# REPORTE MENSUAL

# RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA

## OC124016

## JULIO 2024

ifx Networks | CARE Centro de Atención Regional

## Contenido

## *1. INFORMACIÓN TÉCNICA DEL INFORME*

| | |
|---|---|
| Nombre | Informe de disponibilidad de servidores y recursos de **RAMA JUDICIAL – CONSEJO SUPERIOR DE LA JUDICATURA** alojados en Infraestructura IFX |
| Descripción | En el presente informe se visualiza la disponibilidad de los servidores y recursos contratados por **RAMA JUDICIAL – CONSEJO SUPERIOR DE LA JUDICATURA,** en el acuerdo marco Nube Privada IV OC 124016. |
| Finalidad | El informe presentado, se puede utilizar para evaluar la disponibilidad de los servidores y recursos contratados, bajo el acuerdo marco. |
| Parámetros | **Rango de fechas**<br>Período del informe: mensual<br>Fecha de inicio: 1 de JULIO de 2024<br>Fecha de final: 31 de JULIO de 2024 |
| Atributos de entrada | • Estado, % Memory Used, CPU LOAD, DISK SPACE USED, Top de Usados. |
| Tablas vistas o utilizadas | Reporte Mensual **RAMA JUDICIAL – CONSEJO SUPERIOR DE LA JUDICATURA** |
| Salida | Este informe contiene tablas en las que se visualizan porcentajes de uso y disponibilidad de las entradas evaluadas para determinar la disponibilidad. |
| Uso | El documento se genera como parte de la documentación entregada a final de cada mes y compone el esquema de gestión de disponibilidad de los servicios contratados por parte de **RAMA JUDICIAL – CONSEJO SUPERIOR DE LA JUDICATURA** |

## 2. ALOJAMIENTO DE INFRAESTRUCTURA

| OC | SID | DESCRIPCIÓN | SUBTIPO | NOMBRE DEL EQUIPO | MODELO | SERIAL | UNIDAD DE RACK | RACK |
|---|---|---|---|---|---|---|---|---|
| 1 | 2081796 | npn04--Alojamiento deinfraestructura - Housing -Cross Conexión - Oro - Puntos de red: 4 - Capacidadde energía: 1 KVA -Capacidad en unidades: 4 U -Rack/M - Cantidad: 8 | CROSS CONEXIÓN DC Torre central | N/A | N/A | N/A | 31-32-37-45-46 | 31-32-69 |
| 2 | 2081805 | npn04--Alojamiento deinfraestructura - Housing -Full Rack - Oro - Puntos dered: 4 - Capacidad deenergía: 4 KVA - Capacidaden unidades: 42 U - Rack/M -Cantidad: 2 | Full Rack DC Torre central | N/A | N/A | N/A | N/A | 31-32 |
| 3 | 2081807 | npn04--Alojamiento deinfraestructura - Housing/Collocation - EnergíaAdicional KVA - Oro - KVA/Mes - Cantidad: 4 | Energía Adicional DC Torre central | Disponible para uso de la unidad | | | | |
| 4 | 2081810 | npn04--Alojamiento deinfraestructura - Housing/Colocation - Puntode Red Adicional - Oro - 10Gbps - Upra/M - Cantidad: 4 | Punto de Red Adicional DC Torre central | Se está dando uso de los 4 puntos de red adicionales por el proveedor CIRION | | | | 31 |
| 11 | 2081817 | npn04--IaaS Procesamiento -Balanceador de Carga AltaCapacidad - Oro - HostingNube Privada - SesionesCapa L4 (entre 36 y 100Millones) - RAM entre 64GB y128GB - U_Mes - Cantidad: 2 | Balanceador DC Torre central | FORTI/PPLA | ADC-2200F | SN: FAD22FT221000028 | 10 | 32 |
| 11 | 2081818 | npn04--IaaS Procesamiento -Balanceador de Carga AltaCapacidad - Oro - HostingNube Privada - SesionesCapa L4 (entre 36 y 100Millones) - RAM entre 64GB y128GB - U_Mes - Cantidad: 2 | Balanceador DC Torre central | FORTI/BK | ADC-2200F | SN: FAD22FT221000027 | 9 | 32 |
| 30 | 2082020 | npn04--IaaS Seguridad - Appliance Anti Ddos - AltaCapacidad - Oro - Hostingfísico - Rol de Inspección - 50Gbps - Paquetes PorSegundo | DDOS DC Torre central | FORTIDDOS FORTINET 2000E/PPLA | 2000E | SN: FI2KETB20000015 | 31-32 | 32 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | (MPPS) - 45000000- Mes - Cantidad: 2 | | | | | | |
| 30 | 2082021 | npn04--IaaS Seguridad - Appliance Anti Ddos - AltaCapacidad - Oro - Hostingfísico - Rol de Inspección - 50Gbps - Paquetes PorSegundo (MPPS) - 45000000- Mes - Cantidad: 2 | DDOS DC Torre central | FORTIDDOS FORTINET 2000E/BK | 2000E | SN: FI2KE581900004 9 | 35-36 | 32 |
| 31 | 2082016 | npn04--IaaS Seguridad - Firewall Nueva Generación - Media Capacidad - Oro - Hosting físico - Rol deFirewall - 40 Gbps - SesionesConcurrentes - 15000000 -Mes - Cantidad: 2 | FIREWALL | PALACIO - PPLA | FortiGate 900G | SN: FG9H0GTB2390 0205 | N/A | N/A |
| 31 | 2082017 | npn04--IaaS Seguridad - Firewall Nueva Generación - Media Capacidad - Oro - Hosting físico - Rol deFirewall - 40 Gbps - SesionesConcurrentes - 15000000 -Mes - Cantidad: 2 | FIREWALL | PALACIO - BK | FortiGate 900G | SN: FG9H0GTB2390 0440 | N/A | N/A |
| 32 | 2082018 | npn04--IaaS Seguridad - Firewall Nueva Generación - Alta Capacidad - Oro - Hosting físico - Rol deFirewall - 500 Gbps - Sesiones Concurrentes - 150000000 - Mes - Cantidad:2 | FIREWALL DC Torre central | DATACENTER - BK | FORTIGATE-4400F | SN: FG440FTK219001 83 | 27-30 | 32 |
| 32 | 2082019 | npn04--IaaS Seguridad - Firewall Nueva Generación - Alta Capacidad - Oro - Hosting físico - Rol deFirewall - 500 Gbps - Sesiones Concurrentes - 150000000 - Mes - Cantidad:2 | FIREWALL DC Torre central | DATA CENTER - PPLA | FORTIGATE-4400F | SN: FG440FTK219001 84 | 5-8 | 32 |
| 33 | 2082013 | npn04--IaaS Seguridad - WebAplication Firewall - AltaCapacidad - Oro - Hostingfísico - Desempeño WAF(Gbps) - 10 - Mes - Cantidad:3 | WAF DC Torre central | DATACENTER - PPLA | KEMP LM-X25 | SN: TSCC820 05608 | 14 | 31 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 33 | 2082014 | npn04--IaaS Seguridad - WebAplication Firewall - AltaCapacidad - Oro - Hostingfísico - Desempeño WAF(Gbps) - 10 - Mes - Cantidad:3 | WAF DC Torre central | DATACENTER - BK | KEMP LM-X25 | SN: TSCB72000545 | 13 | 31 |
| 33 | 2082015 | npn04--IaaS Seguridad - WebAplication Firewall - AltaCapacidad - Oro - Hostingfísico - Desempeño WAF(Gbps) - 10 - Mes - Cantidad:3 | WAF | SEDE CAN | KEMP LM-X25 | SN: TSCC82005629 | N/A | N/A |

Infraestructura utilizada para la ubicación de los equipos de conectividad (proveedor IFX), de los equipos de seguridad perimetral (IFX), de los equipos de seguridad proactiva (Entidad), los cuales se encuentran en calidad de collocation y la Entidad de acuerdo con las necesidades ha contratado energía y puntos de red adicionales (proveedor CIRION) para el funcionamiento de la misma.

## 1. ALMACENAMIENTO

| OC | SID | DESCRIPCIÓN |
|---|---|---|
| 5 | 2081815 | IaaS almacenamiento - Almacenamiento SAN Alto Rendimiento - Oro - Alta - Nube Privada - Capacidad: 900TB a <1000TB - FC >= 8 Gbps - SSD - RAID: 5 - IOPS READ 72000 / WRITE 30000 - GB/Mes - Cantidad: 3700000 |
| 6 | 2081811 | IaaS almacenamiento - Almacenamiento SAN Alto Rendimiento - Oro - Alta - Nube Privada - Capacidad: 100TB a <200TB - FC >= 8 Gbps - SSD - RAID: 5 - IOPS READ 72000 / WRITE 30000 - GB/Mes - Cantidad: 100000 |
| 7 | 2081814 | IaaS almacenamiento - Backup de Datos - Alta - Capacidad: 200TB a <300TB - Disco Duro Externo - Mensual - GB/Mes - Cantidad: 250000 |
| 8 | 2081812 | IaaS almacenamiento - Backup de Datos - Alta - Capacidad: 100TB a <200TB - Almacenamiento SAN - Diaria - GB/Mes - Cantidad: 165000 |
| 9 | 2081813 | IaaS almacenamiento - Backup de Datos - Alta - Capacidad: 100TB a <200TB - Almacenamiento SAN - Semanal - GB/Mes - Cantidad: 185000 |
| 47 | 2082100 | npn04--IaaS almacenamiento- Almacenamiento SAN AltoRendimiento - Oro - Alta -Nube Privada - Capacidad 100TB a <200TB - FC >= 8Gbps - SSD - RAID: 5 - IOPSREAD 72000 / WRITE 30000- GB/Mes - Cantidad: 100000 |
| 48 | 2082101 | npn04--IaaS almacenamiento- Almacenamiento SAN AltoRendimiento - Oro - Alta -Nube Privada - Capacidad 100TB a <200TB - FC >= 8Gbps - SSD - RAID: 5 - IOPSREAD 72000 / WRITE 30000- GB/Mes - Cantidad: 100000 |
| 49 | 2082102 | npn04--IaaS almacenamiento- Almacenamiento SAN AltoRendimiento - Oro - Alta -Nube Privada - Capacidad:100TB a <200TB - FC >= 8Gbps - SSD - RAID: 5 - IOPSREAD 72000 / WRITE 30000- GB/Mes - Cantidad: 150000 |

El almacenamiento total aprovisionado en la infraestructura contratada, de conformidad con las solicitudes de la Entidad, a corte 31 de JULIO de 2024 es de: **3879483 (GB)**

El almacenamiento total presentado adicional es de: **3760928 (GB)**

Total, contratado de Almacenamiento SAN alto rendimiento: **4000000(GB)**

A corte 30 de JULIO 2024 la entidad cuenta con un almacenamiento disponible de **239072 (GB)**

**Acorde a la información suministrada con anterioridad a la fecha la entidad cuenta con almacenamiento disponible correspondiente a los siguientes ítems:**

**Ítem 49 de la Orden de compra 150000 GB**

**npn04--IaaS almacenamiento - Almacenamiento SAN Alto Rendimiento - Oro - Alta - Nube Privada - Capacidad: 100TB a <200TB - FC >= 8 Gbps - SSD - RAID: 5 - IOPS READ 72000 / WRITE 30000 - GB/Mes - Cantidad: 150000**

El cual se estima sea utilizado por la entidad a partir del mes de agosto 2024.

(Remitirse al anexo "**Inventario_Servicios_CSJ_JULIO_2024.xls**" para ver el detalle)

## *3. BACKUPS*

| No | ARTICULO | SIDOC124016 |
|---|---|---|
| 7 | npn04--IaaS almacenamiento- Backup de Datos - Alta - Capacidad: 200TB a <300TB- Disco Duro Externo -Mensual - GB/Mes -Cantidad: 250000 | 2081814 |
| 8 | npn04--IaaS almacenamiento- Backup de Datos - Alta - Capacidad: 100TB a <200TB- Almacenamiento SAN -Diaria - GB/Mes - Cantidad:165000 | 2081812 |
| 9 | npn04--IaaS almacenamiento- Backup de Datos - Alta - Capacidad: 100TB a <200TB- Almacenamiento SAN - Semanal - GB/Mes -Cantidad: 185000 | 2081813 |

El almacenamiento backup total usado en la infraestructura contratada, según el cuadro de la página 20 del documento "veeam backup CSJ_PDF", donde se resta la sumatoria de la columna 1 "CAPACIDAD", menos la sumatoria de la columna 2, "ESPACIO,ESPACIO LIBRE", de conformidad con las solicitudes de la Entidad, a corte 30 de JULIO de 2024, esta utilizando, una capacidad de 798389,1 GB en almacenamiento físico total, pero la entidad actualmente tiene contratado, el siguiente almacenamiento en sus órdenes de compra y se desglosa de la siguiente manera:

• Total, contratado de Almacenamiento BK de datos diario y semanal:
350000 GB

• A la fecha la entidad, está consumiendo 324500 GB de almacenamiento de BK diario y semanal, los cuales se sacan de la sumatoria de la columna "CAPACIDAD" menos "ESPACIO", de la
tabla "DIARIO-SEMANAL".

**• Acorde a la información suministrada con anterioridad y realizando la resta entre lo consumido, menos el almacenamiento contratado la entidad no supera el almacenamiento contratado para este ítem de BK de datos diario y semanal.**

• Para los Backus Mensuales la entidad tiene contratado un espacio de Almacenamiento físico mensual de: 250000 GB

• A la fecha la entidad, está consumiendo 473889,1 GB de almacenamiento de BK Mensual, los cuales se sacan de la sumatoria

de la columna "CAPACIDAD" menos "ESPACIO LIBRE", de la tabla "MENSUALES

**• Acorde a la información suministrada con anterioridad y realizando la resta entre lo consumido, menos el almacenamiento contratado la entidad supera en 249526,1 GB, el almacenamiento BK MENSUAL.**

Los backups se ejecutan de la siguiente manera:

**Diarios:** De domingo a viernes 20:00pm
**Semanales:** Todos los sábados 20:00pm
**Mensuales:** Último domingo de cada mes 22:00pm

**NOTA:** Por motivos de seguridad, no es viable remitir fotografías de los backups ejecutados.

| DIARIOS - SEMANALES | | | |
|---|---|---|---|
| REPOSITORIOS | CAPACIDAD FISICA PRESENTADA | CAPACIDAD FISICA LIBRE | CAPACIDAD NETA SIN DE DUPLICACION USO TOTAL DE LA HERRAMIENTA |
| UNIDAD 1 | 90 TB | 12,7 TB | 205,9 TB |
| UNIDAD 2 | 90 TB | 5,1 TB | 185,4 TB |
| UNIDAD 3 | 90 TB | 14,5 TB | 209,7 TB |
| UNIDAD 4 | 90 TB | 3,2 TB | 210, 1TB |

| MENSUALES | | | |
|---|---|---|---|
| REPOSITORIOS | CAPACIDAD FISICA PRESENTADA | CAPACIDAD FISICA LIBRE | CAPACIDAD NETA SIN DE DUPLICACION USO TOTAL DE LA HERRAMIENTA |
| UNIDAD 1 | 90 TB | 8,5 TB | 179,8 TB |
| UNIDAD 2 | 90 TB | 6,1 TB | 156,2TB |
| UNIDAD 3 | 90 TB | 19,9 MB | 93,7 TB |
| UNIDAD 4 | 90 TB | 6,3 TB | 94,6 TB |
| UNIDAD 5 | 69,1 TB | 17,9 TB | 51,2 TB |
| UNIDAD 6 | 100 TB | 16,4 TB | 175,1 TB |

**NOTA**: Por favor tener en cuenta, que las dos primeras columnas, hacen referencia al espacio físico, tanto usado como libre, la tercera columna, hace referencia al especio que nos muestra la herramienta que consume en el espacio libre disponible (espacio total team sin de duplicación).
Tener en cuenta que el documento veeam backup CSJ.PDF, no se modifica porque son los valores que nos genera la herramienta, al momento de extraer los datos, pero si son la base para realizar los cálculos de los espacios a la fecha de corte.

(Remitirse al anexo "**Inventario_Servicios_CSJ_JULIO_2024.xls**" para ver el detalle)

## *4. REPLICACIÓN*

| No | ARTICULO | SIDOC124016 |
|---|---|---|
| 10 | npn04--IaaS almacenamiento- Replicación Local de Datos -Oro - Alta - Nube Privada -Capacidad: 900TB a<1000TB - 10 Gbps - Restauración: 10TB / hora -GB/Mes - Cantidad: 2910000 | 2081816 |

La replicación total contratada, de conformidad con las solicitudes de la Entidad, a corte 30 de JULIO de 2024 es de: **2,36 (P)**

Total, contratado de replicación local de datos: **2.91 (P)**

**NOTA:** La replicación de gestión de grabaciones se ejecuta diario después de la 1:00am, con un tiempo estimado de 8 horas, (replicación granular la cual se realiza sobre los archivos que presentaron alguna modificación durante el día), las copias se ejecutan en maquinas alternas.

En anexo "**Inventario_Servicios_CSJ_JULIO_2024.xls**" se encontrarán más detalles de las ejecuciones mencionadas.

## *6.SERVICIOS POR APLICACIÓN*

A continuación, se resumen las principales actividades en la provisión de los servicios y aplicaciones para Consejo Superior de la Judicatura:

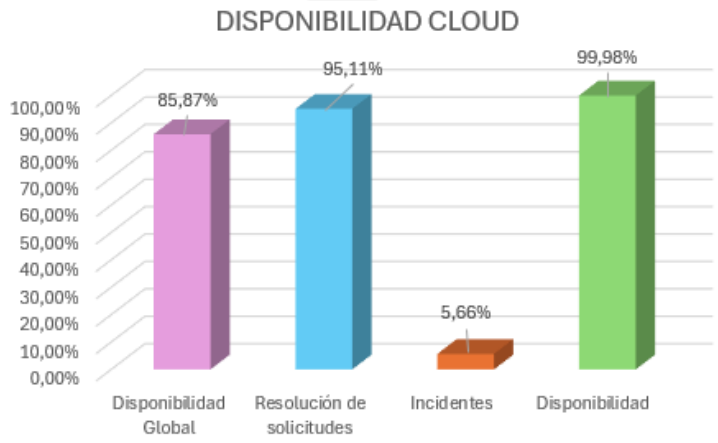
- **Capacitación SST:** líneas de OC 16 y 38
- **Cobro coactivo:** líneas de OC 17 y 38
- **core-impact:** Línea de OC 12
- **Efinomina:** Líneas de OC 14,18,26,27,38 y 39
- **Fuse:** Línea OC 17
- **Gestión grabaciones:** Líneas de OC 12,13, 14,15,17,19,20,22,23,25,28,35,36 y 38
- **InsightVM console:** línea OC 27
- **InsightVM scan:** línea OC 27
- **Insightappsec scan:** línea OC 25
- **Isigthwm scan:** línea OC 26
- **Ivanti:** Líneas de OC 17,18,20,21,22,28,38 y 42
- **Jurisprudencia ADA:** Líneas de OC 17,20,21 y 22
- **JXXIWeb:** Líneas de OC 24,25 y 38
- **Kactus:** Líneas de OC 24,25 y 38
- **MV Seccionales:** Línea de OC 15
- **PIBOT_ASURE:** Líneas de OC 16 y 23
- **Portal Consejo de estado:** Línea de OC 23
- **Portal WEB y AC:** Líneas de OC 14,15,17,18,19,22,34,36,38,39 y 42
- **PORTALPRORJ:** Líneas de OC 13,15,22,37,38,40,41 y 42
- **Rapid7 Collector:** Líneas de OC 25,26 y 27
- **Rapid7 Honeypot:** Línea de OC 15
- **Rapid7 Metaexploit:** Líneas de OC 14 y 15

- **Rapid7 Network Sensor:** Línea de OC 25
- **Rapid7 Orchestrator:** Línea de OC 14
- **relatoria P&S:** Líneas de OC 17 y 38
- **Replicacion Dominio Activo:** Línea de OC 14
- **REPLICACION GEOGRAFICA:** Línea de OC 15
- **RestitucionTierras:** Líneas de OC 17,37 y 42
- **SGSI:** Líneas de OC 17 y 38
- **SIBD:** Líneas de OC 22 y 38
- **Sigobius:** Líneas de OC 17 y 38
- **SIRNA:** Líneas de OC 12,17,19,22,25 y 38
- **SolarWinds Database:** Línea de OC 38
- **SolarWinds NPM-NTA:** Línea de OC 21
- **SolarWinds Patch Manager:** Línea de OC 25
- **SolarWinds Pooling Engine:** Línea de OC 21
- **SolarWinds WSUS:** Línea de OC 25
- **WSO2:** Líneas de OC 12,36 y 37

(Remitirse al anexo "**Inventario_Servicios_CSJ_JULIO_2024.xls**" para ver el detalle "maquinas")

## *7.DISPONIBILIDAD GLOBAL CLOUD DEL MES DE JULIO*

| Disponibilidad Global mes de JULIO | Numero de tickets mes de JULIO | Imputabilidad por ANS |
|---|---|---|
| | **50 solicitudes** | **0 solicitudes** |
| | **3 incidentes** | **0 incidentes** |
| 97% | Total 53 tickets | 0 tickets |



CONTROL DOCUMENTAL

ELABORADO POR

| Fecha | Autor | Ingeniero |
|---|---|---|
| 05-08-2024 | IFX Networks | Juan Carlos Romero |
| | | |
| | | |

REVISADO POR

| Fecha | Autor | Ingeniero |
|---|---|---|
| | IFX Networks | |
| | | |

## 1. INTRODUCCIÓN

El presente documento resume las principales actividades en la provisión de los servicios de Soporte técnico para **Consejo Superior de la Judicatura** durante el periodo 1 julio a31 de julio del 2024.

| CONSUMO TOTAL HORAS MES DE JULIO | |
|---|---|
| • Casos Reportados Netsuite | 115 |
| Sesiones de Seguimiento | 5 |
| Sesiones de Trabajo | 0 |
| Casos Escalados Medio Digital - Whatsapp | 10 |
| Horas Disponibilidad del Recurso Fines de Semana | 270 |
| Total Horas Consumidas de las 300 - Experto Master | 400 |

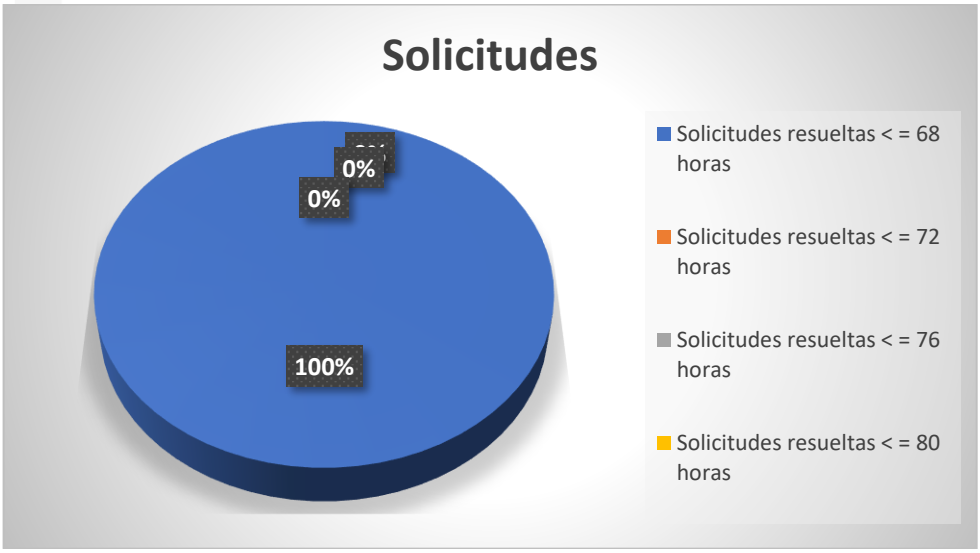
## 2. INDICADORES DEL CENTRO CONSOLIDADO DE SERVICIOS

Con base en la información provista por el sistema de Netsuite, se elaboró el presente reporte el cual muestra el comportamiento de los problemas y requerimientos con enfoque en los días 01 enero a 31 de julio, para el **Consejo Superior de la Judicatura**. Estas mediciones se basan en el número de casos reportados por la aplicación.

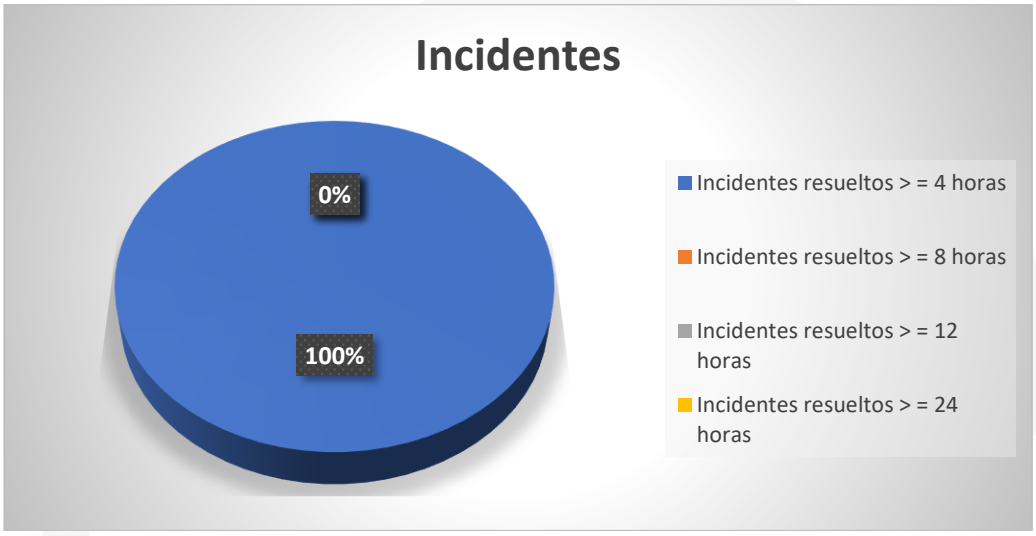
| | Volumen en 1 julio a |
|---|---|
| Casos Reportados | 20 |
| Solicitudes | 19 |
| Incidencias | 1 |
| WA - AF | 0 |

## 2.1 TASA DE RESOLUCIÓN DE PROBLEMAS

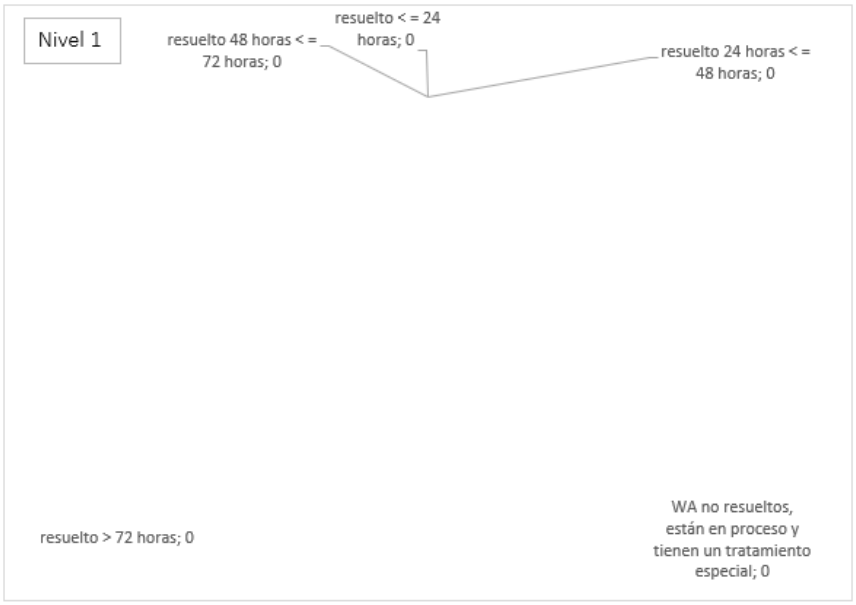
| Tiempo de Gestión | Solicitudes |
|---|---|
| Solicitudes resueltas < = 68 horas | 19 |
| Solicitudes resueltas < = 72 horas | |
| Solicitudes resueltas < = 76 horas | 0 |
| Solicitudes resueltas < = 80 horas | 0 |
| Solicitudes no resueltas > 80 horas, están en proceso y/o tienen un tratamiento especial | 0 |
| **Total** | **19** |

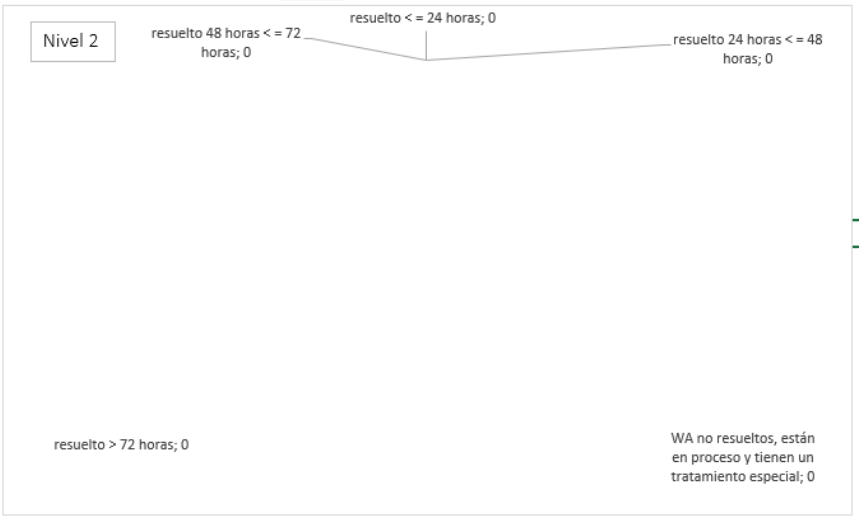


| Tiempo de Gestión | Incidentes Penalizados |
|---|---|
| Incidentes resueltos > = 4 horas | 1 |
| Incidentes resueltos > = 8 horas | 0 |
| Incidentes resueltos > = 12 horas | 0 |
| Incidentes No resueltos > 24 horas | 0 |
| **Total** | **0** |

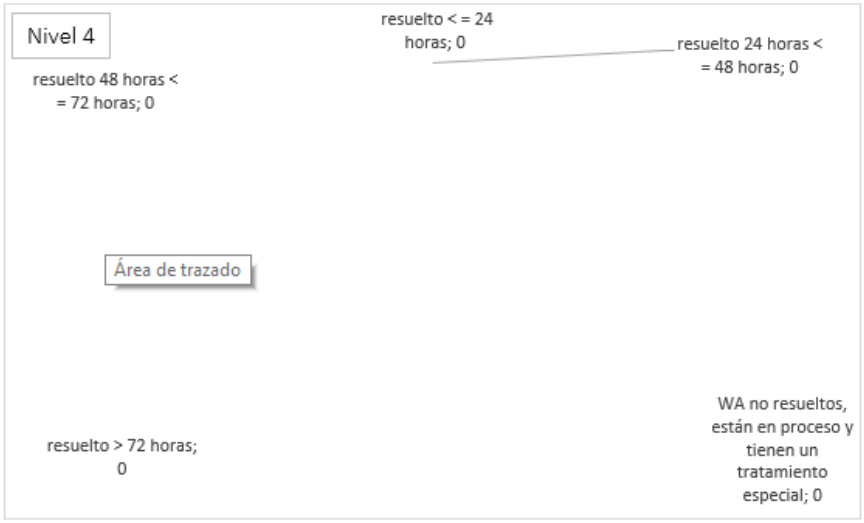


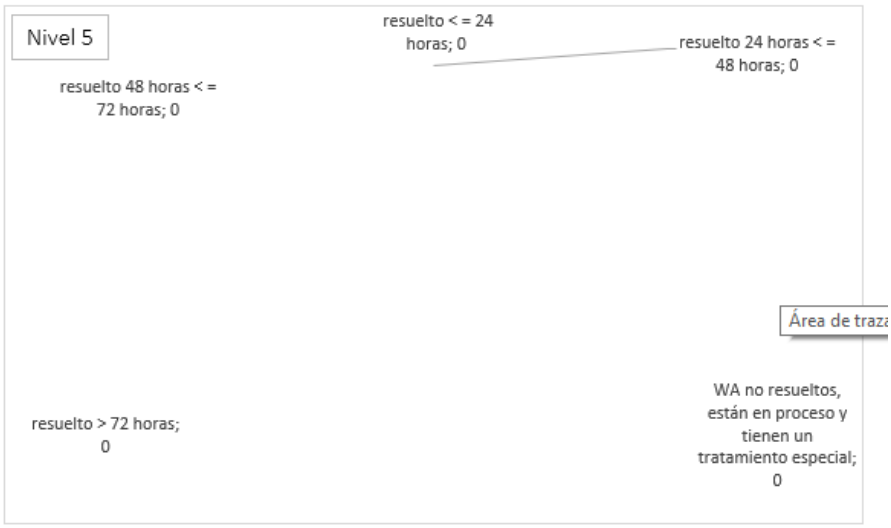

| WA (Ajustes Funcionales) | | | | | |
|---|---|---|---|---|---|
| Tiempo de Gestión | Nivel 1 | Nivel 2 | Nivel 3 | Nivel 4 | Nivel 5 |
| resuelto < = 24 horas | 0 | 0 | 0 | 0 | 0 |
| resuelto 24 horas < = 48 horas | 0 | 0 | 0 | 0 | 0 |
| resuelto 48 horas < = 68 horas | 0 | 0 | 0 | 0 | 0 |
| resuelto > 68 horas | 0 | 0 | 0 | 0 | 0 |
| WA no resueltos, están en proceso y tienen un tratamiento especial | 0 | 0 | 0 | 0 | 0 |
| **Total** | **0** | **0** | **0** | **0** | **0** |


Nivel 1
resuelto 48 horas < = 72 horas; 0
resuelto < = 24 horas; 0
resuelto 24 horas < = 48 horas; 0
resuelto > 72 horas; 0
WA no resueltos, están en proceso y tienen un tratamiento especial; 0


Nivel 2
resuelto 48 horas < = 72 horas; 0
resuelto < = 24 horas; 0
resuelto 24 horas < = 48 horas; 0
resuelto > 72 horas; 0
WA no resueltos, están en proceso y tienen un tratamiento especial; 0


Nivel 3
resuelto < = 24 horas; 0
resuelto 24 horas < = 48 horas; 0
resuelto 48 horas < = 72 horas; 0
resuelto > 72 horas; 0
WA no resueltos, están en proceso y tienen un tratamiento especial; 0




## 2.2 LISTADO DE CASOS REPORTADOS

Se anexa al presente documento los casos que fueron reportados por la aplicación Netsuite consolidados a través del archivo **"2 - Casos CSJ Acumulativo 1 julio a 31 de julio del 2024.xlsx"** y los casos que fueron reportados por la aplicación WhatsApp consolidados a través del archivo **"Casos Reportados Medio Digital - Whatsapp"** este archivo se puede ver en el drive "https://ifxusa-my.sharepoint.com/:x:/r/personal/desarrollocsj_ifxcorp_com/_layouts/15/Doc.aspx?sourcedoc=%7B69A6AAC0-913F-491D-866B-DB9F5BCDDAEE%7D&file=casos%20reportados%20por%20medio%20digital.xlsx&action=default&mobileredirect=true" los cuales contienen la información detallada de cada uno desde el 1 de julio a 31 de julio del 2024.

## 2.3 BOLSA DE HORAS SEGÚN CONTRATO

| Item | Hora Experto | Alcance |
|---|---|---|
| CASO: Incidencia | 400 horas / mes | Interrupción completa del servicio, Fallo total en el funcionamiento del servicio que se encuentra en producción, Intermitencias / Problemas de latencia o pérdida de paquetes, Infección por Virus o Código Malicioso, Phishing, Modificación o Eliminación no autorizada de un sitio, Divulgación no autorizada de información sensible, Acceso o Intentos de Acceso no autorizados |
| CASO: Solicitud | | Reportes, Informes, Monitoreo, Certificaciones, Restauración de Backups BD, Repositorios Códigos Fuentes, Reuniones |
| CASO: WA - AF (Ajustes Funcionales) | | Mantenimiento sobre aplicaciones aplicando el ciclo de vida del software (Levantamiento de Información, Análisis y Diseño, Codificación, Pruebas, Documentación) |
| CASO: WA - AF (Mejoras Funcionales) | 100 horas / mes | Requerimientos Nuevos sobre aplicaciones aplicando el ciclo de vida del software (Levantamiento de Información, Análisis y Diseño, Codificación, Pruebas, Documentación) |

## 2.4 ESTADO DE LAS HORAS CONSUMIDAS DE LOS CASOS REPORTADOS

El estado de los casos a la fecha 31 de julio de 2024. De acuerdo con la matriz que se muestra a continuación se ha cumplido con la cantidad de horas las cuales son 400 – Horas Experto según orden de compra.

| Etiquetas de fila | Suma de Horas Hombre | Horas Presupuesto | Horas Disponible |
|---|---|---|---|
| Caso | 130 | 400 | 270 |
| 2024 | 130 | | |
| Solicitud | 126 | | |
| Incidencia | 4 | | |
| Total Horas Casos Reportados Netsuite | 130 | 400 | 270 |
| | | 270 | 270 |
| | | 270 | 270 |
| | | 270 | 270 |
| | | 270 | 270 |
| Horas consumidasde las 400 - Exp | 400 | 400 | 0 |

No se reportaron casos relacionados con WA – MF para este mes de julio que corresponden a las 100 Horas Experto Máster.

| Etiquetas de fila | Suma de Horas Hombre | Horas Presupuesto | Horas Disponibles |
|---|---|---|---|
| CASO | 0 | 100 | 100 |
| 2024 | 0 | | |
| WA | 0 | | |
| MF | 0 | | |
| Total Horas Casos Reportados Netsuite | 0 | 100 | 100 |
| Total Horas Consumidas de las 100 - Exp | 0 | 100 | 100 |

## 3. DISPONIBILIDAD E INDISPONIBILIDAD DE LOS SERVICIOS DE HOSTING

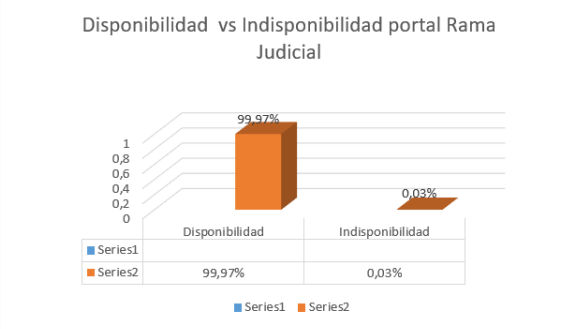
### 3.1. GRÁFICO DE DISPONIBILIDAD E INDISPONIBILIDAD DE LOS SERVICIOS DEL PORTAL DE RAMA JUDICIAL

Se visualiza a través de la siguiente matriz los datos de disponibilidad, indisponibilidad y tiempo de caída de las aplicaciones que están soportadas al Consejo Superior de la Judicatura:

Nota: para el mes de julio hacemos acotar que a razón del paso a producción de los nuevos portales Liferay 7.1, para Rama Judicial y publicaciones procesales, no se estarán justificando los tiempos de caída de las mismas, ya que actualmente se encuentran en fase de estabilización de los servicios y de la arquitectura.

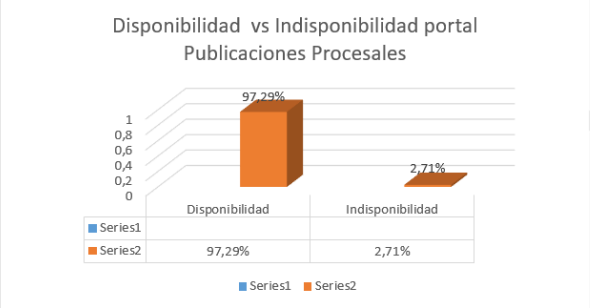
Portal Rama Judicial

| Item | Aplicación | Disponibilidad | Indisponibilidad | Tiempo de duracion (Caida en horas) | Tiempo de duracion | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | Dias | Horas | Minutos | Segundos |
| 1 | Portal de la Rama Judicial | 99,97% | 0,03% | 0,212222222 | 0 | 0 | 12 | 44 |
| | **Totales** | 99,97% | 0,03% | 0,212222222 | **0** | 0 | 12 | 44 |



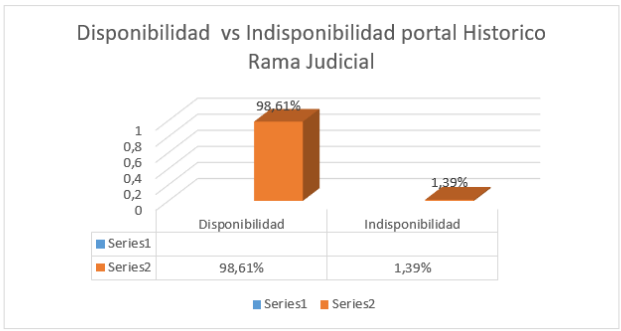
## Portal Publicaciones Procesales

| Item | Aplicación | Disponibilidad | Indisponibilidad | Tiempo de duracion (Caida en horas) | Tiempo de duracion | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | Dias | Horas | Minutos | Segundos |
| 1 | Publicaciones Procesales | 97,29% | 2,71% | 20,13 | 0 | 20 | 7 | 48 |
| | **Totales** | 97,29% | 2,71% | 20,13 | **0** | 20 | 7 | 48 |




## Portal Histórico Rama Judicial

| Item | Aplicación | Disponibilidad | Indisponibilidad | Tiempo de duracion (Caida en horas) | Tiempo de duracion | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | Dias | Horas | Minutos | Segundos |
| 1 | Portal Historico | 98,61% | 1,39% | 10,35166667 | 0 | 10 | 21 | 6 |
| | **Totales** | 98,61% | 1,39% | 10,35166667 | **0** | 10 | 21 | 6 |

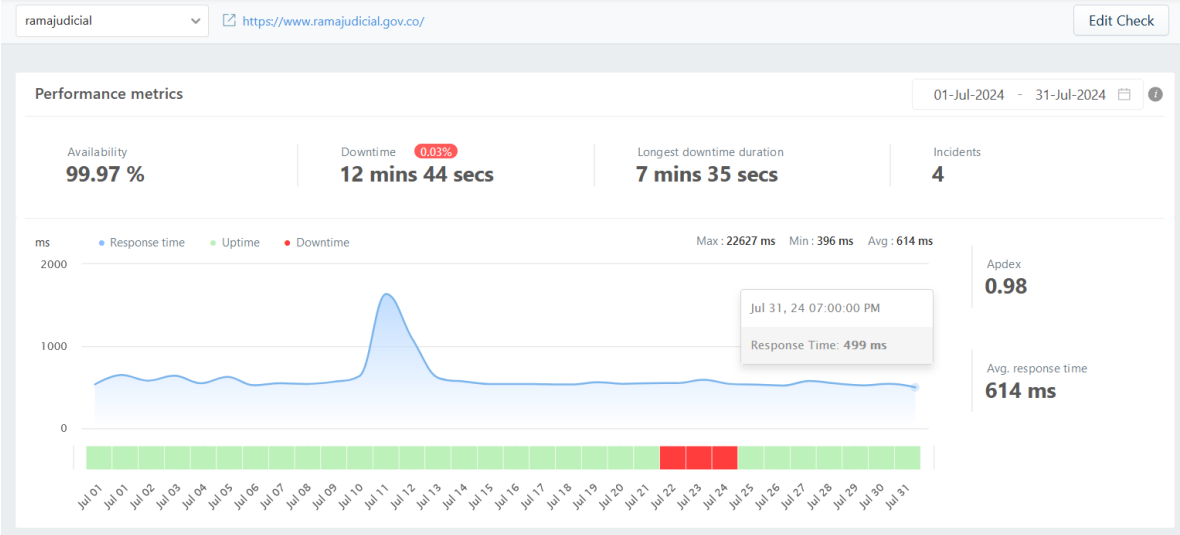



## 3.2 PORTAL DE LA RAMA JUDICIAL

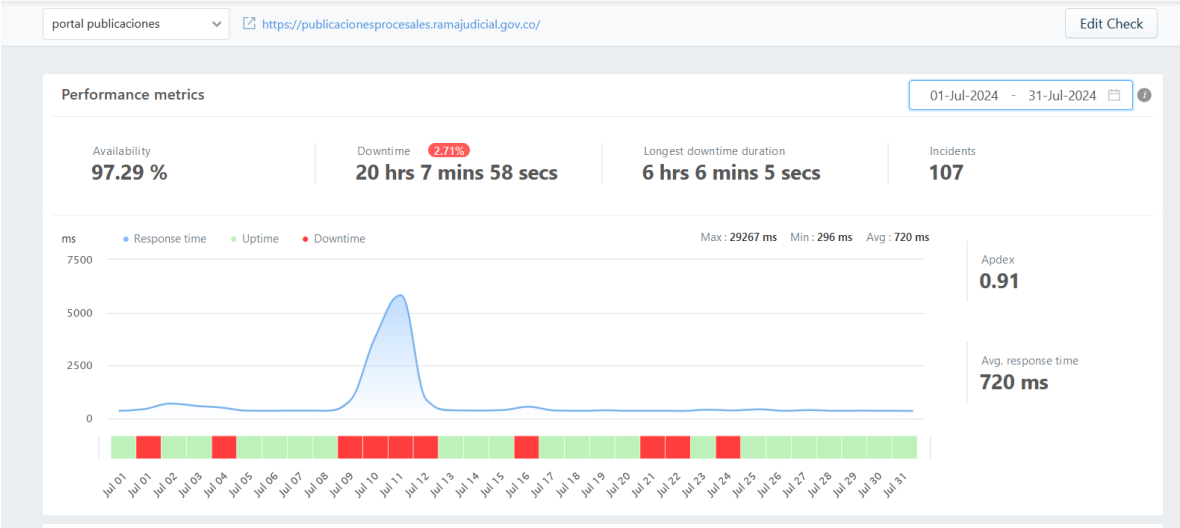
### Grafica de la información consolidada de disponibilidad e indisponibilidad del portal del mes de julio

Nota: para el mes de julio hacemos acotar que a razón del paso a producción de los nuevos portales Liferay 7.1, para Rama Judicial y publicaciones procesales, no se estarán justificando los tiempos de caída de las mismas, ya que actualmente se encuentran en fase de estabilización de los servicios y de la arquitectura.

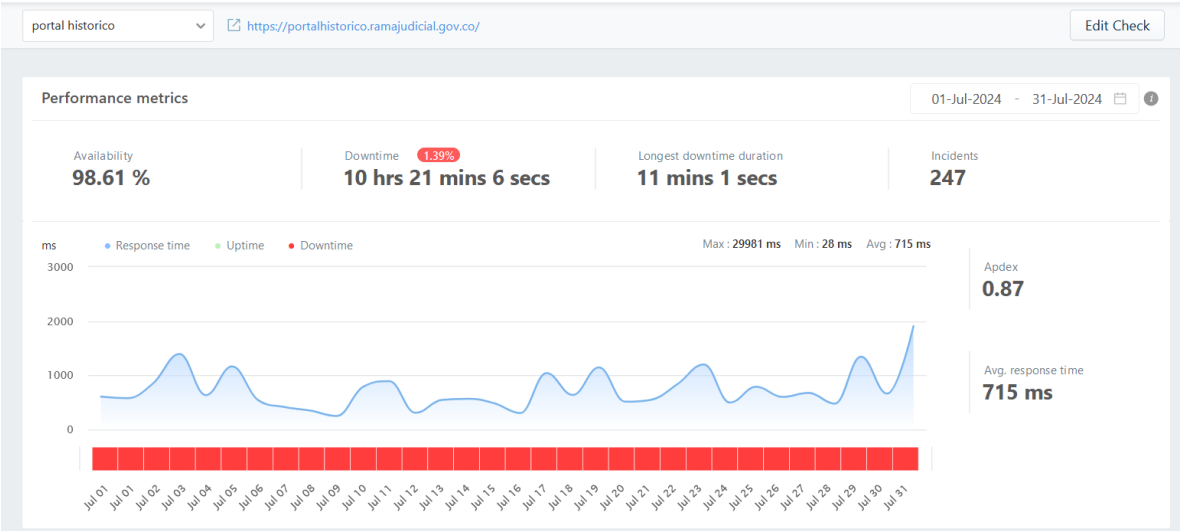
## Portal Rama Judicial




## Portal Publicaciones Procesales



Portal Histórico Rama Judicial




- TT544033 RV: Certificaciones disponibilidad portal Rama Judicial año 2023.

A través del presente drive https://drive.google.com/drive/folders/1kZx3eIpxxGU_0HqLd7aqEiZ3ie4En1CD?usp=sharing se cargan las certificaciones y están ubicadas las del mes de julio de acuerdo con que la rama judicial mediante la herramienta NOC solicita si se tiene alguna información adicional

Acciones Inmediatas realizadas de acuerdo con lo recomendado por equipo de especialistas de IFX

BITACORA DE ACTIVIDADES QUE SE EJECUTARON PARA MITIGAR LOS INCONVENIENTE DE INDISPONIBILIDAD DEL PORTAL DE RAMA JUDICIAL Y SUS APLICACIONES CONEXAS

| ITEM | ACTIVIDAD | FECHA DE EJECUCION | TRABAJO REALIZADO (OPCIONAL) | AREA ENCARGADA |
|---|---|---|---|---|
| 1 | Ajustes en buscador de publicaciones procesales | 12/07/2024 | | Desarrollo |
| 2 | Validación de valores de tunning en instancias de Rama Judicial | 17/07/2024 | | Desarrollo |

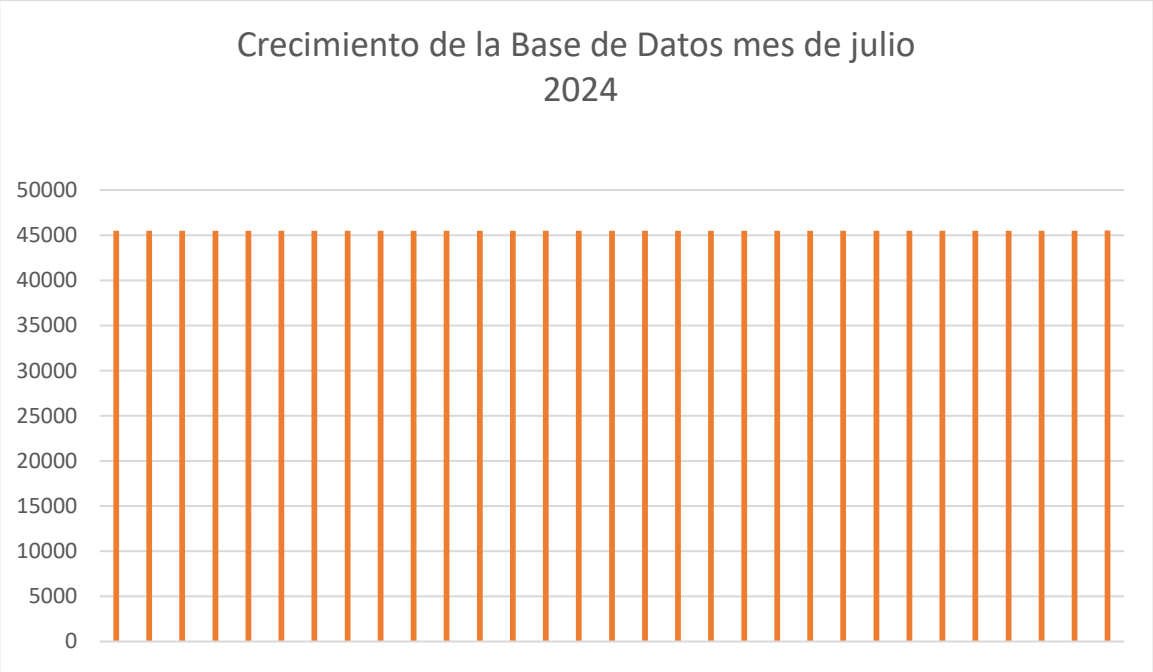
### 3.2.2 CRECIMIENTO DE LA BASE DE DATOS – INSTANCIA CSJPORTALDB01

De acuerdo con la solicitud escalada en el **caso TT520553 RV: Crecimiento de la BD de la maquina CSJPORTALDB01** del portal de rama judicial, se agrega el presente informe consolidado del crecimiento que tuvo la BD en el mes de julio.

BASE DE DATOS lportalramaprod

| TAMAÑO (MB0 | FECHA | AUMENTO TAMAÑO (MB) POR DIA |
|---|---|---|
| | | |

Grafica del crecimiento de la BD lportalramaprod de la INSTANCIA CSJPORTALB01

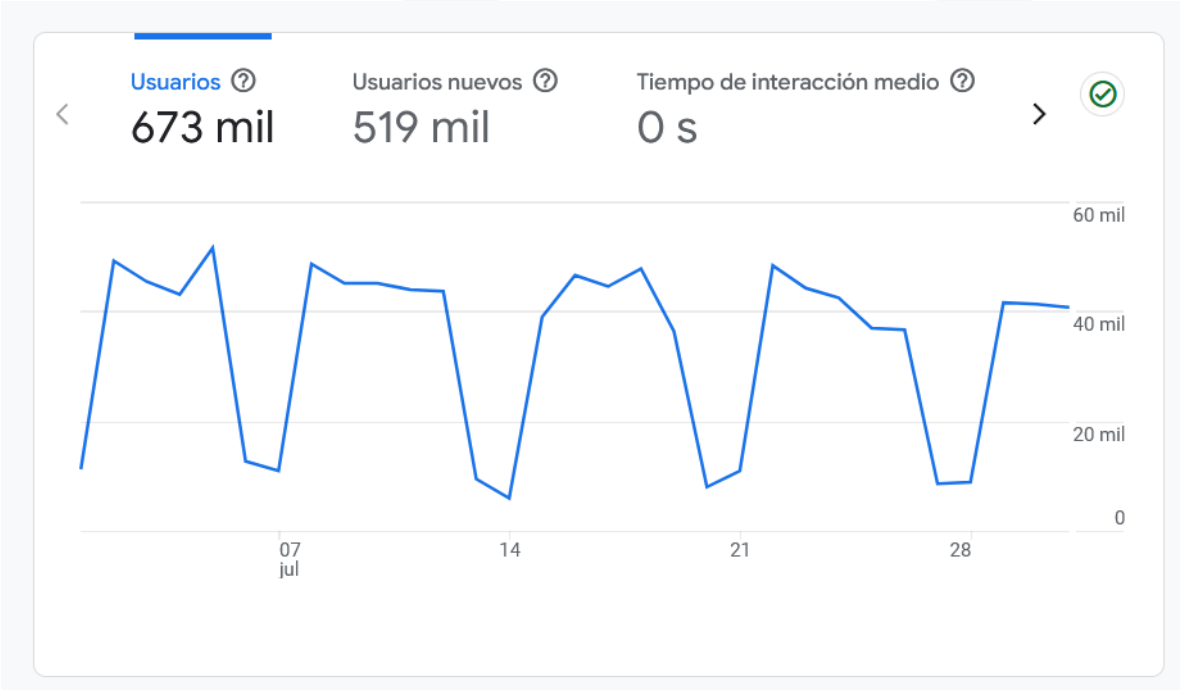



**Nota**: Actualmente la grafica de crecimiento de la base de datos se encuentra en blanco a razón que desde la salida a producción del nuevo portal no estamos recopilando esta información, de igual forma se debe escalar el tema al administrador de la base de datos (ing Edgar Rubiano), para agregar dichos scripts y poder adjuntar los datos respectivos en el informe.

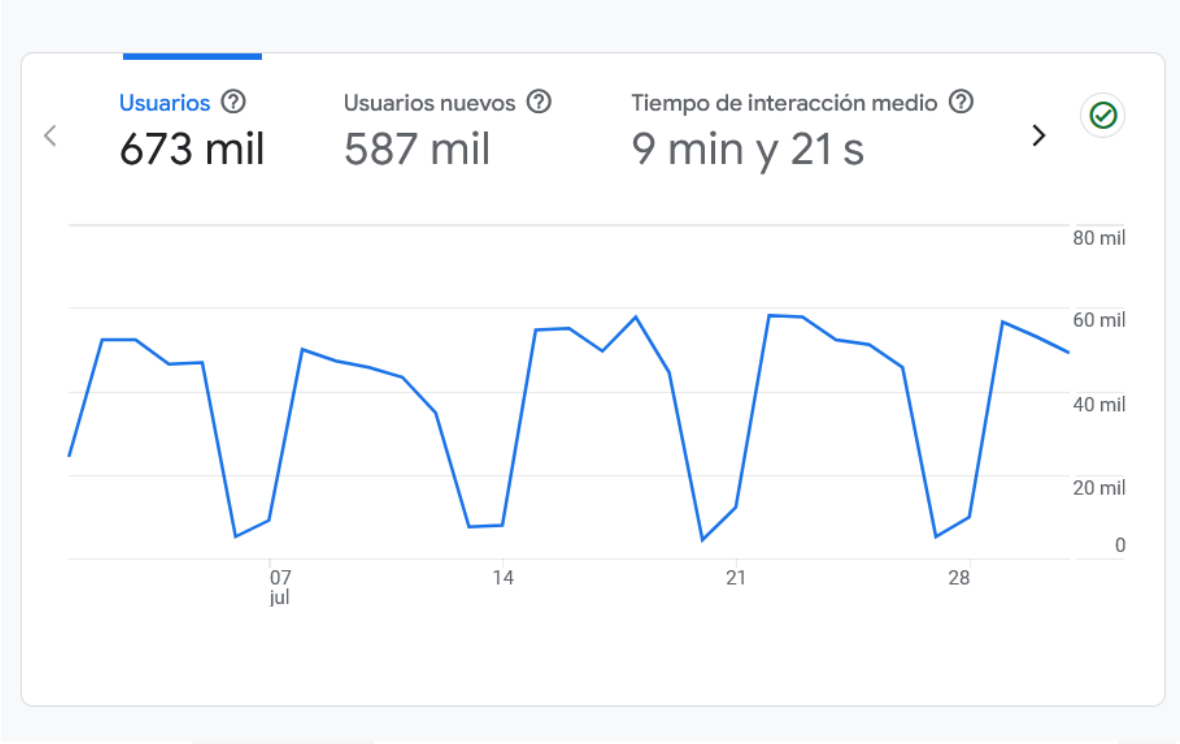
## 4. ESTADISTICAS PORTAL DE LA RAMA JUDICIAL

### 4.1 RESUMEN DEL PORTAL

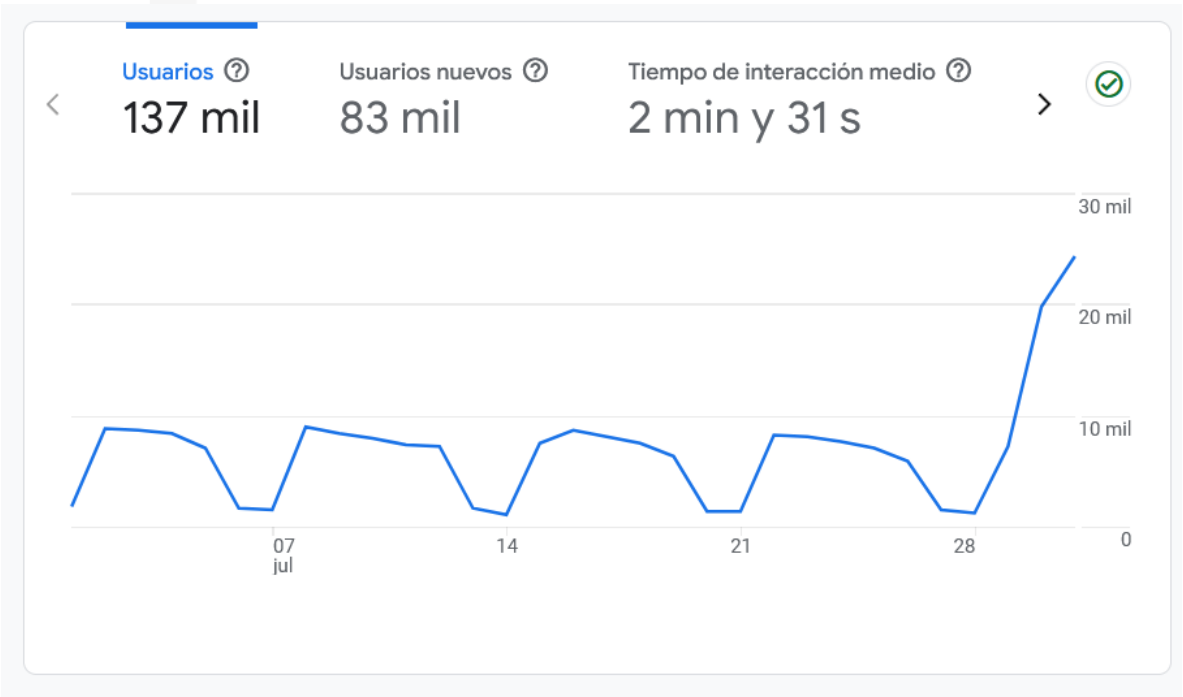
En la respectiva grafica se observa un comportamiento constante durante el mes de julio para el portal Rama Judicial.




En la respectiva grafica se observa un comportamiento constante durante el mes de julio para el portal Publicaciones Procesales




En la respectiva grafica se observa un comportamiento constante durante el mes de julio para el portal Historico Rama Judicial.



## 8. ESQUEMA DE SEGURIDAD

| OC | SID | DESCRIPCIÓN | SUBTIPO | NOMBRE DEL EQUIPO | MODELO | SERIAL | UNIDAD DE RACK | RACK |
|---|---|---|---|---|---|---|---|---|
| 11 | 2081817 | npn04--IaaS Procesamiento -Balanceador de Carga AltaCapacidad - Oro - HostingNube Privada - SesionesCapa L4 (entre 36 y 100Millones) - RAM entre 64GB y128GB - U_Mes - Cantidad: 2 | Balanceador DC Torre central | FORTI/PPLA | ADC-2200F | SN: FAD22FT2210000028 | 10 | 32 |
| 11 | 2081818 | npn04--IaaS Procesamiento -Balanceador de Carga AltaCapacidad - Oro - HostingNube Privada - SesionesCapa L4 (entre 36 y 100Millones) - RAM entre 64GB y128GB - U_Mes - Cantidad: 2 | Balanceador DC Torre central | FORTI/BK | ADC-2200F | SN: FAD22FT2210000027 | 9 | 32 |
| 30 | 2082020 | npn04--IaaS Seguridad - Appliance Anti Ddos - AltaCapacidad - Oro - Hostingfísico - Rol de Inspección - 50Gbps - Paquetes PorSegundo (MPPS) - 45000000- Mes - Cantidad: 2 | DDOS DC Torre central | FORTIDDOS FORTINET 2000E/PPLA | 2000E | SN: FI2KETB20000015 | 31-32 | 32 |
| 30 | 2082021 | npn04--IaaS Seguridad - Appliance Anti Ddos - AltaCapacidad - Oro - Hostingfísico - Rol de Inspección - 50Gbps - Paquetes PorSegundo (MPPS) - 45000000- Mes - Cantidad: 2 | DDOS DC Torre central | FORTIDDOS FORTINET 2000E/BK | 2000E | SN: FI2KE581900004 9 | 35-36 | 32 |
| 31 | 2082016 | npn04--IaaS Seguridad - Firewall Nueva Generación - Media Capacidad - Oro - Hosting físico - Rol deFirewall - 40 Gbps - SesionesConcurrentes - 15000000 -Mes - Cantidad: 2 | FIREWALL | PALACIO - PPLA | FortiGate 900G | SN: FG9H0GTB23900205 | N/A | N/A |
| 31 | 2082017 | npn04--IaaS Seguridad - Firewall Nueva Generación - Media Capacidad - Oro - Hosting físico - Rol deFirewall - 40 Gbps - SesionesConcurrentes - 15000000 -Mes - Cantidad: 2 | FIREWALL | PALACIO - BK | FortiGate 900G | SN: FG9H0GTB23900440 | N/A | N/A |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 32 | 2082018 | npn04--IaaS Seguridad - Firewall Nueva Generación - Alta Capacidad - Oro - Hosting físico - Rol deFirewall - 500 Gbps - Sesiones Concurrentes - 150000000 - Mes - Cantidad:2 | FIREWALL DC Torre central | DATACENTER - BK | FORTIGATE-4400F | SN: FG440FTK21900183 | 27-30 | 32 |
| 32 | 2082019 | npn04--IaaS Seguridad - Firewall Nueva Generación - Alta Capacidad - Oro - Hosting físico - Rol deFirewall - 500 Gbps - Sesiones Concurrentes - 150000000 - Mes - Cantidad:2 | FIREWALL DC Torre central | DATA CENTER - PPLA | FORTIGATE-4400F | SN: FG440FTK21900184 | 5-8 | 32 |
| 33 | 2082013 | npn04--IaaS Seguridad - WebAplication Firewall - AltaCapacidad - Oro - Hostingfísico - Desempeño WAF(Gbps) - 10 - Mes - Cantidad:3 | WAF DC Torre central | DATACENTER - PPLA | KEMP LM-X25 | SN: TSCC82005608 | 14 | 31 |
| 33 | 2082014 | npn04--IaaS Seguridad - WebAplication Firewall - AltaCapacidad - Oro - Hostingfísico - Desempeño WAF(Gbps) - 10 - Mes - Cantidad:3 | WAF DC Torre central | DATACENTER - BK | KEMP LM-X25 | SN: TSCB72000545 | 13 | 31 |
| 33 | 2082015 | npn04--IaaS Seguridad - WebAplication Firewall - AltaCapacidad - Oro - Hostingfísico - Desempeño WAF(Gbps) - 10 - Mes - Cantidad:3 | WAF | SEDE CAN | KEMP LM-X25 | SN: TSCC82005629 | N/A | N/A |
| 44 | 2082108 | Servicios Complementarios - Experto Master - Región 1 - Hora/M - Cantidad: 980 | Transversales a servicios de SP | | | | | |

## 9. Horas experto de los ítems 44 y esquema de compensación.

El servicio experto es prestado por los siguientes especialistas con una bolsa de 160 horas al mes:

Edward Wilman Sierra Leon
Victor Hugo Galvis Botia
Jose Camilo Calvo Velandia

Estas horas se usan para la atención de solicitudes, incidentes y actividades de gestión para las diferentes soluciones de seguridad de CSJ en el horario no hábil de

la entidad. El detalle de las horas adicionales utilizadas para atender solicitudes e incidencias durante el mes se detallan a continuación:

| Ingeniero Residente: | Edward Wilman Sierra leon | | | | |
|---|---|---|---|---|---|
| **Item** | **Fecha y Hora de inicio** | **Fecha y Hora de finalización** | **Cantidad de Horas** | **Tipo de Hora extra** | **Actividad Realizada** |
| 1 | 7/12/2024 18:00 | 7/12/2024 20:15 | 3 | Diurna | Migración a AWS; TT864501 RV: Solicitud de apertura Redes sociales e IP priorizada 15 y 16 de Julio 2024 |
| 2 | 7/13/2024 8:40 | 7/13/2024 13:16 | 3 | Diurna | Migración a AWS |
| 3 | 7/13/2024 14:00 | 7/13/2024 16:15 | 2 | Diurna | TT864076 RV: ACTIVACION DE SERVICIOS - CSJ - CHOCÓ BOJAYA-DKO 8529888, 8529894 - Marcela Narvaez |
| 4 | 7/15/2024 18:00 | 7/15/2024 19:16 | 1 | Diurna | TT865366 RV: Solicitud de puertos y conectividad maquinas nuevas y consulta azul; TT865402 RV: Habilitar IP y Dominios para aplicativo SIPOST |
| 5 | 7/18/2024 18:00 | 7/18/2024 19:32 | 2 | Diurna | TT867075 RV: SOLICTUD NUEVO SEGMENTO CALLE 72 \|\| DSAJB; TT866832 Solicitud verificación comportamiento de MV pivot AWS SID 2081994 2082001 2082002 2081996; TT867104 RV: Solicitud VPN para ing. Yesid Olaya |
| 6 | | | | | |
| 7 | | | | | |
| 8 | | | | | |
| | | | | | |
| | | | | | |
| Total horas Extras | | | 11 | | |

| Ingeniero Residente: | Victor Galvis | | | | |
|---|---|---|---|---|---|
| **Item** | **Fecha y Hora de inicio** | **Fecha y Hora de finalización** | **Cantidad de Horas** | **Tipo de Hora extra** | **Actividad Realizada** |
| 1 | 5/7/2024 21:00 | 6/7/2024 12:00 | 3:00:00 | Diurna/Nocturna | VM Cirion - Reinicio Allot |
| 2 | 6/7/2024 8:00 | 6/7/2024 10:00 | 2:00:00 | Diurna/Nocturna | Problemas salida Internet servidor de BK |
| 3 | 11/7/2024 19:00 | 11/7/2024 21:00 | 2:00:00 | Diurna | Salida a Internet servidores para actualización Casos: TT863905, TT863901 y TT863888 |
| 4 | | | | | |
| 5 | | | | | |
| 6 | | | | | |
| 7 | | | | | |
| 8 | | | | | |
| 9 | | | | | |
| 10 | | | | | |
| Total horas Extras | | | 7:00:00 | | |

| Ingeniero Residente: | Camilo Calvo | | | | |
|---|---|---|---|---|---|
| **Item** | **Fecha y Hora de inicio** | **Fecha y Hora de finalización** | **Cantidad de Horas** | **Tipo de Hora extra** | **Actividad Realizada** |
| 1 | 1/7/2024 16:00 | 1/7/2024 17:00 | 1:00:00 | Diurna/Nocturna | Reunion: Validacion Portal Restitucion V3 |
| 2 | 4/7/2024 18:00 | 4/7/2024 19:00 | 1:00:00 | Diurna/Nocturna | Reunion: Sesión 24 Migración AWS - EPM - Revisión Base de datos |
| 3 | | | | | |
| 4 | | | | | |
| 4 | | | | | |
| 4 | | | | | |
| 7 | | | | | |
| 8 | | | | | |
| Total horas Extras | | | 2:00:00 | | |

## a. Inventario de equipos de seguridad perimetral.

A continuación, se presenta el inventario de los equipos de seguridad administrados por IFX Networks:

| No | Descripción | Hostname | Serial | SID | Ubicación | Version Firmware |
|---|---|---|---|---|---|---|
| 1 | FortiGate-4400F HA | FTG_CSJ_DC_TC_MASTER | FG440FTK21900184 | 2082019 | DC IFX | v7.0.14 |
| | | FTG_CSJ_DC_TC_SLAVE | FG440FTK21900183 | 2082018 | DC IFX | v7.0.14 |
| 2 | FORTIADC 2200F HA | FADC_CSJ_TC_MASTER | FAD22FT221000027 | 2081818 | DC IFX | v6.1.3 |
| | | FADC_CSJ_TC_ SLAVE | FAD22FT221000028 | 2081817 | DC IFX | v6.1.3 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 3 | WAF KEMP Loadmaster x25 HA | WAF_TORRRE_CENTRAL | TSCC82005608 | 2082013 | DC IFX | 7.2.59.3.22368 |
| | | WAF_TORRRE_CENTRAL | TSCC8200529 | 2082014 | DC IFX | 7.2.59.3.22368 |
| 4 | Fortigate 900G HA | FGT_900G_CSJ_PALACIO_M | FG9H0GTB23900440 | 2082016 | PALACIO | V7.2.6 |
| | | FGT_900G_CSJ_PALACIO_S | FG9H0GTB23900205 | 2082017 | PALACIO | V7.2.6 |
| 5 | WAF KEMP Loadmaster x25 | WAF_CAN | TSCC82005629 | 2082015 | CAN | 7.2.59.3.22368 |
| 6 | FortiDDos 2000E HA | CSJ_FDDoS_MASTER | FI-2KE5819000049 | 2082020 | DC IFX | v6.3.3 |
| | | CSJ_FDDoS_SLAVE | FI-2KETB20000015 | 2082021 | DC IFX | v6.3.3 |

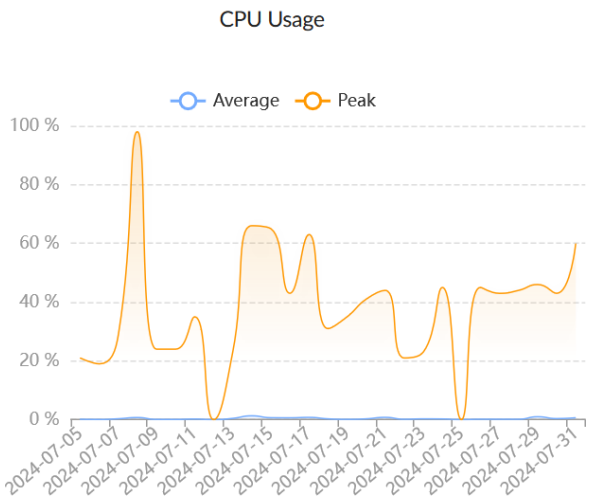
### 10.1 Actualización de firmware.

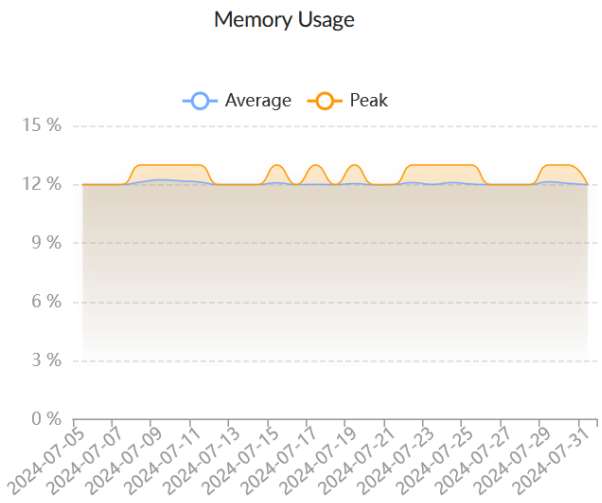
El plan de trabajo para la actualización del firmware será compartido, presentado y ejecutado con la autorización de los ingenieros Datacenter del CONSEJO SUPERIOR DE LA JUDICATURA.

| Equipos | Versión Firmware | Fecha de Ejecucion | Versión Por Actualizar |
|---|---|---|---|
| FTG_CSJ_DC_TC_MASTER | V7.0.14 | Actualizado | N/A |
| FTG_CSJ_DC_TC_SLAVE | v7.0.14 | Actualizado | N/A |
| FADC_CSJ_TC_MASTER | V6.1.3 | Por definir | V7.1.0 |
| FADC_CSJ_TC_MASTER | V6.1.3 | Por definir | V7.1.0 |
| WAF_TORRRE_CENTRAL KEMP | 7.2.59.3.22368 | Actualizado | N/A |
| WAF_TORRRE_CENTRAL KEMP | 7.2.59.3.22368 | Actualizado | N/A |
| FGT_900G_CSJ_PALACIO_M | V7.2.6 | Actualizado | N/A |
| FGT_900G_CSJ_PALACIO_S | V7.2.6 | Actualizado | N/A |
| WAF_CAN KEMP | 7.2.59.3.22368 | Actualizado | N/A |
| CSJ_FDDoS_MASTER | V5.7.3 | Actualizado | N/A |
| CSJ_FDDoS_SLAVE | V5.7.3 | Actualizado | N/A |

## 10. FIREWALL PERIMETRAL

Durante julio, el consumo promedio de CPU y memoria en el firewall perimetral estuvieron dentro de sus valores de operación normal.

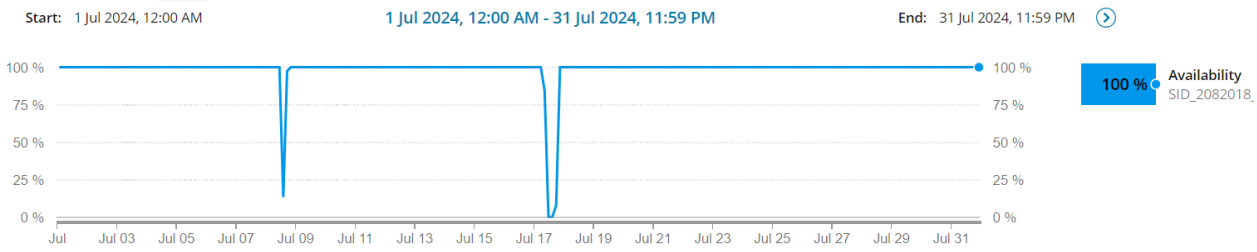



En la gráfica de rendimiento "CPU Usage", la curva color naranja muestra los picos de consumo de una o varias de las 160 CPUs del appliance FortiGate-4400F, cuando estos picos ocurren las tareas que los generan son desbordadas a las otras CPUs del appliance por lo que la curva color azul se muestra el promedio en el consumo real de CPU en ese mismo instante.

### 11.1 Disponibilidad mensual firewall perimetral.

Durante julio se obtuvo 100% de disponibilidad en el firewall perimetral. Los eventos del pasado 8 y 17 de julio se deben a una novedad en el sistema de monitoreo que no afecto los servicios que IFX Networks presta a la rama judicial, relacionados con los tickets TT862004 y TT866155.

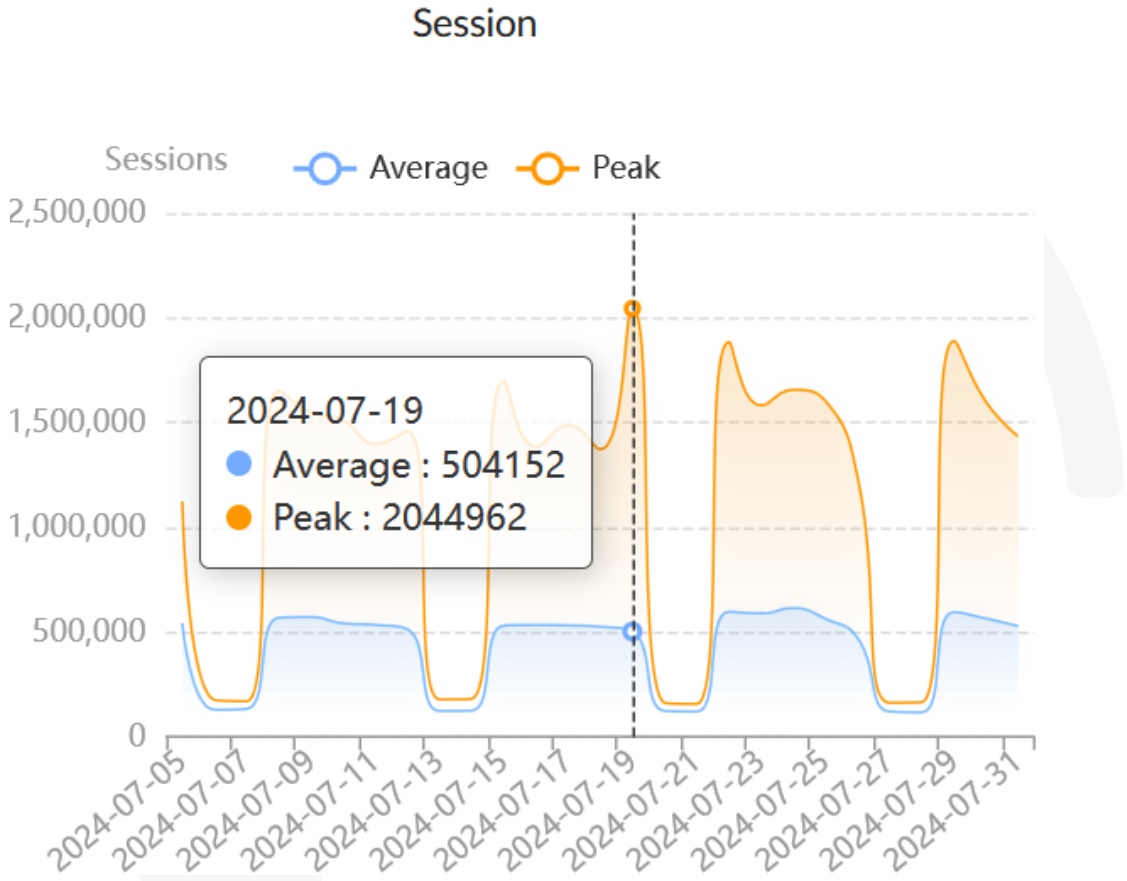



**Availability Statistics** HELP

| PERIOD | AVAILABILITY |
|---|---|
| Today | 100.000 % |
| Yesterday | 100.000 % |
| Last 7 Days | 100.000 % |
| Last 30 Days | 98.333 % |
| This Month | 100.000 % |
| Last Month | 98.366 % |
| This Year | 99.692 % |

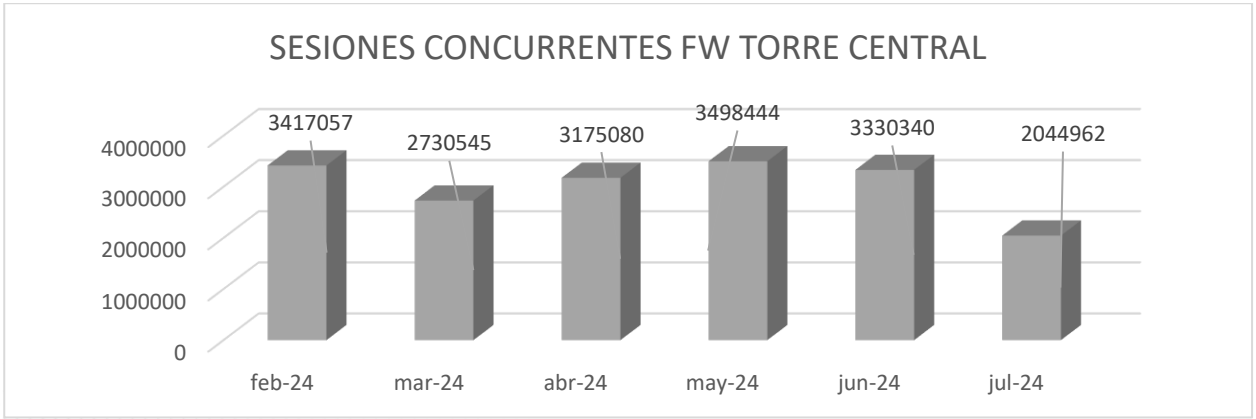
### 11.2 Cantidad de sesiones firewall perimetral.

Durante julio se presentó un máximo de 2.044.962 sesiones TCP concurrentes, cantidad que se encuentra dentro del rango máximo soportado por el appliance Fortinet FG- 4400F cuyo valor es de 210 millones.




### 11.3 Histórico de sesiones de los últimos 6 meses en el firewall perimetral.

Durante julio se presentó un leve descenso en las sesiones en el FW perimetral correspondientes a 2.044.962 de sesiones:



| MES | SESIONES |
|---|---|
| **feb-24** | 3417057 |
| **mar-24** | 2730545 |
| **abr-24** | 3175080 |
| **may-24** | 3498444 |
| **jun-24** | 3330340 |
| **jul-24** | 2044962 |

### 11.4 Aplicaciones y protocolos por ancho de banda firewall perimetral.

Amazon AWS fue la aplicación con mayor consumo de ancho de banda durante julio:

Top Applications by Bandwidth

| # | Application | Bandwidth | Sent | Received |
|---|---|---|---|---|
| 1 | Amazon-AWS | | | 439.08 TB |
| 2 | HTTPS | | | 246.93 TB |
| 3 | SSL | | | 110.75 TB |
| 4 | Microsoft.SharePoint | | | 62.46 TB |
| 5 | TCP/1433 | | | 33.72 TB |
| 6 | DTLS | | | 26.17 TB |
| 7 | Microsoft.365.Portal | | | 26.01 TB |
| 8 | Microsoft.Portal | | | 22.22 TB |
| 9 | OneDrive | | | 19.42 TB |
| 10 | TCP/9443 | | | 19.03 TB |

SMB, HTTPS y DNS fueron las aplicaciones con mayor consumo de sesiones durante julio:

Top Applications by Sessions

| # | Application | Sessions |
|---|---|---|
| 1 | DNS | 2,743,127,476 |
| 2 | SMB | 2,104,946,555 |
| 3 | HTTPS | 1,398,789,489 |
| 4 | Microsoft.Windows.Update | 738,330,187 |
| 5 | SSL | 593,586,872 |
| 6 | Microsoft.365.Portal | 576,525,623 |
| 7 | Microsoft.Portal | 536,068,484 |
| 8 | ESET-Eset.Service | 403,260,545 |
| 9 | HTTP | 358,209,900 |
| 10 | SQUID | 353,702,297 |

### 11.5 Top de destinos web por sesiones firewall perimetral.

La IP 8.243.164.19 (CTL Colombia) tuvo la mayor cantidad de consumo de ancho de banda durante el mes de julio:

Top Bandwidth IP

| # | Hostname(or IP) | Sessions |
|---|---|---|
| 1 | 8.243.164.19 | 438,177,961 |
| 2 | 172.28.107.71 | 390,693,020 |
| 3 | microsoft.com | 282,047,746 |
| 4 | 8.243.164.21 | 278,887,727 |
| 5 | 192.168.213.94 | 268,256,701 |
| 6 | windowsupdate.com | 253,183,459 |
| 7 | spotify.com | 211,880,470 |
| 8 | 172.16.182.100 | 166,845,267 |
| 9 | 3.131.127.126 | 103,844,000 |
| 10 | 13.58.19.32 | 103,588,416 |

### 11.6 Top de usuarios con peticiones bloqueadas por el firewall perimetral.

Las IPs 172.16.35.145 y 172.16.33.29, hosts de Cundinamarca, Bogota; Edificio Nemqueteba, presentaron la mayor cantidad de peticiones bloqueadas durante julio:

Top Web Users by Blocked Requests

| # | User (or IP) | Hostname | Requests |
|---|---|---|---|
| 1 | 172.16.35.145 | 172.16.35.145 | 18,175,728 |
| 2 | 172.16.33.29 | 172.16.33.29 | 15,506,861 |
| 3 | 192.168.199.32 | 192.168.199.32 | 10,620,180 |
| 4 | 172.16.182.155 | 172.16.182.155 | 9,577,596 |
| 5 | 172.16.56.165 | 172.16.56.165 | 6,892,840 |
| 6 | 172.28.69.113 | 172.28.69.113 | 6,590,937 |
| 7 | 192.168.66.85 | 192.168.66.85 | 6,305,088 |
| 8 | 172.25.13.191 | 172.25.13.191 | 5,704,110 |
| 9 | 192.168.46.197 | 192.168.46.197 | 5,550,432 |
| 10 | 192.168.100.183 | 192.168.100.183 | 5,130,911 |

Se recomienda verificar los hosts del listado a fin de que no continúen intentando conexiones a destinos bloqueados por el firewall perimetral y se descarte software malicioso instalado intentando hacer estas conexiones.

### 11.7 Top de las categorías más bloqueadas por el firewall perimetral.

Internet Radio and TV fue la categoría con mayor cantidad de bloqueos durante julio.

Top Blocked Web Categories

| # | Category | Requests |
|---|---|---|
| 1 | Internet Radio and TV | 277,007,011 |
| 2 | Games | 16,879,937 |
| 3 | Streaming Media and Download | 8,953,633 |
| 4 | Proxy Avoidance | 6,172,796 |
| 5 | Unrated | 4,011,162 |
| 6 | Social Networking | 3,721,114 |
| 7 | Entertainment | 849,161 |
| 8 | Information Technology | 623,584 |
| 9 | Malicious Websites | 472,901 |
| 10 | Society and Lifestyles | 316,896 |

### 11.8 Top de IP más activos Firewall Perimetral

Los hosts con mayor cantidad de peticiones durante julio fueron los dispositivos del breakout de Cirion 10.101.100.0/24 "SDWAN LUMEN":

Top Web IP by Allowed Requests

| # | IP | Requests |
|---|---|---|
| 1 | 10.101.100.114 | 11,437,103 |
| 2 | 10.101.100.38 | 6,702,313 |
| 3 | 10.101.100.34 | 6,430,976 |
| 4 | 10.101.100.194 | 5,141,349 |
| 5 | 10.101.100.122 | 5,111,053 |
| 6 | 10.101.100.70 | 4,641,033 |
| 7 | 10.101.100.134 | 4,640,105 |
| 8 | 10.101.102.6 | 3,643,315 |
| 9 | 10.101.100.170 | 3,507,547 |
| 10 | 10.101.101.50 | 3,372,141 |

### 11.9 Top de categorías más visitadas Firewall Perimetral

La categoría más visitada durante julio fue Information Technology:

Top Allowed Web Categories

| # | catdesc | requests |
|---|---|---|
| 1 | Information Technology | 452735423 |
| 2 | Overrride_permitidas | 710585 |

### 11.10 Top de consumo ancho de banda por usuario Firewall Perimetral

Las maquinas con IP 172.28.107.90 y 172.28.107.84 de la nube privada de IFX presentaron el mayor consumo de ancho de banda durante julio:

Top IP by Bandwidth

| # | IP | Bandwidth | Sent | Received |
|---|---|---|---|---|
| 1 | 172.28.107.90 | | | 127.70 TB |
| 2 | 172.28.107.84 | | | 90.10 TB |
| 3 | 172.31.10.41 | | | 83.05 TB |
| 4 | 172.28.107.80 | | | 78.10 TB |
| 5 | 172.28.107.86 | | | 71.06 TB |
| 6 | 172.17.201.251 | | | 66.86 TB |
| 7 | 172.17.201.252 | | | 32.92 TB |
| 8 | 10.1.2.31 | | | 31.97 TB |
| 9 | 172.28.107.79 | | | 29.45 TB |
| 10 | 172.27.64.17 | | | 28.13 TB |

## 11. TRÁFICO VPN FIREWALL PERIMETRAL

El top 10 de los usuarios conectados a la VPN SSL durante julio fue el siguiente:

Copy of InformeVPNssl_EDWSI(SSL - Dialup IPsec)_2023-05-16 14:25:10

| # | f_user | devname | vpn_type_group | end_time | remip | connections | Duration | bandwidth | traffic_in | traffic_out |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | cvillam | CSJ_FTG_DC_TC_FG4400_ | ssl-tunnel | 2024-07-31 23:54:07 | 181.55.51.20 | 92 | 627:09:13 | 4.58 GB | 580926907 | 4339839360 |
| 2 | Ecoralb | CSJ_FTG_DC_TC_FG4400_ | ssl-tunnel | 2024-07-31 23:53:07 | 190.25.107.154 | 187 | 598:35:10 | 21.11 GB | 2643224909 | 20020498563 |
| 3 | jariasu | CSJ_FTG_DC_TC_FG4400_ | ssl-tunnel | 2024-07-31 22:45:43 | 181.137.8.129 | 87 | 486:26:51 | 682.44 MB | 212194115 | 503400327 |
| 4 | lmarinmo | CSJ_FTG_DC_TC_FG4400_ | ssl-tunnel | 2024-07-30 22:46:41 | 181.136.233.42 | 86 | 457:29:24 | 18.65 GB | 1197235700 | 18830896280 |
| 5 | ssuareza | CSJ_FTG_DC_TC_FG4400_ | ssl-tunnel | 2024-07-31 14:41:52 | 181.58.39.249;181.58.39.80 | 151 | 380:42:25 | 8.88 GB | 735880196 | 8800600520 |
| 6 | lbarrerf | CSJ_FTG_DC_TC_FG4400_ | ssl-tunnel | 2024-07-31 23:56:37 | 186.155.116.70;190.25.78.236;191.156.150.83;191.156.151.9;191.156.153.235;191.156.158.125;201.244.129.84;201.244.162.151 | 73 | 377:07:11 | 46.67 GB | 2645357338 | 47470420848 |
| 7 | csichaca | CSJ_FTG_DC_TC_FG4400_ | ssl-tunnel | 2024-07-31 23:58:05 | 172.29.100.35;181.234.176.19;186.102.100.54;186.102.114.126;186.102.20.19;186.102.25.34;186.102.36.239;186.102.57.16;186.102.58.164;186.102.6.94;186.102.64.117;186.102.69.108;186.102.71.174;186.114.113.55;186.114.96.7;186.168.239.139 | 82 | 358:38:54 | 11.06 GB | 1136681765 | 10737248364 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 8 | pfajardg | CSJ_FTG_DC_TC_FG4400_ | ssl-tunnel | 2024-07-31 23:58:40 | 186.81.100.20 | 76 | 345:13:55 | 16.63 GB | 933378682 | 16919413052 |
| 9 | felixrlaraa@corteconstitucional.gov.co | CSJ_FTG_DC_TC_FG4400_ | ssl-tunnel | 2024-07-31 23:59:31 | 179.19.227.246;179.19.74.171;179.19.95.49;181.49.66.8;186.154.32.251;186.154.39.91;186.155.16.133;186.29.33.8;190.217.28.29 | 70 | 288:06:28 | 10.71 GB | 728548994 | 10774072853 |
| 10 | mpradilm@cendoj.ramajudicial.gov.co | CSJ_FTG_DC_TC_FG4400_ | ssl-tunnel | 2024-07-31 06:00:13 | 186.84.89.178;191.156.244.205;191.156.244.64;191.156.245.46;191.156.246.155;191.156.247.80;191.156.248.111;191.156.248.55;191.156.248.99;191.156.249.101;191.156.253.181;191.156.253.44;191.156.254.6;191.156.32.253;191.156.33.9;191.156.34.143;191.156.34.174;191.156.34.224;191.156.35.111;191.156.38.188;191.156.38.232;191.156.38.252;191.156.38.77;191.156.39.105;191.156.40.107;191.156.40.108;191.156.40.13;191.156.40.61; | 166 | 276:09:48 | 41.40 GB | 3033134293 | 41418994135 |

## 12.1 VPN IPSEC Site To Site Firewall Perimetral

El consumo de ancho de banda de las VPN IPSec Site to Site durante julio fue el siguiente:

VPN Site to Site(Site-to-Site IPsec)

| # | vpnname | remip | locip | Duration | bandwidth | traffic_in | traffic_out |
|---|---|---|---|---|---|---|---|
| 1 | VPN_AZURE | 52.240.53.161 | 190.217.24.4 | 2292603 | 57271694954875 | 35946120545742 | 21325574409133 |
| 2 | VPN_ORACLE | 129.213.6.36 | 190.217.80.4 | 2292333 | 2218001588266 | 2062941961506 | 155059626760 |
| 3 | VPN_SIUG_AWS-2 | 34.224.152.152 | 190.217.24.4 | 2292529 | 175418310588 | 42100731723 | 133317578865 |
| 4 | VPN_SIUG_AWS | 34.194.187.190 | 190.217.24.4 | 2292543 | 175375105814 | 43245843892 | 132129261922 |
| 5 | VPN_AZURE-ANALY | 20.124.34.235 | 190.217.24.4 | 2292603 | 130056680218 | 6652350869 | 123404329349 |
| 6 | VPN_Tierras | 181.225.76.196 | 190.217.24.4 | 2291835 | 38755346522 | 37676934703 | 1078411819 |
| 7 | VPN_Linktic | 3.222.171.115 | 190.217.24.4 | 2292591 | 815773322 | 803484689 | 12288633 |
| 8 | VPN_INPEC | 190.25.112.10 | 190.217.19.156 | 2292002 | 633676472 | 528423698 | 105252774 |
| 9 | VPN_REGISTRADU | 201.232.123.20 | 190.217.24.4 | 2292603 | 275652503 | 144053133 | 131599370 |
| 10 | OCI_EXADATA_FAB | 150.136.25.96 | 190.217.24.4 | 2292439 | 92941576 | 0 | 92941576 |
| 11 | VPN_AZURE-VWAN2 | 4.153.117.131 | 190.217.24.4 | 2291555 | 54371114 | 37841753 | 16529361 |
| 12 | VPN_FISCALIA | 190.157.218.66 | 190.217.24.4 | 2290845 | 35988155 | 34329260 | 1658895 |
| 13 | VPN_AZURE-VWAN | 4.153.117.133 | 190.217.24.4 | 2291666 | 15834188 | 15825160 | 9028 |

## 12.2 Top de intrusiones detectadas por el IPS del firewall perimetral

Las intrusiones detectadas y bloqueadas por los perfiles IPS del FortiGate durante julio fueron los siguientes:

Top Attacks

| # | Attack Name | Severity | CVE-ID | Counts |
|---|---|---|---|---|
| 1 | Spring.Framework.SerializationUtils.Insecure.Deserialization | Critical | CVE-2022-22965 | 480,440 |
| 2 | tcp_syn_flood | Critical | | 161,237 |
| 3 | Adobe.ColdFusion.Multiple.Vulnerabilities | Critical | CVE-2013-0625,CVE-2013-0629,CVE-2013-0631,CVE-2013-0632 | 95,120 |
| 4 | tcp_src_session | Critical | | 67,472 |
| 5 | Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload | Critical | CVE-2017-11317,CVE-2017-11357,CVE-2019-18935 | 63,142 |
| 6 | HTTP.URI.Java.Expression.Language.Code.Injection | Critical | CVE-2021-22053,CVE-2022-26134 | 62,590 |
| 7 | Ivanti.EPMM.CVE-2023-35082.Authentication.Bypass | Critical | CVE-2023-35082 | 62,480 |
| 8 | Apache.Log4j.Error.Log.Remote.Code.Execution | Critical | CVE-2021-4104,CVE-2021-44228,CVE-2021-45046 | 61,110 |
| 9 | Zabbix.Frontend.CVE-2022-23131.Privilege.Elevation | Critical | CVE-2022-23131 | 60,352 |
| 10 | Remote.CMD.Shell | Critical | | 60,266 |

Las víctimas de intrusión detectadas en el firewall central durante julio fueron los siguientes hosts:

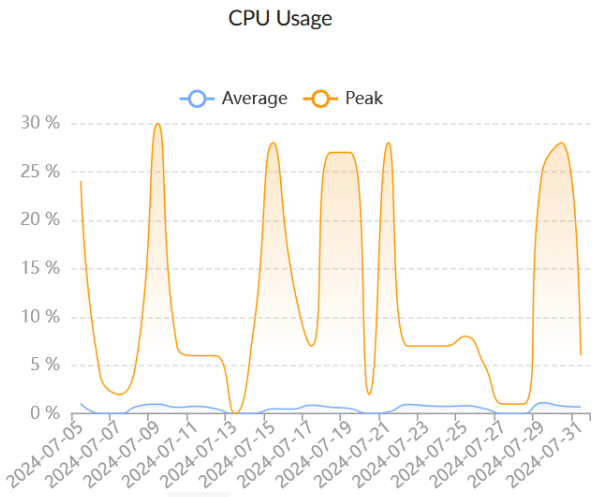
Top 20 Intrusion Victims

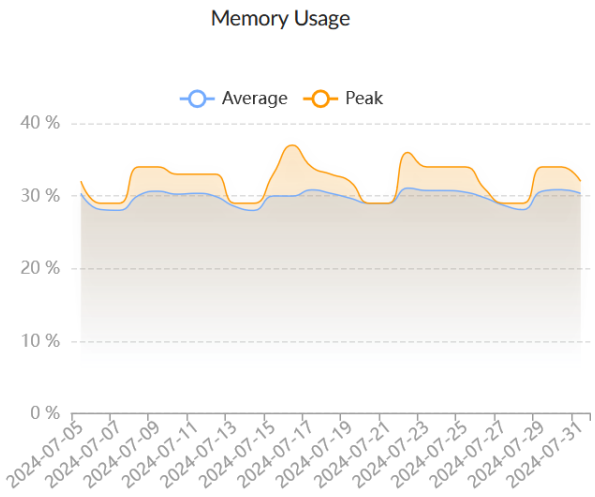
| # | Attack Victim | Counts (Critical / High / Medium) | Percent of Total Attacks |
|---|---|---|---|
| 1 | 172.17.202.39 | 9,624,200 | 96.75% |
| 2 | 190.217.24.172 | 156,746 | 1.58% |
| 3 | 190.217.24.176 | 59,551 | 0.60% |
| 4 | 172.17.201.26 | 58,716 | 0.59% |
| 5 | 172.17.201.101 | 10,491 | 0.11% |
| 6 | 192.168.213.94 | 8,495 | 0.09% |
| 7 | 34.29.85.190 | 4,685 | 0.05% |
| 8 | 34.16.47.102 | 4,265 | 0.04% |
| 9 | 192.168.55.4 | 2,837 | 0.03% |
| 10 | 108.179.229.152 | 2,794 | 0.03% |
| 11 | 190.217.24.69 | 2,201 | 0.02% |
| 12 | 172.17.201.52 | 2,194 | 0.02% |
| 13 | 193.106.191.201 | 1,731 | 0.02% |
| 14 | 172.17.201.13 | 1,604 | 0.02% |
| 15 | 172.17.202.239 | 1,438 | 0.01% |
| 16 | 172.17.201.68 | 1,342 | 0.01% |
| 17 | 186.112.121.169 | 1,122 | 0.01% |
| 18 | 172.16.6.66 | 1,104 | 0.01% |
| 19 | 179.13.6.213 | 1,072 | 0.01% |
| 20 | 172.27.117.117 | 1,067 | 0.01% |

Los hosts 190.217.24.172 y 190.217.24.176 son aplicaciones web del CSJ, el host 172.17.202.39 está en el CAN, sin embargo, estas aplicaciones están siendo protegidas por los WAF Torre Central y el WAF CAN.

## 12. FIREWALL SEDE PALACIO

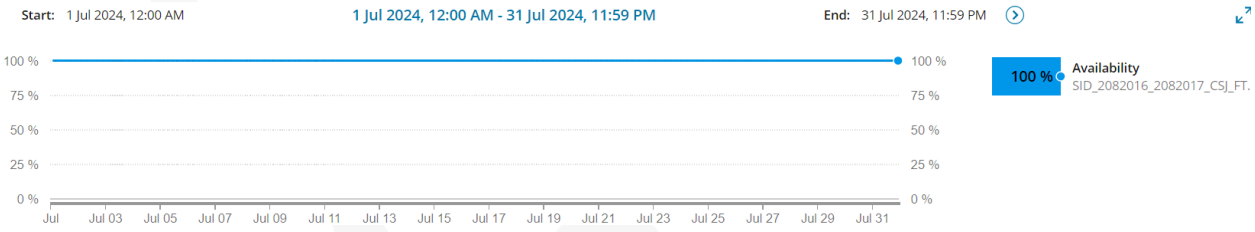
Durante julio, el consumo de CPU y memoria en el Firewall de Palacio se mantuvo dentro de sus valores de operación normal.




### a. Disponibilidad Mensual Firewall Palacio

Durante julio se obtuvo 100% de disponibilidad en el firewall de Palacio.



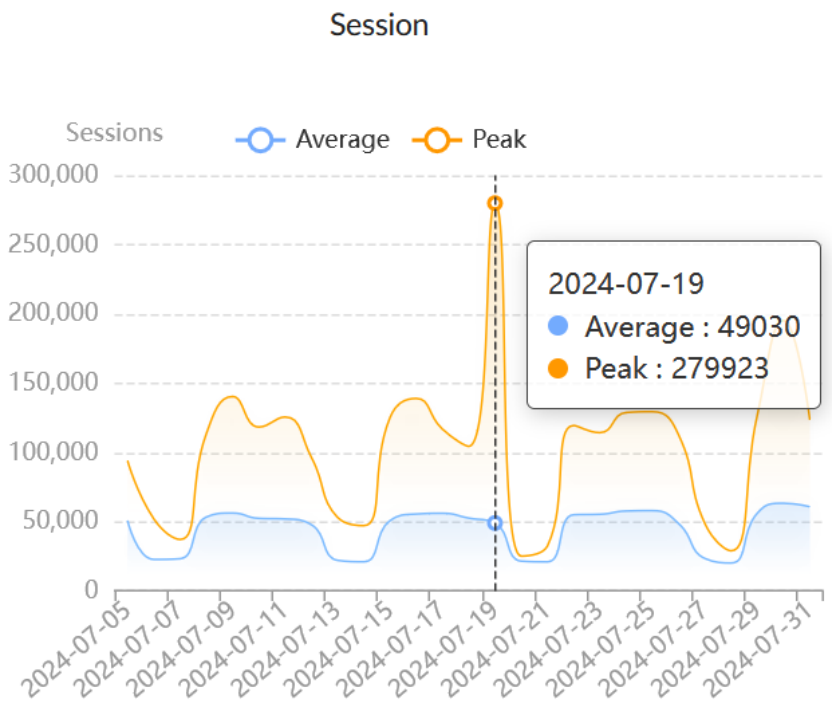
El valor de disponibilidad del 100% que presenta el gráfico lo genera automáticamente la herramienta de monitoreo, quien de los resultados diarios del mes calcula la media mensual de disponibilidad y redondea al valor del 100%.

**Availability Statistics**

| PERIOD | AVAILABILITY |
|---|---|
| Today | 100.000 % |
| Yesterday | 100.000 % |
| Last 7 Days | 100.000 % |
| Last 30 Days | 100.000 % |
| This Month | 100.000 % |
| Last Month | 100.000 % |
| This Year | 99.298 % |

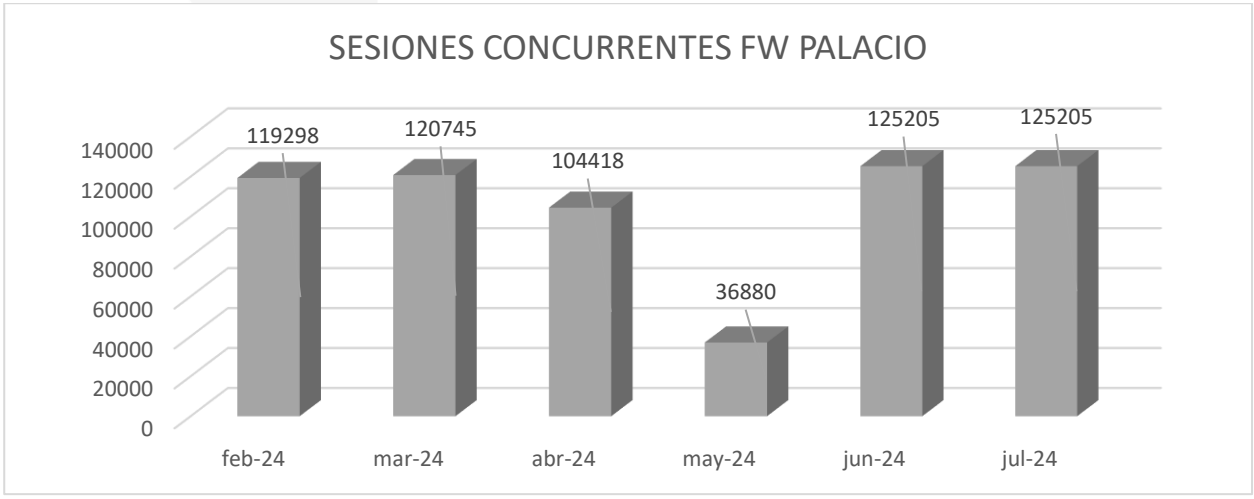
## Cantidad de Sesiones Firewall Palacio

Durante julio se presentó un máximo de 279.923 sesiones concurrentes que están dentro del rango de sesiones soportadas por el equipo Fortigate 900G de 16 Millones.




### a. Histórico de Sesiones Últimos 6 meses Firewall Palacio

En el último mes se presentó reducción en la cantidad de las sesiones del firewall de Palacio:



| MES | SESIONES |
|---|---|
| feb-24 | 119298 |
| mar-24 | 120745 |
| abr-24 | 104418 |
| may-24 | 36880 |
| jun-24 | 125205 |
| jul-24 | 125205 |

### b. Aplicaciones y protocolos por ancho de banda firewall Palacio

Las aplicaciones Microsoft.Portal, HTTPS y Microsoft.SharePoint consumieron la mayor cantidad de ancho de banda durante julio:

Top Applications by Bandwidth

| # | Application | Bandwidth | Sent | Received |
|---|---|---|---|---|
| 1 | Microsoft.Portal | | | 24.13 TB |
| 2 | HTTPS | | | 8.03 TB |
| 3 | Microsoft.SharePoint | | | 5.79 TB |
| 4 | HTTPS.BROWSER | | | 4.42 TB |
| 5 | OneDrive | | | 3.27 TB |
| 6 | SMB | | | 1.86 TB |
| 7 | MS-SQL | | | 1.79 TB |
| 8 | Lifesize | | | 1.77 TB |
| 9 | SSL | | | 1.53 TB |
| 10 | Microsoft.365.Portal | | | 1.27 TB |

SMB y DNS fueron las aplicaciones con mayor consumo de sesiones durante julio:

Top Applications by Sessions

| # | Application | Sessions |
|---|---|---|
| 1 | SMB | 476,190,332 |
| 2 | DNS | 229,553,308 |
| 3 | HTTP.BROWSER | 52,248,372 |
| 4 | Microsoft.Windows.Update | 45,867,333 |
| 5 | Microsoft.365.Portal | 37,119,720 |
| 6 | HTTPS | 34,091,379 |
| 7 | Microsoft.Portal | 31,992,790 |
| 8 | SQUID | 29,840,108 |
| 9 | SSL | 27,240,895 |
| 10 | tcp/8530 | 26,606,365 |

### c. Top de IP por ancho de banda firewall Palacio.

La dirección IP 172.28.93.2 consumió la mayor cantidad de ancho de banda durante julio:

Top Bandwidth IP

| # | IP | Bandwidth |
|---|---|---|
| 1 | 172.28.93.2 | 9.70 TB |
| 2 | 172.16.6.9 | 2.65 TB |
| 3 | 172.16.5.33 | 434.70 GB |
| 4 | 172.17.114.19 | 409.16 GB |
| 5 | 172.16.2.59 | 384.74 GB |
| 6 | 172.16.4.96 | 372.42 GB |
| 7 | 172.16.4.66 | 359.25 GB |
| 8 | 172.28.92.23 | 353.62 GB |
| 9 | 172.28.92.34 | 311.65 GB |
| 10 | 172.29.154.21 | 289.61 GB |

### d. Top de destinos web por ancho de banda Firewall Palacio.

20.60.0.104, 13.107.138.10 y 13.107.136.10, fueron destinos más visitados durante julio:

Top Websites and Category by Bandwidth

| # | Site | Category | Bytes |
|---|---|---|---|
| 1 | 20.60.0.104 | | 9.37 TB |
| 2 | 13.107.136.10 | | 3.36 TB |
| 3 | 13.107.138.10 | | 2.77 TB |
| 4 | 20.60.0.100 | | 2.61 TB |
| 5 | 172.190.220.253 | | 1.10 TB |
| 6 | 20.168.235.216 | | 642.24 GB |
| 7 | 20.60.128.228 | | 621.62 GB |
| 8 | 13.107.246.33 | | 524.19 GB |
| 9 | 52.104.3.39 | | 471.48 GB |
| 10 | 20.209.74.225 | | 435.91 GB |

### e. Top de usuarios con peticiones bloqueadas por el Firewall Palacio.

172.16.4.222 (host de la LAN Palacio), 172.28.93.142 (host de la Comisión Nacional de Disciplina Judicial) y 172.26.4.227 (host de la LAN Palacio) presentan la mayor cantidad de conexiones bloqueadas durante JULIO.

Top Web Users by Blocked Requests

| # | User (or IP) | Hostname | Requests |
|---|---|---|---|
| 1 | 172.16.4.222 | 172.16.4.222 | 159,283 |
| 2 | 172.28.93.142 | 172.28.93.142 | 131,202 |
| 3 | 172.16.4.227 | 172.16.4.227 | 102,473 |
| 4 | 192.168.230.53 | 192.168.230.53 | 88,535 |
| 5 | 192.168.8.55 | 192.168.8.55 | 77,076 |
| 6 | 172.16.4.182 | 172.16.4.182 | 62,453 |
| 7 | 172.16.5.57 | 172.16.5.57 | 54,921 |
| 8 | 172.16.4.220 | 172.16.4.220 | 47,139 |
| 9 | 172.16.6.110 | 172.16.6.110 | 37,261 |
| 10 | 192.168.230.28 | 192.168.230.28 | 28,989 |

Se recomienda verificar los hosts del listado a fin de que no continúen intentando conexiones a destinos bloqueados por el firewall perimetral y se descarte software malicioso instalado intentando hacer estas conexiones

### f. Top de las categorías más bloqueadas por el Firewall Palacio.

Las categorías más bloqueadas durante julio en el firewall Palacio fueron Unrated, Proxy Avoidance y Streaming Media and Download:

Top Blocked Web Categories

| # | Category | Requests |
|---|---|---|
| 1 | Unrated | 6,076,012 |
| 2 | Proxy Avoidance | 1,002,849 |
| 3 | Streaming Media and Download | 954,661 |
| 4 | Social Networking | 551,730 |
| 5 | Games | 152,447 |
| 6 | Entertainment | 47,001 |
| 7 | Society and Lifestyles | 36,050 |
| 8 | Phishing | 19,472 |
| 9 | Gambling | 18,387 |
| 10 | Newly Observed Domain | 15,802 |

### g. Top de IP más activas Firewall Palacio

172.16.4.90 y 172.28.54.20 (Servidores de antivirus) presentaron la mayor cantidad de conexiones durante julio:

Top Web IP by Allowed Requests

| # | IP | Requests |
|---|---|---|
| 1 | 172.16.4.90 | 22,807,793 |
| 2 | 172.28.54.20 | 22,099,162 |
| 3 | 172.16.1.7 | 525,425 |
| 4 | 172.29.97.20 | 504,856 |
| 5 | 172.17.114.158 | 494,338 |
| 6 | 172.16.5.100 | 431,637 |
| 7 | 172.16.2.215 | 409,254 |
| 8 | 172.16.6.121 | 408,674 |
| 9 | 172.17.114.232 | 406,691 |
| 10 | 172.16.2.99 | 371,260 |

### h. Top de las categorías más visitadas firewall Palacio.

Las categorías más visitadas por los usuarios de la red Palacio fueron Information Technology y Search Engines and Portals.

Top Allowed Web Categories

| # | Category | Requests |
|---|---|---|
| 1 | Information Technology | 30,866,009 |
| 2 | Search Engines and Portals | 8,451,606 |
| 3 | Business | 2,020,998 |
| 4 | Information and Computer Security | 721,212 |
| 5 | Web Analytics | 543,934 |
| 6 | Web-based Applications | 218,264 |
| 7 | Finance and Banking | 109,963 |
| 8 | Overrride_permitidas | 109,575 |
| 9 | Online Meeting | 87,157 |
| 10 | Secure Websites | 32,653 |

### i. Top de consumo ancho de banda por usuario Firewall Palacio

172.28.93.2 (host de la Comisión Nacional de Disciplina Judicial) y 172.29.154.58 (host de comisión nacional de disciplina judicial) y presentaron la mayor cantidad de conexiones durante julio:

Top IP by Bandwidth

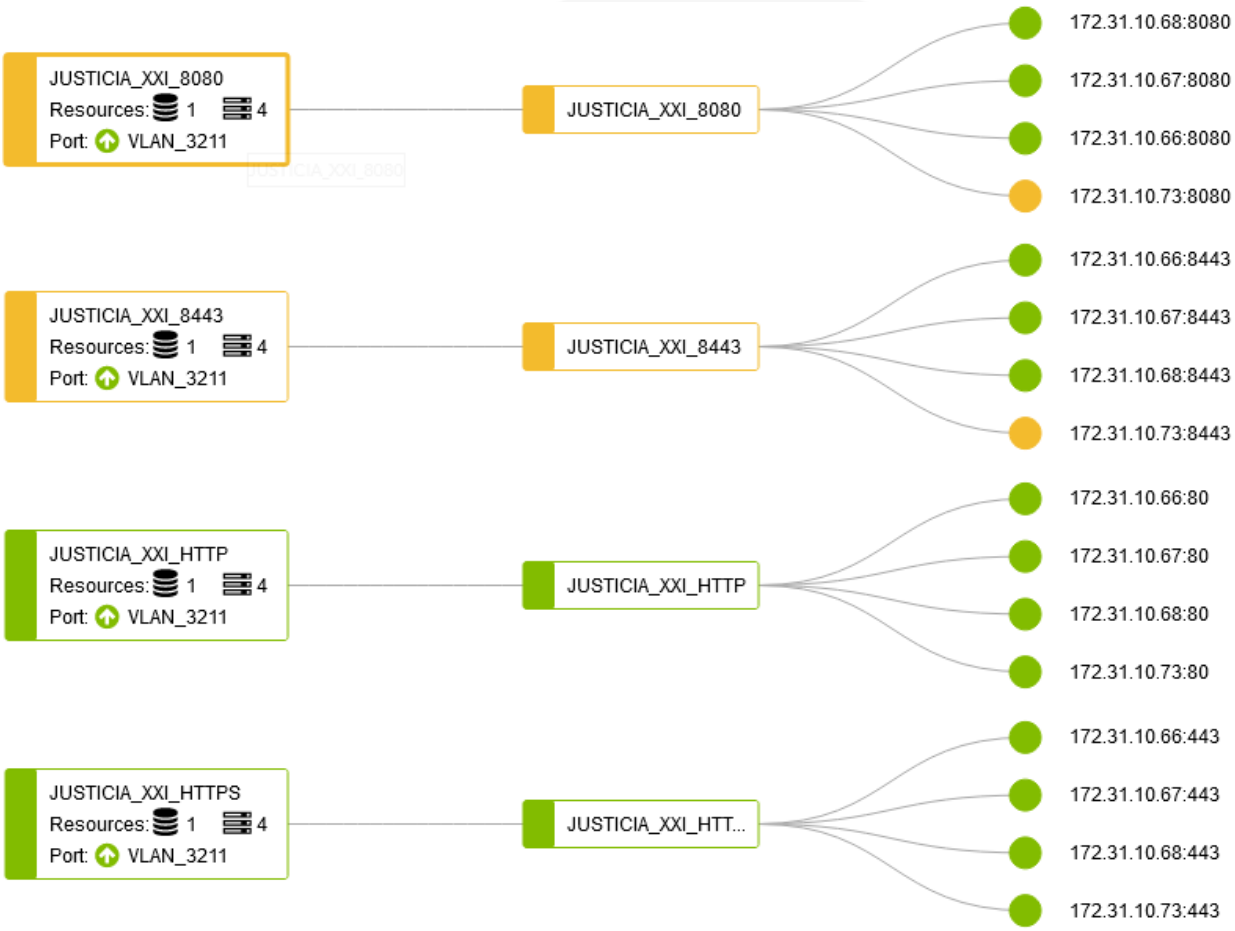
| # | IP | Bandwidth | Sent | Received |
|---|---|---|---|---|
| 1 | 172.28.93.2 | | | 9.72 TB |
| 2 | 172.29.154.58 | | | 8.50 TB |
| 3 | 172.17.201.251 | | | 4.43 TB |
| 4 | 172.16.6.9 | | | 2.64 TB |
| 5 | 172.17.201.252 | | | 2.19 TB |
| 6 | 10.101.250.4 | | | 1.89 TB |
| 7 | 172.16.4.121 | | | 960.68 GB |
| 8 | 172.17.202.250 | | | 958.03 GB |
| 9 | 172.28.107.59 | | | 738.68 GB |
| 10 | 172.28.92.15 | | | 695.12 GB |

## 13. BALANCEADOR DE CARGA FORTIADC

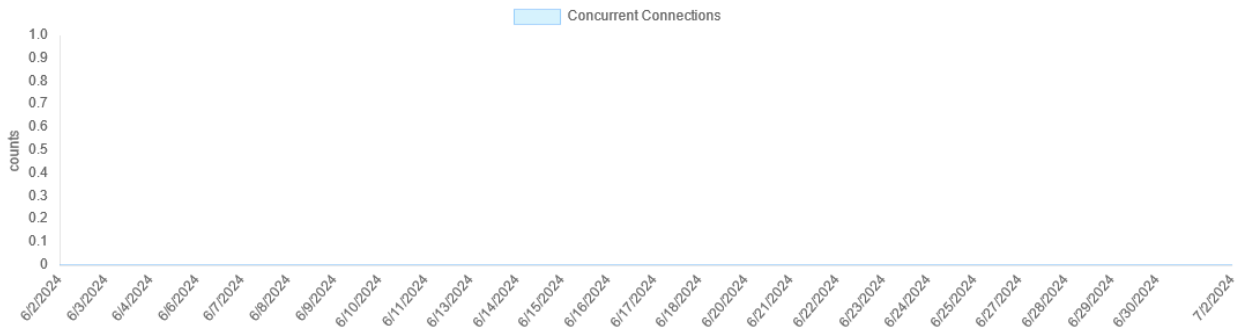
A continuación, se observan los diferentes servicios balanceados.

### a. Justicia XXI

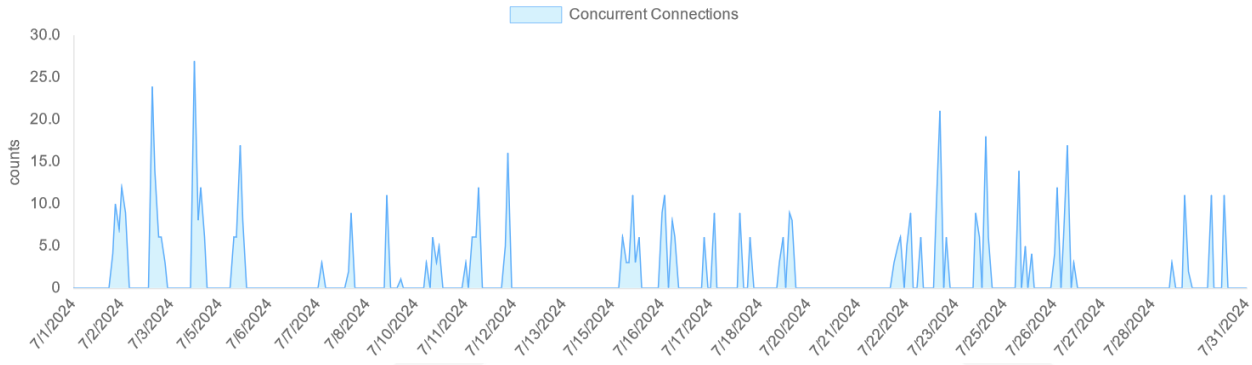
Se encuentra balanceado en el FortiADC:



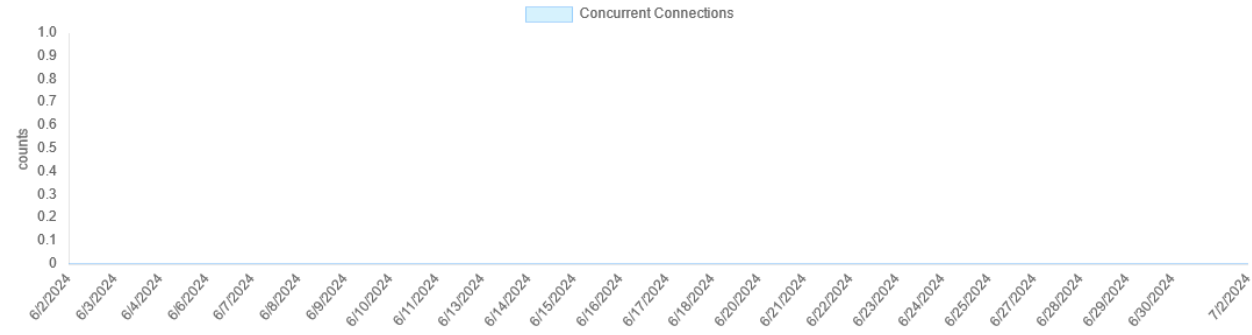

Durante JULIO no se presentó tráfico por el puerto 8080:



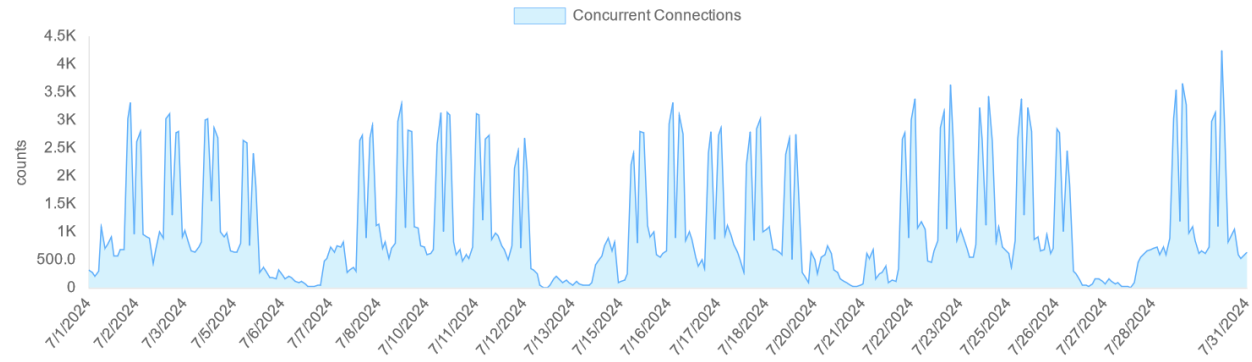
Conexiones concurrentes por el puerto 8443:




Conexiones concurrentes por el puerto 80:




Conexiones concurrentes por el puerto 443:

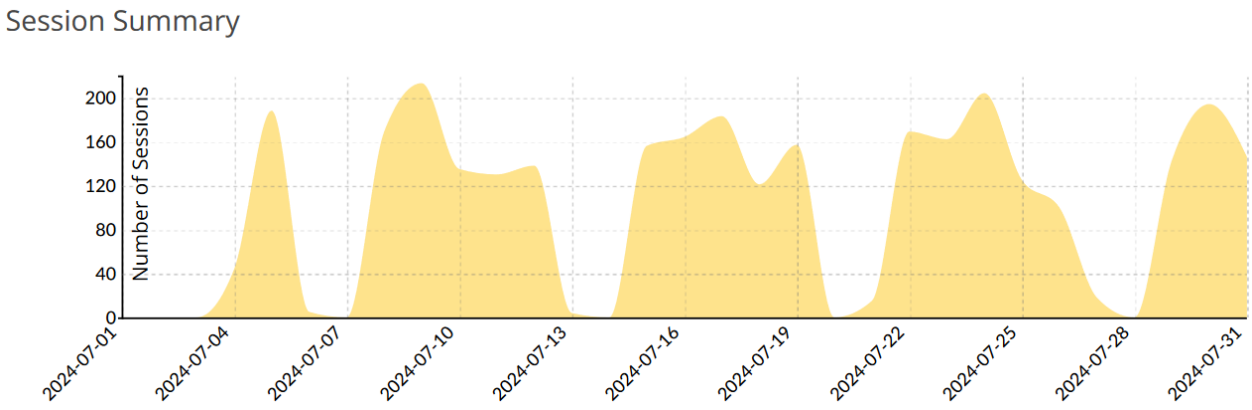



### b. Kactus RDP

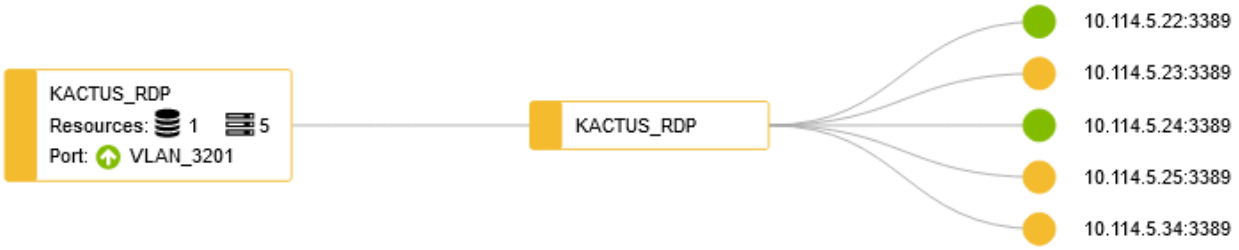
Esta aplicación se encuentra en el Firewall utilizando la siguiente configuración:

| Name | Type | Virtual Server IP | Load Balancing Method | Real Servers | Interface |
|---|---|---|---|---|---|
| IPv4 Virtual Server 1/4 | | | | | |
| KACTUS_RDP | TCP | 10.114.5.38:3389 | Static | 10.114.5.24<br>10.114.5.22 | Vlan_2000 |

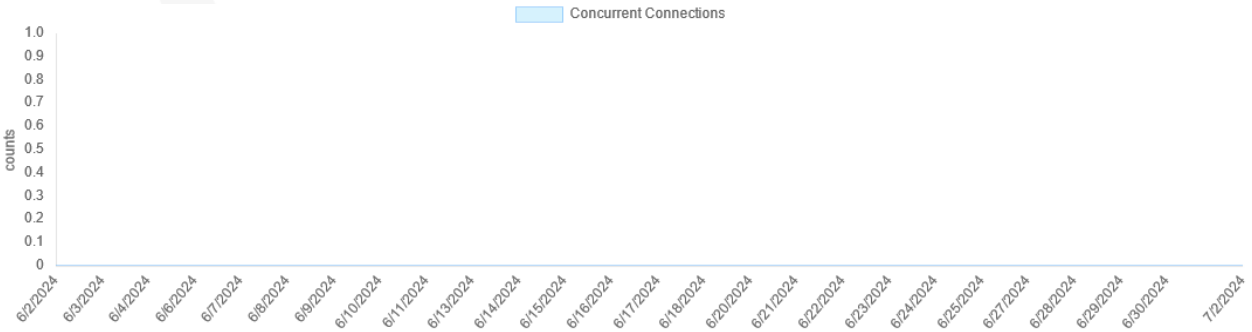
A continuación, se observa el número de sesiones concurrentes para este aplicativo.




También se encuentra balanceado en el FortiADC utilizando la siguiente configuración:

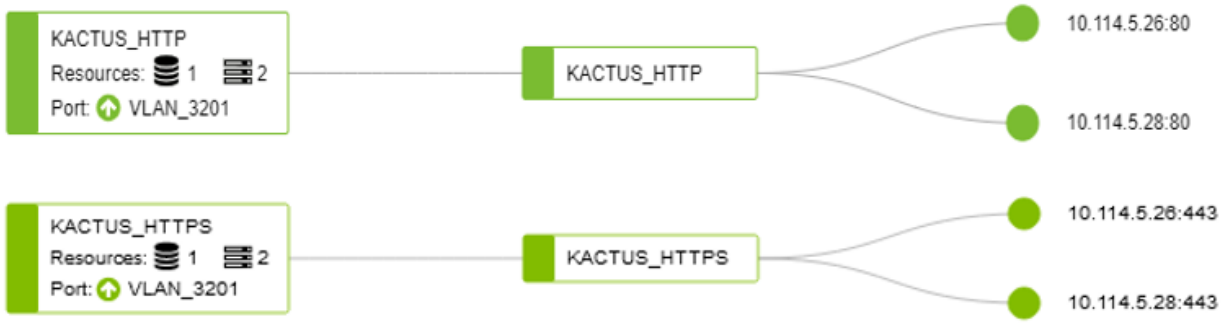



En el FortiADC no se observan sesiones concurrentes:

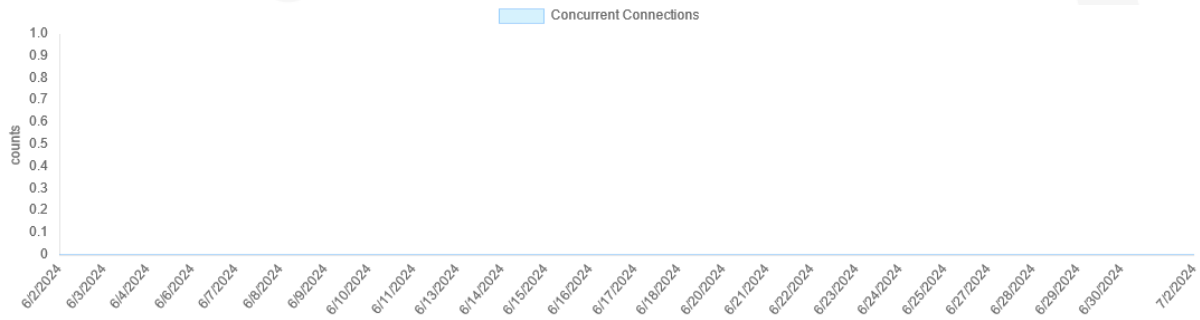


### c. Kactus WEB

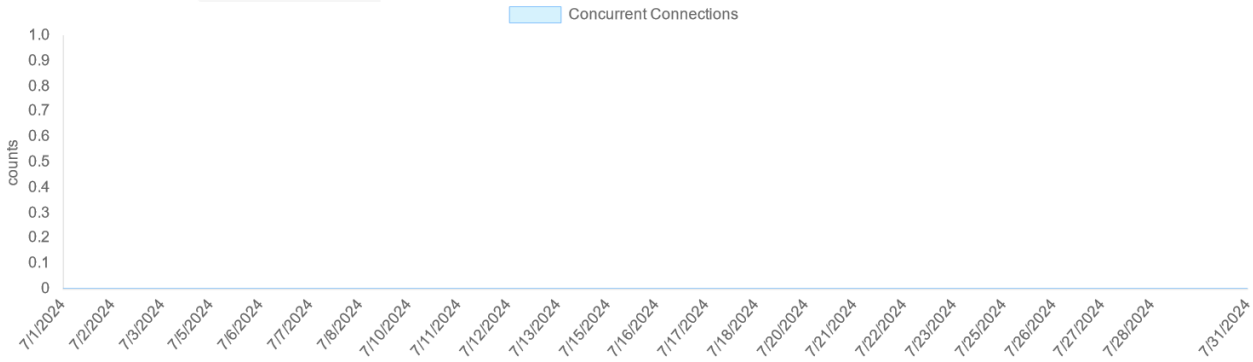
Se encuentra balanceado en el FortiADC:




En el FortiADC no se observan sesiones concurrentes por el puerto 80.




Por HTTPS se observan las siguientes conexiones del mes de JULIO:



### d. SIRNA

Este servicio se encuentra balanceado en el FortiGate perimetral:

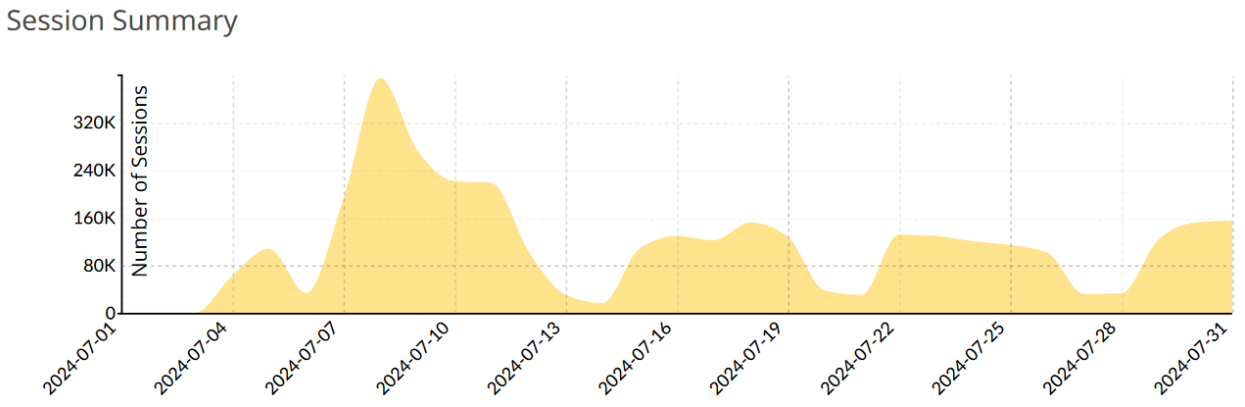
Configuración de balanceo de CRM en el Firewall.

| Name | Type | Virtual Server IP | Load Balancing Method | Health Check | Real Servers |
|---|---|---|---|---|---|
| IPv4 Virtual Server 4 | | | | | |
| CRM_HTTP_HTTPS_444 | IP | 10.244.2.236:0-65535 | Round Robin | Health_CRM_HTTP_HTTPS_444 | 10.244.2.226<br>10.244.2.227 |

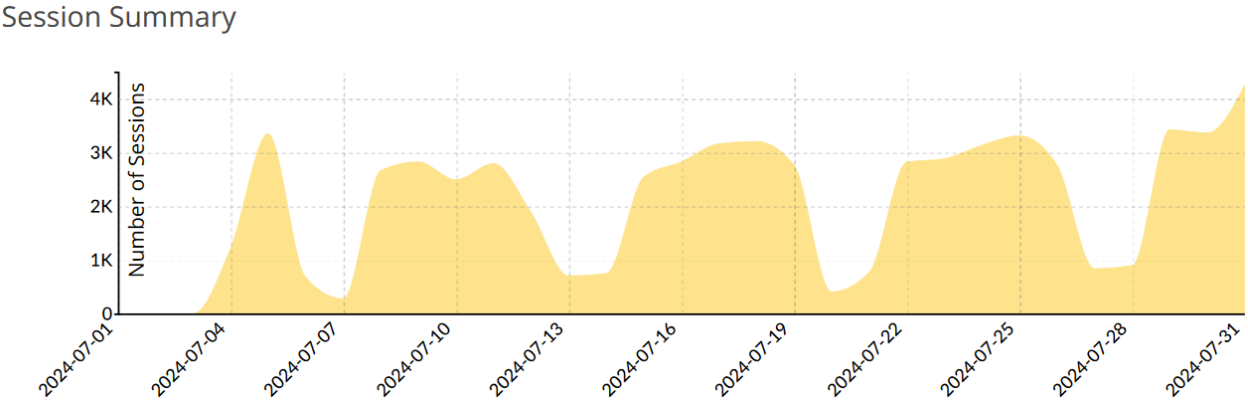
Configuración de balanceo de Sharepoint en el firewall perimetral.

| Name | Type | Virtual Server IP | Load Balancing Method | Health Check | Real Servers |
|---|---|---|---|---|---|
| IPv4 Virtual Server 1/4 | | | | | |
| SHAREPOINT | IP | 10.244.2.237:0-65535 | Round Robin | HLTCK_443 | 10.244.2.229<br>10.244.2.228 |

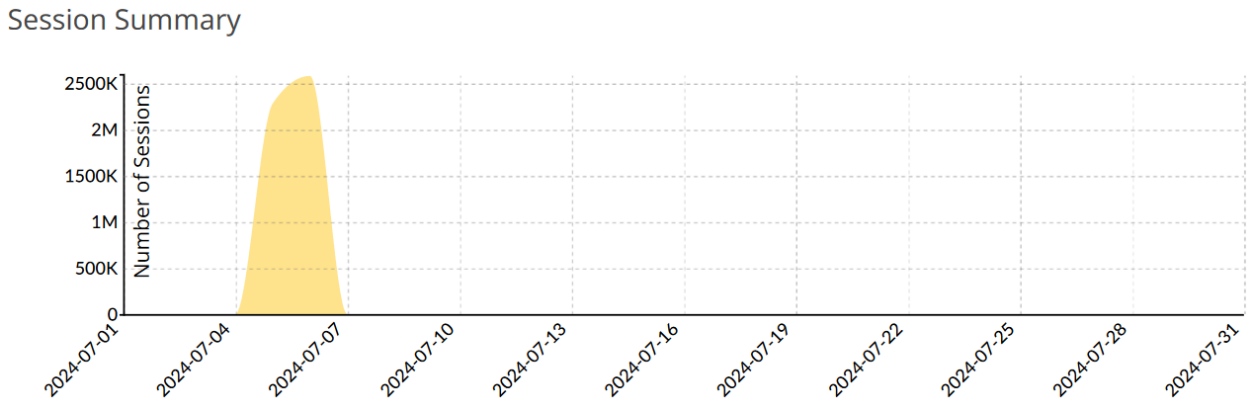
Las sesiones en el firewall para SIRNA 4443 fueron:




Las sesiones en el firewall para CRM 443 fueron:



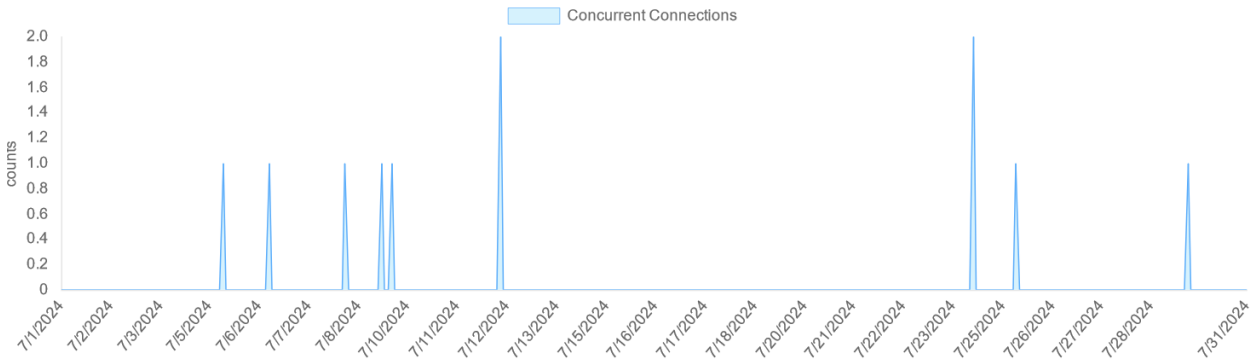
Las sesiones en el firewall para Sharepoint 444 fueron:




### e. Convocatoria Peritos.

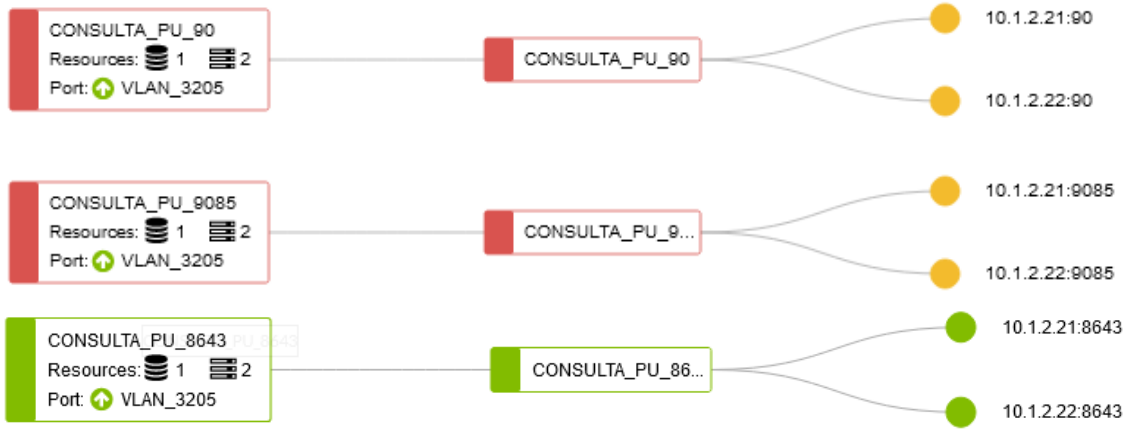
Este servicio se encuentra balanceado en el FortiADC:


Las sesiones concurrentes fueron las siguientes:

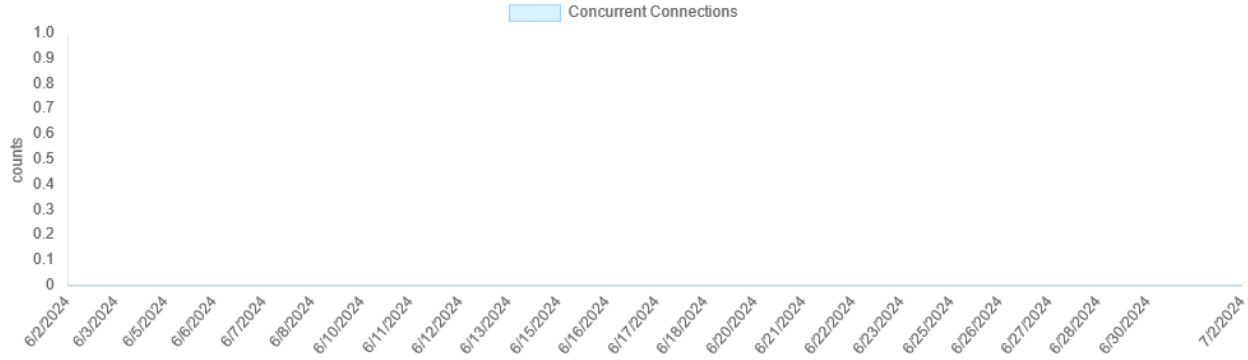


### f. Consulta De Procesos Nacional Unificada (CPNU)

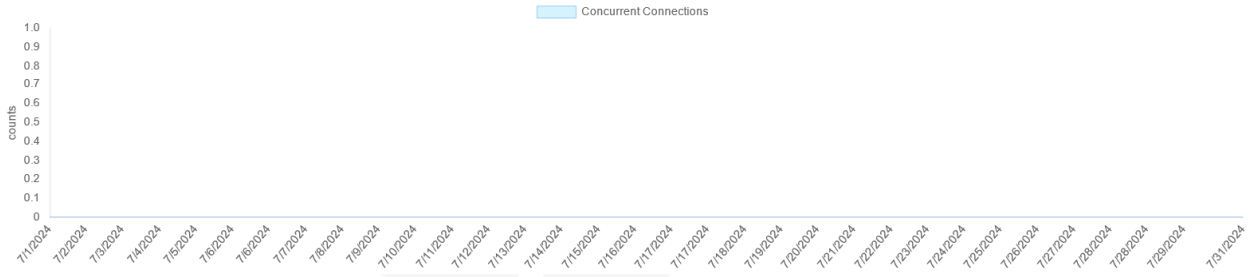
A continuación, se muestra la configuración de balanceo para esta aplicación en el FortiADC:



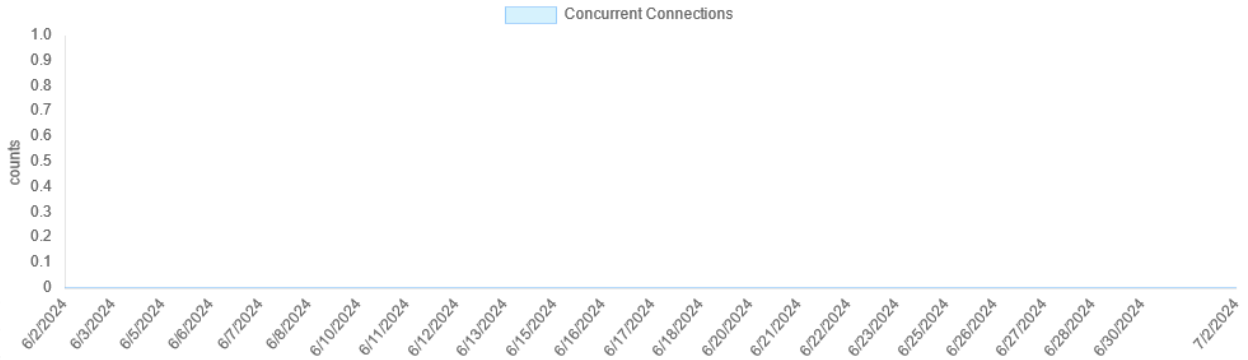

Durante JULIO no se tuvieron sesiones concurrentes por el puerto HTTP:



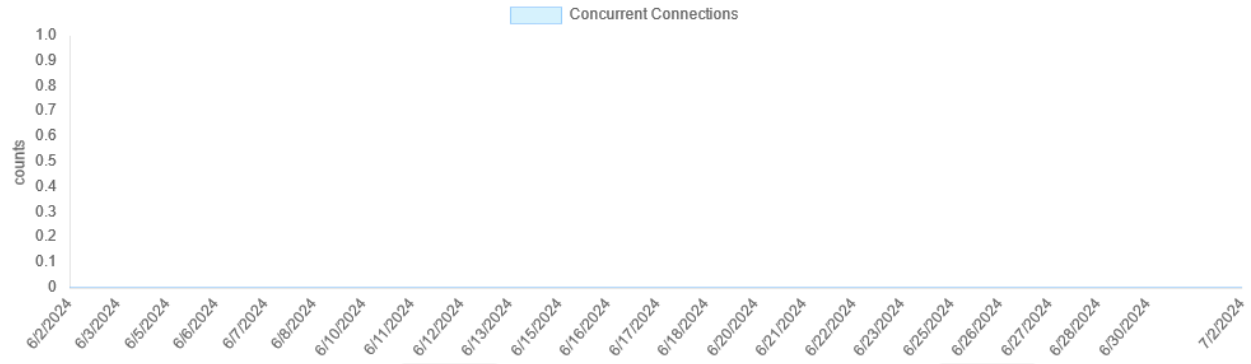

Las sesiones concurrentes por HTTPS fueron:



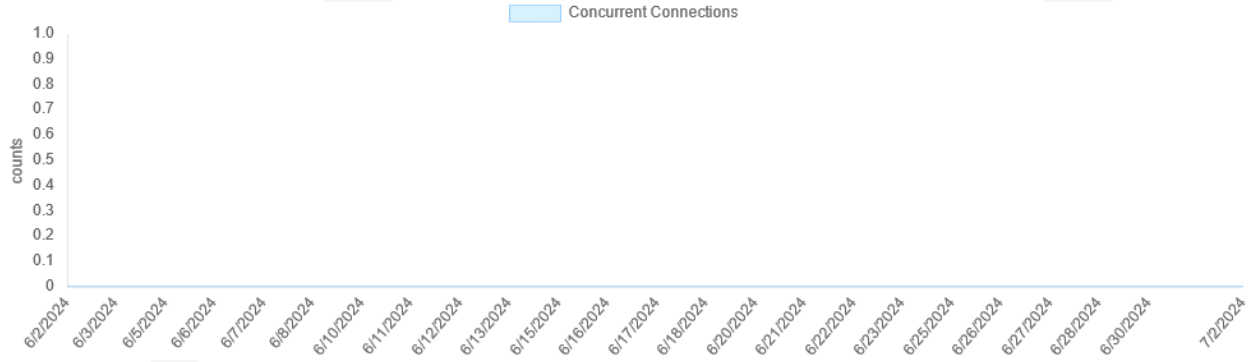

No se tuvieron sesiones concurrentes por el puerto 4431:



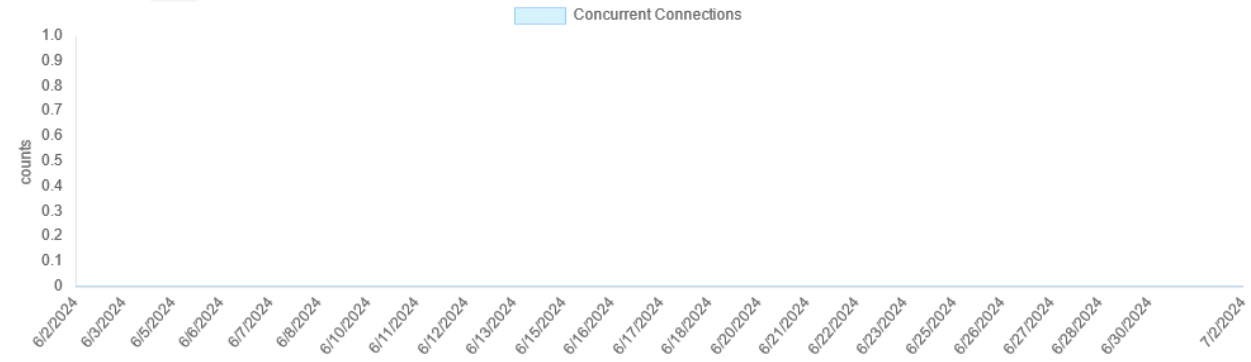
No se tuvieron sesiones concurrentes por el puerto 4432:



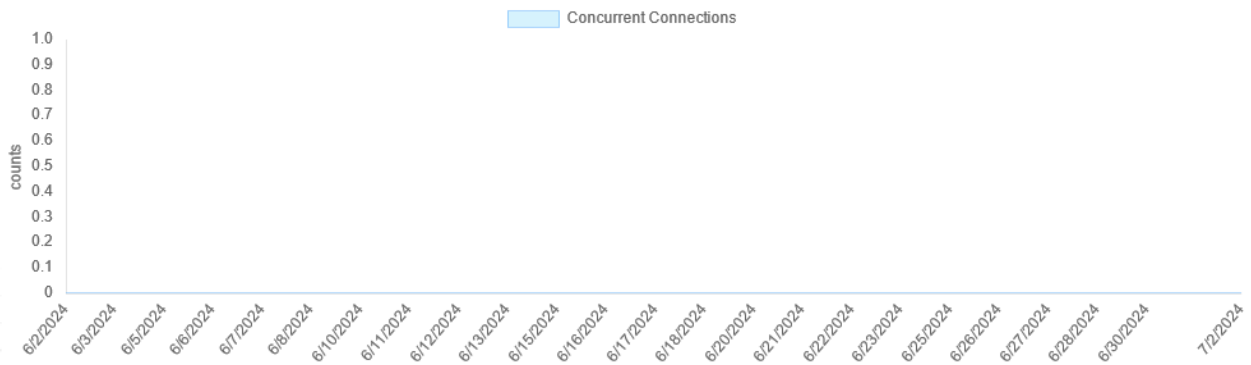

No se tuvieron sesiones concurrentes por el puerto 4435:



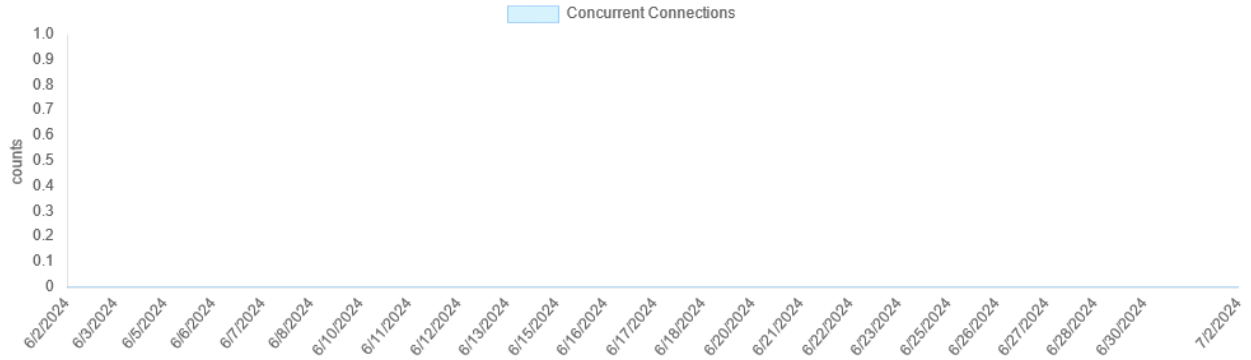

No se tuvieron sesiones concurrentes por el puerto 4436:



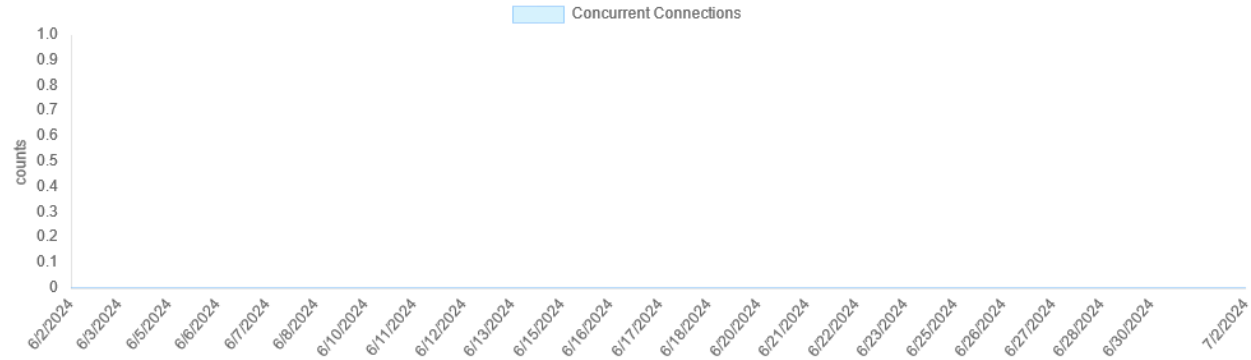

No se tuvieron sesiones concurrentes por el puerto 444:



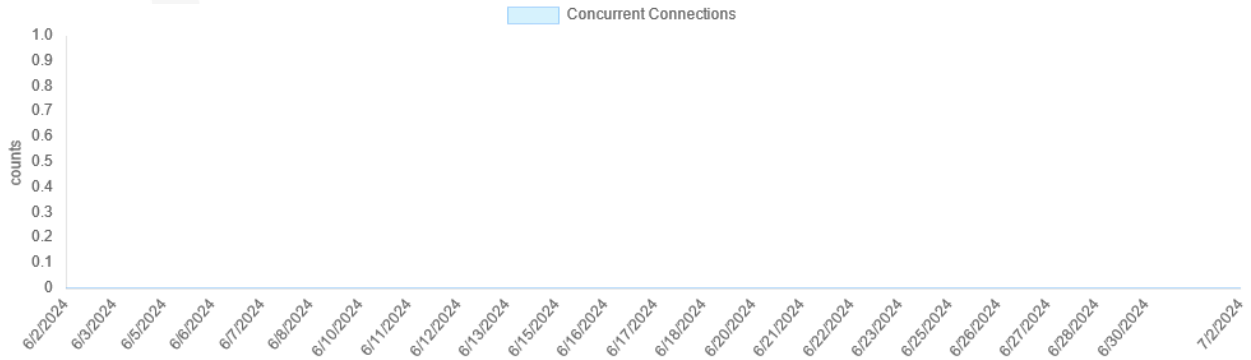
No se tuvieron sesiones concurrentes por el puerto 448:



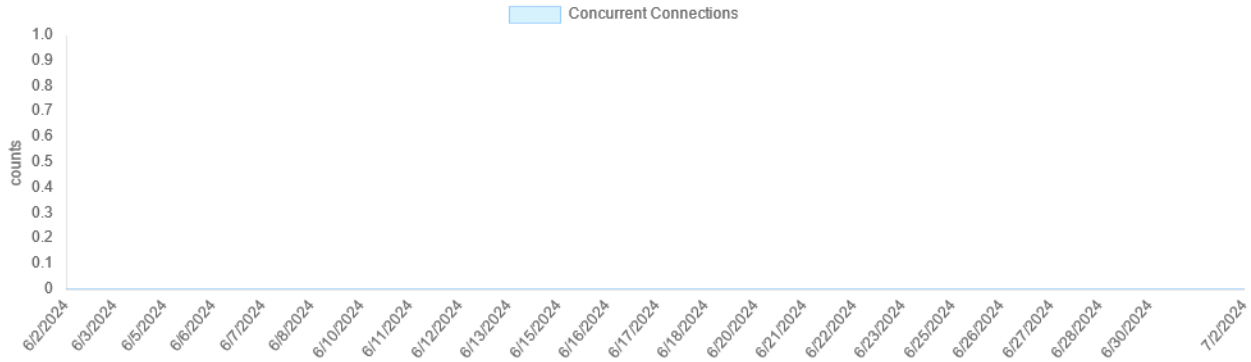

No se tuvieron sesiones concurrentes por el puerto 449:



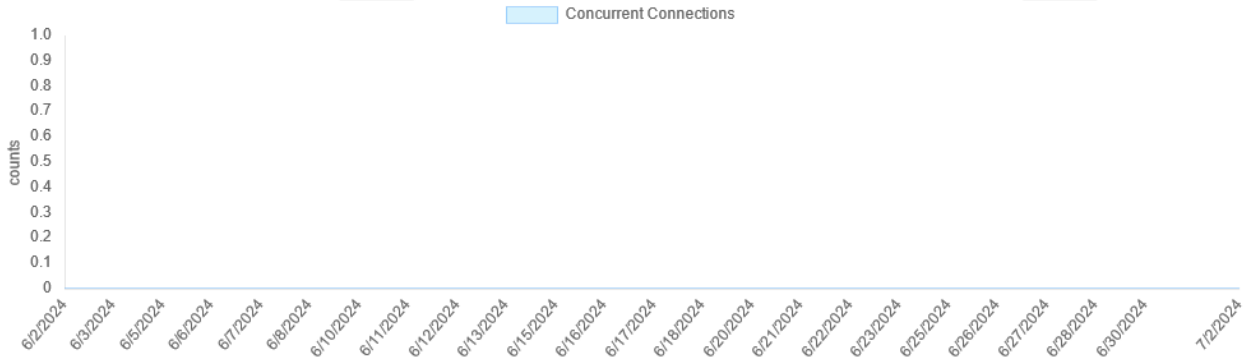

No se tuvieron sesiones concurrentes por el puerto 8085:



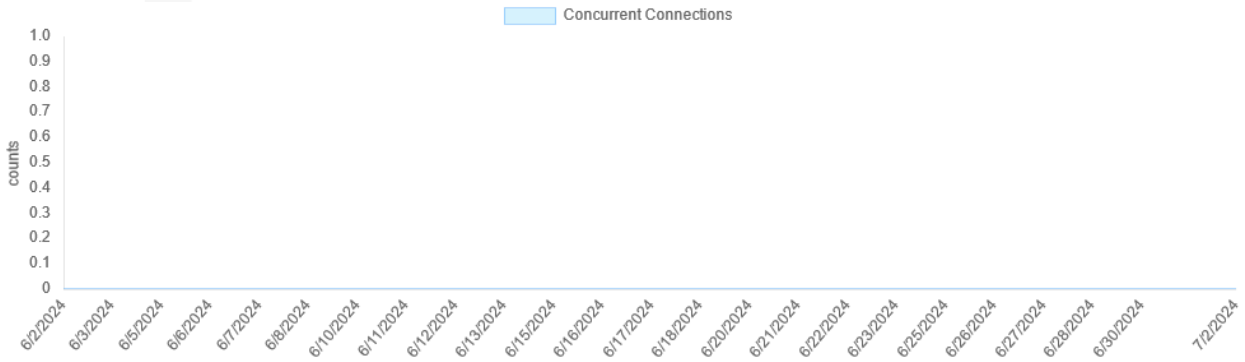
No se tuvieron sesiones concurrentes por el puerto 90:




No se tuvieron sesiones concurrentes por el puerto 9085:



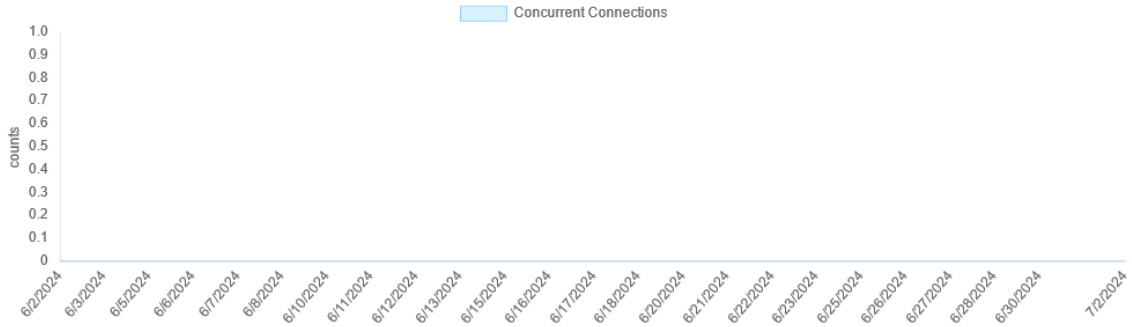

No se tuvieron sesiones concurrentes por el puerto 8643:




### g. SIERJU

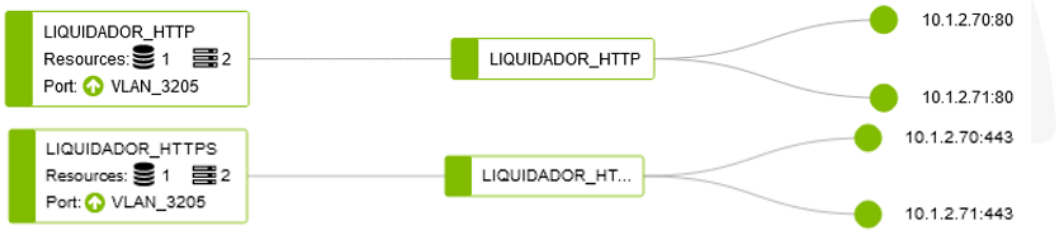
La configuración de balanceo para esta aplicación en el balanceador FortiADC es:

Durante JULIO no se observan conexiones concurrentes para este aplicativo:

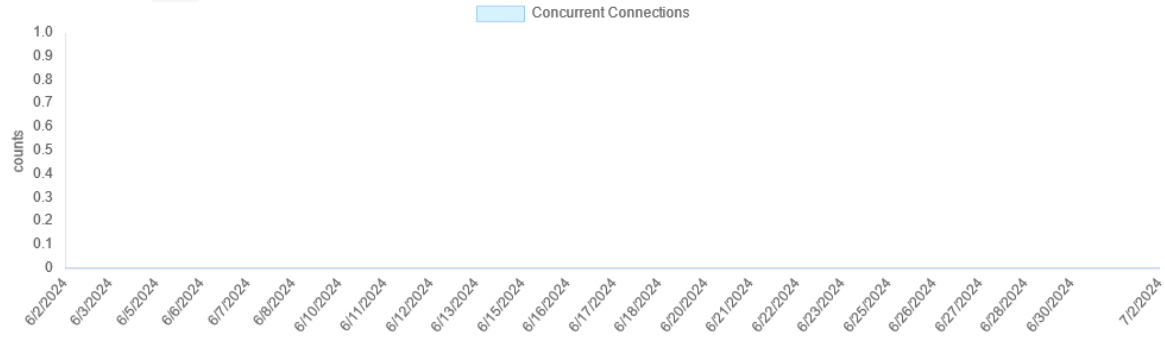



### h. Liquidador de Sentencias

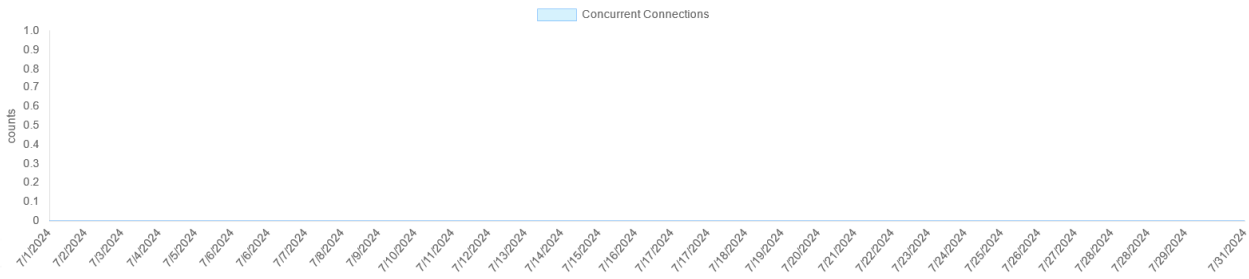
Virtual server Liquidador de Sentencias balanceador FortiADC




Durante JULIO no se observan conexiones concurrentes para este aplicativo por HTTP:



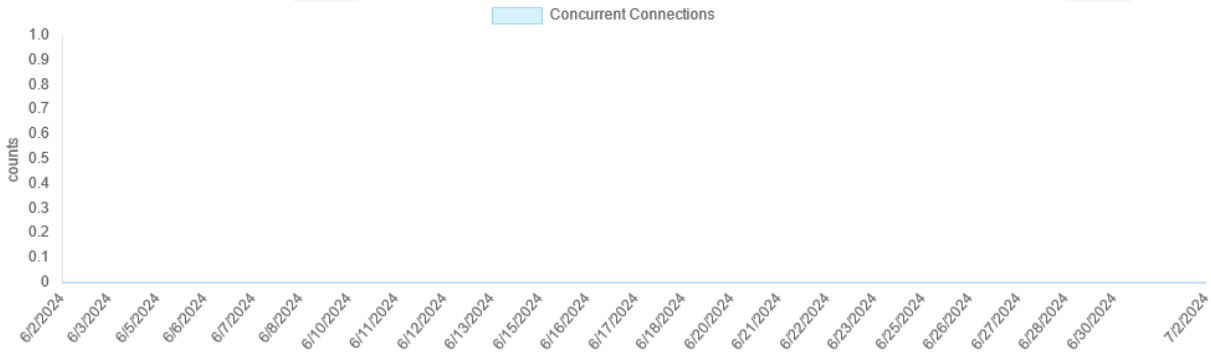

Las sesiones concurrentes por HTTPS fueron:



### i. Consulta Jurisprudencia

Virtual server Consulta Jurisprudencia se encuentra en el balanceador FortiADC.

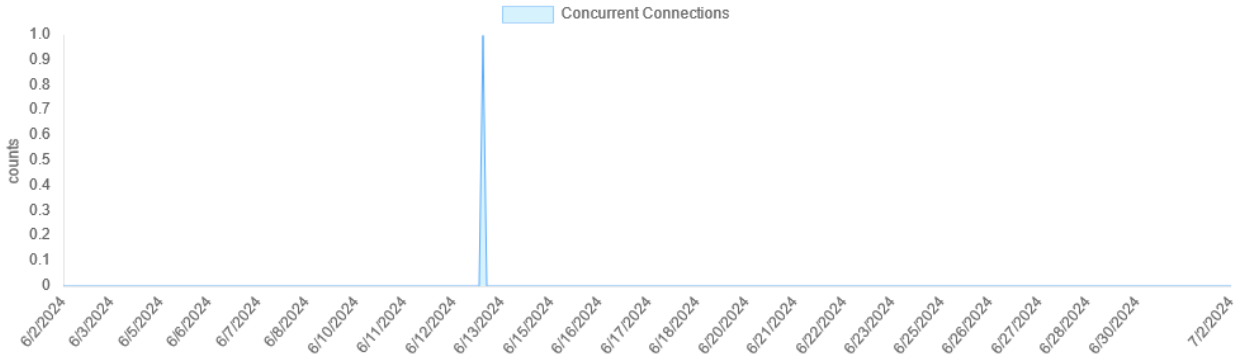

Durante JULIO no se observan conexiones concurrentes para este aplicativo:




### j. API Gestión de Audiencias

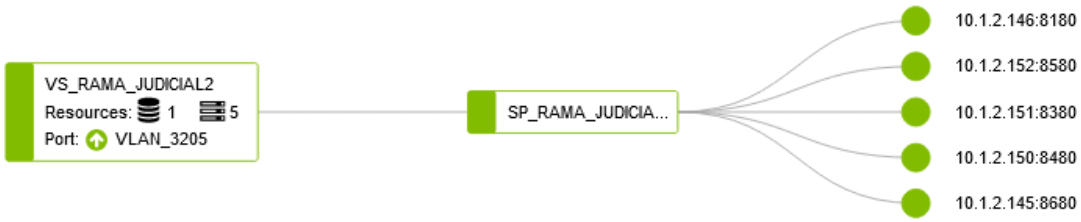
Virtual server API Gestión de Audiencias balanceador FortiADC.


Las sesiones concurrentes por HTTPS para este aplicativo:

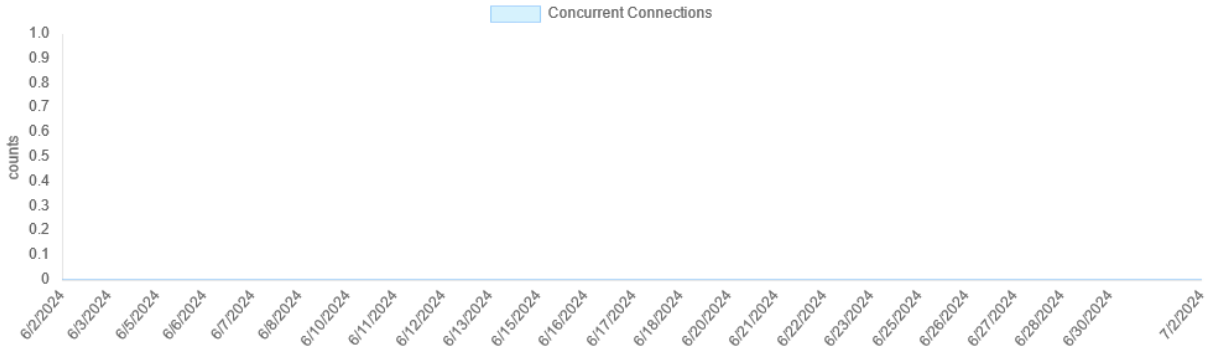


### k. Portal Alterno de la Rama Judicial

Se encuentran balanceado en el FortiADC:

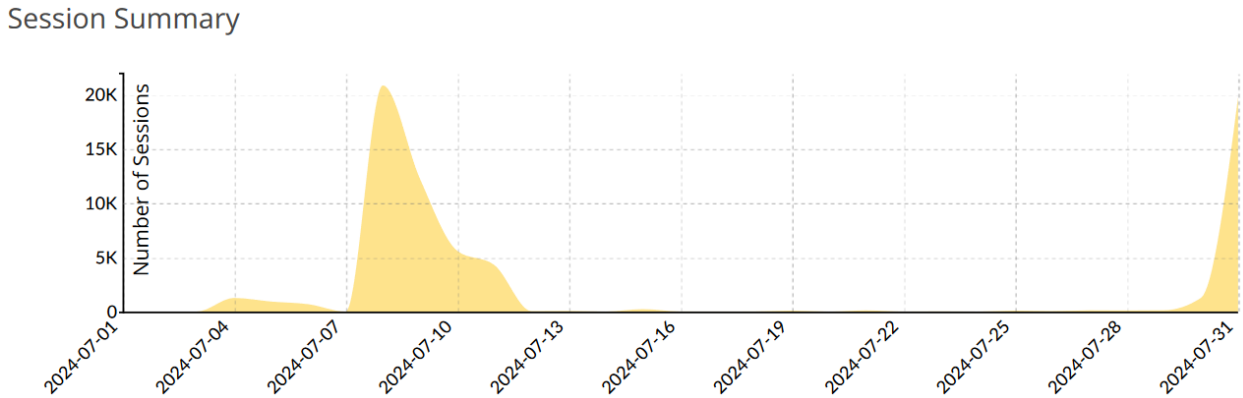



Durante JULIO no se observan conexiones concurrentes para este aplicativo:



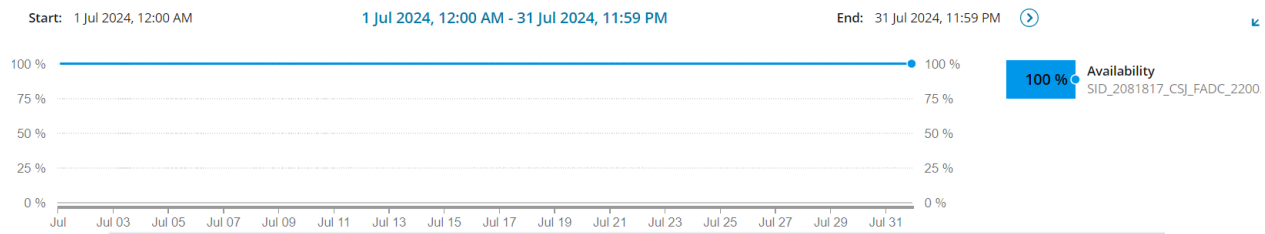

### l. Portal de la Rama Judicial

Las sesiones Historico_Portal Rama Judicial fueron:



### m. Disponibilidad y performance.

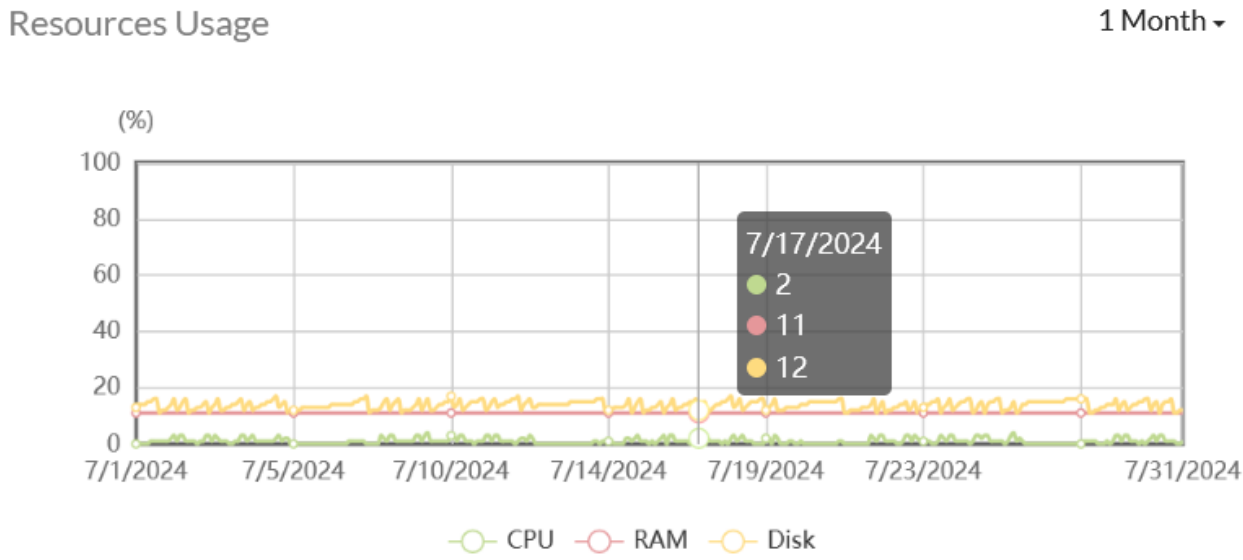
Durante JULIO se obtuvo 100% de disponibilidad en el FortiADC de Torre Central.




**Availability Statistics**

| PERIOD | AVAILABILITY |
|---|---|
| Today | 100.000 % |
| Yesterday | 100.000 % |
| Last 7 Days | 100.000 % |
| Last 30 Days | 100.000 % |
| This Month | 100.000 % |
| Last Month | 100.000 % |
| This Year | 99.923 % |

Durante julio se observa consumo de CPU del 2%, memoria 11% y disco 12%:



## 14. TRÁFICO DE WEB APPLICATION FIREWALL (WAF) TORRE CENTRAL

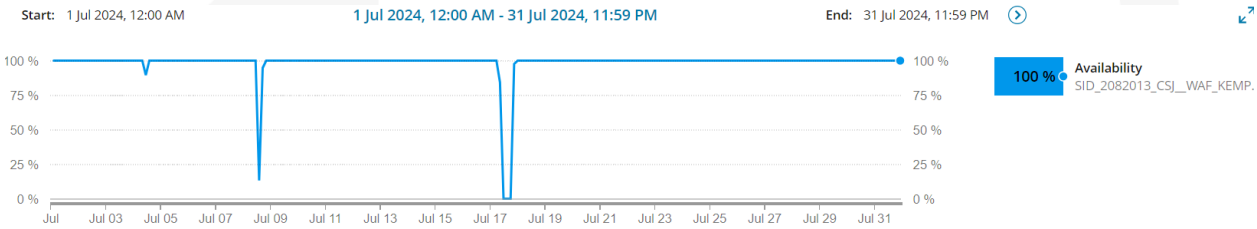
Para la protección de las aplicaciones web se tienen configuradas las siguientes políticas en los Firewall de Aplicaciones Web:

| Item | Solución WAF | Cantidad de políticas de servidores |
|---|---|---|
| 1 | WAF TORRE CENTRAL | 159 |
| 2 | WAF CAN | 67 |

A continuación, se muestran las estadísticas para cada uno de los WAF.

### a. Web application firewall datacenter principal IFX.

Durante el mes de JULIO se obtuvo una disponibilidad del 100 % en el Kemp de Torre Central.




El valor de disponibilidad del 100% que presenta el gráfico lo genera automáticamente la herramienta de monitoreo, quien de los resultados diarios del mes calcula la media mensual de disponibilidad y redondea al valor del 100%.

Los eventos del pasado 8 y 17 de julio se deben a una novedad en el sistema de monitoreo que no afecto los servicios que IFX Networks presta a la rama judicial, relacionados con los tickets TT862004 y TT866155.

**Availability Statistics**

| PERIOD | AVAILABILITY |
|---|---|
| Today | 100.000 % |
| Yesterday | 100.000 % |
| Last 7 Days | 100.000 % |
| Last 30 Days | 98.256 % |
| This Month | 100.000 % |
| Last Month | 98.291 % |
| This Year | 99.633 % |

### b. Uso de políticas de los servidores en el WAF principal Torre Central.

La aplicación web más consultada durante julio fue publicacionesprocesales.ramajudicial.gov.co - 190.217.24.175 (172.17.201.100:443) con 62'348.555 sesiones web correspondiente al 36,86%

| # | Name | Virtual IP Address | Total Conns | % del total |
|---|---|---|---|---|
| 1 | publicacionesprocesales.ramajudicial.gov.co - 190.217.24.175 | 172.17.201.100:443 | 62348555 | 36,86% |
| 2 | procesojudicial.ramajudicial.gov.co TYBA PRUEBAS | 172.17.201.249:443 | 45271903 | 26,77% |
| 3 | nuevoportal.ramajudicial.gov.co Y cndj.gov.co 190.217.24.176 | 172.17.201.101:443 | 29700894 | 17,56% |
| 4 | siicor.corteconstitucional.gov.co - 190.217.24.62 | 172.17.201.13:443 | 16725567 | 9,89% |
| 5 | consejodeestado.gov.co - 190.217.24.60 | 172.17.201.52:443 | 3550830 | 2,10% |
| 6 | consultajurisprudencial.ramajudicial.gov.co 8080 | 172.17.201.110:8080 | 2686532 | 1,59% |
| 7 | sirna.ramajudicial.gov.co | 172.17.201.28:443 | 1744417 | 1,03% |
| 8 | apigestionaudiencias1.ramajudicial.gov.co | 172.17.201.42:443 | 1341069 | 0,79% |
| 9 | liquidador.ramajudicial.gov.co | 172.17.201.56:443 | 504155 | 0,30% |
| 10 | seccionalescsj.ramajudicial.gov.co-intrajud.ramajudicial.gov.co | 172.17.201.8:443 | 485514 | 0,29% |
| | Otras aplicaciones | | 4770564 | 2,82% |
| | Total | | 169130000 | 100,00% |

### c. Top de peticiones por país WAF principal IFX.

Durante JULIO, el país desde donde se recibieron más peticiones de conexión fue Colombia:

Top 10 Countries

Total

| Country | Requests | Blocked |
|---|---|---|
| Colombia | 111.214 M | 27824745 |
| Private | 18546255 | 4893654 |
| United States | 25078485 | 1336388 |
| Argentina | 1247404 | 312285 |
| IPrep | 158193 | 158193 |
| Brazil | 1089995 | 146821 |
| Russia | 3398678 | 48507 |
| Panama | 117922 | 44335 |
| Costa Rica | 150296 | 41824 |
| Bangladesh | 262934 | 39233 |

## d. Top de ataques por política WAF principal IFX.

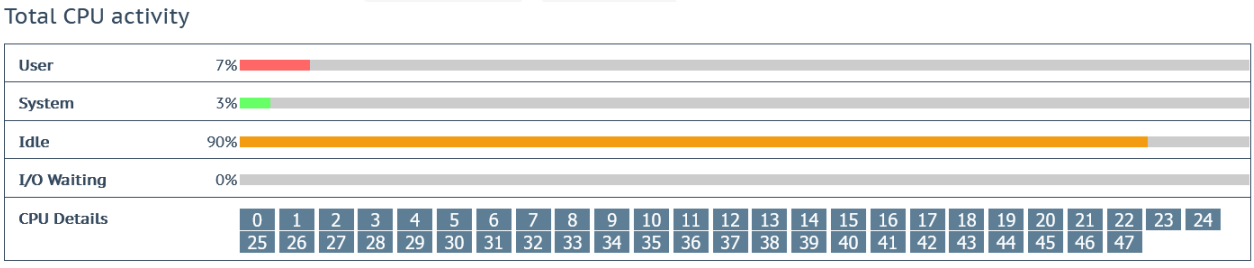
La siguiente tabla muestra el top 10 de las reglas o virtual services que proporcionaron mayor protección contra ataques a las aplicaciones web durante JULIO. Sobre las aplicaciones *publicacionesprocesales.ramajudicial.gov.co* y *consejodeestado.gov.co* han sido prevenidas la mayor cantidad de ataques durante JULIO:

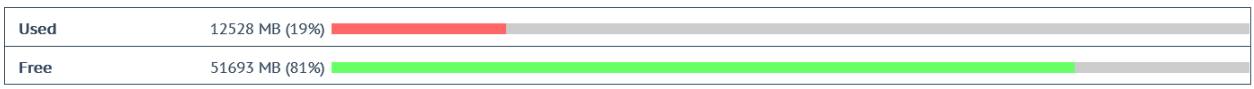
| # | Name | Virtual IP Address | Total Events | % del total |
|---|---|---|---|---|
| 1 | procesojudicial.ramajudicial.gov.co TYBA PRUEBAS | 172.17.201.249:443 | 215458755 | 38,20% |
| 2 | publicacionesprocesales.ramajudicial.gov.co - 190.217.24.175 | 172.17.201.100:443 | 116750204 | 20,70% |
| 3 | procesos.ramajudicial.gov.co_procesoscs CONSULTA AZUL | 172.17.201.26:8443 | 97615442 | 17,31% |
| 4 | nuevoportal.ramajudicial.gov.co Y cndj.gov.co 190.217.24.176 | 172.17.201.101:443 | 56678685 | 10,05% |
| 5 | siicor.corteconstitucional.gov.co - 190.217.24.62 | 172.17.201.13:443 | 32242367 | 5,72% |
| 6 | VS_Sicof_WILDFLY | 172.17.201.51:8080 | 8386661 | 1,49% |
| 7 | sirna.ramajudicial.gov.co | 172.17.201.28:443 | 6981274 | 1,24% |
| 8 | antecedentesdisciplinarios.cndj.gov.co | 172.17.201.31:443 | 5738408 | 1,02% |
| 9 | consejodeestado.gov.co - 190.217.24.60 | 172.17.201.52:443 | 4857689 | 0,86% |
| 10 | consultajurisprudencial.ramajudicial.gov.co 8080 | 172.17.201.110:8080 | 4619747 | 0,82% |
| | Otras aplicaciones | | 14701482 | 2,61% |
| | Total | | 564030714 | 100,00% |

NOTA: Los dispositivos Kemp X.25 no suministran en sus estadísticas mensuales información detallada acerca de picos de consumo, horarios específicos ni los tipos de ataques dirigidos hacia las aplicaciones web.

## e. Consumo de recursos WAF principal IFX.

El WAF KEMP de Torre Central presentó consumo de CPU del 7%, memoria de 19% y disco en un 88%.



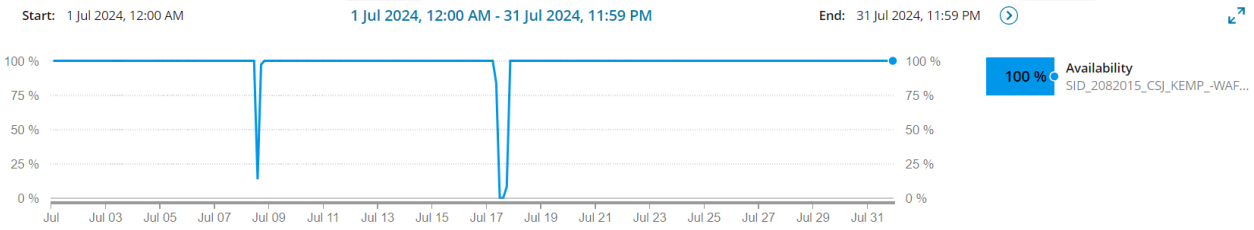
Disk Usage

| | | |
|---|---|---|
| /var/log (24.61 GB) | 0.32 GB (1%) | |
| /var/log/ userlog (886.34 GB) | 782.85 GB (88%) | |

## 15. TRÁFICO DE WEB APPLICATION FIREWALL (WAF) CAN

### a. Disponibilidad WAF CAN.

Durante julio se obtuvo 100 % de disponibilidad en el WAF de CAN.




El valor de disponibilidad del 100% que presenta el gráfico lo genera automáticamente la herramienta de monitoreo, quien de los resultados diarios del mes calcula la media mensual de disponibilidad y redondea al valor del 100%.

Los eventos del pasado 8 y 17 de julio se deben a una novedad en el sistema de monitoreo que no afecto los servicios que IFX Networks presta a la rama judicial, relacionados con los tickets TT862004 y TT866155.

**Availability Statistics**

| PERIOD | AVAILABILITY |
|---|---|
| Today | 100.000 % |
| Yesterday | 100.000 % |
| Last 7 Days | 100.000 % |
| Last 30 Days | 98.345 % |
| This Month | 100.000 % |
| Last Month | 98.378 % |
| This Year | 99.048 % |

### b. Uso de políticas de servidores WAF CAN.

La aplicación más consultada durante julio fue cortesuprema.gov.co_Palacio con un 73% del total:

| # | Name | Virtual IP Address | Total Conns | % del total |
|---|---|---|---|---|
| **1** | cortesuprema.gov.co_Palacio | 172.17.202.239:443 | 8646321 | 73% |
| **2** | sso.cortesuprema.gov.co | 172.17.202.141:443 | 469701 | 4% |
| **3** | samairj.consejodeestado.gov.co | 172.17.202.38:443 | 339180 | 3% |
| **4** | relatoria.cndj.gov.co | 172.17.202.66:443 | 338516 | 3% |
| **5** | sso.cortesuprema.gov.co Redirect | 172.17.202.141:80 | 295320 | 2% |
| **6** | cortesuprema_Palacio Redirect | 172.17.202.239:80 | 275182 | 2% |
| **7** | restituciontierras.ramajudicial.gov.co | 172.17.202.37:443 | 252378 | 2% |
| **8** | convocatorias.consejodeestado.gov.co | 172.17.202.147:443 | 227192 | 2% |
| **9** | linkce.consejodeestado.gov.co | 172.17.202.42:443 | 151295 | 1% |
| **10** | capacitacion.ramajudicial.gov.co 443 | 172.17.202.13:443 | 115120 | 1% |
| | Otras aplicaciones | | 731781 | 6% |
| | Total | | 11841986 | 100% |

### c. Top de peticiones por país WAF CAN.

El país desde donde más se reciben peticiones de conexión es Estados Unidos:

Total

| Country | Requests | Blocked |
|---|---|---|
| United States | 4345924 | 162506 |
| IPrep | 4604 | 4604 |
| Germany | 24987 | 3916 |
| China | 14507 | 1233 |
| Private | 1066278 | 908 |
| Singapore | 19858 | 898 |
| Hong Kong | 3206 | 539 |
| United Kingdom | 7140 | 381 |
| Russia | 32863 | 338 |
| Malaysia | 1061 | 333 |

### d. Top de ataques por política WAF CAN.

La siguiente tabla muestra el top 10 de las reglas o virtual services que proporcionaron mayor protección contra ataques a las aplicaciones web durante julio. Sobre la aplicación cortesuprema.gov.co_Palacio ha sido prevenida la mayor cantidad de ataques durante julio:

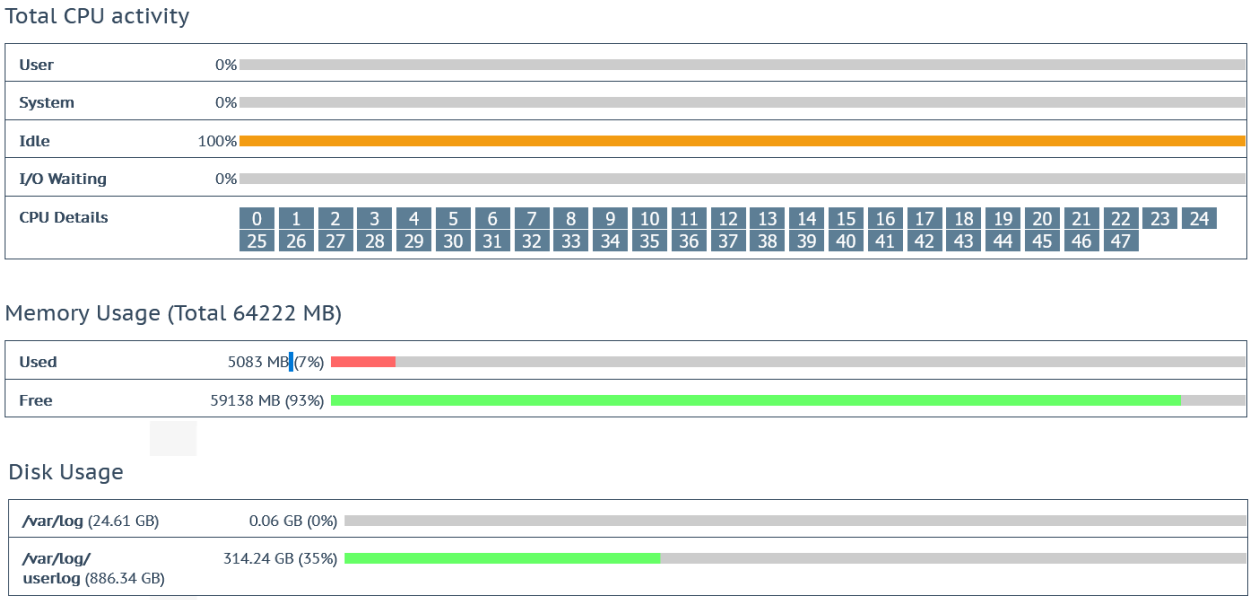
| # | Name | Virtual IP Address | Total Events | % del total |
|---|---|---|---|---|
| 1 | cortesuprema.gov.co_Palacio | 172.17.202.239:443 | 85323580 | 87% |
| 2 | sso.cortesuprema.gov.co | 172.17.202.141:443 | 3293013 | 3% |
| 3 | restituciontierras.ramajudicial.gov.co | 172.17.202.37:443 | 2138993 | 2% |
| 4 | linkce.consejodeestado.gov.co | 172.17.202.42:443 | 1348992 | 1% |
| 5 | convocatorias.consejodeestado.gov.co | 172.17.202.147:443 | 1028518 | 1% |
| 6 | capacitacion.ramajudicial.gov.co 443 | 172.17.202.13:443 | 940219 | 1% |
| 7 | siapoas.ramajudicial.gov.co | 172.17.202.43:443 | 864887 | 1% |
| 8 | samairj.consejodeestado.gov.co | 172.17.202.38:443 | 678567 | 1% |
| 9 | sigobius.consejodeestado.gov.co_443 | 172.17.202.29:443 | 422603 | 0% |
| 10 | efipruebas2.ramajudicial.gov.co | 172.17.202.150:443 | 421107 | 0% |

| | | | | |
|---|---|---|---|---|
| | Otras aplicaciones | | 2083988 | 2% |
| | Total | | 98544467 | 100% |

NOTA: Los dispositivos Kemp X.25 no suministran en sus estadísticas mensuales información detallada acerca de picos de consumo, horarios específicos ni los tipos de ataques dirigidos hacia las aplicaciones web.

### e. Consumo de recursos WAF CAN.

El WAF KEMP del CAN presentó consumo de CPU del 0%, memoria de 7% y disco en un 35%.



### f. Certificado wildcard Rama Judicial *.ramajudicial.gov.co

Este certificado tiene vigencia hasta el 25 de JULIO de 2025, como se puede observar en la siguiente imagen:


Otros certificados digitales presentan las siguientes vigencias:

*.consejodeestado.gov.co
[Expires: Oct 5 23:59:59 2024 GMT]

*.corteconstitucional.gov.c
[Expires: Sep 30 23:59:59 2024 GMT]

*.cortesuprema.gov.co
[Expires: Oct 2 23:59:59 2024 GMT]

Estos certificados se encuentran instalados en los siguientes dispositivos para cifrar el tráfico hacia las aplicaciones.

| N° | Descripción | Hostname | Ubicación | Versión Firmware |
|---|---|---|---|---|
| 1 | **FortiGate-4400F HA** | FTG_CSJ_DC_TC_MASTER | DC IFX | V7.0.14 |
| | | FTG_CSJ_DC_TC_SLAVE | DC IFX | v6.4.11 |
| 2 | **FORTIADC** | FADC_CSJ_TC_MASTER | DC IFX | v6.1.3 |
| | | FADC_CSJ_TC_ SLAVE | DC IFX | v6.1.3 |
| 3 | **FortiGate 900G HA** | FGT_CSJ_PALACIO_M | PALACIO | V7.2.6 |
| | | FGT_CSJ_PALACIO_S | PALACIO | V7.2.6 |
| 4 | **KEMP Loadmaster x25 HA** | WAF_TORRRE_CENTRAL_MASTER | DC IFX | V7.2.59.3.22368 |
| | | WAF_TORRRE_CENTRAL_SLAVE | DC IFX | V7.2.59.3.22368 |
| 6 | **KEMP Loadmaster x25** | WAF_CAN | DC CAN | V7.2.59.3.22368 |

### g. Intentos login fallidos a Firewalls

Durante julio se presentaron 8 intentos de login administrativo hacia los firewall perimetrales. El acceso administrativo se encuentra protegido controles de "Restrict login to trusted hosts":

Top 100 Failed Admin Logins

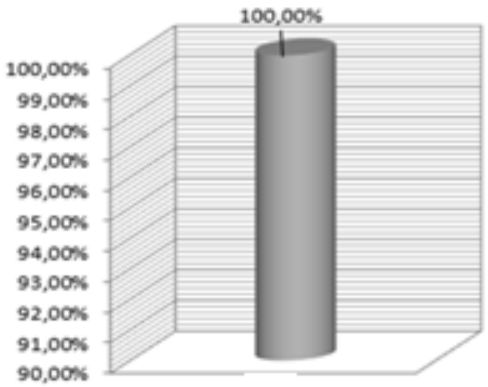
| # | Login Source | User Name | Total Number of Failed Logins |
|---|---|---|---|
| 1 | https(172.25.11.41) | Unknown | 7 |
| 2 | https(172.25.11.41) | ut.dfbanguero.50 | 4 |
| 3 | https(172.16.226.32) | jose.cardenas | 3 |
| 4 | ssh(200.91.237.26) | jccalvo | 2 |
| 5 | ssh(186.102.104.166) | jccalvo | 1 |
| 6 | https(10.101.250.4) | victor.galvis | 1 |
| 7 | https(172.25.11.41) | dfernanp | 1 |
| 8 | https(10.0.0.62) | jccalvo | 1 |

Nota: Se han descartado los intentos de acceso fallidos de los 3 ingenieros residentes al validarse que se trató de errores al introducir la contraseña o el token.

## 16. DISPONIBILIDAD SEGURIDAD GLOBAL DEL MES DE JULIO

| DISPONIBILIDAD GLOBAL | NUMERO DE TICKETS POR IMPUTABILIDAD | |
|---|---|---|
| | RESPONSABILIDAD IFX (NUMERO TICKETS) | RESPONSABILIDAD CLIENTE (NUMERO TICKETS) |
| 100.00% | 0 | 0 |

| MES | DISPONIBILIDAD (%) |
|---|---|
| JULIO | 100% |



### a. Anexo de las solicitudes e incidentes de seguridad reportadas.

Se adjunta documento "Anexo CSJ-Consolidado casos JULIO 2024.xlsx", con los casos presentados y cerrados durante el mes.

## 17. CONSUMO MOTORES BASES DE DATOS

A continuación, se desglosas los motores bases de datos contratados bajo acuerdo marco:

- CPU
- Memoria RAM
- Disco

(Remitirse al documento "**Anexo consumo motores base de datos**" para ver el detalle)

## 18. GESTIÓN FINANCIERA

### *19.1 Tabla información Gestión financiera*

| | |
|---|---|
| **Fecha de inicio** | 5-feb-24 |
| **Fecha de finalización** | 4-dic-24 |
| **Valor inicial** | $ 15.516.011.530,00 |
| **Plazo** | 10 meses |
| **Items de la Orden de Compra** | 49 lineas - SID |
| **AMP** | Nube Privada IV - CEE-308- AMP-2022- # Proceso CCENEG-061-1-2022 |
| **Valor facturado a la fecha** | $ 7.407.024.856,47 |
| **% Valor facturado** | 47,74% |
| **Valor pagado a la fecha** | $ 7.407.024.856,47 |
| **% Valor pagado** | 47,74% |

### *19.2 Tabla Facturación*

| FACTURA | FECHA EMISIÓN | VALOR (IVA incluido) | PERIODO FACTURADO | FECHA DE PAGO | ESTADO |
|---|---|---|---|---|---|
| IFXC-402862 | miércoles, 3 de abril de 2024 | $ 1.318.151.327,59 | 05 al 29 de Febrero 2024 | jueves, 18 de abril de 2024 | Pagada |
| IFXC-403030 | viernes, 19 de abril de 2024 | $ 1.530.871.522,52 | 01 al 31 de Marzo 2024 | lunes, 6 de mayo de 2024 | Pagada |

| | | | | | |
|---|---|---|---|---|---|
| IFXC-405204 | martes, 28 de mayo de 2024 | $ 1.510.877.833,00 | 01 al 30 de Abril 2024 | miércoles, 5 de junio de 2024 | Pagada |
| IFXC-407246 | martes, 18 de junio de 2024 | $ 1.520.031.300,36 | 01 al 31 de Mayo 2024 | jueves, 27 de junio de 2024 | Pagada |
| IFXC-409336 | martes, 16 de julio de 2024 | $ 1.527.092.873,00 | 01 al 30 de Junio 2024 | lunes, 29 de julio de 2024 | Pagada |

## *19.3 Tabla ANS*

| ANS (sin IVA incluido) | |
|---|---|
| 05 al 29 de Febrero 2024 | No se generaron ANS durante el periodo |
| 01 al 31 de Marzo 2024 | $ 6.034.935,00 |
| 01 al 30 de Abril 2024 | $ 9.379.680,00 |
| 01 al 31 de Mayo 2024 | No se generaron ANS durante el periodo |
| 01 al 30 de Junio 2024 | $ 1.703.940,00 |
| **Total ANS** | **$ 17.118.555,00** |

## 19. RECOMENDACIONES

- Depurar las políticas y objetos que no se estén usando en los dispositivos de seguridad. Esta depuración se debe revisar en conjunto con los ingenieros del CSJ para determinar si las políticas y estos objetos y políticas no se van a volver a utilizar.

- Revisar los hosts como más peticiones bloqueadas para descartar que tengan instalado algún programa maligno intentando hacer estas conexiones a sitios de Botnet, C&C (comando y control) y/o a cualquier otro destino malicioso.

- Depurar los usuarios de las VPN locales que ya no se encuentran en uso y continuar la migración de los usuarios locales aún en uso hacia el directorio activo unificado.

- Coordinar con los administradores de las aplicaciones web que se encuentran protegidas por el WAF unas reuniones de trabajo para validar los perfiles de protección aplicados y determinar si es necesario un nuevo afinamiento de estos.

- Depurar las políticas del FortiADC que no registraron tráfico durante el mes ya que posiblemente sean de aplicaciones que no están utilizan el balanceador. Esta depuración se debe revisar en conjunto con los ingenieros del CSJ para determinar si las políticas y estos objetos y políticas no se van a volver a utilizar.