REPORTE MENSUAL

RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA

OC124016

JUNIO 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 JUNIO de 2024 Fecha de final: 30 de JUNIO de 2024
Atributos de entrada	• Estado, % Memory Used, CPU LOAD, DISK SPACE USED, Top de Usados.
Tablas vistas o utilizadas	Reporte Mensual **RAMA JUDICIAL – CONSEJO SUPERIOR DE LA JUDICATURA**
Salida	Este informe contiene tablas en las que se visualizan porcentajes de uso y disponibilidad de las entradas evaluadas para determinar la disponibilidad.
Uso	El documento se genera como parte de la documentación entregada a final de cada mes y compone el esquema de gestión de disponibilidad de los servicios contratados por parte de **RAMA JUDICIAL – CONSEJO SUPERIOR DE LA JUDICATURA**

2. ALOJAMIENTO DE INFRAESTRUCTURA

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

		(MPPS) - 45000000- Mes - Cantidad: 2						
30	2082021	npn04--IaaS Seguridad - Appliance Anti Ddos - AltaCapacidad - Oro - Hostingfísico - Rol de Inspección - 50Gbps - Paquetes PorSegundo (MPPS) - 45000000- Mes - Cantidad: 2	DDOS DC Torre central	FORTIDDOS FORTINET 2000E/BK	2000E	SN: FI2KE581900004 9	35-36	32
31	2082016	npn04--IaaS Seguridad - Firewall Nueva Generación - Media Capacidad - Oro - Hosting físico - Rol deFirewall - 40 Gbps - SesionesConcurrentes - 15000000 -Mes - Cantidad: 2	FIREWALL	PALACIO - PPLA	FortiGate 900G	SN: 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	DATACENTE R - BK	FORTIGAT E-4400F	SN: FG440FT K219001 83	27-30	32
32	2082019	npn04--IaaS Seguridad - Firewall Nueva Generación - Alta Capacidad - Oro - Hosting físico - Rol deFirewall - 500 Gbps - Sesiones Concurrentes - 150000000 - Mes - Cantidad:2	FIREWALL DC Torre central	DATA CENTER - PPLA	FORTIGAT E-4400F	SN: FG440FT K219001 84	5-8	32
33	2082013	npn04--IaaS Seguridad - WebAplication Firewall - AltaCapacidad - Oro - Hostingfísico - Desempeño WAF(Gbps) - 10 - Mes - Cantidad:3	WAF DC Torre central	DATACENTE R - PPLA	KEMP LM-X25	SN: TSCC820 05608	14	31

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

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

1. ALMACENAMIENTO

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

El almacenamiento total aprovisionado en la infraestructura contratada, de conformidad con las solicitudes de la Entidad, a corte 30 de JUNIO de 2024 es de: **3929599 (GB)**

El almacenamiento total presentado adicional es de: **3814325 (GB)**

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

A corte 30 de JUNIO 2024 la entidad cuenta con un almacenamiento disponible de **185675(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_JUNIO_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 JUNIO de 2024, esta utilizando, una capacidad de **1050519 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 566620 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 supera en 216620 GB, 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

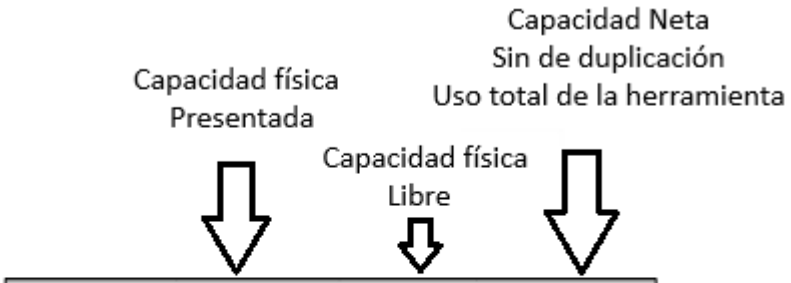
- A la fecha la entidad, está consumiendo 518200 GB de almacenamiento de BK Mensual, los cuales se sacan de la sumatoria de la columna "CAPACIDAD" menos "ESPACIO LIBRE", de la tabla "MENSUALES

- **Acorde a la información suministrada con anterioridad y realizando la resta entre lo consumido, menos el almacenamiento contratado la entidad supera en 233899 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	ESPACIO USADO
UNIDAD 1	80 TB	39,6 TB	129,6 TB
UNIDAD 2	80 TB	53 TB	4,3 TB
UNIDAD 3	78,2 TB	21,7 TB	25,8 TB
UNIDAD 4	110 TB	63,1 TB	112,5 TB
UNIDAD 01 GT	150 TB	15,8 TB	174,1 TB
UNIDAD 02 GT	150 TB	286,5 GB	249,6 TB
UNIDAD 03 GT	150 TB	40,8 TB	350,9 TB

MENSUALES			
REPOSITORIOS	CAPACIDAD	ESPACIO LIBRE	ESPACIO USADO
UNIDAD 1	90 TB	8,5 TB	178,1 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	94,6 TB
UNIDAD 5	69,1 TB	8,8 TB	94,1 TB
UNIDAD 6	89,1 TB	4,6 TB	176,9 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_JUNIO_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 JUNIO 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_JUNIO_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:

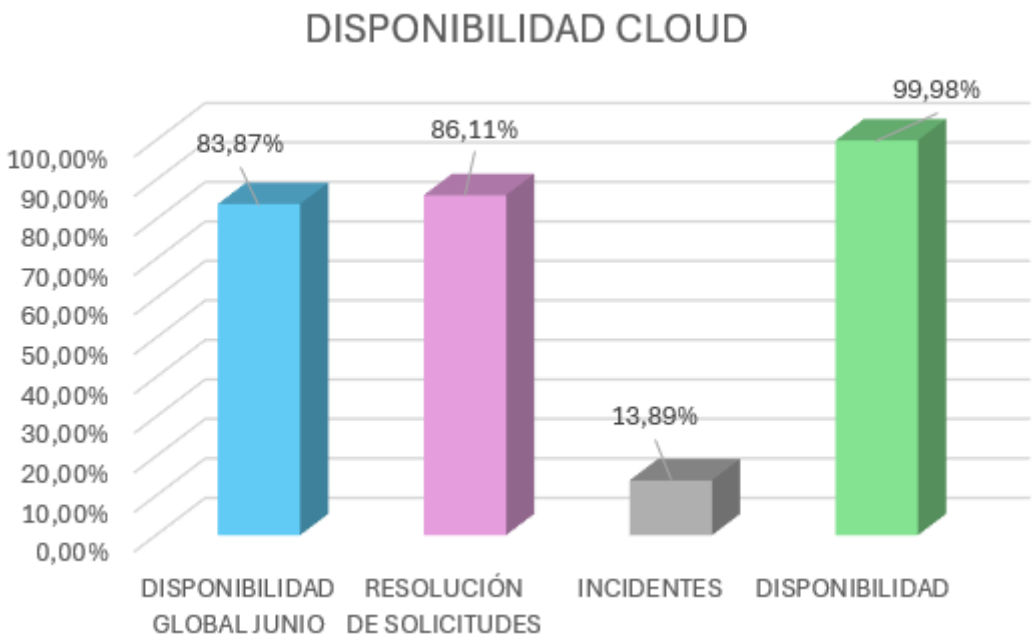
- **Capacitación SST:** líneas de OC 16 y 38
- **Cobro coactivo:** líneas de OC 17 y 38
- **core-impact:** Línea de OC 12
- **Efinomina:** Líneas de OC 14,18,26,27,38 y 39
- **Fuse:** Línea OC 17
- **Gestión grabaciones:** Líneas de OC 12,13, 14,15,17,19,20,22,23,25,28,35,36 y 38
- **InsightVM console:** 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_JUNIO_2024.xls**" para ver el detalle "maquinas")

7.DISPONIBILIDAD GLOBAL CLOUD DEL MES DE JUNIO

Disponibilidad Global mes de JUNIO	Numero de tickets mes de JUNIO	Imputabilidad por ANS
	31 solicitudes	**0 solicitudes**
	5 incidentes	**0 incidentes**
95%	Total 36 tickets	0 tickets



CONTROL DOCUMENTAL

ELABORADO POR

Fecha	Autor	Ingeniero
04-07-2024	IFX Networks	Juan Carlos Romero

REVISADO POR

Fecha	Autor	Ingeniero
	IFX Networks	

8. CONTENIDO DESAROLLO

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 junio a30 de junio del 2024.

CONSUMO TOTAL HORAS MES DE JUNIO	
• Casos Reportados Netsuite	62
Sesiones de Seguimiento	5
Sesiones de Trabajo	0
Casos Escalados Medio Digital - Whatsapp	6
Horas Disponibilidad del Recurso Fines de Semana	**327**
Total Horas Consumidas de las 300 - Experto Master	**400**

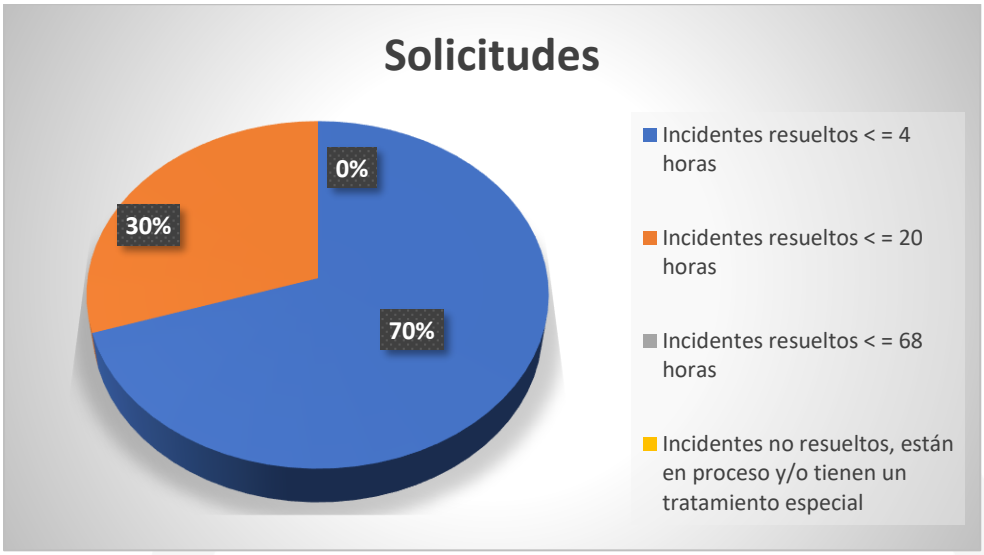
2. INDICADORES DEL CENTRO CONSOLIDADO DE SERVICIOS

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

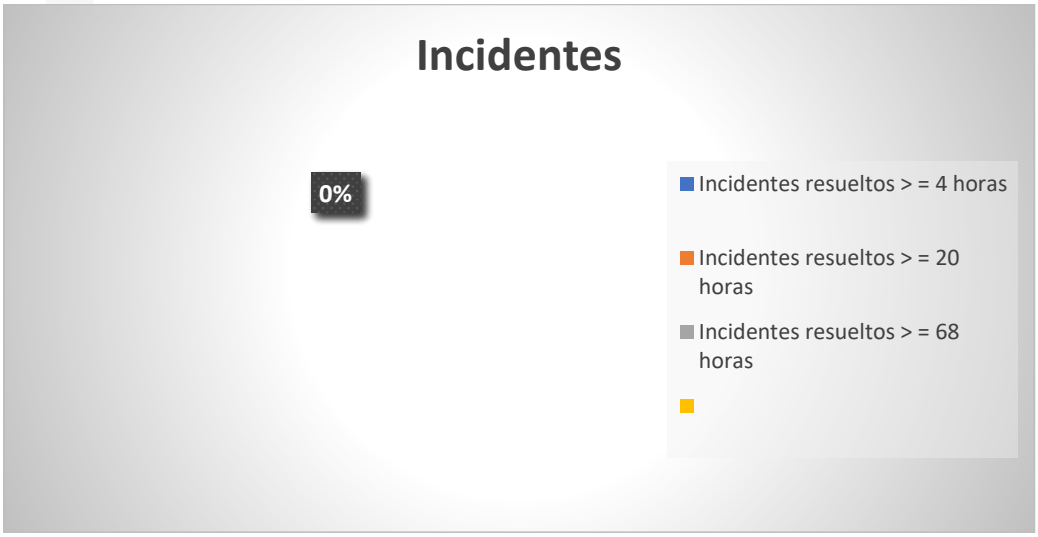
	Volumen en 1 junio a
Casos Reportados	10
Solicitudes	10
Incidencias	0
WA - AF	0

2.1 TASA DE RESOLUCIÓN DE PROBLEMAS

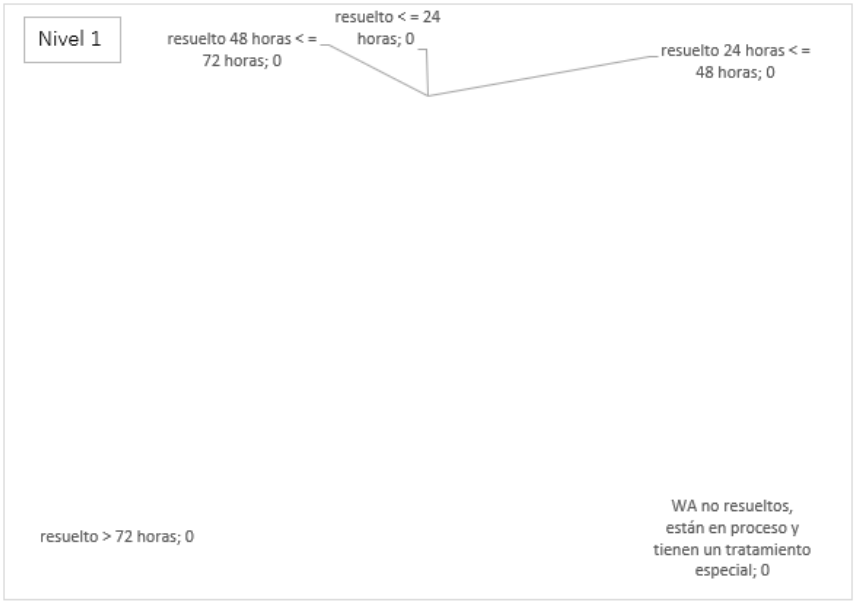
Tiempo de Gestión	Solicitudes
Solicitudes resueltas < = 4 horas	7
Solicitudes resueltas < = 20 horas	3
Solicitudes resueltas < = 68 horas	0
Solicitudes no resueltas, están en proceso y/o tienen un tratamiento especial	0
Total	**10**

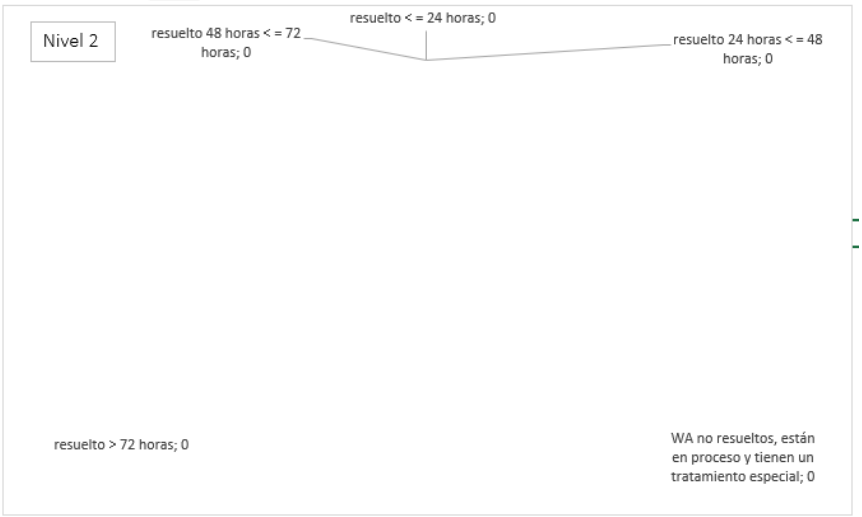


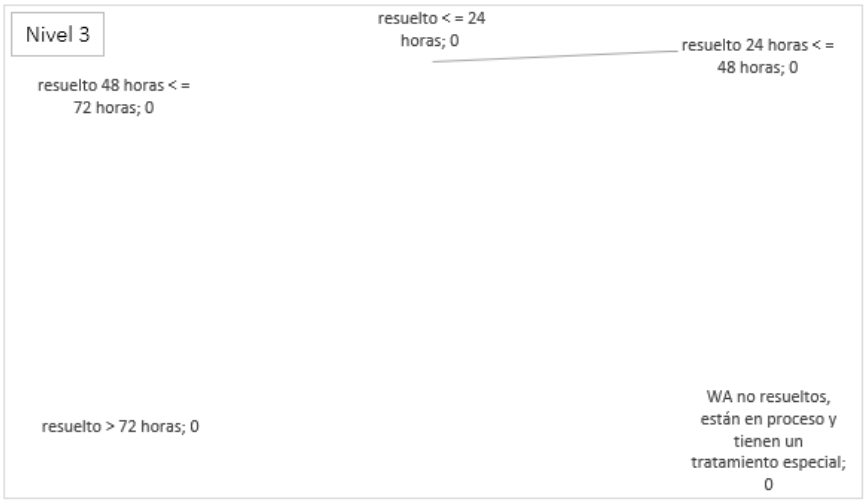
Tiempo de Gestión	Incidentes Penalizados
Incidentes resueltos > = 4 horas	0
Incidentes resueltos > = 20 horas	0
Incidentes resueltos > = 68 horas	0
Total	0

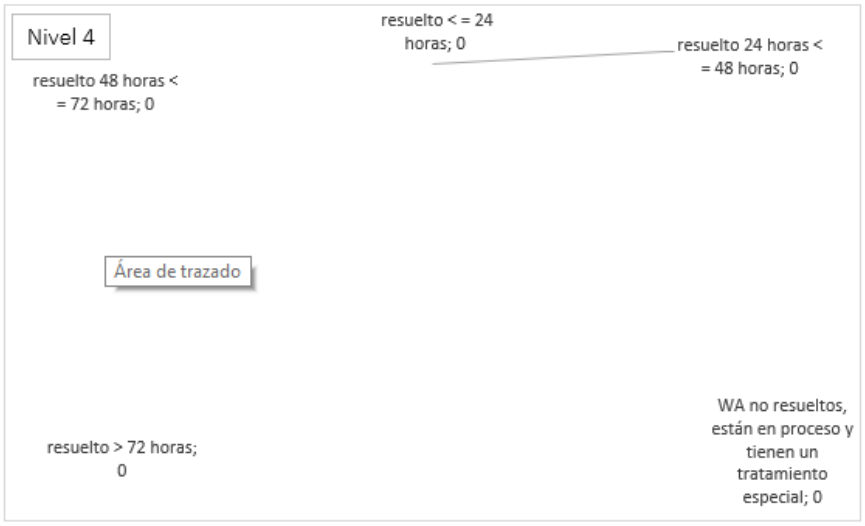


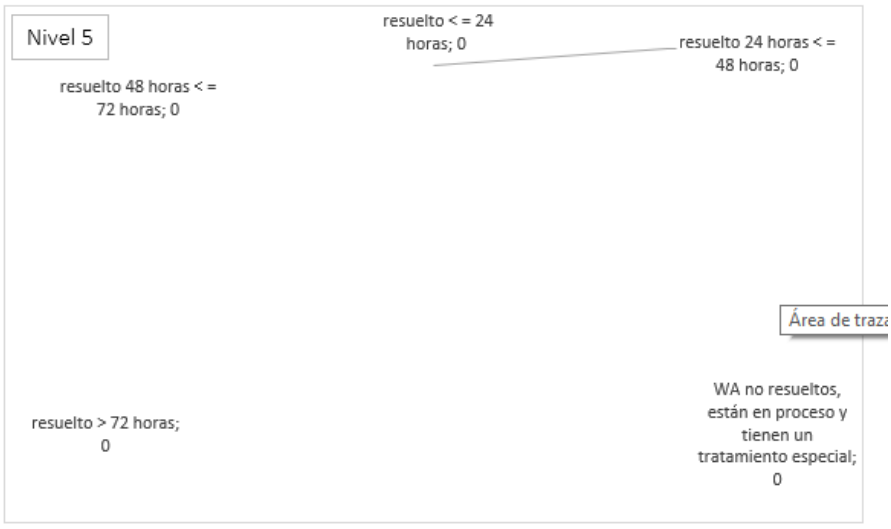
WA (Ajustes Funcionales)					
Tiempo de Gestión	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
resuelto < = 24 horas	0	0	0	0	0
resuelto 24 horas < = 48 horas	0	0	0	0	0
resuelto 48 horas < = 68 horas	0	0	0	0	0
resuelto > 68 horas	0	0	0	0	0
WA no resueltos, están en proceso y tienen un tratamiento especial	0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






Nivel 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


Nivel 4
resuelto < = 24 horas; 0
resuelto 24 horas < = 48 horas; 0
resuelto 48 horas < = 72 horas; 0
Área de trazado
resuelto > 72 horas; 0
WA no resueltos, están en proceso y tienen un tratamiento especial; 0


Nivel 5
resuelto < = 24 horas; 0
resuelto 24 horas < = 48 horas; 0
resuelto 48 horas < = 72 horas; 0
Área de traza
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 junio a 30 de junio del 2024.xlsx"** y los casos que fueron reportados por la aplicación WhatsApp consolidados a través del archivo **"Casos Reportados Medio Digital - Whatsapp"** este archivo se puede ver en el drive "https://ifxusa-my.sharepoint.com/:x:/r/personal/desarrollocsj_ifxcorp_com/_layouts/15/Doc.aspx?sourcedoc=%7B69A6AAC0-913F-491D-866B-DB9F5BCDDAEE%7D&file=casos%20reportados%20por%20medio%20digital.xlsx&action=default&mobileredirect=true" los cuales contienen la información detallada de cada uno desde el 1 de junio a 30 de junio 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 junio 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	73	400	327
2024	73		
Solicitud	73		
Incidencia	0		
Total Horas Casos Reportados Netsuite	73	400	327
		327	327
		327	327
		327	327
		327	327
Horas consumidasde las 400 - Exp	400	400	0

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

Etiquetas de fila	Suma de Horas Hombre	Horas Presupuesto	Horas Disponibles
CASO	0	100	100
2023	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

Para los portales de Rama Judicial y Publicaciones Procesales el equipo de desarrollo de IFX está prestando colaboración en la administración y estabilización de los mismos, pero las actividades operativas están compartidas con el equipo de UTDI y los proveedores que hicieron entrega de estos, aun con temas de garantía, por esta razón de parte de Desarrollo IFX no podemos justificar los tiempos de caída de los servicios de dichos portales.

Adicionalmente para el portal Histórico Rama Judicial (Liferay 6), actualmente se encuentra desplegado en servidores de la nube de AZURE, por lo cual tampoco podemos justificar los tiempos de indisponibilidad de este.

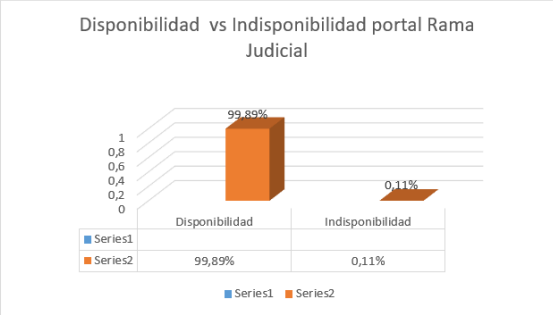
3.1. GRÁFICO DE DISPONIBILIDAD E INDISPONIBILIDAD DE LOS SERVICIOS DEL PORTAL DE RAMA JUDICIAL

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

Nota: para el mes de junio hacemos acotar que a razón del paso a producción del nuevo portal Liferay 7.1, y la salida a producción del portal de publicaciones procesales, no se estarán justificando los tiempos de caída de las mismas, ya que actualmente no tenemos la administración completa de dichas aplicaciones, así mismo con el portal histórico el cual fue llevado al datacenter de Azure

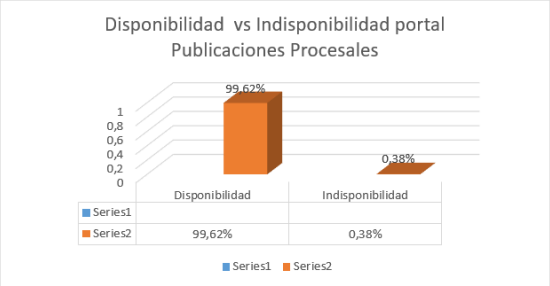
Portal Rama Judicial

Item	Aplicación	Disponibilidad	Indisponibilidad	Tiempo de duracion (Caida en horas)	Tiempo de duracion			
					Dias	Horas	Minutos	Segundos
1	Portal de la Rama Judicial	99,89%	0,11%	0,806111111	0	0	48	22
	Totales	99,89%	0,11%	0,806111111	**0**	0	48	22



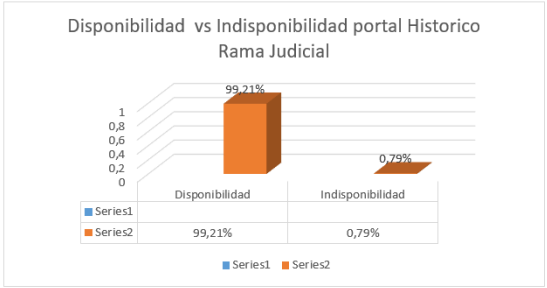
Portal Publicaciones Procesales

Item	Aplicación	Disponibilidad	Indisponibilidad	Tiempo de duracion (Caida en horas)	Tiempo de duracion			
					Dias	Horas	Minutos	Segundos
1	Publicaciones Procesales	99,62%	0,38%	2,721388889	0	2	43	17
	Totales	99,62%	0,38%	2,721388889	**0**	2	43	17



Portal Histórico Rama Judicial

Item	Aplicación	Disponibilidad	Indisponibilidad	Tiempo de duracion (Caida en horas)	Tiempo de duracion			
					Dias	Horas	Minutos	Segundos
1	Portal Historico	99,21%	0,79%	5,711944444	0	5	42	43
	Totales	99,21%	0,79%	5,711944444	**0**	5	42	43

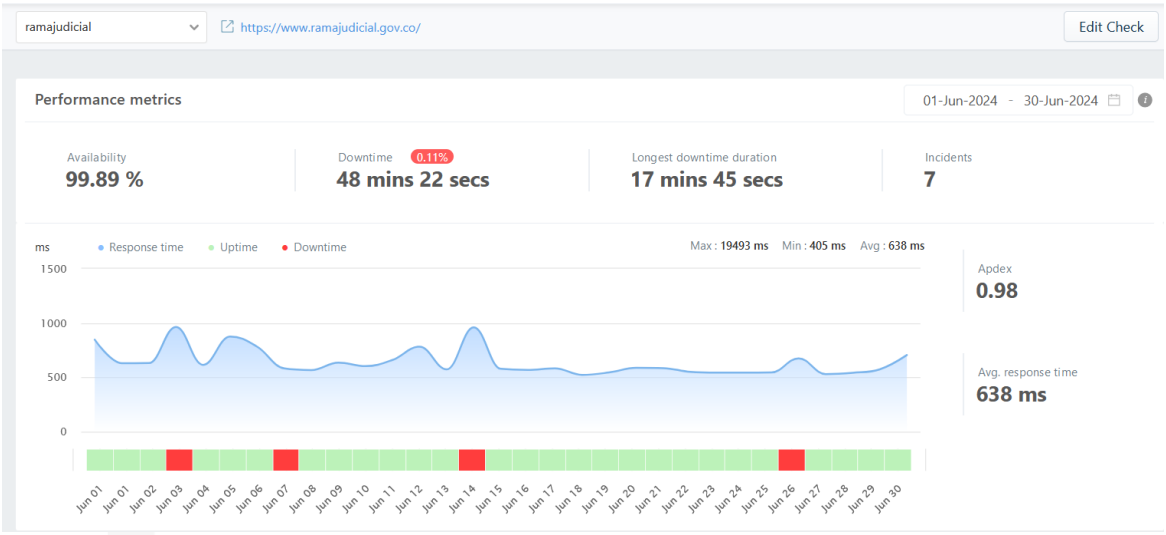


3.2 PORTAL DE LA RAMA JUDICIAL

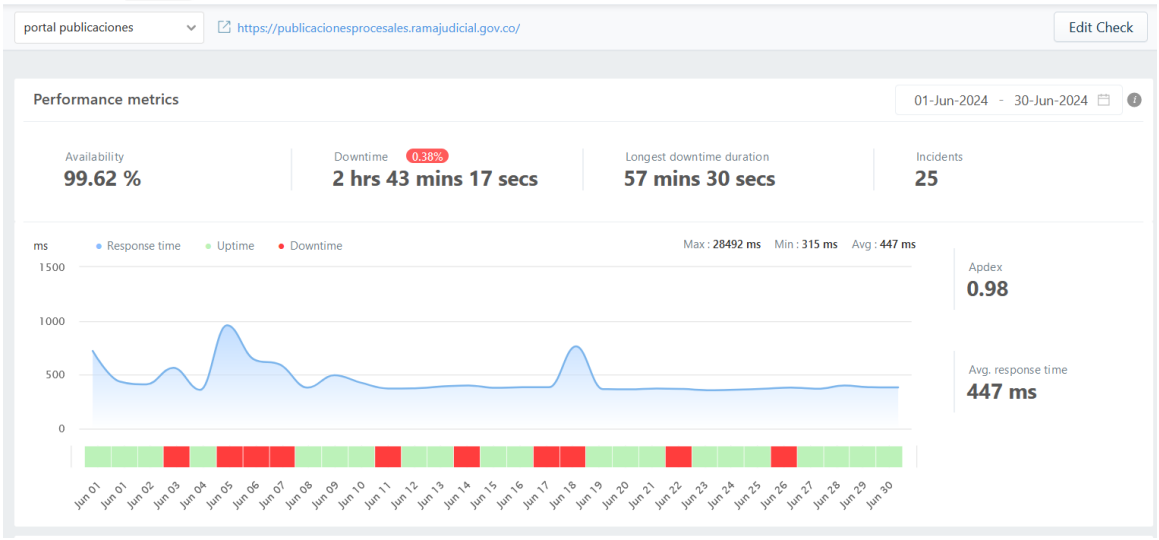
Grafica de la información consolidada de disponibilidad e indisponibilidad del portal del mes de junio

Nota: para el mes de junio hacemos acotar que a razón del paso a producción del nuevo portal Liferay 7.1, y la salida a producción del portal de publicaciones procesales, no se estarán justificando los tiempos de caída de las mismas.

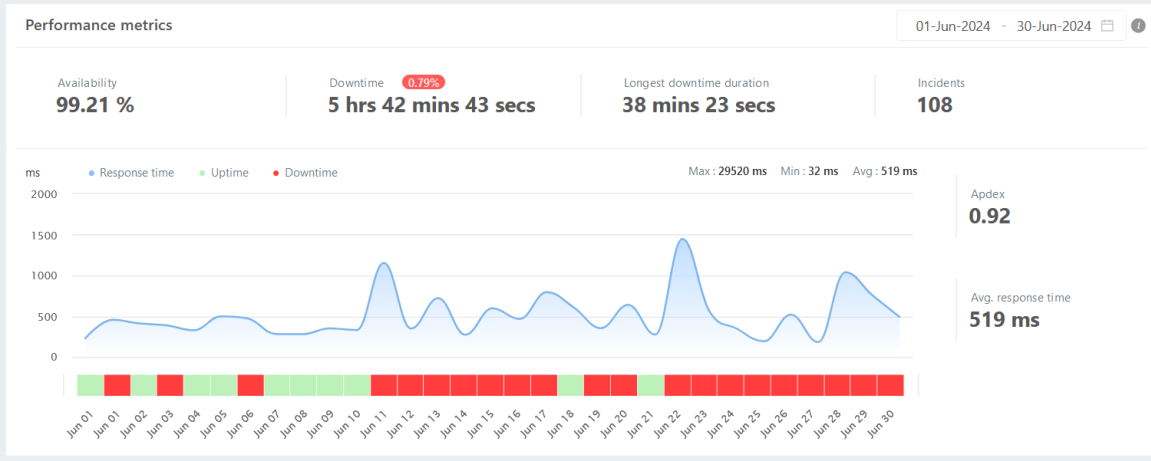
Portal Rama Judicial



Portal Publicaciones Procesales



Portal Histórico Rama Judicial



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

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

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

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

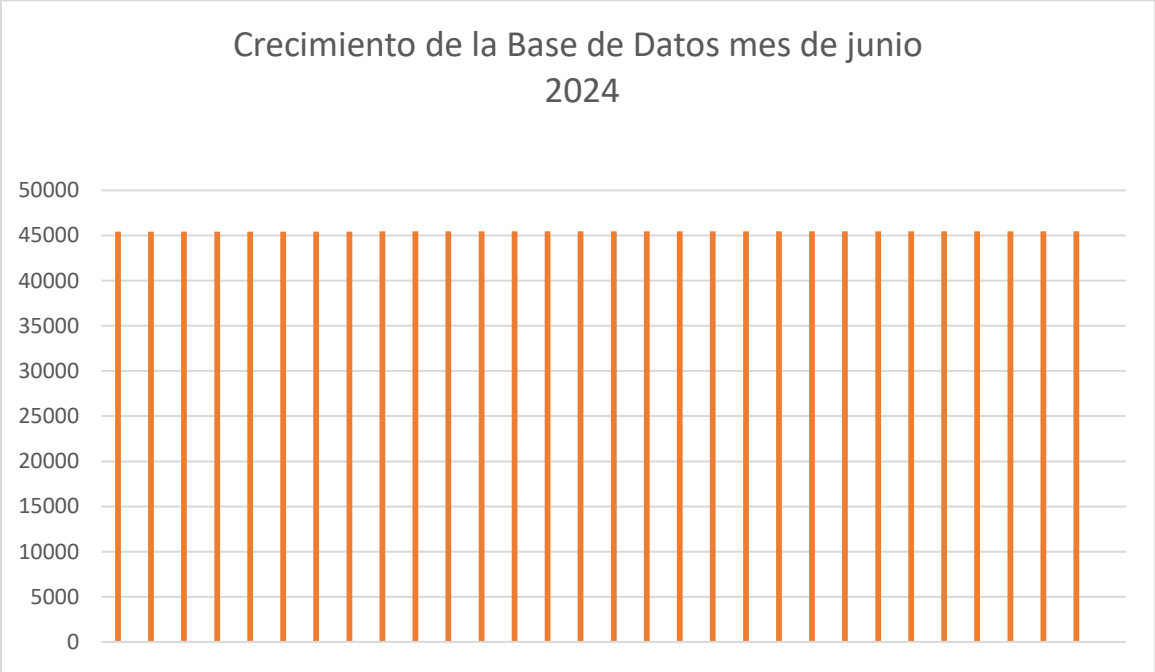
- No se ejecutaron actividades para mitigar inconvenientes de indisponibilidad

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 junio.

- No hubo crecimiento en la base de datos mencionadas

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 junio para el portal Rama Judicial.

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

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

9. 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 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
44	2082108	Servicios Complementarios - Experto Master - Región 1 - Hora/M - Cantidad: 980	Transversales a servicios de SP					

10. Horas experto de los ítems 44 y esquema de compensación.

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

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

Estas horas se usan para la atención de solicitudes, incidentes y actividades de gestión para las diferentes soluciones de seguridad de CSJ en el horario no hábil de la entidad. El detalle de las horas adicionales utilizadas para atender solicitudes e incidencias durante el mes se detallan a continuación:

Ingeniero Residente:	Edward Wilman Sierra leon				
Item	**Fecha y Hora de inicio**	**Fecha y Hora de finalización**	**Cantidad de Horas**	**Tipo de Hora extra**	**Actividad Realizada**
1	6/7/2024 18:00	6/7/2024 19:01	1	Diurna	TT848184 RE: Reporte Vpn conexiones fuera del pais mes mayo; TT848228 Fwd: Solicitud de extensión permisos VPN
2					
3					
4					
5					
6					
7					
8					
Total horas Extras			1		

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	15/6/2024 6:00:00 AM	15/6/2024 7:00:00 PM	13:00:00	Diurna/Nocturna	VM de energia Palacio de Justicia, Problemas VPN Azure, VM fibra Optica Cirion
2	16/6/2024 9:00:00 AM	16/6/2024 10:00:00 AM	1:00:00	Diurna/festiva	VM electrica Palacio de Justicia
3	16/6/2024 11:00:00 AM	16/6/2024 4:00:00 PM	5:00:00	Diurna/festiva	VM electrica Palacio de Justicia
4	18/6/2024 6:00:00 PM	18/6/2024 7:00:00 PM	1:00:00	Diurna	TT849811 RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA
5					
6					
7					
8					
9					
10					
Total horas Extras			20:00:00		

Ingeniero Residente:	Camilo Calvo

Item	Fecha y Hora de inicio	Fecha y Hora de finalización	Cantidad de Horas	Tipo de Hora extra	Actividad Realizada
1					
2					
3					
4					
4					
4					
7					
8					
Total horas Extras			0:00:00		

a. Inventario de equipos de seguridad perimetral.

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

No	Descripción	Hostname	Serial	SID	Ubicación	Version Firmware
1	FortiGate-4400F HA	FTG_CSJ_DC_TC_MASTER	FG440FTK21900184	2082019	DC IFX	v7.0.14
		FTG_CSJ_DC_TC_SLAVE	FG440FTK21900183	2082018	DC IFX	v7.0.14
2	FORTIADC 2200F HA	FADC_CSJ_TC_MASTER	FAD22FT221000027	2081818	DC IFX	v6.1.3
		FADC_CSJ_TC_ SLAVE	FAD22FT221000028	2081817	DC IFX	v6.1.3
3	WAF KEMP Loadmaster x25 HA	WAF_TORRRE_CENTRAL	TSCC82005608	2082013	DC IFX	7.2.59.3.22368
		WAF_TORRRE_CENTRAL	TSCC8200529	2082014	DC IFX	7.2.59.3.22368
4	Fortigate 900G HA	FGT_900G_CSJ_PALACIO_M	FG9H0GTB23900440	2082016	PALACIO	V7.2.6
		FGT_900G_CSJ_PALACIO_S	FG9H0GTB23900205	2082017	PALACIO	V7.2.6
5	WAF KEMP Loadmaster x25	WAF_CAN	TSCC82005629	2082015	CAN	7.2.59.3.22368
6	FortiDDos 2000E HA	CSJ_FDDoS_MASTER	FI-2KE5819000049	2082020	DC IFX	v6.3.3
		CSJ_FDDoS_SLAVE	FI-2KETB20000015	2082021	DC IFX	v6.3.3

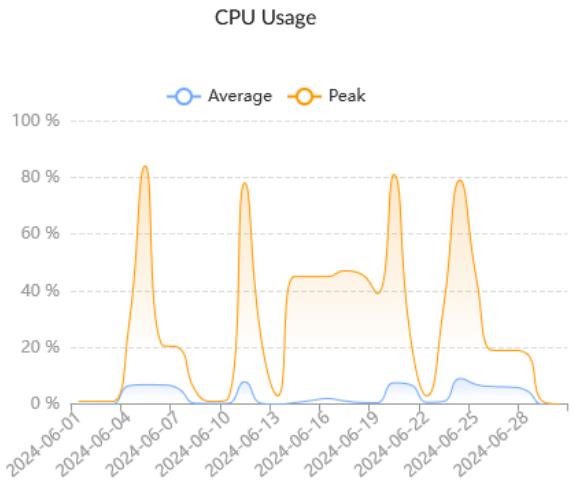
10.1 Actualización de firmware.

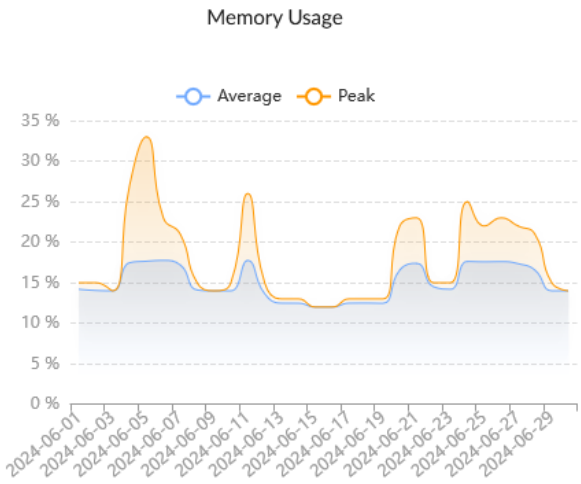
El plan de trabajo para la actualización del firmware será compartido, presentado y ejecutado con la autorización de los ingenieros Datacenter del CONSEJO SUPERIOR DE LA JUDICATURA.

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

11. FIREWALL PERIMETRAL

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

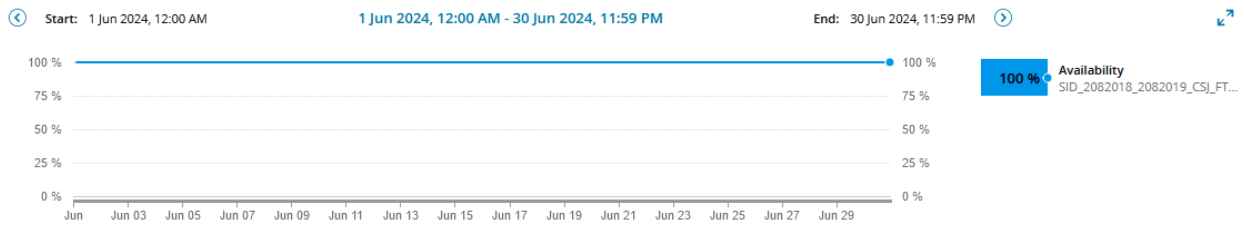




En la gráfica de rendimiento "CPU Usage", la curva color naranja muestra los picos de consumo de una o varias de las 160 CPUs del appliance FortiGate-4400F, cuando estos picos ocurren las tareas que los generan son desbordadas a las otras CPUs del appliance por lo que la curva color azul se muestra el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

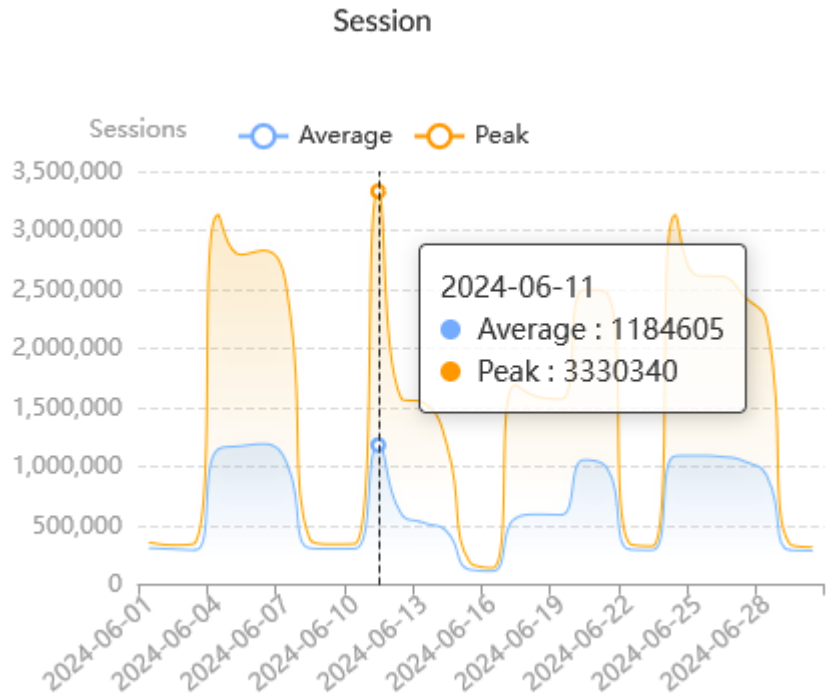
11.1 Disponibilidad mensual firewall perimetral.

Durante junio se obtuvo 100% de disponibilidad en el firewall perimetral sin la ocurrencia de novedades y/o eventos.



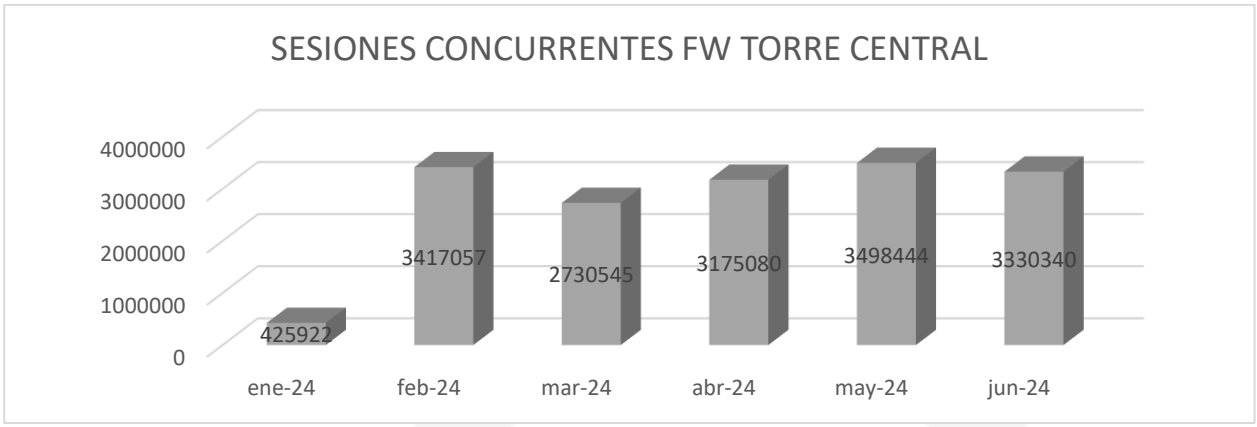
11.2 Cantidad de sesiones firewall perimetral.

Durante junio se presentó un máximo de 3.330.340 sesiones TCP concurrentes, cantidad que se encuentra dentro del rango máximo soportado por el appliance Fortinet FG- 4400F cuyo valor es de 210 millones.



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

Durante junio se presentó un leve descenso en las sesiones en el FW perimetral correspondientes a 3’330.340 de sesiones:



MES	SESIONES
ene-24	425922
feb-24	3417057
mar-24	2730545
abr-24	3175080
may-24	3498444
jun-24	3330340

11.4 Aplicaciones y protocolos por ancho de banda firewall perimetral.

HTTPS (web seguro) fue la aplicación con mayor consumo de ancho de banda durante junio:

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	HTTPS			240.31 TB
2	SSL			129.85 TB
3	Microsoft.SharePoint			54.69 TB
4	TCP/1433			46.49 TB
5	SMB			33.06 TB
6	DTLS			24.60 TB
7	TCP/9443			23.61 TB
8	Akamai-CDN			21.88 TB
9	Microsoft.Portal			20.72 TB
10	Microsoft-Office365			18.70 TB

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

Top Applications by Sessions

#	Application	Sessions
1	SMB	2,329,654,314
2	HTTPS	1,895,138,875
3	DNS	1,314,877,122
4	Microsoft.Windows.Update	642,342,956
5	SSL	511,448,169
6	Microsoft.Portal	456,187,822
7	Microsoft.365.Portal	413,519,564
8	TCP/UDP_8037	398,180,131
9	Rapid7-Web	350,248,717
10	ESET-Eset.Service	346,381,530

11.5 Top de IP por ancho de banda firewall perimetral.

La IP 172.31.10.41 (aplicación Árbol tutela Justicia_XXI_DB) tuvo la mayor cantidad de consumo de ancho de banda durante el mes de junio:

Top Bandwidth IP

#	IP	Bandwidth
1	172.31.10.41	85.44 TB
2	172.16.182.85	5.11 TB
3	10.101.100.114	3.09 TB
4	10.101.100.38	2.08 TB
5	10.101.100.98	1.24 TB
6	10.101.100.122	1.06 TB
7	10.101.100.182	1.05 TB
8	10.101.100.34	936.13 GB
9	10.101.100.138	892.38 GB
10	10.101.100.70	883.29 GB

11.6 Top de destinos web por sesiones firewall perimetral.

Los destinos en Internet con mayor cantidad de sesiones durante junio fueron 8.243.164.19 (CTL Colombia), 172.28.107.71, microsoft.com y windowsupdate.com.

Top Destinations by Sessions

#	Hostname(or IP)	Sessions
1	8.243.164.19	429,737,816
2	172.28.107.71	424,301,341
3	microsoft.com	328,941,783
4	windowsupdate.com	311,033,198
5	8.243.164.21	250,897,225
6	spotify.com	137,110,957
7	13.58.19.32	123,177,981
8	3.139.243.230	122,811,174
9	3.131.127.126	122,427,880
10	172.28.146.154	119,698,422

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

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

Top Web Users by Blocked Requests

#	User (or IP)	Hostname	Requests
1	172.16.35.145	172.16.35.145	6,805,491
2	172.16.33.29	172.16.33.29	6,422,166
3	192.168.199.32	192.168.199.32	5,907,801
4	192.168.46.197	192.168.46.197	5,815,222
5	172.25.110.163	172.25.110.163	5,350,158
6	172.25.118.34	172.25.118.34	5,087,456
7	172.28.5.203	172.28.5.203	4,263,036
8	192.168.125.26	192.168.125.26	3,685,044
9	192.168.123.17	192.168.123.17	3,485,256
10	192.168.140.20	192.168.140.20	3,131,947

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

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

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

Top Blocked Web Categories

#	Category	Requests
1	Internet Radio and TV	141,704,636
2	Proxy Avoidance	7,971,134
3	Streaming Media and Download	6,850,504
4	Social Networking	5,079,774
5	Games	4,216,685
6	Unrated	1,819,670
7	Information Technology	1,113,373
8	Entertainment	569,019
9	Malicious Websites	461,920
10	Society and Lifestyles	274,752

11.9 Top de IP más activos Firewall Perimetral

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

Top Web IP by Allowed Requests

#	IP	Requests
1	10.101.100.114	11,463,189
2	10.101.100.34	6,554,116
3	10.101.100.38	6,248,587
4	10.101.100.194	5,616,508
5	10.101.100.122	4,946,614
6	10.101.100.134	4,414,248
7	10.101.100.70	4,296,512
8	10.101.101.246	3,770,044
9	172.28.238.182	3,707,718
10	10.101.100.170	3,562,504

11.10 Top de categorías más visitadas Firewall Perimetral

La categoría más visitada durante junio fue Information Technology:

Top Allowed Web Categories

#	Category	Requests
1	Information Technology	363,053,065
2	Overrride_permitidas	506,440

11.11 Top de consumo ancho de banda por usuario Firewall Perimetral

La aplicación 172.31.10.41 (Árbol tutela Justicia_XXI_DB) y el WAF del atacenter CAN 172.17.201.252 presentaron el mayor consumo de ancho de banda durante junio:

Top IP by Bandwidth

#	IP	Bandwidth	Sent / Received
1	172.31.10.41		95.82 TB
2	172.17.201.252		60.43 TB
3	172.17.201.251		46.99 TB
4	10.1.2.31		44.79 TB
5	172.27.64.17		27.68 TB
6	172.27.64.61		15.15 TB
7	10.244.2.239		13.17 TB
8	172.28.108.48		10.73 TB
9	172.28.107.71		9.75 TB
10	erubianr		8.12 TB

12. TRÁFICO VPN FIREWALL PERIMETRAL

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

#	f_user	devname	vpn_type_group	end_time	remip	connections	Duration	bandwidth	traffic_in	traffic_out
1	Ecoralb	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-07-01 00:00:07	186.102.24.23;186.28.123.175;186.28.44.62;186.29.129.175;186.29.129.91;186.29.184.66;201.245.255.228	314	709:25:12	12.76 GB	1688515353	12007931229
2	cvillam	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-06-30 23:53:04	181.55.51.20	81	563:05:42	4.91 GB	603779896	4665504090
3	pfajardg	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-06-30 12:26:47	186.81.100.20	68	383:46:15	19.58 GB	1045829115	19983284227
4	jariasu	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-06-30 23:52:33	181.137.8.129	58	335:16:06	646.02 MB	146742095	530663062
5	csichaca	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel;ssl-web	2024-06-29 21:53:46	138.84.41.125;181.55.70.80;186.102.11.77;186.102.23.14;186.102.25.207;186.102.34.1;186.102.61.250;186.102.63.121;186.102.7.53;186.102.82.31;186.102.89.68;186.102.94.35;186.114.104.11;186.168.239.139;186.82.128.39;186.84.20.59;186.84.21.87;191.156.58.101;191.156.62.59	105	322:20:59	5.80 GB	1240019248	4990173185
6	lmarinmo	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-06-30 06:42:42	181.136.233.42	79	304:42:56	5.02 GB	519906125	4866763013
7	lbarrerf	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-06-29 12:50:35	186.155.110.85;186.30.62.21;191.156.148.83;191.156.151.13;191.156.156.172;191.156.159.165;191.156.182.95;191.156.187.214;191.156.225.239;201.244.161.87	55	295:00:29	39.63 GB	2157486274	4039433 6413
8	froaga	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-06-29 16:13:37	186.28.160.77;186.29.216.119;186.31.213.177;190.26.136.235	47	281:56:54	41.79 GB	11480574756	33393292775
9	mgarciacon	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-06-29 18:24:06	181.234.130.11;190.107.30.70;191.106.177.63;191.106.224.0;38.51.234.69;45.225.227.33	184	279:31:39	7.93 GB	998443751	7519425521
10	jlsarmiento	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-06-28 10:58:40	181.51.34.36	115	278:06:49	31.96 GB	1657694231	3265462 1344

12.1 VPN IPSEC Site To Site Firewall Perimetral

El consumo de ancho de banda de las VPN IPSec Site to Site durante junio 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	2589259	79642734691827	52785083557443	26857651134384
2	VPN_ORACLE	129.213.6.36	190.217.80.4	2590010	4794073521168	4672771990940	121301530228
3	VPN_AZURE-ANALY	20.124.34.235	190.217.24.4	2590028	85929613486	6901762749	79027850737
4	VPN_Tierras	181.225.76.196	190.217.24.4	2586886	35075498722	34079657508	995841214
5	VPN_SIUG_AWS-2	34.224.152.152	190.217.24.4	2589818	1875696137	1044130270	831565867
6	VPN_SIUG_AWS	34.194.187.190	190.217.24.4	2589813	1124374572	566608248	557766324
7	VPN_INPEC	190.25.112.10	190.217.19.156	2590141	651966475	544863311	107103164
8	VPN_REGISTRADU	201.232.123.20	190.217.24.4	3293920	348542142	180957859	167584283
9	VPN_Linktic	3.222.171.115	190.217.24.4	3293985	310214626	218143307	92071319
10	OCI_EXADATA_FAB	150.136.25.96	190.217.24.4	2590157	104926484	0	104926484
11	VPN_AZURE-VWAN2	4.153.117.131	190.217.24.4	2589038	51011609	34670811	16340798
12	VPN_FISCALIA	190.157.218.66	190.217.24.4	2589105	41559139	39859862	1699277
13	VPN_AZURE-VWAN	4.153.117.133	190.217.24.4	2588956	20526283	20519959	6324

12.2 Top de intrusiones detectadas por el IPS del firewall perimetral

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

Top Attacks

#	Attack Name	Severity	CVE-ID	Counts
1	tcp_syn_flood	Critical		214,190
2	tcp_src_session	Critical		87,885
3	tcp_port_scan	Critical		87,628
4	ip_dst_session	Critical		74,272
5	Apache.Log4j.Error.Log.Remote.Code.Execution	Critical	CVE-2021-4104,CVE-2021-44228,CVE-2021-45046	5,074
6	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	Critical	CVE-2017-9841	4,058
7	Andromeda	Critical		2,985
8	Andromeda.Botnet	Critical		2,912
9	Amadey.Botnet	Critical		2,453
10	Bash.Function.Definitions.Remote.Code.Execution	Critical	CVE-2014-6271,CVE-2014-6277,CVE-2014-6278,CVE-2014-7169,CVE-2014-7186,CVE-2014-7187	1,545

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

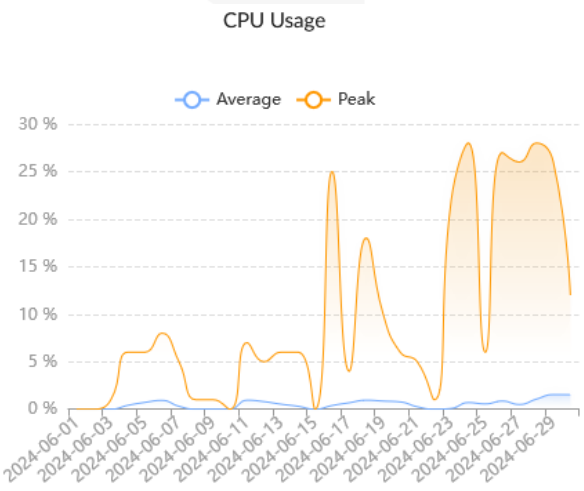
Top Intrusion Victims

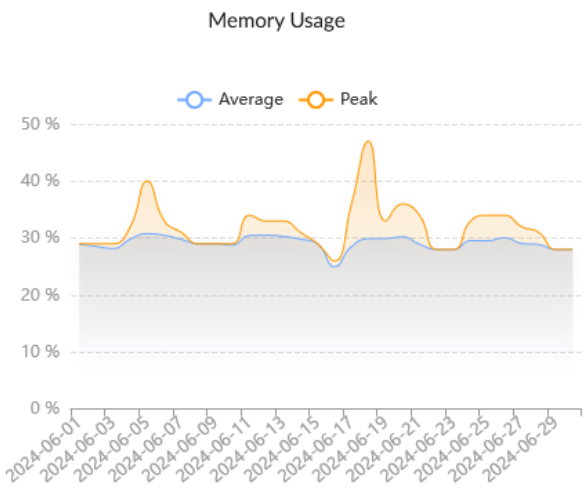
#	Attack Victim	Counts	Critical	High	Medium	Percent of Total Attacks
1	190.217.24.172				225,936	33.22%
2	172.17.201.52				91,041	13.39%
3	172.17.201.26				83,333	12.25%
4	172.17.201.13				75,901	11.16%
5	190.217.24.176				75,281	11.07%
6	192.168.213.94				48,278	7.10%
7	192.168.55.4				26,278	3.86%
8	34.16.47.102				13,322	1.96%
9	34.29.85.190				8,856	1.30%
10	172.17.201.101				8,825	1.30%
11	172.17.202.239				4,170	0.61%
12	222.211.73.134				2,878	0.42%
13	172.28.23.10				2,624	0.39%
14	193.106.191.201				2,453	0.36%
15	172.28.108.91				2,156	0.32%
16	172.27.117.82				2,054	0.30%
17	172.17.201.54				1,706	0.25%
18	172.17.202.66				1,705	0.25%
19	172.17.201.33				1,675	0.25%
20	147.75.63.87				1,551	0.23%

Los hosts 190.217.24.172, 190.217.24.176 y 172.17.201.x son aplicaciones web del CSJ, sin embargo, estás aplicaciones están siendo protegidas por los WAF Torre Central y el WAF CAN.

13. FIREWALL SEDE PALACIO

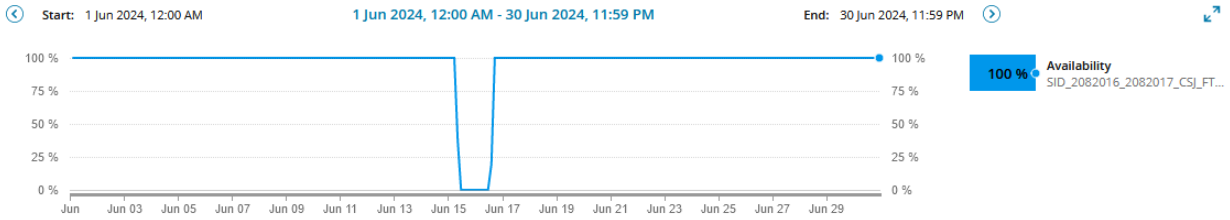
Durante junio, el consumo de CPU y memoria en el Firewall de Palacio se mantuvo dentro de sus valores de operación normal.





a. Disponibilidad Mensual Firewall Palacio

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



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

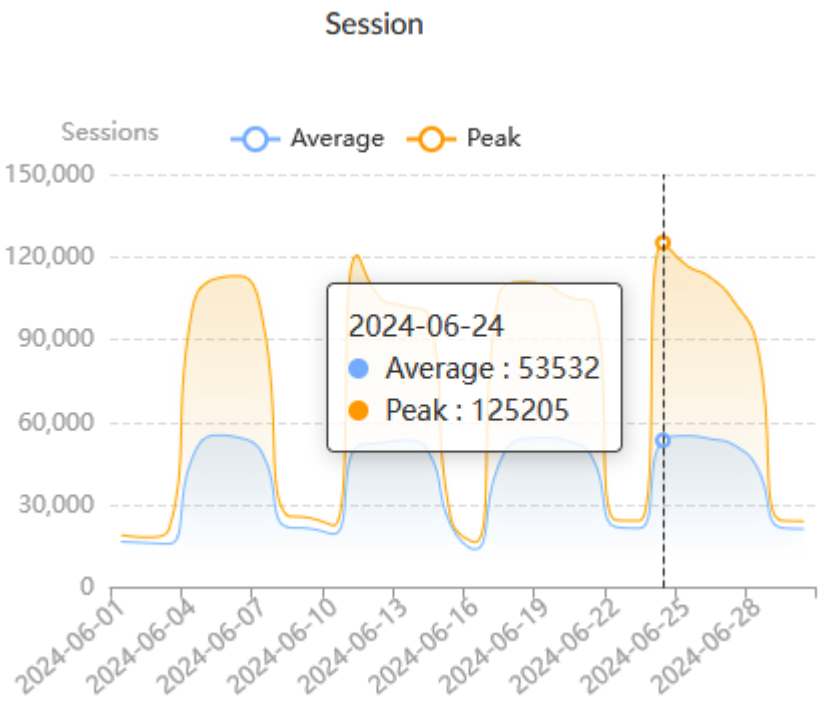
El evento del sábado 16 de junio se debió a ventana de mantenimiento programada: "Migración nueva fibra Nodo Américas". Debido a este evento, la medición de disponibilidad sin redondear para alcanzar el appliance desde la herramienta de monitoreo es del 95.648% imputable a cliente:

Availability Statistics

PERIOD	AVAILABILITY
Today	100,000 %
Yesterday	100,000 %
Last 7 Days	100,000 %
Last 30 Days	95,716 %
This Month	100,000 %
Last Month	95,648 %
This Year	99,183 %

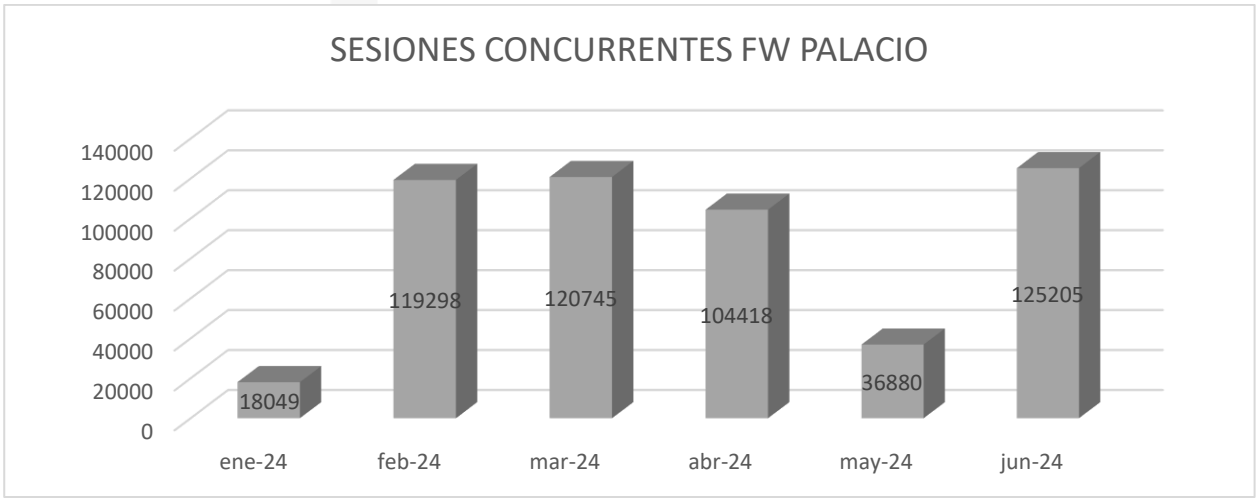
b. Cantidad de Sesiones Firewall Palacio

Durante junio se presentó un máximo de 125.205 sesiones concurrentes que están dentro del rango de sesiones soportadas por el equipo Fortigate 900G de 16 Millones.



c. Histórico de Sesiones Últimos 6 meses Firewall Palacio

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



MES	SESIONES
ene-24	18049
feb-24	119298
mar-24	120745
abr-24	104418
may-24	36880
jun-24	125205

d. Aplicaciones y protocolos por ancho de banda firewall Palacio

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

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	Microsoft.Portal			24.28 TB
2	HTTPS			10.84 TB
3	Microsoft.SharePoint			6.02 TB
4	HTTPS.BROWSER			3.80 TB
5	OneDrive			3.56 TB
6	SSL			2.29 TB
7	MS-SQL			1.89 TB
8	SMB			1.77 TB
9	Akamai-CDN			1.23 TB
10	HTTP.BROWSER			1.16 TB

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

Top Applications by Sessions

#	Application	Sessions
1	SMB	527,484,698
2	DNS	247,663,352
3	HTTP.BROWSER	48,565,449
4	Microsoft.Windows.Update	43,094,015
5	SQUID	36,136,872
6	TCP-3000	31,695,828
7	SSL	30,621,018
8	HTTPS	29,102,664
9	Microsoft.365.Portal	28,931,409
10	Microsoft.Portal	28,585,020

e. Top de IP por ancho de banda firewall Palacio.

La dirección IP 172.16.6.9 consumió la mayor cantidad de ancho de banda durante junio:

Top Bandwidth IP

#	IP	Bandwidth
1	172.16.6.9	11.69 TB
2	172.28.93.2	5.16 TB
3	172.29.154.69	732.19 GB
4	172.16.5.33	681.62 GB
5	172.28.92.23	542.56 GB
6	172.28.92.31	480.39 GB
7	172.16.4.186	396.89 GB
8	172.16.2.59	384.25 GB
9	172.28.92.36	328.31 GB
10	172.16.4.63	324.72 GB

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

stsistemascsj.blob.core.windows.net, 20.60.0.104, 13.107.138.10 y 13.107.136.10, todas en Microsoft Corporation, fueron destinos más visitados durante junio:

Top Websites and Category by Bandwidth

#	Site	Category	Bytes
1	stsistemascsj.blob.core.windows.net		11.63 TB
2	20.60.0.104		4.65 TB
3	13.107.138.10		3.61 TB
4	13.107.136.10		3.31 TB
5	172.190.220.253		1.59 TB
6	52.104.3.39		1.25 TB
7	20.168.235.216		566.07 GB
8	cndjdisciplinaenlinea.file.core.windows.net		515.72 GB
9	20.209.75.97		514.60 GB
10	190.217.24.42		473.14 GB

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

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

Top Web Users by Blocked Requests

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

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

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

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

Top Blocked Web Categories

#	Category	Requests
1	Unrated	1,528,095
2	Social Networking	711,678
3	Proxy Avoidance	645,955
4	Streaming Media and Download	520,646
5	Games	235,378
6	Society and Lifestyles	55,167
7	Entertainment	36,342
8	Newly Observed Domain	18,037
9	Phishing	6,128
10	Pornography	4,735

i. 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 junio:

Top Web IP by Allowed Requests

#	IP	Requests
1	172.16.4.90	23,130,239
2	172.28.54.20	17,918,333
3	172.16.6.9	3,960,230
4	192.168.6.13	554,251
5	172.16.2.99	477,508
6	172.17.114.39	464,463
7	172.16.1.7	413,819
8	172.16.5.100	397,878
9	172.16.3.111	337,762
10	172.28.93.101	319,238

j. 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	22,895,895
2	Search Engines and Portals	6,003,887
3	Business	1,555,247
4	Information and Computer Security	555,255
5	Web Analytics	411,411
6	Web-based Applications	133,979
7	Finance and Banking	89,167
8	Overrride_permitidas	71,140
9	Online Meeting	58,775
10	Secure Websites	25,619

k. Top de consumo ancho de banda por usuario Firewall Palacio

172.16.6.9 (host de la LAN Palacio) y 172.28.93.2 (host de la Comisión Nacional de Disciplina Judicial) presentaron la mayor cantidad de conexiones durante junio:

Top IP by Bandwidth

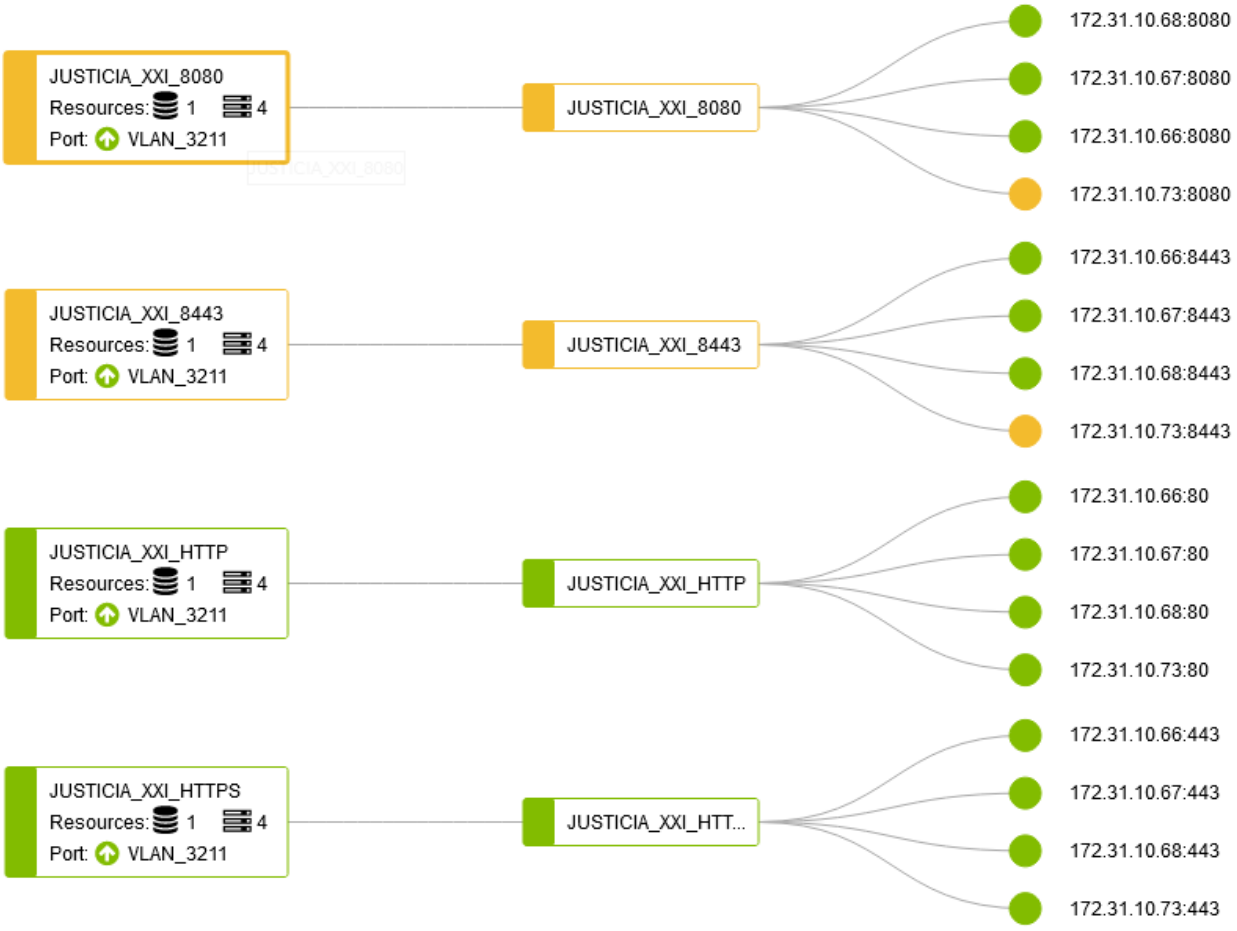
#	IP	Bandwidth	Sent	Received
1	172.16.6.9			11.69 TB
2	172.28.93.2			5.20 TB
3	172.29.154.58			4.27 TB
4	192.168.2.71			3.89 TB
5	172.17.201.252			3.41 TB
6	172.17.201.251			2.88 TB
7	10.101.250.4			1.98 TB
8	172.16.4.121			1.08 TB
9	172.17.202.250			1.08 TB
10	172.16.4.186			890.14 GB

14. BALANCEADOR DE CARGA FORTIADC

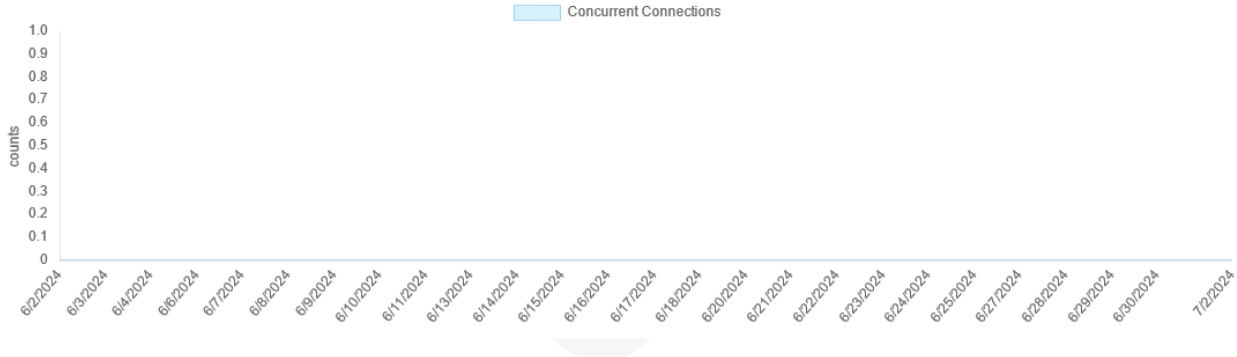
A continuación, se observan los diferentes servicios balanceados.

a. Justicia XXI

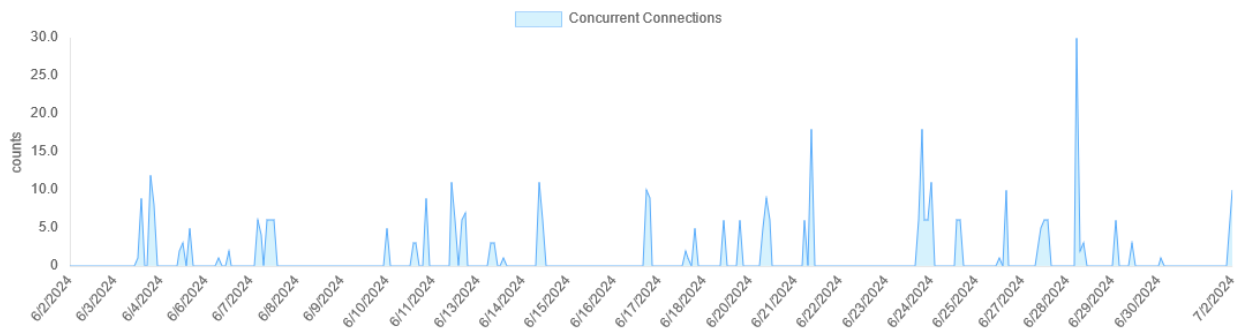
Se encuentra balanceado en el FortiADC:



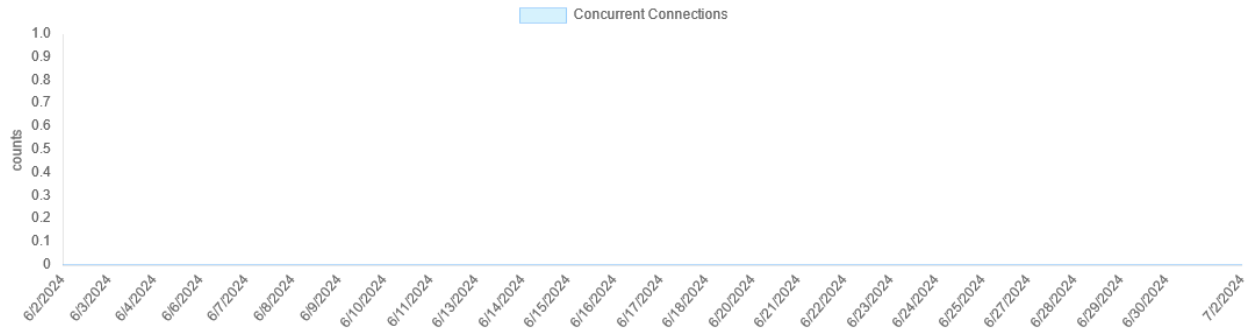
Durante junio no se presentó tráfico por el puerto 8080:



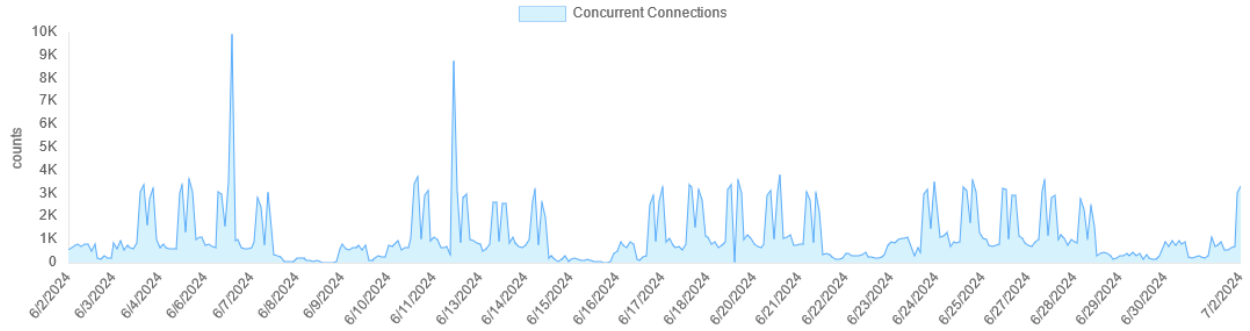
Conexiones concurrentes por el puerto 8443:



Conexiones concurrentes por el puerto 80:



Conexiones concurrentes por el puerto 443:

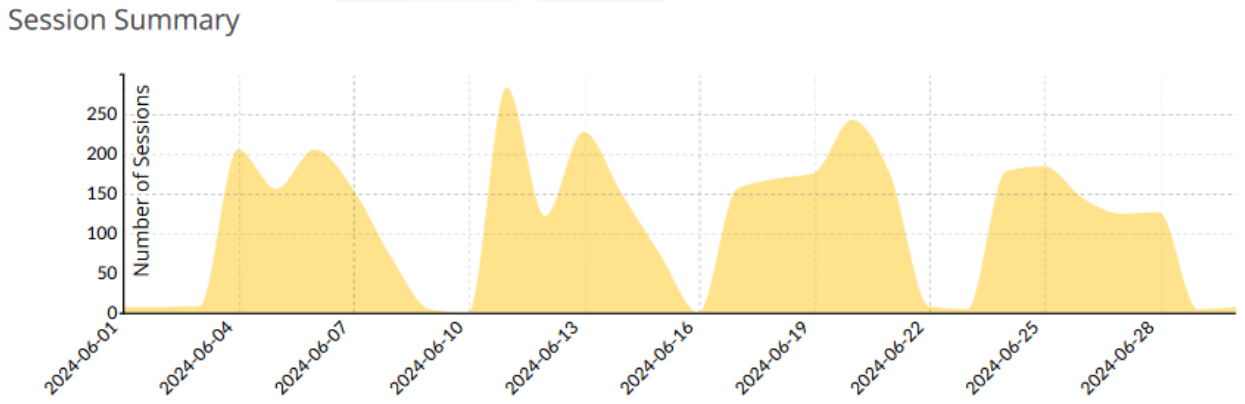


b. Kactus RDP

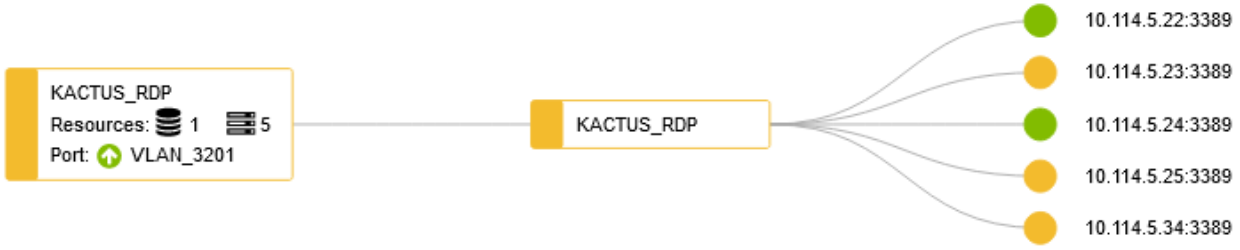
Esta aplicación se encuentra en el Firewall utilizando la siguiente configuración:

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

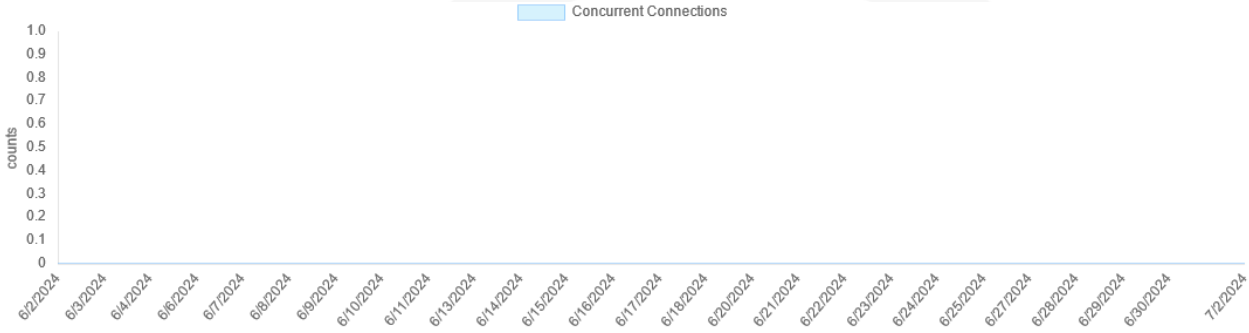
A continuación, se observa el número de sesiones concurrentes para este aplicativo.



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

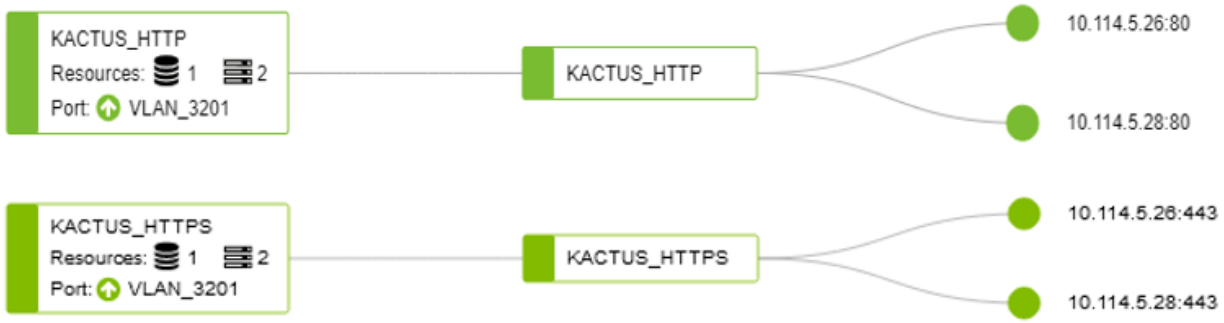


En el FortiADC no se observan sesiones concurrentes:

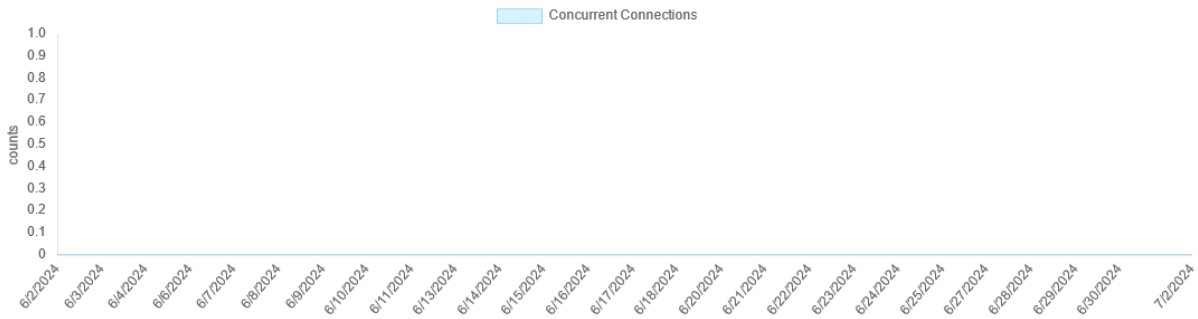


c. Kactus WEB

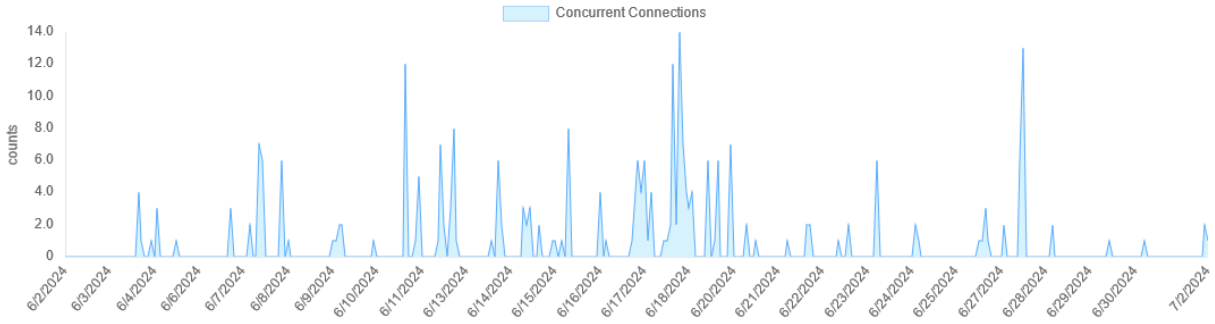
Se encuentra balanceado en el FortiADC:



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



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



d. SIRNA

Este servicio se encuentra balanceado en el FortiGate perimetral:

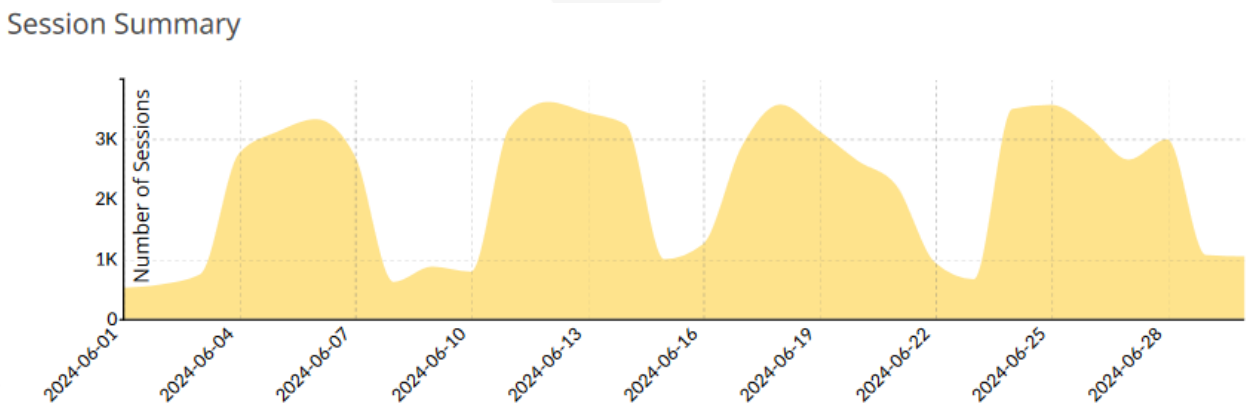
Configuración de balanceo de CRM en el Firewall.

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

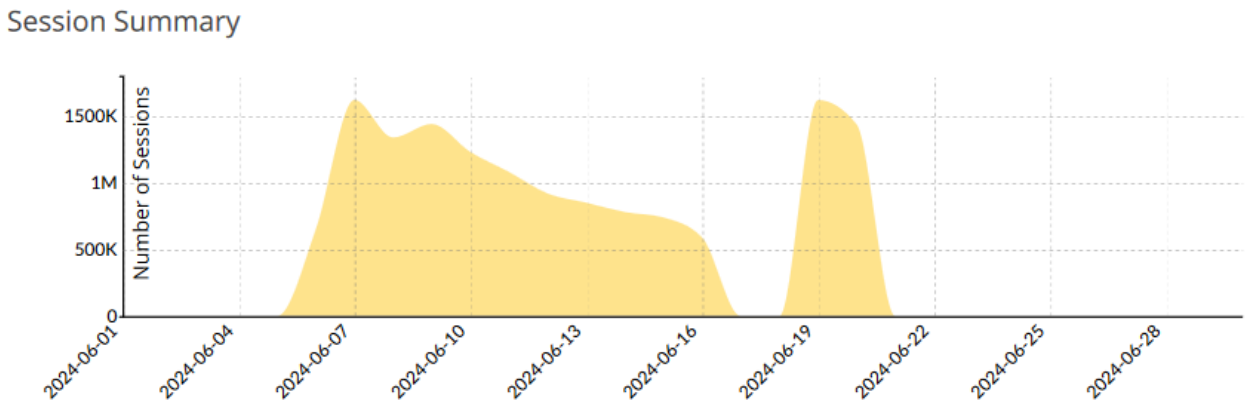
Configuración de balanceo de Sharepoint en el firewall perimetral.

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

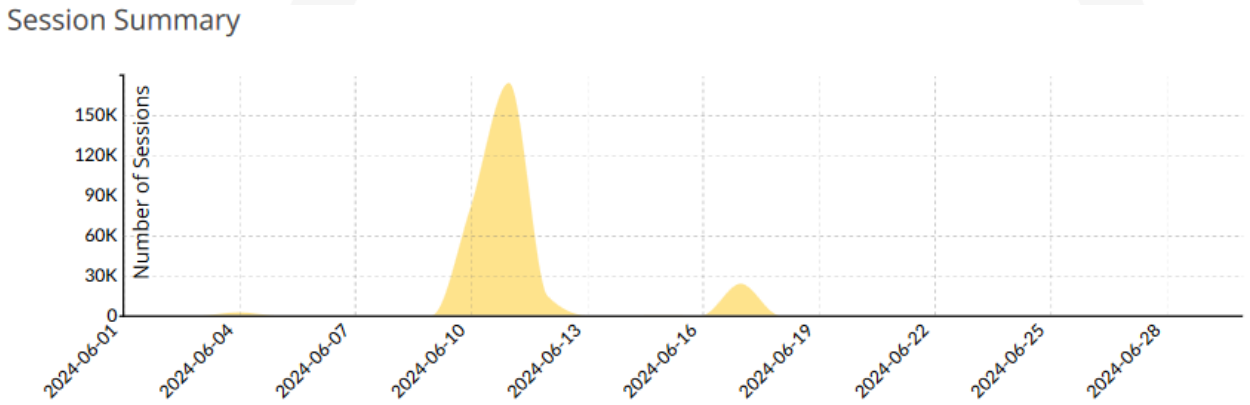
Las sesiones en el firewall para SIRNA 4443 fueron:



Las sesiones en el firewall para CRM 443 fueron:



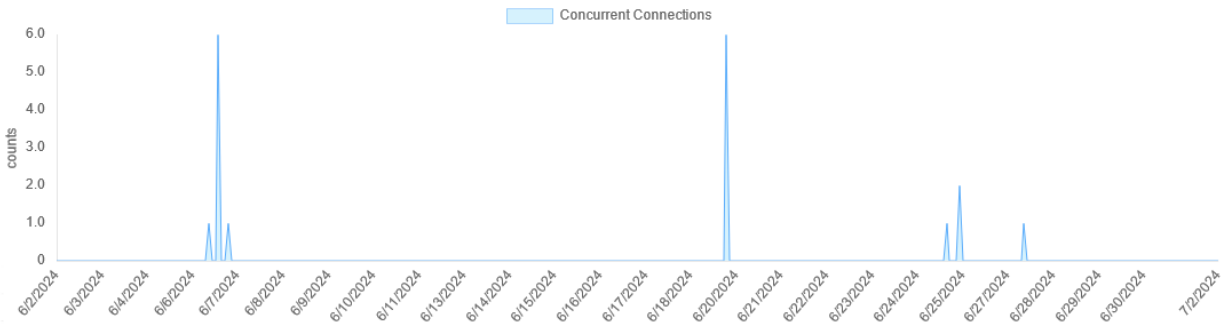
Las sesiones en el firewall para Sharepoint 444 fueron:



e. Convocatoria Peritos.

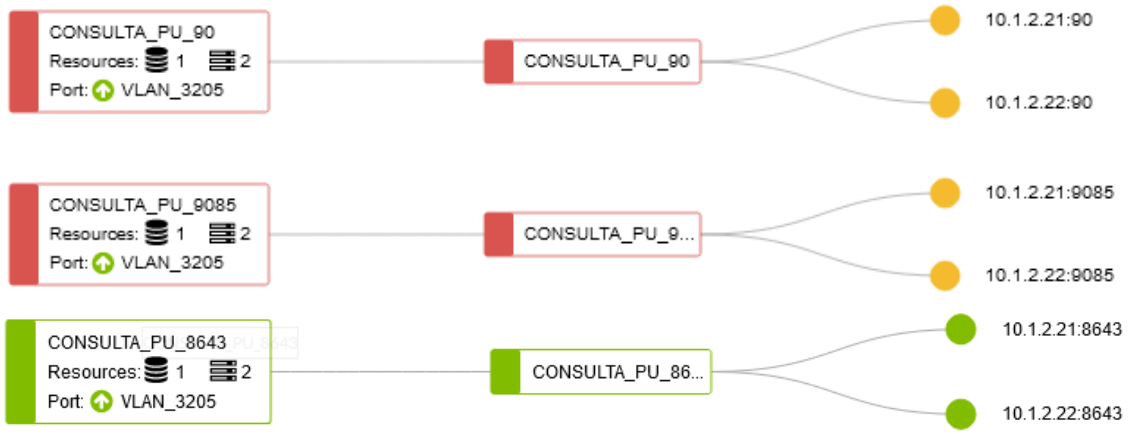
Este servicio se encuentra balanceado en el FortiADC:

Las sesiones concurrentes fueron las siguientes:

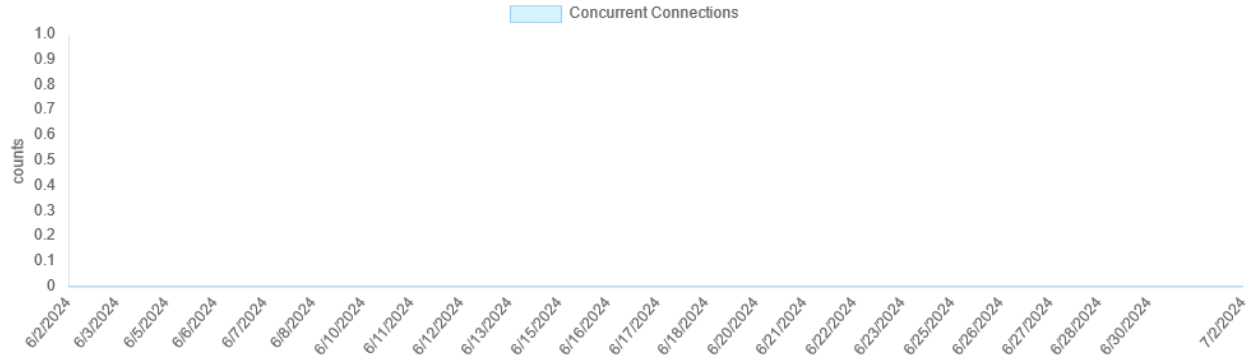


f. Consulta De Procesos Nacional Unificada (CPNU)

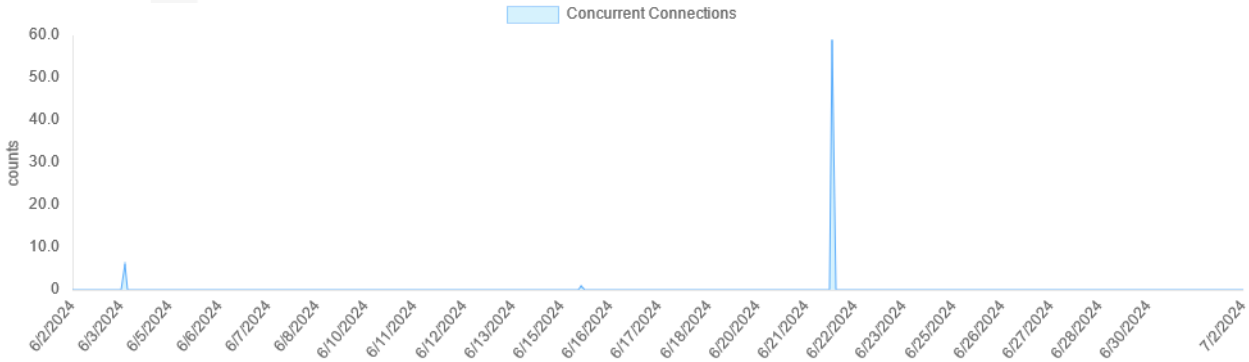
A continuación, se muestra la configuración de balanceo para esta aplicación en el FortiADC:



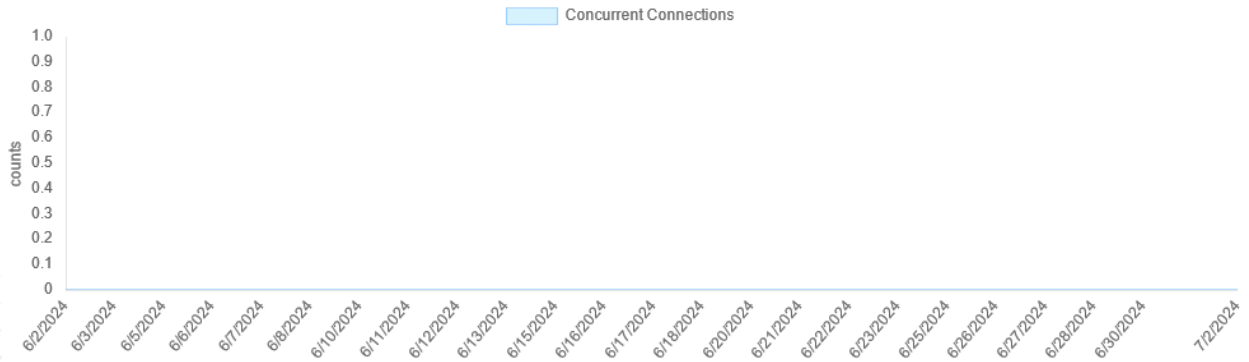
Durante junio no se tuvieron sesiones concurrentes por el puerto HTTP:



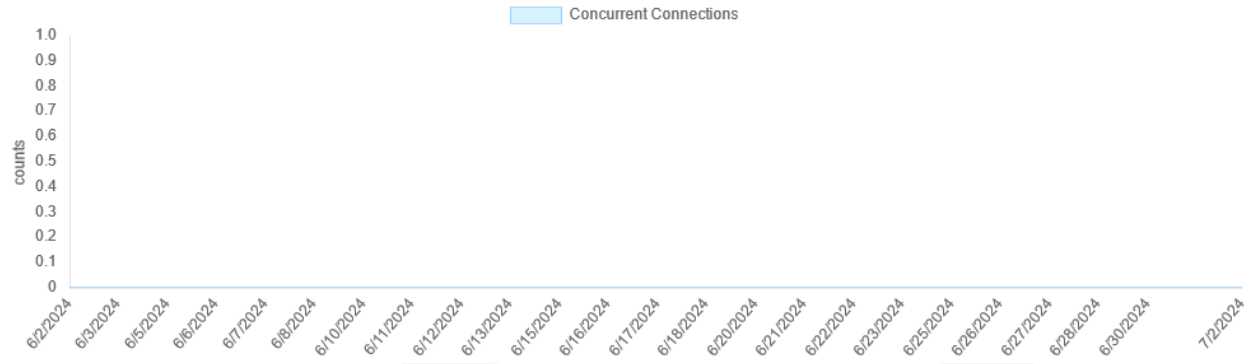
Las sesiones concurrentes por HTTPS fueron:



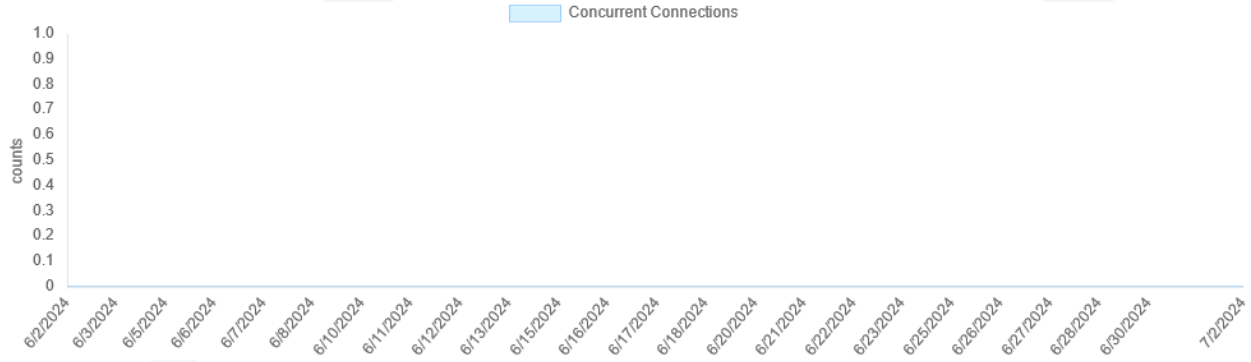
No se tuvieron sesiones concurrentes por el puerto 4431:



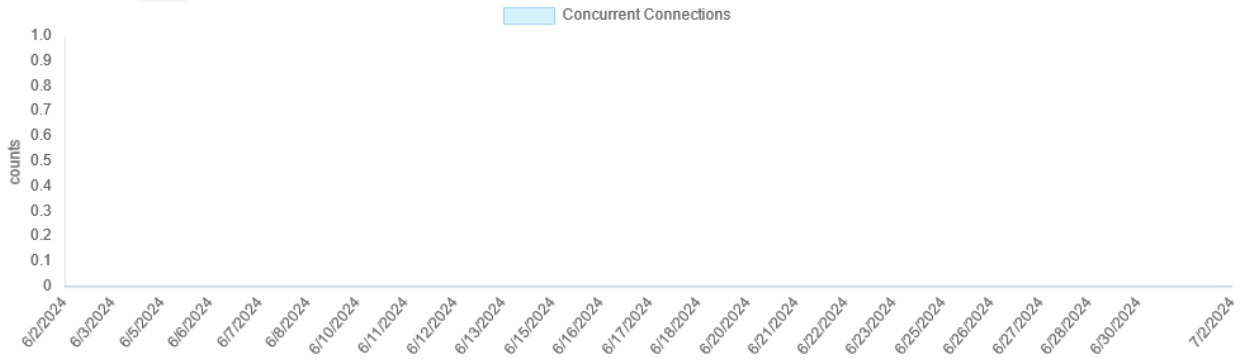
No se tuvieron sesiones concurrentes por el puerto 4432:



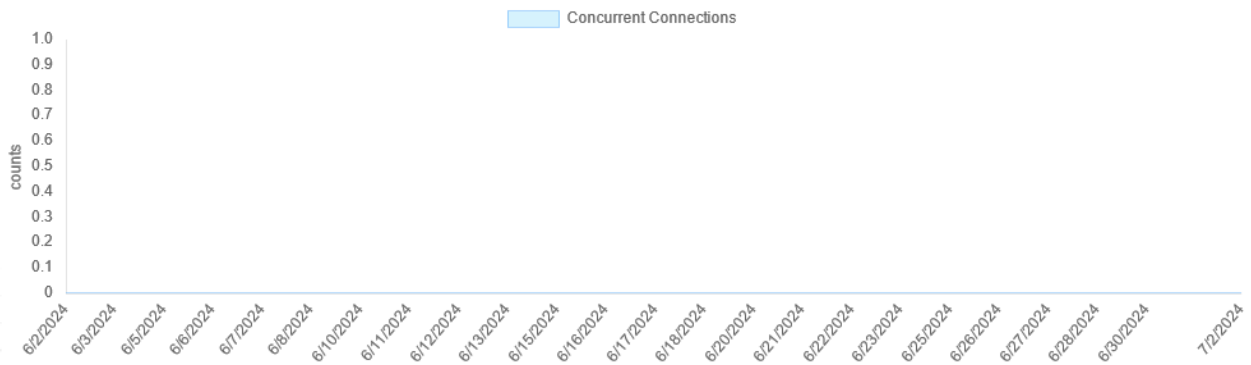
No se tuvieron sesiones concurrentes por el puerto 4435:



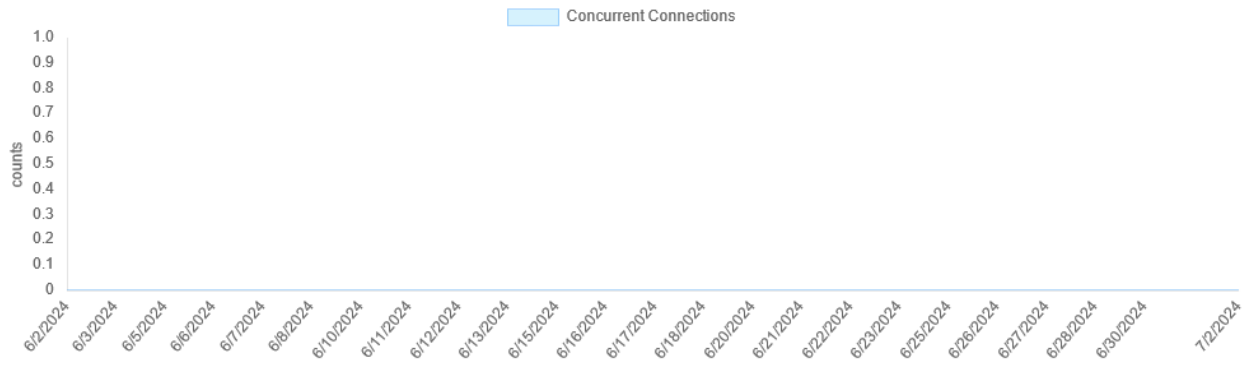
No se tuvieron sesiones concurrentes por el puerto 4436:



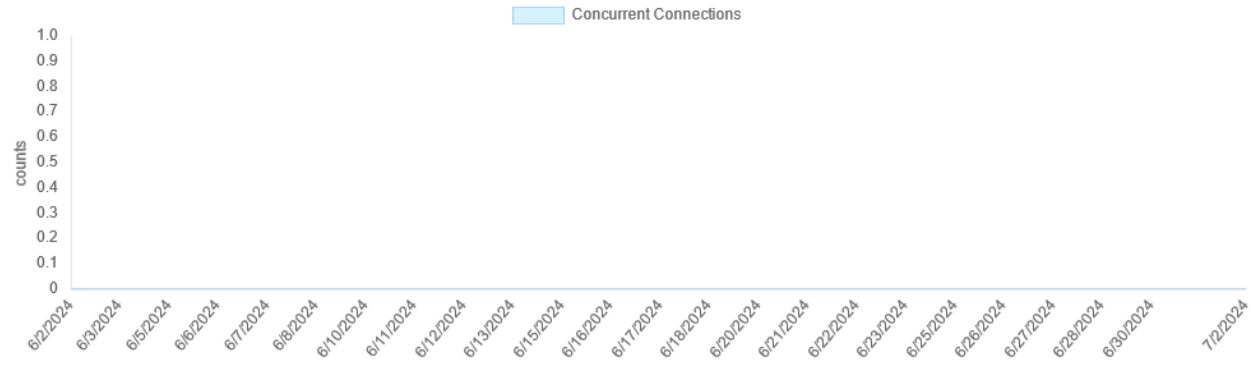
No se tuvieron sesiones concurrentes por el puerto 444:



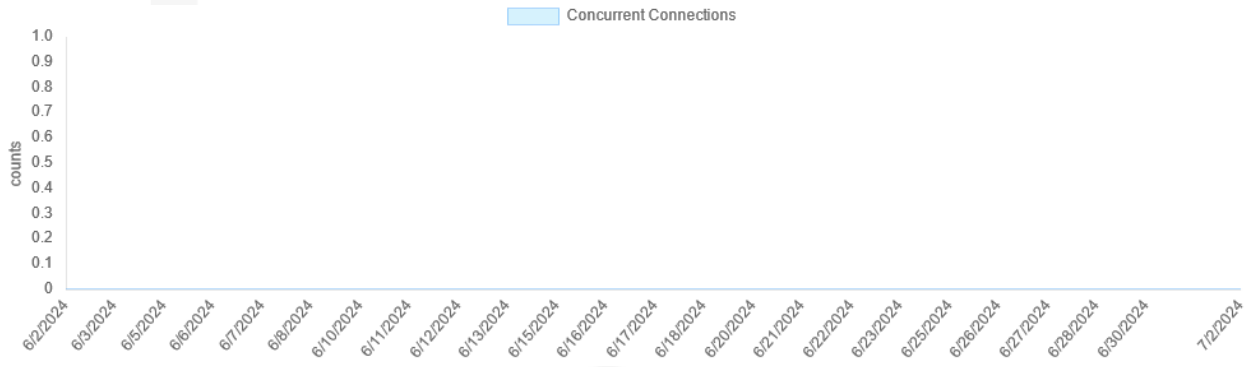
No se tuvieron sesiones concurrentes por el puerto 448:



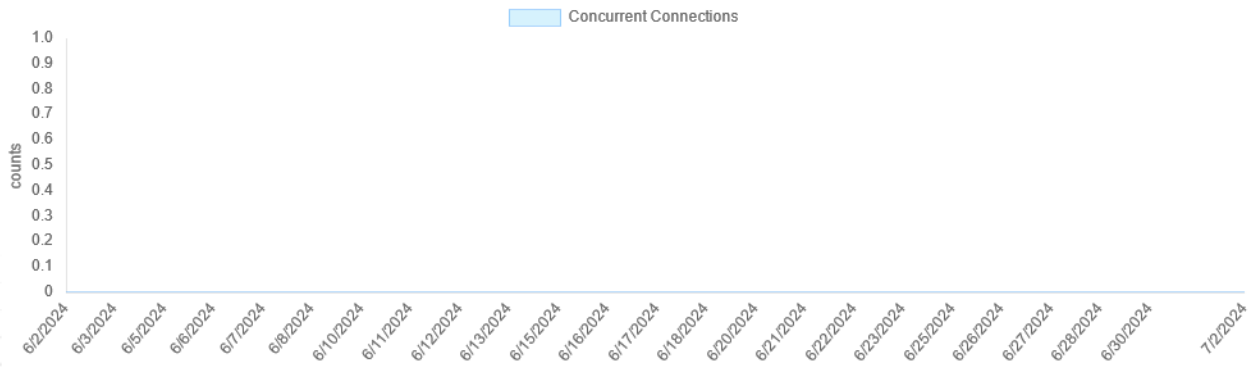
No se tuvieron sesiones concurrentes por el puerto 449:



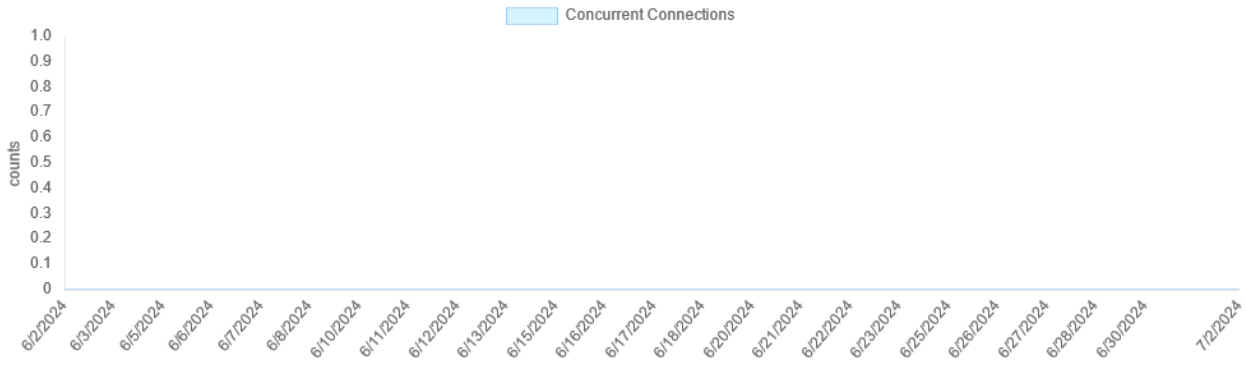
No se tuvieron sesiones concurrentes por el puerto 8085:



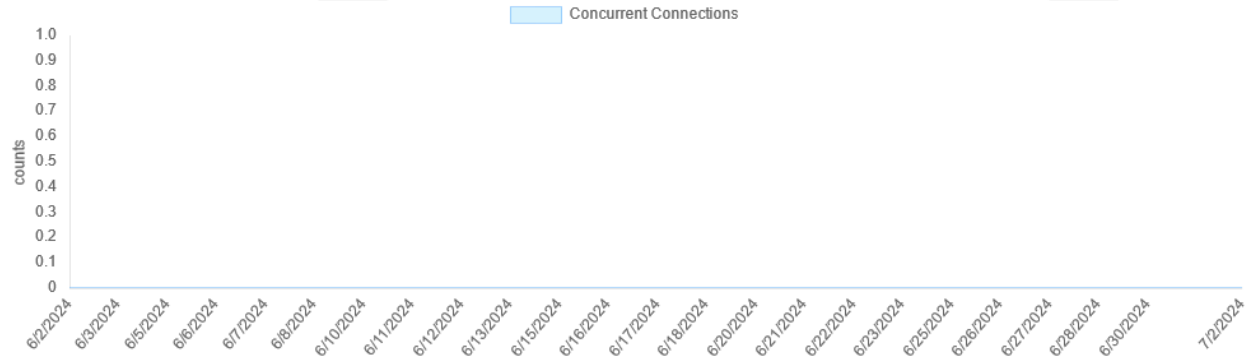
No se tuvieron sesiones concurrentes por el puerto 90:



No se tuvieron sesiones concurrentes por el puerto 9085:



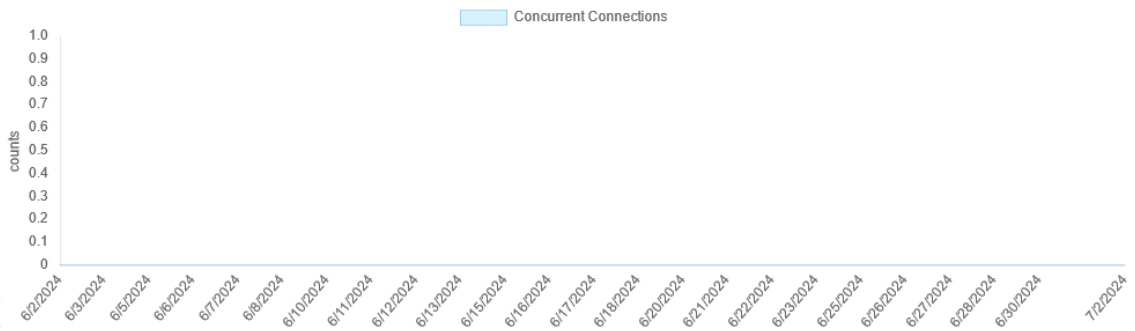
No se tuvieron sesiones concurrentes por el puerto 8643:



g. SIERJU

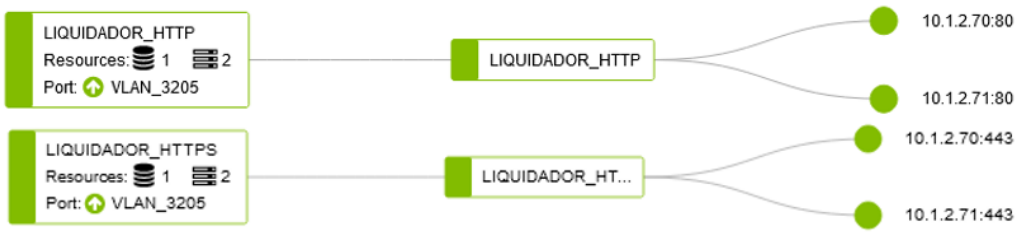
La configuración de balanceo para esta aplicación en el balanceador FortiADC es:

Durante junio no se observan conexiones concurrentes para este aplicativo:

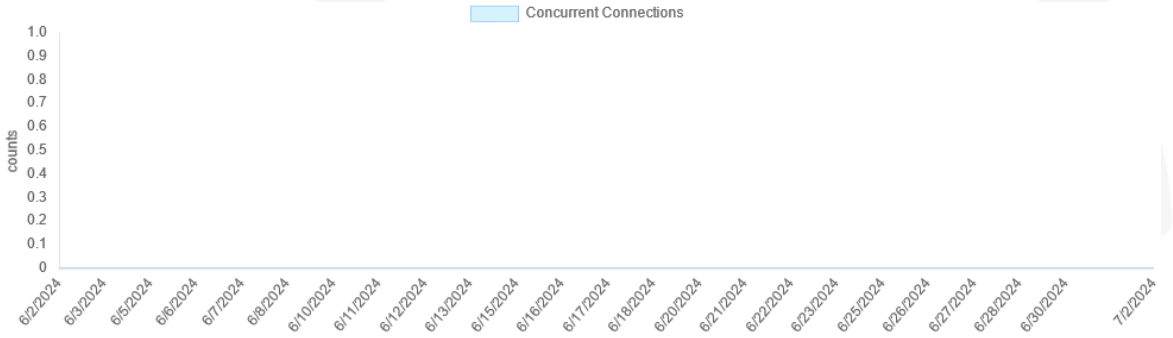


h. Liquidador de Sentencias

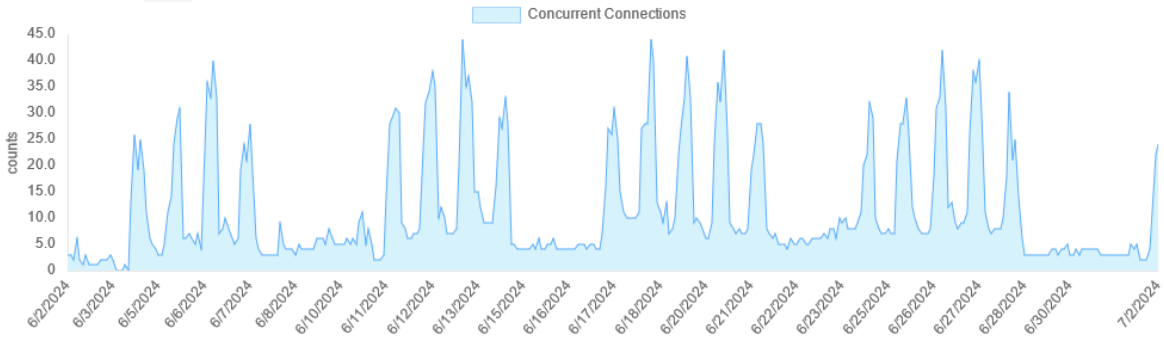
Virtual server Liquidador de Sentencias balanceador FortiADC



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



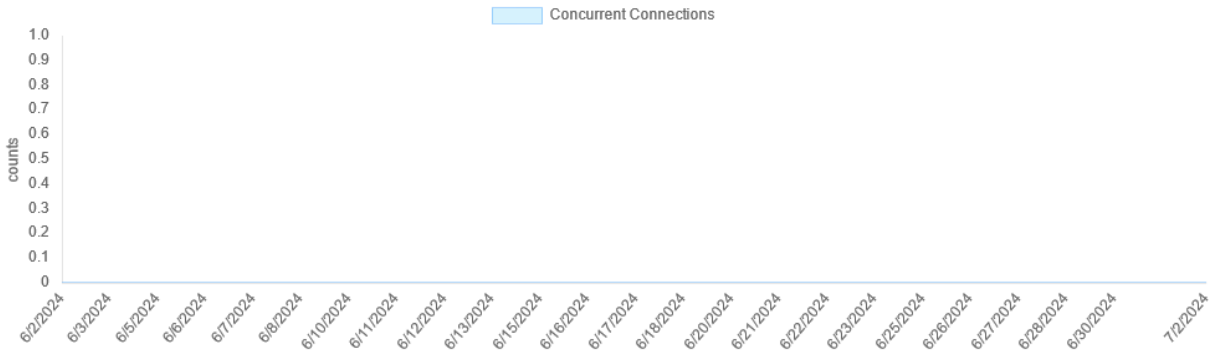
Las sesiones concurrentes por HTTPS fueron:



i. Consulta Jurisprudencia

Virtual server Consulta Jurisprudencia se encuentra en el balanceador FortiADC.

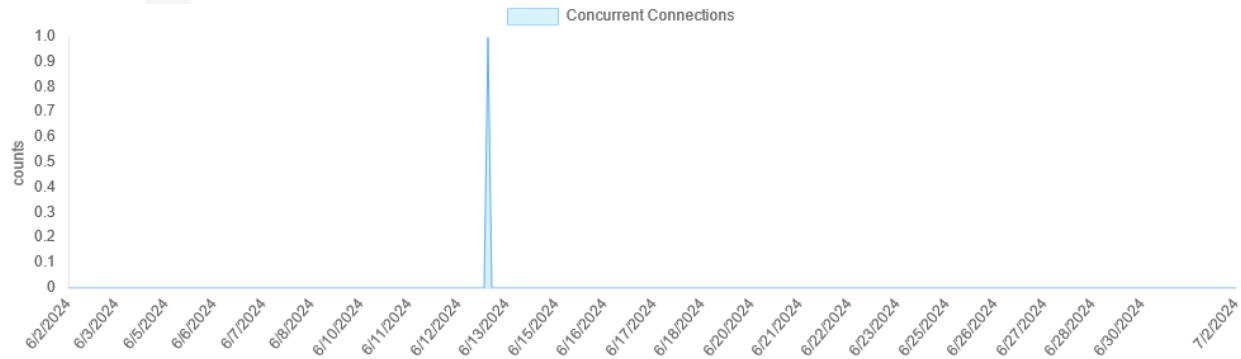
Durante junio no se observan conexiones concurrentes para este aplicativo:



j. API Gestión de Audiencias

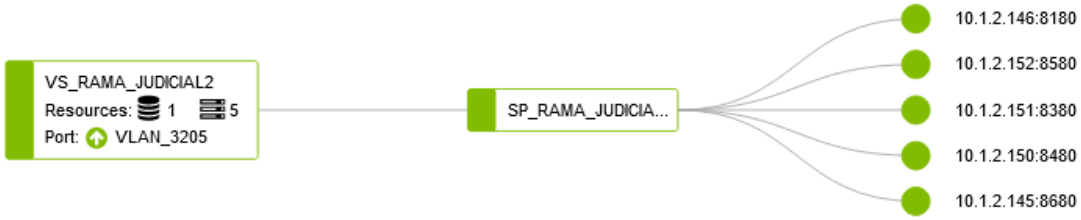
Virtual server API Gestión de Audiencias balanceador FortiADC.

Las sesiones concurrentes por HTTPS para este aplicativo:

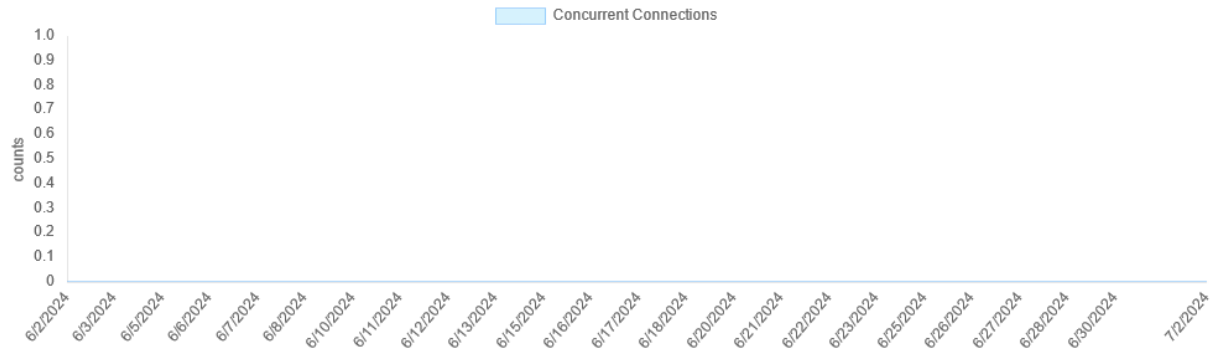


k. Portal Alterno de la Rama Judicial

Se encuentran balanceado en el FortiADC:

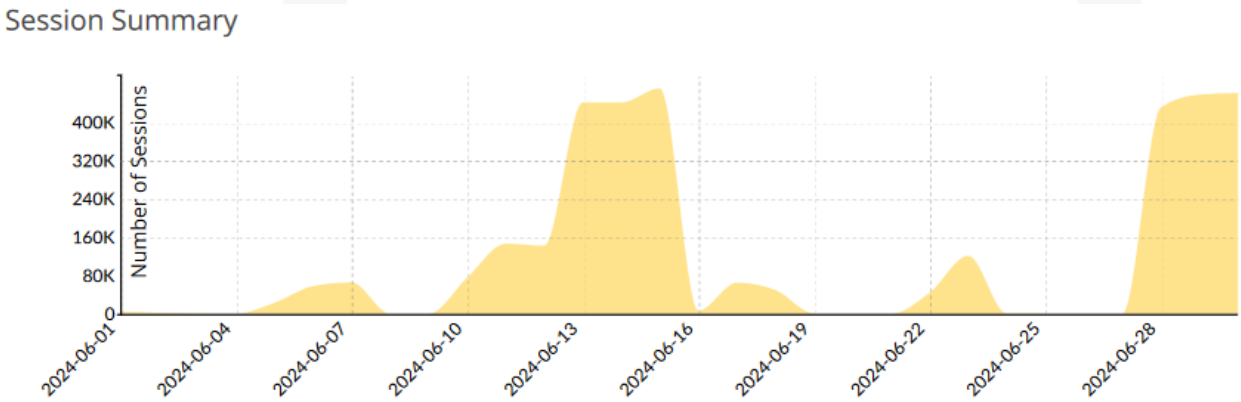


Durante junio no se observan conexiones concurrentes para este aplicativo:



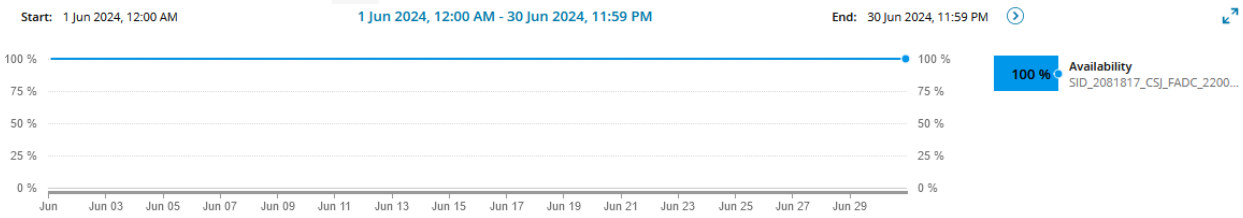
l. Portal de la Rama Judicial

Las sesiones Historico_Portal Rama Judicial fueron:

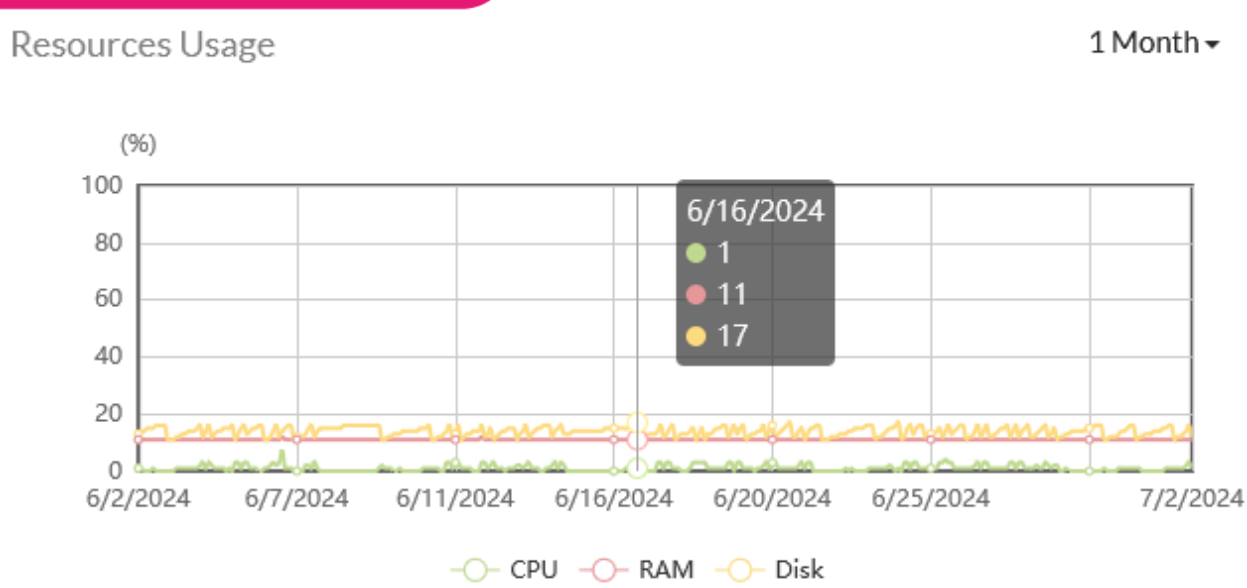


m. Disponibilidad y performance.

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



Durante junio se observa consumo de CPU del 1%, memoria 11% y disco 17%:



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

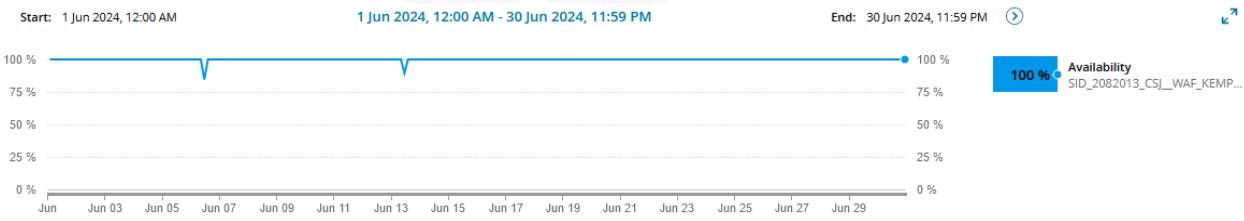
Para la protección de las aplicaciones web se tienen configuradas las siguientes políticas en los Firewall de Aplicaciones Web:

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

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

a. Web application firewall datacenter principal IFX.

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



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

El evento observado en la gráfica del 6 de junio obedece una actividad controlada en los equipos perimetrales y de seguridad del cliente, donde se realizó actualización del

servicio SNMP a SNMP 3, el equipo estuvo siempre operativo y sin afectación, solo se generó alarma a nivel monitoreo.

El evento del 13 de junio se debió a pequeñas latencias en los canales de tráfico del CSJ, durante el mes el equipo estuvo 100% disponible. Debido a estos eventos, la medición de disponibilidad sin redondear para alcanzar el appliance desde la herramienta de monitoreo es del 99.877% imputable a cliente:

Availability Statistics

PERIOD	AVAILABILITY
Today	100,000 %
Yesterday	100,000 %
Last 7 Days	100,000 %
Last 30 Days	99,880 %
This Month	100,000 %
Last Month	99,877 %
This Year	99,865 %

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

La aplicación web más consultada durante junio fue procesos.ramajudicial.gov.co_procesoscs CONSULTA AZUL (172.17.201.26:8443) con 17´608.124 sesiones web correspondiente al 31.98% del total durante junio:

#	Name	Virtual IP Address	Total Conns	% del total
1	procesos.ramajudicial.gov.co_procesoscs CONSULTA AZUL	172.17.201.26:8443	17608124	31,38%
2	procesojudicial.ramajudicial.gov.co TYBA PRUEBAS	172.17.201.249:443	13528015	24,11%
3	publicacionesprocesales.ramajudicial.gov.co - 190.217.24.175	172.17.201.100:443	10020062	17,86%
4	nuevoportal.ramajudicial.gov.co Y cndj.gov.co 190.217.24.176	172.17.201.101:443	6091189	10,85%
5	consejodeestado.gov.co - 190.217.24.60	172.17.201.52:443	3021475	5,38%
6	siicor.corteconstitucional.gov.co - 190.217.24.62	172.17.201.13:443	2739975	4,88%
7	csjinfo.ramajudicial.gov.co	172.17.201.27:443	370615	0,66%
8	sirna.ramajudicial.gov.co	172.17.201.28:443	344478	0,61%
9	www.consejodeestado.gov.co - 190.217.24.60 - Redirect	172.17.201.52:80	277845	0,50%
10	consultajurisprudencial.ramajudicial.gov.co 8080	172.17.201.110:8080	250153	0,45%
	Otras aplicaciones		1866686	3,33%
	Total		56118617	100,00%

c. Top de peticiones por país WAF principal IFX.

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

Top 10 Countries

Total

Country	Requests	Blocked
Colombia	22435498	4509188
Private	3591791	1290700
United States	15158148	688398
Spain	369730	210659
Argentina	257350	52965
Brazil	251320	25222
Russia	892661	10377
Bangladesh	114741	9327
Costa Rica	27480	7864
IPrep	6539	6539

d. Top de ataques por política WAF principal IFX.

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

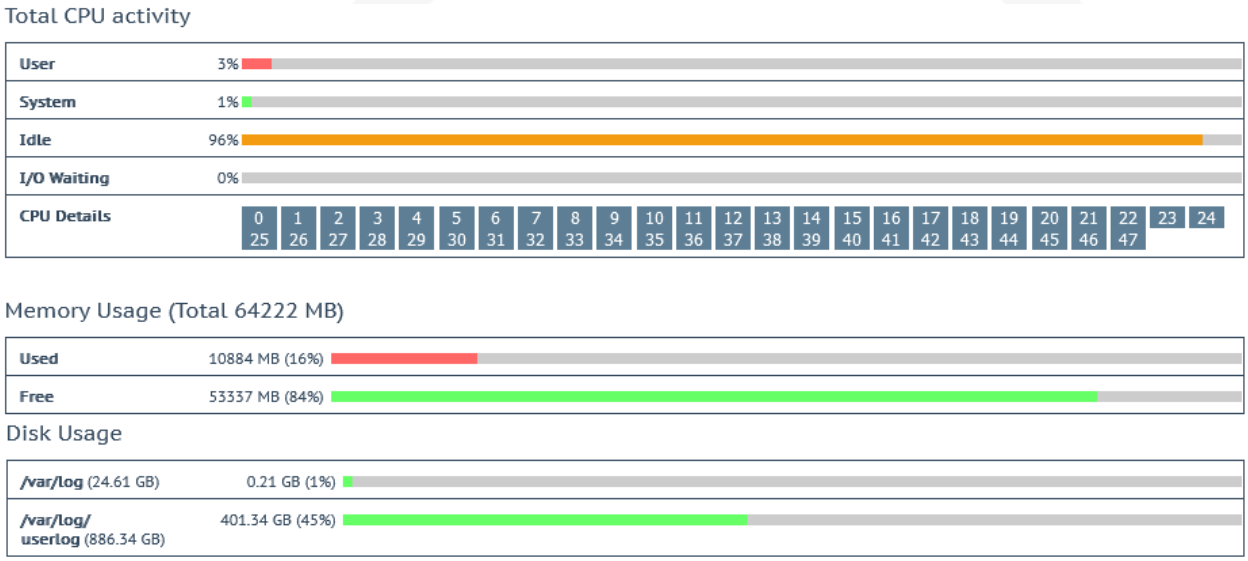
#	Name	Virtual IP Address	Total Events	%del total
1	publicacionesprocesales.ramajudicial.gov.co - 190.217.24.175	172.17.201.100:443	6049876	87,99%
2	consejodeestado.gov.co - 190.217.24.60	172.17.201.52:443	280590	4,08%
3	csjinfo.ramajudicial.gov.co	172.17.201.27:443	209838	3,05%
4	siicor.corteconstitucional.gov.co - 190.217.24.62	172.17.201.13:443	181200	2,64%
5	nuevoportal.ramajudicial.gov.co Y cndj.gov.co 190.217.24.176	172.17.201.101:443	80939	1,18%
6	procesos.ramajudicial.gov.co_procesoscs CONSULTA AZUL	172.17.201.26:8443	37022	0,54%
7	procesojudicial.ramajudicial.gov.co TYBA PRUEBAS	172.17.201.249:443	26977	0,39%
8	jurisprudencia.ramajudicial.gov.co - ayudajurisprudencia.ramajudicial.gov.co _ 8446 - 190.217.24.193-DOWN 7 JUNIO 2024	172.17.201.29:8446	1181	0,02%
9	videoteca.ramajudicial.gov.co Holocausto_lector_videoteca_sidn_443	172.17.201.54:443	1083	0,02%
10	sirna.ramajudicial.gov.co	172.17.201.28:443	711	0,01%

	Otras aplicaciones		6052	0,09%
	Total		6875469	100,00%

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

e. Consumo de recursos WAF principal IFX.

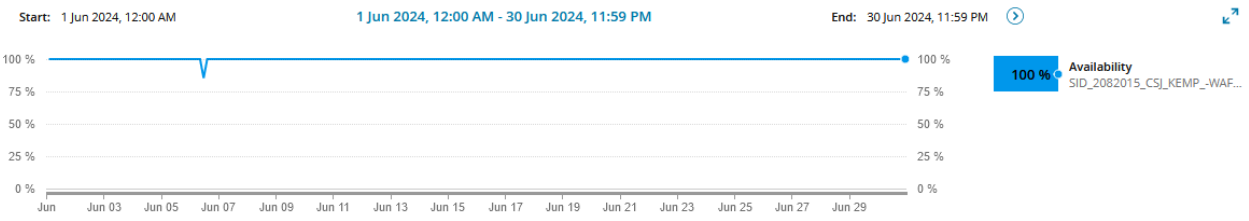
El WAF KEMP de Torre Central presentó consumo de CPU del 3%, memoria de 16% y disco en un 45%.



16. TRÁFICO DE WEB APPLICATION FIREWALL (WAF) CAN

a. Disponibilidad WAF CAN.

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



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

El evento observado en la gráfica del 6 de junio obedece una actividad controlada en los equipos perimetrales y de seguridad del cliente, donde se realizó actualización del

servicio SNMP a SNMP 3, el equipo estuvo siempre operativo y sin afectación, solo se generó alarma a nivel monitoreo. Debido a este evento, la medición de disponibilidad sin redondear para alcanzar el appliance desde la herramienta de monitoreo es del 99.931% imputable a cliente:

Availability Statistics

PERIOD	AVAILABILITY
Today	100,000 %
Yesterday	100,000 %
Last 7 Days	100,000 %
Last 30 Days	99,932 %
This Month	100,000 %
Last Month	99,931 %
This Year	99,170 %

b. Uso de políticas de servidores WAF CAN.

La aplicación más consultada durante junio fue cortesuprema.gov.co_Palacio con un 73.49% del total:

#	Name	Virtual IP Address	Total Conns	% del total
1	cortesuprema.gov.co_Palacio	172.17.202.239:443	8142309	73,49%
2	sso.cortesuprema.gov.co	172.17.202.141:443	430417	3,88%
3	cortesuprema_Palacio Redirect	172.17.202.239:80	323247	2,92%
4	samairj.consejodeestado.gov.co	172.17.202.38:443	314171	2,84%
5	sso.cortesuprema.gov.co Redirect	172.17.202.141:80	308386	2,78%
6	restituciontierras.ramajudicial.gov.co	172.17.202.37:443	263106	2,37%
7	convocatorias.consejodeestado.gov.co	172.17.202.147:443	239303	2,16%
8	linkce.consejodeestado.gov.co	172.17.202.42:443	126106	1,14%
9	serviciopdf.ramajudicial.gov.co	172.17.202.7:443	100348	0,91%
10	siapoas.ramajudicial.gov.co	172.17.202.43:443	94969	0,86%
	Otras Aplicaciones		737472	6,66%
	Total:		11079834	100,00%

c. 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	3829344	141228
IPrep	6177	6177
China	26628	3208
Japan	6182	1536
Private	763978	1234
Singapore	26729	900
Russia	34453	634
Hong Kong	2772	477
Ukraine	3981	426
Spain	12124	308

d. Top de ataques por política WAF CAN.

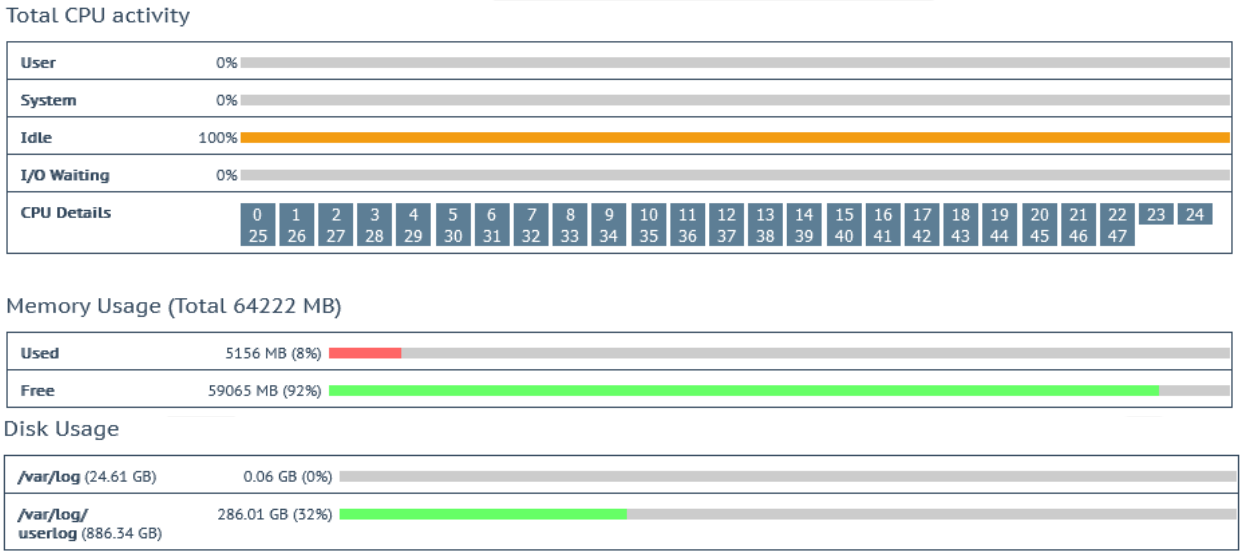
La siguiente tabla muestra el top 10 de las reglas o virtual services que proporcionaron mayor protección contra ataques a las aplicaciones web durante junio. Sobre la aplicación cortesuprema.gov.co_Palacio ha sido prevenida la mayor cantidad de ataques durante junio:

#	Name	Virtual IP Address	Total Events	% del total
1	cortesuprema.gov.co_Palacio	172.17.202.239:443	150509	83,01%
2	convocatorias.consejodeestado.gov.co	172.17.202.147:443	2777	1,53%
3	capacitacion.ramajudicial.gov.co 443	172.17.202.13:443	2623	1,45%
4	efinominapruebas.ramajudicial.gov.co	172.17.202.45:443	2476	1,37%
5	relatoria.cndj.gov.co	172.17.202.66:443	2021	1,11%
6	restituciontierras.ramajudicial.gov.co	172.17.202.37:443	1897	1,05%
7	siapoas.ramajudicial.gov.co	172.17.202.43:443	1605	0,89%
8	predepjudiciales.ramajudicial.gov.co	172.17.202.55:443	1578	0,87%
9	samairj.consejodeestado.gov.co	172.17.202.38:443	1494	0,82%
10	predesarchive.ramajudicial.gov.co	172.17.202.53:443	1450	0,80%
	Otras aplicaciones		12887	7,11%
	Total		181317	100,00%

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

e. Consumo de recursos WAF CAN.

El WAF KEMP del CAN presentó consumo de CPU del 0%, memoria de 8% y disco en un 32%.



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

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

Otros certificados digitales presentan las siguientes vigencias:

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

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

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

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

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

g. Intentos login fallidos a Firewalls

Durante junio se presentaron 32 intentos de login administrativo hacia los firewall perimetrales. El acceso administrativo se encuentra protegido controles de "Restrict login to trusted hosts":

Top 100 Failed Admin Logins

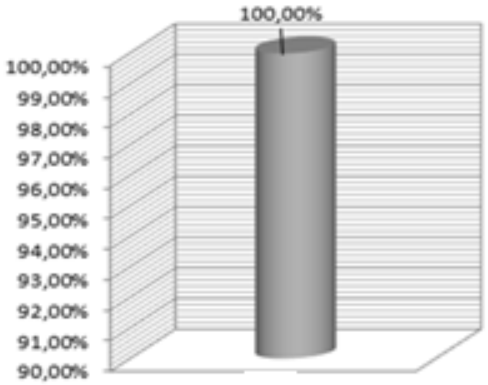
#	Login Source	User Name	Total Number of Failed Logins
1	https(181.214.218.168)	root	7
2	https(194.32.122.8)	administrator	6
3	https(216.24.216.117)	admin	6
4	https(178.175.130.251)	admin	6
5	https(95.181.236.131)	support	6
6	https(84.239.40.220)	admin	5
7	https(84.239.40.199)	User	5
8	https(192.168.193.23)	Unknown	3
9	https(185.11.61.124)	itsupport	2
10	https(192.168.61.177)	jmunozl	2
11	https(192.168.61.177)	teccoorsecpop	2
12	https(172.18.2.241)	RBrinexC	2
13	https(172.16.54.46)	ew	1
14	https(192.168.193.23)	gcastilg	1
15	https(172.18.1.187)	jgarcias	1
16	https(172.18.2.241)	jgarcias	1
17	https(172.16.54.45)	Unknown	1
18	https(192.168.61.177)	Unknown	1
19	https(172.16.54.215)	vgalvis	1
20	https(193.201.9.129)	348934jt80gfj093jswerfg	1
21	https(190.60.96.34)	vgalvis	1
22	https(192.168.123.15)	ARendonC	1
23	https(172.18.2.239)	JParraRu	1
24	https(192.168.123.15)	MAYUDAETB	1
25	https(172.18.2.239)	MAbrilN	1
26	https(192.168.123.15)	MAyudaETB	1
27	https(172.18.2.239)	MMendozT	1
28	https(172.18.2.241)	MMendozT	1
29	https(193.201.9.129)	admin	1
30	https(193.201.9.129)	admin1	1
31	https(193.201.9.129)	admin2	1
32	https(172.18.1.187)	dorjuelb	1

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

17. DISPONIBILIDAD SEGURIDAD GLOBAL DEL MES DE JUNIO

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

MES	DISPONIBILIDAD (%)
JUNIO	100%



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

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

18. 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)

19. 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	$ 5.879.931.983,47
% Valor facturado	37,90%
Valor pagado a la fecha	$ 5.879.931.983,47
% Valor pagado	37,90%

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

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

20. 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 con 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