REPORTE MENSUAL

RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA

OC124016

SEPTIEMBRE 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 SEPTIEMBRE de 2024 Fecha de final: 30 de SEPTIEMBRE 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 (MPPS) - 45000000- Mes - Cantidad: 2	DDOS DC Torre central	FORTIDDOS FORTINET 2000E/PPLA	2000E	SN: FI2KETB 20000015	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: FI2KE58 19000049	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 30 de SEPTIEMBRE de 2024 es de: **3842906(GB)**

El almacenamiento total presentado adicional es de: **3719695 (GB)**

Total, contratado de Almacenamiento SAN alto rendimiento: **4150000(GB)**

A corte 30 de SEPTIEMBRE 2024 la entidad cuenta con un almacenamiento disponible de 10305 (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 encuentra, aprovisionado y disponible para uso de la entidad a partir de mes de **AGOSTO 2024** .

(Remitirse al anexo "**Inventario_Servicios_CSJ_SEPTIEMBRE_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 SEPTIEMBRE, está utilizando, una capacidad de **782.200 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 299000 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 483200 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	4,1 TB	262,8 TB
UNIDAD 2	80 TB	18 TB	235,2 TB
UNIDAD 3	78,2 TB	24,5 TB	223,3 TB
UNIDAD 4	110 TB	2,6 TB	410,5 TB

MENSUALES			
REPOSITORIOS	CAPACIDAD	ESPACIO LIBRE	ESPACIO USADO
UNIDAD 1	90 TB	8,5 TB	178,9 TB
UNIDAD 2	90 TB	6,1 TB	156,2 TB
UNIDAD 3	90 TB	10,9 MB	81,4 TB
UNIDAD 4	90 TB	6,3 TB	106,1 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).

A continuación, se relacionan las tareas de respaldo aprovisionadas para proteger las máquinas virtuales alojadas en la infraestructura de RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA. Las tareas de diseñaron e implementaron basados en las políticas de retención entregadas y establecidas.

Existen Jobs en los cuales se protegen las 162 máquinas virtuales, de estos Jobs están dentro de la política con 30 puntos de retención, donde los backups semanales se ejecutan todos los sábados y los diarios de Domingo a viernes en el mismo horario y una política especial mensual de 12 puntos que se ejecutan en el último domingo de cada mes el Backup de la NAS según lo realizado mediante el caso TT903322 está pendiente por definir la fecha de ejecución o el fin de semana de ejecución por parte de la entidad para la toma de Backup mensuales, una vez contemos con esta información se procederá a estandarizar la política, tener en cuenta que la información esta a corte 30 de septiembre 2024

ALMACENAMIENTO UTILIZADO

DIARIOS-SEMANALES OC 124016			
REPOSITORIO	CAPACIDAD (TB)	ESPACIO LIBRE (TB)	ESPACIO USADO (TB)
UNIDAD 1	80	4,1	262,8
UNIDAD 2	80	18	235,2
UNIDAD 3	78,2	24,5	223,3
UNIDAD 4	110	2,6	410,5
SUMATORIAS	348,2	49,2	1131,8

MENSUALES ANTES DE JULIO - COPIA HACIA AWS - PTE AUTORIZACIÓN DE DEPURACIÓN OC 100980			
REPOSITORIO	CAPACIDAD (TB)	ESPACIO LIBRE (TB)	ESPACIO USADO (TB)
UNIDAD 1	90	8,5	178,9
UNIDAD 2	90	6,1	156,2
UNIDAD 3	90	0,00103	81,4
UNIDAD 4	90	6,3	106,1
UNIDAD 5	100	39,5	94,1
UNIDAD 6	100	16,4	175,1
SUMATORIAS	560	76,80103	791,8

MENSUALES JULIO - OCTUBRE 2024 - OC 100980			
REPOSITORIO	CAPACIDAD (TB)	ESPACIO LIBRE (TB)	ESPACIO USADO (TB)
UNIDAD 1	100	0,0000016	99
UNIDAD 2	120	1,5	117,7
UNIDAD 3	120	2,7	169,8
SUMATORIAS	340	4,2000016	386,5

MENSUAL BACKUP SAN OC 124016			
REPOSITORIO	CAPACIDAD (TB)	ESPACIO LIBRE (TB)	ESPACIO USADO (TB)
NAS	235.5 TB	88,1 TB	147.4 TB

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_SEPTIEMBRE_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 SEPTIEMBRE 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_SEPTIEMBRE_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:

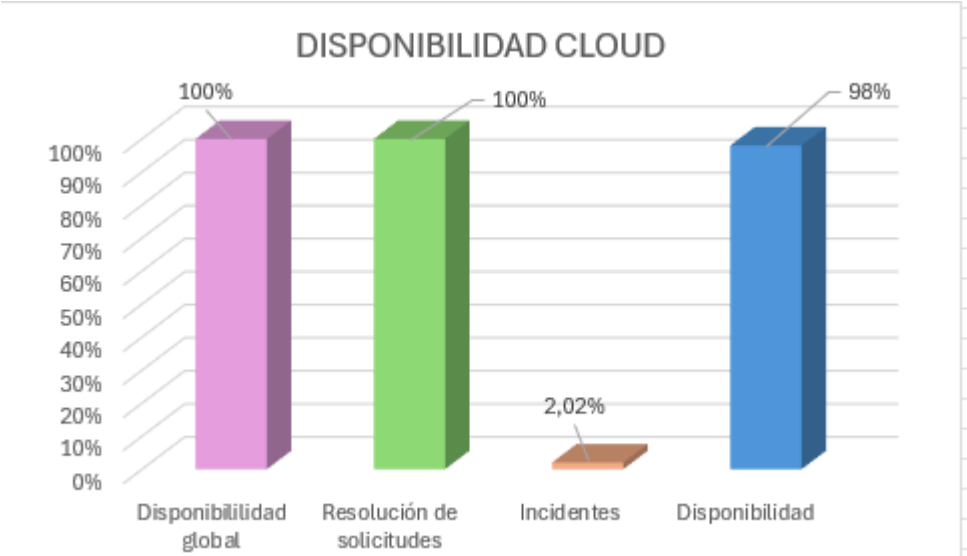
- **Capacitación SST:** líneas de OC 16 y 38
- **Cobro coactivo:** líneas de OC 17 y 38
- **core-impact:** Línea de OC 12
- **Efinomina:** Líneas de OC 14,18,26,27,38 y 39
- **Fuse:** Línea OC 17
- **Gestión grabaciones:** Líneas de OC 12,13, 14,15,17,19,20,22,23,25,28,35,36 y 38
- **InsightVM console:** 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_SEPTIEMBRE_2024.xls**" para ver el detalle "maquinas")

7.DISPONIBILIDAD GLOBAL CLOUD DEL MES DE SEPTIEMBRE

Disponibilidad Global mes de SEPTIEMBRE	Numero de tickets mes de SEPTIEMBRE	Imputabilidad por ANS
	97 solicitudes	**2 solicitudes**
	0 incidentes	**0 incidentes**
100%	Total 97 tickets	2 tickets



CONTROL DOCUMENTAL

ELABORADO POR

Fecha	Autor	Ingeniero
03-10-2024	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 septiembre a30 de septiembre del 2024.

CONSUMO TOTAL HORAS MES DE SEPTIEMBRE	
• Casos Reportados Netsuite	119
Sesiones de Seguimiento	9
Sesiones de Trabajo	0
Casos Escalados Medio Digital - Whatsapp	13
Horas Disponibilidad del Recurso Fines de Semana	259
Total Horas Consumidas de las 300 - Experto Master	400

2.INDICADORES DEL CENTRO CONSOLIDADO DE SERVICIOS

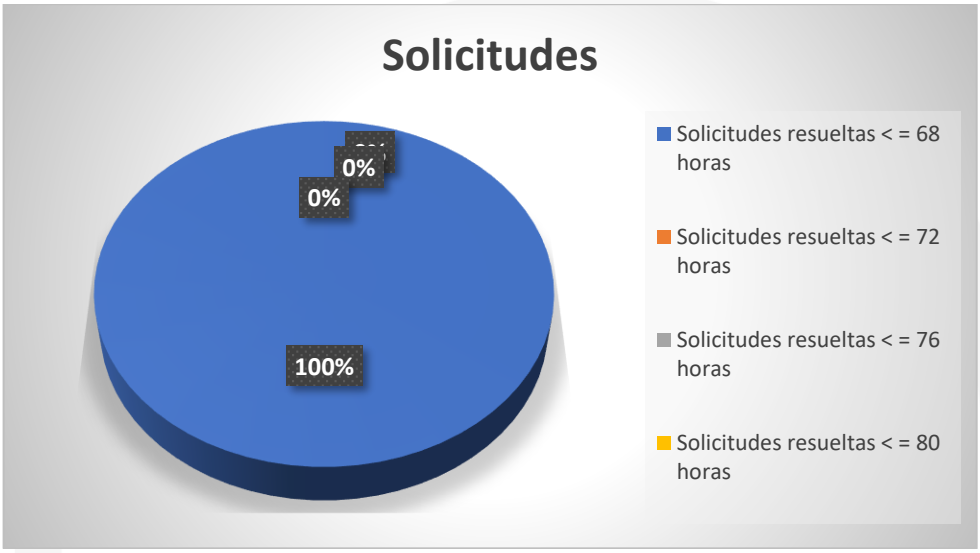
Con base en la información provista por el sistema de Netsuite, se elaboró el presente reporte el cual muestra el comportamiento de los problemas y requerimientos con enfoque en los días 01 enero a 30 de septiembre, para el **Consejo Superior de la Judicatura**. Estas mediciones se basan en el número de casos reportados por la aplicación.

	Volumen en 1 septiembre a
Casos Reportados	24
Solicitudes	24
Incidencias	0
WA – AF	0

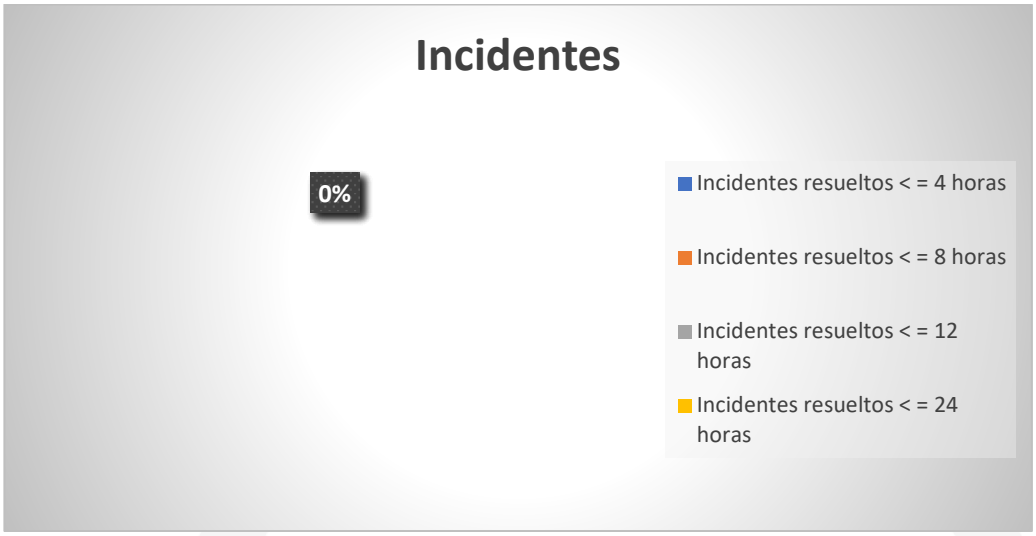
2.1 TASA DE RESOLUCIÓN DE PROBLEMAS

Tiempo de Gestión	Solicitudes
Solicitudes resueltas < = 68 horas	24
Solicitudes resueltas < = 72 horas	0
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	**24**

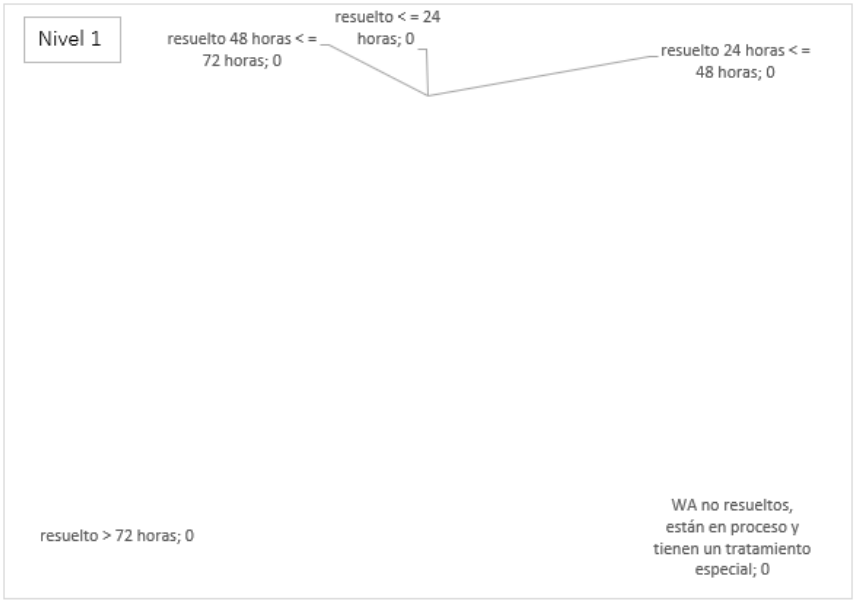


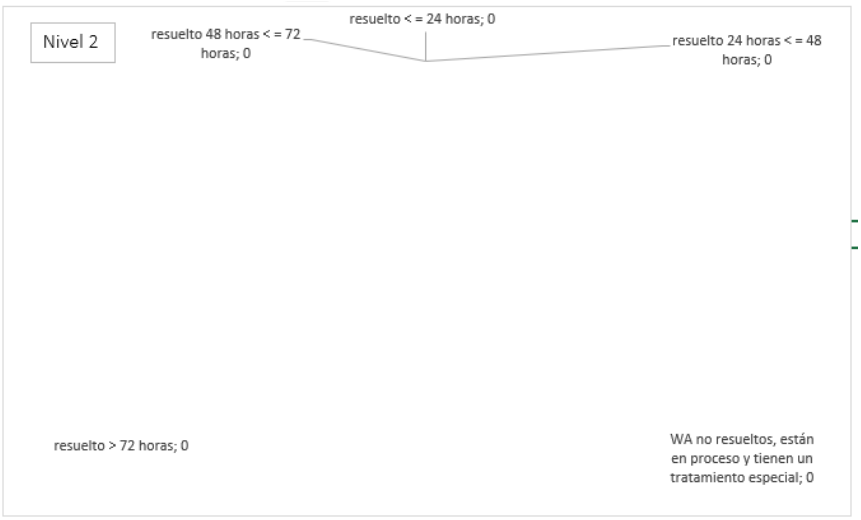
Tiempo de Gestión	Incidentes Penalizados
Incidentes resueltos < = 4 horas	0
Incidentes resueltos < = 8 horas	0
Incidentes resueltos <= 12 horas	0
Incidentes No resueltos < 24 horas	0
Total	**0**

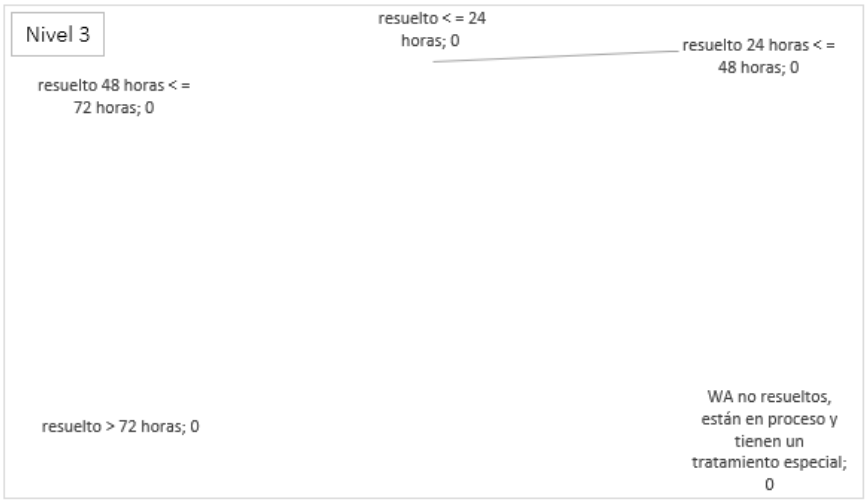


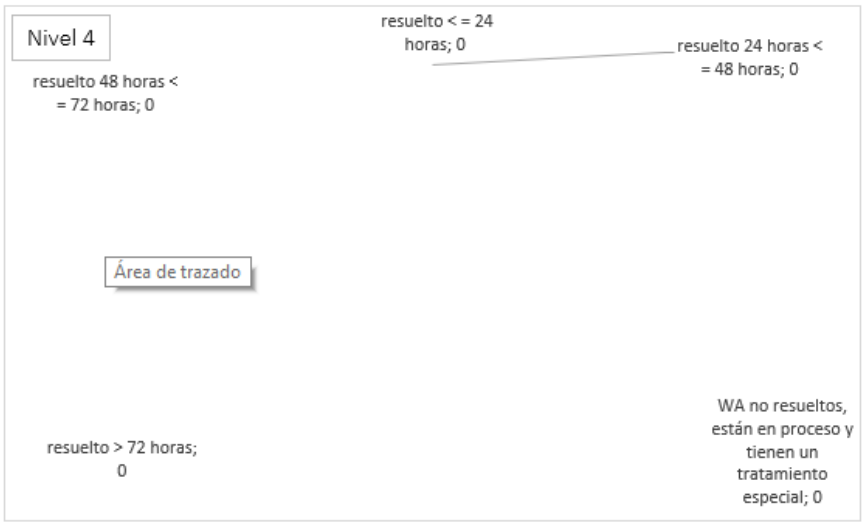
SID Penalizados: No aplica penalización

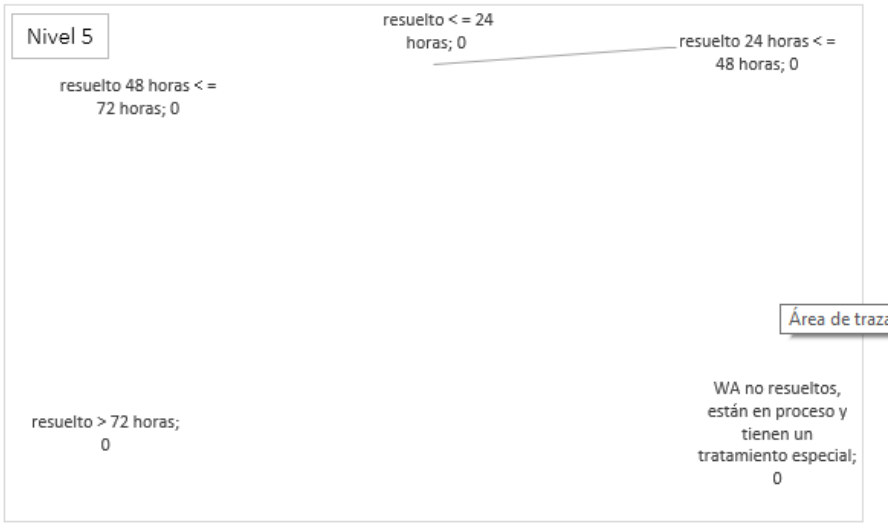
WA (Ajustes Funcionales)					
Tiempo de Gestión	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
resuelto < = 24 horas	0	0	0	0	0
resuelto 24 horas < = 48 horas	0	0	0	0	0
resuelto 48 horas < = 68 horas	0	0	0	0	0
resuelto > 68 horas	0	0	0	0	0
WA no resueltos, están en proceso y tienen un tratamiento especial	0	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 septiembre a 30 de septiembre 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 septiembre a 30 de septiembre 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 30 de septiembre 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	141	400	259
2024	141		
Solicitud	141		
Incidencia	0		
Total Horas Casos Reportados Netsuite	141	400	259
		259	259
		259	259
		259	259
		259	259
Horas consumidasde las 400 - Exp	400	400	0

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

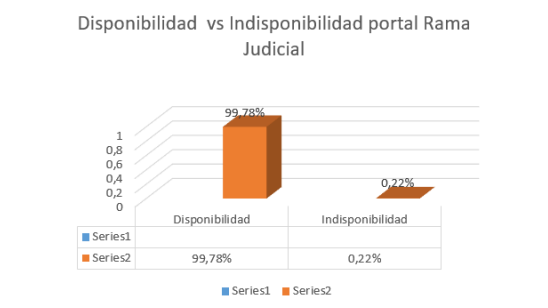
3. *DISPONIBILIDAD E INDISPONIBILIDAD DE LOS SERVICIOS DE HOSTING*

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:

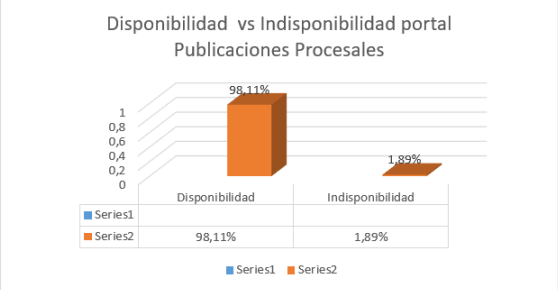
Portal Rama Judicial

Item	Aplicación	Disponibilidad	Indisponibilidad	Tiempo de duracion (Caida en horas)	Tiempo de duracion			
					Dias	Horas	Minutos	Segundos
1	Portal de la Rama Judicial	99,78%	0,22%	1,603888889	0	1	36	14
	Totales	99,78%	0,22%	1,603888889	**0**	1	36	14



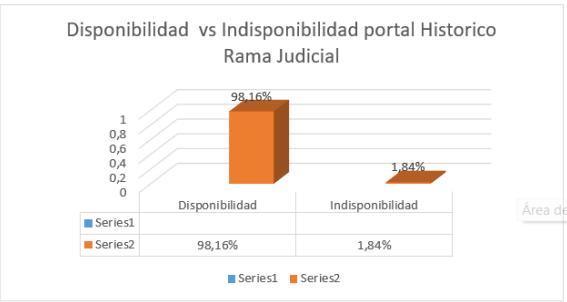
Portal Publicaciones Procesales

Item	Aplicación	Disponibilidad	Indisponibilidad	Tiempo de duracion (Caida en horas)	Tiempo de duracion			
					Dias	Horas	Minutos	Segundos
1	Publicaciones Procesales	98,11%	1,89%	13,59027778	0	13	35	25
	Totales	98,11%	1,89%	13,59027778	**0**	13	35	25



Portal Histórico Rama Judicial

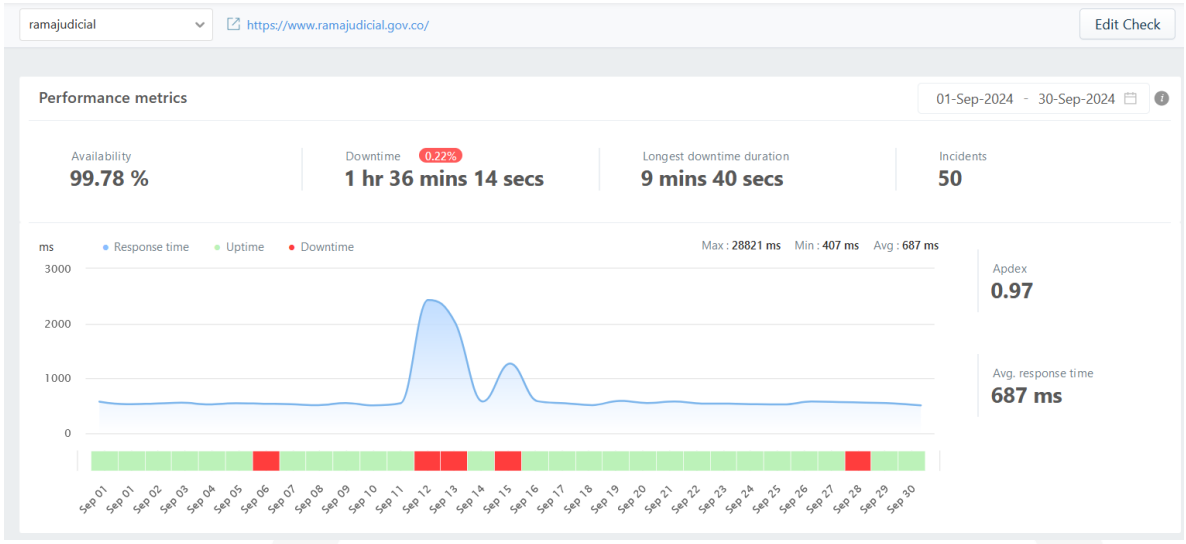
Item	Aplicación	Disponibilidad	Indisponibilidad	Tiempo de duracion (Caida en horas)	Tiempo de duracion			
					Dias	Horas	Minutos	Segundos
1	Portal Historico	98,16%	1,84%	13,23861111	0	13	14	19
	Totales	98,16%	1,84%	13,23861111	**0**	13	14	19



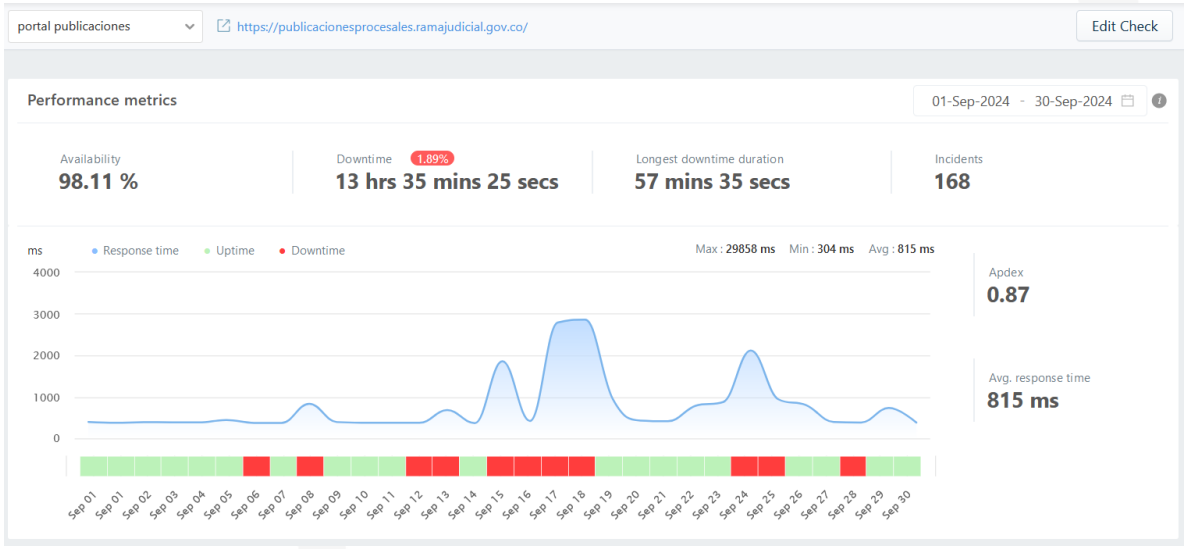
3.2 PORTAL DE LA RAMA JUDICIAL

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

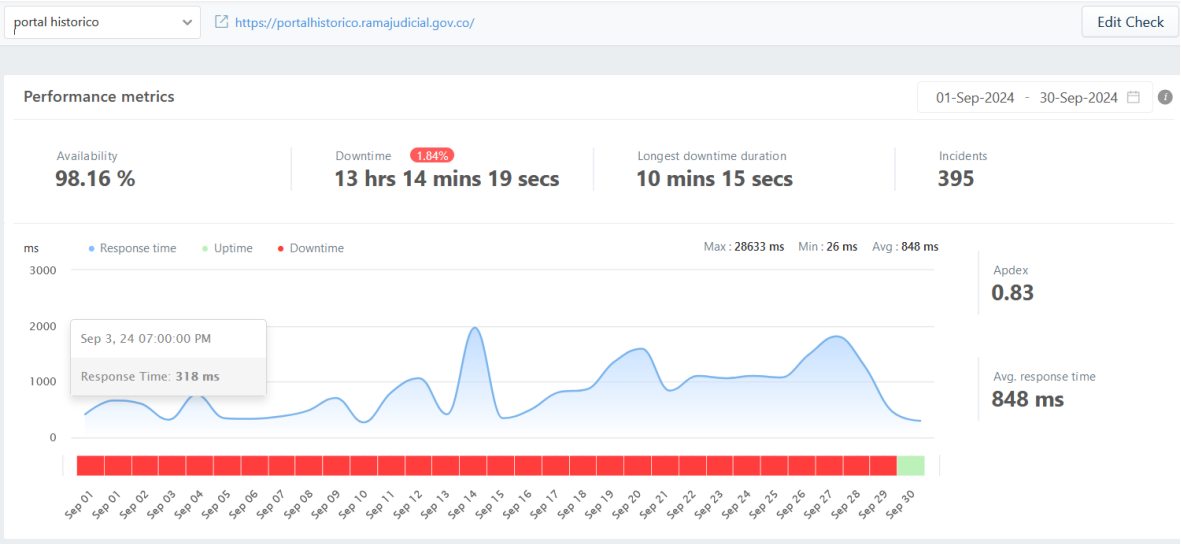
Portal Rama Judicial



Portal Publicaciones Procesales



Portal Histórico Rama Judicial



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	Tunning en datasources	18/09/2024		Desarrollo IFX
2	Ajustes en Índices de Base de Datos	27/09/2024		Equipo UTDI

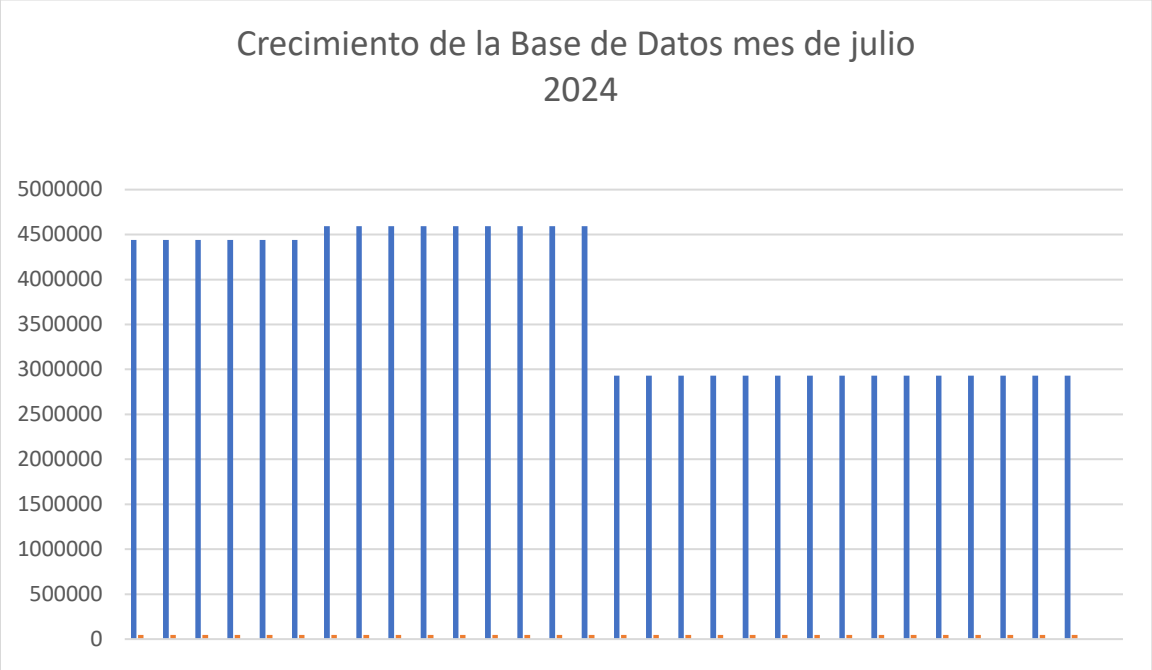
3.2.2 CRECIMIENTO DE LA BASE DE DATOS – INSTANCIA CSJPORTALDB01

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 septiembre.

BASE DE DATOS lportalramaprod

TAMAÑO (MB0	FECHA	AUMENTO TAMAÑO (MB) POR DIA
4440187 MB	01/09/2024	0
4440187 MB	02/09/2024	0
4440187 MB	03/09/2024	0
4440187 MB	04/09/2024	0
4440187 MB	05/09/2024	0
4440187 MB	06/09/2024	151530
4591717 MB	07/09/2024	0
4591717 MB	08/09/2024	0
4591717 MB	09/09/2024	0
4591717 MB	10/09/2024	0
4591717 MB	11/09/2024	0
4591717 MB	12/09/2024	0
4591717 MB	13/09/2024	0
4591717 MB	14/09/2024	0
4591717 MB	15/09/2024	-1662719
2928998 MB	16/09/2024	0
2928998 MB	17/09/2024	0
2928998 MB	18/09/2024	0
2928998 MB	19/09/2024	0
2928998 MB	20/09/2024	0
2928998 MB	21/09/2024	0
2928998 MB	22/09/2024	0
2928998 MB	23/09/2024	2511
2931509 MB	24/09/2024	-2511
2928998 MB	25/09/2024	0
2928998 MB	26/09/2024	0
2928998 MB	27/09/2024	0
2928998 MB	28/09/2024	0
2928998 MB	29/09/2024	412
2929410 MB	30/09/2024	0
		0

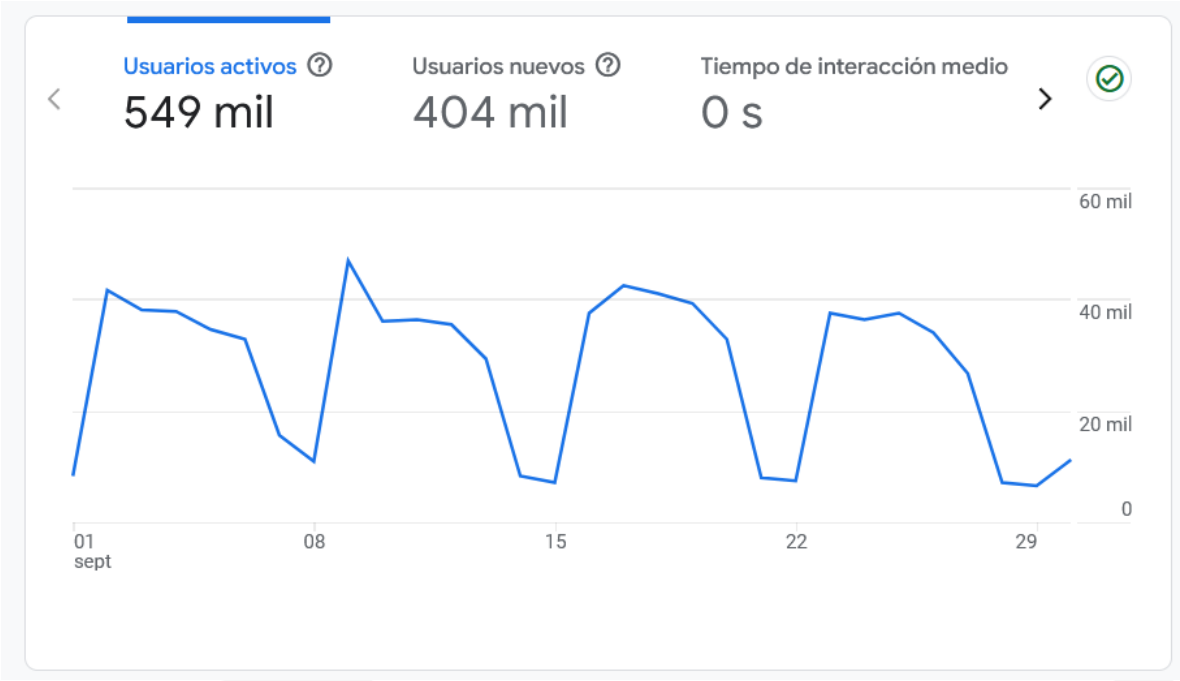
Grafica del crecimiento de la BD Iportalramaprod de la INSTANCIA CSJPORTALB01



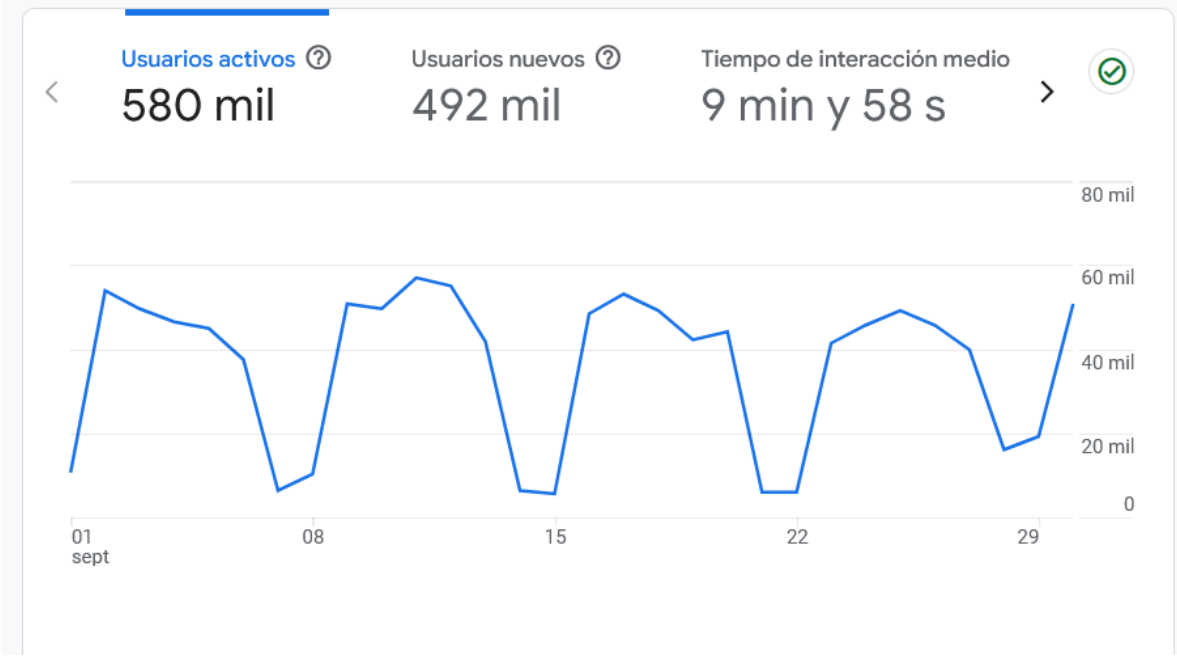
*4. **ESTADISTICAS PORTAL DE LA RAMA JUDICIAL***

4.1 RESUMEN DEL PORTAL

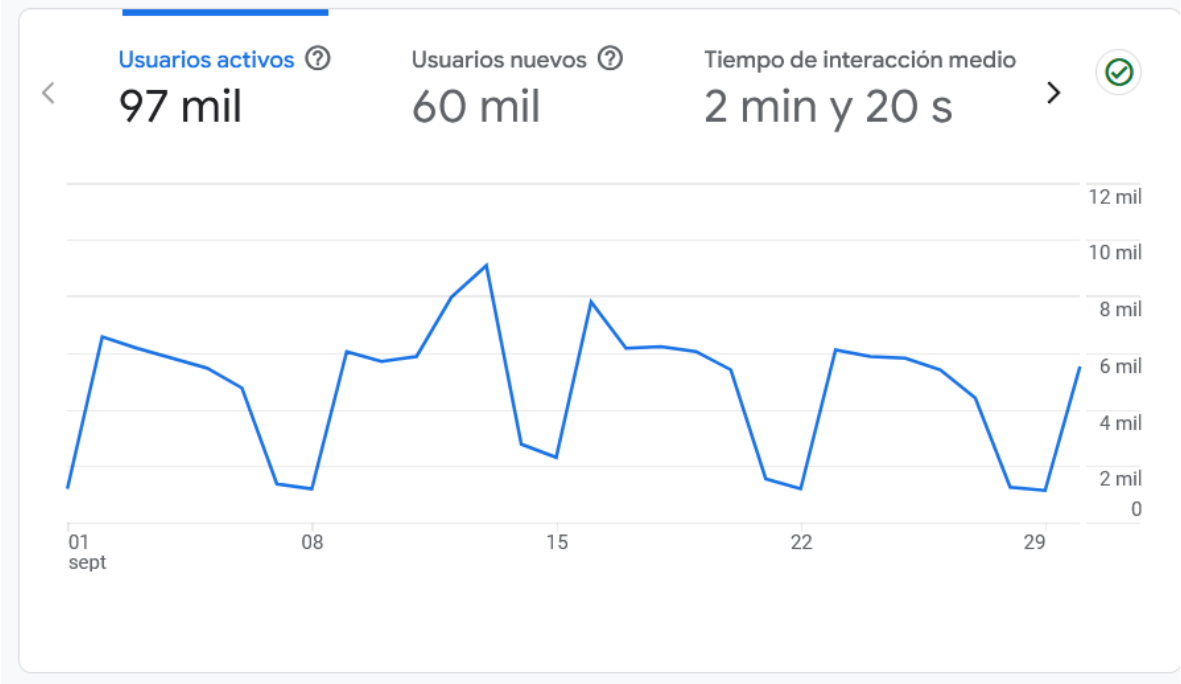
En la respectiva grafica se observa un comportamiento constante durante el mes de septiembre para el portal Rama Judicial.



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



En la respectiva grafica se observa un comportamiento constante durante el mes de septiembre 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					

14.1. 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
Jose Luis Cardenas Rozo
Victor Hugo Galvis Botia

Estas horas se destinan 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	9/20/2024 18:34	9/20/2024 18:54	1	Diurna	TT898974 RV: Permisos conectividad VPN SIRNA - AZURE
2	9/20/2024 21:00	9/20/2024 5:03	8	Nocturna	TT898848 asistencia a ventana el día de hoy 20/09/2024 desde las 9 pm; TT899001 RV: [MEDIA] ID: 37561 || IDS-EXE-CSIN-002: NetLing GPON ONT routers Command Injection Vulnerability Exploit | TT899002 RV: Habilitación de acces"Soporte On Site" <soporte@corteconstitucional.gov.co>o sin restricción de navegación
Total horas Extras			9		

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					
2					
Total horas Extras			0		

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	6/9/2024 18:00	6/9/2024 19:00	1	Diurna	TT891615 Ventana parcheo servidores portal 06092024 RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA
2	9/9/2024 19:00	9/9/2024 20:00	1	Nocturno	Politicas Azure all to all - Desactivación de VPN Azure
3	10/9/2024 21:00	10/9/2024 22:00	1	Nocturno	TT893535 Configuracion politica
4	29/9/2024 11:00:00 am	29/9/2024 1:00:00 pm	2	Diurna	Solicitud urgente de revisión evento de seguridad
5	29/9/2024 8:00:00 pm	29/9/2024 9:00:00 pm	1	Diurna	Actualiación de equipos Cloud
6	30/9/2024 8:00:00 pm	30/9/2024 8:00:00 pm	2	Diurna	Permisos Servidores Linux IFX Tierras permisos de Navegación y Vpn Solicitud Intermitencia de la red
Total horas Extras			8		

14.2. 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

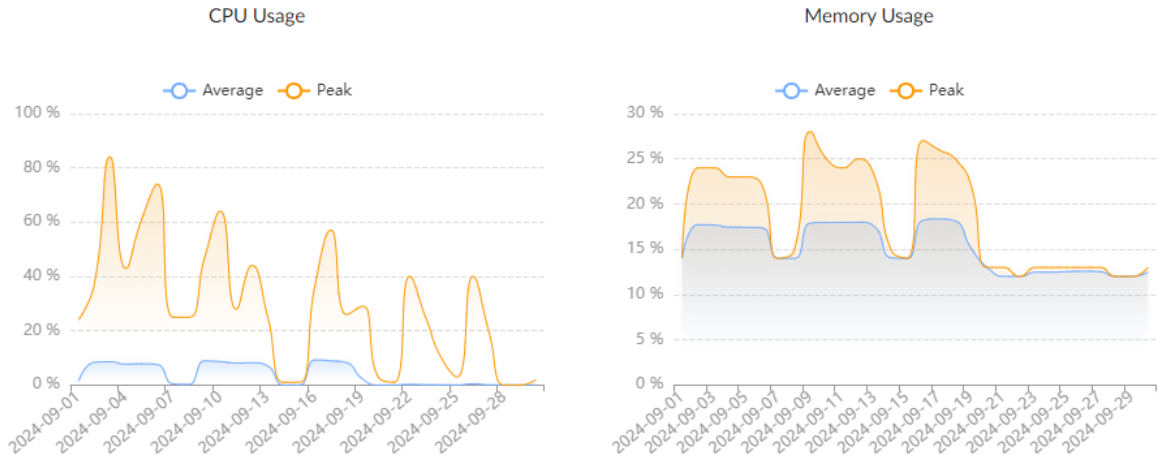
14.3. Actualización de firmware.

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

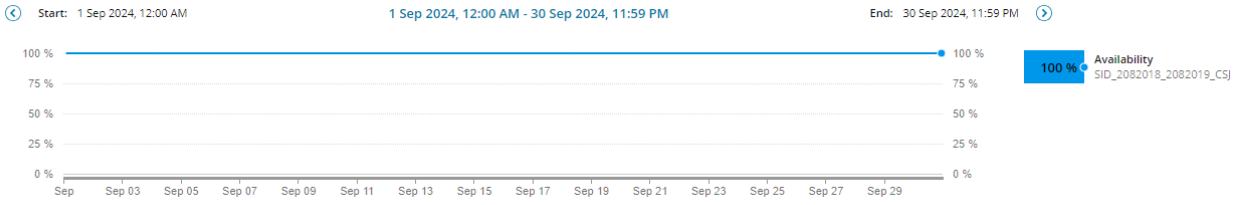
Durante septiembre, el consumo promedio de CPU y memoria (traza azul) en el firewall perimetral estuvieron dentro de sus valores de operación normal.



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.

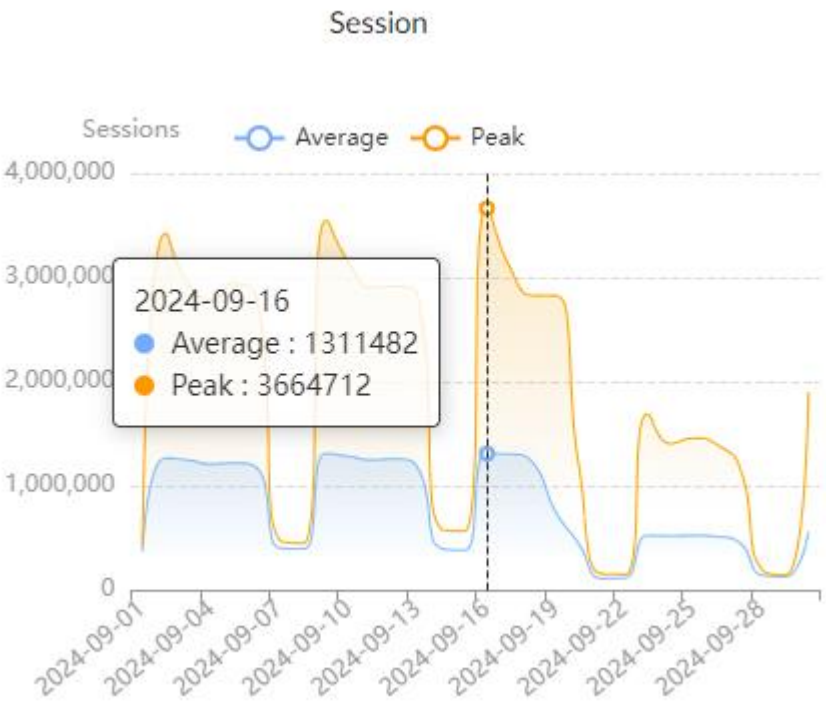
15.1. Disponibilidad mensual firewall perimetral.

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



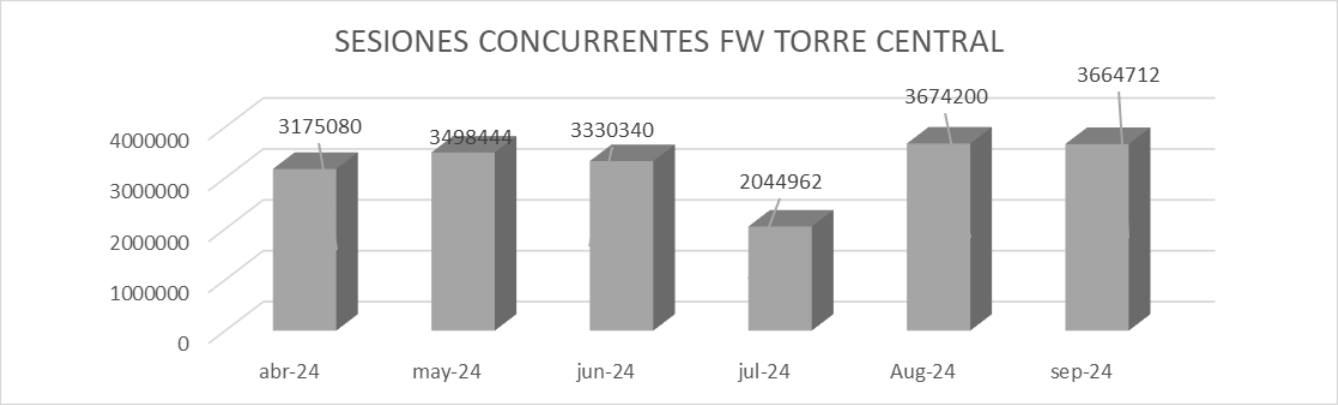
15.2. Cantidad de sesiones firewall perimetral.

Durante septiembre se presentó un máximo de 3664712 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 septiembre se presentó un incremento en las sesiones en el FW perimetral correspondientes a 3664712 sesiones:



MES	SESIONES
MES	SESIONES
abr-24	3175080
may-24	3498444
jun-24	3330340
jul-24	2044962
Aug-24	3674200
sep-24	3664712

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

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

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	HTTPS			218.73 TB
2	Amazon-AWS			118.34 TB
3	Microsoft.SharePoint			83.19 TB
4	SSL			37.63 TB
5	Microsoft.Teams			35.03 TB
6	Microsoft.365.Portal			25.74 TB
7	OneDrive			22.36 TB
8	Microsoft.Portal			20.24 TB
9	WhatsApp			19.52 TB
10	Microsoft.Outlook			19.19 TB

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

Top Applications by Sessions

#	Application	Sessions
1	DNS	3,409,857,252
2	SMB	2,160,570,065
3	HTTPS	1,183,025,325
4	TCP/UDP_8037	711,047,131
5	Microsoft.365.Portal	613,994,646
6	Microsoft.Portal	558,482,410
7	SSL	540,790,739
8	Microsoft.Windows.Update	537,607,273
9	HTTP	451,386,162
10	SQUID	450,394,879

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

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 septiembre:

Top Bandwidth IP

#	IP	Bandwidth
1	172.16.182.85	5.55 TB
2	10.101.100.114	4.58 TB
3	10.101.100.38	2.64 TB
4	172.29.175.46	2.38 TB
5	10.101.101.54	1.96 TB
6	192.168.213.44	1.75 TB
7	10.101.100.34	1.33 TB
8	10.101.101.246	1.22 TB
9	10.101.101.146	1.09 TB
10	10.101.102.6	1.00 TB

15.6. Top de destinos web por sesiones firewall perimetral.

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

Top Destinations by Sessions

#	Hostname(or IP)	Sessions
1	8.243.164.21	447,773,449
2	8.243.164.19	433,752,683
3	172.28.107.61	376,868,168
4	172.28.107.71	344,023,930
5	192.168.213.94	314,405,143
6	microsoft.com	282,488,039
7	172.28.107.58	211,707,871
8	172.16.182.100	210,965,759
9	windowsupdate.com	184,835,099
10	172.29.130.220	131,914,420

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

172.16.56.165 de la sede Valle, Cali; Entreceibas, Calle 8 # 1-16, presentó la mayor cantidad de peticiones bloqueadas durante septiembre:

Top Web Users by Blocked Requests

#	User (or IP)	Hostname	Requests
1	172.16.56.165	172.16.56.165	8,421,130
2	172.28.86.176	172.28.86.176	2,246,018
3	172.28.162.147	172.28.162.147	2,232,583
4	172.16.33.29	172.16.33.29	2,138,957
5	172.27.171.222	172.27.171.222	1,886,794
6	192.168.193.151	192.168.193.151	1,824,099
7	172.25.110.163	172.25.110.163	1,803,081
8	192.168.46.197	192.168.46.197	1,688,565
9	172.28.5.202	172.28.5.202	1,613,013
10	172.29.6.18	172.29.6.18	1,520,655

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.

Streaming Media and Download e Internet Radio and TV fue la categoría con mayor cantidad de bloqueos durante septiembre.

Top Blocked Web Categories

#	Category	Requests
1	Streaming Media and Download	71,264,938
2	Internet Radio and TV	7,771,454
3	Social Networking	6,610,490
4	Proxy Avoidance	5,025,992
5	Games	2,898,454
6	Unrated	2,737,045
7	Entertainment	369,187
8	Information Technology	364,206
9	Malicious Websites	317,566
10	Society and Lifestyles	298,157

15.9. Top de IP más activos Firewall Perimetral

Los hosts con mayor cantidad de peticiones durante septiembre 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	10,253,002
2	10.101.100.38	6,526,274
3	10.101.101.246	6,400,434
4	10.101.100.34	5,681,849
5	10.101.100.194	5,201,206
6	10.101.101.54	4,710,260
7	10.101.101.50	4,254,826
8	10.101.100.98	4,202,513
9	10.101.102.6	3,943,623
10	10.101.100.134	3,565,209

15.10. Top de categorías más visitadas Firewall Perimetral

La categoría más visitada durante septiembre fue Information Technology:

Top Allowed Web Categories

#	Category	Requests
1	Information Technology	368,900,825
2	Overrride_permitidas	491,555

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

Las maquinas con IP 172.28.107.87 que corresponde al traspaso de información de TX_400TB-AWS de la nube privada de IFX, presentó el mayor consumo de ancho de banda durante septiembre:

Top IP by Bandwidth

#	IP	Bandwidth	Sent	Received
1	172.28.107.87			98.40 TB
2	172.28.107.80			58.43 TB
3	172.28.107.79			49.50 TB
4	172.28.107.88			25.74 TB
5	172.28.107.84			21.25 TB
6	172.17.201.251			9.41 TB
7	172.16.182.85			5.54 TB
8	172.27.64.14			5.42 TB
9	10.101.100.114			5.08 TB
10	172.17.201.252			4.82 TB

16. TRÁFICO VPN FIREWALL PERIMETRAL

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

InformeVPNssl_EDWSI(SSL - Dialup IPsec)

#	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	cvillam	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-09-30 23:56:26	1727740586	181.55.51.20	163	675:52:53	7.23 GB	761978171	7006240663
2	Ecoralb	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-09-30 23:59:10	1727740750	186.154.96.194	178	669:36:47	21.97 GB	2722612094	20870661499
3	vperezg	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-09-30 23:57:05	1727740625	129.222.203.156;138.84.40.119;138.84.40.122;138.84.40.22;138.84.40.81;138.84.41.169;138.84.41.174;138.84.41.185;138.84.41.196;138.84.41.199;138.84.41.22	540	504:27:04	734.65 MB	554262969	216068867
4	pfajardg	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-09-30 23:54:20	1727740460	186.81.100.20	80	448:09:44	15.67 GB	1012812085	15817709396

5	ssuareza	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-09-30 23:40:19	1727739619	181.58.39.249;181.58.39.80;191.156.36.17;191.156.41.159	229	431:38:12	4.19 GB	454272378	4049323295
6	lcardenas	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-09-30 22:33:31	1727735611	200.118.63.31	140	399:11:37	46.90 GB	4974663203	45387646679
7	lbarrerf	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-09-30 18:35:54	1727721354	186.155.111.38;186.155.117.107;186.155.45.99;190.27.248.59;191.156.234.149;191.156.234.159;200.119.50.236	112	334:49:47	39.18 GB	2102688183	39965126078
8	csichaca	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel;ssl-web	2024-09-30 23:51:36	1727740296	132.255.23.26;172.29.100	89	334:02:25	5.07 GB	467978046	4976759230
9	lmarinmo	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-10-01 00:01:14	1727740874	181.136.237.173	114	322:47:51	5.62 GB	520904962	5511478055
10	jmonteas	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-09-30 21:40:01	1727732401	167.0.72.207;179.33.128.28;179.33.133.247;179.33.65.174;186.112.50.39;186.112.56.8	164	281:48:49	19.13 GB	1184145591	19358191785

16.1. VPN IPSEC Site To Site Firewall Perimetral

El consumo de ancho de banda de las VPN IPSec Site to Site durante septiembre 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	604201	5757713796637	613312825243	5144400971394
2	VPN_SIUG_AWS	34.194.187.190	190.217.24.4	604201	698558709716	48254556650	650304153066
3	VPN_SIUG_AWS-2	34.224.152.152	190.217.24.4	604201	75230370716	7588203407	67642167309
4	VPN_ORACLE	129.213.6.36	190.217.80.4	604201	59872041414	50071211650	9800829764
5	VPN_Tierras	181.225.76.196	190.217.24.4	604180	19851599052	19300691340	550907712
6	VPN_AZURE-ANALY	20.124.34.235	190.217.24.4	604201	13538839570	1536521647	12002317923
7	VPN_Linktic	3.222.171.115	190.217.24.4	604191	644538150	617428881	27109269
8	VPN_INPEC	190.25.112.10	190.217.19.156	604201	217869827	182025099	35844728
9	VPN_REGISTRADU	201.232.123.20	190.217.24.4	603892	187565889	108911758	78654131
10	VPN_FISCALIA	190.157.218.66	190.217.24.4	604200	11427154	10956388	470766
11	VPN_AZURE-VWAN2	4.153.117.131	190.217.24.4	604201	4155180	2839428	1315752
12	VPN_AZURE-VWAN	4.153.117.133	190.217.24.4	604201	1522584	1522584	0

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

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

Top Attacks

#	Attack Name	Severity	CVE-ID	Counts
1	Spring.Framework.SerializationUtils.Insecure.Deserialization	Critical	CVE-2022-22965	341,216
2	Adobe.ColdFusion.Multiple.Vulnerabilities	Critical	CVE-2013-0625,CVE-2013-0629,CVE-2013-0631,CVE-2013-0632	66,628
3	tcp_syn_flood	Critical		64,768
4	Apache.Log4j.Error.Log.Remote.Code.Execution	Critical	CVE-2021-4104,CVE-2021-44228,CVE-2021-45046	60,348
5	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	Critical	CVE-2017-11317,CVE-2017-11357,CVE-2019-18935	44,486
6	HTTP.URI.Java.Expression.Language.Code.Injection	Critical	CVE-2021-22053,CVE-2022-26134	43,826
7	Ivanti.EPMM.CVE-2023-35082.Authentication.Bypass	Critical	CVE-2023-35082	43,763
8	Remote.CMD.Shell	Critical		42,925
9	F5.BIG-IP.Traffic.Management.User.Interface.Path.Traversal	Critical		42,757
10	Zabbix.Frontend.CVE-2022-23131.Privilege.Elevation	Critical	CVE-2022-23131	42,453

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

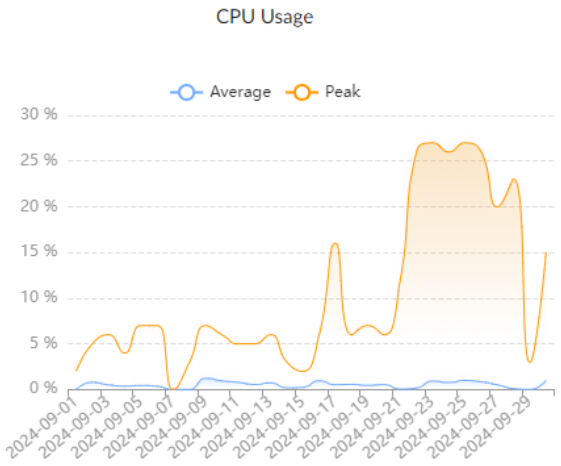
Top Intrusion Victims

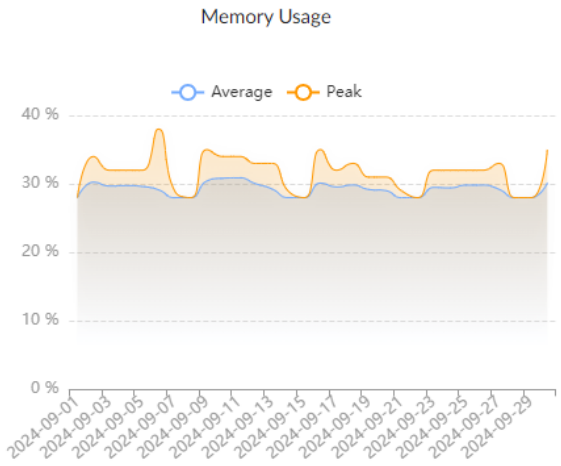
#	Attack Victim	Counts	Critical	High	Medium	Percent of Total Attacks
1	172.17.202.30				28,258,628	33.07%
2	172.17.201.6				28,254,368	33.06%
3	172.17.202.151				28,248,199	33.06%
4	172.17.201.68				196,509	0.23%
5	172.17.201.13				128,084	0.15%
6	172.17.201.52				91,594	0.11%
7	192.168.89.28				56,588	0.07%
8	172.17.201.61				48,749	0.06%
9	190.217.24.176				40,090	0.05%
10	190.217.24.175				30,523	0.04%
11	190.217.24.15				22,590	0.03%
12	172.17.201.101				20,052	0.02%
13	34.29.85.190				11,610	0.01%
14	192.168.213.94				9,418	0.01%
15	34.16.47.102				8,993	0.01%
16	172.17.201.100				8,347	0.01%
17	172.17.202.73				4,737	0.01%
18	172.17.201.33				4,701	0.01%
19	66.23.203.210				4,108	0.00%
20	172.17.201.54				4,021	0.00%

Los hosts 172.17.201.X, 172.17.202.X, son aplicaciones web protegidas por los WAF Torre Central y el WAF CAN. Se debe verificar los demás hosts con software antivirus

17. FIREWALL SEDE PALACIO

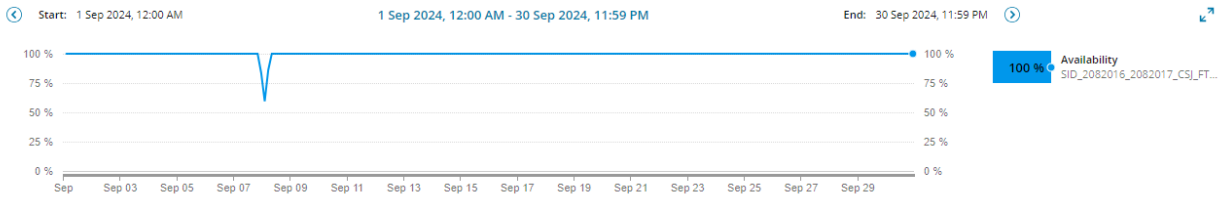
Durante septiembre, el consumo de CPU y memoria en el Firewall de Palacio se mantuvo dentro de sus valores de operación normal.



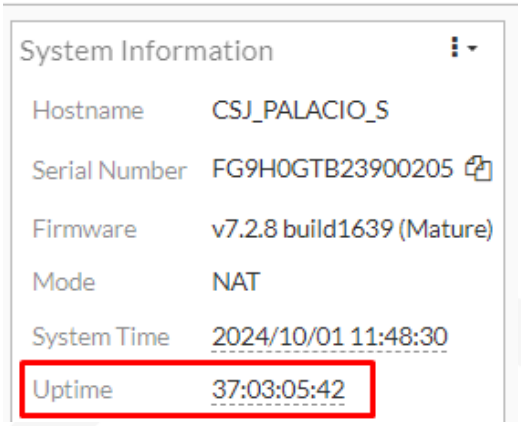


17.1. Disponibilidad Mensual Firewall Palacio

Durante septiembre se obtuvo 100% de disponibilidad en el servicio firewall Palacio. El evento del 8 de septiembre puede suceder por intermitencias en la red MPLS de CSJ, pero los equipos estuvieron disponibles 100%



Días sin caídas de equipo Firewall 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%.

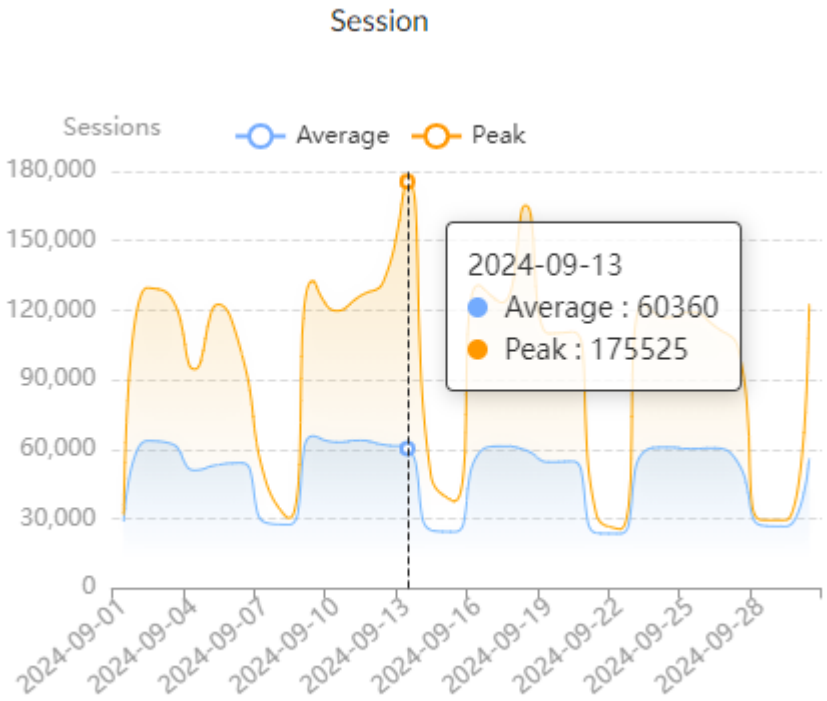
Un valor más exacto de la disponibilidad 99.699 %

Availability Statistics

PERIOD	AVAILABILITY
Today	100.000 %
Yesterday	100.000 %
Last 7 Days	100.000 %
Last 30 Days	99.704 %
This Month	100.000 %
Last Month	99.699 %

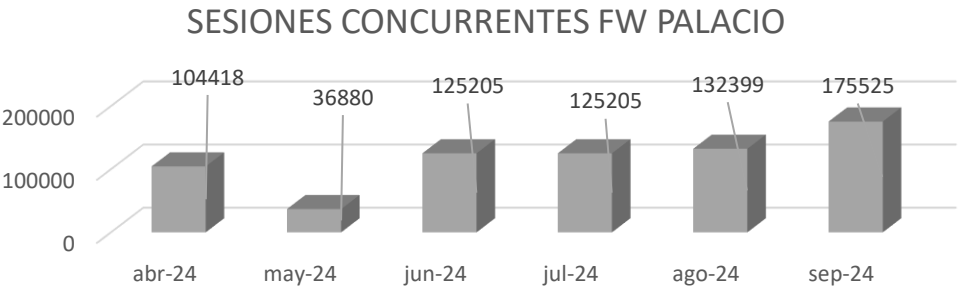
17.2. Cantidad de Sesiones Firewall Palacio

Durante septiembre se presentó un máximo de 175525 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

Sesiones concurrentes



MES	SESIONES
abr-24	104418
may-24	36880
jun-24	125205
jul-24	125205
ago-24	132399
sep-24	175525

17.4. Aplicaciones y protocolos por ancho de banda firewall Palacio

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

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	Microsoft.Portal			18.63 TB
2	Microsoft.SharePoint			7.26 TB
3	HTTPS.BROWSER			3.79 TB
4	OneDrive			3.18 TB
5	SSL			3.07 TB
6	Microsoft.365.Portal			1.35 TB
7	Microsoft.Outlook			1.20 TB
8	Microsoft.Teams			856.98 GB
9	Apple.Services			750.38 GB
10	HTTPS			727.56 GB

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

Top Applications by Sessions

#	Application	Sessions
1	SMB	412,536,706
2	DNS	59,178,857
3	HTTP.BROWSER	47,717,213
4	Microsoft.365.Portal	38,762,143
5	Microsoft.Windows.Update	34,306,719
6	SSL	34,053,962
7	Microsoft.Portal	31,612,964
8	HTTPS.BROWSER	25,972,324
9	tcp/44345	20,904,650
10	Microsoft.Outlook	18,103,796

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 septiembre:

Top Bandwidth IP

#	IP	Bandwidth
1	172.28.93.2	9.46 TB
2	172.16.2.59	536.78 GB
3	172.28.92.36	519.22 GB
4	172.16.4.66	511.90 GB
5	172.16.5.33	457.76 GB
6	172.28.93.51	444.50 GB
7	172.28.92.23	440.09 GB
8	172.28.92.31	420.85 GB
9	192.168.2.209	413.18 GB
10	172.28.92.13	347.40 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 (Microsoft Sharepoint) y 190.217.24.42 (apigestionaudiencias) y fueron destinos más visitados durante septiembre:

Top Websites and Category by Bandwidth

#	Site	Category	Bytes
1	20.60.0.104		8.63 TB
2	13.107.136.10		4.14 TB
3	13.107.138.10		3.50 TB
4	190.217.24.42		1.11 TB
5	172.190.220.253		968.14 GB
6	cndjdisciplinaenlinea.file.core.windows.net		844.03 GB
7	20.168.235.216		652.23 GB
8	20.60.128.228		636.55 GB
9	13.107.246.40		494.62 GB
10	52.239.171.228		351.17 GB

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

172.16.6.57, 172.16.6.79 y 172.16.6.49 (hosts de la LAN Palacio) presentaron la mayor cantidad de conexiones bloqueadas durante septiembre.

Top Web Users by Blocked Requests

#	User (or IP)	Hostname	Requests
1	172.16.6.57	172.16.6.57	358,338
2	172.16.6.79	172.16.6.79	344,339
3	172.16.6.49	172.16.6.49	254,470
4	172.16.5.3	172.16.5.3	242,563
5	172.16.4.103	172.16.4.103	110,890
6	172.16.2.8	172.16.2.8	80,909
7	172.16.6.161	172.16.6.161	80,027
8	172.29.136.13	172.29.136.13	76,275
9	172.16.4.182	172.16.4.182	61,501
10	172.16.6.109	172.16.6.109	59,795

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 septiembre en el firewall Palacio fueron Unrated, Social Network y Proxy Avoidance:

Top Blocked Web Categories

#	Category	Requests
1	Unrated	8,863,881
2	Social Networking	800,330
3	Proxy Avoidance	795,624
4	Streaming Media and Download	430,920
5	Phishing	335,855
6	Games	90,421
7	Newly Observed Domain	51,405
8	Entertainment	43,598
9	Society and Lifestyles	35,252
10	Newsgroups and Message Boards	16,497

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 septiembre:

Top Web IP by Allowed Requests

#	IP	Requests
1	172.16.4.90	24,218,722
2	172.28.54.20	14,447,725
3	172.16.4.100	769,894
4	192.168.8.19	660,276
5	172.16.5.100	579,569
6	172.16.2.99	468,671
7	172.16.5.68	461,490
8	172.17.114.39	443,588
9	172.16.6.121	437,408
10	192.168.8.24	388,002

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	31,950,195
2	Search Engines and Portals	5,311,294
3	Business	1,780,936
4	Information and Computer Security	824,532
5	Web Analytics	533,609
6	Web-based Applications	184,796
7	Overrride_permitidas	108,849
8	Finance and Banking	89,932
9	Online Meeting	49,740
10	Secure Websites	35,749

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 septiembre:

Top IP by Bandwidth

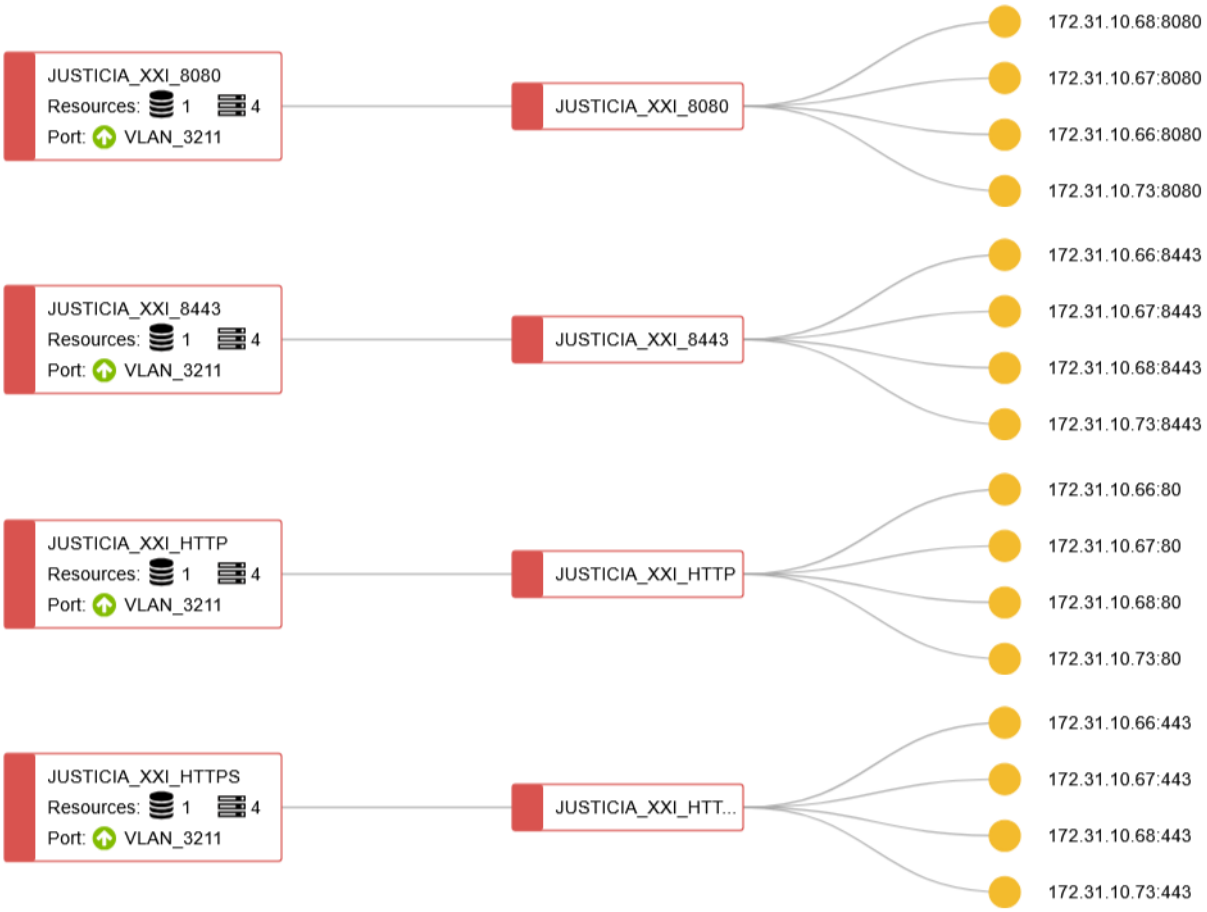
#	IP	Bandwidth	Sent	Received
1	172.28.93.2			9.44 TB
2	172.29.154.58			6.42 TB
3	172.16.6.92			847.96 GB
4	172.16.4.66			603.89 GB
5	172.28.92.15			594.77 GB
6	172.28.92.13			586.75 GB
7	172.29.65.72			580.23 GB
8	172.16.2.59			578.22 GB
9	172.28.92.36			511.69 GB
10	172.16.5.33			455.42 GB

18. BALANCEADOR DE CARGA FORTIADC

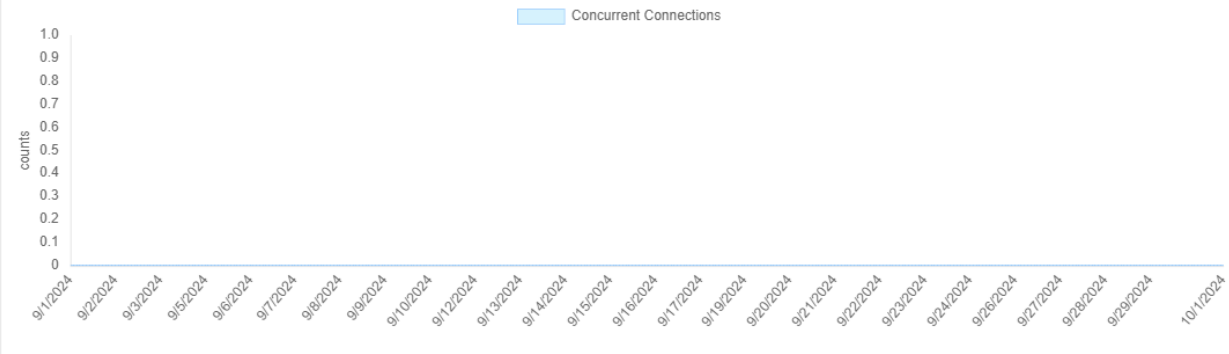
A continuación, se observan los diferentes servicios balanceados.

18.1. Justicia XXI

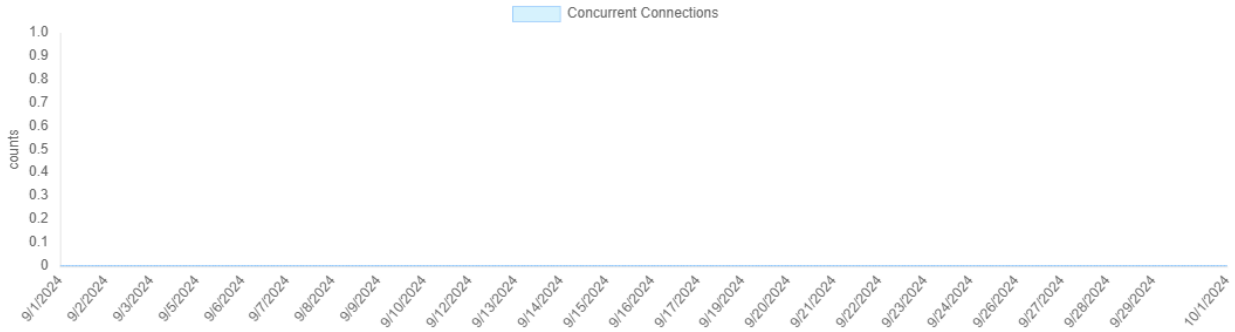
Se encuentra balanceado en el FortiADC:



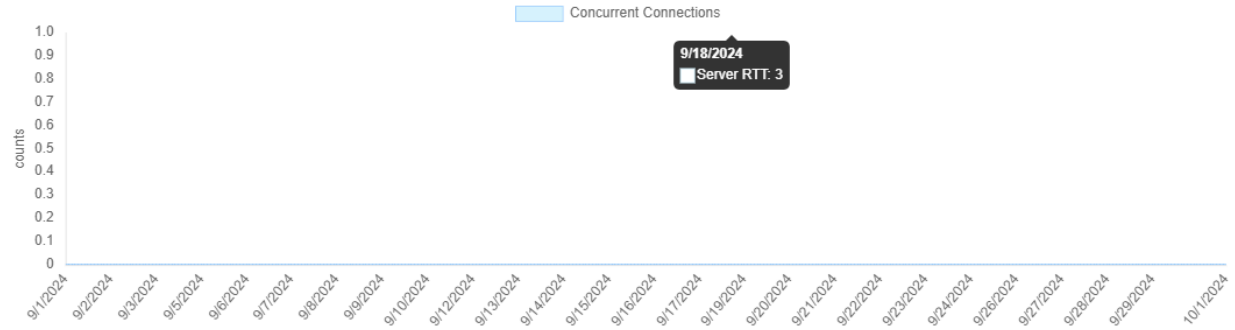
Durante septiembre no se presentó tráfico por el puerto 8080:



Conexiones concurrentes por el puerto 8443:



Conexiones concurrentes por el puerto 443:

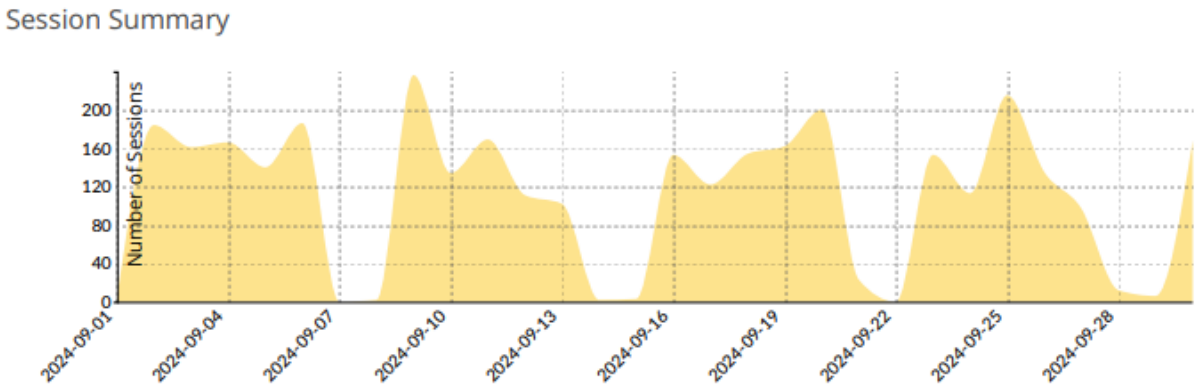


18.2. Kactus RDP

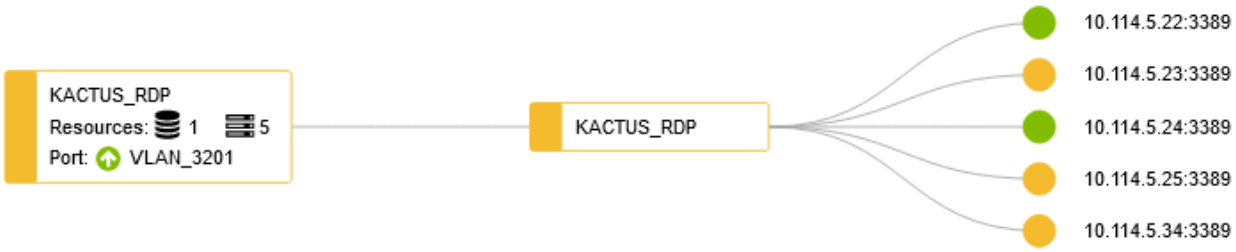
Esta aplicación se encuentra en el Firewall utilizando la siguiente configuración:

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

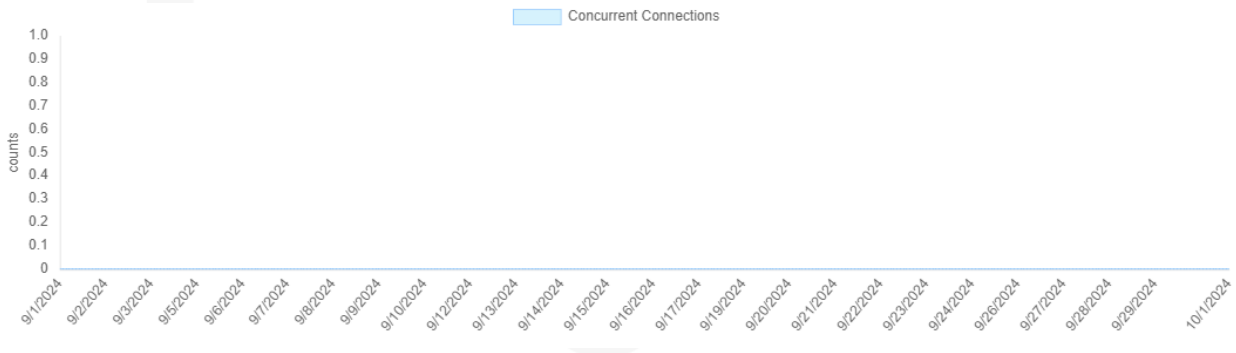
A continuación, se observa el número de sesiones concurrentes para este aplicativo.



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

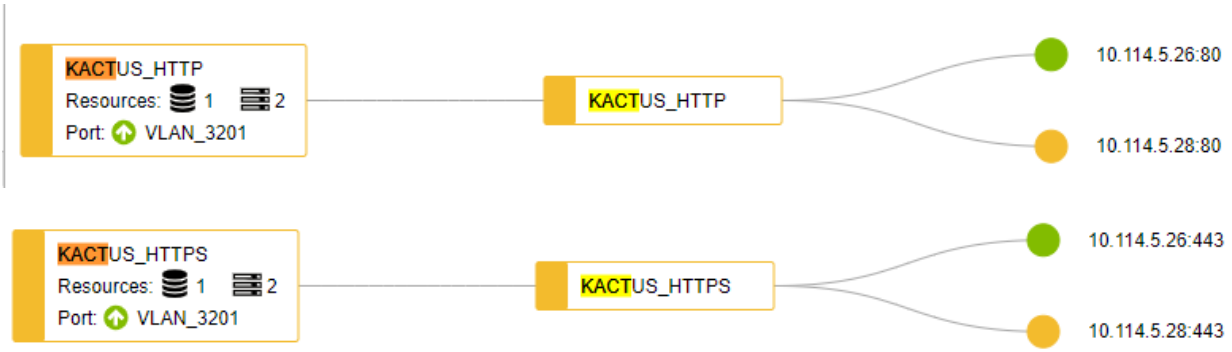


En el FortiADC no se observan sesiones concurrentes:

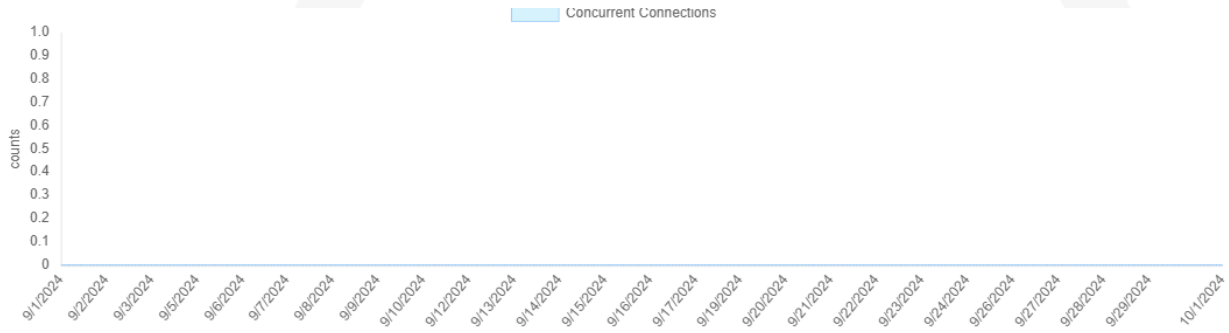


18.3. Kactus WEB

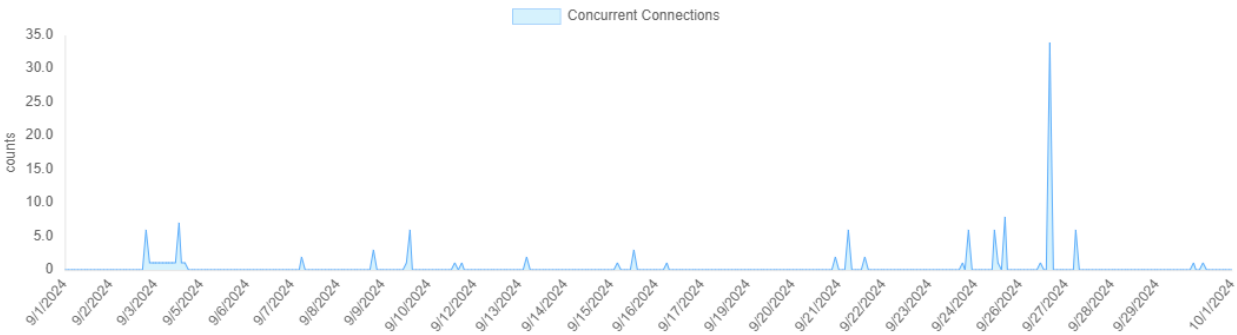
Se encuentra balanceado en el FortiADC:



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



Por HTTPS se observan las siguientes conexiones del mes:



18.4. SIRNA

Este servicio se encuentra balanceado en el FortiGate perimetral:

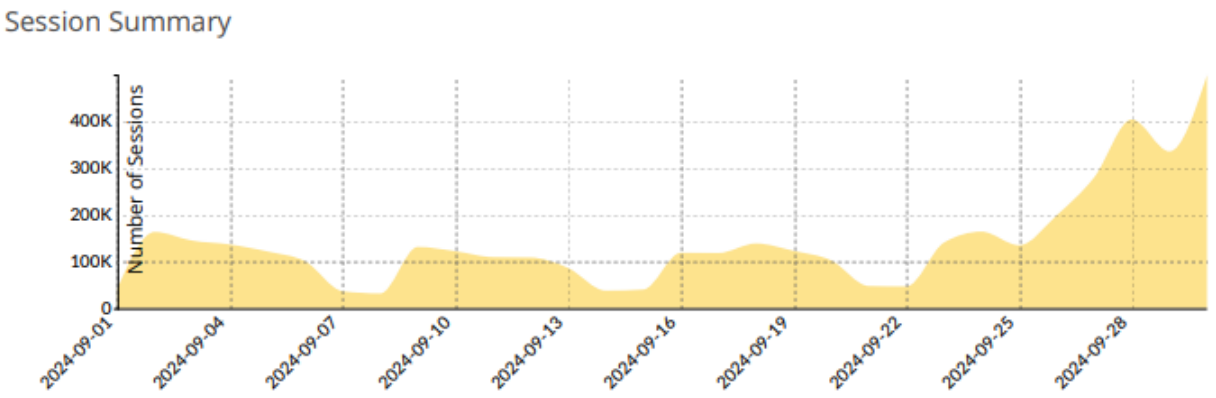
Configuración de balanceo de CRM en el Firewall.

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

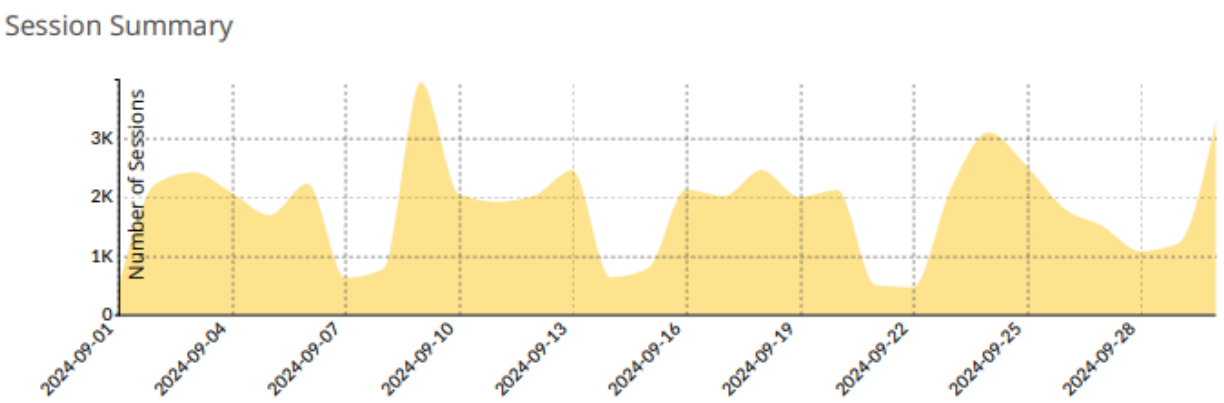
Configuración de balanceo de Sharepoint en el firewall perimetral.

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

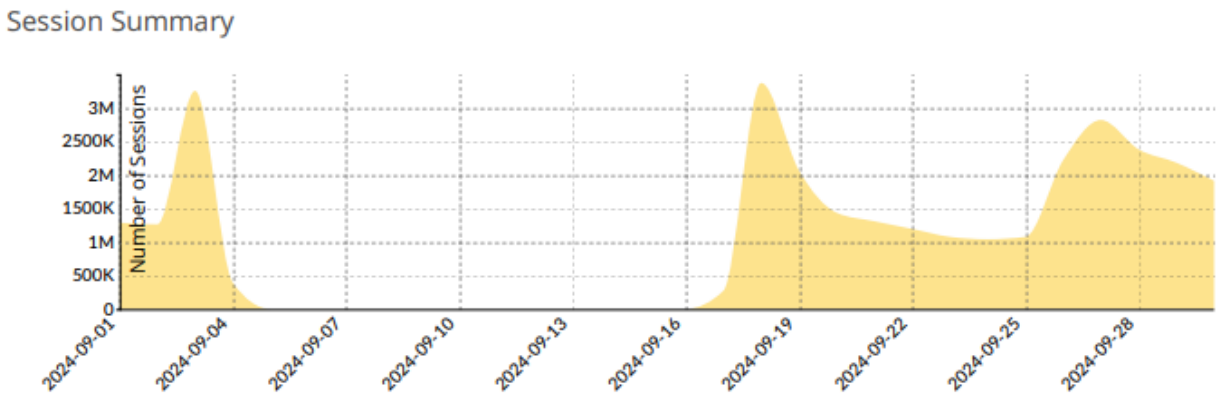
Las sesiones en el firewall para SIRNA 443 fueron:



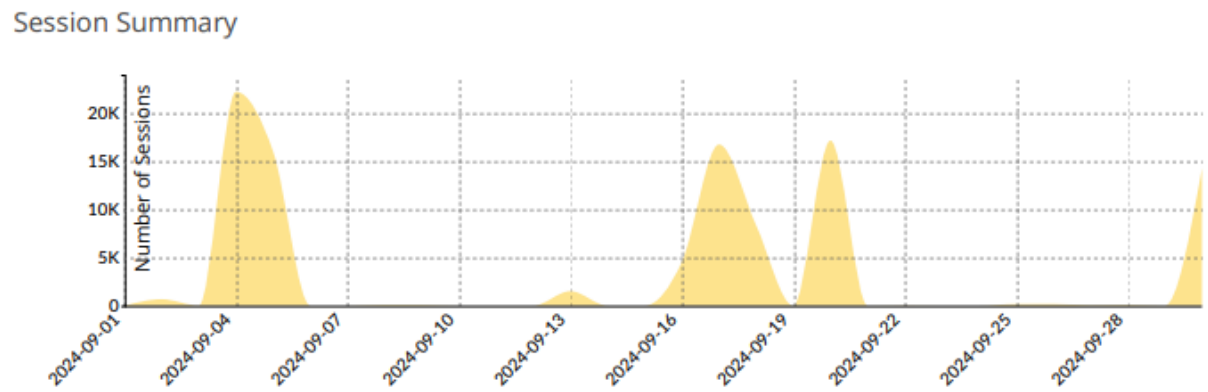
Las sesiones en el firewall para SIRNA 4443 fueron:



Las sesiones en el firewall para CRM 443 fueron:



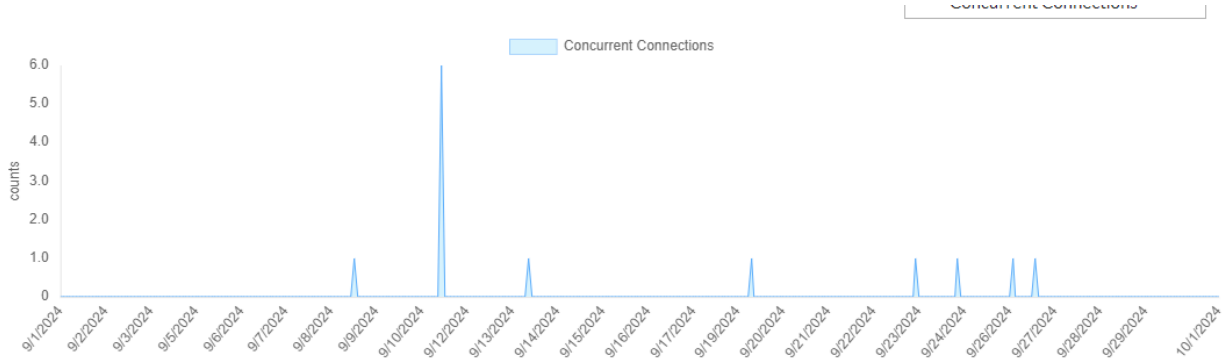
Las sesiones en el firewall para Sharepoint 444 fueron:



18.5. Convocatoria Peritos.

Este servicio se encuentra balanceado en el FortiADC:

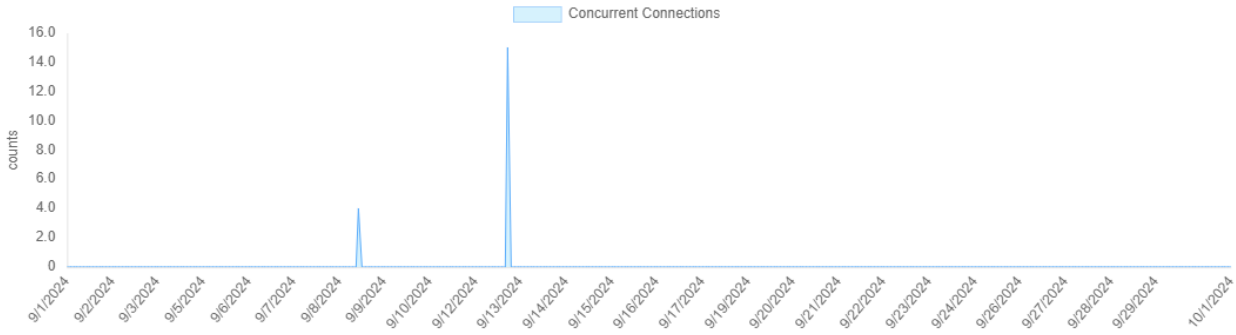
Las sesiones concurrentes fueron las siguientes:



18.6. SIERJU

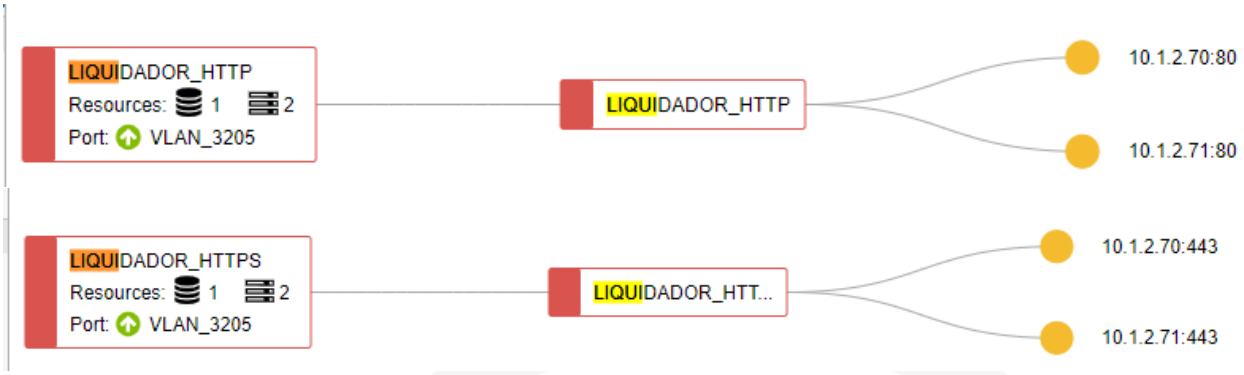
La configuración de balanceo para esta aplicación en el balanceador FortiADC es:

Durante septiembre no se observan conexiones concurrentes para este aplicativo:

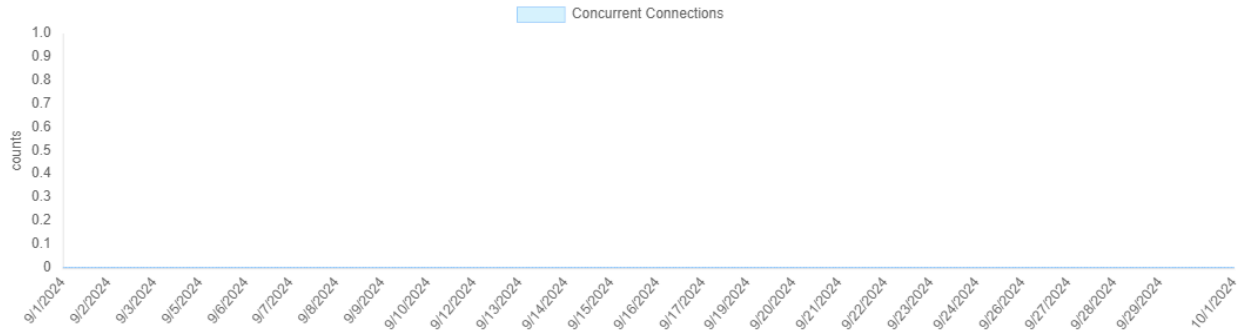


18.7. Liquidador de Sentencias

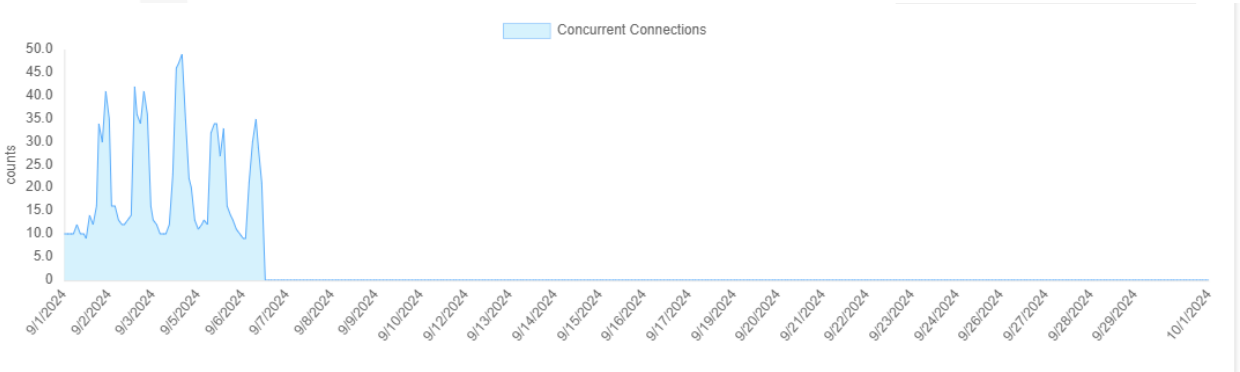
Virtual server Liquidador de Sentencias balanceador FortiADC



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



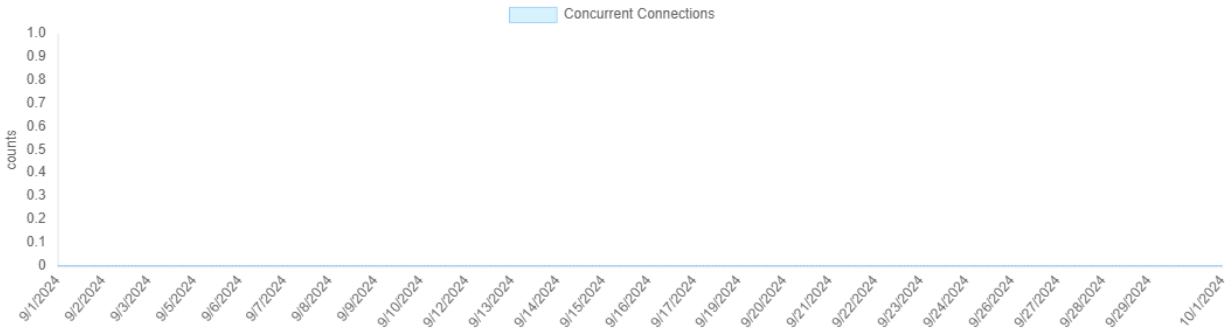
Las sesiones concurrentes por HTTPS fueron:



18.8. Consulta Jurisprudencia

Virtual server Consulta Jurisprudencia se encuentra en el balanceador FortiADC.

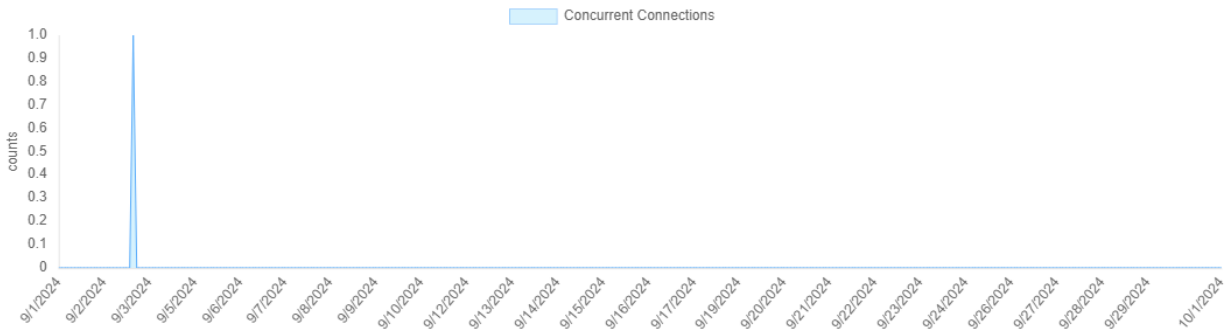
Durante septiembre no se observan conexiones concurrentes para este aplicativo:



18.9. API Gestión de Audiencias

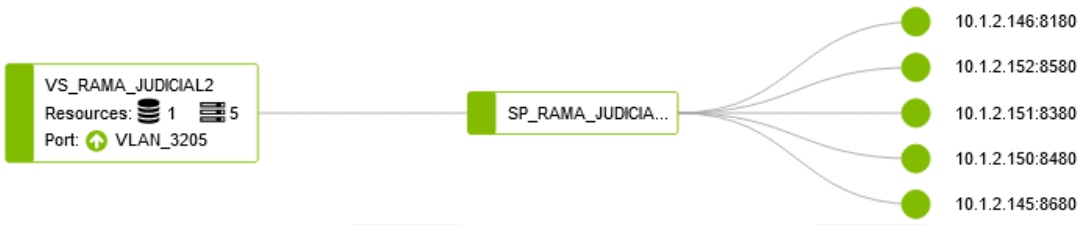
Virtual server API Gestión de Audiencias balanceador FortiADC.

Las sesiones concurrentes por HTTPS para este aplicativo:

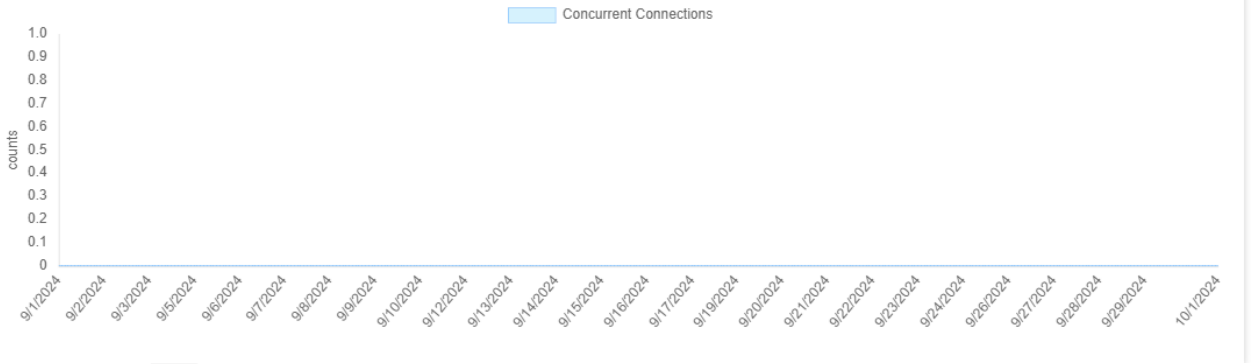


18.10. Portal Alterno de la Rama Judicial

Se encuentran balanceado en el FortiADC:

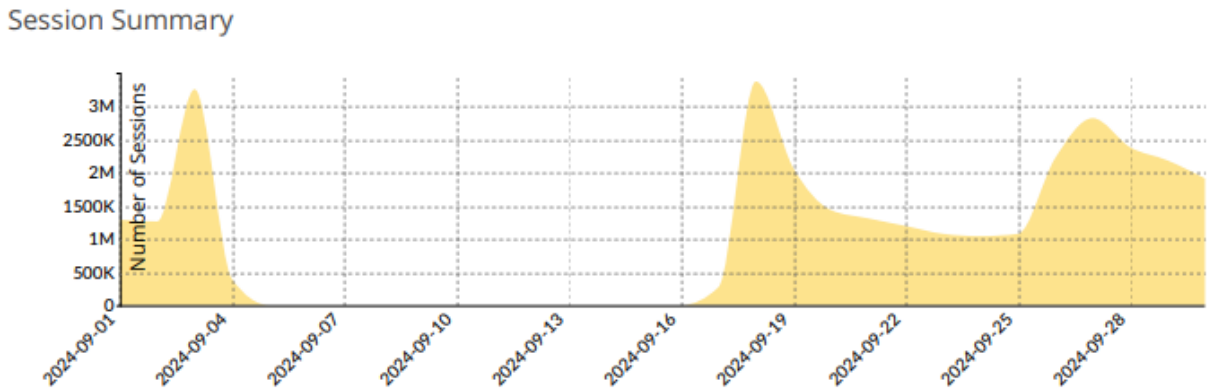


Durante septiembre no se observan conexiones concurrentes para este aplicativo:



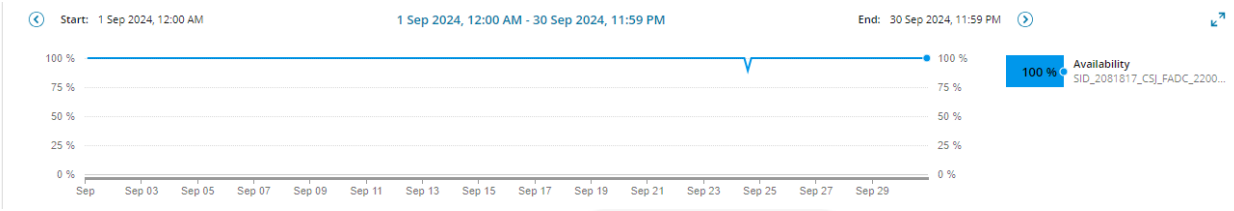
18.11. Portal de la Rama Judicial

Las sesiones Historico_Portal Rama Judicial fueron:



18.12. Disponibilidad y performance.

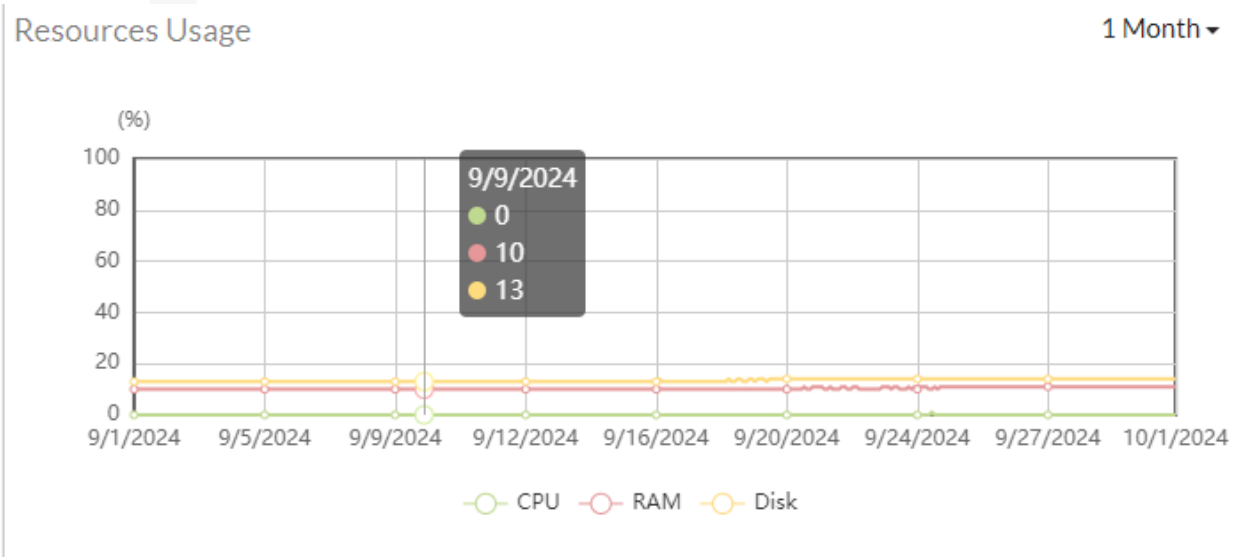
Durante septiembre se obtuvo 100% de disponibilidad en el FortiADC de Torre Central.



Availability Statistics

PERIOD	AVAILABILITY
Today	100.000 %
Yesterday	100.000 %
Last 7 Days	99.814 %
Last 30 Days	99.954 %
This Month	100.000 %
Last Month	99.954 %

Durante septiembre se observa consumo de CPU del 0%, memoria 10% y disco 13%:



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

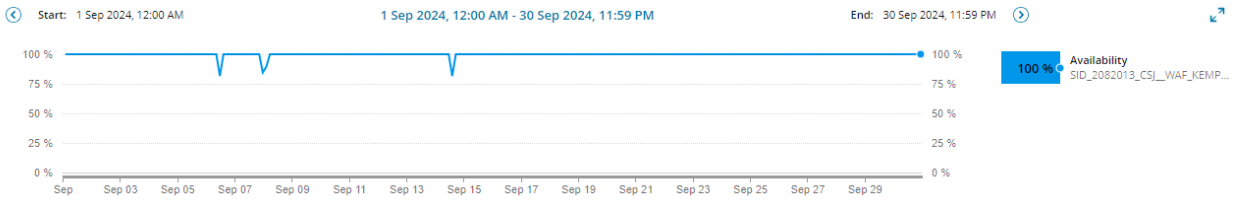
Para la protección de las aplicaciones web se tienen configuradas las siguientes políticas en los Firewall de Aplicaciones Web:

Item	Solución WAF	Cantidad de políticas de servidores
1	WAF TORRE CENTRAL	155
2	WAF CAN	68

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

19.1. Web application firewall datacenter principal IFX.

Durante septiembre se obtuvo disponibilidad del 100 % en el Kemp de Torre Central. Los eventos del 6, 8 y 14 de septiembre 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 99.732%

Availability Statistics

PERIOD	AVAILABILITY
Today	100.000 %
Yesterday	100.000 %
Last 7 Days	100.000 %
Last 30 Days	99.735 %
This Month	100.000 %
Last Month	99.732 %

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

La aplicación web más consultada durante septiembre fue publicacionesprocesales.ramajudicial.gov.co (172.17.201.100:443) con 29267663 sesiones web correspondiente al 45%

#	Política	Virtual IP Address	Total Conns	% del total
1	publicacionesprocesales.ramajudicial.gov.co - 190.217.24.175	172.17.201.100:443	29267663	45,0%
2	nuevoportal.ramajudicial.gov.co Y cndj.gov.co 190.217.24.176	172.17.201.101:443	17945733	27,6%
3	siicor.corteconstitucional.gov.co - 190.217.24.62	172.17.201.13:443	7760081	11,9%
4	consejodeestado.gov.co - 190.217.24.60	172.17.201.52:443	3208395	4,9%
5	apigestionaudiencias1.ramajudicial.gov.co	172.17.201.42:443	1262087	1,9%
6	sirna.ramajudicial.gov.co	172.17.201.28:443	1129431	1,7%
7	sistemaaudiencias.ramajudicial.gov.co	172.17.201.44:443	953235	1,5%
8	antecedentesdisciplinarios.cndj.gov.co	172.17.201.31:443	471955	0,7%
9	videoteca.ramajudicial.gov.co Holocausto_lector_videoteca_sidn_443	172.17.201.54:443	386541	0,6%
10	seccionalescsj.ramajudicial.gov.co-intrajud.ramajudicial.gov.co	172.17.201.8:443	342876	0,5%
	Otros		**2373063**	3,6%
	Total		**65101060**	100.00%

19.3. Top de peticiones por país WAF principal IFX.

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

Top 10 Countries

Total

Country	Requests	Blocked
Private	8456839	2745885
Colombia	23946013	1381608
IPrep	790212	790212
United States	7564114	159488
Russia	2442450	44858
Argentina	326235	18005
Brazil	175343	13443
Panama	80335	12405
Singapore	30046	12074
United Kingdom	87662	8668

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 septiembre. Sobre la aplicación *publicacionesprocesales.ramajudicial.gov.co* han sido prevenidas la mayor cantidad de ataques durante el mes:

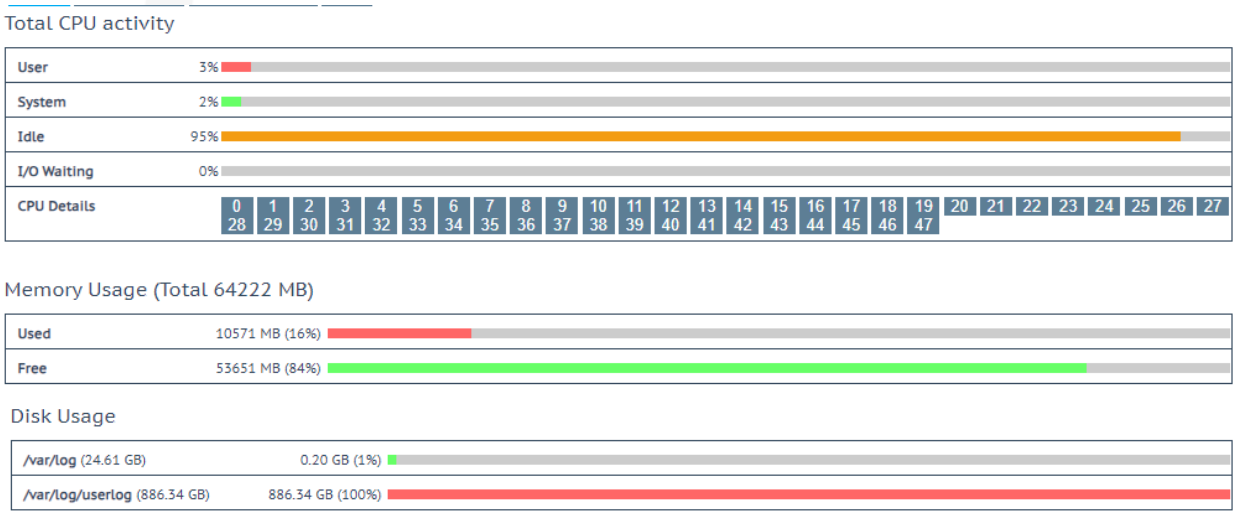
#	Política	Virtual IP Address	Total Conns	% del total
1	publicacionesprocesales.ramajudicial.gov.co - 190.217.24.175	172.17.201.100:443	56060167	41,2%
2	nuevoportal.ramajudicial.gov.co Y cndj.gov.co 190.217.24.176	172.17.201.101:443	31363766	23,0%
3	siicor.corteconstitucional.gov.co - 190.217.24.62	172.17.201.13:443	18469400	13,6%
4	apigestionaudiencias1.ramajudicial.gov.co	172.17.201.42:443	6342596	4,7%

5	consejodeestado.gov.co - 190.217.24.60	172.17.201.52:443	4326959	3,2%
6	sirna.ramajudicial.gov.co	172.17.201.28:443	4177080	3,1%
7	VS_Sicof_WILDFLY	172.17.201.51:8080	3735374	2,7%
8	consultajurisprudencial.ramajudicial.gov.co 8080	172.17.201.110:8080	2082318	1,5%
9	seccionalescsj.ramajudicial.gov.co-intrajud.ramajudicial.gov.co	172.17.201.8:443	1611346	1,2%
10	sistemaaudiencias.ramajudicial.gov.co	172.17.201.44:443	1366229	1,0%
	Otros		**6583798**	4,8%
	Total		**136119033**	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.

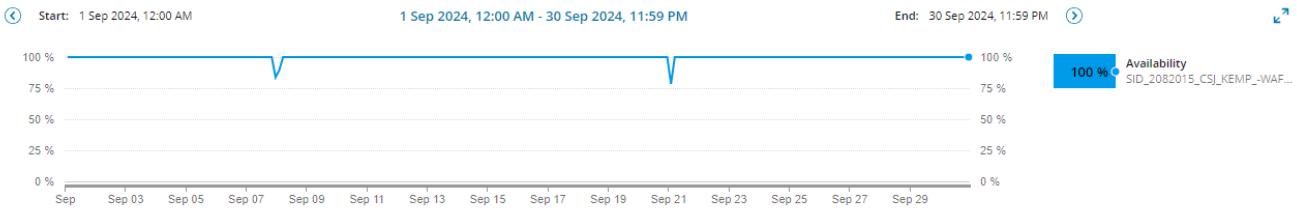
El WAF KEMP de Torre Central presentó consumo de CPU del 3%, memoria de 16% y disco en un 100% y 1%



20. TRÁFICO DE WEB APPLICATION FIREWALL (WAF) CAN

20.1. Disponibilidad WAF CAN.

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



Estadísticas tomadas el día 1 de octubre, los picos observados en la grafica puede corresponder a latencias sobre la red MPLS de CSJ que no es administrada por IFX, esto debido a que el WAF esta en el Datacenter del CAN propiedad de CSJ. Disponibilidad monitoreo 99.792

Availability Statistics

PERIOD	AVAILABILITY
Today	100.000 %
Yesterday	100.000 %
Last 7 Days	100.000 %
Last 30 Days	99.795 %
This Month	100.000 %
Last Month	99.792 %

20.2. Uso de políticas de servidores WAF CAN.

La aplicación más consultada durante septiembre fue cortesuprema.gov.co_Palacio con un 78,3% del total:

#	Política	Virtual IP Address	Total Conns	% del total
1	cortesuprema.gov.co_Palacio	172.17.202.239:443	12995554	78,3%
2	http_190.217.24.78-8888-tematres3-vocab-index.php	172.17.202.110:8888	595275	3,6%
3	sso.cortesuprema.gov.co	172.17.202.141:443	724110	4,4%
4	restituciontierras.ramajudicial.gov.co	172.17.202.37:443	265380	1,6%
5	samairj.consejodeestado.gov.co	172.17.202.38:443	257104	1,5%
6	relatoria.cndj.gov.co	172.17.202.66:443	250793	1,5%
7	linkce.consejodeestado.gov.co	172.17.202.42:443	168931	1,0%
8	serviciopdf.ramajudicial.gov.co	172.17.202.7:443	147664	0,9%

9	capacitacion.ramajudicial.gov.co 443	172.17.202.13:443	117595	0,7%
10	siapoas.ramajudicial.gov.co	172.17.202.43:443	1081904	6,5%
	Otros		**6319645**	38,1%
	Total		**16604310**	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
United States	6515588	62242
Private	1183428	9666
Singapore	63423	5665
IPrep	4862	4862
Spain	25028	2205
Netherlands	83625	1221
China	10801	1218
Bulgaria	72448	1169
Russia	70493	701
United Kingdom	8320	696

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 septiembre. Sobre la aplicación cortesuprema.gov.co_Palacio ha sido prevenida la mayor cantidad de ataques durante septiembre:

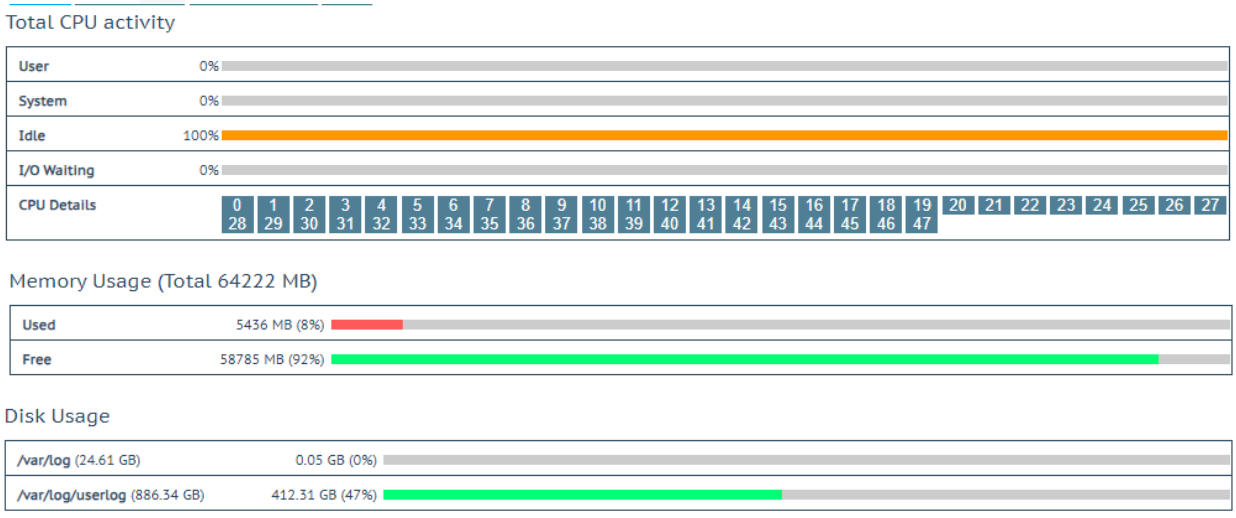
#	Política	Virtual IP Address	Total Conns	% del total
1	cortesuprema.gov.co_Palacio	172.17.202.239:443	178659769	88,3%
2	sso.cortesuprema.gov.co	172.17.202.141:443	5537475	2,7%

3	restituciontierras.ramajudicial.gov.co	172.17.202.37:443	3513427	1,7%
4	linkce.consejodeestado.gov.co	172.17.202.42:443	2447446	1,2%
5	siapoas.ramajudicial.gov.co	172.17.202.43:443	1714153	0,8%
6	convocatorias.consejodeestado.gov.co	172.17.202.147:443	1669344	0,8%
7	capacitacion.ramajudicial.gov.co 443	172.17.202.13:443	1598364	0,8%
8	relatoria.cndj.gov.co	172.17.202.66:443	1151642	0,6%
9	samairj.consejodeestado.gov.co	172.17.202.38:443	1091252	0,5%
10	http_190.217.24.78-8888-tematres3-vocab-index.php	172.17.202.110:8888	781159	0,4%
	Otros		**4258648**	2,1%
	Total		**202422679**	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 47%.



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

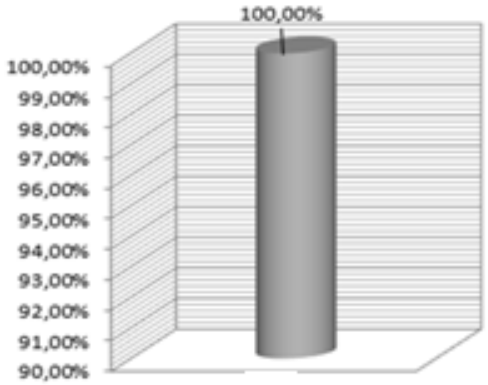
Durante septiembre se presentaron los siguientes intentos de ingreso administrativo hacia los firewall perimetrales. El acceso administrativo se encuentra protegido controles de "Restrict login to trusted hosts",

#	Login Source	User Name	Total Number of Failed Logins
1	https(172.29.116.72)	mvidalm	3
2	https(172.16.54.215)	victor.galvis	2
3	https(10.0.1.251)	jose.cardenas	1
4	ssh(172.16.54.104)	esierra	1
5	https(10.0.0.25)	esierra	1
6	https(172.16.55.52)	dasarmiento	1
7	https(10.0.1.173)	esierra	1
8	ssh(185.11.61.88)	admin_weegle	1
9	ssh(62.122.184.252)	RPM	1
10	https(10.0.1.146)	vglavis	1

21. DISPONIBILIDAD SEGURIDAD GLOBAL DEL MES DE SEPTIEMBRE

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

MES	DISPONIBILIDAD (%)
SEPTIEMBRE	100%



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

Se adjunta documento "Anexo CSJ-Consolidado casos septiembre 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	$ 10.473.475.679,02
% Valor facturado	67,50%
Valor pagado a la fecha	$ 10.473.475.679,02
% Valor pagado	67,50%

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	viernes, 20 de septiembre de 2024	Pagada
IFXC-413631	lunes, 16 de septiembre de 2024	$ 1.537.322.933,70	01 al 30 de Agosto 2024	martes, 1 de octubre 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
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
01 al 30 de Agosto 2024	No se generaron ANS durante el periodo
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.