

**SECURESOFT CORPORATION**

**e-Secure Consulting Group**

**REPORTE DE SALUD**

**Preparado para:**



**Fecha de elaboración:**

**${fecha\_actual}**

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

**S.A.C. y TRANSPORTES BLINDADOS HERMES S.**

**INDICE**

[**I. OBJETIVO 3**](#_Toc90044526)

[**II. ALCANCES 3**](#_Toc90044527)

[**III. ESTADO DE LAS PLATAFORMAS 3**](#_Toc90044528)

[**1. Firewall Palo Alto Activo 3**](#_Toc90044529)

[**1.1. Certificados 3**](#_Toc90044530)

[**1.2. Licencias 3**](#_Toc90044531)

[**1.3. Estado 4**](#_Toc90044532)

[**1.4. Vista del Sistema Palo Alto 5**](#_Toc90044533)

[**1.5. Recursos 5**](#_Toc90044534)

[**1.6. Visualización de las sesiones bgp del Sistema Palo Alto 6**](#_Toc90044535)

[**2. Firewall PaloAlto Pasivo 7**](#_Toc90044536)

[**2.1. Certificados 7**](#_Toc90044537)

[**2.2. Licencias 7**](#_Toc90044538)

[**2.3. Firewall PaloAlto 2 8**](#_Toc90044539)

[**2.4. Vista del Sistema Palo Alto 9**](#_Toc90044540)

[**2.5. RECURSOS 9**](#_Toc90044541)

[**2.6. Visualización de las sesiones bgp del Sistema Palo Alto 10**](#_Toc90044542)

[**IV. Seguridad PaloAlto 11**](#_Toc90044543)

[**1. Eventos de Seguridad 11**](#_Toc90044544)

[**2. Aplicaciones Detectadas 11**](#_Toc90044545)

[**3. Top 10 de los usuarios que realizan tráfico malicioso en las últimas 24h 12**](#_Toc90044546)

[**4. Categoría de amenazas durante las últimas 24 horas. 12**](#_Toc90044547)

[**V. Estados de Servidores 13**](#_Toc90044548)

[**VI. CONCLUSIONES 14**](#_Toc90044549)

# OBJETIVO

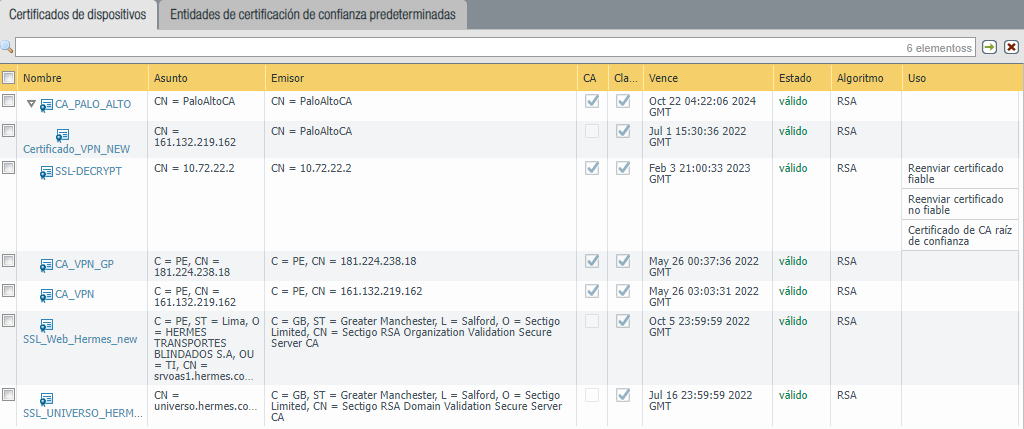
Este documento dará a conocer el estado de las plataformas de seguridad durante el último día.

# ALCANCES

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

# ESTADO DE LAS PLATAFORMAS

* 1. **Firewall Palo Alto Activo**
  2. **Certificados**



Se valida que los certificados se encuentran actualizados.

* 1. **Licencias**

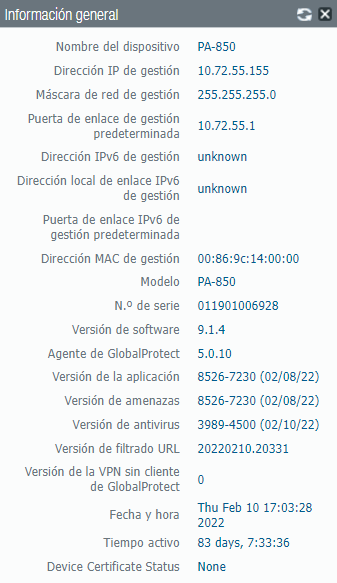
Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

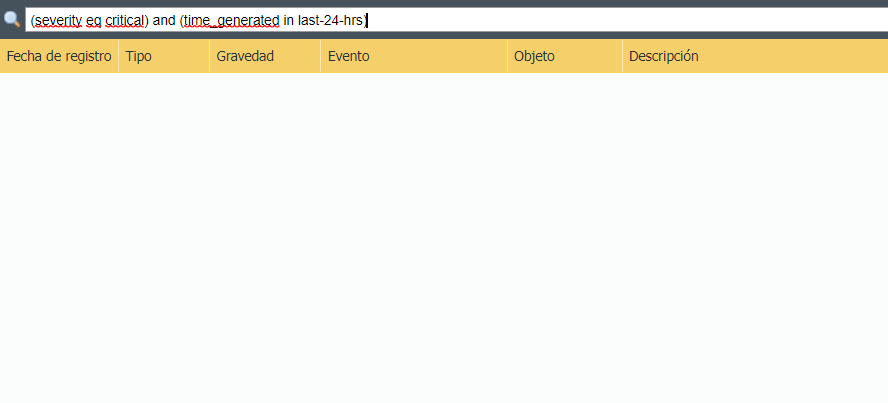
Se observa licencia caducada. Se viene revisando bajo **SOL 247246.**

* 1. **Estado**

****



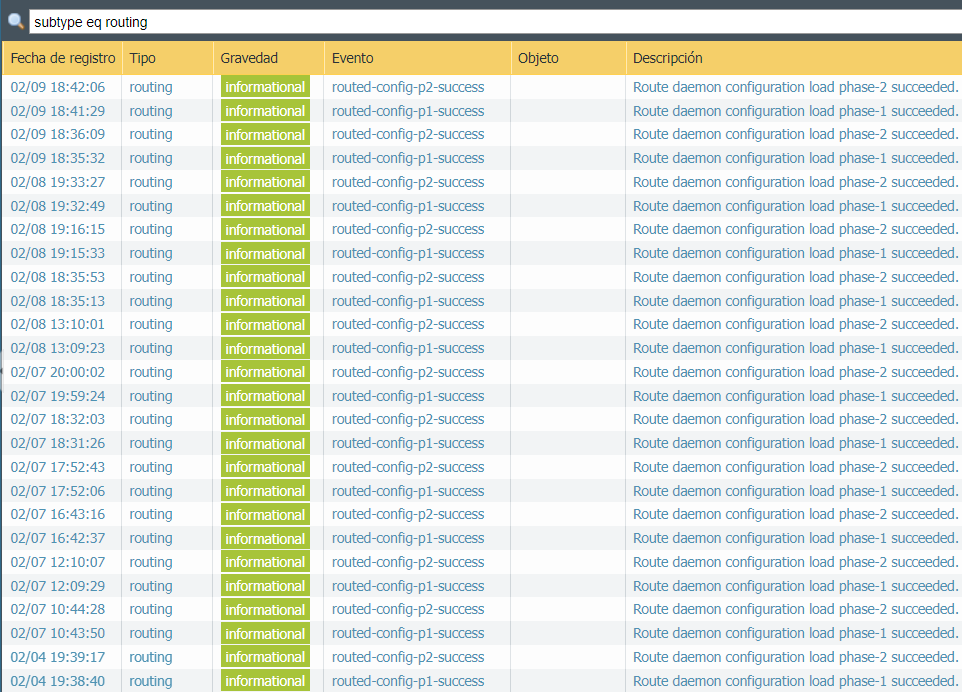
* 1. **Vista del Sistema Palo Alto**

****

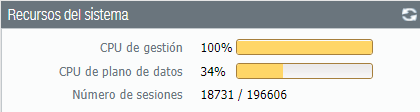
* No se observaron alertas críticas en el equipo.
  1. **Recursos**

${graph1554}

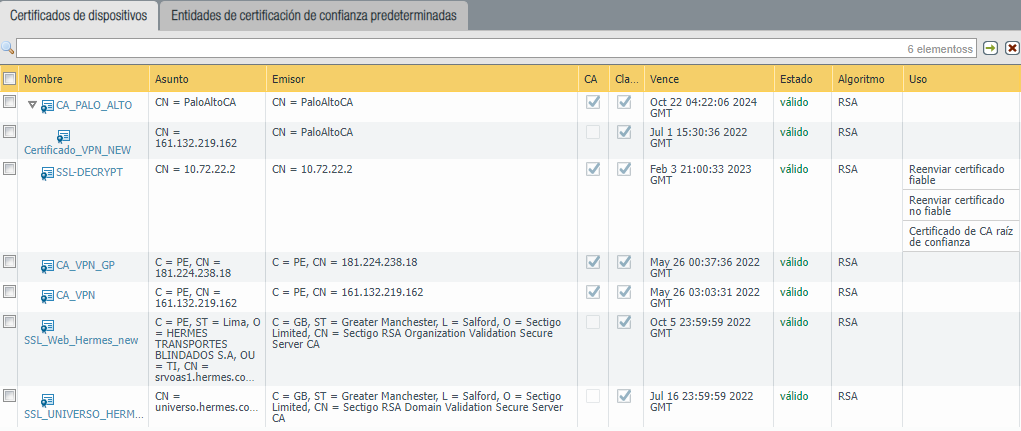
* 1. **Visualización de las sesiones bgp del Sistema Palo Alto**



* + - No se observan alertas críticas en el equipo.



* 1. **Firewall PaloAlto Pasivo**
  2. **Certificados**



Se valida que los certificados se encuentran actualizados.

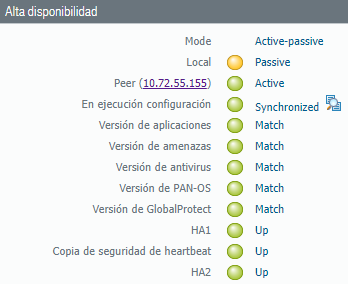
* 1. **Licencias**

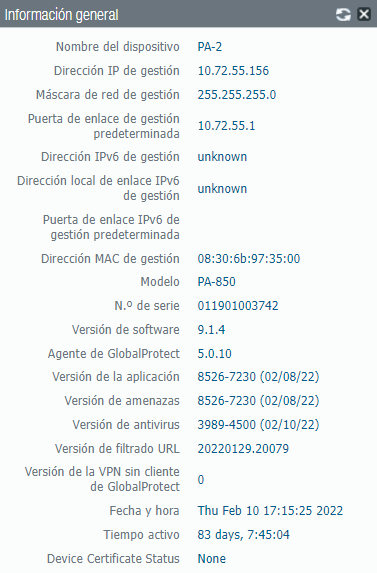
Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

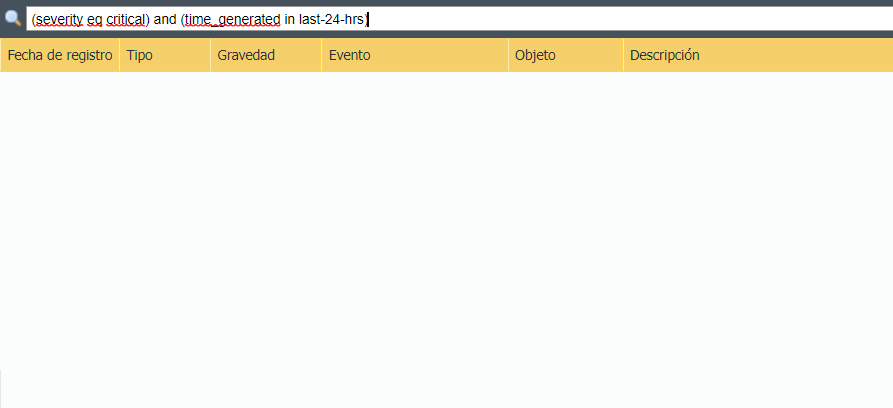
Se observan licencias vencidas. Se viene revisando bajo **SOL247246.**

* 1. **Firewall PaloAlto 2**

****



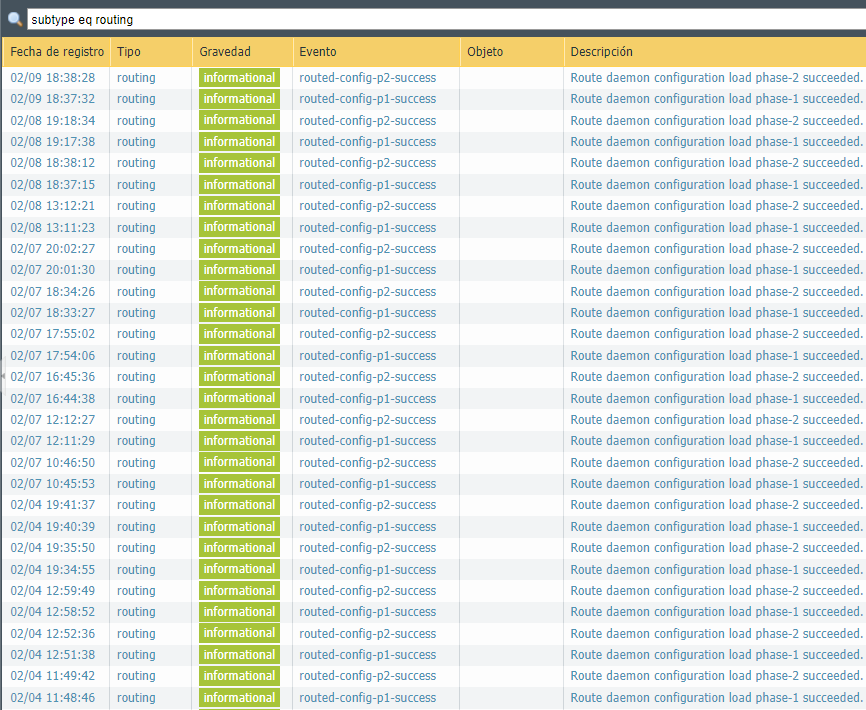
* 1. **Vista del Sistema Palo Alto**

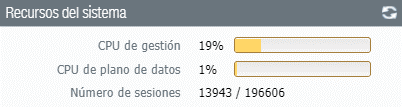
****

* No se observaron alertas críticas en el equipo.
  1. **RECURSOS**

${graph1556}

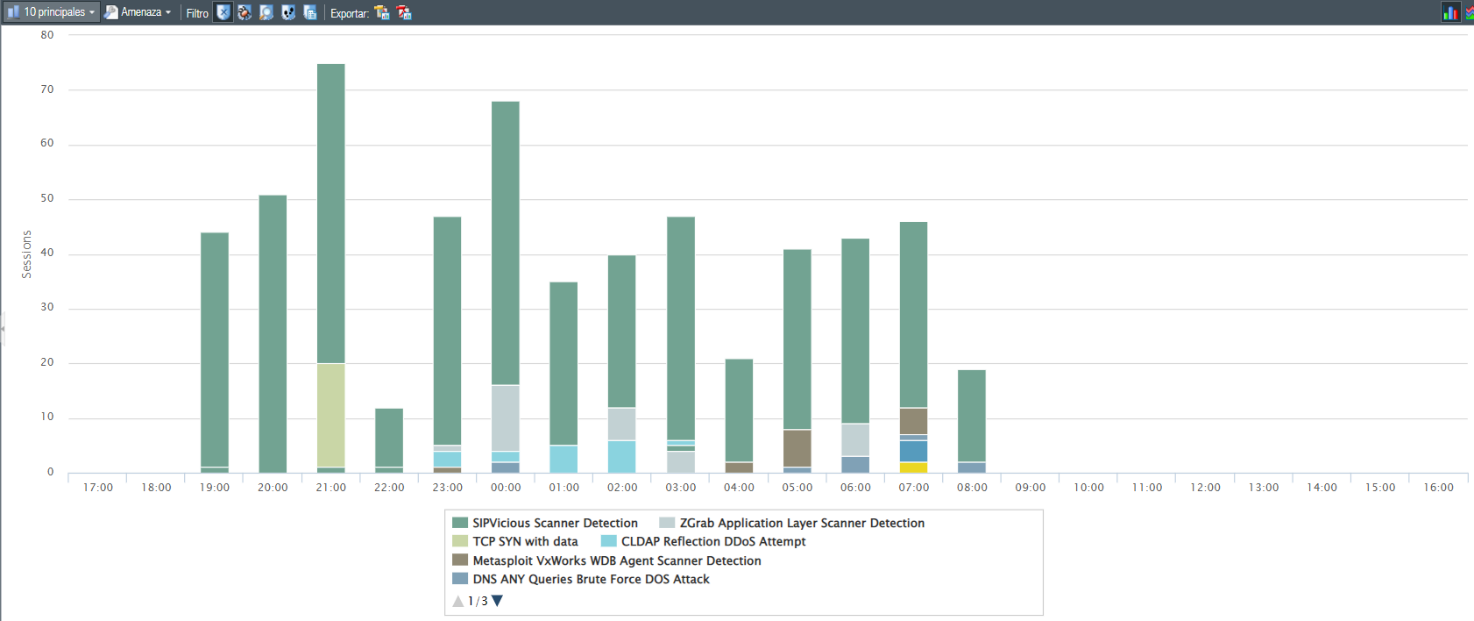
* 1. **Visualización de las sesiones bgp del Sistema Palo Alto**





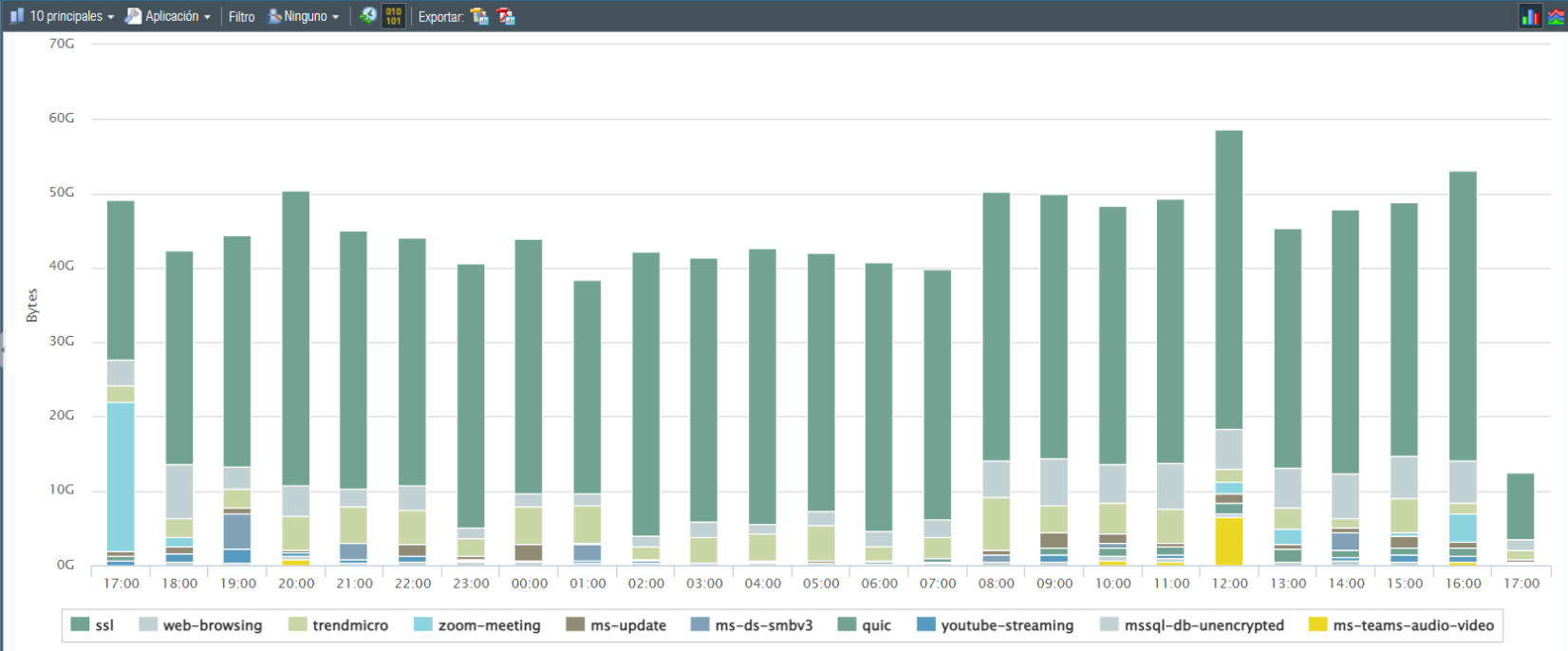
# Seguridad PaloAlto

1. **Eventos de Seguridad**

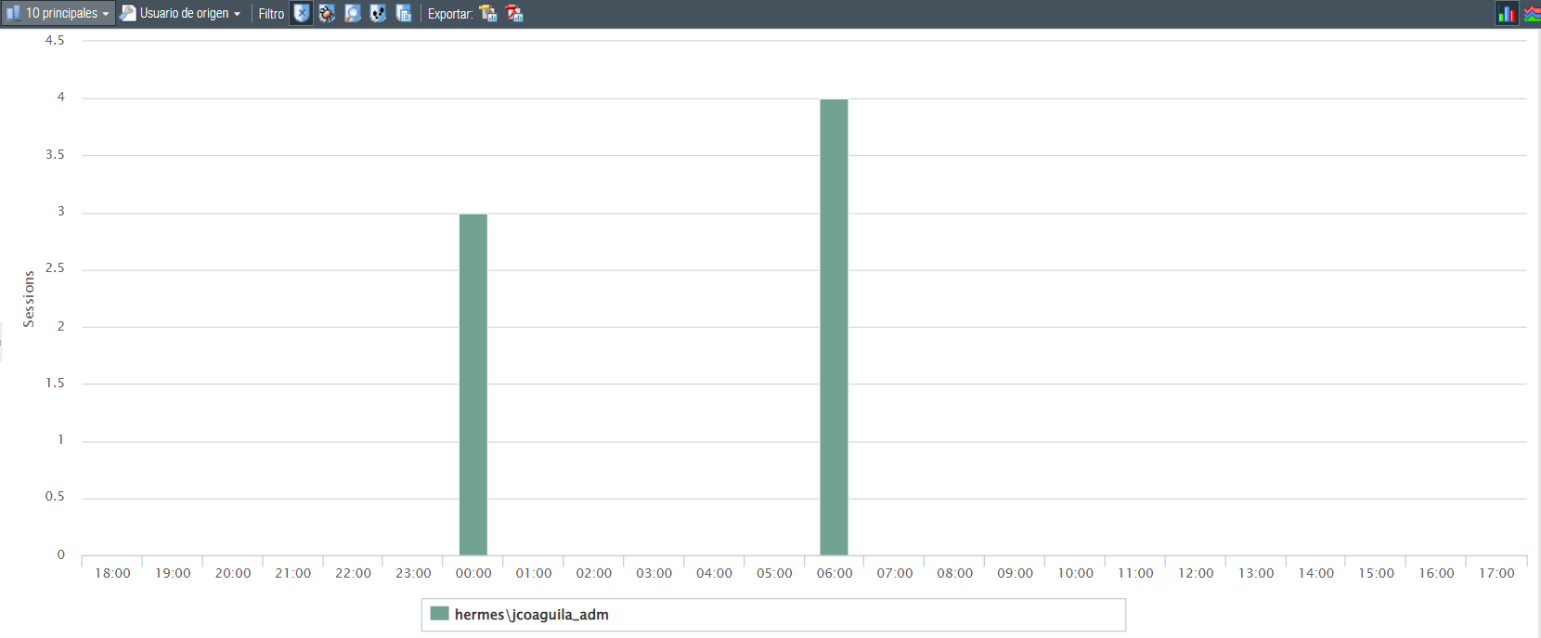
****

Se observaron eventos de seguridad, se viene revisando bajo el ticket **SOL XXXX.**

1. **Aplicaciones Detectadas**

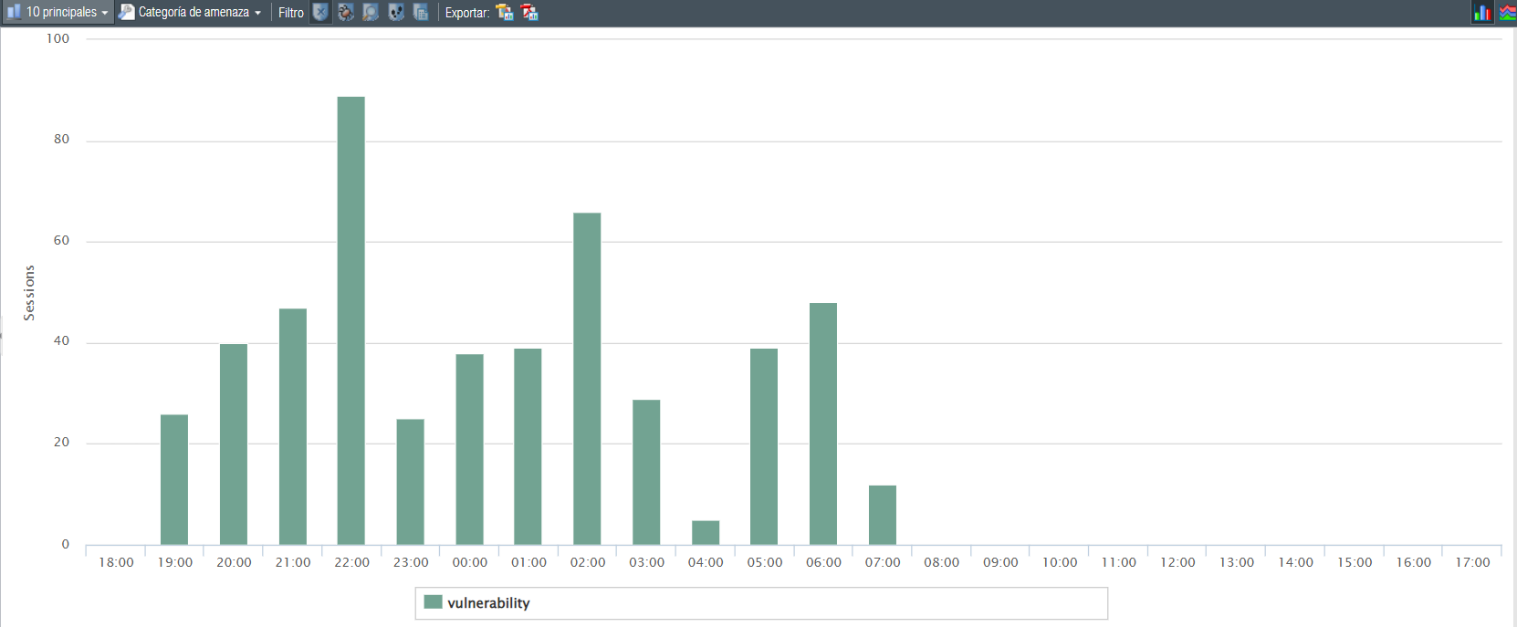


1. **Top 10 de los usuarios que realizan tráfico malicioso en las últimas 24h**

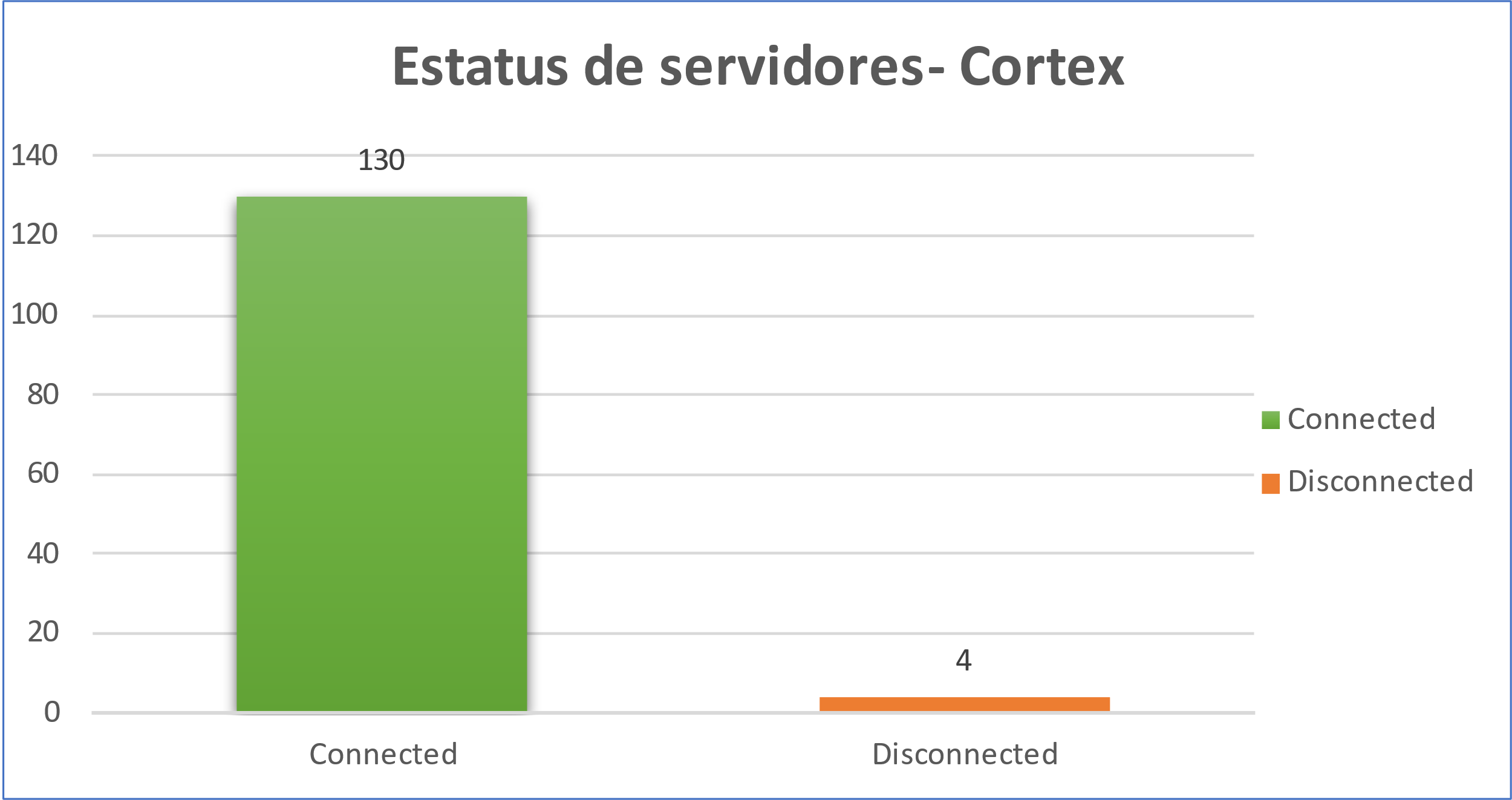


Se presentaron usuarios que realizaron tráfico malicioso en las últimas 24 horas

1. **Categoría de amenazas durante las últimas 24 horas.**



# Estados de Servidores

****

Se visualizan 134 servidores, de los cuales 130 están conectados y 4 desconectados.

* Detalle de Servidores desconectados

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Endpoint Name** | **Endpoint Type** | **Endpoint Status** | **Operating System** | **IP Address** |
| LPT-JBABARC | Workstation | Disconnected | Windows 10 | 10.72.3.235 |
| SRVSOPHOS | Server | Disconnected | Windows Server 2016 | 10.72.11.71 |
| srvtableau.hermes.com.pe | Server | Disconnected | RHEL 7.9 | 10.72.21.100 |
| RECLAMO07 | Workstation | Disconnected | Windows 10 | 10.72.6.53 |

* La PC **LPT-JBABARC** se viene revisando bajo el **INC 281865.** Donde comentan que se encuentre apagado, se estará validando el lunes 24/01/2022.
* El servidor **SRVSOPHOS** se viene revisando bajo el **INC 291647.** Donde en el ticket **INC 289793** mencionan que se gestionará para dar de baja al servidor.
* Los servidores **srvtableau.hermes.com.pe** se está trabajando con el cliente y fabricante bajo el ticket SOL 262508.
* La PC **RECLAMO07** se viene revisando bajo el **INC 290086.**

# CONCLUSIONES

* Los recursos de los equipos se encuentran estables.
* Las conexiones de los equipos se encuentran estables.
* Se verifica que los certificados fueron actualizados correctamente.
* No se observan alertas críticas en el sistema del equipoactualmente.
* Se observa licencia caducada. Se viene revisando bajo **SOL247246**. Donde se indica que la licencia vencida no afecta la operatividad de los servicios. Se valida que es un servicio adicional en la nube de palo alto la cual no se ha utilizado esto se activó durante las licencias temporales que se activaron en algún momento durante un proceso de renovación de licenciamiento, he revisado las licencias adquiridas en las renovaciones anteriores y no está el servicio adicional Logging Service.
* Se observa servidores desconectados.
* La PC **LPT-JBABARC** se viene revisando bajo el **INC 281865.** Donde comentan que se encuentre apagado, se estará validando el lunes 24/01/2022.
* El servidor **SRVSOPHOS** se viene revisando bajo el **INC 291647.** Donde en el ticket **INC 289793** mencionan que se gestionará para dar de baja al servidor.
* Los servidores **srvtableau.hermes.com.pe** se está trabajando con el cliente y fabricante bajo el ticket SOL 262508.
* La PC **RECLAMO07** se viene revisando bajo el **INC 290086.**
* Se observaron eventos de seguridad el día ${fecha\_antes\_salsh}, se revisó bajo el ticket **SOL XXXX**. Se valida que las firmas fueron bloqueadas, así mismo no se presentaron alertas en las últimas 24 horas.
* Se observaron eventos de seguridad el día ${fecha\_hoy}, se está revisando bajo el ticket **SOL XXXX.**

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