **Throughput**

${graph1029}

* *La interfaz* ***eth0*** *tuvo un promedio de* ***14.39 Kbps*** *de tráfico entrante durante el último día.*
* *La interfaz* ***eth0*** *tuvo un promedio de* ***25.41 Kbps*** *de tráfico saliente durante el último día.*
* *La interfaz* ***eth1*** *no se visualiza tráfico entrante.*
* *La interfaz* ***eth1*** *no se visualiza tráfico saliente.*
* *La interfaz* ***eth2*** *tuvo un promedio de* ***113.57 bps*** *de tráfico entrante durante el último día.*
* *La interfaz* ***eth2*** *tuvo un promedio de* ***928.11 Kbps*** *de tráfico saliente durante el último día.*
* *La interfaz* ***eth3*** *tuvo un promedio de* ***929.85 Kbps*** *de tráfico entrante durante el último día.*
* *La interfaz* ***eth3*** *tuvo un promedio de* ***113.57 bps*** *de tráfico saliente durante el último día.*
* *La interfaz* ***Io*** *tuvo un promedio de* ***374.72 bps*** *de tráfico entrante durante el último día.*
* *La interfaz* ***Io*** *tuvo un promedio de* ***374.72 bps*** *de tráfico saliente durante el último día.*
* *La interfaz* ***Tap0*** *no se visualiza tráfico entrante.*
* *La interfaz* ***Tap0*** *no se visualiza tráfico saliente.*

### GWT 02

* **Recursos**

${graph1024}

* *Se observó un uso de CPU del* ***19.70%*** *durante el transcurso de la semana.*
* *Se observó un uso de Memoria de* ***95.23%*** *durante el transcurso de la semana.*
* *Se observó un uso de Disco de* ***49%*** *durante el transcurso de la semana.*
* **Conexiones concurrentes**

**${graph1025}**

* *Se observó* ***7.17*** *k conexiones durante el transcurso de la semana.*
* **Throughput**

${graph1030}

* *La interfaz* ***eth0*** *tuvo un promedio de* ***75.81 Mbps*** *de tráfico entrante durante el último día.*
* *La interfaz* ***eth0*** *tuvo un promedio de* ***3.21 Mbps*** *de tráfico saliente durante el último día.*
* *La interfaz* ***eth1*** *no se visualiza tráfico entrante.*
* *La interfaz* ***eth1*** *no se visualiza tráfico saliente.*
* *La interfaz* ***eth2*** *tuvo un promedio de* ***157.94 Mbps*** *de tráfico entrante durante el último día.*
* *La interfaz* ***eth2*** *tuvo un promedio de* ***207.01 Mbps*** *de tráfico saliente durante el último día.*
* *La interfaz* ***eth3*** *tuvo un promedio de* ***207.13 Mbps*** *de tráfico entrante durante el último día.*
* *La interfaz* ***eth3*** *tuvo un promedio de* ***157.9 Mbps*** *de tráfico saliente durante el último día.*
* *La interfaz* ***eth4*** *tuvo un promedio de* ***412.08 Mbps*** *de tráfico entrante durante el último día.*
* *La interfaz* ***eth4*** *tuvo un promedio de* ***100.55 Mbps*** *de tráfico saliente durante el último día.*
* *La interfaz* ***eth5*** *tuvo un promedio de* ***100.58 Mbps*** *de tráfico entrante durante el último día.*
* *La interfaz* ***eth5*** *tuvo un promedio de* ***412.19 Mbps*** *de tráfico saliente durante el último día.*
* *La interfaz* ***Io*** *tuvo un promedio de* ***362.82 bps*** *de tráfico entrante durante el último día.*
* *La interfaz* ***Io*** *tuvo un promedio de* ***362.82 bps*** *de tráfico saliente durante el último día.*
* *La interfaz* ***Tap0*** *no se visualiza tráfico entrante.*
* *La interfaz* ***Tap0*** *no se visualiza tráfico saliente.*

## IMPERVA COT1

### MX02 COT1

* **Recursos**

${graph1063}

* *Se observó un uso de CPU del* ***1****% durante el transcurso de la semana.*
* *Se observó un uso de Memoria de* ***88.28%*** *durante el transcurso de la semana.*
* *Se observó un uso de Disco de* ***49.47%*** *durante el transcurso de la semana.*
* **Conexiones concurrentes**

**${graph1061}**

* *Se observó* ***42.87 k*** *conexiones durante el transcurso de la semana.*
* **Throughput**

${graph1068}

* *La interfaz* ***eth0*** *tuvo un promedio de* ***75.81 kbps*** *de tráfico entrante durante el último día.*
* *La interfaz* ***eth0*** *tuvo un promedio de* ***3.21 kbps*** *de tráfico saliente durante el último día.*
* *La interfaz* ***eth1*** *no se visualiza tráfico entrante.*
* *La interfaz* ***eth1*** *no se visualiza tráfico saliente.*

### GW03 COT1

* **Recursos**

${graph1064}

* *Se observó un uso de CPU del* ***0.05%*** *durante el transcurso de la semana.*
* *Se observó un uso de Memoria de* ***64.52%*** *durante el transcurso de la semana.*
* *Se observó un uso de Disco de* ***49.66%*** *durante el transcurso de la semana.*
* *Se observa cortes en la gráfica, debido a pérdida ICMP Se notificó en el* ***INC 242456.***
* **Conexiones concurrentes**

**${graph1062}**

* *Se observó* ***0.83 k*** *conexiones durante el transcurso de la semana.*
* **Throughput**

${graph1067}

* *La interfaz* ***eth1*** *no se visualiza tráfico entrante.*
* *La interfaz* ***eth1*** *no se visualiza tráfico saliente.*
* *La interfaz* ***eth2*** *tuvo un promedio de* ***1.79 kbps*** *de tráfico entrante durante el último día.*
* *La interfaz* ***eth2*** *tuvo un promedio de* ***199.22 bps*** *de tráfico saliente durante el último día.*
* *La interfaz* ***eth3*** *tuvo un promedio de* ***192.22 bps*** *de tráfico entrante durante el último día.*
* *La interfaz* ***eth3*** *tuvo un promedio de* ***1.79 kbps*** *de tráfico saliente durante el último día.*
* *La interfaz* ***eth4*** *no se visualiza tráfico entrante.*
* *La interfaz* ***eth4*** *no se visualiza tráfico saliente.*
* *La interfaz* ***eth5*** *no se visualiza tráfico entrante.*
* *La interfaz* ***eth5*** *no se visualiza tráfico saliente.*
* *La interfaz* ***Io*** *tuvo un promedio de* ***319.01 bps*** *de tráfico entrante durante el último día.*
* *La interfaz* ***Io*** *tuvo un promedio de* ***319.01 bps*** *de tráfico saliente durante el último día.*
* *La interfaz* ***Tap0*** *no se visualiza tráfico entrante.*
* *La interfaz* ***Tap0*** *no se visualiza tráfico saliente.*

# TICKETS REPORTADOS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **N° Ticket** | **Prioridad** | **Categoria** | **Fecha/hora apertura** | **Resumen** |
|  |  |  |  |  |

# CONCLUSIONES

* Se observa que los recursos de las gráficas son estables.
* Se observa algunas gráficas se encuentran con data incompleta debido a la reciente integración de los equipos a nuestra plataforma de monitoreo.
* Se observa data de los **Throughput** durante el transcurso de la semana.
* Se observa un alto consumo de memoria en los equipos **IMPERVA**, se indicó que son consumos normales por sus procesos locales.
* Se observa cortes en la gráfica del equipo **IMPERVA - GW03 - COT1** debido a pérdida ICMP Se notificó en el **INC 242456.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CONTROL DE CAMBIOS** | | | | |
| **Revisión** | **Hecha por** | **Aprobada por** | **Fecha** | **Motivo** |
| 00 | ${autor} | Supervisor CyberSOC | 12/01/2022 | Versión Inicial |