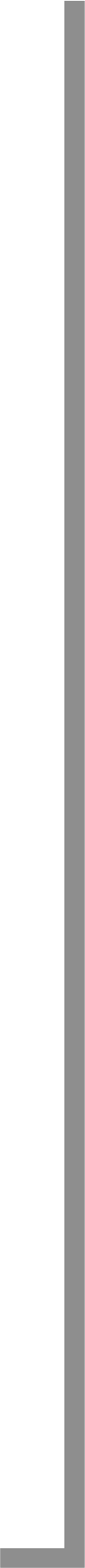
**SECURESOFT CORPORATION**



**e-Secure Consulting Group**

**REPORTE DIARIO**

**ESTADO DE SALUD**

**Preparado para:**



**Fecha:**

**${fecha\_dia\_antes}**



**El presente documento contiene información estrictamente privada y confidencial para SECURESOFT CORPORATION S.A.C. y BANCO PICHINCHA S.A.**

INDICE

[I. OBJETIVO 3](#_Toc93125607)

[II. ALCANCES 3](#_Toc93125608)

[III. CAPACIDAD TOTAL DE LOS EQUIPOS 3](#_Toc93125609)

[IV. ESTADO DE PLATAFORMAS 4](#_Toc93125610)

[**1.** **FIREWALLS CHECKPOINT** 4](#_Toc93125611)

[**1.1.** **FIREWALL BASADRE (172.19.64.2)** 4](#_Toc93125612)

[**1.2.** **IREWALL DINERS (172.19.210.2)** 5](#_Toc93125613)

[**2.** **BALANCEADOR F5 (172.16.1.249)** 6](#_Toc93125614)

[**3.** **FIREWALLS PALO ALTO** 7](#_Toc93125615)

[**3.1.** **PANORAMA (172.16.2.155)** 7](#_Toc93125616)

[**3.2.** **CLÚSTER INTERNO** 8](#_Toc93125617)

[**A.** **FIREWALL INTERNO 01 (172.17.23.25)** 8](#_Toc93125618)

[**B.** **FIREWALL INTERNO 02 (172.17.23.26)** 9](#_Toc93125619)

[**3.3.** **CLÚSTER PERIMETRAL** 10](#_Toc93125620)

[ **Certificados** 10](#_Toc93125621)

[**A.** **FIREWALL PERIMETRAL 01 (172.17.23.20)** 11](#_Toc93125622)

[**B.** **FIREWALL PERIMETRAL 02 (172.17.23.21)** 12](#_Toc93125623)

[**4.** **PROXY MCAFEE** 13](#_Toc93125624)

[**4.1.** **FILTRO WEB - PROXY 01 (172.16.1.78)** 13](#_Toc93125625)

[**4.2.** **FILTRO WEB - PROXY 02 (172.16.1.79)** 13](#_Toc93125626)

[**4.3.** **PROXY REPORTER (172.16.2.128)** 14](#_Toc93125627)

[**5.** **FORTIANALIZER CARSA (172.31.5.252)** 14](#_Toc93125628)

[**6.** **FIREWALL CARSA – FORTINET (172.31.5.254)** 15](#_Toc93125629)

[**7.** **CITRIX** 16](#_Toc93125630)

[**7.1.** **BALACEADOR DDOS ACTIVO (172.17.23.32)** 16](#_Toc93125631)

[**7.2.** **BALACEADOR DDOS PASIVO (172.17.23.33)** 16](#_Toc93125632)

[**8.** **IBM** 17](#_Toc93125633)

[**8.1.** **OPTIM (172.16.1.197)** 17](#_Toc93125634)

[**8.2.** **QRADAR (172.16.1.210)** 17](#_Toc93125635)

[**8.3.** **GUARDIUM (172.16.1.231)** 19](#_Toc93125636)

[**9.** **MCAFEE (172.17.23.29)** 19](#_Toc93125637)

[**9.1.** **ATD** 19](#_Toc93125638)

[**9.2.** **TIE (172.16.2.153)** 20](#_Toc93125639)

[**9.3.** **Antivirus ePo (172.16.1.229)** 20](#_Toc93125640)

[V. RESUMEN DE LOS EVENTOS 21](#_Toc93125641)

[VI. DETALLE DEL EVENTO 21](#_Toc93125642)

[VII. CONCLUSIONES 21](#_Toc93125643)

[VIII. ESTATUS DE LOS TICKETS REPORTADOS 22](#_Toc93125644)

1. **OBJETIVO**

Este documento dará a conocer el estado de salud de plataformas de seguridad.

1. **ALCANCES**

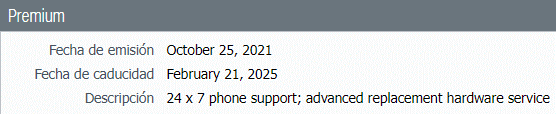
Este documento servirá como herramienta para verificar el estado de las plataformas de seguridad y su correcto funcionamiento.

1. **CAPACIDAD TOTAL DE LOS EQUIPOS**

|  |  |  |
| --- | --- | --- |
| **EQUIPO** | **CAPACIDAD TOTAL** | |
| **Memoria** | **Disco** |
| Firewall Basadre | 3.9 GB | 251 GB |
| Firewall Diners | 3.9 GB | 251 GB |
| Balanceador F5 | 7.9 GB | 500 GB |
| Palo Alto FW Panorama | 7.8 GB | 86.9 GB |
| Balanceador Citrix- DDOS Activo | 12.27 GB | 147.55 MB |
| Balanceador Citrix- DDOS Pasivo | 12.27 GB | 147.55 MB |
| Palo Alto FW Interno 01 | 15.3 GB | 240 GB |
| Palo Alto FW Interno 02 | 15.3 GB | 240 GB |
| Palo Alto FW Externo 01 | 15.3 GB | 240 GB |
| Palo Alto FW Externo 02 | 15.3 GB | 240 GB |
| Filtro Web Proxy 01 | 96.37 MB | 600 GB |
| Filtro Web Proxy 02 | 96.37 MB | 600 GB |
| Proxy Reporter | 16 GB | 50 GB |
| Firewall Carsa - Fortinet | 1.9 GB | 14.97 GB |
| Fortianalizer Carsa | 5.8 GB | 916.77 GB |
| IBM Guardium | 32.83 GB | 236.365 GB |
| IBM Optim | 16 GB | 1.02 TB |
| IBM Qradar | 23.59 GB | 16.10 TB |
| McAfee ATD | 251.81 GB | 61.88 GB |
| McAfee TIE | 7.98 GB | 102.53 GB |
| McAfee Antivirus ePo | 16 GB | 399.53 GB |
| Citrix Application Delivery Management | 5.49 GB | 112 GB |

1. **ESTADO DE PLATAFORMAS**
2. **FIREWALLS CHECKPOINT**
   1. **FIREWALL BASADRE (172.19.64.2)**

* **Licencias**

****

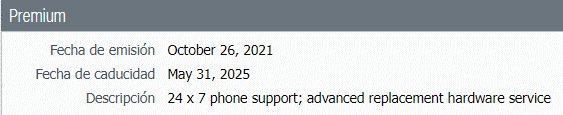
* **Recursos**

${graph1384}

* *Se observó un uso de CPU de* ***00%*** *durante el transcurso del día.*
* *Se observó un uso de Disco de* ***4%*** *durante el transcurso del día.*
* *Se observó un uso de Memoria del* ***47.65%*** *durante el transcurso del día.*
* *Se observan* *picos de consumo de CPU, por 1 min, el mayor llegó hasta* ***58%.*** *No se considera crítico debido a que se encuentra dentro del umbral.*
* **Conexiones Concurrentes**

${graph1343}

* *Se observó* ***51.35 k*** *conexiones durante el transcurso del día.*
  1. **IREWALL DINERS (172.19.210.2)**
* **Licencias**



* **Recursos**

${graph1388}

* *Se observó un uso de CPU de* ***5.32%*** *durante el transcurso del día.*
* *Se observó un uso de Disco de* ***3%*** *durante el transcurso del día.*
* *Se observó un uso de Memoria del* ***47.41%*** *durante el transcurso del día.*
* *Se observan* *picos de consumo de CPU, por 1 min, el mayor llegó hasta* ***46%.*** *No se considera crítico debido a que se encuentra dentro del umbral.*
* **Conexiones Concurrentes**

${graph1345}

* *Se observó* ***51.35 k*** *conexiones durante el transcurso del día.*

1. **BALANCEADOR F5 (172.16.1.249)**

* **Recursos**

${graph1377}

* *Se observó un uso de CPU de* ***6.92%*** *durante el transcurso del día.*
* *Se observó un uso de Disco de* ***8%*** *durante el transcurso del día.*
* *Se observó un uso de Memoria del* ***70%*** *durante el transcurso del día.*
* *Se observan* *picos de consumo de CPU, por 1 min, el mayor llegó hasta* ***70%.*** *No se considera crítico debido su duración.*
* **Conexiones Concurrentes**

${graph1378}

* *Se observó* ***191.19 k*** *conexiones durante el transcurso del día.*
* *Se observa un consumo estable, dentro del horario laboral.*
* **Bytes por Segundo**

${graph2307}

* *Se observó* ***34.17 KB*** *del cliente por segundo durante el transcurso del día.*
* *Se observó* ***33.16 KB*** *de servidor por segundo durante el transcurso del día.*
* *Se observa un consumo estable, dentro del horario laboral.*

1. **FIREWALLS PALO ALTO**
   1. **PANORAMA (172.16.2.155)**

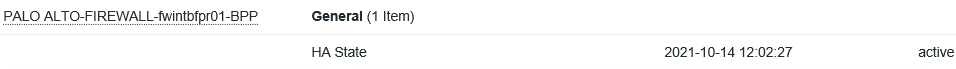
* **Recursos**

${graph1340}

* *Se observó un uso de CPU del* ***3.42%*** *durante el transcurso del día.*
* *Se observó un uso de Disco de* ***36.91%*** *durante el transcurso del día.*
* *Se observó un uso de Memoria del* ***76.93%*** *durante el transcurso del día.*
* *Se observa cortes en la gráfica, es debido a la intermitencia en nuestra VPN, se valida que la plataforma se encontró estable durante el día.*
  1. **CLÚSTER INTERNO**

1. **FIREWALL INTERNO 01 (172.17.23.25)**

* **Estado**



* *Se observa que el FW Interno 01 se encuentra activo.*
* **Recursos**

${graph1346}

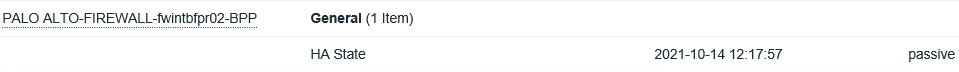
* *Se observó un uso de CPU de* ***1.22%*** *durante el transcurso del día.*
* *Se observó un uso de Disco de* ***23.01%*** *durante el transcurso del día.*
* *Se observó un uso de Memoria del* ***40.55%*** *durante el transcurso del día.*
* **Conexiones Concurrentes**

${graph1347}

* *Se observó* ***1.01 K.*** *sesiones durante el transcurso del día.*

1. **FIREWALL INTERNO 02 (172.17.23.26)**

* **Estado**



* *Se observa que el FW Interno 02 se encuentra suspendido.*
* **Recursos**

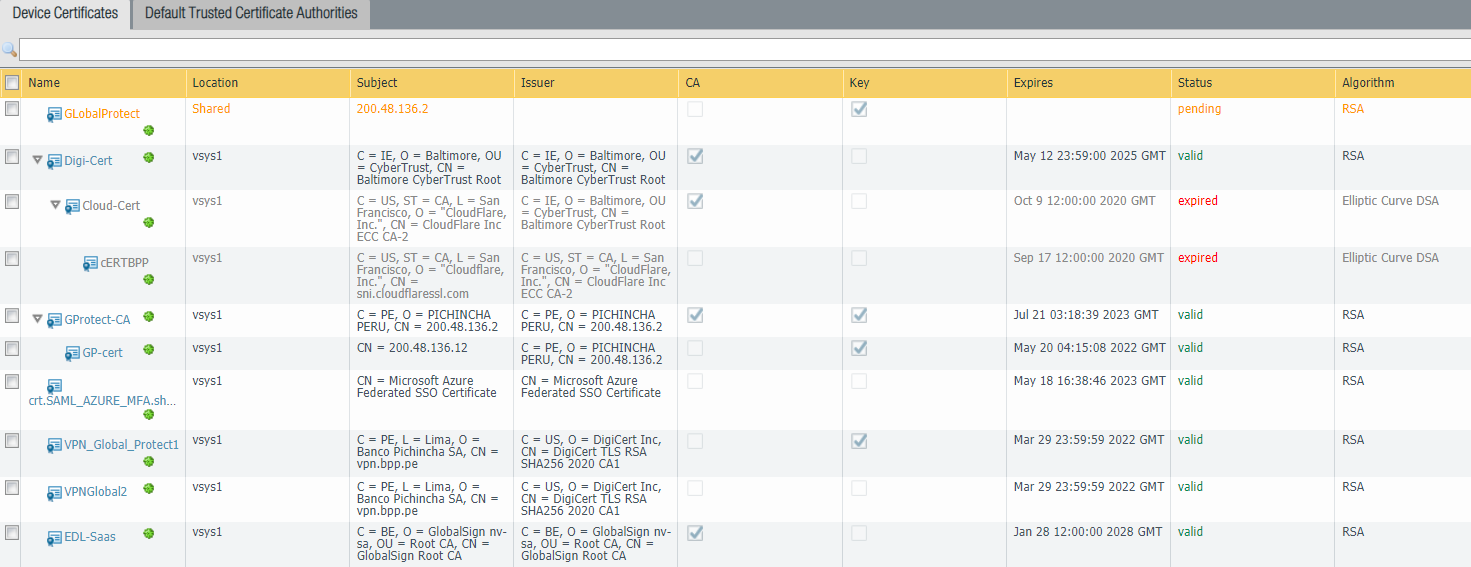
${graph1348}

* *Se observó un uso de CPU de* ***1.04%*** *durante el transcurso del día.*
* *Se observó un uso de Disco de* ***18.44%*** *durante el transcurso del día.*
* *Se observó un uso de Memoria del* ***1%*** *durante el transcurso del día.*
* *Se observa un* *pico de consumo de CPU, por 1 min, el cual llego hasta* ***7%.*** *Se encuentra dentro del umbral.*
* **Conexiones Concurrentes**

${graph1349}

* *Se observó* ***986.25 k*** *sesiones durante el transcurso del día.*

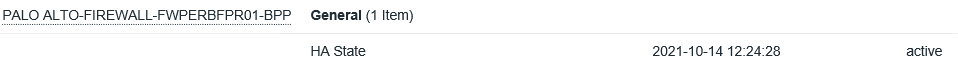
* 1. **CLÚSTER PERIMETRAL**
* **Certificados**



* *Se observa certificados expirados.*

1. **FIREWALL PERIMETRAL 01 (172.17.23.20)**

* **Estado**



* *Se observa que el FW Externo 01 se encuentra activo.*
* **Recursos**

${graph1350}

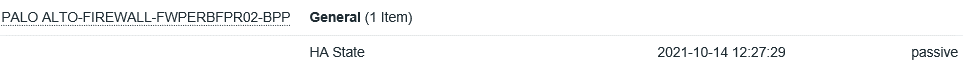
* *Se observó un uso de CPU de* ***2.16%*** *durante el transcurso del día.*
* *Se observó un uso de Disco de* ***48.75%*** *durante el transcurso del día.*
* *Se observó un uso de Memoria del* ***68.98%*** *durante el transcurso del día.*
* **Conexiones Concurrentes**

${graph1351}

* *Se observó* ***31.95 K*** *de sesiones durante el transcurso del día.*

1. **FIREWALL PERIMETRAL 02 (172.17.23.21)**

* **Estado**



* *Se observa que el FW Externo 02 se encuentra pasivo.*
* **Recursos**

${graph1352}

* *Se observó un uso de CPU de* ***1.07%*** *durante el transcurso del día.*
* *Se observó un uso de Disco de* ***38.69%*** *durante el transcurso del día.*
* *Se observó un uso de Memoria del* ***46%*** *durante el transcurso del día.*
* *Se observa* *un pico de consumo de CPU, por 1min, el cual llego hasta* ***5%*** *Se encuentra dentro del umbral.*
* **Conexiones Concurrentes**

${graph1353}

* *Se observó* ***31.34 K*** *de sesiones durante el transcurso del día.*

1. **PROXY MCAFEE** 
   1. **FILTRO WEB - PROXY 01 (172.16.1.78)**

* **Recursos**

${graph1381}

* *Se observó un uso de CPU de* ***27.22%*** *durante el transcurso del día.*
* *Se observó un uso de Disco de* ***13.00%*** *durante el transcurso del día.*
* *Se observó un uso de Memoria de* ***32%*** *durante el transcurso del día.*
* *Se observa* *un pico de consumo de CPU, por 1min, el cual llego hasta* ***81%****. No se considera critico debido a la duración del tiempo.*
  1. **FILTRO WEB - PROXY 02 (172.16.1.79)**
* **Recursos**

${graph1382}

* *Se observó un uso de CPU de* ***36.02%*** *durante el transcurso del día.*
* *Se observó un uso de Memoria de* ***12%*** *durante el transcurso del día.*
* *Se observó un uso de Disco de* ***19%*** *durante el transcurso del día.*
* *Se observa* *un pico de consumo de CPU, por 1min, el cual llegó hasta* ***68%.*** *No se considera critico debido a la duración del tiempo.*
  1. **PROXY REPORTER (172.16.2.128)**
* **Recursos**

${graph1380}

* *Se observó un uso de CPU de* ***32%*** *durante el transcurso del día.*
* *Se observó un uso de Disco de* ***27.19%*** *durante el transcurso del día.*
* *Se observó un uso de Memoria de* ***13.00%*** *durante el transcurso del día.*
* *Se observa* *un pico de consumo de CPU, por 1min, el cual llegó hasta* ***82%.*** *No se considera crítico debido a la duración del tiempo.*

1. **FORTIANALIZER CARSA (172.31.5.252)**

* **Recursos**

${graph1337}

* *Se observó un uso de CPU de* ***48.41%*** *durante el transcurso del día.*
* *Se observó un uso de Disco de* ***0.19%*** *durante el transcurso del día.*
* *Se observó un uso de Memoria del* ***52%*** *durante el transcurso del día.*
* *se observa* *un pico de consumo de CPU, por 1min, el cual llegó hasta* ***16%.*** *Se encuentra dentro del umbral.*
* **Estado de Dispositivos Integrados**



1. **FIREWALL CARSA – FORTINET (172.31.5.254)**

* **Recursos**

${graph1338}

* *Se observó un uso de CPU de* ***0.06%*** *durante el transcurso del día.*
* *Se observó un uso de Disco de* ***54.00%*** *durante el transcurso del día.*
* *Se observó un uso de Memoria de* ***1%*** *durante el transcurso del día.*
* *Se revisó mediante* ***SOL 63069*** *que el estado actual del disco es 1,* *el cual valida lo visto a nivel de Zabbix.*
* **Conexiones**

${graph1339}

* *Se observó* ***311.79 k*** *sesiones durante el transcurso del día.*

1. **CITRIX**
   1. **BALACEADOR DDOS ACTIVO (172.17.23.32)**

* **Recursos**

${graph1357}

* *Se observó un uso de CPU de* ***0%*** *durante el transcurso del día.*
* *Se observó un uso de Disco de* ***5%*** *durante el transcurso del día.*
* *Se observó un uso de Memoria del* ***53%*** *durante el transcurso del día.*
  1. **BALACEADOR DDOS PASIVO (172.17.23.33)**
* **Recursos**

${graph1360}

* *Se observó un uso de CPU de* ***2.59%*** *durante el transcurso del día.*
* *Se observó un uso de Disco de* ***5.99%*** *durante el transcurso del día.*
* *Se observó un uso de Memoria del* ***23.89%*** *durante el transcurso del día.*

1. **IBM**
   1. **OPTIM (172.16.1.197)**

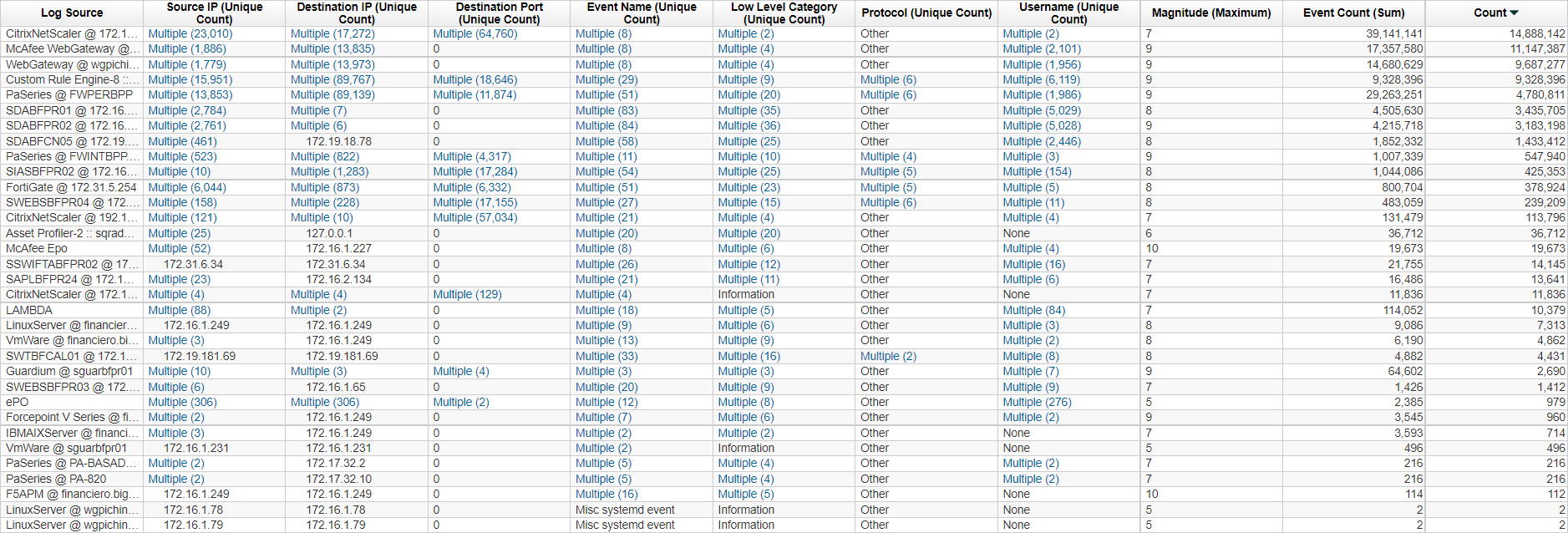
* **Recursos**

${graph2306}

* *Se observó un uso de CPU de* ***31.00%*** *durante el transcurso del día.*
* *Se observó un uso de Memoria de* ***7.86%*** *durante el transcurso del día.*
* *Se observó un uso de Disco C del* ***24%*** *durante el transcurso del día.*
* *Se observó un uso de Disco E del* ***24%*** *durante el transcurso del día.*
* *Se observa* *un pico de consumo de CPU, por 1min, el cual llego hasta* ***22%*** *No se considera crítico debido a que se encuentra dentro del umbral.*
  1. **QRADAR (172.16.1.210)**
* **Recursos**

${graph1389}

* *Se observó un uso de CPU de* ***9.21%*** *durante el transcurso del día.*
* *Se observó un uso de Disco de* ***59.00%*** *durante el transcurso del día*
* *Se observó un uso de Memoria de* ***45.06%*** *durante el transcurso del día.*
* *Se observó* *un pico de consumo de CPU, por 10 min, el cual llego hasta* ***41%*** *Se encuentra dentro del umbral.*
* **Principales orígenes de registro**



* 2. **GUARDIUM (172.16.1.231)**
* **Recursos**

${graph1354}

* *Se observó un uso de Memoria de* ***38.99%*** *durante el transcurso del día.*
* *Se observó un uso de CPU de* ***99.43%*** *durante el transcurso del día*
* *Se observó un uso de Disco de* ***0.91%*** *durante el transcurso del día.*

1. **MCAFEE (172.17.23.29)**
   1. **ATD**

* **Recursos**

${graph1336}

* *Se observó un uso de CPU de* ***10.45%*** *durante el transcurso del día.*
* *Se observó un uso de Disco de* ***55%*** *durante el transcurso del día.*
* *Se observó un uso de Memoria de* ***75%*** *durante el transcurso del día.*
  1. **TIE (172.16.2.153)**
* **Recursos**

${graph1376}

* *Se observó un uso de CPU de* ***1.33%*** *durante el transcurso del día.*
* *Se observó un uso de Disco de* ***47%*** *durante el transcurso del día.*
* *Se observó un uso de Memoria de* ***37.47%*** *durante el transcurso del día.*
  1. **Antivirus ePo (172.16.1.229)**
* **Recursos**

${graph2297}

* *Se observó un uso de CPU de* ***63.26%*** *durante el transcurso del día.*
* *Se observó un uso de Memoria del* ***21.86%*** *durante el transcurso del día.*
* *Se observó un uso de Disco C de* ***73.14%*** *durante el transcurso del día.*
* *Se observó un uso de Disco E de* ***73.14%*** *durante el transcurso del día.*
* *Se observó* *un pico de consumo de CPU, por un 1 min, el mayor llegó hasta* ***51%.*** *No se considera critico debido a que se encuentra dentro del umbral.*

1. **RESUMEN DE LOS EVENTOS**

* (\*) Se detectaron **00** eventos el día **${fecha\_antes\_salsh}.**

1. **DETALLE DEL EVENTO**

* Los eventos se encuentran en el archivo **SOC\_FOR\_05\_RPD\_BPP\_${fecha\_antes}\_Eventos.**

1. **CONCLUSIONES**

* En los **FIREWALLS** **CHECKPOINT:**
  + En **BASADRE** se observó picos de consumo de CPU, por 1 min, el mayor llegó hasta **58%**. No se considera crítico debido a que se encuentra dentro del umbral.
  + En **DINNERS** se observó picos de consumo de CPU, por 1 min, el mayor llegó hasta **46%**. No se considera crítico debido a que se encuentra dentro del umbral
* En los recursos del equipo **BALANCEADOR F5** se observó picos de consumo de CPU, por 1 min, el mayor llegó hasta **70%**. No se considera crítico debido su duración.
* Los recursos en el **FIREWALLS PALO ALTO:**
  + En **PANORAMA** se observó cortes en la gráfica, es debido a la intermitencia en nuestra VPN, se valida que la plataforma se encontró estable durante el día.
  + Se observó en el **FIREWALL INTERNO 02** un pico de consumo de CPU, por 1 min, el cual llego hasta **7%**. Se encuentra dentro del umbral.
* Los recursos en el **CLÚSTER PERIMETRAL:**
  + En el **FIREWALL PERIMETRAL 02** se observó un pico de consumo de CPU, por 1min, el cual llego hasta **5%** Se encuentra dentro del umbral.
* Los recursos en el **PROXY MCAFEE:**
  + En el **PROXY 01** se observó un pico de consumo de CPU, por 1min, el cual llego hasta **81%**. No se considera critico debido a la duración del tiempo.
  + En el **PROXY 02,** se observó un pico de consumo de CPU, por 1min, el cual llegó hasta **68%**. No se considera critico debido a la duración del tiempo.
  + En el **PROXY REPORTER**, se observó un pico de consumo de CPU, por 1min, el cual llegó hasta **82%.** No se considera crítico debido a la duración del tiempo.
* En el **FORTIANALIZER CARSA** se observó un pico de consumo de CPU, por 1min, el cual llegó hasta **16%**. Se encuentra dentro del umbral.
* Los recursos en el **FIREWALL CARSA - FORTINE** se observó sus recursos estables durante el día.
* Los recursos en **el BALANCEADOR CITRIX (DDOS ACTIVO y DDOS PASIVO)** fueron estables durante el día.
* Los recursos en el **CITRIX APLICACIONES Y COMPONENTES** fueron estables durante el día.
* Los recursos en los equipos **IBM:**
  + En el **OPTIM** se observó un pico de consumo de CPU, por 1min, el cual llego hasta **22%** No se considera crítico debido a que se encuentra dentro del umbral.
  + En el **QRADAR** se observó un pico de consumo de CPU, por 10 min, el cual llego hasta **41%** Se encuentra dentro del umbral.
* Los recursos en **MCAFEE:**
  + En **ATD y TIE** fueron estables durante el día.
  + en el **ANTIVIRUS ePo** se observó un pico de consumo de CPU, por un 1 min, el mayor llegó hasta **51%**. No se considera critico debido a que se encuentra dentro del umbral.
* Los eventos se encuentran en el archivo **SOC\_FOR\_05\_RPD\_BPP\_${fecha\_antes}\_Eventos.**
* Se adjunta archivos del estado de actualización del **DAT y AMCORE.**

1. **ESTATUS DE LOS TICKETS REPORTADOS**

* Se observó un consumo alto de CPU en **PROXY 01**, se revisó mediante el INC **76172**. El alto consumo de CPU se debe a que se escanean archivos grandes, por lo que al descargar un archivo de 1GB por ej, pasara por el Anti-Malware y esto consumo bastante CPU. Este operando con normalidad el clúster, pero tiene picos de peticiones y de CPU que coinciden con el GAM-Server en fecha y hora, y si envían archivos muy grandes que descarguen de la WEB, como una ISO de 700 MB, esto es entendible.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CONTROL DE CAMBIOS | | | | |
| Revisión | Hecha por | Aprobada por | Fecha | Motivo |
| 01 | ${autor} | Supervisor CyberSOC | 15/01/2022 | Versión Inicial |