

# SECURE SOFT CORPORATION

**e-Secure Consulting Group**

**REPORTE SERVICIO GESTIONADO**

## Preparado para:



**Fecha:**

**Febrero del 2022**



**El presente documento contiene información estrictamente privada y confidencial para Securesoft Corp S.A.C. y Tienda Ripley.**

## OBJETIVO

Este documento dará a conocer el estado de la gestión del servicio de administración remota, soporte y monitoreo de las plataformas de seguridad de Tienda Ripley durante el último mes.

## ALCANCES

Este documento servirá como herramienta para verificar el correcto funcionamiento de los equipos, estado de las atenciones de los requerimientos y la recolección de eventos e información obtenida de las diferentes plataformas integradas en el SIEM.

## ESTADO DE SALU

## PLATAFORMA: CHECKPOINT

## Smart Center Tienda Virtual - 172.19.200.8

## Recursos

## ${graph1610}

## Smart Reporter Tienda Virtual - 172.19.200.7

## Recursos

**${graph1612}**

## FWEC01 - Tienda Virtual 01 - 172.19.200.2

## Recursos

${graph1583}

## Conexiones concurrentes

${graph1584}

## FWEC02 - Tienda Virtual 02 - 172.19.200.3

## Recursos

${graph1585}

## Conexiones concurrentes

${graph1586}

## Firewall Perimetral Tienda 01 – 172.19.200.161

## Recursos

${graph1592}

## Conexiones concurrentes

${graph1593}

## Firewall Perimetral 02 -- 172.19.200.162

## Recursos

${graph1594}

## Conexiones

${graph1595}

## FW CC01 - 172.19.200.53

## Recursos

${graph1402}

## Conexiones concurrentes

${graph1403}

## FW CC02 - 172.19.200.55

## Recursos

${graph1404}

## Conexiones concurrentes

${graph1405}

## FW VPN 01 - 172.19.200.46

## Recursos

${graph1596}

## Conexiones concurrentes

${graph1597}

## FW VPN 02 - 172.19.200.47

## Recursos

${graph1598}

## Conexiones concurrentes

${graph1599}

## FW PR01 LVL3 – 172.19.200.21

## Recursos

${graph1588}

## Conexiones concurrentes

${graph1589}

## FW PR02 LVL3 – 172.19.200.22

## Recursos

${graph1590}

## Conexiones concurrentes

${graph1591}

## PLATAFORMA: F5

## Balanceador (LCTV01) - Publicaciones – Activo - 172.19.200.37

## Recursos

${graph1573}

## Balanceador (LCTV02) - Publicaciones – Pasivo - 172.19.200.38

## Recursos

${graph1575}

## WAF (LTMTV01) - Aplicaciones – Activo - 172.19.200.28

## Recursos

${graph1577}

## WAF (LTMTV02) - Aplicaciones – Pasivo - 172.19.200.29

## Recursos

${graph1579}

## PLATAFORMA: MCAFEE

## Proxy - Tienda 01- 172.19.50.32

## Recursos

${graph1602}

## Conexiones concurrentes

${graph1603}

## Proxy - Tienda 02- 172.19.50.33

## Recursos

${graph1606}

## Conexiones concurrentes

${graph1607}

## EPO TIENDA (ANTIVIRUS) - 10.21.2.233

## Recursos

${graph2296}

## PLATAFORMA: PULSE SECURE

## Pulse Secure Nodo 01 – 172.20.200.101

## Recursos

${graph1615}

## Conexiones concurrentes

${graph1614}

## Pulse Secure Nodo 02 – 172.20.200.102

## Recursos

${graph1617}

## Conexiones concurrentes

${graph1616}

## Top 10 categorías de navegación más frecuentadas

## 

## Top 10 de URL más visitadas

## 

## Top 10 de usuarios con más consumo de ancho de banda

## 

## Top 10 usuarios de Facebook

## 

## Top 10 usuarios de Youtube

Gráfico

Descripción generada automáticamente

## 

1. **RECOMENDACIONES**
   * Restringir, a nivel de políticas en el AD, el perfil por default que se le brinda a los usuarios cuando se ingresa un equipo nuevo. Con esto se tendrá un mayor control de los nuevos kioscos que ingresen a producción. Con la finalidad que se aplique el perfil que le corresponde y no obtenga el perfil de AD por default (otorga mayores permisos de los que requiere).
   * Segmentar la red para evitar que ante una amenaza de malware se propague debido a que la red sea plana.
   * Revisar los permisos a nivel de perfiles web para navegación, a fin de mitigar el riesgo de infección a través de este medio.

## CONCLUSIONES

* Los recursos de las plataformas de seguridad estuvieron estables durante el mes.
* La categoría de navegación más frecuente durante el mes fue **Business.**
* La Url más visitada durante el mes, fue **dsmim.deepsecurity.trendmicro.com**.
* El usuario con más consumo de ancho de banda durante el mes fue **kioscotv.**
* El usuario que más consumió la aplicación Facebook durante el mes fue **kioscotv**.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CONTROL DE CAMBIOS** | | | | |
| **Revisión** | **Hecha por** | **Aprobada por** | **Fecha** | **Motivo** |
| 00 | ${autor} | Supervisor CyberSOC | 14/02/2022 | Versión Inicial |

* El usuario que más consumió la aplicación Youtube durante el mes fue **kioscotv.**