

**SECURESOFT CORPORATION**

**e-Secure Consulting Group**

**REPORTE DIARIO - SALUD**

**Preparado para:**



**Fecha de elaboración:**

**${fecha\_actual}**

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

**S.A.C. y Banco Ripley.**

**INDICE**

[**I. OBJETIVO 3**](#_Toc86329546)

[**II. ALCANCES 3**](#_Toc86329547)

[**III. UMBRALES CONFIGURADOS 3**](#_Toc86329548)

[**IV. ESTADO DE LAS PLATAFORMAS 4**](#_Toc86329549)

[**1. CHECKPOINT 4**](#_Toc86329550)

[**2. F5 17**](#_Toc86329551)

[**3. JUNIPER 22**](#_Toc86329552)

[**4. Fortinet 23**](#_Toc86329553)

[**5. MCAFFE 24**](#_Toc86329554)

[**6. CLOUD COMPUTING 28**](#_Toc86329555)

[**V. CONCLUSIONES 31**](#_Toc86329556)

[**VI. RECOMENDACIONES 31**](#_Toc86329557)

# OBJETIVO

Este documento dará a conocer el estado de las plataformas de salud durante el último día.

# ALCANCES

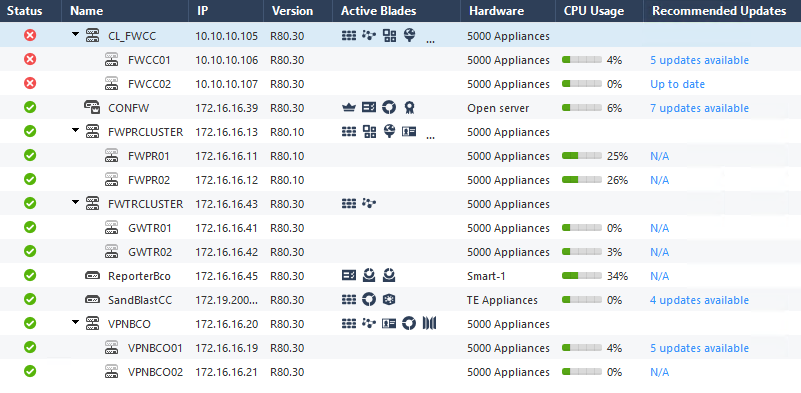
Este documento servirá como herramienta para verificar el estado de las plataformas y su correcto funcionamiento.

# UMBRALES CONFIGURADOS

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **EQUIPO** | **UMBRAL WARNING  CPU/MEMORIA** | **UMBRAL HIGH CPU/MEMORIA** | **UMBRAL DISASTER CPU/MEMORIA** | **UMBRAL WARNING Disco** | **UMBRAL DISASTER Disco** |
| Smart Center Banco | 70% | 80% | 90% | 80% | 90% |
| Smart Reporter Banco | 70% | 80% | 90% | 80% | 90% |
| Firewall Perimetral Banco 01 | 70% | 80% | 90% | 80% | 90% |
| Firewall Perimetral Banco 02 | 70% | 80% | 90% | 80% | 90% |
| Firewall Transaccional Banco 01 | 70% | 80% | 90% | 80% | 90% |
| Firewall Transaccional Banco 02 | 70% | 80% | 90% | 80% | 90% |
| Firewall VPN Banco 01 | 70% | 80% | 90% | 80% | 90% |
| Firewall VPN Banco 02 | 70% | 80% | 90% | 80% | 90% |
| Firewall QA Banco | 70% | 80% | 90% | 80% | 90% |
| Smart Center Home Banking | 70% | 80% | 90% | 80% | 90% |
| Smart Reporter Home Banking | 70% | 80% | 90% | 80% | 90% |
| Smart Center Contingencia | 70% | 80% | 90% | 80% | 90% |
| Firewall VPN SSL Banco 01 | 70% | 80% | 90% | 80% | 90% |
| Firewall VPN SSL Banco 02 | 70% | 80% | 90% | 80% | 90% |
| Firewall Primario de Sede Contingencia | 70% | 80% | 90% | 80% | 90% |
| Firewall Secundario de Sede Contigencia | 70% | 80% | 90% | 80% | 90% |
| LCBQA01 | 70% | 80% | 90% | 80% | 90% |
| BIGIP01 | 70% | 80% | 90% | 80% | 90% |
| BIGIP02 | 70% | 80% | 90% | 80% | 90% |
| LCCC01 | 70% | 80% | 90% | 80% | 90% |
| LCCC02 | 70% | 80% | 90% | 80% | 90% |
| Pulse Secure | 70% | 80% | 90% | 80% | 90% |
| FortiMail | 70% | 80% | 90% | 80% | 90% |
| Proxy Banco 01 | 70% | 80% | 90% | 80% | 90% |
| Proxy Banco 02 | 70% | 80% | 90% | 80% | 90% |
| TIE | 70% | 80% | 90% | 80% | 90% |
| ePo Antivirus | 70% | 80% | 90% | 80% | 90% |
| Servidor NSM HB | 70% | 80% | 90% | 80% | 90% |
| Sandblast Cloud Computing | 70% | 80% | 90% | 80% | 90% |
| Firewall Cloud Computing 01 | 70% | 80% | 90% | 80% | 90% |
| Firewall Cloud Computing 02 | 70% | 80% | 90% | 80% | 90% |

# ESTADO DE LAS PLATAFORMAS

* 1. **CHECKPOINT** 
     + **ESTADO DE LOS FIREWALLS**



* **Smart Center BANCO RIPLEY – Recursos**

${graph1439}

* *Se observó un uso de CPU de 4.95% durante el transcurso del día.*
* *Se observó un uso de Disco del 54.86% durante el transcurso del día.*
* *Se observó un uso de Memoria de 36.56% durante el transcurso del día.*
* **Smart Center HomeBanking BANCO RIPLEY – Recursos**

${graph1443}

* *Se observó un uso de CPU de 15.86% durante el transcurso del día.*
* *Se observó un uso de Disco del 25 % durante el transcurso del día.*
* *Se observó un uso de Memoria de 77.93% durante el transcurso del día.*
* **Smart Center Contingencia BANCO RIPLEY – Recursos**

${graph1441}

* *Se observó un uso de CPU de 2.87 % durante el transcurso del día.*
* *Se observó un uso de Disco del 2% durante el transcurso del día.*
* *Se observó un uso de Memoria de 50.13% durante el transcurso del día.*
* **Smart Reporter – Recursos**

${graph1445}

* *Se observó un uso de CPU de 10.04% durante el transcurso del día.*
* *Se observó un uso de Disco del 50.54% durante el transcurso del día.*
* *Se observó un uso de Memoria de 58.75% durante el transcurso del día.*
* **Smart Reporter HomeBanking BANCO RIPLEY – Recursos**

${graph1447}

* *Se observó un uso de CPU de 59.07% durante el transcurso del día.*
* *Se observó un uso de Disco del 72.11% durante el transcurso del día.*
* *Se observó un uso de Memoria de 85.31% durante el transcurso del día.*
* **Firewall Perimetral 01 – Recursos**

${graph1410}

* *Se observó un uso de CPU de 21.34% durante el transcurso del día.*
* *Se observó un uso de Disco del 99.66% durante el transcurso del día.*
* *Se observó un uso de Memoria de 36% durante el transcurso del día.*
* **Firewall Perimetral 01 – Conexiones concurrentes**

${graph1411}

* *Se observó 20.11 K conexiones durante el transcurso del día.*
* **Firewall Perimetral 02 – Recursos**

${graph1412}

* *Se observó un uso de CPU de 17.98% durante el transcurso del día.*
* *Se observó un uso de Disco del 15.99% durante el transcurso del día.*
* *Se observó un uso de Memoria de 51.60% durante el transcurso del día.*
* **Firewall Perimetral 02 – Conexiones concurrentes**

${graph1413}

* *Se observó 20.11 K conexiones durante el transcurso del día.*
* **Firewall Transaccional Banco 01 – Recursos**

${graph1420}

* *Se observó un uso de CPU de 5.42% durante el transcurso del día.*
* *Se observó un uso de Disco del 12% durante el transcurso del día.*
* *Se observó un uso de Memoria de 21.00% durante el transcurso del día.*
* **Firewall Transaccional Banco 01 – Conexiones concurrentes**

${graph1421}

* *Se observó 1.13 K conexiones durante el transcurso del día.*
* **Firewall Transaccional Banco 02 – Recursos**

${graph1422}

* *Se observó un uso de CPU de 0.35% durante el transcurso del día.*
* *Se observó un uso de Disco del 9% durante el transcurso del día.*
* *Se observó un uso de Memoria de 19.00% durante el transcurso del día.*
* **Firewall Transaccional Banco 02 – Conexiones concurrentes**

${graph1423}

* *Se observó 1.14 K conexiones durante el transcurso del día.*
* **Firewall VPN Banco 01 – Recursos**

${graph1424}

* *Se observó un uso de CPU de 13.64 % durante el transcurso del día.*
* *Se observó un uso de Disco del 78% durante el transcurso del día.*
* *Se observó un uso de Memoria de 27.02% durante el transcurso del día.*
* **Firewall VPN Banco 01 – Conexiones concurrentes**

${graph1425}

* *Se observó 1.09k conexiones durante el transcurso del día.*
* **Firewall VPN SSL Banco 01 – Recursos**

${graph1428}

* *Se observó un uso de CPU de 1.67% durante el transcurso del día.*
* *Se observó un uso de Memoria de 36.14% durante el transcurso del día.*
* **Firewall VPN SSL Banco 01 – Conexiones concurrentes**

${graph1429}

* *Se observó 6.03 K conexiones durante el transcurso del día.*
* **Firewall VPN SSL Banco 02 – Recursos**

${graph1430}

* *Se observó un uso de CPU de 0.05% durante el transcurso del día.*
* *Se observó un uso de Memoria de 21% durante el transcurso del día.*
* **Firewall VPN SSL Banco 02 – Conexiones concurrentes**

${graph1431}

* *Se observó 603.96 conexiones durante el transcurso del día.*
* **Firewall QA – Recursos**

${graph1414}

* *Se observó un uso de CPU de 41.70% durante el transcurso del día.*
* *Se observó un uso de Disco del 90.22% durante el transcurso del día.*
* *Se observó un uso de Memoria de 51.00% durante el transcurso del día.*
* **Firewall QA – Conexiones concurrentes**

${graph1415}

* *Se observó 1.51 K conexiones durante el transcurso del día.*
* **Firewall Primario de Sede Contingencia – Recursos**

${graph1406}

* *Se observó un uso de CPU de 0.39% durante el transcurso del día.*
* *Se observó un uso de Disco del 9% durante el transcurso del día.*
* *Se observó un uso de Memoria de 20% durante el transcurso del día.*
* **Firewall Primario de Sede Contingencia – Conexiones concurrentes**

${graph1407}

* *Se observó 82.16 conexiones durante el transcurso del día.*

* **Firewall Secundario de Sede Contingencia – Recursos**

${graph1408}

* *Se observó un uso de CPU de 0.54% durante el transcurso del día.*
* *Se observó un uso de Disco del 9% durante el transcurso del día.*
* *Se observó un uso de Memoria de 21% durante el transcurso del día.*
* **Firewall Secundario de Sede Contingencia – Conexiones concurrentes**

${graph1409}

* *Se observó 87.25 conexiones durante el transcurso del día.*
  1. **F5**
     + **ESTADO DE LOS BALANCEADORES**
* **LCBQA01 – Recursos**

${graph1394}

* *Se observó un uso de CPU de 31.43% durante el transcurso del día.*
* *Se observó un uso de Disco del 27% durante el transcurso del día.*
* *Se observó un uso de Memoria de 3% durante el transcurso del día.*
* **LCBQA01 – Conexiones concurrentes**

${graph1395}

* *Se observó 104.67 conexiones durante el transcurso del día.*
* **BIGIP01 – Recursos**

${graph1390}

* *Se observó un uso de CPU de 10.38% durante el transcurso del día.*
* *Se observó un uso de Disco del 62% durante el transcurso del día.*
* *Se observó un uso de Memoria de 8% durante el transcurso del día.*
* **BIGIP01 – Conexiones concurrentes**

${graph1391}

* *Se observó 136.29 conexiones durante el transcurso del día.*
* **BIGIP02 – Recursos**

${graph1392}

* *Se observó un uso de CPU de 10.96% durante el transcurso del día.*
* *Se observó un uso de Disco del 65% durante el transcurso del día.*
* *Se observó un uso de Memoria de 9% durante el transcurso del día.*
* **BIGIP02 – Conexiones concurrentes**

${graph1393}

* *Se observó 450.54 conexiones durante el transcurso del día.*
* **LCCC01 – Recursos**

${graph1396}

* *Se observó un uso de CPU de 12.96% durante el transcurso del día.*
* *Se observó un uso de Disco del 74% durante el transcurso del día.*
* *Se observó un uso de Memoria de 3.09% durante el transcurso del día.*
* **LCCC01 – Conexiones concurrentes**

${graph1397}

* *Se observó 12.43 K conexiones durante el transcurso del día.*
* **LCCC02 – Recursos**

${graph1398}

* *Se observó un uso de CPU de 13.03% durante el transcurso del día.*
* *Se observó un uso de Disco del 46% durante el transcurso del día.*
* *Se observó un uso de Memoria de 3% durante el transcurso del día.*
* **LCCC02 – Conexiones concurrentes**

${graph1399}

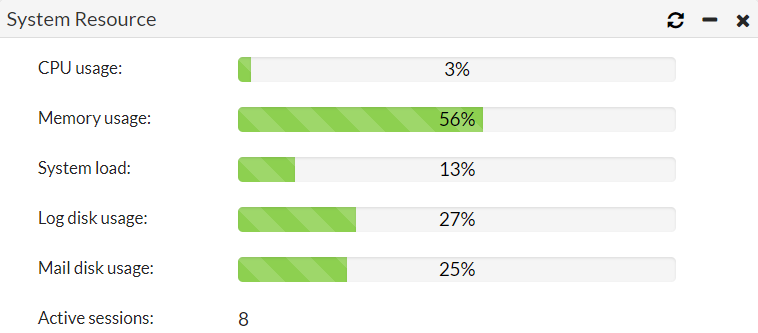
* *Se observó 66.47 conexiones durante el transcurso del día.*
  1. **JUNIPER**
     + **ESTADO**
* **PEBRIVPNJUN-Pulse Secure – Recursos**

${graph1450}

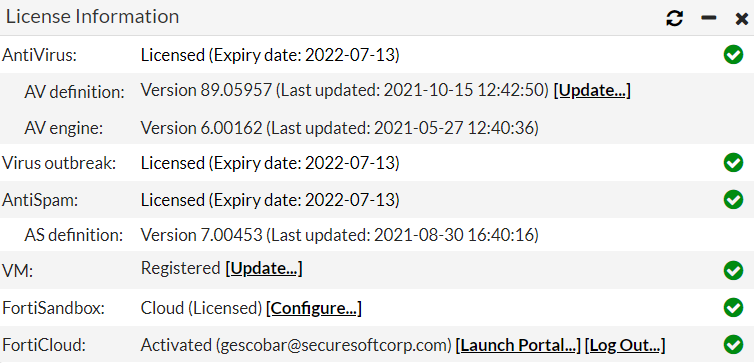
* *Se observó un uso de CPU de 5.82% durante el transcurso del día.*
* *Se observó un uso de Disco del 13% durante el transcurso del día.*
* *Se observó un uso de Memoria de 10.80% durante el transcurso del día.*
* **PEBRIVPNJUN-Pulse Secure - Conexiones concurrentes**

${graph1449}

* *Se observó 98.16 conexiones durante el transcurso del día.*
  1. **Fortinet**
* **FortiMail – Recursos**



* **FortiMail - Licencias**



* 1. **MCAFFE**
     + **ESTADO DE LOS EQUIPOS**
* **Proxy Usuarios 01 - McAfee – Recursos**

${graph1434}

* *Se observó un uso de CPU de 2.04% durante el transcurso del día.*
* *Se observó un uso de Disco del 22% durante el transcurso del día.*
* *Se observó un uso de Memoria de 18.24% durante el transcurso del día.*
* **Proxy Usuarios 01 - McAfee - Conexiones concurrentes**

${graph1435}

* *Se observó 1.65 K conexiones durante el transcurso del día.*
* **Proxy Usuarios 02 - McAfee – Recursos**

${graph1436}

* *Se observó un uso de CPU de 0.11% durante el transcurso del día.*
* *Se observó un uso de Disco del 18% durante el transcurso del día.*
* *Se observó un uso de Memoria de 14.00% durante el transcurso del día.*
* **Proxy Usuarios 02 - McAfee - Conexiones concurrentes**

${graph1437}

* *Se observó 0.11 conexiones durante el transcurso del día.*
* **TIE ESX – Recursos**

${graph1401}

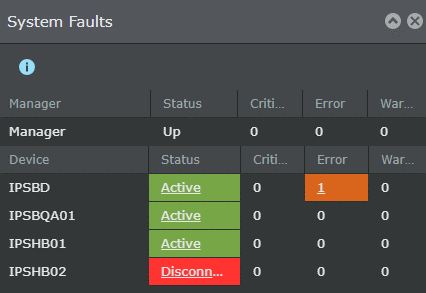
* *Se observó un uso de CPU de 14.96% durante el transcurso del día.*
* *Se observó un uso de Disco del 95% durante el transcurso del día.*
* *Se observó un uso de Memoria de 44% durante el transcurso del día.*
* **McAfee - ePo Antivirus – Recursos**

${graph2294}

* *Se observó un uso de CPU de 5.65 % durante el transcurso del día.*
* *Se observó un uso de Memoria de 50.34% durante el transcurso del día.*
* *Se observó un uso de* ***Disco C*** *del 69.53% durante el transcurso del día.*
* *Se observó un uso de* ***Disco D*** *del 25.44% durante el transcurso del día.*
* **Servidor NSM HB – Recursos**

${graph2295}

* *Se observó un uso de CPU de -% durante el transcurso del día.*
* *Se observó un uso de Disco del 51% durante el transcurso del día.*
* *Se observó un uso de Memoria de -% durante el transcurso del día.*
* **NSM (172.19.200.68) – Estado de salud de los IPS**



* 1. **CLOUD COMPUTING**
     + **ESTADO**
* **Cloud Computing - CheckPoint - SandBlast CC- Recursos**

${graph1416}

* *Se observó un uso de CPU de 0.97% durante el transcurso del día.*
* *Se observó un uso de Disco del 19% durante el transcurso del día.*
* *Se observó un uso de Memoria de 22.91% durante el transcurso del día.*
* **Cloud Computing - CheckPoint - SandBlast CC- Conexiones concurrentes**

${graph1417}

* *Se observó 611.68 conexiones durante el transcurso del día.*
* **Cloud Computing - CheckPoint - Firewall CC 01 – Recursos**

${graph1402}

* *Se observó un uso de CPU de 7.51% durante el transcurso del día.*
* *Se observó un uso de Disco del 10% durante el transcurso del día.*
* *Se observó un uso de Memoria de 27.08% durante el transcurso del día.*
* **Cloud Computing - CheckPoint - Firewall CC 01 – Conexiones concurrentes**

${graph1403}

* *Se observó 258.38 K conexiones durante el transcurso del día.*
* **Cloud Computing - CheckPoint - Firewall CC 02 – Recursos**

${graph1404}

* *Se observó un uso de CPU de 0.14 % durante el transcurso del día.*
* *Se observó un uso de Disco del 10% durante el transcurso del día.*
* *Se observó un uso de Memoria de 19.00% durante el transcurso del día.*
* **Cloud Computing - CheckPoint - Firewall CC 02- Conexiones concurrentes**

${graph1405}

* *Se observó 257.86 K conexiones durante el transcurso del día.*

# CONCLUSIONES

1. El estado de los firewalls se encuentra estable durante el día.
2. El uso de memoria en los firewalls fue estable durante el día.
3. El uso del CPU se encuentra entre los umbrales establecidos.
4. El equipo Fortimail, se encuentra estable.
5. Se observa alto consumo de CPU en el **SmartReporter HomeBanking**. Según lo mencionado en el ticket **INC 115013** este consumo es un comportamiento normal debido a que dicho equipo solo cuenta con 2 CPUs por lo cual la carga que lleva y procesa genera estos altos picos en el consumo del CPU.
6. Se observan alertas de licencias expiradas en el **SmartCenter**, se reportaron bajo el **INC 164088**. Se valida que no serán renovados.
7. Se observa una alerta en el NSM, esta es **Error** en **IPS-INTERNET-BR**, fue reportado bajo el ticket **INC 219986**. Según lo comentado por el ingeniero asignado, la causa raíz de la alerta es por una falta de actualización del GAM Engine en el sensor IPS debido a que no tiene acceso a la red externa para realizar dicha actualización.

# RECOMENDACIONES

1. Medidas de protección contra subidas y bajadas de tensión.
2. Mantener los equipos actualizados, tanto a nivel de sistema operativo como de controladores.
3. Es recomendable realizar la depuración de logs o backups más antiguos para evitar que el disco se llene.
4. Terminar procesos que puedan afectar los consumos elevados de CPU o de memoria y de ser necesario aumentar los recursos de los equipos para que estos no se esfuercen al ejecutar sus procesos.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CONTROL DE CAMBIOS** | | | | |
| **Revisión** | **Hecha por** | **Aprobada por** | **Fecha** | **Motivo** |
| 00 | ${autor} | Supervisor CyberSOC | ${fecha\_hoy} | Versión Inicial |