**SECURESOFT CORPORATION**

**e-Secure Consulting Group**

**REPORTE MENSUAL**

**Preparado para:**



**Fecha de elaboración:**

**${fecha\_actual}**

****

**El presente documento contiene información estrictamente privada y confidencial entre SECURESOFT CORPORATION S.A.C. y PROCESOS DE MEDIOS DE PAGO S.A.**

1. **OBJETIVO**

Este documento dará a conocer el estado de las plataformas de seguridad durante el último mes.

1. **ALCANCES**

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

1. **ESTADO DE LAS PLATAFORMAS**

# FIREWALL CHECKPOINT

**CONSOLA DE GESTIÓN (172.30.0.223)**

* **Recursos:**

${graph1143}

* Se observó que el uso promedio de **CPU** durante el mes es de 3.99%.
* Se observó que el uso promedio de **Disco** durante el mes es de 78.66%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 55.17%.

**FIREWALL SG5400 INTERNO PRIMARIO (172.30.0.2)**

* **Recursos:**

${graph1369}

* Se observó que el uso promedio de **CPU** durante el mes es de 11.31%.
* Se observó que el uso promedio de **Disco** durante el mes es de 20%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 19.82%.
* **Conexiones Recurrentes:**

${graph1372}

* Se observó un uso promedio de **24.52 K** conexiones concurrentes durante el mes.

**FIREWALL SG5400 INTERNO SECUNDARIO (172.30.0.3)**

* **Recursos:**

${graph1428}

* Se observó que el uso promedio de **CPU** durante el mes es de 3.68%.
* Se observó que el uso promedio de **Disco** durante el mes es de 18.47%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 19.58%.
* **Conexiones Recurrentes:**

${graph1431}

* Se observó un uso promedio de **24.52 K** conexiones concurrentes durante el mes.

**FIREWALL SG6200 CHECKPOINT EXTERNO PRIMARIO (172.30.1.2)**

* **Recursos:**

${graph1497}

* Se observó que el uso promedio de **CPU** durante el mes es de 0.94%.
* Se observó que el uso promedio de **Disco** durante el mes es de 6.66%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 21%.
* **Conexiones Recurrentes:**

${graph1500}

* Se observó un uso promedio de **1.53 K** conexiones concurrentes durante el mes.

**FIREWALL SG6200 CHECKPOINT EXTERNO SECUNDARIO (172.30.1.3)**

* **Recursos:**

${graph1509}

* Se observó que el uso promedio de **CPU** durante el mes es de 0%.
* 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 21%.
* **Conexiones Recurrentes:**

${graph1512}

* Se observó un uso promedio de **1.32 K** conexiones concurrentes durante el mes.

# BALANCEADORES F5

**BALANCEADOR F5 - BIG-IP-5250V - LTM01 (172.30.0.219)**

* **Recursos:**

${graph1336}

* Se observó que el uso promedio de **Disco** durante el mes es de 24%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 9%.
* Se observó que el uso promedio de **CPU** durante el mes es de 4.57%.
* **Conexiones Recurrentes:**

${graph1338}

* Se observó un uso promedio de **320.73 K** conexiones concurrentes durante el mes.
* **Bytes Per Second**

${graph1332}

**BALANCEADOR F5 - BIG-IP-5250V - LTM02 (172.30.0.220)**

* **Recursos:**

${graph1351}

* Se observó que el uso promedio de **Disco** durante el mes es de 24%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 2%.
* Se observó que el uso promedio de **CPU** durante el mes es de 3%.
* **Conexiones Recurrentes:**

${graph1353}

* Se observó un uso promedio de **8.26** conexiones concurrentes durante el mes.
* **Bytes Per Second**

${graph1347}

# WAF F5

**WAF F5 - BIG-IP 5250V - ASM01 (172.30.0.217)**

* **Recursos:**

${graph1276}

* Se observó que el uso promedio de **Disco** durante el mes es de 24%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 6.24%.
* Se observó que el uso promedio de **CPU** durante el mes es de 21.85%.
* **Conexiones Recurrentes:**

${graph1278}

* Se observó un uso promedio de **1.02 K** conexiones concurrentes durante el mes.
* **Bytes Per Second**

${graph1272}

**WAF F5 - BIG-IP 5250V - ASM02 (172.30.0.218)**

* **Recursos:**

${graph1291}

* Se observó que el uso promedio de **Disco** durante el mes es de 24%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 5%.
* Se observó que el uso promedio de **CPU** durante el mes es de 18.91%.
* **Conexiones Recurrentes:**

${graph1293}

* Se observó un uso promedio de **3.16** conexiones concurrentes durante el mes.
* **Bytes Per Second**

${graph1287}

# VPN SSL - PULSE SECURE

[**PULSE SECURE VIRTUAL**](https://172.26.157.226/zabbix/hosts.php?form=update&hostid=10304&groupid=30) **(172.40.0.5)**

* **Recursos**

${graph1601}

* Se observó que el uso promedio de **CPU** durante el mes es de 4.16%.
* Se observó que el uso promedio de **Disco** durante el mes es de 39.69%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 5.53%.
* **Conexiones Concurrentes**

${graph1585}

* Se observo un uso promedio de **108.93** conexiones concurrentes durante el mes.

# CISCO ASA

[**Cisco**](https://172.26.157.226/zabbix/hosts.php?form=update&hostid=10304&groupid=30) **ASA 5525 – MOVISTAR (172.30.1.4)**

* **UpTime**



* **Recursos**

${graph1190}

* Se observó que el uso promedio de **CPU** durante el mes es de 4.23%.

[**Cisco**](https://172.26.157.226/zabbix/hosts.php?form=update&hostid=10304&groupid=30) **ASA 5525 – OPTICAL (172.30.1.5)**

* **UpTime**



* **Recursos**

${graph1240}

* Se observó que el uso promedio de **CPU** durante el mes es de 12.53%.

[**Cisco**](https://172.26.157.226/zabbix/hosts.php?form=update&hostid=10304&groupid=30) **ASA 5506 – INTERNO WIFI (172.30.1.8)**

* **UpTime**



* **Recursos**

${graph1187}

* Se observó que el uso promedio de **CPU** durante el mes es de 2.87%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 72%.

# IPS CISCO

[**Consola de Gestión IPS**](https://172.26.157.226/zabbix/hosts.php?form=update&hostid=10304&groupid=30) **(172.30.0.237)**

* **Recursos**

${graph1602}

* Se observó que el uso promedio de **Disco** durante el mes es de 43.43%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 49.39%.
* Se observó que el uso promedio de **CPU** durante el mes es de 32.18%.

[**IPS**](https://172.26.157.226/zabbix/hosts.php?form=update&hostid=10304&groupid=30) **7030 Lince (172.30.0.234)**

* **Recursos**

${graph1603}

* Se observó que el uso promedio de **CPU** durante el mes es de 7.10%.
* Se observó que el uso promedio de **Disco** durante el mes es de 46.46%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 79.16%.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

[**IPS**](https://172.26.157.226/zabbix/hosts.php?form=update&hostid=10304&groupid=30) **7120 Monterrico (172.30.0.236)**

* **Recursos**

${graph1604}

* Se observó que el uso promedio de **CPU** durante el mes es de 29.56%.
* Se observó que el uso promedio de **Disco** durante el mes es de 56.86%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 62.85%.

Imagen que contiene Rectángulo

Descripción generada automáticamente

[**IPS**](https://172.26.157.226/zabbix/hosts.php?form=update&hostid=10304&groupid=30) **7030 Monterrico (172.30.0.235)**

* **Recursos**

${graph1605}

* Se observó que el uso promedio de **CPU** durante el mes es de 2.07%.
* Se observó que el uso promedio de **Disco** durante el mes es de 50.29%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 73.28%.

Gráfico

Descripción generada automáticamente

# ANTISPAM - CISCO

**ANTISPAM ESA PRIMARIO (192.168.100.31)**

* **Status**

**UPTIME**



* **Recursos**

${graph1578}

* Se observó que el uso promedio de **CPU** durante el mes es de 58.66%.
* Se observó que el uso promedio de **Disco** durante el mes es de 100%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 2%.

**ANTISPAM ESA SECUNDARIO (192.168.100.32)**

**Status**

* **Uptime**



* **Recursos**

${graph1579}

* Se observó que el uso promedio de **CPU** durante el mes es de 48.27%.
* Se observó que el uso promedio de **Disco** durante el mes es de 100%
* Se observó que el uso promedio de **Memoria** durante el mes es de 2%.

**ANTISPAM ESA SMA (192.168.100.30)**

**Status**

* **Uptime**



* **Recursos**

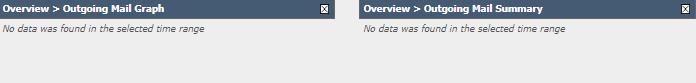
${graph1580}

* Se observó que el uso promedio de **CPU** durante el mes es de 0.59%.
* Se observó que el uso promedio de **Disco** durante el mes es de 100%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 2%.
* **Correos entrantes**

Gráfico

Descripción generada automáticamente

* **Correos salientes**



# IPS SONICWALL

# SONICWALL SOHO (172.30.1.106)

* **Recursos**

${graph1487}

* Se observó que el uso promedio de **CPU** durante el mes es de 14.47%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 43.52%.
* **Conexiones Concurrentes**

${graph1488}

* Se observó un uso promedio de **27.29** conexiones concurrentes durante el mes.

# SONICWALL SOHO250 (172.30.1.107)

* **Recursos**

${graph1490}

* Se observó que el uso promedio de **CPU** durante el mes es de 0.01%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 60.40%.
* **Conexiones Concurrentes**

${graph1491}

* Se observó un uso promedio de **8.67** conexiones concurrentes durante el mes.

# FIREWALL JUNIPER

# JUNIPER DMZ01 (172.30.1.104)

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media

* **Recursos**

${graph1363}

* Se observó que el uso promedio de **CPU** durante el mes es de 15.05%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 28%.

# JUNIPER PERSO 172.30.1.105

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

* **Recursos**

${graph1364}

* Se observó que el uso promedio de **CPU** durante el mes es de 10.77%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 28.43%.

# JUNIPER DMZ02 (172.30.1.108)

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

* **Recursos**

${graph1365}

* Se observó que el uso promedio de **CPU** durante el mes es de 11.46%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 29.65%.

# RSA

# RSA SIEM

**RSA-SECURITY ANALITICS-ESA-MC (172.30.0.29)**

${graph1717}

* Se observó que el uso promedio de **CPU** durante el mes es de 2.88%.
* Se observó que el uso promedio de **Disco** durante el mes es de 0%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 21%.

**RSA-SECURITY ANALITICS - HYBRIDLOG-MC (172.30.0.28)**

${graph1688}

* Se observó que el uso promedio de **CPU** durante el mes es de 11.23%.
* Se observó que el uso promedio de **Disco** durante el mes es de 23%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 46.13%.

**RSA-SECURITY ANALITICS - SARE-MC (172.30.0.30)**

${graph1718}

* Se observó que el uso promedio de **CPU** durante el mes es de 2%.
* Se observó que el uso promedio de **Disco** durante el mes es de 0%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 46.84%.

# RSA SECUREID

**RSA-AUTHENTICATION MANAGER - TOKENS-MC (172.16.28.29)**

${graph2000}

* Se observó que el uso promedio de **CPU** durante el mes es de 1.005%.
* Se observó que el uso promedio de **Disco** durante el mes es de 16%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 95.95%.

# Resumen

|  |  |  |
| --- | --- | --- |
| Host | Status | Disponibilidad |
| IPS CISCO | | |
| IPS 7120 (Monterrico) | UP | 100% |
| IPS 7030 (Lince) | UP | 100% |
| IPS 7030 (Monterrico) | UP | 100% |
| "CONSOLA DE ADMINISTRACION VIRTUAL FIRESIGHT" | UP | 100% |
| FIREWALL CHECKPOINT (EXTERNO) | | |
| FIREWALL SG6200 | UP | 100% |
| FIREWALL SG6200 | UP | 100% |
| SMART-1 5 | UP | 100% |
| FIREWALL CHECKPOINT (INTERNO) | | |
| FIREWALL SG5400 | UP | 100% |
| FIREWALL SG5400 | UP | 100% |
| BALANCEADOR F5 | | |
| BALANCEADOR F5 - BIG-IP 5250V - LTM01 | UP | 100% |
| BALANCEADOR F5 - BIG-IP 5250V - LTM02 | UP | 100% |
| WAF F5 | | |
| WAF F5 - BIG-IP-5250V - ASM01 | UP | 100% |
| WAF F5 - BIG-IP-5250V - ASM02 | UP | 100% |
| SECURITY ANALYITCS RSA | | |
| Series5S HeadUnit-Anlytics Svr 10 User TR - ESA | UP | 100% |
| Series5S HeadUnit-Anlytics Svr 10 User TR - HYBRIDLOG | UP | 100% |
| Series6S HeadUnit-Anlytics Svr 10 User TR - SARE | UP | 100% |
| TOKEN RSA | | |
| Token RSA SecurID Authentication Manager | UP | 100% |
| ANTISPAM CISCO | | |
| ESA-ESP-1Y-S3 | Premium SW Bundle (AS+AV+OF+ENC+DLP) 1YR Lic, 500-999 Users | UP | 100% |
| ESA-ESP-1Y-S3 | Premium SW Bundle (AS+AV+OF+ENC+DLP) 1YR Lic, 500-999 Users | UP | 100% |
| ESA-ESP-1Y-S3 | Premium SW Bundle (AS+AV+OF+ENC+DLP) 1YR Lic, 500-999 Users | UP | 100% |
| FIREWALL JUNIPER (PERSONALIZACION) | | |
| SRX320HE2 - SRX SERVICES GATEWAY 320 WITH 2XGE + 6XFE PORTS, 1XMINI-PIM SLOT, 2GB DRAM AND 2GB | UP | 100% |
| SVC-ND-SRX320 - Juniper Care NextDay Support for SRX320 | UP | 100% |
| SVC-ND-SRX320 - Juniper Care NextDay Support for SRX320 | UP | 100% |
| IPS SONIC WALL | | |
| SONICWALL SOHO | UP | 100% |
| SONICWALL SOHO250 | UP | 100% |
| VPN SSL | | |
| VPN Pulse Secure Virtual | UP | 100% |
| VPN, FIREWALL CISCO ASA (INTERNET) | | |
| CISCO ASA 5525 CON FIREPOWER - OPTICAL | UP | 100% |
| CISCO ASA 5525 CON FIREPOWER - MOVISTAR | UP | 100% |
| CISCO ASA 5525 CON FIREPOWER - INTERNO WIFI | UP | 100% |

# CONCLUSIONES

* Se valida que el promedio de los recursos de los firewalls de la plataforma **CHECK POINT** se encuentran estables.
* Se valida que el promedio de los recursos de los balanceadores de la plataforma **F5** se encuentran estables.
* Se valida que el promedio de los recursos de los WAF de la plataforma **F5** se encuentran estables.
* Se valida que el promedio de los recursos de la VPN SSL de la plataforma **PULSE SECURE VIRTUAL** se encuentran estables.
* Se valida que el promedio de los recursos de los firewalls de la plataforma **JUNIPER** se encuentran estables.
* Se valida que el promedio de los recursos de los firewalls de la plataforma **CISCO ASA** se encuentran estables.
* Se valida que el promedio de los recursos de los IPS de la plataforma **CISCO** se encuentran estables.
* Se valida que el promedio de los recursos de los antispam de la plataforma **CISCO** se encuentran estables.
* Se valida que el promedio de los recursos de los IPS de la plataforma **SONICWALL** se encuentran estables.
* Se observa un alto consumo de disco en el CHECKPOINT-MANAGEMENT FIREWALL-MC, el cual fue reportado bajo INC 290276.
* Se observa las conexiones concurrentes estable.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Tabla de Criterios del consumo de Recursos de las plataformas** | | | | | |
| **Estado** | **CPU** | **Memoria** | **Disco** | **Conexiones** | **Acciones** |
| Crítico | Mayor/igual a 90 % | Mayor/igual a 90 % | Mayor/igual a 90 % | Mayor/igual a 90 % | Hacer la revisión urgente del inconveniente, de ser necesario se abrirá un caso con el fabricante. |
| Alertado | Entre 80 y 90 % | Entre 80 y 90 % | Entre 80 y 90 % | Entre 80 y 90 % | Revisar el motivo del incremento de la utilización de los recursos. |
| Normal | Hasta 80% | Hasta 80% | Hasta 80% | Hasta 80% | Monitorear si está incrementándose la utilización. Si se mantiene debajo de lo declarado no será necesario realizar alguna acción. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CONTROL DE CAMBIOS** | | | | |
| **Revisión** | **Hecha por** | **Aprobada por** | **Fecha** | **Motivo** |
| a00 | ${autor} | Supervisor CyberSOC | 12/03/2022 | Versión Inicial |