REPORTE MENSUAL

RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA

OC124016

AGOSTO 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** Período del informe: mensual Fecha de inicio: 1 de AGOSTO de 2024 Fecha de final: 31 de AGOSTO 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	Balanceador DC Torre central	FORTI/BK	ADC-2200F	SN: FAD22FT221000027	9	32

		64GB y128GB - U_Mes - Cantidad: 2						
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: FG9H0G TB2390 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: FG9H0G TB2390 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: 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

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 AGOSTO de 2024 es de: **3840906(GB)**

El almacenamiento total presentado adicional es de: **3717695 (GB)**

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

A corte 30 de AGOSTO 2024 la entidad cuenta con un almacenamiento disponible de 12305(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_AGOSTO_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 31 de Agosto, está utilizando, una capacidad de 948200 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 483200 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 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 499600 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 233200 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	ESPACIO LIBRE	ESPACIO USADO
UNIDAD 1	80 TB	871,1 GB	183,6 TB
UNIDAD 2	80 TB	11,3 TB	248,8 TB
UNIDAD 3	78,2 TB	16,6 TB	168,9 TB
UNIDAD 4	110 TB	8,4 TB	420,8 TB

MENSUALES			
REPOSITORIOS	CAPACIDAD	ESPACIO LIBRE	ESPACIO USADO
UNIDAD 1	90 TB	8,5 TB	178,5 TB
UNIDAD 2	90 TB	6,1 TB	156,2 TB
UNIDAD 3	90 TB	10,9 MB	93,2 TB
UNIDAD 4	90 TB	6,3 TB	94,2 TB
UNIDAD 5	100 TB	39,5 TB	94,1 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_AGOSTO_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 AGOSTO 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_AGOSTO_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

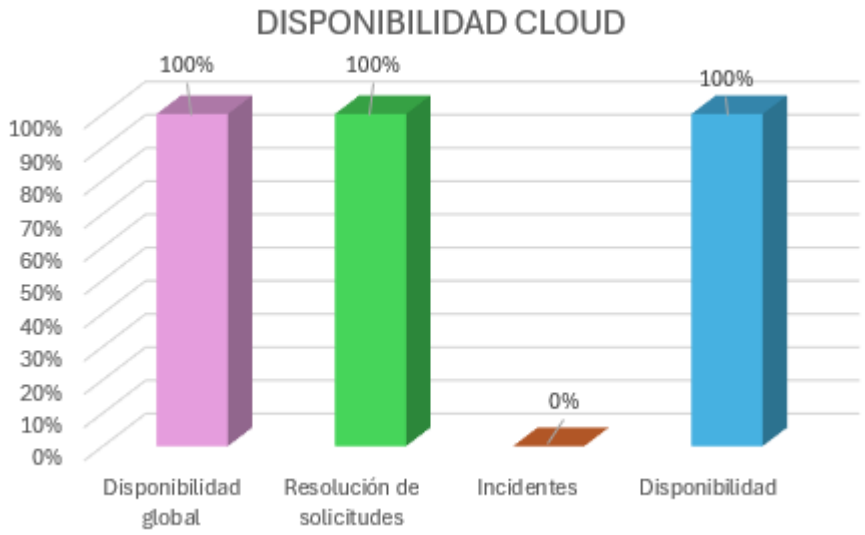
- **Insightappsec scan:** línea OC 25
- **Isigthwm scan:** línea OC 26
- **Ivanti:** Líneas de OC 17,18,20,21,22,28,38 y 42
- **Jurisprudencia ADA:** Líneas de OC 17,20,21 y 22
- **JXXIWeb:** Líneas de OC 24,25 y 38
- **Kactus:** Líneas de OC 24,25 y 38
- **MV Seccionales:** Línea de OC 15
- **PIBOT_ASURE:** 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_AGOSTO_2024.xls**" para ver el detalle "maquinas")

7.DISPONIBILIDAD GLOBAL CLOUD DEL MES DE AGOSTO

Disponibilidad Global mes de AGOSTO	Numero de tickets mes de AGOSTO	Imputabilidad por ANS
	77 solicitudes	**0 solicitudes**
	0 incidentes	**0 incidentes**
100%	Total 77 tickets	0 tickets



CONTROL DOCUMENTAL

ELABORADO POR

Fecha	Autor	Ingeniero
03-09-2024	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 agosto a31 de agosto del 2024.

CONSUMO TOTAL HORAS MES DE AGOSTO	
• Casos Reportados Netsuite	98
Sesiones de Seguimiento	7
Sesiones de Trabajo	0
Casos Escalados Medio Digital - Whatsapp	19
Horas Disponibilidad del Recurso Fines de Semana	276
Total Horas Consumidas de las 300 - Experto Master	400

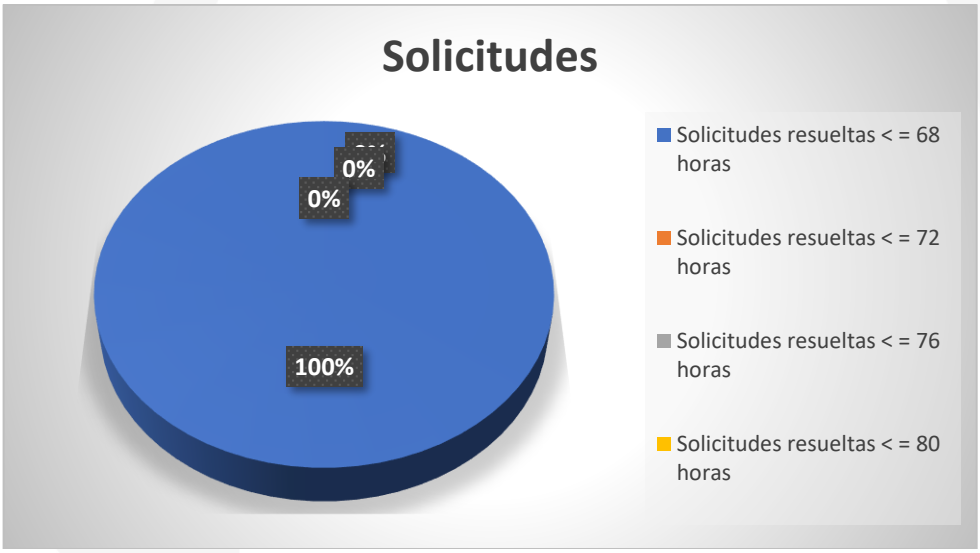
2.INDICADORES DEL CENTRO CONSOLIDADO DE SERVICIOS

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 agosto, para el Consejo Superior de la Judicatura. Estas mediciones se basan en el número de casos reportados por la aplicación.

	Volumen en 1 agosto a
Casos Reportados	21
Solicitudes	20
Incidencias	1
WA – AF	0

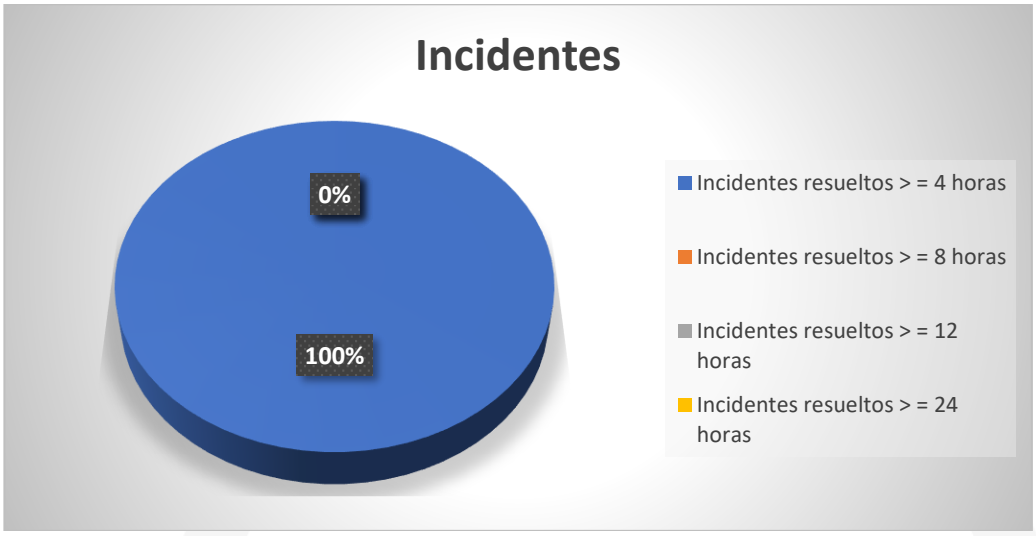
2.1 TASA DE RESOLUCIÓN DE PROBLEMAS

Tiempo de Gestión	Solicitudes
Solicitudes resueltas < = 68 horas	20
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	**20**



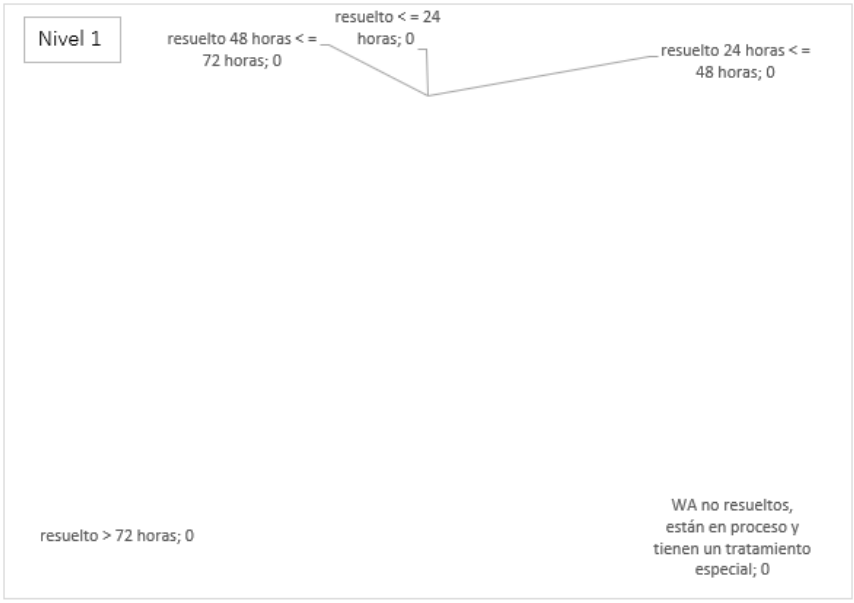
Tiempo de Gestión	Incidentes Penalizados
Incidentes resueltos < = 4 horas	1
Incidentes resueltos < = 8 horas	0
Incidentes resueltos <= 12 horas	0
Incidentes No resueltos < 24 horas	0
Total	**0**

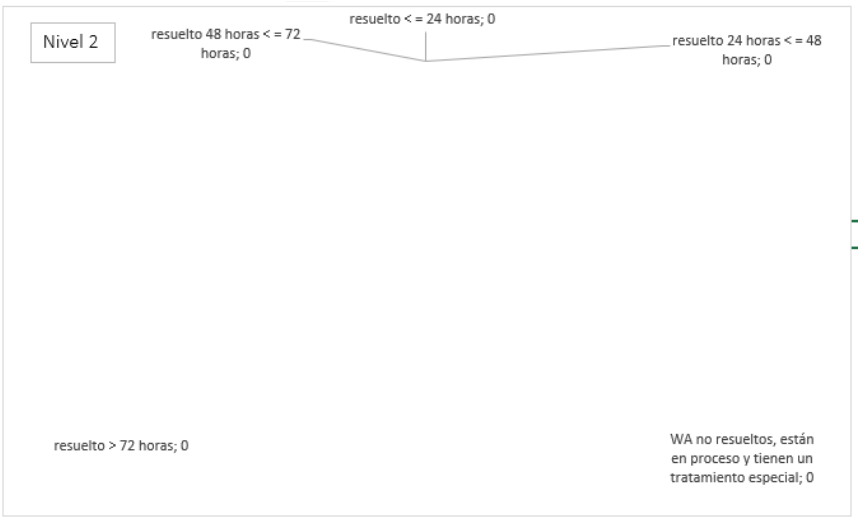
Ticket Penalizado: TT883048

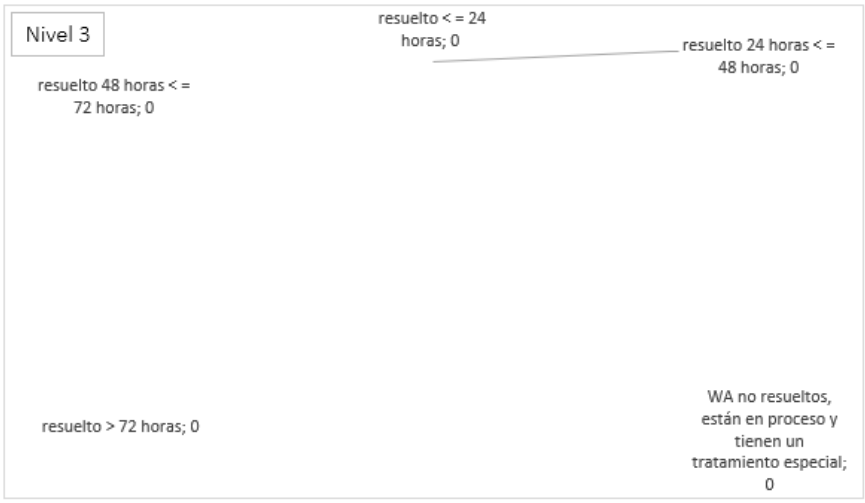


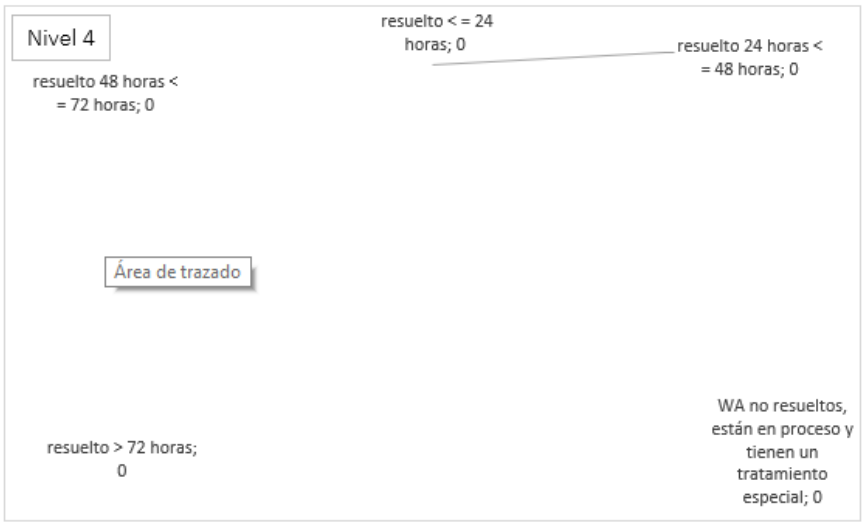
RV: Reporte de falla e inconsistencia en la página y usuario de la página Web de la Comisión Nacional de Género

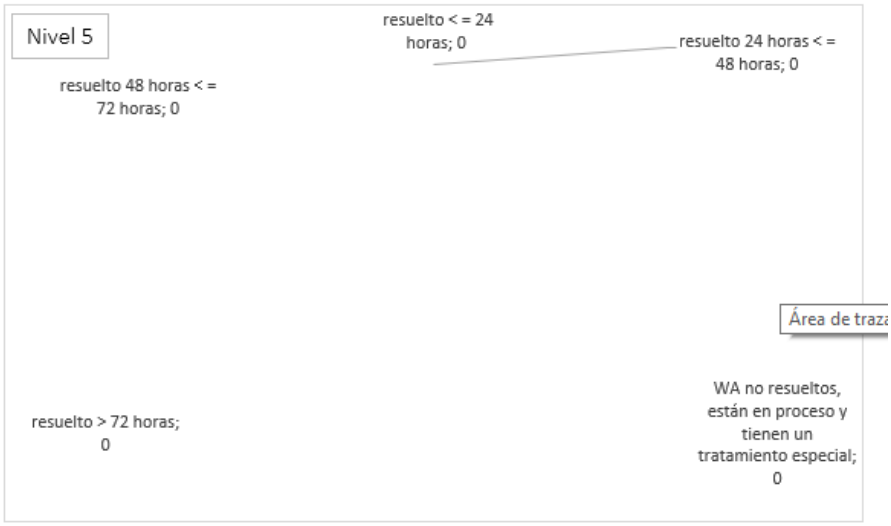
WA (Ajustes Funcionales)					
Tiempo de Gestión	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
resuelto < = 24 horas	0	0	0	0	0
resuelto 24 horas < = 48 horas	0	0	0	0	0
resuelto 48 horas < = 68 horas	0	0	0	0	0
resuelto > 68 horas	0	0	0	0	0
WA no resueltos, están en proceso y tienen un tratamiento especial	0	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 agosto a 31 de agosto 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&mobile

redirect=true" los cuales contienen la información detallada de cada uno desde el 1 de agosto a 31 de agosto 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 agosto 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	124	400	276
⊟2024	124		
⊞Solicitud	123		
⊞Incidencia	1		
Total Horas Casos Reportados Netsuite	124	400	276
		276	276
		276	276
		276	276
		276	276
Horas consumidasde las 400 - Exp	400	400	0

No se reportaron casos relacionados con WA – MF para este mes de agosto 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

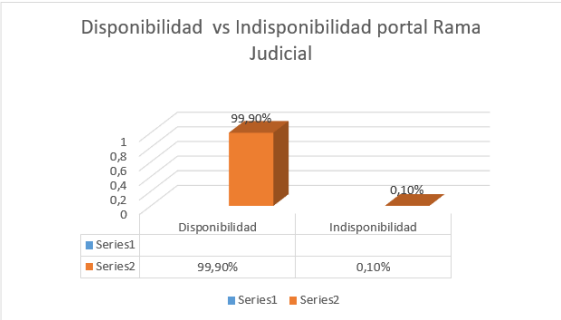
3. *DISPONIBILIDAD E INDISPONIBILIDAD DE LOS SERVICIOS DE HOSTING*

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:

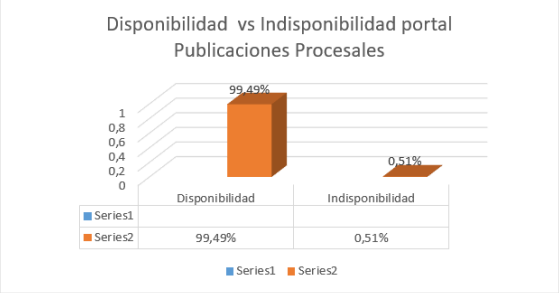
Portal Rama Judicial

Item	Aplicación	Disponibilidad	Indisponibilidad	Tiempo de duracion (Caida en horas)	Tiempo de duracion			
					Dias	Horas	Minutos	Segundos
1	Portal de la Rama Judicial	99,90%	0,10%	0,736111111	0	0	44	10
	Totales	99,90%	0,10%	0,736111111	**0**	0	44	10



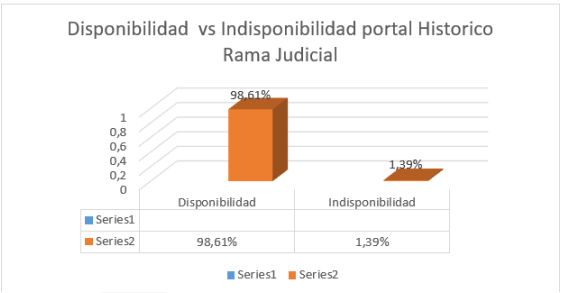
Portal Publicaciones Procesales

Item	Aplicación	Disponibilidad	Indisponibilidad	Tiempo de duracion (Caida en horas)	Tiempo de duracion			
					Dias	Horas	Minutos	Segundos
1	Publicaciones Procesales	99,49%	0,51%	3,793888889	0	3	47	38
	Totales	99,49%	0,51%	3,793888889	**0**	3	47	38



Portal Histórico Rama Judicial

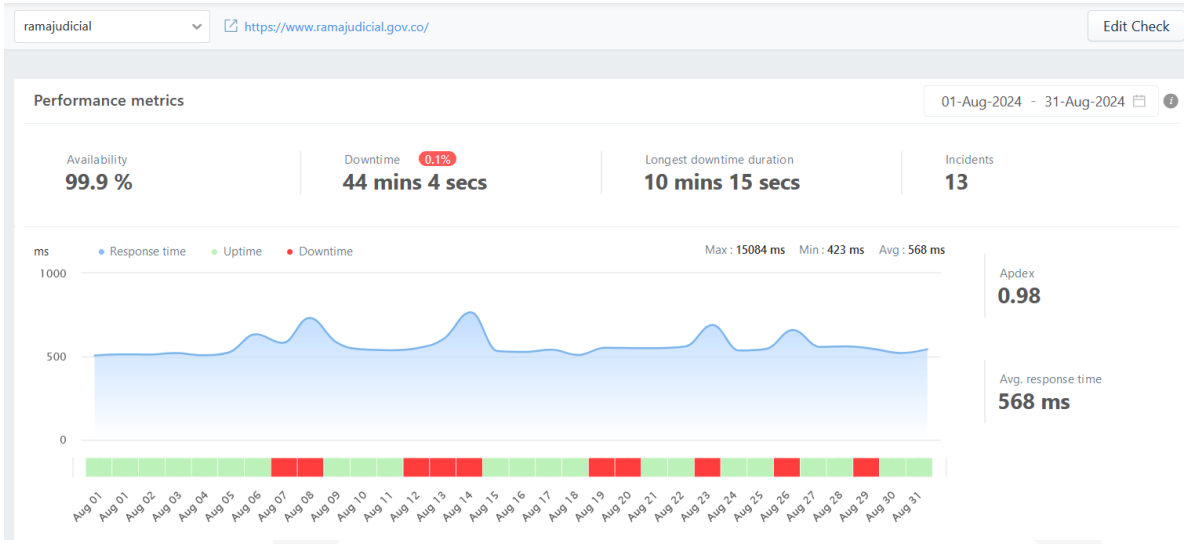
Item	Aplicación	Disponibilidad	Indisponibilidad	Tiempo de duracion (Caida en horas)	Tiempo de duracion			
					Dias	Horas	Minutos	Segundos
1	Portal Historico	98,61%	1,39%	10,35166667	0	10	21	6
	Totales	98,61%	1,39%	10,35166667	**0**	10	21	6



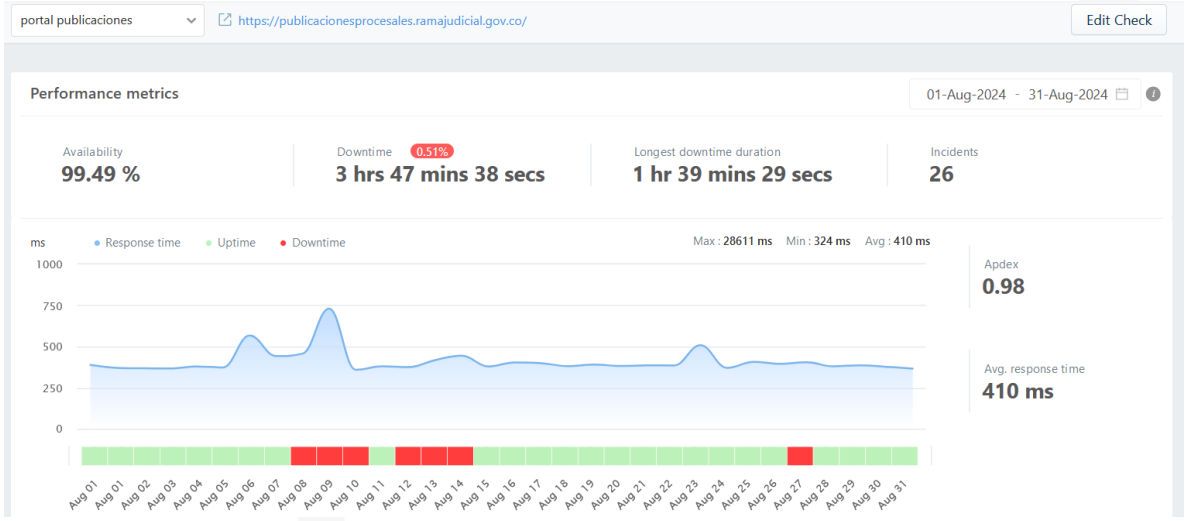
3.2 PORTAL DE LA RAMA JUDICIAL

Grafica de la información consolidada de disponibilidad e indisponibilidad del portal del mes de agosto

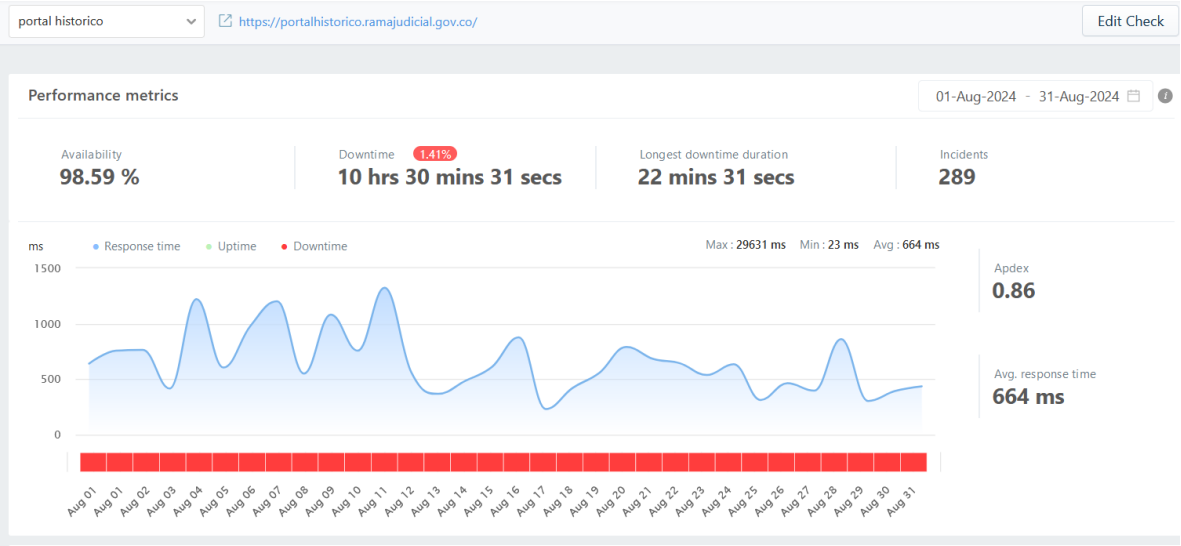
Portal Rama Judicial



Portal Publicaciones Procesales



Portal Histórico Rama Judicial



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

No se ejecutaron actividades

3.2.2 CRECIMIENTO DE LA BASE DE DATOS – INSTANCIA CSJPORTALDB01

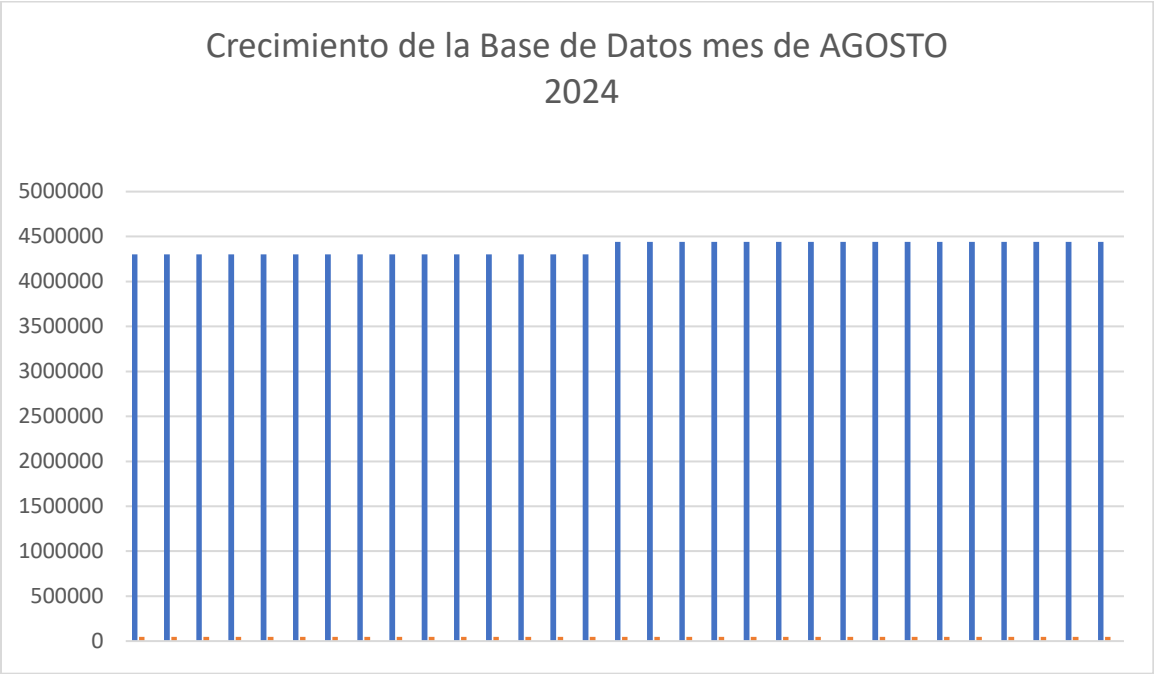
De acuerdo con la solicitud escalada en el **caso TT520553 RV: Crecimiento de la BD de la maquina CSJPORTALDB01** del portal de rama judicial, se agrega el presente informe consolidado del crecimiento que tuvo la BD en el mes de agosto.

BASE DE DATOS lportalramaprod

TAMAÑO (MB0	FECHA	AUMENTO TAMAÑO (MB) POR DIA
4302432 MB	2024-08-01 00:00:00.437	0
4302432 MB	2024-08-02 00:00:00.303	0
4302432 MB	2024-08-03 00:00:00.320	0
4302432 MB	2024-08-04 00:00:00.407	0
4302432 MB	2024-08-05 00:00:00.477	0
4302432 MB	2024-08-06 00:00:00.877	0

4302432 MB	2024-08-07 00:00:00.447	0
4302432 MB	2024-08-08 00:00:01.060	0
4302432 MB	2024-08-09 00:00:00.250	0
4302432 MB	2024-08-10 00:00:00.257	0
4302432 MB	2024-08-11 00:00:00.587	0
4302432 MB	2024-08-12 00:00:01.087	0
4302432 MB	2024-08-13 00:00:01.103	0
4302432 MB	2024-08-14 00:00:00.737	0
4302432 MB	2024-08-15 00:00:00.177	0
4440187 MB	2024-08-16 00:00:00.673	137755
4440187 MB	2024-08-17 00:00:00.820	0
4440187 MB	2024-08-18 00:00:00.587	0
4440187 MB	2024-08-19 00:00:00.490	0
4440187 MB	2024-08-20 00:00:00.567	0
4440187 MB	2024-08-21 00:00:00.810	0
4440187 MB	2024-08-22 00:00:00.503	0
4440187 MB	2024-08-23 00:00:01.113	0
4440187 MB	2024-08-24 00:00:00.747	0
4440187 MB	2024-08-25 00:00:01.097	0
4440187 MB	2024-08-26 00:00:00.567	0
4440187 MB	2024-08-27 00:00:00.227	0
4440187 MB	2024-08-28 00:00:00.243	0
4440187 MB	2024-08-29 00:00:00.547	0
4440187 MB	2024-08-30 00:00:00.647	0
4440187 MB	2024-08-31 00:00:00.583	0

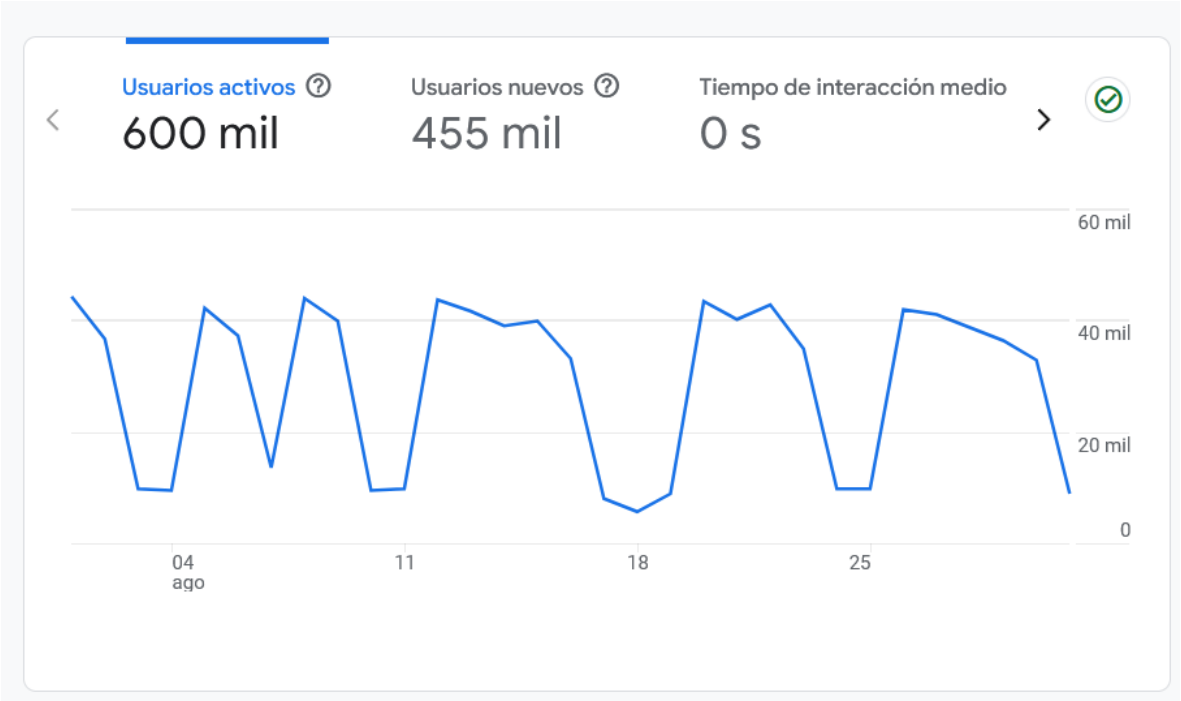
Grafica del crecimiento de la BD Iportalramaprod de la INSTANCIA CSJPORTALB01



*4. **ESTADISTICAS PORTAL DE LA RAMA JUDICIAL***

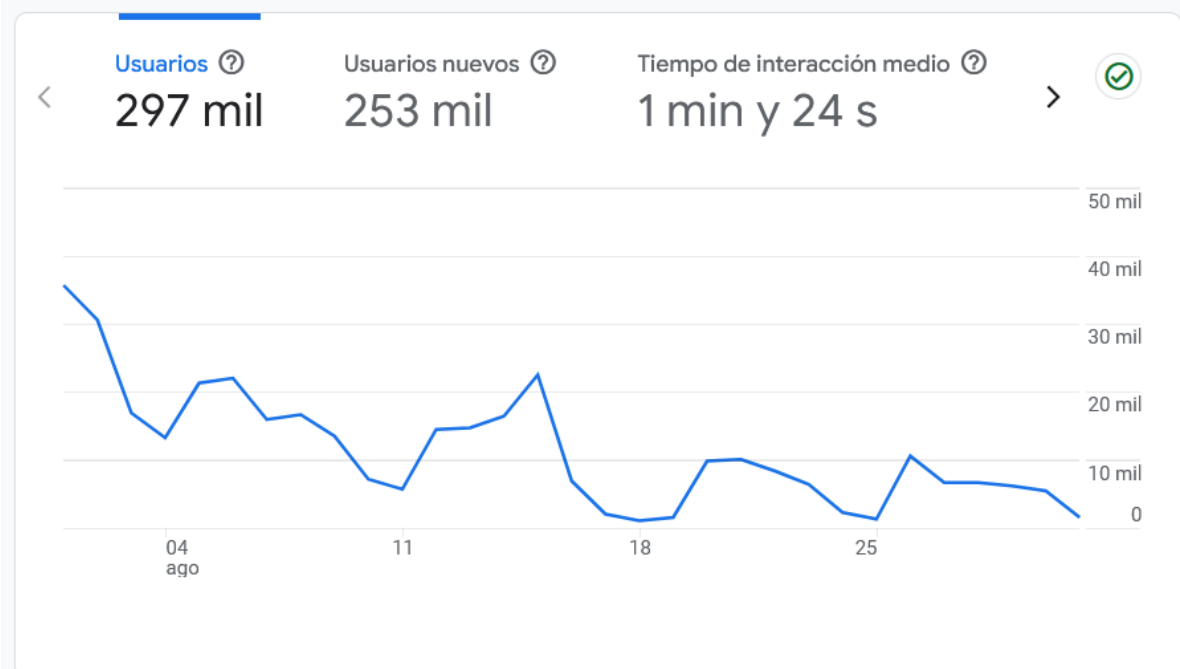
4.1 RESUMEN DEL PORTAL

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



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

En la respectiva grafica se observa un comportamiento constante durante el mes de agosto 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: FAD22FT221000028	10	32
11	2081818	npn04--IaaS Procesamiento -Balanceador de Carga AltaCapacidad - Oro - HostingNube Privada - SesionesCapa L4 (entre 36 y 100Millones) - RAM entre	Balanceador DC Torre central	FORTI/BK	ADC-2200F	SN: FAD22FT221000027	9	32

		64GB y128GB - U_Mes - Cantidad: 2						
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					

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	8/3/2024 15:25	8/3/2024 15:56	1	Diurna	TT874833 RV: Solicitud Permisos SIRNA AZURE - Salida de Correos; VENTANA MANTENIMIENTO PASO SIRNA - AZURE
2	8/3/2024 17:13	8/3/2024 18:24	1	Diurna	VENTANA MANTENIMIENTO PASO SIRNA - AZURE
3	8/9/2024 21:00	8/9/2024 21:19	1	Diurna	TT877388 RV: Ampliar política de Seguridad
4	8/30/2024 18:00	8/30/2024 18:36	1	Diurna	VENTANA: Implementación nuevo aplicativo de agendamiento de audiencias judiciales y portal de grabaciones de audiencias | TT887518 RV: Pruebas de envío de tutelas a la Corte Constitucional | TT887517 RV: Pruebas de envío de tutelas a la Corte Constitucional
5	8/30/2024 19:10	8/30/2024 19:59	1	Diurna	TT887541 RV: Reporte de posible compromiso de cuentas de correo institucional | TT887553 RV: Solicitud de apertura Redes sociales 2 al 6 de septiembre
Total horas Extras			5		

Ingeniero Residente:	Jose Luis Cardenas

Item	Fecha y Hora de inicio	Fecha y Hora de finalización	Cantidad de Horas	Tipo de Hora extra	Actividad Realizada
1	8/23/2024 21:00	8/24/2024 1:00	4	Nocturno	Reinicio HUB SDWAN MERAKI
2	8/24/2024 6:00	8/25/2024 11:00	10	Diurna/Nocturno	TT883531 Acompañamiento ventana apagado FW Palacio Justicia manos remotas
3	8/25/2024 16:57	8/25/2024 17:57	1	Diurna	TT884361 Indisponibilidad servidor 192.168.209.32
4	8/27/2024 18:00	8/27/2024 19:00	1	Nocturno	Requerimientos para Ejecución de Estrategia de Transferencia de archivos superiores a 5 TB
5	8/28/2024 18:12	8/28/2024 19:12	1	Nocturno	TT886279 RV: Permiso de Conectividad Equipo Palacio-IFX RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA
6	8/28/2024 18:10	8/28/2024 19:15	1	Nocturno	TT886277 RV: Solicitud Subdominio - Ip RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA
Total horas Extras			18		

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	8/17/2024 12:00	8/17/2024 13:00	1	Diurna	
2	8/22/2024 0:00	8/22/2024 2:00	2	Nocturno	
3					
Total horas Extras			3		

14.1. Inventario de equipos de seguridad perimetral.

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

#	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

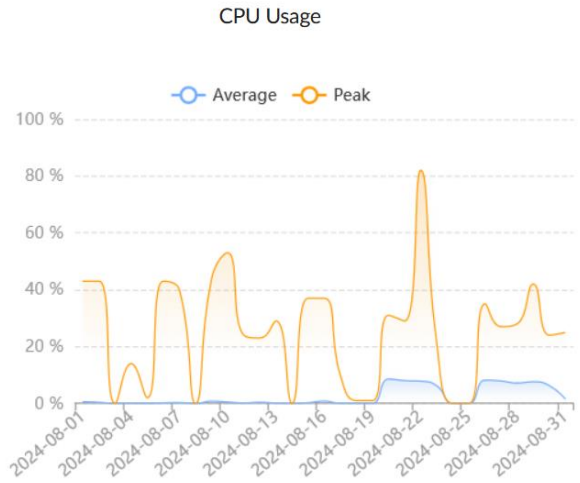
14.2. Actualización de firmware.

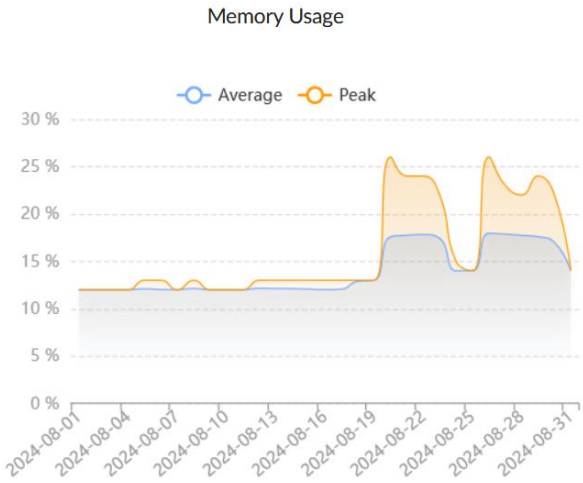
El plan de trabajo para la actualización del firmware será compartido, presentado y ejecutado con la autorización de los ingenieros Datacenter del CONSEJO SUPERIOR DE LA JUDICATURA.

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

15. FIREWALL PERIMETRAL

Durante agosto, el consumo promedio de CPU y memoria (traza azul) en el firewall perimetral estuvieron dentro de sus valores de operación normal.

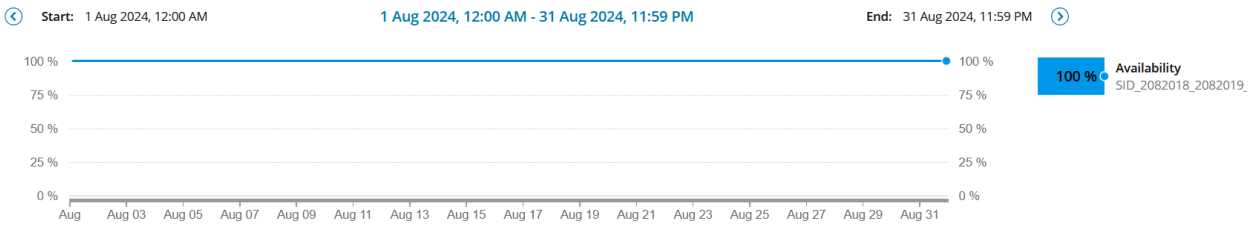




En la gráfica de rendimiento "CPU Usage", la curva color naranja muestra los picos de consumo de una o varias de las 160 CPUs del appliance FortiGate-4400F, cuando estos picos ocurren las tareas que generan estos picos son desbordadas a las otras CPUs por lo que la curva color azul se muestra el promedio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

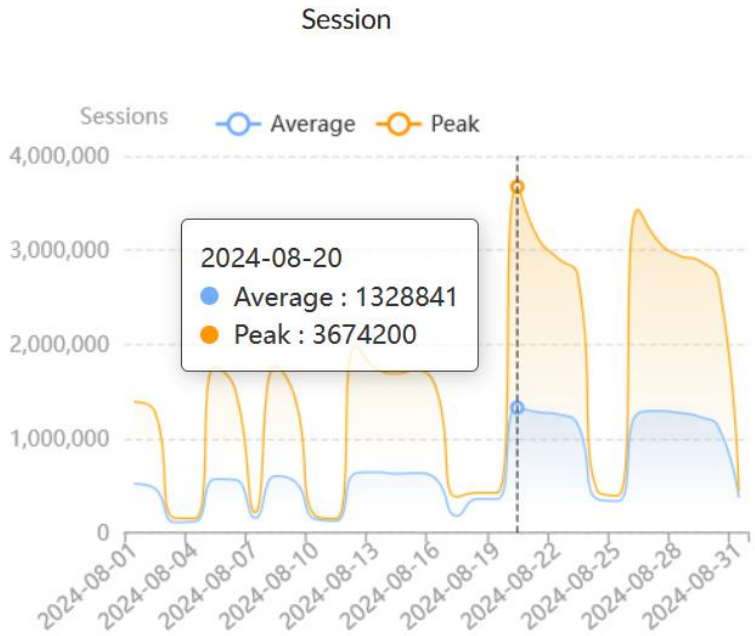
15.1. Disponibilidad mensual firewall perimetral.

Durante agosto se obtuvo 100% de disponibilidad en el firewall perimetral.



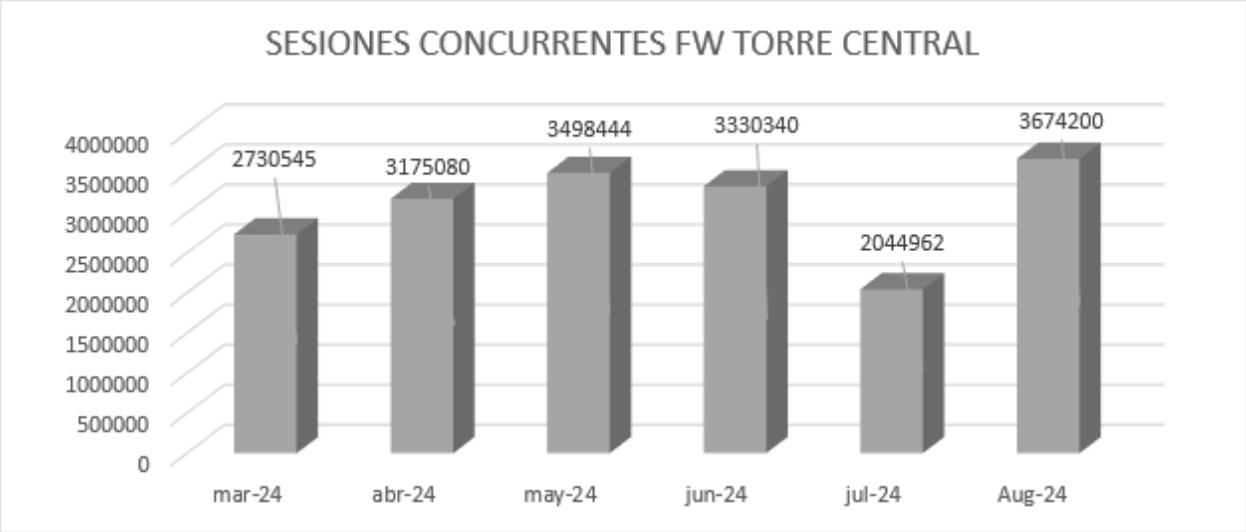
15.2. Cantidad de sesiones firewall perimetral.

Durante agosto se presentó un máximo de 3674200 sesiones TCP concurrentes, cantidad que se encuentra dentro del rango máximo soportado por el appliance Fortinet FG- 4400F cuyo valor es de 210 millones.



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

Durante agosto se presentó un incremento en las sesiones en el FW perimetral correspondientes a 3674200 sesiones:



MES	SESIONES
mar-24	2730545
abr-24	3175080
may-24	3498444
jun-24	3330340
jul-24	2044962
Aug-24	3674200

15.4. Aplicaciones y protocolos por ancho de banda firewall perimetral.

Amazon AWS, HTTPS y Microsoft.SharePoint fue la aplicación con mayor consumo de ancho de banda durante agosto:

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	Amazon-AWS			93.77 TB
2	HTTPS			93.46 TB
3	Microsoft.SharePoint			78.27 TB
4	SSL			47.79 TB
5	Microsoft.365.Portal			30.99 TB
6	Microsoft.Teams			25.02 TB
7	Microsoft.Portal			24.63 TB
8	OneDrive			21.94 TB
9	Microsoft.Outlook			18.51 TB
10	WhatsApp			17.96 TB

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

Top Applications by Sessions

#	Application	Sessions
1	SMB	1,986,518,889
2	DNS	1,565,039,118
3	HTTPS	1,498,679,479
4	Microsoft.Windows.Update	792,873,326
5	TCP/UDP_8037	628,950,053
6	Microsoft.365.Portal	622,784,953
7	SSL	580,252,698
8	Microsoft.Portal	578,367,600
9	TCP/5508	416,843,701
10	ESET-Eset.Service	412,736,060

15.5. Top de IP por ancho de banda firewall perimetral.

172.31.10.41 (Aplicación Árbol tutela) y 172.16.182.85 (PC de la sede Valle, Cali; Palacio de Justicia) tuvieron la mayor cantidad de consumo de ancho de banda durante el mes de agosto:

Top Bandwidth IP

#	IP	Bandwidth
1	172.31.10.41	6.65 TB
2	172.16.182.85	6.13 TB
3	10.101.100.114	3.47 TB
4	10.101.100.38	2.75 TB
5	10.101.100.182	1.85 TB
6	10.101.100.138	1.14 TB
7	10.101.102.6	1.04 TB
8	10.101.100.122	1,011.79 GB
9	10.101.100.82	990.58 GB
10	172.29.175.46	988.87 GB

15.6. Top de destinos web por sesiones firewall perimetral.

Los destinos en Internet con mayor cantidad de sesiones durante agosto fueron 8.243.164.19 y 8.243.164.21 (CTL Colombia).

Top Destinations by Sessions

#	Hostname(or IP)	Sessions
1	8.243.164.19	528,890,995
2	172.28.107.71	362,420,229
3	8.243.164.21	342,037,679
4	172.28.107.61	316,724,673
5	microsoft.com	302,679,972
6	windowsupdate.com	247,280,201
7	172.28.107.58	233,150,507
8	spotify.com	169,518,340
9	8.243.200.3	105,929,324
10	172.29.130.220	96,716,377

15.7. Top de usuarios con peticiones bloqueadas por el firewall perimetral.

192.168.50.34 de la sede Cundinamarca, Bogotá; Juzgados de Menores, presentó la mayor cantidad de peticiones bloqueadas durante agosto:

Top Web Users by Blocked Requests

#	User (or IP)	Hostname	Requests
1	192.168.50.34	192.168.50.34	19,560,198
2	172.16.33.29	172.16.33.29	6,544,531
3	172.27.91.49	172.27.91.49	5,531,739
4	172.27.179.89	172.27.179.89	5,149,212
5	172.16.156.78	172.16.156.78	4,962,656
6	192.168.46.197	192.168.46.197	4,727,728
7	192.168.199.32	192.168.199.32	4,703,673
8	172.25.110.163	172.25.110.163	4,297,091
9	172.25.13.191	172.25.13.191	4,028,032
10	172.17.98.11	172.17.98.11	3,891,326

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.

15.8. Top de las categorías más bloqueadas por el firewall perimetral.

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

Top Blocked Web Categories

#	Category	Requests
1	Internet Radio and TV	181,649,958
2	Streaming Media and Download	8,085,770
3	Games	6,049,527
4	Social Networking	5,763,382
5	Proxy Avoidance	5,480,490
6	Unrated	3,446,421
7	Entertainment	706,966
8	Malicious Websites	382,208
9	Information Technology	374,645
10	Society and Lifestyles	321,896

15.9. Top de IP más activos Firewall Perimetral

Los hosts con mayor cantidad de peticiones durante agosto 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	10,953,227
2	10.101.100.38	6,929,436
3	10.101.100.34	6,324,709
4	10.101.101.54	4,734,332
5	10.101.100.194	4,628,688
6	10.101.101.50	4,290,666
7	10.101.100.134	4,244,098
8	10.101.102.6	3,878,698
9	10.101.100.70	3,851,290
10	10.101.100.98	3,817,602

15.10. Top de categorías más visitadas Firewall Perimetral

La categoría más visitada durante agosto fue Information Technology:

Top Allowed Web Categories

#	Category	Requests
1	Information Technology	379,330,813
2	Overrride_permitidas	569,960

15.11. Top de consumo ancho de banda por usuario Firewall Perimetral

Las maquinas con IP 172.28.107.80 - TX_400TB-AWS de la nube privada de IFX presentó el mayor consumo de ancho de banda durante agosto:

Top IP by Bandwidth

#	IP	Bandwidth	Sent	Received
1	172.28.107.80		55.78 TB	
2	172.28.107.79		18.66 TB	
3	172.17.201.251		14.97 TB	
4	172.28.107.89		13.30 TB	
5	172.17.201.252		10.38 TB	
6	200.7.97.132		8.83 TB	
7	172.31.10.41		7.70 TB	
8	172.16.182.85		6.15 TB	
9	erubianr		4.04 TB	
10	10.244.2.239		3.91 TB	

16. TRÁFICO VPN FIREWALL PERIMETRAL

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

#	Usuario_VPN	devname	Tipo de conexión	Ultima Conexión	fv_dtime_tz_conv_e_time_t	IPs de origen de la conexión	Cantidad de conexiones	Duración	Consumo	traffic_in	traffic_out
1	Ecoralb	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-08-31 23:56:19	1725148579	186.154.96.194;190.25.107.154	140	669:43:42	15.10 GB	1781844896	14430096623
2	cvillam	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-08-31 23:53:58	1725148438	172.18.136.192;181.55.51.20;186.102.86.37	95	667:11:50	6.22 GB	678052169	600390212
3	pfajardg	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-08-31 17:48:06	1725126486	186.81.100.20	91	440:13:41	17.82 GB	994364469	181407455641
4	ssuareza	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-08-31 23:51:30	1725148290	181.58.39.249;181.58.39.80;186.87.10.8	156	421:57:33	10.02 GB	887296284	9876858982
5	lmarinmo	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-08-30 22:46:33	1725057993	181.136.233.42;181.136.237.173	87	417:49:53	5.70 GB	548327679	5574249871
6	rgutierm	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-08-30 21:23:42	1725053022	179.19.145.29;179.19.58.74;179.19.60.167;179.19.62.250;181.59.148.79;181.59.148.92;181.159.2.91;191.107.27.255;45.238.182.123;45.238.183.182;45.238.182.194;45.238.183.247	89	388:58:37	2.45 GB	229957992	2404189047

7	jariasu	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-08-30 23:16:14	1725059774	181.137.8.129	79	371:10:25	2.27 GB	261624388	2178148451
8	lbarrerf	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-08-31 02:53:12	1725072792	186.154.108.10;186.154.150.5;186.155.107.108;186.155.46.48;191.156.177.139;191.156.177.219;191.156.182.0;191.156.182.194;191.156.183.166;191.156.184.63;191.156.224.76;191.156.228.167;191.156.230.235;191.156.230.47;191.156.234.114;191.156.48.228;191.156.49.68;191.156.58.139;191.156.6.137;191.156.62.169;191.156.63.243;191.156.63.44;200.119.50.236;201.244.129.84	134	370:48:25	35.55 GB	2609590674	35562987564

9	csichaca	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-08-31 23:53:50	1725148430	172.29.100.35;172.29.100.38;181.234.182.48;181.55.70.74;186.102.18.129;186.102.19.225;186.102.24.105;186.102.61.35;186.102.7.224;186.102.7.85;186.102.97.77;186.102.96.0;186.103.11.169;186.103.62.65;186.114.113.55;186.114.116.200;186.114.121.172;186.114.127.104;186.114.96.143;186.114.98.173;186.168.232.185	99	349:19:29	8.00 GB	724885604	786276528
10	cpalacip@cendoj.ramajudicial.gov.co	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-08-31 00:07:15	1725062835	186.155.19.59;186.29.35.144;190.24.57.151	48	307:32:58	89.30 MB	93407458	232838

16.1. VPN IPSEC Site To Site Firewall Perimetral

El consumo de ancho de banda de las VPN IPSec Site to Site durante agosto 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	2677803	25055221614590	2189626553351	22865595061239
2	VPN_ORACLE	129.213.6.36	190.217.80.4	2677599	1823739872536	1773211453472	50528419064
3	VPN_SIUG_AWS	34.194.187.190	190.217.24.4	2676950	762897437463	114818706680	648078730783
4	VPN_SIUG_AWS-2	34.224.152.152	190.217.24.4	2676968	385808499179	177934815422	207873683757
5	VPN_AZURE-ANALY	20.124.34.235	190.217.24.4	2677803	88009469270	6722453251	81287016019
6	VPN_Tierras	181.225.76.196	190.217.24.4	2677666	76723283322	74727022117	1996261205
7	VPN_INPEC	190.25.112.10	190.217.19.156	2677724	834608245	690363103	144245142
8	VPN_REGISTRADU	201.232.123.20	190.217.24.4	2677646	574058442	292654028	281404414
9	VPN_Linktic	3.222.171.115	190.217.24.4	2677490	167675464	98039361	69636103
10	VPN_AZURE-VWAN2	4.153.117.131	190.217.24.4	2676720	52557492	31495276	21062216
11	VPN_FISCALIA	190.157.218.66	190.217.24.4	2677494	47181851	45291436	1890415
12	OCI_EXADATA_FAB	150.136.25.96	190.217.24.4	2677572	14346384	0	14346384
13	VPN_AZURE-VWAN	4.153.117.133	190.217.24.4	2675745	9914684	9897004	17680

16.2. Top de intrusiones detectadas por el IPS del firewall perimetral

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

Top Attacks

#	Attack Name	Severity	CVE-ID	Counts
1	Spring.Framework.SerializationUtils.Insecure.Deserialization	Critical	CVE-2022-22965	364,212
2	Adobe.ColdFusion.Multiple.Vulnerabilities	Critical	CVE-2013-0625,CVE-2013-0629,CVE-2013-0631,CVE-2013-0632	70,663
3	Apache.Log4j.Error.Log.Remote.Code.Execution	Critical	CVE-2021-4104,CVE-2021-44228,CVE-2021-45046	62,650
4	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	Critical	CVE-2017-11317,CVE-2017-11357,CVE-2019-18935	47,288
5	HTTP.URI.Java.Expression.Language.Code.Injection	Critical	CVE-2021-22053,CVE-2022-26134	46,640
6	Ivanti.EPMM.CVE-2023-35082.Authentication.Bypass	Critical	CVE-2023-35082	46,528
7	F5.BIG-IP.Traffic.Management.User.Interface.Path.Traversal	Critical		45,759
8	Remote.CMD.Shell	Critical		45,549
9	Zabbix.Frontend.CVE-2022-23131.Privilege.Elevation	Critical	CVE-2022-23131	45,404
10	Citrix.Application.Delivery.Controller.VPNs.Path.Traversal	Critical		43,429

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

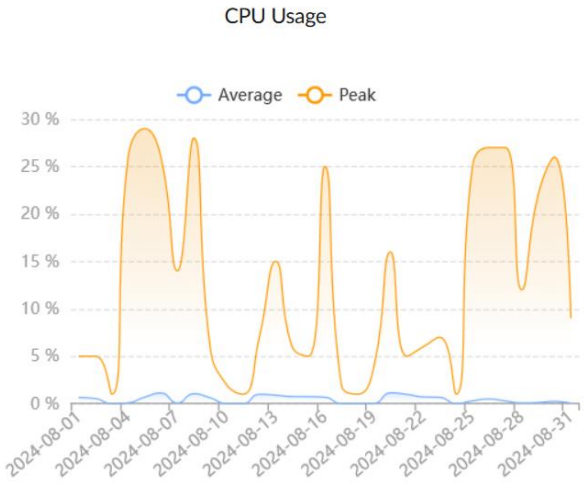
Top Intrusion Victims

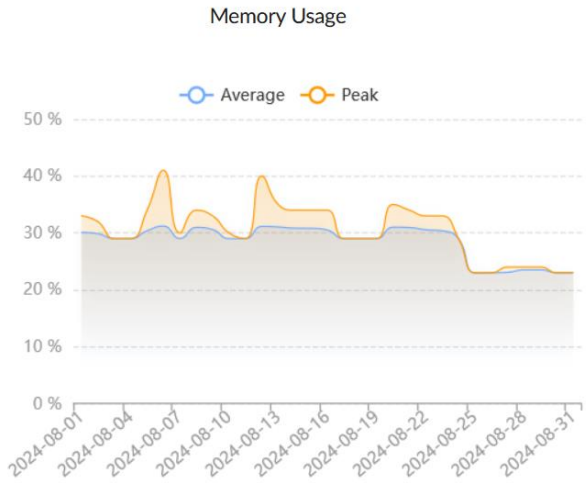
#	Attack Victim	Counts	Critical	High	Medium	Percent of Total Attacks
1	172.17.201.16				1,198,024	32.95%
2	172.17.201.68				383,858	10.56%
3	172.17.202.30				366,647	10.08%
4	172.17.201.6				365,843	10.06%
5	172.17.202.151				364,484	10.02%
6	172.17.201.75				166,142	4.57%
7	172.17.202.147				165,750	4.56%
8	172.17.201.152				165,038	4.54%
9	172.17.201.13				112,910	3.11%
10	172.17.201.52				92,141	2.53%
11	172.17.201.110				80,936	2.23%
12	172.17.202.102				77,562	2.13%
13	190.217.24.176				25,258	0.69%
14	172.17.201.54				19,296	0.53%
15	190.217.24.69				12,788	0.35%
16	34.29.85.190				10,407	0.29%
17	172.29.182.99				9,395	0.26%
18	172.28.108.88				8,276	0.23%
19	192.168.213.94				6,281	0.17%
20	172.17.202.56				4,816	0.13%

Los hosts 172.17.201.X, 172.17.202.X, 190.217.24.X son aplicaciones web protegidas por los WAF Torre Central y el WAF CAN. Se debe verificar los demás hosts con software antivirus: 172.29.182.99 (host de Cundinamarca, Bogotá; Calle 11 # 9-24), 172.28.108.88 y 192.168.213.94 (servidores del datacenter CAN).

17. FIREWALL SEDE PALACIO

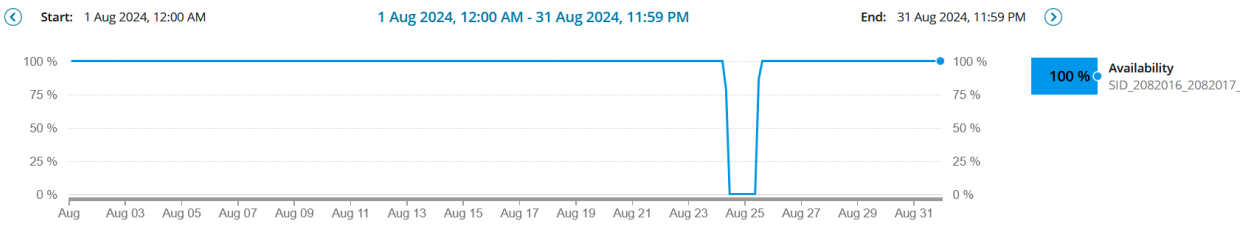
Durante agosto, el consumo de CPU y memoria en el Firewall de Palacio se mantuvo dentro de sus valores de operación normal.





17.1. Disponibilidad Mensual Firewall Palacio

Durante agosto se obtuvo 100% de disponibilidad en el servicio firewall Palacio. El evento del 25 de agosto corresponde a la ventana de mantenimiento eléctrica programada por parte de cliente y relacionada con la solicitud "TT883531 Acompañamiento ventana apagado FW Palacio Justicia manos remotas":



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%.

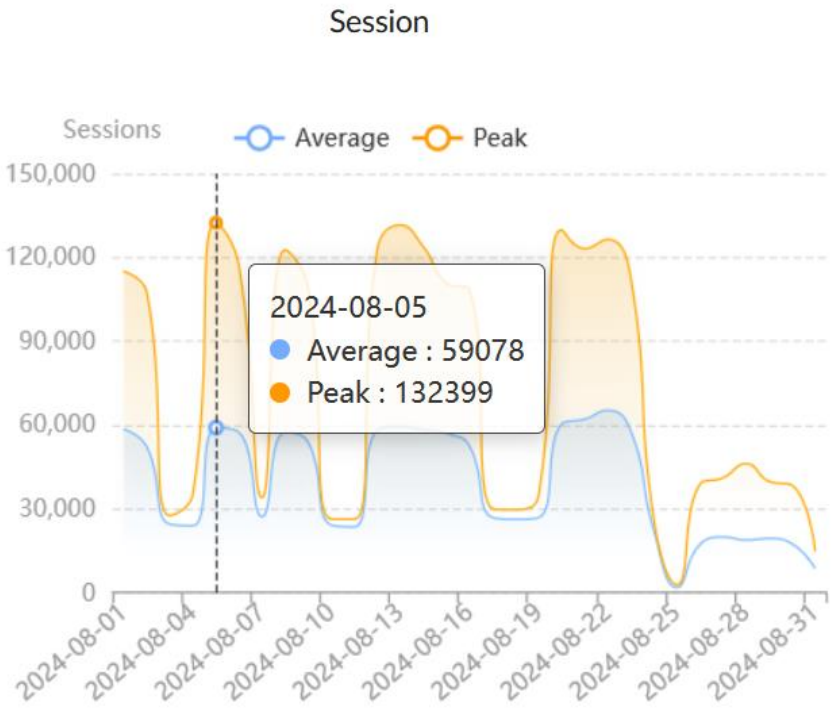
Un valor más exacto de la disponibilidad de agosto debido a la ventana de mantenimiento eléctrica fue 96.618% como se muestra a continuación:

Availability Statistics

PERIOD	AVAILABILITY
Today	100.000 %
Yesterday	100.000 %
Last 7 Days	94.630 %
Last 30 Days	96.548 %
This Month	100.000 %
Last Month	96.618 %

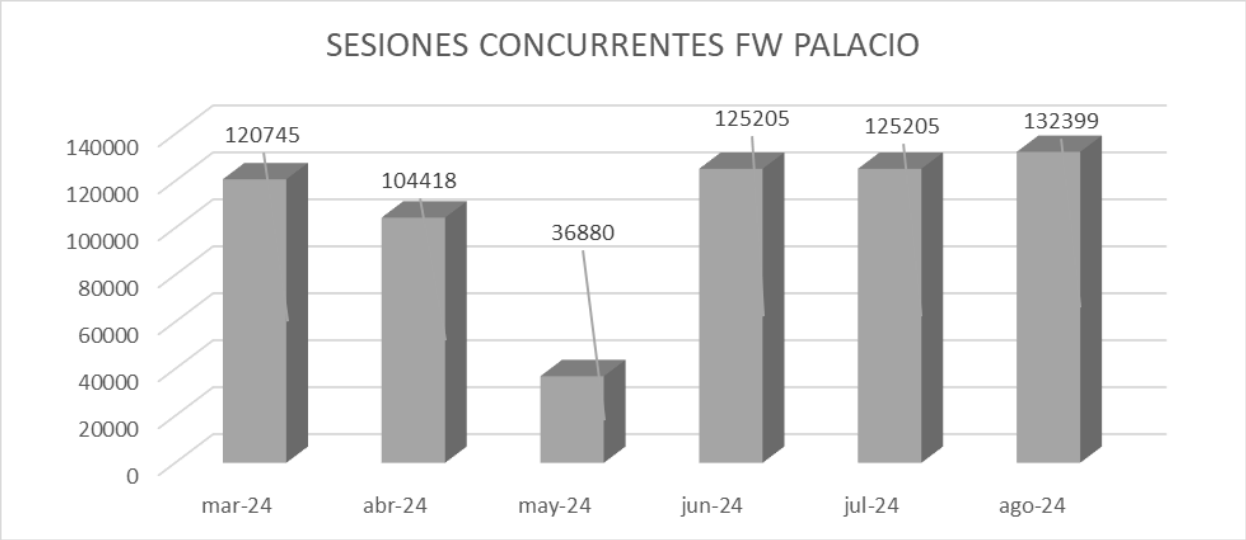
17.2. Cantidad de Sesiones Firewall Palacio

Durante agosto se presentó un máximo de 132399 sesiones concurrentes que están dentro del rango de sesiones soportadas por el equipo Fortigate 900G de 16 Millones.



17.3. Histórico de Sesiones Últimos 6 meses Firewall Palacio

Durante el mes de agosto se presentaron 132399 en la cantidad de las sesiones del firewall Palacio:



MES	SESIONES
mar-24	120745
abr-24	104418
may-24	36880
jun-24	125205
jul-24	125205
ago-24	132399

17.4. Aplicaciones y protocolos por ancho de banda firewall Palacio

Microsoft.Portal consumió la mayor cantidad de ancho de banda durante agosto:

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	Microsoft.Portal			21.82 TB
2	Microsoft.SharePoint			7.44 TB
3	HTTPS.BROWSER			5.64 TB
4	OneDrive			3.55 TB
5	SSL			2.60 TB
6	Microsoft.365.Portal			1.54 TB
7	Google.Services			1.54 TB
8	Microsoft.Outlook			1.12 TB
9	HTTP.BROWSER			1.09 TB
10	Microsoft.Teams			878.97 GB

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

Top Applications by Sessions

#	Application	Sessions
1	SMB	460,116,514
2	DNS	50,558,889
3	Microsoft.Windows.Update	48,865,800
4	HTTP.BROWSER	47,798,046
5	Microsoft.365.Portal	39,507,168
6	Microsoft.Portal	33,488,066
7	SSL	33,062,517
8	HTTPS.BROWSER	27,612,736
9	Microsoft.Outlook	21,203,747
10	Rapid7.Insight.Agent	20,769,195

17.5. 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 agosto:

Top Bandwidth IP

#	IP	Bandwidth
1	172.28.93.2	10.55 TB
2	192.168.2.209	862.16 GB
3	172.29.154.28	781.71 GB
4	172.28.93.46	720.10 GB
5	172.16.2.59	651.06 GB
6	172.29.154.13	468.90 GB
7	172.16.4.66	463.26 GB
8	172.28.92.23	442.30 GB
9	172.16.5.33	424.50 GB
10	172.28.93.251	380.32 GB

17.6. Top de destinos web por ancho de banda Firewall Palacio.

20.60.0.104, 13.107.136.10, 13.107.138.10 y 172.190.220.253 fueron destinos más visitados durante agosto:

Top Websites and Category by Bandwidth

#	Site	Category	Bytes
1	20.60.0.104		10.28 TB
2	13.107.136.10		3.69 TB
3	13.107.138.10		3.46 TB
4	172.190.220.253		1.76 TB
5	13.107.246.40		802.68 GB
6	20.60.128.228		703.85 GB
7	20.168.235.216		675.91 GB
8	52.104.3.39		660.23 GB
9	190.217.24.42		581.22 GB
10	procesojudicial.ramajudicial.gov.co		367.06 GB

17.7. Top de usuarios con peticiones bloqueadas por el Firewall Palacio.

172.16.3.220, 172.16.3.222 y 172.16.4.222 (hosts de la LAN Palacio) presentaron la mayor cantidad de conexiones bloqueadas durante agosto.

Top Web Users by Blocked Requests

#	User (or IP)	Hostname	Requests
1	172.16.3.220	172.16.3.220	292,388
2	172.16.3.222	172.16.3.222	178,319
3	172.16.4.222	172.16.4.222	131,109
4	172.16.4.182	172.16.4.182	71,873
5	172.16.6.90	172.16.6.90	61,868
6	172.16.3.221	172.16.3.221	54,102
7	172.16.6.183	172.16.6.183	53,471
8	192.168.8.23	192.168.8.23	51,845
9	172.28.93.61	172.28.93.61	51,170
10	172.28.93.103	172.28.93.103	48,683

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.

17.8. Top de las categorías más bloqueadas por el Firewall Palacio.

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

Top Blocked Web Categories

#	Category	Requests
1	Unrated	7,857,951
2	Proxy Avoidance	810,500
3	Streaming Media and Download	439,728
4	Social Networking	405,945
5	Newly Observed Domain	120,194
6	Games	109,582
7	Entertainment	44,117
8	Society and Lifestyles	15,644
9	Phishing	9,733
10	Remote Access	3,634

17.9. 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 agosto:

Top Web IP by Allowed Requests

#	IP	Requests
1	172.16.4.90	24,122,256
2	172.28.54.20	15,679,301
3	192.168.8.23	754,181
4	172.16.1.7	603,551
5	172.28.93.101	467,406
6	172.16.6.121	445,670
7	192.168.2.132	423,477
8	172.16.5.100	396,924
9	172.16.5.68	392,913
10	172.17.114.232	388,271

17.10. 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	34,748,435
2	Search Engines and Portals	6,878,918
3	Business	1,829,257
4	Information and Computer Security	711,184
5	Web Analytics	543,882
6	Web-based Applications	192,822
7	Finance and Banking	103,637
8	Overrride_permitidas	97,503
9	Online Meeting	51,632
10	Secure Websites	31,179

17.11. 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) presentaron la mayor cantidad de conexiones durante agosto:

Top IP by Bandwidth

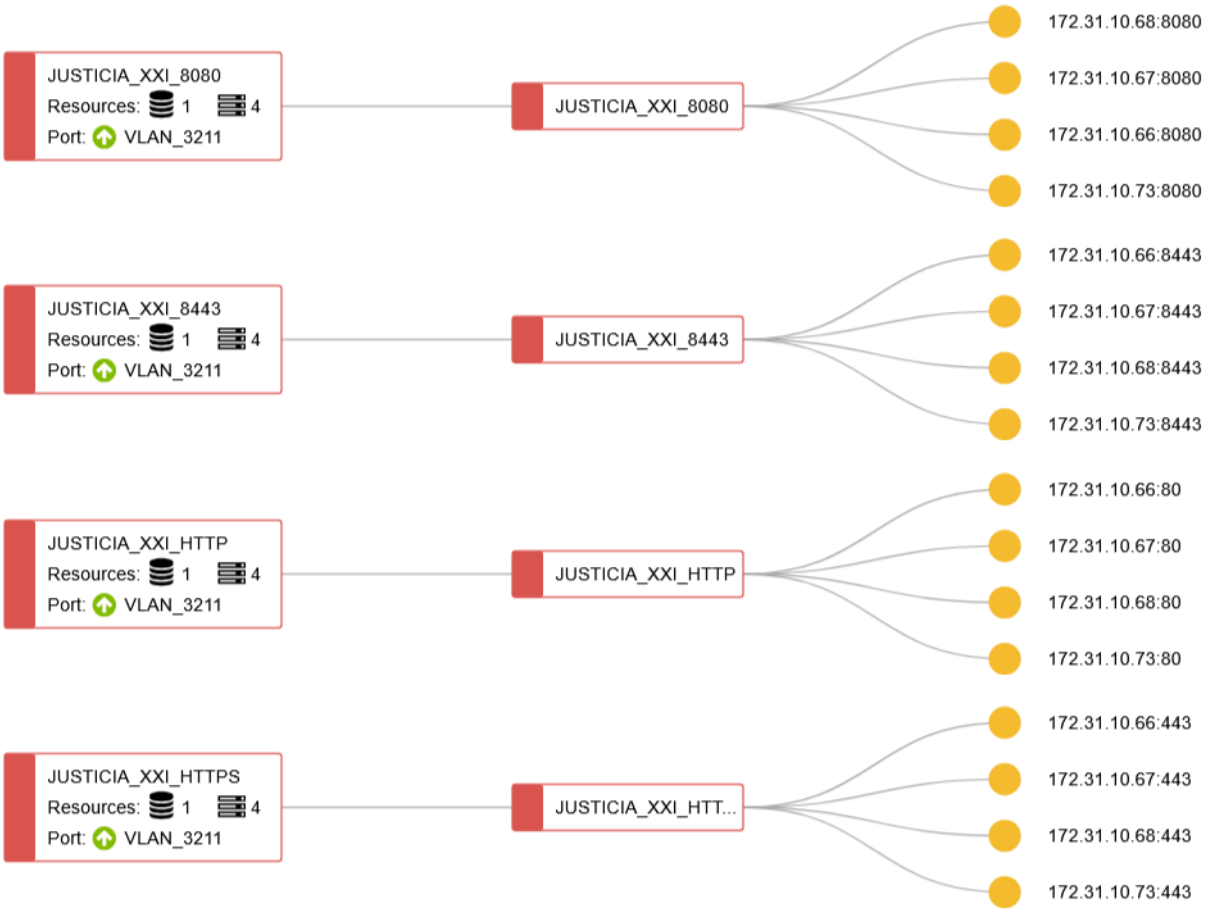
#	IP	Bandwidth	Sent	Received
1	172.28.93.2			10.54 TB
2	172.29.154.58			7.84 TB
3	192.168.2.209			866.55 GB
4	172.16.3.34			815.78 GB
5	172.28.92.15			793.77 GB
6	172.29.154.28			779.51 GB
7	172.28.93.46			719.83 GB
8	172.16.2.59			711.40 GB
9	172.28.92.23			589.22 GB
10	172.16.4.66			511.85 GB

18. BALANCEADOR DE CARGA FORTIADC

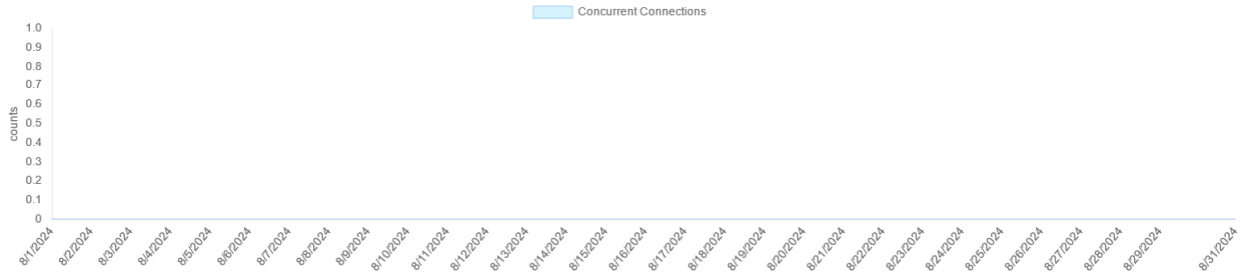
A continuación, se observan los diferentes servicios balanceados.

18.1. Justicia XXI

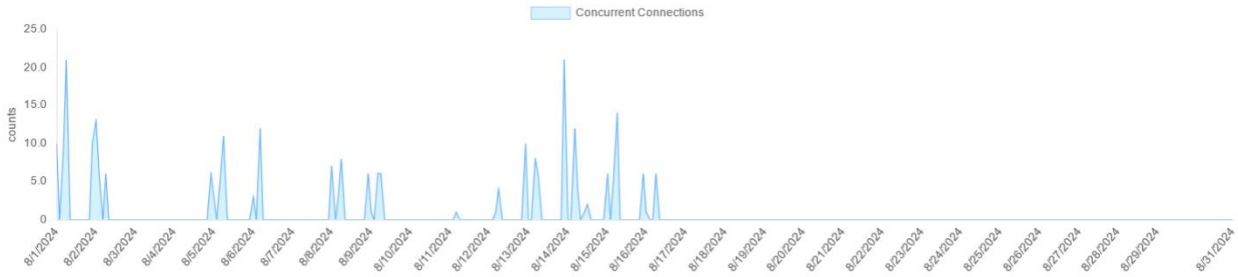
Se encuentra balanceado en el FortiADC:



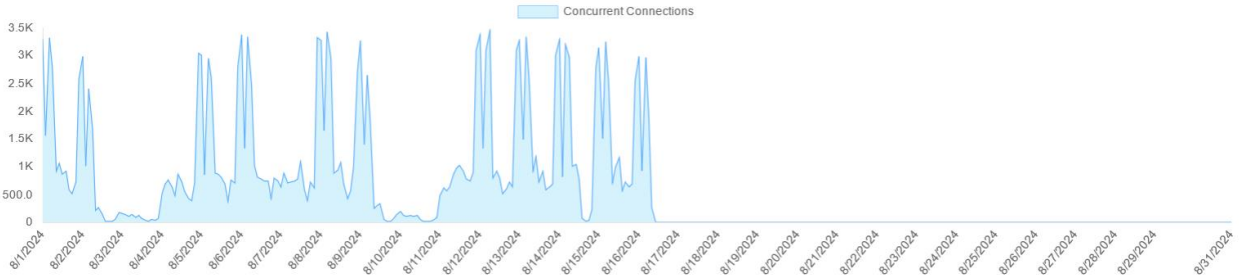
Durante agosto no se presentó tráfico por el puerto 8080:



Conexiones concurrentes por el puerto 8443:



Conexiones concurrentes por el puerto 443:

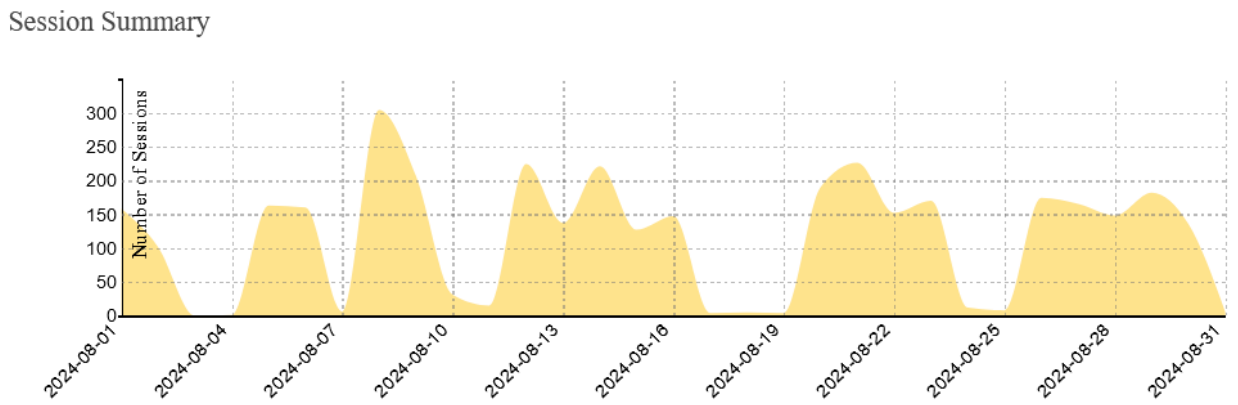


18.2. Kactus RDP

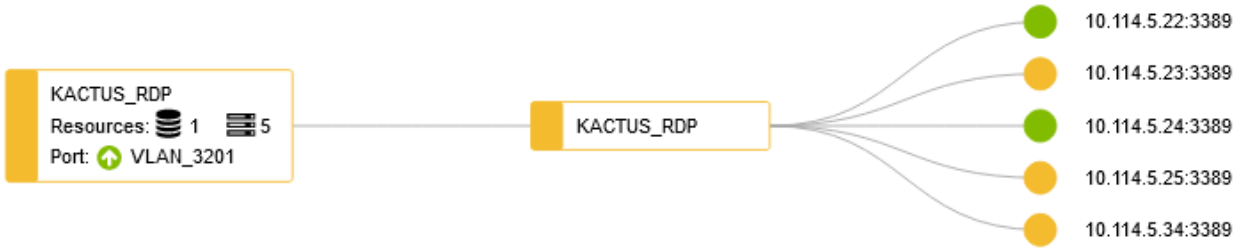
Esta aplicación se encuentra en el Firewall utilizando la siguiente configuración:

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 10.114.5.22	Vlan_2000

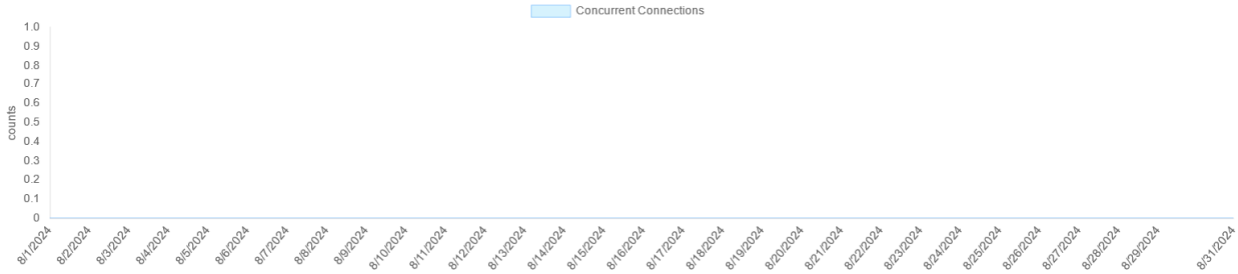
A continuación, se observa el número de sesiones concurrentes para este aplicativo.



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

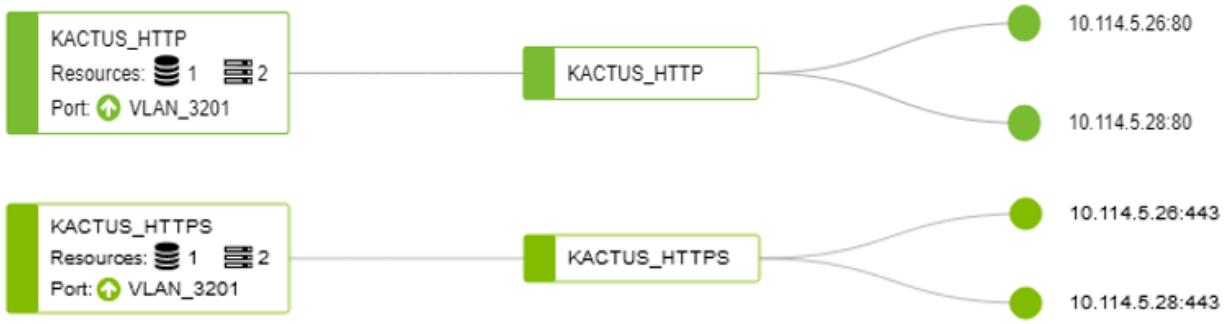


En el FortiADC no se observan sesiones concurrentes:

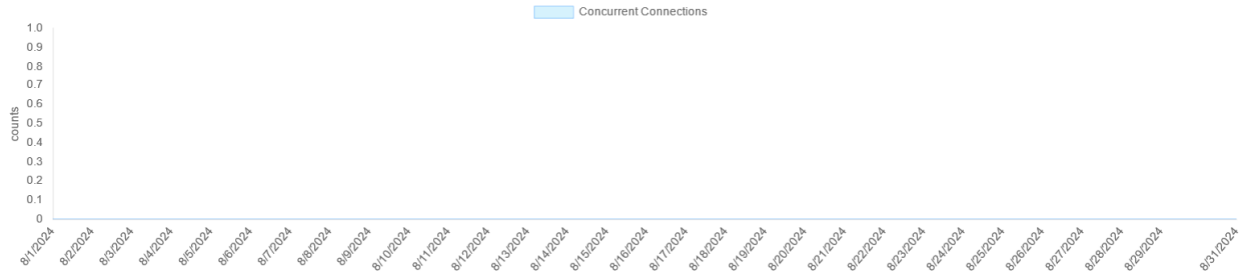


18.3. Kactus WEB

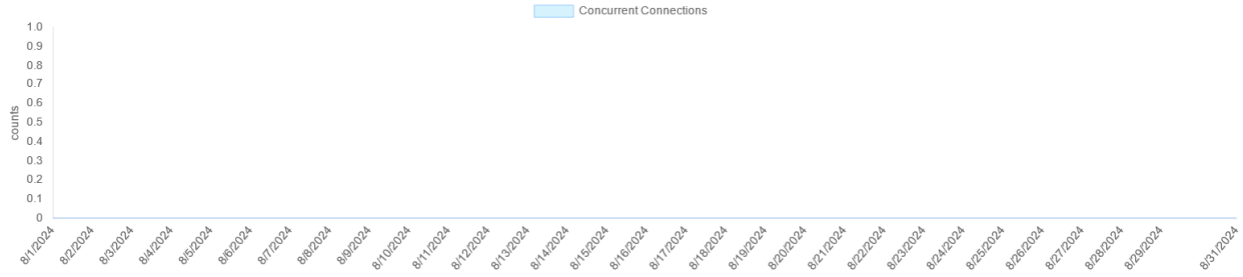
Se encuentra balanceado en el FortiADC:



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



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



18.4. SIRNA

Este servicio se encuentra balanceado en el FortiGate perimetral:

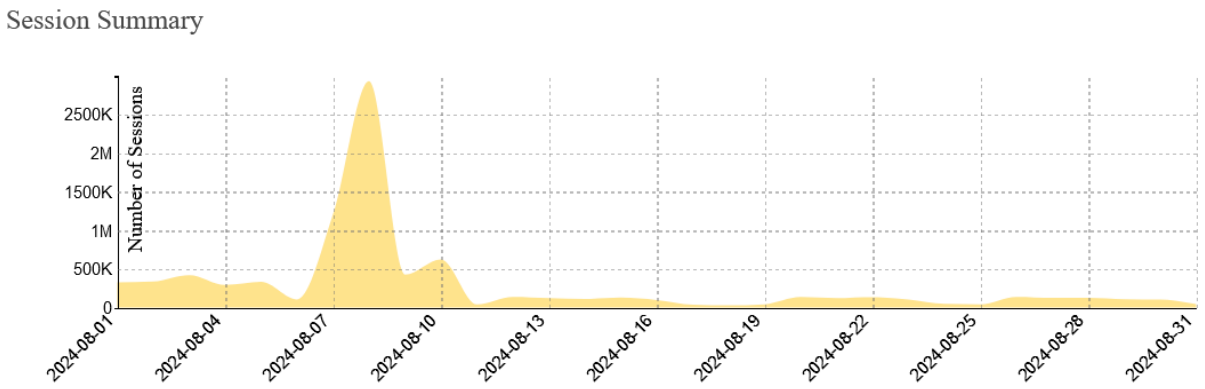
Configuración de balanceo de CRM en el Firewall.

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 10.244.2.227

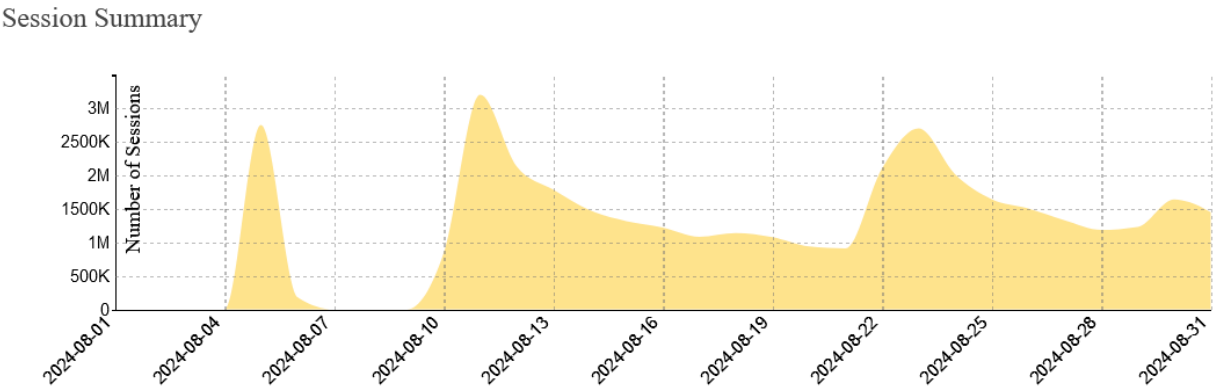
Configuración de balanceo de Sharepoint en el firewall perimetral.

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 10.244.2.228

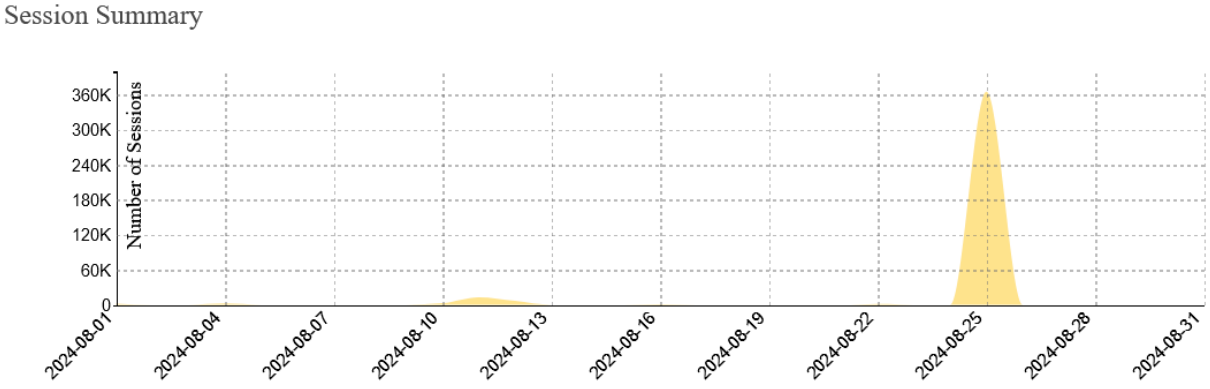
Las sesiones en el firewall para SIRNA 443 fueron:



Las sesiones en el firewall para CRM 443 fueron:



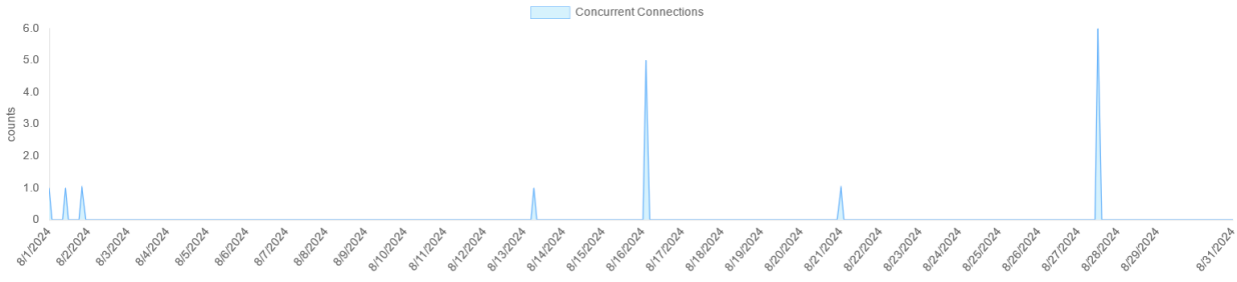
Las sesiones en el firewall para Sharepoint 444 fueron:



18.5. Convocatoria Peritos.

Este servicio se encuentra balanceado en el FortiADC:

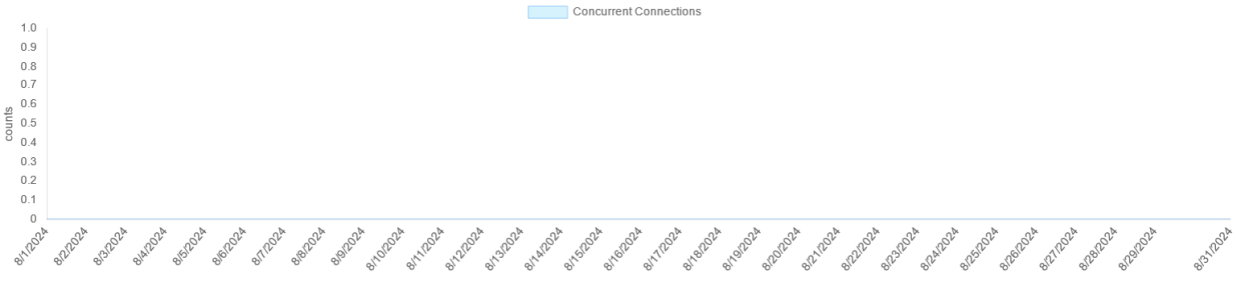
Las sesiones concurrentes fueron las siguientes:



18.6. SIERJU

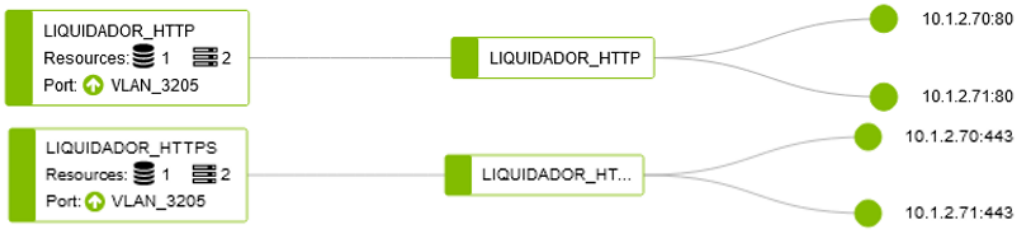
La configuración de balanceo para esta aplicación en el balanceador FortiADC es:

Durante agosto no se observan conexiones concurrentes para este aplicativo:

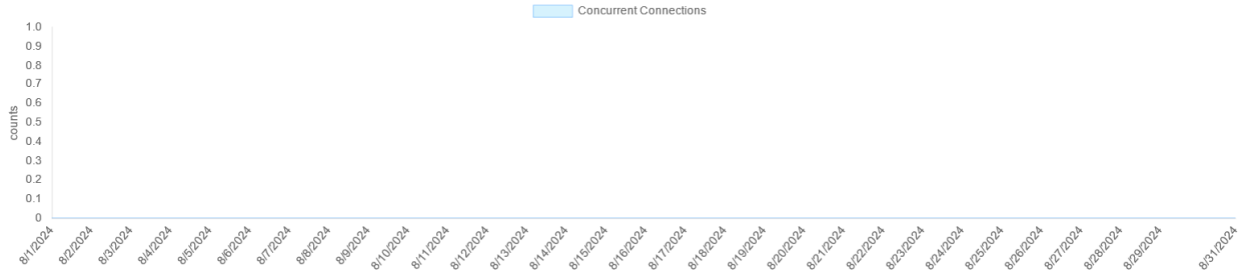


18.7. Liquidador de Sentencias

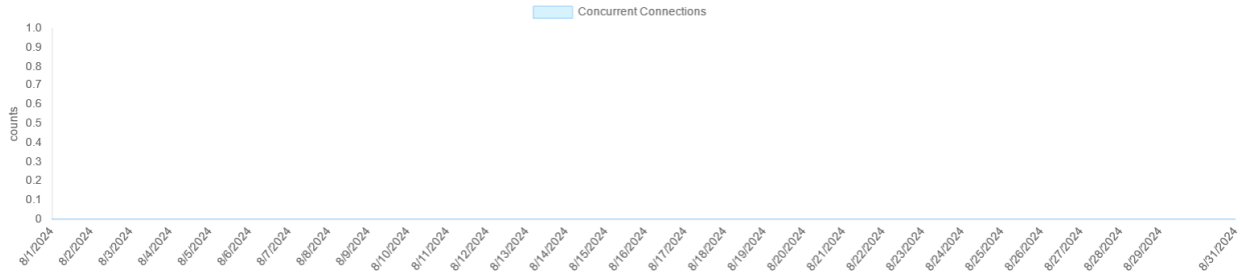
Virtual server Liquidador de Sentencias balanceador FortiADC



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



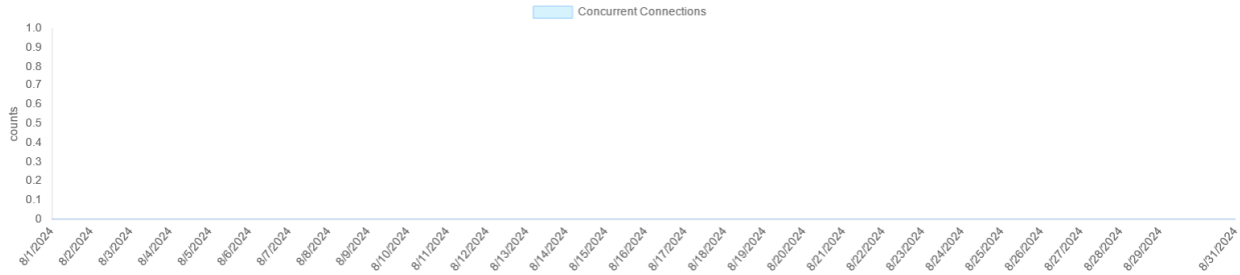
Las sesiones concurrentes por HTTPS fueron:



18.8. Consulta Jurisprudencia

Virtual server Consulta Jurisprudencia se encuentra en el balanceador FortiADC.

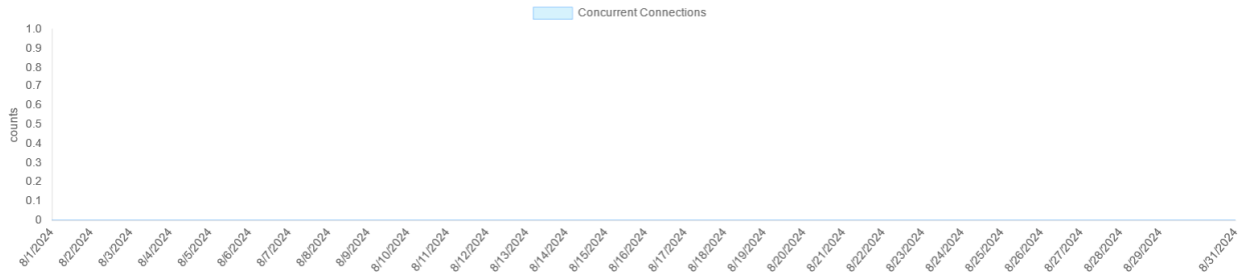
Durante agosto no se observan conexiones concurrentes para este aplicativo:



18.9. API Gestión de Audiencias

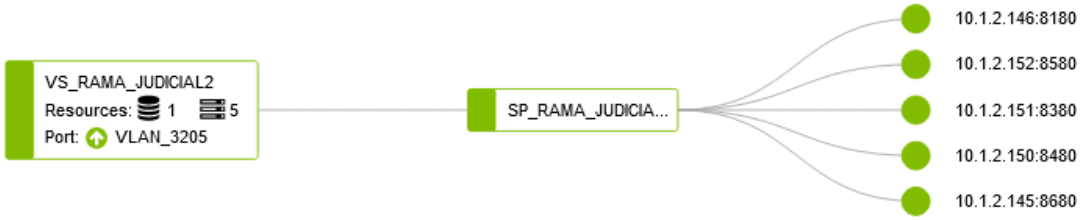
Virtual server API Gestión de Audiencias balanceador FortiADC.

Las sesiones concurrentes por HTTPS para este aplicativo:

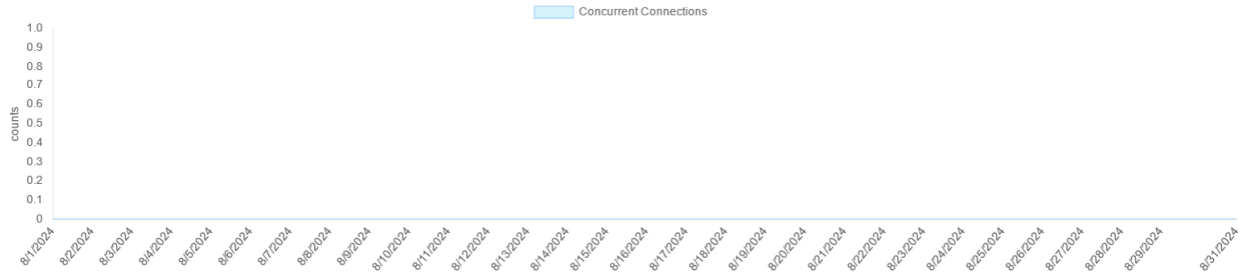


18.10. Portal Alterno de la Rama Judicial

Se encuentran balanceado en el FortiADC:

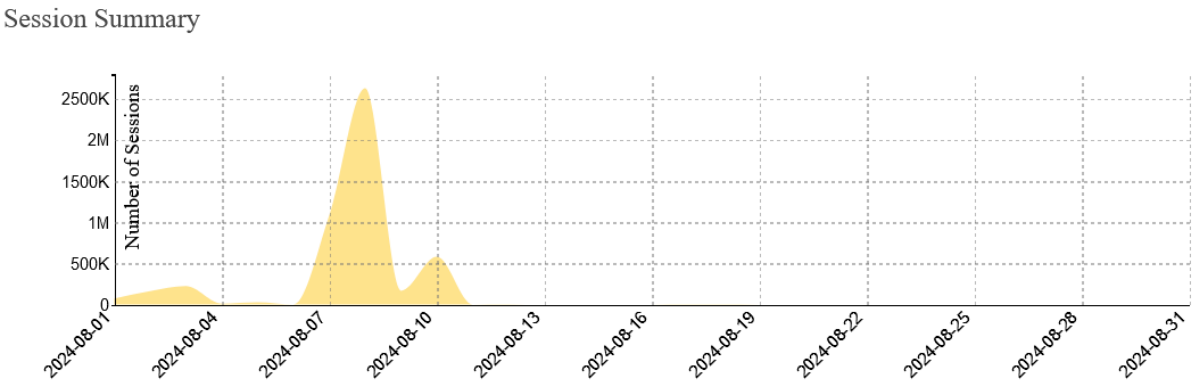


Durante agosto no se observan conexiones concurrentes para este aplicativo:



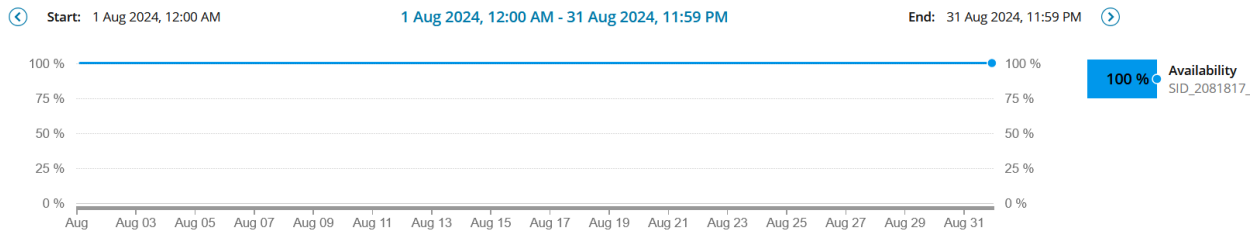
18.11. Portal de la Rama Judicial

Las sesiones Historico_Portal Rama Judicial fueron:

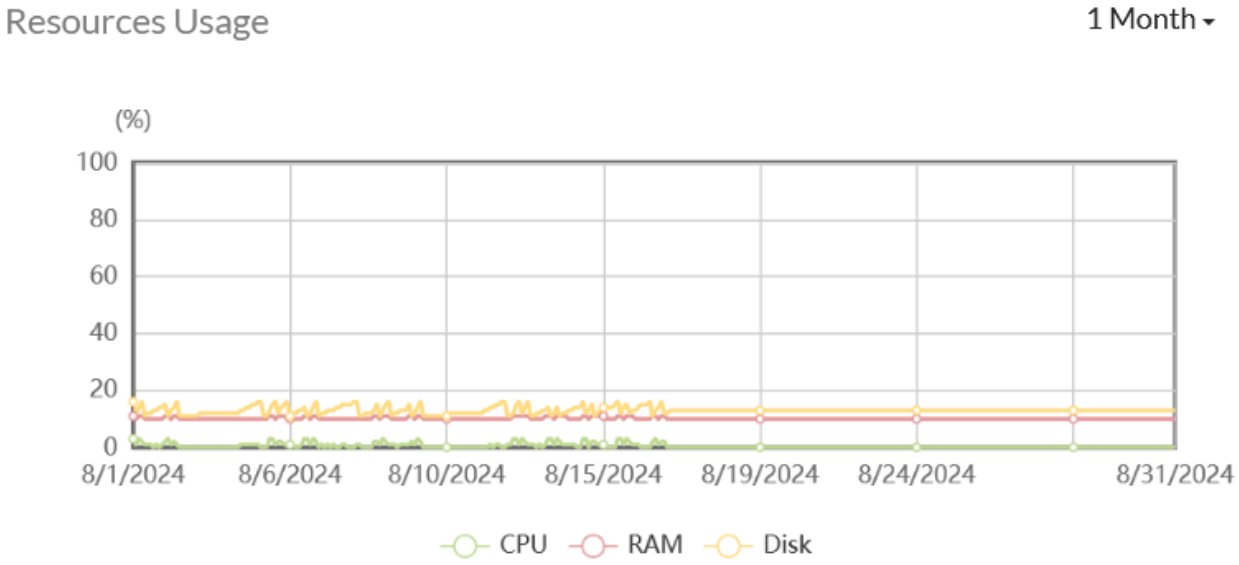


18.12. Disponibilidad y performance.

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



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



19. TRÁFICO DE WEB APPLICATION FIREWALL (WAF) TORRE CENTRAL

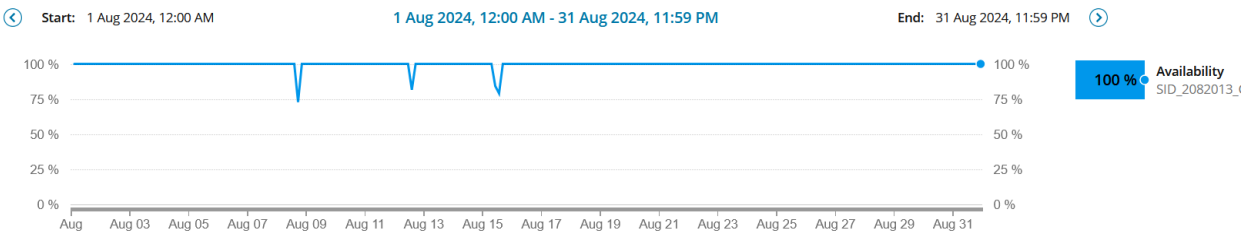
Para la protección de las aplicaciones web se tienen configuradas las siguientes políticas en los Firewall de Aplicaciones Web:

Item	Solución WAF	Cantidad de políticas de servidores
1	WAF TORRE CENTRAL	162
2	WAF CAN	67

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

19.1. Web application firewall datacenter principal IFX.

Durante agosto se obtuvo disponibilidad del 100 % en el Kemp de Torre Central. Los eventos del 8, 12 y 15 de agosto ocurrieron en el sistema de monitoreo que no afectaron los servicios que IFX Networks presta a la Rama Judicial.



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%.

Un valor más exacto es de 99.643%

Availability Statistics

PERIOD	AVAILABILITY
Today	100.000 %
Yesterday	100.000 %
Last 7 Days	100.000 %
Last 30 Days	99.636 %
This Month	100.000 %
Last Month	99.643 %

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

La aplicación web más consultada durante agosto fue publicacionesprocesales.ramajudicial.gov.co (172.17.201.100:443) con 11’248.637 sesiones web correspondiente al 50,31%

#	Name	Virtual IP Address	Total Conns	% del total
1	publicacionesprocesales.ramajudicial.gov.co - 190.217.24.175	172.17.201.100:443	11248637	50,31%
2	nuevoportal.ramajudicial.gov.co Y cndj.gov.co 190.217.24.176	172.17.201.101:443	5588954	25,00%
3	siicor.corteconstitucional.gov.co - 190.217.24.62	172.17.201.13:443	2226884	9,96%
4	consejodeestado.gov.co - 190.217.24.60	172.17.201.52:443	877085	3,92%
5	sirna.ramajudicial.gov.co	172.17.201.28:443	374889	1,68%
6	apigestionaudiencias1.ramajudicial.gov.co	172.17.201.42:443	289228	1,29%
7	consultajurisprudencial.ramajudicial.gov.co 8080	172.17.201.110:8080	288191	1,29%
8	liquidador.ramajudicial.gov.co	172.17.201.56:443	149579	0,67%
9	antecedentesdisciplinarios.cndj.gov.co	172.17.201.31:443	139845	0,63%
10	videoteca.ramajudicial.gov.co Holocausto_lector_videoteca_sidn_443	172.17.201.54:443	120455	0,54%
	Otras aplicaciones		1055525	4,72%
	Total		22359272	100,00%

19.3. Top de peticiones por país WAF principal IFX.

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

Top 10 Countries

Total

Country	Requests	Blocked
Colombia	11355749	2760224
Private	2475825	721494
United States	2092274	172841
IPrep	29242	29242
Argentina	125103	24050
Panama	40222	14381
Russia	630952	11791
Brazil	58132	9501
Bangladesh	25357	5737
Mexico	16991	4843

19.4. Top de ataques por política WAF principal IFX.

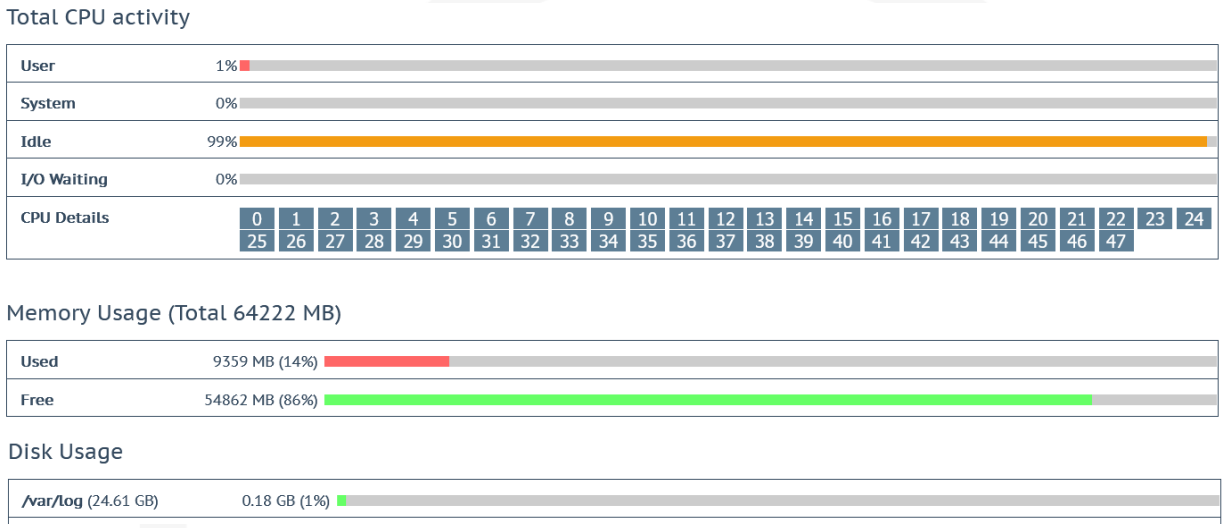
La siguiente tabla muestra el top 10 de las reglas o virtual services que proporcionaron mayor protección contra ataques a las aplicaciones web durante agosto. Sobre la aplicación *publicacionesprocesales.ramajudicial.gov.co* han sido prevenidas la mayor cantidad de ataques durante agosto:

#	Name	Virtual IP Address	Total Events	% del total
1	publicacionesprocesales.ramajudicial.gov.co - 190.217.24.175	172.17.201.100:443	3684072	97,02%
2	nuevoportal.ramajudicial.gov.co Y cndj.gov.co 190.217.24.176	172.17.201.101:443	78706	2,07%
3	siicor.corteconstitucional.gov.co - 190.217.24.62	172.17.201.13:443	17466	0,46%
4	videoteca.ramajudicial.gov.co Holocausto_lector_videoteca_sidn_443	172.17.201.54:443	4614	0,12%
5	consejodeestado.gov.co - 190.217.24.60	172.17.201.52:443	4335	0,11%
6	jurisprudencia.ramajudicial.gov.co - 190.217.24.193	172.17.201.29:8446	1152	0,03%
7	iedoc.consejodeestado.gov.co 448	172.17.201.60:448	996	0,03%
8	sirna.ramajudicial.gov.co	172.17.201.28:443	572	0,02%
9	actosadministrativos.ramajudicial.gov.co	172.17.201.30:443	469	0,01%
10	sistemaaudiencias.ramajudicial.gov.co	172.17.201.44:443	465	0,01%
	Otras aplicaciones		4337	0,11%
	Total		3797184	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.

19.5. Consumo de recursos WAF principal IFX.

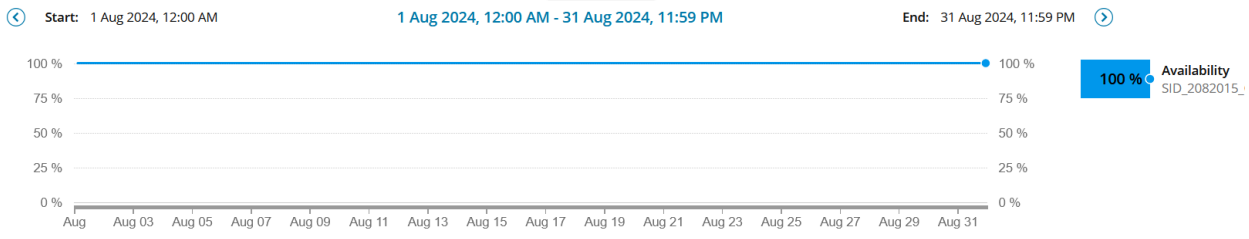
El WAF KEMP de Torre Central presentó consumo de CPU del 1%, memoria de 14% y disco en un 1%.



20. TRÁFICO DE WEB APPLICATION FIREWALL (WAF) CAN

20.1. Disponibilidad WAF CAN.

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



20.2. Uso de políticas de servidores WAF CAN.

La aplicación más consultada durante agosto fue cortesuprema.gov.co_Palacio con un 97,02% del total:

#	Name	Virtual IP Address	Total Events	% del total
1	publicacionesprocesales.ramajudicial.gov.co - 190.217.24.175	172.17.201.100:443	3684072	97,02%
2	nuevoportal.ramajudicial.gov.co Y cndj.gov.co 190.217.24.176	172.17.201.101:443	78706	2,07%
3	siicor.corteconstitucional.gov.co - 190.217.24.62	172.17.201.13:443	17466	0,46%
4	videoteca.ramajudicial.gov.co Holocausto_lector_videoteca_sidn_443	172.17.201.54:443	4614	0,12%
5	consejodeestado.gov.co - 190.217.24.60	172.17.201.52:443	4335	0,11%
6	jurisprudencia.ramajudicial.gov.co - 190.217.24.193	172.17.201.29:8446	1152	0,03%
7	iedoc.consejodeestado.gov.co 448	172.17.201.60:448	996	0,03%
8	sirna.ramajudicial.gov.co	172.17.201.28:443	572	0,02%
9	actosadministrativos.ramajudicial.gov.co	172.17.201.30:443	469	0,01%
10	sistemaaudiencias.ramajudicial.gov.co	172.17.201.44:443	465	0,01%
	Otras aplicaciones		4337	0,11%
	Total		3797184	100,00%

20.3. Top de peticiones por país WAF CAN.

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

Top 10 Countries

Total

Country	Requests	Blocked
Bulgaria	249165	202817
United States	7013939	130614
Private	1432465	7002
IPrep	6489	6489
Spain	16875	1130
Russia	47959	934
China	10392	680
Singapore	70549	593
Hong Kong	10180	468
Ukraine	2080	468

20.4. Top de ataques por política WAF CAN.

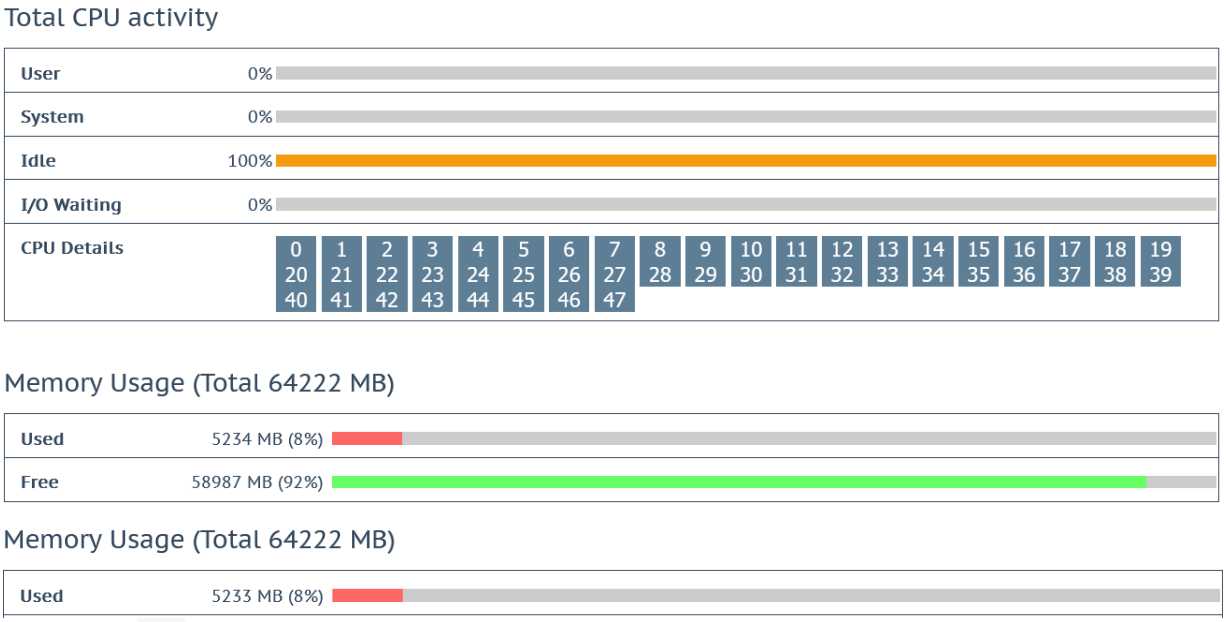
La siguiente tabla muestra el top 10 de las reglas o virtual services que proporcionaron mayor protección contra ataques a las aplicaciones web durante agosto. Sobre la aplicación cortesuprema.gov.co_Palacio ha sido prevenida la mayor cantidad de ataques durante agosto:

#	Name	Virtual IP Address	Total Events	% del total
1	cortesuprema.gov.co_Palacio	172.17.202.239:443	642849	89,99%
2	precalificacion.ramajudicial.gov.co	172.17.202.102:443	9306	1,30%
3	relatoria.cndj.gov.co	172.17.202.66:443	9191	1,29%
4	siapoas.ramajudicial.gov.co	172.17.202.43:443	5898	0,83%
5	convocatorias.consejodeestado.gov.co	172.17.202.147:443	4974	0,70%
6	capacitacion.ramajudicial.gov.co 443	172.17.202.13:443	4816	0,67%
7	efinominapruebas.ramajudicial.gov.co	172.17.202.45:443	4731	0,66%
8	samairj.consejodeestado.gov.co	172.17.202.38:443	3234	0,45%
9	restituciontierras.ramajudicial.gov.co	172.17.202.37:443	3059	0,43%
10	predesarchive.ramajudicial.gov.co	172.17.202.53:443	2985	0,42%
	Otras aplicaciones		23328	3,27%
	Total		714371	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.

20.5. Consumo de recursos WAF CAN.

El WAF KEMP del CAN presentó consumo de CPU del 0%, memoria de 8% y disco en un 8%.



20.6. Certificado wildcard Rama Judicial *.ramajudicial.gov.co

Este certificado tiene vigencia hasta el 25 de abril 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]

*.cndj.gov.co
[Expires: Jan 24 23:59:59 2025 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

20.7. Intentos login fallidos a Firewalls

Durante agosto se presentaron los siguientes intentos de ingreso administrativo hacia los firewall perimetrales. El acceso administrativo se encuentra protegido controles de "Restrict login to trusted hosts", sin embargo se agrega 94.141.120.23 a las listas negras de IPs maliciosas reportadas.

#	Login Source	User Name	Total Number of Failed Logins
1	ssh(94.141.120.23)	root	57
2	ssh(94.141.120.23)	postgres	10
3	https(10.0.1.160)	jose.cardenas	9
4	ssh(94.141.120.23)	weblogic	8
5	ssh(94.141.120.23)	User	8
6	ssh(94.141.120.23)	sprixin	7
7	ssh(94.141.120.23)	odoo	6
8	ssh(94.141.120.23)	test	6
9	ssh(94.141.120.23)	ubuntu	6
10	ssh(94.141.120.23)	testing	6

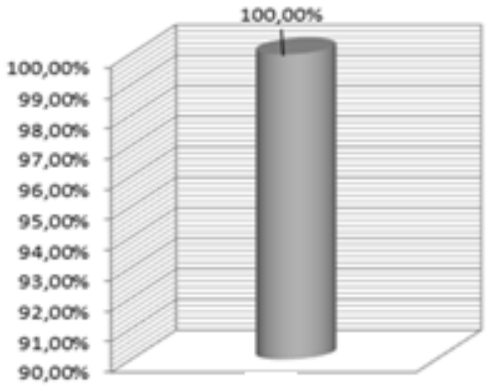
21. DISPONIBILIDAD SEGURIDAD GLOBAL DEL MES DE AGOSTO

La disponibilidad global de agosto en los dispositivos y los servicios de seguridad fue del 100%.

No se presentaron tickets tipo incidencia que hayan afectado esta disponibilidad:

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

MES	DISPONIBILIDAD (%)
AGOSTO	100%



21.1. Anexo de las solicitudes e incidentes de seguridad reportadas.

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

9. 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)

10. 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	$ 8.936.152.745,33
% Valor facturado	57,59%
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
IFXC - 411473	viernes, 16 de agosto de 2024	$ 1.529.127.888,86	01 al 31 de Julio 2024		Pendiente

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
01 al 31 de Julio 2024	No se generaron ANS durante el periodo
Descuento SID 2081861 "Disponibilidad del servicio en instalaciones DC" - 05 de Febrero 2024 al 31 de julio de 2024	$ 469.024,14
Total ANS	**$ 17.587.579,14**

11. 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.