

# SECURESOFT CORPORATION

**e-Secure Consulting Group**

**REPORTE MENSUAL**

**Preparado para:**



**Fecha de elaboración:**

**Febrero 2022**

**El presente documento contiene información estrictamente privada y confidencial entre SECURESOFT CORPORATION S.A.C. y BBVA Banco Continental.**

### OBJETIVO

Este documento dará a conocer el estado de las plataformas de seguridad del mes de **Diciembre** del 2021, teniendo en cuenta la disponibilidad del monitoreo y recursos de ser posible.

### ALCANCE

Este documento servirá como herramienta para verificar el estado de las plataformas de seguridad y su correcto funcionamiento, abarcando tanto la disponibilidad por ICMP tanto el estado de sus recursos por SNMP en caso aplique.

### ESTADO DE LAS PLATAFORMAS

* 1. **FIREEYE ANTIMALWARE**
* **IA 2200 (118.180.55.229) – Recursos**

${graph1779}

* Se observó que el uso promedio de **CPU** durante el mes es de 0.42%.
* Se observó que el uso promedio de **Disco** durante el mes es de 41%.
* **ANTIMALWARE - HX – Recursos**

${graph1684}

* Se observó que el uso promedio de **CPU** durante el mes es de 50.02%.
* Se observó que el uso promedio de **Disco** durante el mes es de 78%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 76.6%.
  1. **SYMANTEC**
* **PROXY CONTINGENCIA – Recursos**

${graph1735}

* Se observó que el uso promedio de **CPU** durante el mes es de 2.96%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 14%.
* **PROXY CONTINGENCIA – Conexiones**

${graph1736}

* Se observó un uso promedio de **0.26** conexiones con servidores durante el mes.
* **FILTRO WEB PROXY01 – Recursos**

${graph1731}

* Se observó que el uso promedio de **CPU** durante el mes es de 7.05%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 17.55%
* **FILTRO WEB PROXY01 – Conexiones**

${graph1732}

* Se observó un uso promedio de **3.05 K** conexiones con clientes durante el mes.
* Se observó un uso promedio de **854.6** conexiones con servidores durante el mes.
* **FILTRO WEB PROXY02 – Recursos**

${graph1733}

* Se observó que el uso promedio de **CPU** durante el mes es de 7.28%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 15.76%.
* **FILTRO WEB PROXY02 – Conexiones**

${graph1734}

* Se observó un uso promedio de **3.13 K** conexiones con clientes durante el mes.
* Se observó un uso promedio de **876.41** conexiones con servidores durante el mes.
* **SSL VISIBILITY – Recursos**

${graph1752}

* Se observó que el uso promedio de **CPU** durante el mes es de 3.21%.
* Se observó que el uso promedio de **Disco** durante el mes es de 20.81%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 29%.
  1. **CISCO**
* **SENSOR INTERNET – Recursos**

${graph1729}

* Se observó que el uso promedio de **CPU** durante el mes es de 14.07%.
* Se observó que el uso promedio de **Disco** durante el mes es de 44%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 85.54%.
* **IPS-SPAIN – Recursos**

${graph1724}

* Se observó que el uso promedio de **CPU** durante el mes es de 1.21%.
* Se observó que el uso promedio de **Disco** durante el mes es de 39%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 30.12%.
  1. **FIREPOWER**
* **FIREPOWER MANAGEMENT CENTER – Recursos**

${graph1721}

* Se observó que el uso promedio de **CPU** durante el mes es de **8.76%.**
* Se observó que el uso promedio de **Memoria** durante el mes es de **51.61%.**
  1. **CHECKPOINT**
* **FIREWALL APN 1 – Recursos**

${graph1698}

* Se observó que el uso promedio de **CPU** durante el mes es de 3.24%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 16.25%.
* Se observó que el uso promedio de **Disco** durante el mes es de 38.94%.
* **FIREWALL – CHASSIS MANAGER – Recursos**

${graph1778}

* Se observó que el uso promedio de **CPU** durante el mes es de 0%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 55.61%.
* Se observó que el uso promedio de **Disco** durante el mes es de 28.43%.
* **FIREWALL CHASSIS 01 – Recursos**

${graph2355}

* Se observó que el uso promedio de **Memoria** durante el mes es de 49.30%.
* Se observó que el uso promedio de **CPU** durante el mes es de 0.39%.
* Se observó que el uso promedio de **Disco** durante el mes es de 62.07%.
* **FIREWALL CHASSIS 01 – Conexiones concurrentes**

${graph1759}

* Se observó un uso promedio de **204.03** conexiones concurrentes durante el mes.
* **FIREWALL CHASSIS 01 – Firewall Virtual APN – Consumo de CPU**

${graph2349}

* Se observó que el uso promedio de **CPU** durante el mes es de 0%.
* **FIREWALL CHASSIS 01 – Firewall Virtual Desarrollo – Consumo de CPU**

${graph2351}

* Se observó que el uso promedio de **CPU** durante el mes es de 0%.
* **FIREWALL CHASSIS 01 – Firewall Virtual Core – Consumo de CPU**

${graph2350}

* Se observó que el uso promedio de **CPU** durante el mes es de 0%.
* **FIREWALL CHASSIS 01 – Firewall Virtual Externos – Consumo de CPU**

${graph2352}

* Se observó que el uso promedio de **CPU** durante el mes es de 0%.
* **FIREWALL CHASSIS 01 – Firewall Virtual Interno – Consumo de CPU**

${graph2353}

* Se observó que el uso promedio de **CPU** durante el mes es de 0%.
* **FIREWALL CHASSIS 01 – Firewall Virtual Proveedores – Consumo de CPU**

${graph2354}

* Se observó que el uso promedio de **CPU** durante el mes es de 0%.
* **FIREWALL CHASSIS 01 – Firewall Virtual SedeCentral – Consumo de CPU**

${graph2356}

* Se observó que el uso promedio de **CPU** durante el mes es de 0.00%.
* **FIREWALL CHASSIS 02 – Recursos**

${graph2341}

* Se observó que el uso promedio de **CPU** durante el mes es de 0.96%.
* Se observó que el uso promedio de **Disco** durante el mes es de 28.43%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 55.61%.
* **FIREWALL CHASSIS 02 – Conexiones concurrentes**

${graph1760}

* Se observó un uso promedio de **485.18** conexiones concurrentes durante el mes.
* **FIREWALL CHASSIS 02 – Firewall Virtual APN – Consumo de CPU**

${graph2342}

* Se observó que el uso promedio de **CPU** durante el mes es de 0%.
* **FIREWALL CHASSIS 02 – Firewall Virtual Desarrollo – Consumo de CPU**

${graph2343}

* Se observó que el uso promedio de **CPU** durante el mes es de 0%.
* **FIREWALL CHASSIS 02 – Firewall Virtual Core – Consumo de CPU**

${graph2344}

* Se observó que el uso promedio de **CPU** durante el mes es de 1.32%.
* **FIREWALL CHASSIS 02 – Firewall Virtual Externos – Consumo de CPU**

${graph2345}

* Se observó que el uso promedio de **CPU** durante el mes es de 0.64%.
* **FIREWALL CHASSIS 02 – Firewall Virtual Interno – Consumo de CPU**

${graph2346}

* Se observó que el uso promedio de **CPU** durante el mes es de 0%.
* **FIREWALL CHASSIS 02 – Firewall Virtual Proveedores – Consumo de CPU**

${graph2347}

* Se observó que el uso promedio de **CPU** durante el mes es de 0%.
* **FIREWALL CHASSIS 02 – Firewall Virtual SedeCentral – Consumo de CPU**

${graph2348}

* Se observó que el uso promedio de **CPU** durante el mes es de 0%.
* **FIREWALL CONTINGENCIA -Recursos**

${graph1701}

* Se observó que el uso promedio de **CPU** durante el mes es de 0.89%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 28.00%.
* Se observó que el uso promedio de **Disco** durante el mes es de 33.10%.
* **FIREWALL CONTINGENCIA - Conexiones concurrentes**

${graph1702}

* Se observó un uso promedio de **114.37** conexiones concurrentes durante el mes.
  1. **IMPERVA**
* **DATABASE PRINCIPAL01 - Recursos**

${graph1690}

* Se observó que el uso promedio de **CPU** durante el mes es de 15.06%.
* Se observó que el uso promedio de **Disco** durante el mes es de 33%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 77.97%.
* **DATABASE PRINCIPAL02 – Recursos**

${graph1691}

* Se observó que el uso promedio de **CPU** durante el mes es de 23.94%.
* Se observó que el uso promedio de **Disco** durante el mes es de 31%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 77%.
* **DATABASE PRINCIPAL03 – Recursos**

${graph1692}

* Se observó que el uso promedio de **CPU** durante el mes es de 11.75%.
* Se observó que el uso promedio de **Disco** durante el mes es de 40%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 76.99%.
* **DATABASE PRINCIPAL04 – Recursos**

${graph1693}

* Se observó que el uso promedio de **CPU** durante el mes es de 3.30%.
* Se observó que el uso promedio de **Disco** durante el mes es de 39%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 74.72%.
* **MANAGEMENT DBF – Recursos**

${graph1694}

* Se observó que el uso promedio de CPU durante el mes es de 5.25%.
* Se observó que el uso promedio de Disco durante el mes es de 73%.
* Se observó que el uso promedio de Memoria durante el mes es de 41.29%.
  1. **PULSE SECURE**
* **CLUSTERVPN01 - Recursos**

${graph1744}

* Se observó que el uso promedio de **CPU** durante el mes es de 2.64%.
* Se observó que el uso promedio de **Disco** durante el mes es de 7%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 25.96%.
* **CLUSTERVPN01 – Conexiones Concurrentes**

${graph1745}

* Se observó un uso promedio de **48.71** usuarios concurrentes durante el mes.
* **CLUSTERVPN02 – Recursos**

${graph1746}

* Se observó que el uso promedio de **CPU** durante el mes es de 9.69%.
* Se observó que el uso promedio de **Disco** durante el mes es de 7.81%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 26.30%.
* **CLUSTERVPN02 – Conexiones Concurrentes**

${graph1747}

* Se observó un uso promedio de **48.71** usuarios concurrentes durante el mes.
* **CLUSTERVPN01\_VIRTUAL – Recursos**

${graph1740}

* Se observó que el uso promedio de **CPU** durante el mes es de 1.18%.
* Se observó que el uso promedio de **Disco** durante el mes es de 48.56%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 7.10%.
* **CLUSTERVPN01\_VIRTUAL – Conexiones Concurrentes**

${graph1741}

* Se observó un uso promedio de **619.98** usuarios concurrentes durante el mes.
* **CLUSTERVPN02\_VIRTUAL – Recursos**

${graph1742}

* Se observó que el uso promedio de **CPU** durante el mes es de 2.22%.
* Se observó que el uso promedio de **Disco** durante el mes es de 45.67%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 7.62%.
* **CLUSTERVPN02\_VIRTUAL – Conexiones Concurrentes**

${graph1743}

* Se observó un uso promedio de **619.99** usuarios concurrentes durante el mes.
  1. **QRADAR**
* **SIEM01 – Recursos**

${graph1749}

* Se observó que el uso promedio de **CPU** durante el mes es de 31.25%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 56.41%
* Se observó que el uso promedio de **Disco** durante el mes es de 82.96%.
  1. **SKYBOX**
* **AUDITORIA DE FIREWALL – Recursos**

${graph1711}

* Se observó que el uso promedio de **CPU** durante el mes es de 1.00%.
* Se observó que el uso promedio de **Disco** durante el mes es de 6%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 88.88%

### CONCLUSIONES

* Se valida que el promedio de los recursos de los equipos de la plataforma **FIREEYE** se encuentran estables.
* Se valida que el promedio de los recursos de los equipos de la plataforma **SYMANTEC** se encuentran estables.
* Se valida que el promedio de los recursos de los equipos de la plataforma **CISCO** se encuentran estables.
* Se valida que el promedio de los recursos de Management center de la plataforma **FIREPOWER** se encuentran estables.
* Se valida que el promedio de los recursos de los equipos de la plataforma **IMPERVA** se encuentran estables.
* Se valida que el promedio de los recursos de los firewalls de la plataforma **CHECKPOINT** se encuentran estables.
* Se valida que el promedio de los recursos de los equipos de la plataforma **PULSE SECURE** se encuentran estables.
* Se valida que el promedio de los recursos del SIEM de la plataforma **QRADAR** se encuentran estables.
* Se valida que el promedio de los recursos de la Auditoria de Firewall de la plataforma **SKYBOX** se encuentran estables.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CONTROL DE CAMBIOS** | | | | |
| **Revisión** | **Hecha por** | **Aprobada por** | **Fecha** | **Motivo** |
| 00 | ${autor} | Supervisor CyberSOC | 24/02/2022 | Versión Inicial |