**SECURESOFT CORPORATION**

**e-Secure Consulting Group**

**ESTADO DE PLATAFORMAS DE SEGURIDAD**

**Reporte Diario**

**Preparado para:**



**Fecha de elaboración:**

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



**El presente documento contiene información estrictamente privada y confidencial para Securesoft Corporation S.A.C. y Camposol.**

# OBJETIVO

Este documento dará a conocer la distribución de consumo de Internet y el estado de salud de las plataformas durante el último día.

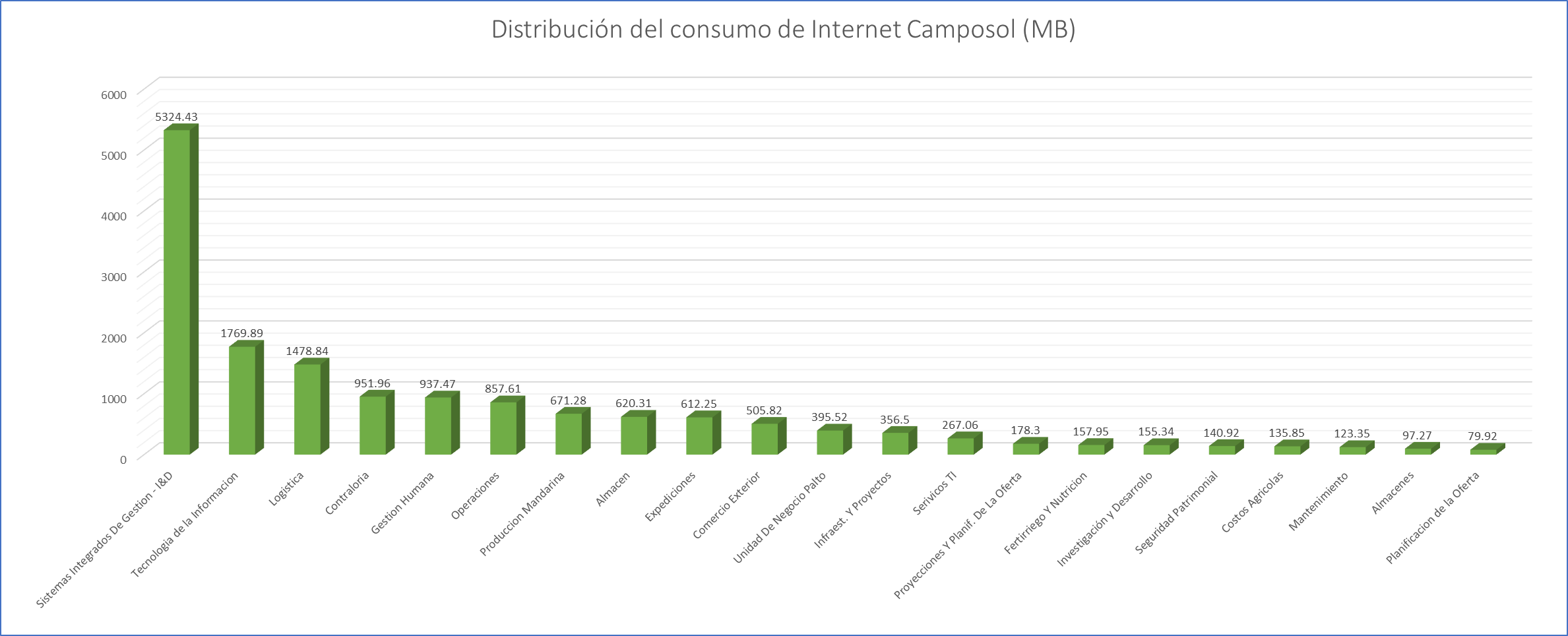
# ALCANCE

Este documento servirá como herramienta para verificar el consumo adecuado de Internet y el correcto funcionamiento de los equipos.

# CONTENIDO

## **PLATAFORMA EPO MCAFEE**

* **Distribución del consumo de Internet por Área (${fecha\_antes\_salsh} 00:00 – 23:59)**

****

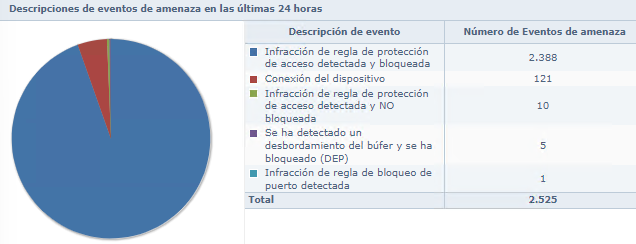
* El área **“Sistemas Integrados De Gestion - I&D”** es el que tiene el mayor consumo con un total de **5324.43 MB.**
* **Distribución del consumo de Internet por Usuario (${fecha\_antes\_salsh} 00:00 – 23:59)**



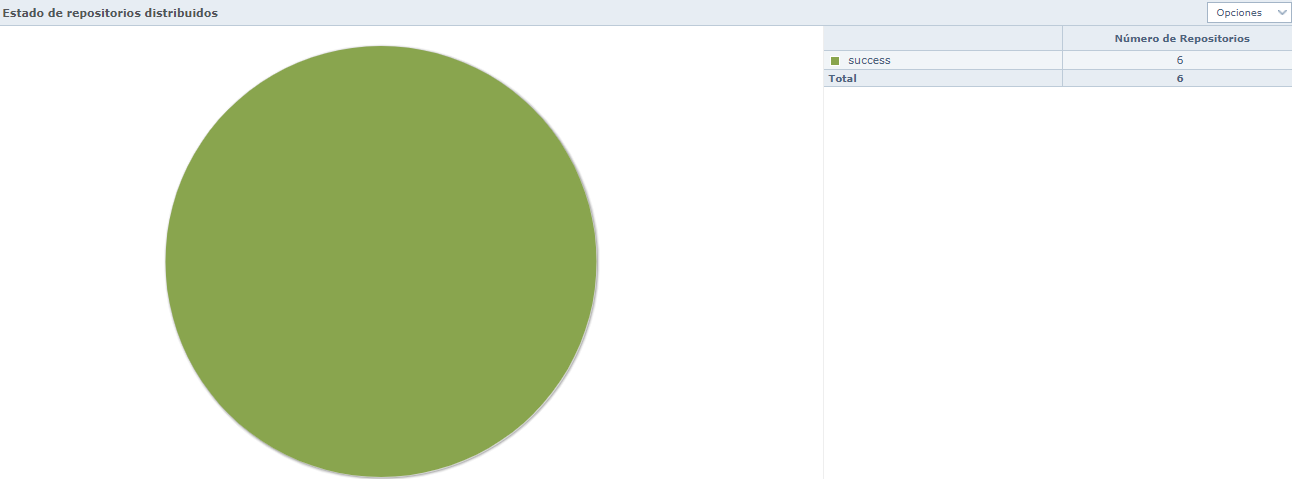
* El usuario que consumió más internet es **“mvalle”** con un total de **3543.04 MB.**
* **Recursos**

${graph2293}

* Se observó un uso de CPU de 2.79% durante el transcurso del día.
* Se observó un uso de Memoria de 77.45% durante el transcurso del día.
* Se observó un uso de Disco C de 55.13% durante el transcurso del día.
* Se observó un uso de Disco D de 31.12% durante el transcurso del día.
* Se observó un uso de Disco E de 31.12% durante el transcurso del día.
* **Eventos de Amenaza**

****

* Se presentaron eventos durante las últimas 24 horas.
* **Estado de Repositorios**



* Se observa que la replicación de los repositorios se realizó con éxito.

## **PLATAFORMAS CHECKPOINT**

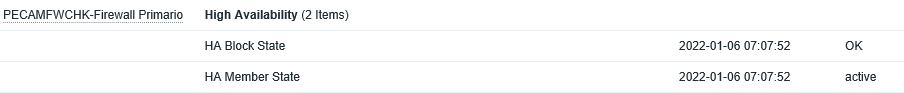
* 1. **SMARTCENTER**

*Recursos*

**${graph1489}**

* Se observó un uso de CPU 7.35% durante el transcurso del día.
* Se observó un uso de Disco de 88.85% durante el transcurso del día.
* Se observó un uso de Memoria de 45.33% durante el transcurso del día.
  1. **FIREWALL PRIMARIO**

*Estado*

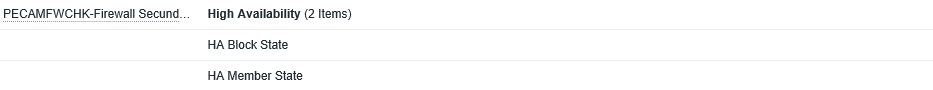


*Recursos*

${graph1477}

* Se observó un uso de CPU de 6.43% durante el transcurso del día.
* Se observó un uso de Disco de 21% durante el transcurso del día.
* Se observó un uso de Memoria de 17.90% durante el transcurso del día.
  1. **FIREWALL SECUNDARIO**

*Estado*

****

*Recursos*

${graph1479}

* Se observó un uso de CPU de 6.43% durante el transcurso del día.
* Se observó un uso de Disco de 21% durante el transcurso del día.
* Se observó un uso de Memoria de 17.90% durante el transcurso del día.
  1. **FIREWALL HOLANDA**

*Recursos*

**${graph1475}**

* Se observó un uso de CPU de 5.62% durante el transcurso del día.
* Se observó un uso de Disco de 59% durante el transcurso del día.
* Se observó un uso de Memoria de 54.25% durante el transcurso del día.
  1. **FIREWALL USA**

*Recursos*

**${graph1481}**

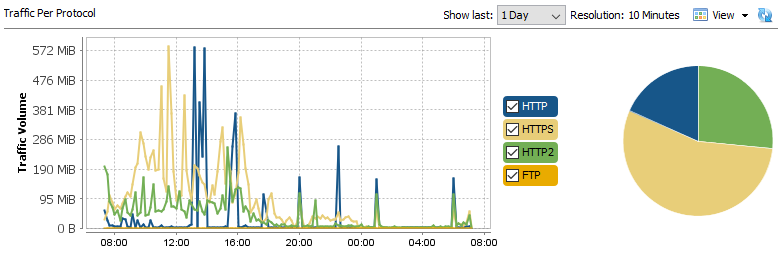
* Se observó un uso de CPU de 3.57% durante el transcurso del día.
* Se observó un uso de Disco de 56% durante el transcurso del día.
* Se observó un uso de Memoria de 43.09% durante el transcurso del día.
  1. **FIREWALL VPN**

*Recursos*

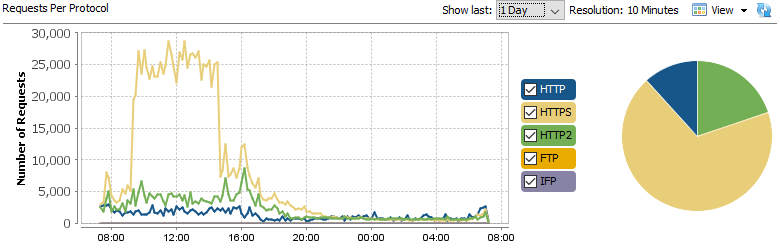
**${graph1483}**

* Se observó un uso de CPU de 0.08% durante el transcurso del día.
* Se observó un uso de Disco de 11% durante el transcurso del día.
* Se observó un uso de Memoria de 29.43% durante el transcurso del día. 
  1. **PROXY 01 MCAFEE**

*Traffic Per Protocol*

****

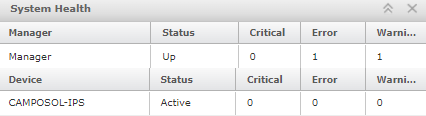
*Requests Per Protocol*

****

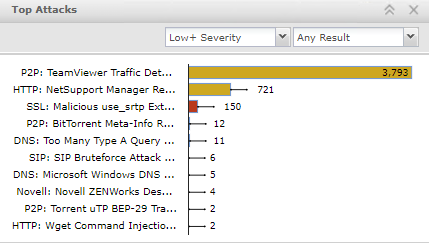
* Se observa que las conexiones se encuentran estables.

## **PLATAFORMA NSM** **MCAFEE**

* **Estado de salud**

****

* **Eventos**

****

# CONCLUSIONES

* El área **“Sistemas Integrados** **De** **Gestion** **- I&D**” es el que tiene el mayor consumo con un total de **5324.43 MB**.
* El usuario que consumió más internet es **“mvalle**”con un total de **3543.04MB.**
* La alerta del alto uso de memoria del equipo **Antivirus ePO** fue reportado bajo el **INC 231832,** donde después de la revisión, el Ing. asignado mencionó que siempre ha presentado este comportamiento con el consumo de memoria, y se estará validando si es posible reducir este consumo. Actualmente se encuentra dentro del umbral.
* Los recursos de los Firewalls son estables.
* Se observa alerta de Error y Warning en el **NSM,** fue notificado bajo el ticket **INC 242220,** donde se menciona que el Warning presentado es debido a que en las políticas está habilitado el envío de syslogs, y la alerta de "Error" es debido a que el email server se encuentra dañado y se validó con el onsite que están tratando de levantarlo.
* Se valida que el tráfico por protocolo se encuentra dentro de los umbrales, en el horario laboral de Camposol.
* Se adjunta el archivo **SOC\_FOR\_05\_RPD\_CAM\_AMCORE\_${fecha\_antes}**.
* Se adjunta el archivo **SOC\_FOR\_05\_RPD\_CAM\_NAVEGACION A INTERNET\_${fecha\_antes}**.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Revisión** | **Hecha por** | **Aprobada por** | **Fecha** | **Motivo** |
| 00 | ${autor} | Supervisor CyberSOC | 09/01/22 | Versión Inicial |