REPORTE MENSUAL

RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA

OC124016

ABRIL 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 ABRIL de 2024 Fecha de final: 30 de ABRIL 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 190000049	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.

3. 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 ABRIL de 2024 es de: **4348862 (P)**

El almacenamiento total presentado adicional es de: **4231001 (P)**

Total, contratado de Almacenamiento SAN alto rendimiento: **4150000 (4.15P)**

Acorde a la información suministrada con anterioridad, a la fecha la entidad supera en 81001GB, el almacenamiento contratado

(Remitirse al anexo "**Inventario_Servicios_CSJ_ABRIL_2024.xls**" para ver el detalle)

4. 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, de conformidad con las solicitudes de la Entidad, a corte 30 de ABRIL de 2024 es de **918300 GB** y se desglosa de la siguiente manera:

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

- **Acorde a la información suministrada con anterioridad, a la fecha la entidad supera en 195000 GB, el almacenamiento BK de datos diario y semanal.**

- Total, contratado de Almacenamiento BK de datos mensual: 250000 GB

- **Acorde a la información suministrada con anterioridad, a la fecha la entidad supera en 123300 GB, el almacenamiento BK de datos mensual.**

Actualmente la entidad cuenta con 208 máquinas virtuales y 2 máquinas físicas en producción y estado ON, de las cuales se ejecutan backups 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.

(Remitirse al anexo "**Inventario_Servicios_CSJ_ABRIL_2024.xls**" para ver el detalle)

5. 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 ABRIL 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_ABRIL_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

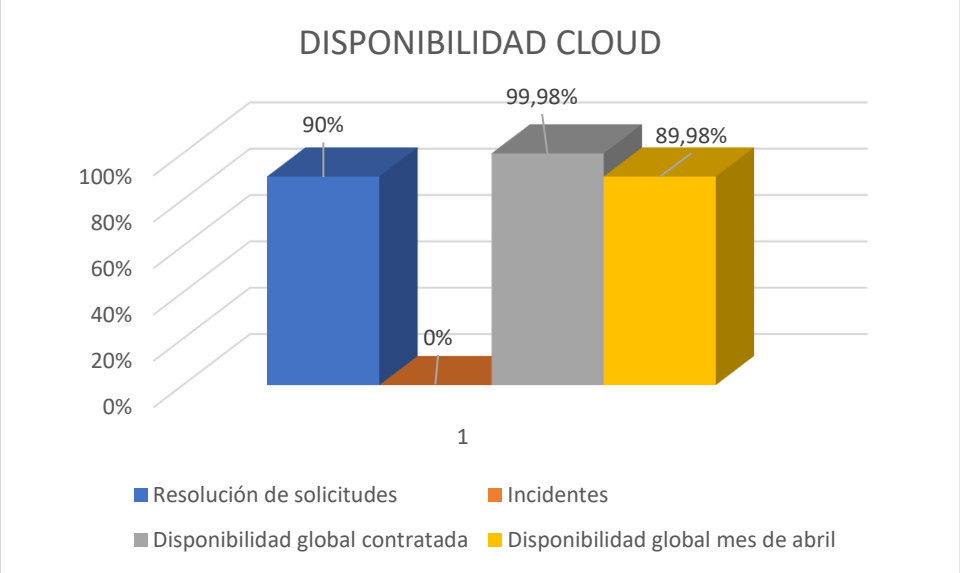
- **Fuse:** Línea OC 17
- **Gestión grabaciones:** Líneas de OC 12,13, 14,15,17,19,20,22,23,25,28,35,36 y 38
- **InsightVM console:** línea OC 27
- **InsightVM scan:** línea OC 27
- **Insightappsec scan:** línea OC 25
- **Isigthwm scan:** línea OC 26
- **Ivanti:** Líneas de OC 17,18,20,21,22,28,38 y 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_ABRIL_2024.xls**" para ver el detalle "maquinas")

7.DISPONIBILIDAD GLOBAL CLOUD DEL MES DE ABRIL

Disponibilidad Global mes de abril	Numero de tickets mes de abril	Imputabilidad por ANS
	49 solicitudes	**3 solicitudes**
	4 incidentes	**0 incidentes**
89,98%	Total 53 tickets	3 tickets



CONTROL DOCUMENTAL

ELABORADO POR

Fecha	Autor	Ingeniero
03-05-2024	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 abril a 30 de abril del 2024.

CONSUMO TOTAL HORAS MES DE ABRIL	
• Casos Reportados Netsuite	107
Sesiones de Seguimiento	8
Sesiones de Trabajo	0
Casos Escalados Medio Digital - Whatsapp	5
Horas Disponibilidad del Recurso Fines de Semana	280
Total Horas Consumidas de las 300 - Experto Master	400

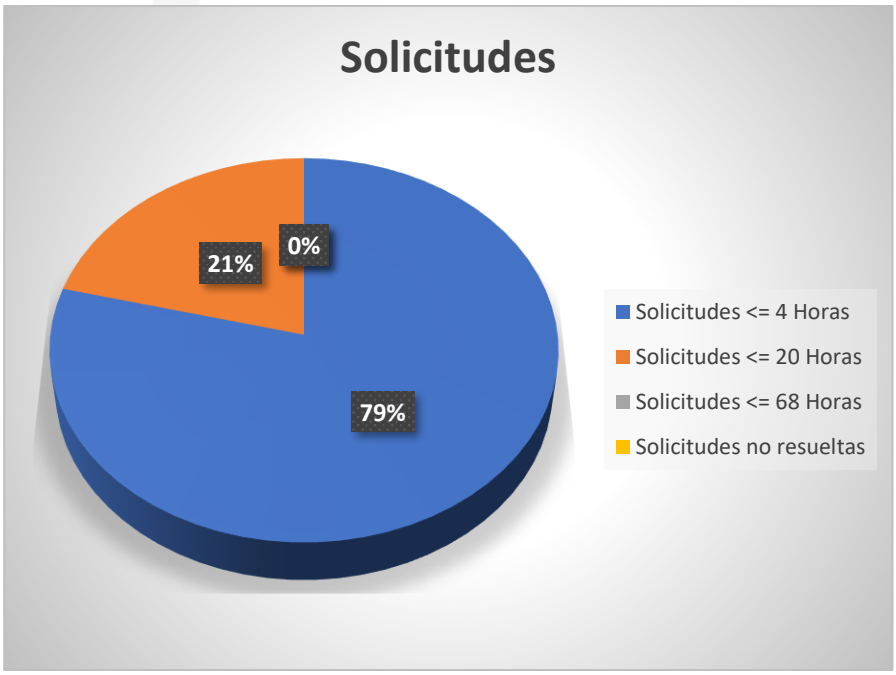
2. INDICADORES DEL CENTRO CONSOLIDADO DE SERVICIOS

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

	Volumen en 1 abril a 30 de abril
Casos Reportados	19
Solicitudes	19
Incidencias	0
WA - AF	0

2.1 TASA DE RESOLUCIÓN DE PROBLEMAS

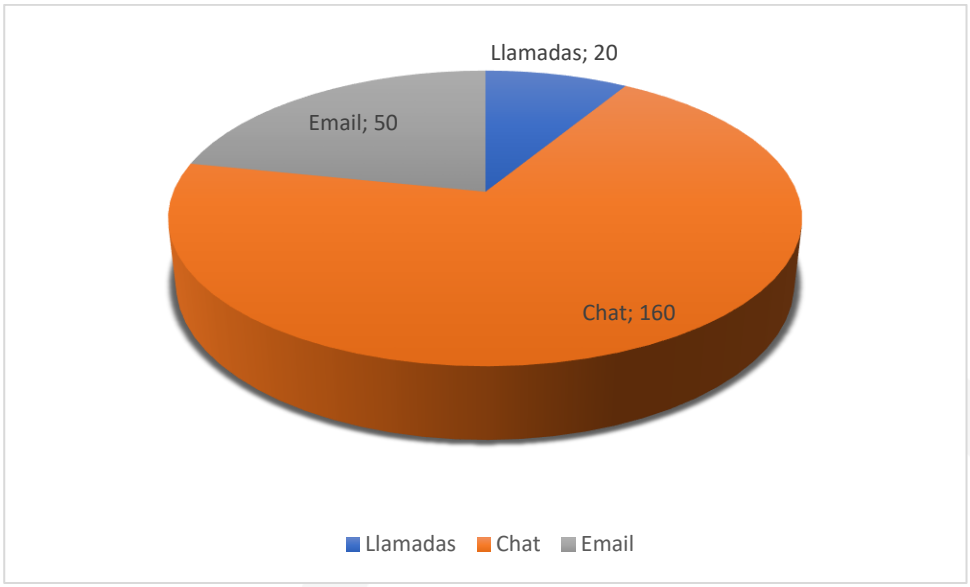
Tiempo de Gestión	Solicitudes
Solicitudes resueltas < = 4 horas	15
Solicitudes resueltas < = 20 horas	4
Solicitudes resueltas < = 68 horas	0
Solicitudes no resueltas, están en proceso y/o tienen un tratamiento especial	0
Total	**19**

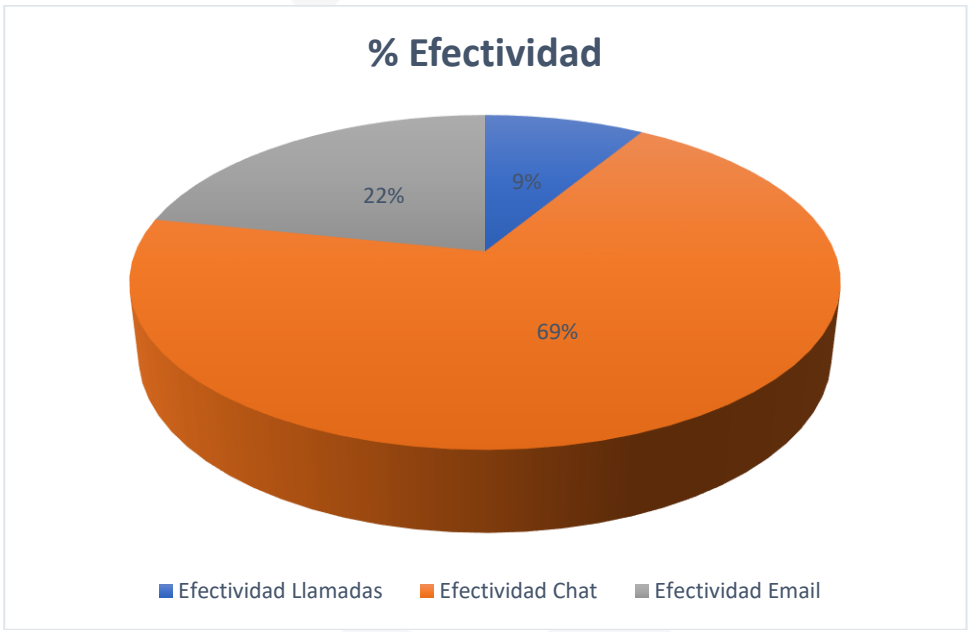


Tiempo de Gestión	Incidentes Penalizados
Incidentes resueltos > = 4 horas	0
Incidentes resueltos > = 20 horas	0
Incidentes resueltos > = 68 horas	0
Total	0

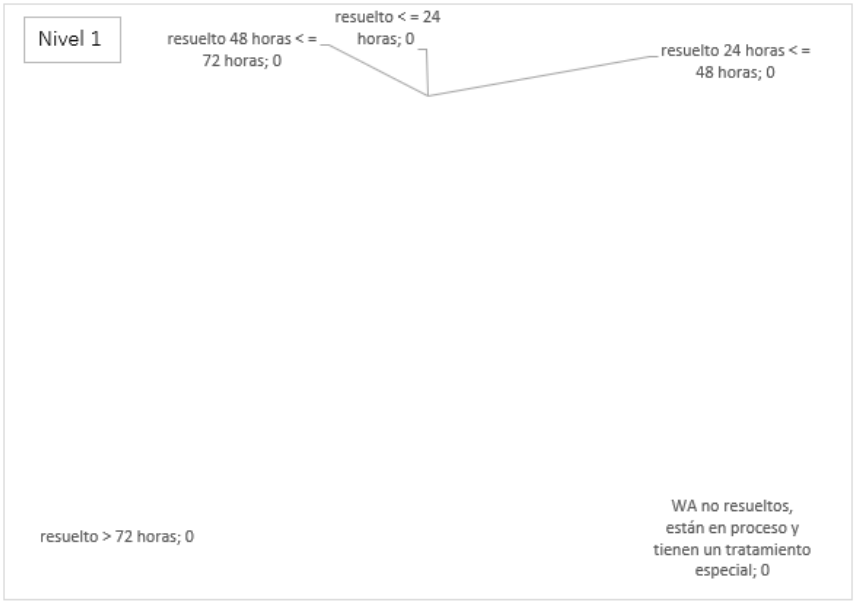
Canales de Atención	Cantidad
Llamadas	20
Chat	160
Email	50
Total	230
Efectividad	%
Efectividad Llamadas	8,70
Efectividad Chat	69,57
Efectividad Email	21,74
Efectividad Total en Canales de Atención	100

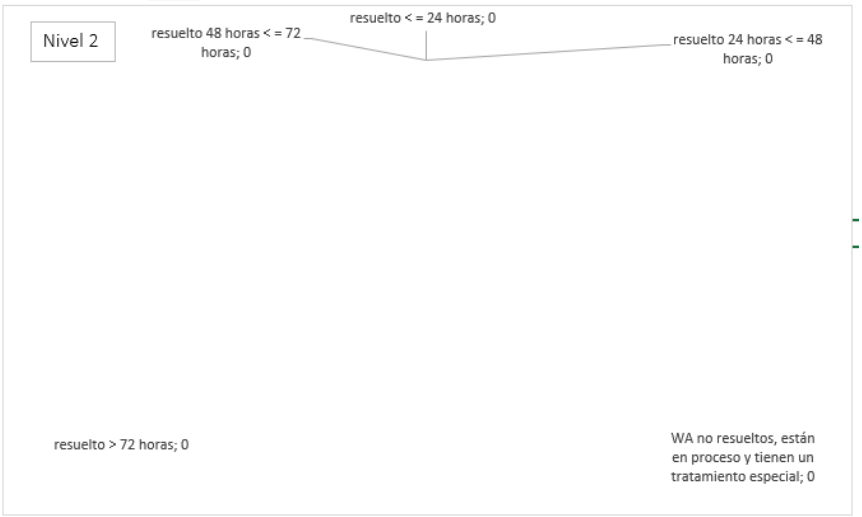
No conformidad	0

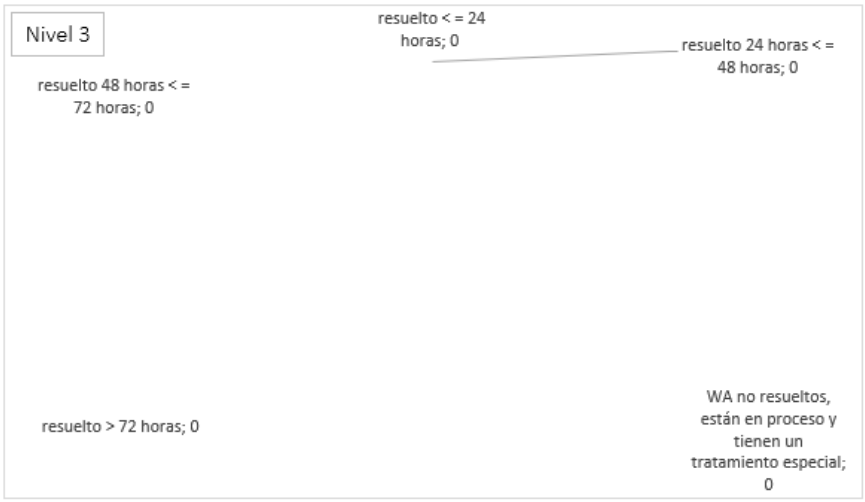

Llamadas; 20
Email; 50
Chat; 160
Llamadas
Chat
Email

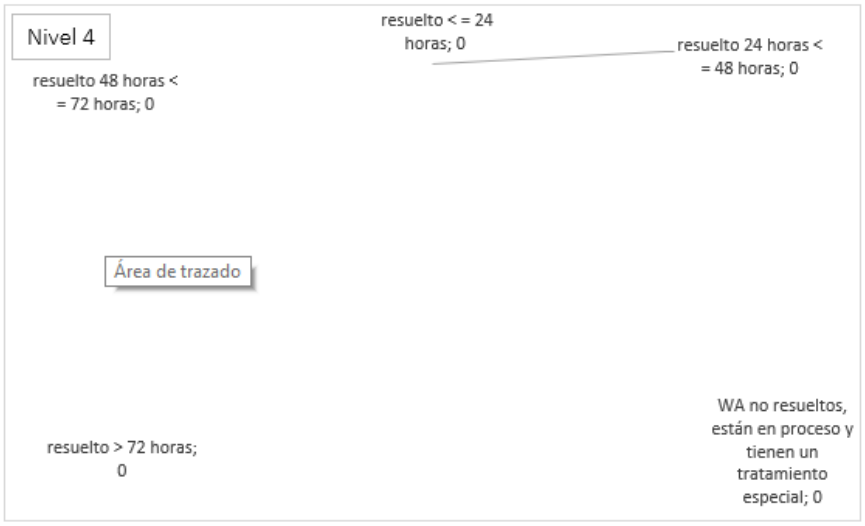

% Efectividad
9%
22%
69%
Efectividad Llamadas
Efectividad Chat
Efectividad Email

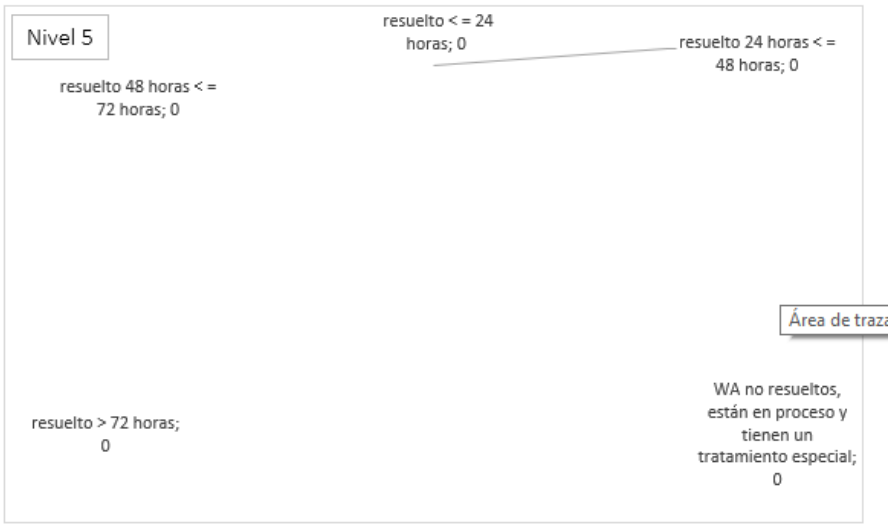
WA (Ajustes Funcionales)					
Tiempo de Gestión	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
resuelto < = 24 horas	0	0	0	0	0
resuelto 24 horas < = 48 horas	0	0	0	0	0
resuelto 48 horas < = 68 horas	0	0	0	0	0
resuelto > 68 horas	0	0	0	0	0
WA no resueltos, están en proceso y tienen un tratamiento especial	0	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 abril a 30 de abril 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/doc2.aspx?sourcedoc=%7B96925709-4929-4307-ABF8-E1C234334116%7D&file=Seguimiento%20Casos%20Portal%20Rama%20Judicial.xlsx&action=default&mobileredirect=true , los cuales contienen la información detallada de cada uno desde el 1 de abril a 30 de abril del 2024.

2.3 TIEMPOS INDISPONIBILIDAD PORTAL

Fecha	Hora inicio	Tiempo total
1/04/2024	15:25	0:26:41
10/04/2024	11:01	0:02:44
11/04/2024	0:07	0:04:36
18/04/2024	20:00	1:10:21
19/04/2024	0:07	0:00:29
19/04/2024	8:25	0:01:00
21/04/2024	7:40	0:02:40
23/04/2024	7:57	0:02:10
23/04/2024	16:01	0:00:14
23/04/2024	20:25	0:01:10
24/04/2024	21:07	0:02:50
24/04/2024	21:26	0:02:05
24/04/2024	22:06	0:00:35
25/04/2024	9:06	0:01:25
25/04/2024	15:01	0:01:26
25/04/2024	15:07	0:00:39
26/04/2024	9:38	0:01:25
27/04/2024	0:00	1:41:42

2.4 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 abril 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	120	400	280
2024	120		
Solicitud	120		
Incidencia	0		
Total Horas Casos Reportados Netsuite	120	400	280
		280	280
		280	280
		280	280
		280	280
Horas consumidasde las 400 - Exp	400	400	0

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

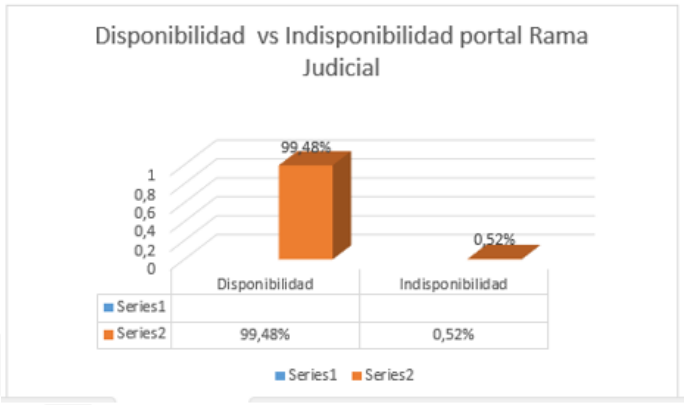
Etiquetas de fila	Suma de Horas Hombre	Horas Presupuesto	Horas Disponibles
CASO	0	100	100
2023	0		
WA	0		
MF	0		
Total Horas Casos Reportados Netsuite	0	100	100
Total Horas Consumidas de las 100 - Exp	0	100	100

3. DISPONIBILIDAD E INDISPONIBILIDAD DE LOS SERVICIOS DE HOSTING

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

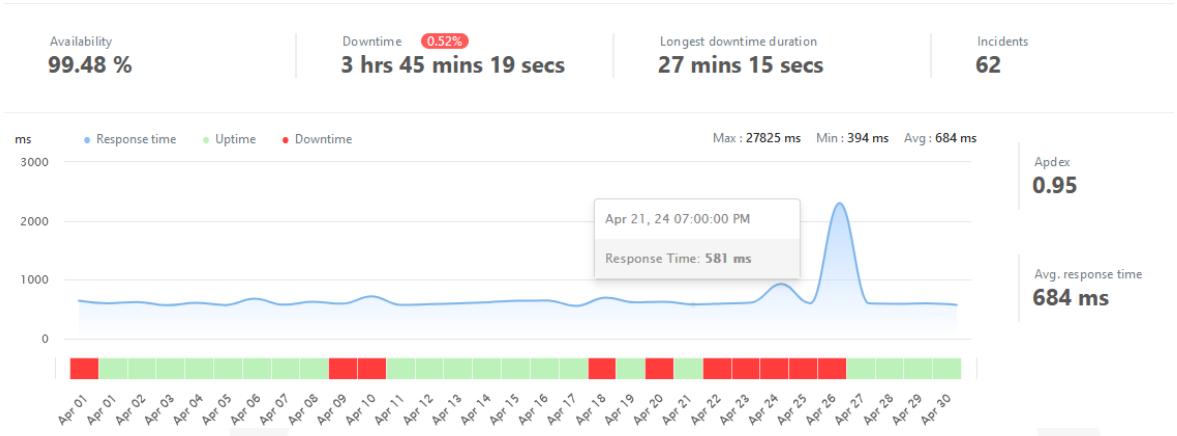
Se visualiza a través de la siguiente matriz los datos de disponibilidad, indisponibilidad y tiempo de caída de las aplicaciones que están soportadas al Consejo Superior de la Judicatura:

Item	Aplicación	Disponibilidad	Indisponibilidad	Tiempo de duracion (Caida en horas)	Tiempo de duracion			
					Dias	Horas	Minutos	Segundos
1	Portal de la Rama Judicial	99,48%	0,52%	3,755277778	0	3	45	19
	Totales	99,48%	0,52%	3,755277778	**0**	3	45	19



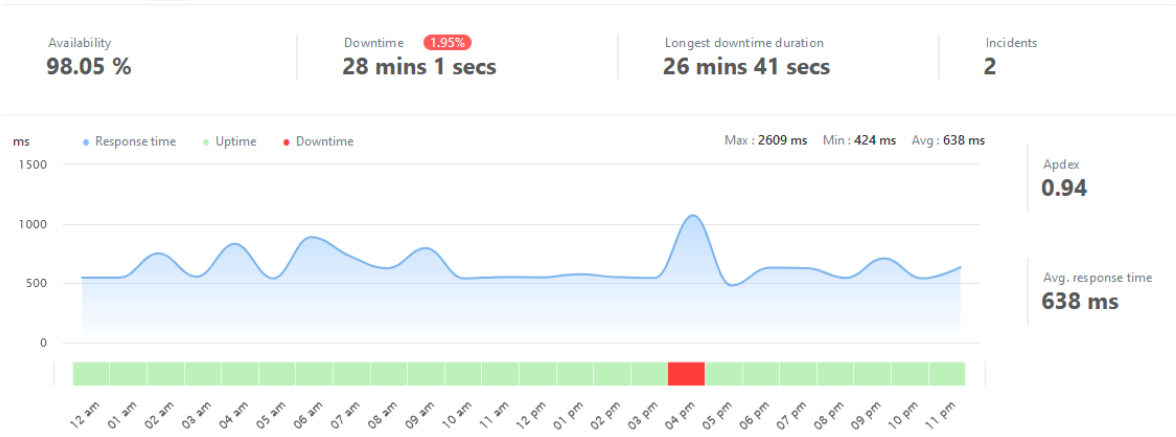
3.2 PORTAL DE LA RAMA JUDICIAL

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

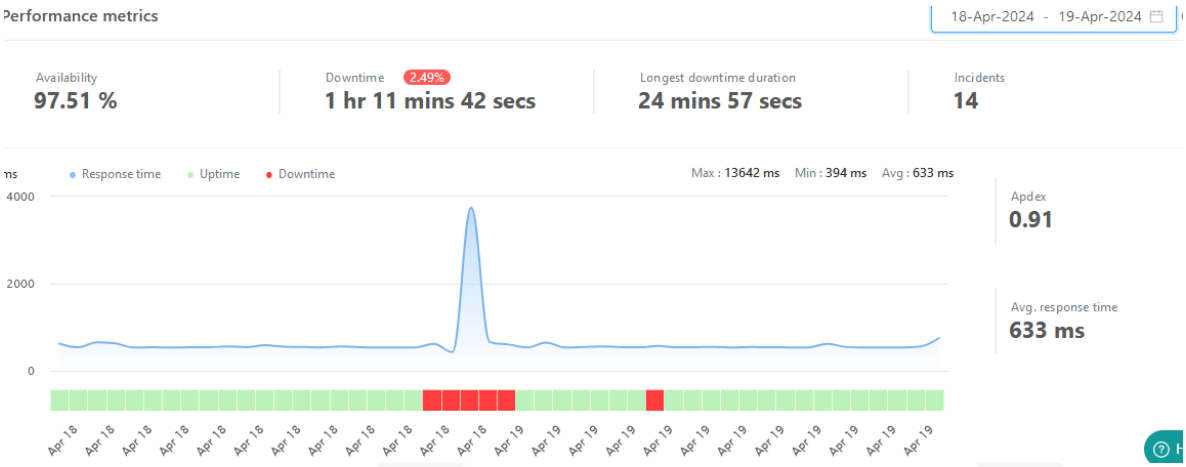


En la gráfica se puede observar que el portal tuvo los siguientes datos en la disponibilidad

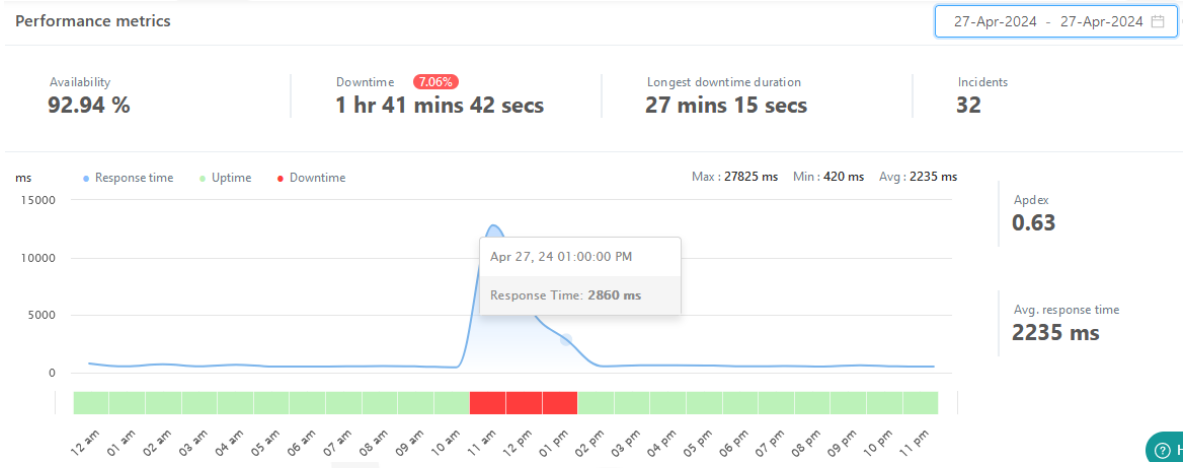
% de Disponibilidad: 99,48%
% de Indisponibilidad: 0,52%
Tiempo total de eventos del mes: 3 horas 45 minuto 19 segundos
Promedio en el tiempo de respuesta que tuvo el portal: 684 ms



01 de abril 2024
% de Disponibilidad: 98,05%
% de Indisponibilidad: 1,95%
Tiempo total de eventos del mes: 28 minuto 1 segundos
Promedio en el tiempo de respuesta que tuvo el portal: 638 ms
Detalle incidente: En horas de la tarde se produjo incidente a nivel del área de conectividad donde se vieron afectadas todas las apps de CSJ.



18-19 de abril 2024
% de Disponibilidad: 97,51%
% de Indisponibilidad: 2.49%
Tiempo total de eventos del mes: 1 hora 11 minuto 42 segundos
Promedio en el tiempo de respuesta que tuvo el portal: 633 ms
Detalle incidente: Ventana de pruebas realizada para validación del portal de Liferay 7.1.



27 de abril 2024
% de Disponibilidad: 92,94%
% de Indisponibilidad: 7,06%
Tiempo total de eventos del mes: 1 hora 41 minuto 42 segundos
Promedio en el tiempo de respuesta que tuvo el portal: 2235 ms
Detalle incidente: Ventana de pruebas realizada para validación del portal de Liferay 7.1.

- TT544033 RV: Certificaciones disponibilidad portal Rama Judicial año 2024.

A través del presente anexo **Certificaciones Periodo abril 2024** encontrarán todos los documentos requeridos por la Rama Judicial mediante la herramienta NOC.

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				

3.2.2 CRECIMIENTO DE LA BASE DE DATOS – INSTANCIA CSJPORTALDB01

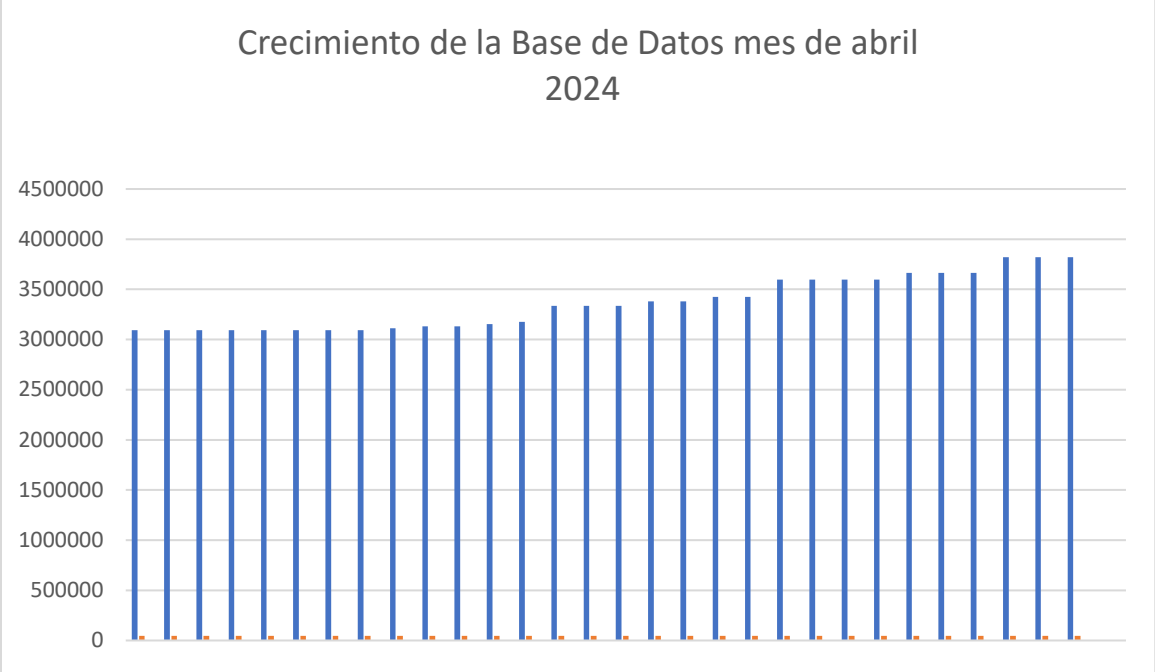
De acuerdo con la solicitud escalada en el **caso TT520553 RV: Crecimiento de la BD de la maquina CSJPORTALDB01** del portal de rama judicial, se agrega el presente informe consolidado del crecimiento que tuvo la BD en el mes de abril.

BASE DE DATOS lportalramaprod

TAMAÑO (MB0	FECHA	AUMENTO TAMAÑO (MB) POR DIA
3092333 MB	2024-04-01 00:00:00.547	0
3092333 MB	2024-04-02 00:00:01.120	0
3092333 MB	2024-04-03 00:00:00.370	0
3092333 MB	2024-04-04 00:00:00.573	0
3092333 MB	2024-04-05 00:00:00.507	0
3092333 MB	2024-04-06 00:00:00.570	0
3092333 MB	2024-04-07 00:00:00.663	0
3092333 MB	2024-04-08 00:00:00.713	17980
3110313 MB	2024-04-09 00:00:00.657	19777
3130090 MB	2024-04-10 00:00:01.003	0

3130090 MB	2024-04-11 00:00:00.753	21756
3151846 MB	2024-04-12 00:00:01.077	23931
3175777 MB	2024-04-13 00:00:00.263	160714
3336491 MB	2024-04-14 00:00:00.563	0
3336491 MB	2024-04-15 00:00:00.750	0
3336491 MB	2024-04-16 00:00:01.050	42395
3378886 MB	2024-04-17 00:00:01.100	0
3378886 MB	2024-04-18 00:00:00.773	46636
3425522 MB	2024-04-19 00:00:00.527	0
3425522 MB	2024-04-20 00:00:00.220	169799
3595321 MB	2024-04-21 00:00:00.483	0
3595321 MB	2024-04-22 00:00:00.827	0
3595321 MB	2024-04-23 00:00:01.087	0
3595321 MB	2024-04-24 00:00:00.793	68279
3663600 MB	2024-04-25 00:00:00.513	0
3663600 MB	2024-04-26 00:00:00.177	0
3663600 MB	2024-04-27 00:00:00.303	157724
3821324 MB	2024-04-28 00:00:00.980	0
3821324 MB	2024-04-29 00:00:00.210	0
3821324 MB	2024-04-30 00:00:00.310	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 abril

Link del informe https://analytics.google.com/analytics/web/?authuser=2#/p352626126/reports/dashboard?params=_u..nav%3Dmaui%26_u.date00%3D20231001%26_u.date01%3D20231031&r=reporting-hub&collectionId=5424623797

5. ESQUEMA DE SEGURIDAD

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

31	2082017	npn04--IaaS Seguridad - Firewall Nueva Generación - Media Capacidad - Oro - Hosting físico - Rol deFirewall - 40 Gbps - SesionesConcurrentes - 15000000 -Mes - Cantidad: 2	FIREWALL	PALACIO - BK	FortiGate 900G	SN: FG9H0GTB23900440	N/A	N/A
32	2082018	npn04--IaaS Seguridad - Firewall Nueva Generación - Alta Capacidad - Oro - Hosting físico - Rol deFirewall - 500 Gbps - Sesiones Concurrentes - 150000000 - Mes - Cantidad:2	FIREWALL DC Torre central	DATACENTER - BK	FORTIGATE-4400F	SN: FG440FTK21900183	27-30	32
32	2082019	npn04--IaaS Seguridad - Firewall Nueva Generación - Alta Capacidad - Oro - Hosting físico - Rol deFirewall - 500 Gbps - Sesiones Concurrentes - 150000000 - Mes - Cantidad:2	FIREWALL DC Torre central	DATA CENTER - PPLA	FORTIGATE-4400F	SN: FG440FTK21900184	5-8	32
33	2082013	npn04--IaaS Seguridad - WebAplication Firewall - AltaCapacidad - Oro - Hostingfísico - Desempeño WAF(Gbps) - 10 - Mes - Cantidad:3	WAF DC Torre central	DATACENTER - PPLA	KEMP LM-X25	SN: TSCC82005608	14	31
33	2082014	npn04--IaaS Seguridad - WebAplication Firewall - AltaCapacidad - Oro - Hostingfísico - Desempeño WAF(Gbps) - 10 - Mes - Cantidad:3	WAF DC Torre central	DATACENTER - BK	KEMP LM-X25	SN: TSCB72000545	13	31
33	2082015	npn04--IaaS Seguridad - WebAplication Firewall - AltaCapacidad - Oro - Hostingfísico - Desempeño WAF(Gbps) - 10 - Mes - Cantidad:3	WAF	SEDE CAN	KEMP LM-X25	SN: TSCC82005629	N/A	N/A
44	2082108	Servicios Complementarios - Experto Master - Región 1 - Hora/M - Cantidad: 980	Transversales a servicios de SP					

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
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:

Item	Fecha y Hora de inicio	Fecha y Hora de finalización	Cantidad de Horas	Tipo de Hora extra	Actividad Realizada
1	4/19/2024 19:45	4/19/2024 20:16	1:00:00	Diurna	TT824790 Actualización formato permisos conectividad 19042024
2	4/23/2024 18:00	4/23/2024 19:03	1:00:00	Diurna	TT826421 RV: Solicitud validación conectividad, TT826414 RV: Solicitud de permisos adicionales de navegación, TT826407 RV: VPN Azure
3	4/26/2024 18:00	4/26/2024 18:27	1:00:00	Diurna	TT827982 RV: Solicitud permisos de navegación_Unidad de Apoyo Investigativo; TT827988 RV: Solicitud habilitar acceso SSH a servidores azure
Total horas Extras			3:00:00		

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	4/4/2024 7:00	4/4/2024 11:00	4:00:00	Diurna	Ventana de cambio Firewall 3500F a 900G Palacio
2	4/12/2024 18:00	4/12/2024 19:00	1:00:00	Diurna	Cambio de DNS CNDJ y caso
3	4/12/2024 21:00	4/13/2024 1:00	4:00:00	Nocturna	Ventana reinicio HUBs
4	4/18/2024 19:00	4/19/2024 0:00	5:00:00	Diurna	Pruebas Nuevo Portal WEB
5	4/26/2024 19:00	4/26/2024 20:00	1:00:00	Diurna	TT822677 RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA
10					
Total horas Extras			15:00:00		

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	4/4/2024 6:00	4/4/2024 11:00	5:00:00	Diurna/Nocturna	Ventana de cambio Firewall 3500F a 900G Palacio
2	4/4/2024 11:00	4/4/2024 12:00	1:00:00	Diurna/Nocturna	Actualizacion FortiAnalyzer 800F
3	4/11/2024 18:00	4/11/2024 19:00	1:00:00	Diurna/Nocturna	Reunion: RE: Fallas DAU CAN
4	4/16/2024 18:00	4/16/2024 19:00	1:00:00	Diurna/Nocturna	TT823014 RV: SOLICITUD Ingreso por VPN RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA
4	4/27/2024 9:00	4/27/2024 15:00	6:00:00	Diurna/Nocturna	ventana mantenimiento: Ventana de mantenimiento Portales
4	4/29/2024 18:00	4/29/2024 19:00	1:00:00	Diurna/Nocturna	Reunion: TT822677 Programacion Sesiones Parchado Abril 2024 RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA
7					
8					
Total horas Extras			15:00:00		

14.2. Inventario de equipos de seguridad perimetral.

A continuación, se presenta el inventario de 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

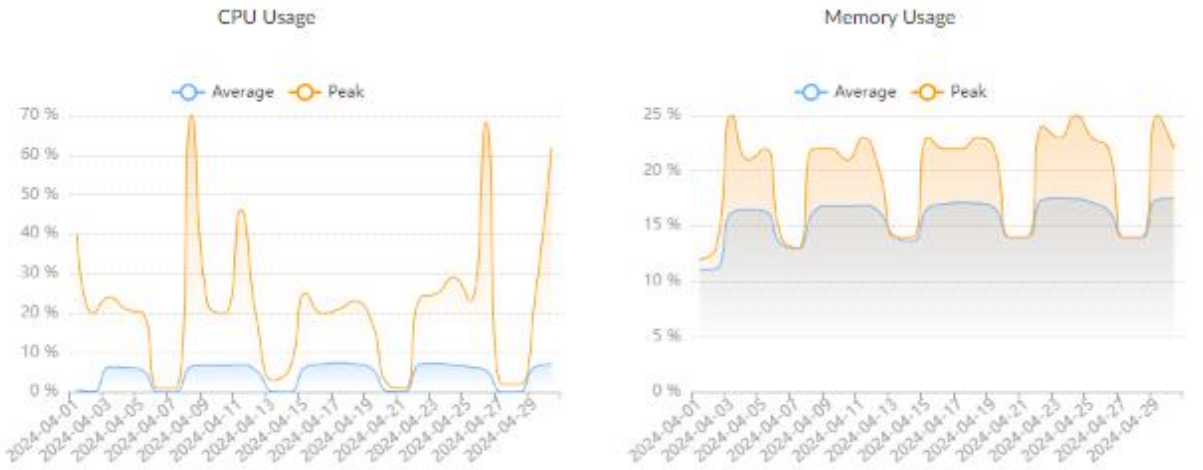
14.3. Actualización de firmware.

El plan de trabajo 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

14. FIREWALL PERIMETRAL

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

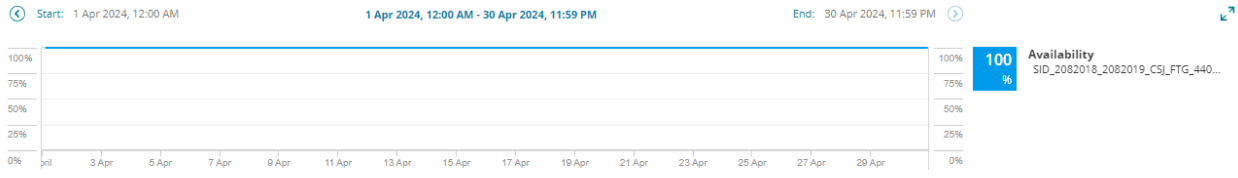


Los Firewall perimetrales dentro de sus características del equipo contienen varias CPU que realizan diferentes tareas en su procesamiento del tráfico, por tanto, se puede esperar que en su funcionamiento una o varias de sus CPU sean más utilizadas que otras por algún tipo de inspección especial que este realizando.

La gráfica de color naranja muestra cuales fueron los picos más altos de uso de las CPUs durante el mes, mientras que el promedio de funcionamiento del Firewall, se muestra en la gráfica de color azul.

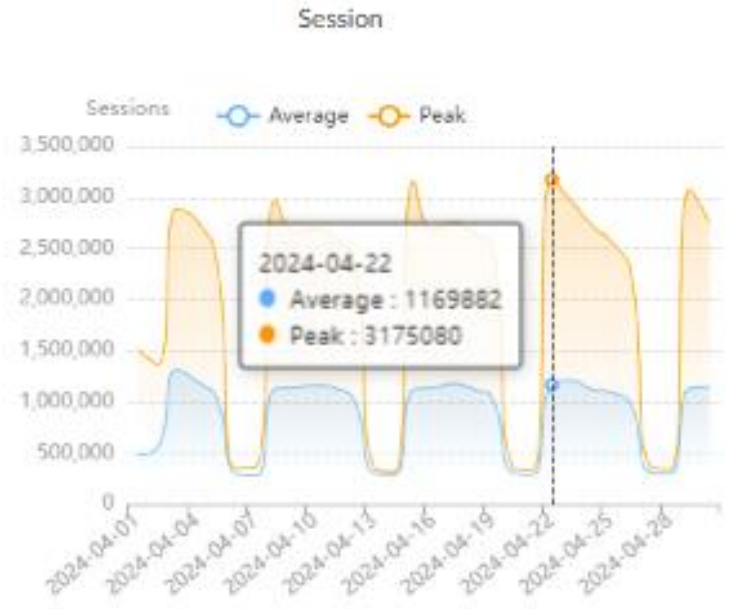
15.1. Disponibilidad mensual firewall perimetral.

Durante abril se obtuvo una disponibilidad del 100 % en el firewall perimetral.



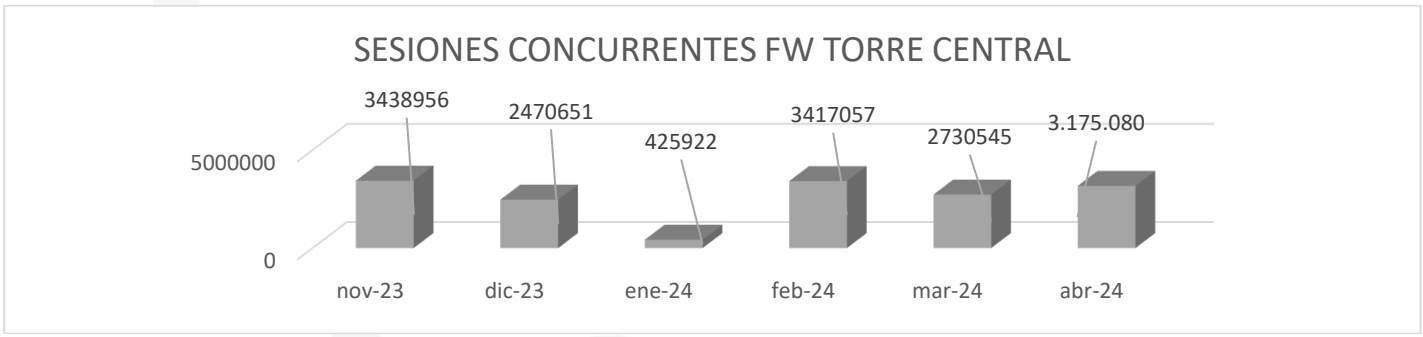
15.2. Cantidad de sesiones firewall perimetral.

Durante abril se presentó un máximo de 3.175.080 sesiones TCP concurrentes, cantidad que se encuentra dentro del rango máximo soportado por el equipo Fortinet FG- 4400F cuyo valor es de 210 millones.



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

En el último mes se presentó una reducción en las sesiones del FW perimetral:



MES	SESIONES
nov-23	3438956
dic-23	2470651
ene-24	425922
feb-24	3417057
mar-24	2730545
abr-24	3.175.080

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

En el top de aplicaciones con mayor consumo de ancho de banda está HTTPS:

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	HTTPS			269.69 TB
2	Microsoft.SharePoint			65.03 TB
3	SSL			40.25 TB
4	DTLS			30.50 TB
5	Microsoft.365.Portal			24.13 TB
6	Microsoft.Portal			22.20 TB
7	OneDrive			20.91 TB
8	SMB			19.06 TB
9	Microsoft.Outlook			17.23 TB
10	TCP/9443			16.60 TB

Con el mayor consumo de sesiones están SMB, HTTPS y DNS:

Top Applications by Sessions

#	Application	Sessions
1	SMB	2,476,649,098
2	HTTPS	1,849,631,652
3	DNS	1,360,093,961
4	Microsoft.Windows.Update	724,690,430
5	SSL	706,870,105
6	Microsoft.Portal	517,573,814
7	Microsoft.365.Portal	480,323,922
8	Microsoft-Office365	449,583,588
9	TCP/448	411,497,662
10	TCP/5508	327,297,592

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

El WAF 172.17.201.251 en IFX presentó la mayor cantidad de sesiones:

Top IP by Bandwidth

#	IP	Bandwidth	Sent	Received
1	172.17.201.251			73.11 TB
2	172.17.201.252			47.91 TB
3	172.27.64.17			33.59 TB
4	10.244.2.239			15.12 TB
5	erubianr			10.79 TB
6	172.27.64.61			9.69 TB
7	172.28.108.45			4.97 TB
8	10.101.100.114			4.60 TB
9	172.28.146.20			3.45 TB
10	172.28.107.59			3.30 TB

15.6. Top de destinos web por ancho de banda firewall perimetral.

Los destinos en Internet con mayor consumo de ancho de banda durante abril fueron 8.243.164.19 (rns1co.cirion.live), 35.186.224.25 y Publicación_Consulta_Nacional_Unif (190.217.24.6):

Top Destination by Sessions

#	Destination	Sessions
1	8.243.164.19	378579275
2	35.186.224.25	293682210
3	190.217.24.69	210976968
4	8.243.164.21	172996273
5	190.217.24.155	116009678
6	8.243.200.3	98478057
7	10.1.2.22	91125170
8	10.1.2.21	88813100
9	190.217.24.172	77918126
10	172.28.146.154	75413292

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

El Top de IP con mayor número de peticiones bloqueadas durante abril fue:

Top Web Users by Blocked Requests

#	User (or IP)	Hostname	Requests
1	172.16.33.29	172.16.33.29	25,422,753
2	172.16.33.247	172.16.33.247	19,304,321
3	172.16.56.165	172.16.56.165	14,959,916
4	192.168.125.26	192.168.125.26	14,903,842
5	192.168.50.34	192.168.50.34	12,455,226
6	192.168.61.130	192.168.61.130	6,504,869
7	172.27.90.208	172.27.90.208	6,403,453
8	172.28.34.125	172.28.34.125	6,084,956
9	172.16.35.145	172.16.35.145	6,062,630
10	172.27.90.93	172.27.90.93	6,008,530

Se recomienda verificar los equipos en lista para 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.

Las categorías con mayor número de bloqueos durante abril fueron Internet Radio and TV, Streaming Media and Download y Social Networking.

Top Blocked Web Categories

#	Category	Requests
1	Internet Radio and TV	302,762,444
2	Streaming Media and Download	8,202,369
3	Social Networking	6,400,955
4	Proxy Avoidance	5,246,800
5	Games	4,432,632
6	Unrated	1,550,316
7	Information Technology	1,063,494
8	Entertainment	901,996
9	Illegal or Unethical	187,714
10	Gambling	172,700

15.9. Top de IP más activos Firewall Perimetral

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

Top Web IP by Allowed Requests

#	IP	Requests
1	10.101.100.114	11,250,434
2	10.101.100.38	10,457,502
3	10.101.100.34	9,754,488
4	10.101.100.122	6,455,588
5	10.101.100.170	5,598,804
6	10.101.100.70	5,594,232
7	10.101.100.138	5,501,706
8	10.101.100.194	5,470,397
9	10.101.100.134	5,380,354
10	10.101.101.246	4,361,815

15.10. Top de categorías más visitadas Firewall Perimetral

La categoría más visitada durante abril fueron Information Technology:

Top Allowed Web Categories

#	Category	Requests
1	Information Technology	474,230,607
2	Overrride_permitidas	714,411
3	Unrated	10

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

172.17.201.251 (WAF de Torre Central) y172.17.202.251 (WAF CAN) presentaron el mayor consumo de ancho de banda durante abril:

Top IP by Bandwidth

#	IP	Bandwidth	Sent	Received
1	172.17.201.251			73.11 TB
2	172.17.201.252			47.91 TB
3	172.27.64.17			33.59 TB
4	10.244.2.239			15.12 TB
5	erubianr			10.79 TB
6	172.27.64.61			9.69 TB
7	172.28.108.45			4.97 TB
8	10.101.100.114			4.60 TB
9	172.28.146.20			3.45 TB
10	172.28.107.59			3.30 TB

15. TRÁFICO VPN FIREWALL PERIMETRAL

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

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

#	f_user	devname	vpn_type_group	end_time	remip	connections	Duration	bandwidth	traffic_in	traffic_out
1	cvillam	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-04-30 23:59:14	181.55.51.20	96	703:21:08	5.87 GB	676500676	5630309230
2	lmarinmo	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-05-01 00:00:22	181.136.233.42;191.91.108.168	148	659:35:29	20.86 GB	1952116064	20449170102
3	Ecoralb	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-04-29 01:04:19	186.28.125.121	115	516:32:04	24.32 GB	2849718256	23265664120
4	pmarulac	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-04-30 22:22:18	190.248.105.47	112	501:07:42	6.76 GB	835148119	6421898184
5	jariasu	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-04-29 16:36:27	181.137.8.129	80	429:18:16	2.05 GB	287463368	1910890275
6	lbarrerf	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-04-30 23:16:27	186.155.145.61;190.26.184.10;191.156.49.119;191.156.50.100;191.156.53.175;191.156.56.136;191.156.57.120;191.156.62.59;201.244.129.88;201.244.250.251	77	403:28:37	47.68 GB	2452919423	4874628 0342

7	Fcaldert	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-04-30 23:57:49	152.202.130.64;152.202.137.180;152.202.173.144;167.0.36.61;186.31.144.125;186.31.144.198;186.31.144.199;186.31.145.210;186.31.146.248;186.31.147.141;186.31.147.95;186.31.149.146;186.31.152.122;186.31.152.184;186.31.152.208;186.31.152.251;186.31.153.181;186.31.153.223;186.31.209.51;186.31.209.75;186.31.210.227;186.31.210.45;186.31.210.84;186.31.214.170;186.31.214.179;186.31.215.28;186.31.219.193;186.31.219.217;186.31.219.230;191.108.189.231;191.108.190.72;191.108.205.50;191.156.248.177;191.156.249.183	199	317:04:48	1.02 GB	428160316	667164576
8	LPineroSe	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-04-30 22:45:36	45.238.181.195;45.238.182.54;45.238.182.80;45.238.183.160;45.238.183.175;45.238.183.195;45.238.183.199;45.238.183.234;45.238.183.253	69	306:32:02	32.89 GB	1717925201	33599479677
9	jalvarap	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-04-30 21:24:28	152.203.194.233;152.203.209.39;191.104.131.231;191.104.134.13;191.104.141.100;191.104.144.196	60	301:28:45	20.48 GB	1242580138	20745624319
10	cpardov	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-04-29 14:48:37	172.16.13.99;172.16.8.135;186.83.104.168	104	290:51:37	12.41 GB	1092482726	12231855890

16.1. VPN IPSEC Site To Site Firewall Perimetral

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

Site-to-Site IPsec

Add Filter

Site-to-Site IPsec Tunnel	Initiating FortiGate	Terminating FortiGate	Duration	Bytes (Sent/Received)
VPN_AZURE	190.217.24.4 Bogota, Colombia	52.240.53.161 Potomac Falls, United States	29d 23h 38m 06s	17.3 TB/645.0 GB
VPN_ORACLE	190.217.80.4 Barrancabermeja, Colombia	129.213.6.36 Ashburn, United States	29d 17h 43m 47s	185.2 GB/2.3 TB
VPN_AZURE-VWAN2	190.217.24.4 Bogota, Colombia	4.153.117.131 Redmond, United States	7d 8h 0m 39s	309.0 GB/7.0 GB
VPN_AZURE-ANALY	190.217.24.4 Bogota, Colombia	20.124.34.235 Potomac Falls, United States	29d 23h 38m 21s	55.7 GB/5.7 GB
VPN_Tierras	190.217.24.4 Bogota, Colombia	181.225.76.196 Anserma, Colombia	29d 23h 24m 47s	561.2 MB/35.7 GB
VPN_AZURE-VWAN	190.217.24.4 Bogota, Colombia	4.153.117.133 Redmond, United States	7d 8h 0m 49s	54.8 MB/24.5 GB
VPN_SIUG_AWS-2	190.217.24.4 Bogota, Colombia	34.224.152.152 Ashburn, United States	29d 23h 33m 29s	395.1 MB/513.4 MB
VPN_SIUG_AWS	190.217.24.4 Bogota, Colombia	34.194.187.190 Ashburn, United States	29d 23h 33m 32s	395.0 MB/513.3 MB
VPN_Linktic	190.217.24.4 Bogota, Colombia	3.222.171.115 Ashburn, United States	29d 23h 34m 41s	291.4 MB/444.6 MB
VPN_REGISTRADU	190.217.24.4 Bogota, Colombia	201.232.123.20 Medellin, Colombia	29d 23h 39m 50s	327.8 MB/369.5 MB
VPN_INPEC	190.217.19.156 Bogota, Colombia	190.25.112.10 Bogota, Colombia	29d 23h 39m 40s	104.2 MB/525.1 MB
VPN_FISCALIA	190.217.24.4 Bogota, Colombia	190.157.218.66 Bogota, Colombia	29d 23h 32m 16s	1.7 MB/37.1 MB
OCI_EXADATA_FAB	190.217.24.4 Bogota, Colombia	150.136.25.96 Ashburn, United States	29d 23h 35m 52s	12.8 MB/0.0 KB

La disponibilidad de equipo durante el mes de abril fue efectivamente del 100% por tanto la caída que muestra la herramienta no fue total. Esta representa una latencia o demora entre la comunicación del equipo de monitoreo y el Firewall, acorde a su

ubicación geográfica en el Palacio de Justicia donde interviene un canal MPLS de un tercero.

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

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

Top Attacks

#	Attack Name	Severity	CVE-ID	Counts
1	tcp_syn_flood	Critical		511,101
2	tcp_src_session	Critical		451,600
3	tcp_port_scan	Critical		197,644
4	Spring.Framework.SerializationUtils.Insecure.Deserialization	Critical	CVE-2022-22965	107,896
5	Apache.Log4j.Error.Log.Remote.Code.Execution	Critical	CVE-2021-4104,CVE-2021-44228,CVE-2021-45046	27,267
6	Adobe.ColdFusion.Multiple.Vulnerabilities	Critical	CVE-2013-0625,CVE-2013-0629,CVE-2013-0631,CVE-2013-0632	20,543
7	F5.BIG.IP.Traffic.Management.User.Interface.Directory.Traversal	Critical	CVE-2020-5902	19,056
8	tcp_dst_session	Critical		15,570
9	Tofsee	Critical		14,764
10	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	Critical	CVE-2017-11317,CVE-2017-11357,CVE-2019-18935	13,846

Las víctimas de intrusión fueron los siguientes hosts:

Top 20 Intrusion Victims

#	Attack Victim	Counts (Critical / High / Medium)	Percent of Total Attacks
1	190.217.24.172	341,714	21.51%
2	190.217.24.69	327,294	20.61%
3	172.17.201.68	220,392	13.88%
4	172.17.201.26	186,040	11.71%
5	192.168.213.110	134,522	8.47%
6	172.17.201.52	111,933	7.05%
7	93.95.230.126	67,824	4.27%
8	172.17.201.25	46,734	2.94%
9	172.17.201.101	40,688	2.56%
10	190.217.24.149	39,205	2.47%
11	185.196.10.85	14,259	0.90%
12	34.29.85.190	10,982	0.69%
13	172.17.202.239	8,909	0.56%
14	34.80.59.191	7,702	0.48%
15	34.16.47.102	7,207	0.45%
16	65.20.73.40	5,153	0.32%
17	176.113.115.135	5,144	0.32%
18	176.113.115.84	5,142	0.32%
19	172.17.201.54	3,945	0.25%
20	45.74.46.163	3,575	0.23%

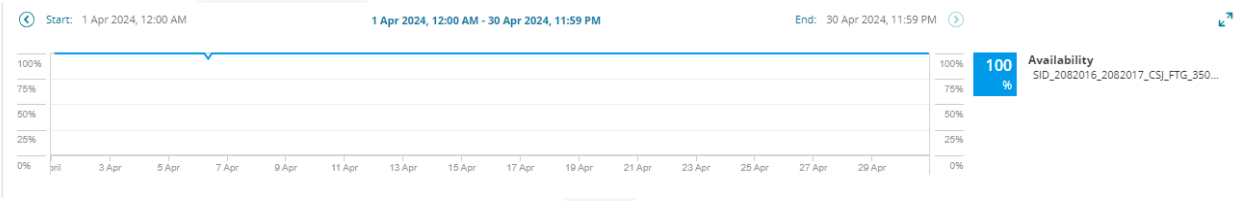
Los hosts 190.217.24.172, 190.217.24.69 son las aplicaciones web, sin embargo, están siendo protegidas por los WAF de Torre Central y del CAN.

16. FIREWALL SEDE PALACIO

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

16.1 Disponibilidad Mensual Firewall Palacio

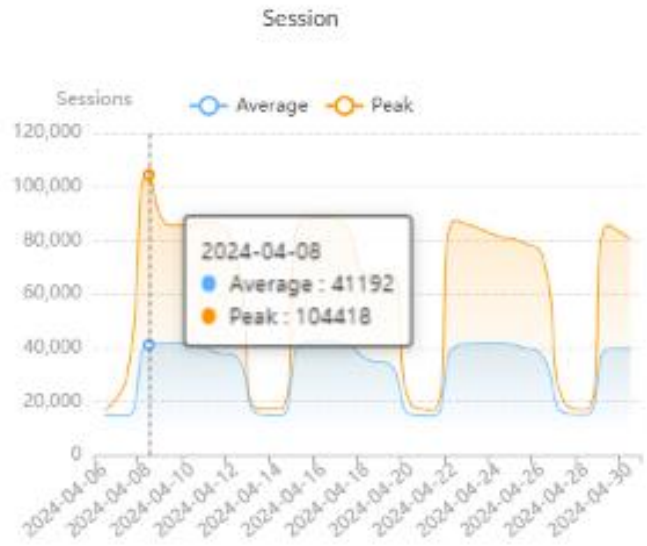
Durante abril se obtuvo una disponibilidad del 100 % en el firewall de Palacio.



La disponibilidad de equipo durante el mes de abril fue efectivamente del 100%, lo que muestra la herramienta no hace referencia a una caída, representa una latencia o demora entre la comunicación del equipo de monitoreo y el Firewall teniendo en cuenta que su ubicación geográfica es el Palacio de Justicia donde interviene un canal MPLS de un tercero.

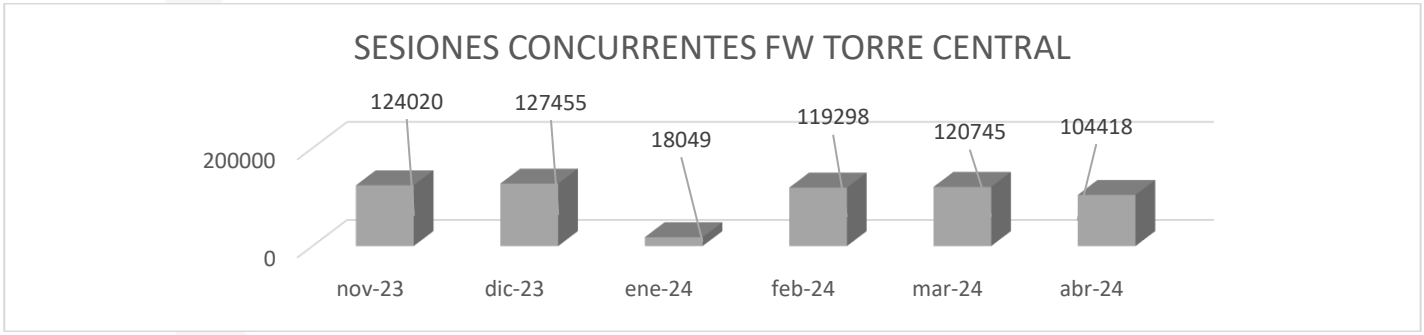
16.2 Cantidad de Sesiones Firewall Palacio

Durante abril se presentó un máximo de 104.418 sesiones concurrentes que están dentro del rango de sesiones soportadas por el equipo Fortigate 900G de 16 Millones.



16.3 Histórico de Sesiones Últimos 6 meses Firewall Palacio

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



MES	SESIONES
nov-23	124020
dic-23	127455
ene-24	18049
feb-24	119298
mar-24	120745
abr-24	104418

16.4 Aplicaciones y protocolos por ancho de banda firewall Palacio

En el siguiente top de aplicaciones de abril se evidencia que las aplicaciones con mayor consumo de ancho de banda fueron HTTPS, Microsoft.Portal y Microsoft.SharePoint:

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	HTTPS			11.49 TB
2	Microsoft.Portal			7.11 TB
3	Microsoft.SharePoint			7.05 TB
4	OneDrive			5.74 TB
5	HTTPS.BROWSER			4.02 TB
6	SMB			3.96 TB
7	SSL			3.58 TB
8	MS-SQL			1.97 TB
9	HTTP			1.67 TB
10	HTTP.BROWSER			1.61 TB

Por sesiones las aplicaciones con mayor consumo fue SMB:

Top Applications by Sessions

#	Application	Sessions
1	SMB	1,043,707,736
2	DNS	283,132,673
3	Microsoft.Windows.Update	54,957,868
4	Microsoft.Portal	39,601,600
5	HTTP.BROWSER	34,700,695
6	Microsoft.365.Portal	34,666,236
7	SQUID	33,033,466
8	SSL	31,437,459
9	HTTP	31,198,925
10	HTTPS	31,062,681

16.5 Top de IP por ancho de banda firewall Palacio.

172.28.93.2 consumió la mayor cantidad de ancho de banda durante abril:

Top Bandwidth IP

#	IP	Bandwidth
1	172.28.93.2	2.69 TB
2	172.17.114.19	1.07 TB
3	172.28.92.15	1.04 TB
4	172.28.92.23	1.03 TB
5	172.16.2.59	955.16 GB
6	172.28.92.31	669.53 GB
7	172.16.5.33	516.80 GB
8	172.16.5.17	439.22 GB
9	172.28.92.20	423.53 GB
10	172.28.92.29	368.81 GB

16.6 Top de destinos web por ancho de bandade Banda Firewall Palacio.

Los destinos más visitados durante abril fueron 13.107.136.10, 13.107.138.10, 20.60.0.104 (Microsoft Corporation):

Top Websites and Category by Bandwidth

#	Site	Category	Bytes
1	13.107.136.10		5.20 TB
2	13.107.138.10		5.13 TB
3	20.60.0.104		2.59 TB
4	172.190.220.253		978.86 GB
5	52.239.171.228		891.34 GB
6	20.60.128.228		733.14 GB
7	20.168.235.216		718.27 GB
8	190.217.24.42		669.43 GB
9	20.209.52.65		527.40 GB
10	20.209.75.97		512.45 GB

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

Top Web Users by Blocked Requests

#	User (or IP)	Hostname	Requests
1	172.16.73.25	172.16.73.25	159,651
2	172.28.93.142	172.28.93.142	148,690
3	172.16.4.227	172.16.4.227	80,113
4	172.16.4.190	172.16.4.190	75,874
5	172.16.4.182	172.16.4.182	62,154
6	172.16.2.75	172.16.2.75	53,550
7	172.29.136.123	172.29.136.123	46,289
8	172.16.5.29	172.16.5.29	41,907
9	172.16.4.242	172.16.4.242	39,607
10	192.168.6.48	192.168.6.48	35,251

Se sugiere verificar estos orígenes para que no continúen enviando peticiones hacia Internet que terminan siendo bloqueados.

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

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

Top Blocked Web Categories

#	Category	Requests
1	Unrated	1,792,924
2	Streaming Media and Download	862,961
3	Social Networking	738,478
4	Proxy Avoidance	572,940
5	Games	182,965
6	Entertainment	62,034
7	Society and Lifestyles	20,875
8	Newly Observed Domain	15,986
9	Spam URLs	11,559
10	Malicious Websites	11,322

16.9 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 abril:

Top Web IP by Allowed Requests

#	IP	Requests
1	172.16.4.90	19,208,128
2	172.28.54.20	7,828,937
3	172.28.93.87	2,081,559
4	172.28.93.45	1,495,026
5	172.16.4.30	1,037,752
6	172.16.0.148	634,523
7	172.16.4.132	493,627
8	192.168.6.66	433,260
9	172.16.6.192	431,324
10	172.16.5.188	426,159

16.10 Top de las categorías más visitadas firewall Palacio.

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

Top Allowed Web Categories

#	Category	Requests
1	Information Technology	37,744,240
2	Search Engines and Portals	8,443,836
3	Business	1,800,765
4	Information and Computer Security	645,871
5	Web Analytics	555,702
6	Web-based Applications	211,789
7	Finance and Banking	92,950
8	Online Meeting	91,224
9	Overrride_permitidas	63,463
10	Secure Websites	22,103

16.11 Top de consumo ancho de banda por usuario Firewall Palacio

172.17.201.251 (WAF) presento la mayor cantidad de conexiones durante abril:

Top IP by Bandwidth

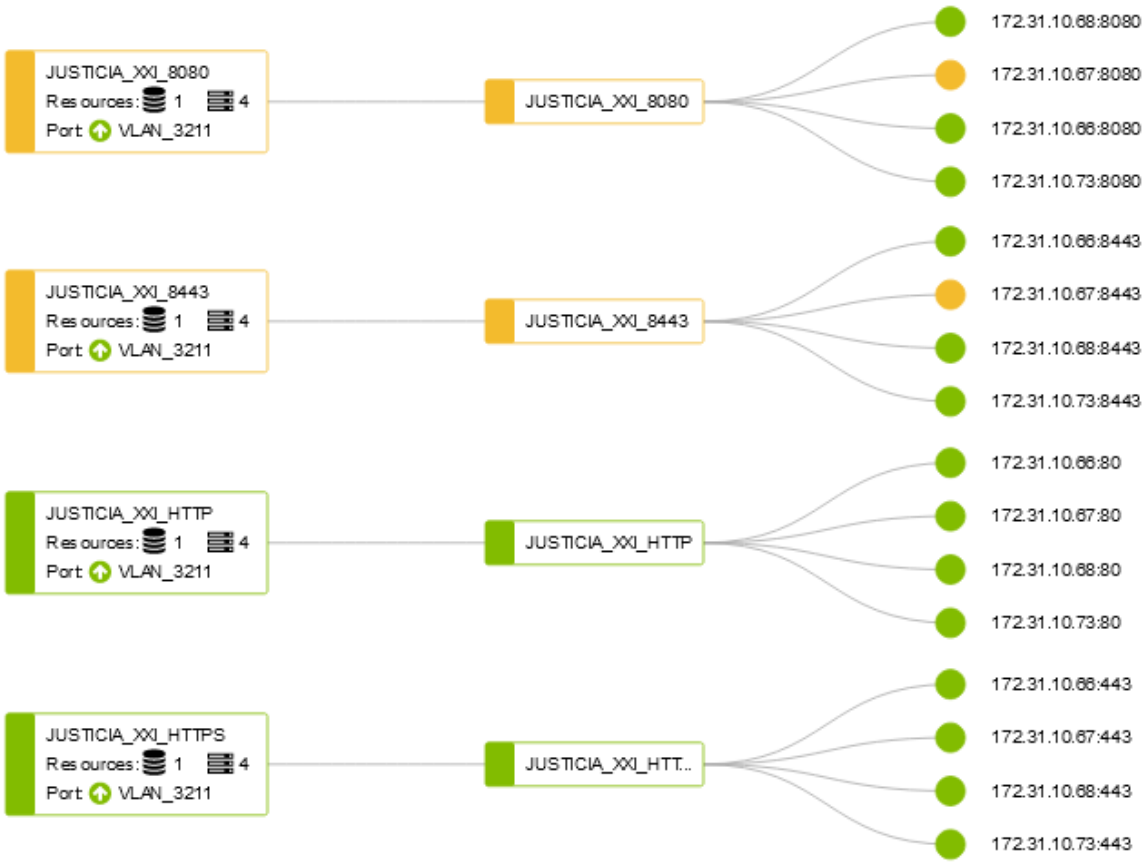
#	IP	Bandwidth	Sent	Received
1	172.17.201.251			5.24 TB
2	172.17.201.252			3.64 TB
3	10.101.250.4			2.92 TB
4	172.28.93.2			2.75 TB
5	172.16.4.121			1.58 TB
6	172.17.202.250			1.57 TB
7	172.28.92.23			1.26 TB
8	172.17.114.19			1.09 TB
9	172.16.2.59			1.07 TB
10	172.28.92.15			1.04 TB

17. BALANCEADOR DE CARGA FORTIADC

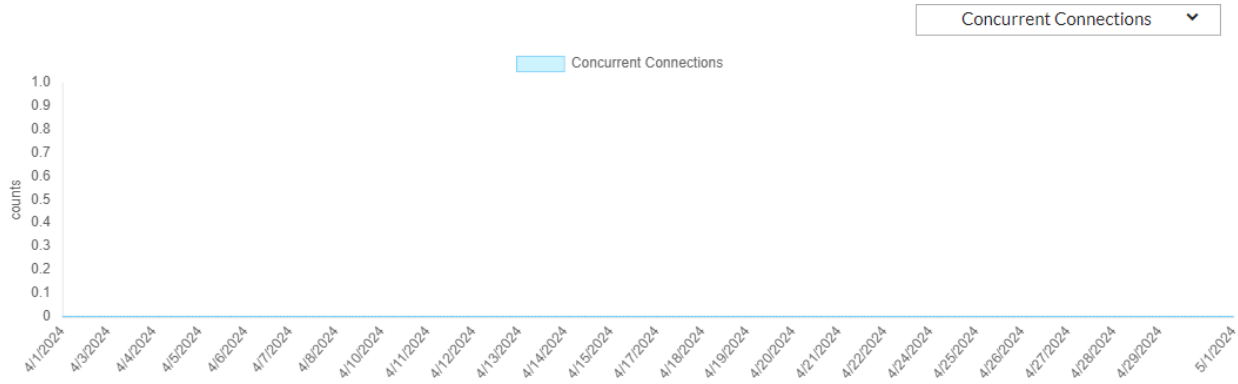
A continuación, se observan los diferentes servicios balanceados.

17.1 Justicia XXI

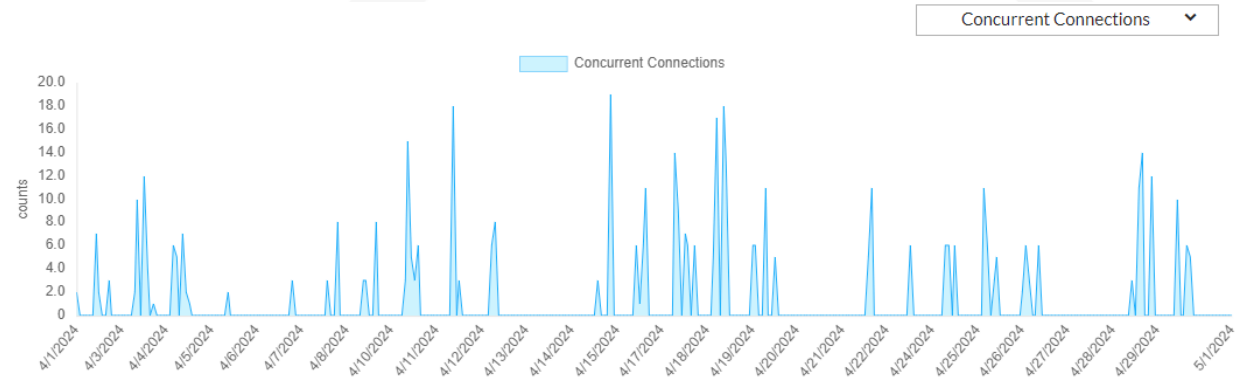
Se encuentra balanceado en el FortiADC:



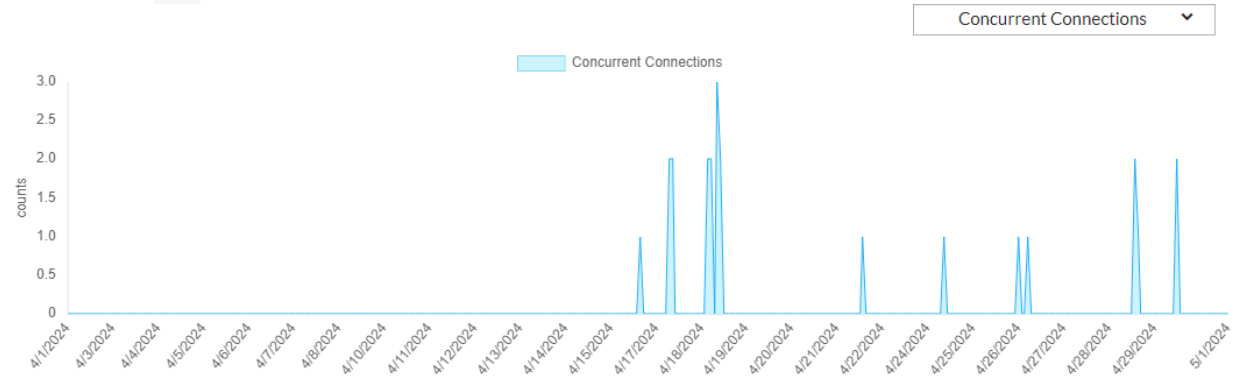
Durante abril no se presentó tráfico por el puerto 8080:



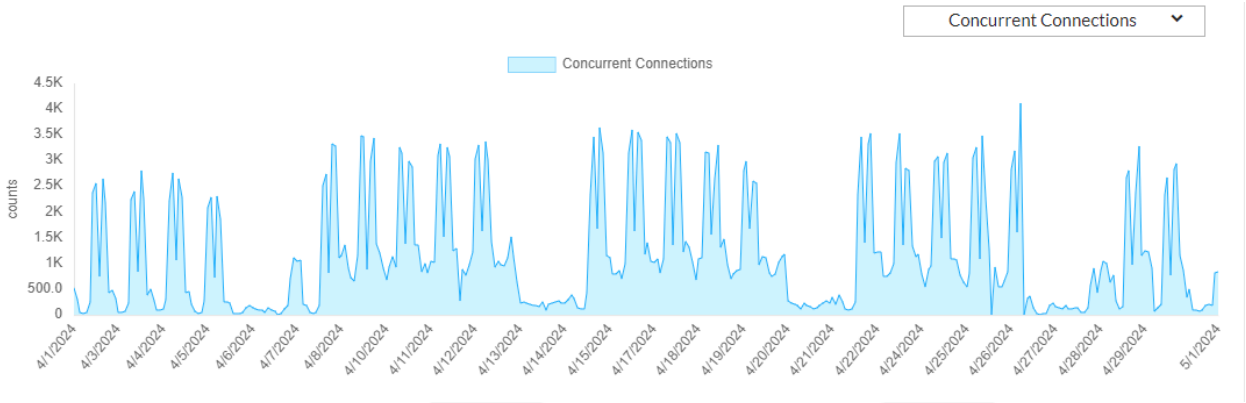
Conexiones concurrentes Virtual Server Justicia XXI con el puerto 8443:



Durante abril no se presentó tráfico por el puerto 80:



Conexiones concurrentes Virtual Server Justicia XXI por el puerto 443:

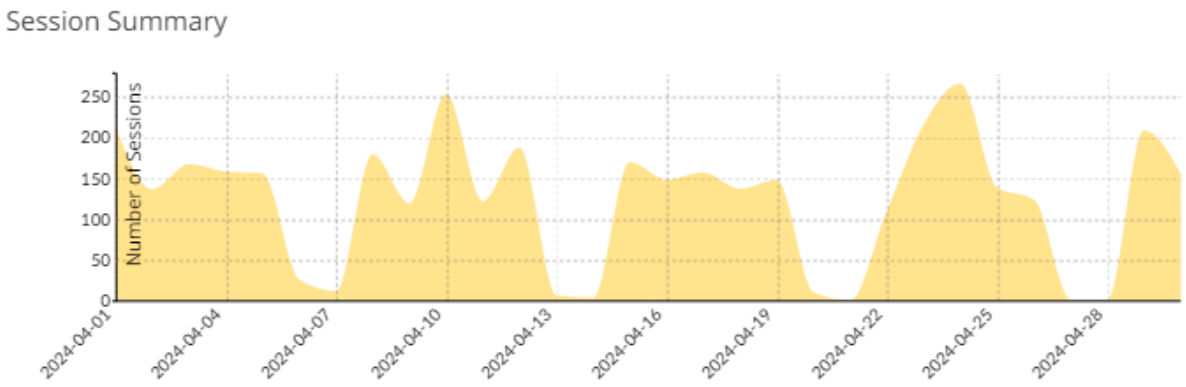


17.2 Kactus RDP

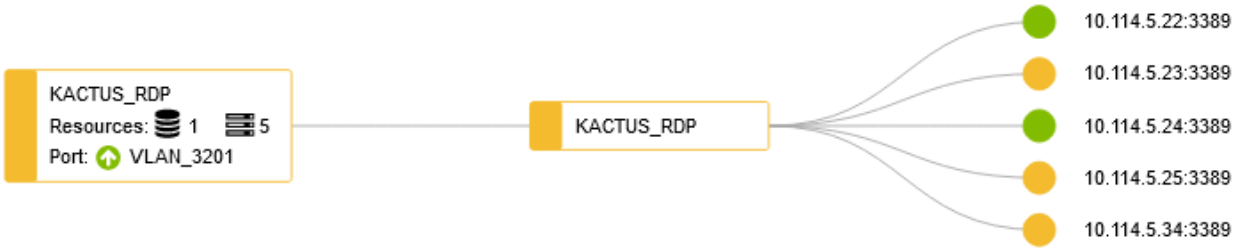
Esta aplicación se encuentra en el Firewall utilizando la siguiente configuración:

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

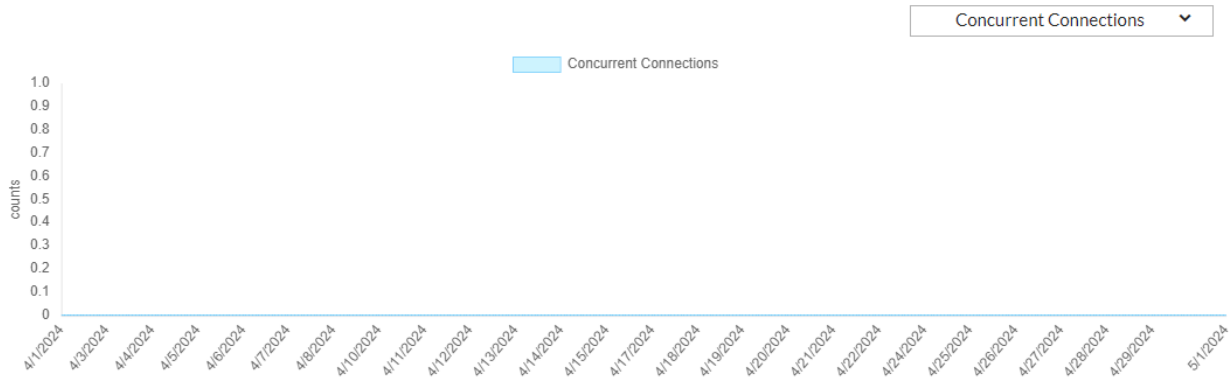
A continuación, se observa el número de sesiones concurrentes para este aplicativo.



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

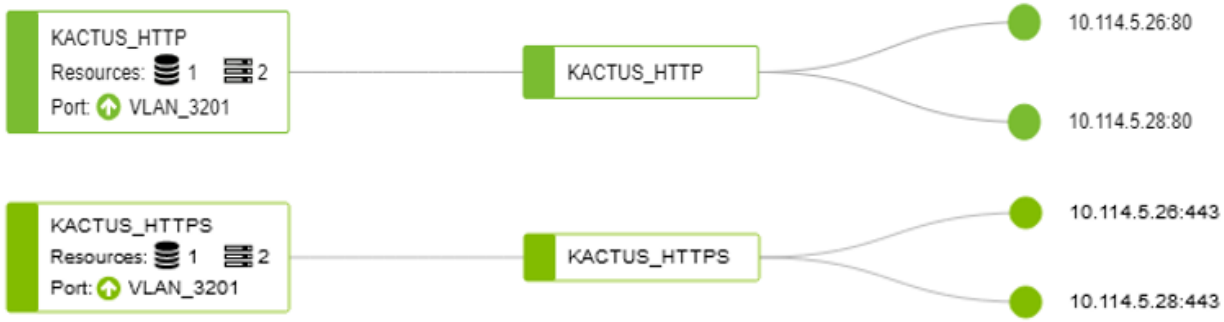


En el FortiADC no se observan sesiones concurrentes:

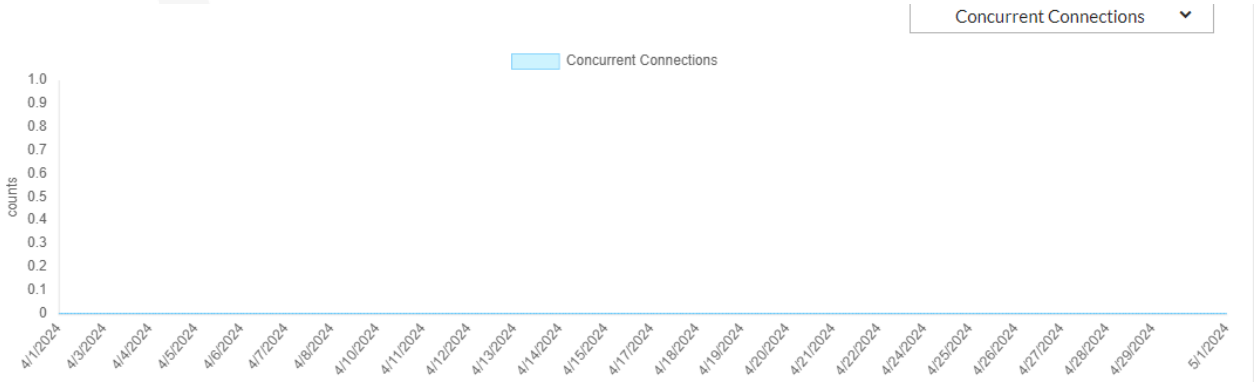


17.3 Kactus WEB

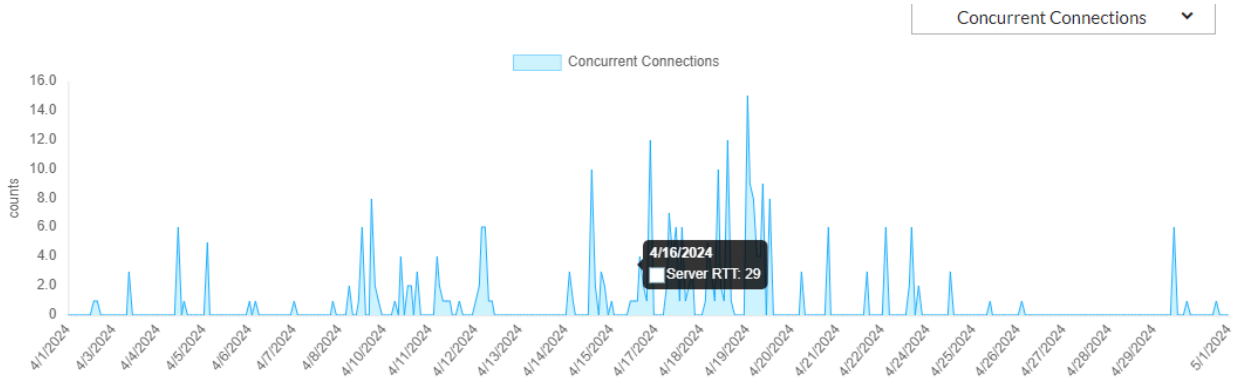
Se encuentra balanceado en el FortiADC:



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



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



17.4 SIRNA

Este servicio se encuentra balanceado en el Fortigate perimetral:

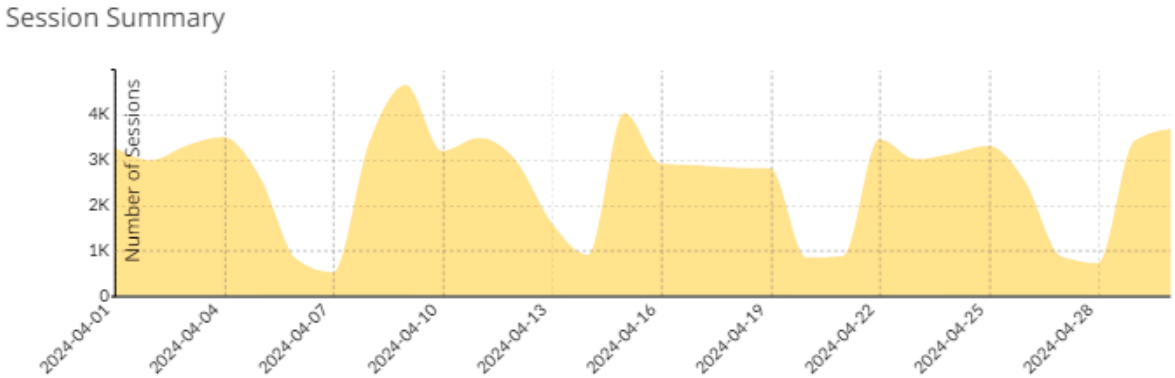
Configuración de balanceo de CRM en el Firewall.

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

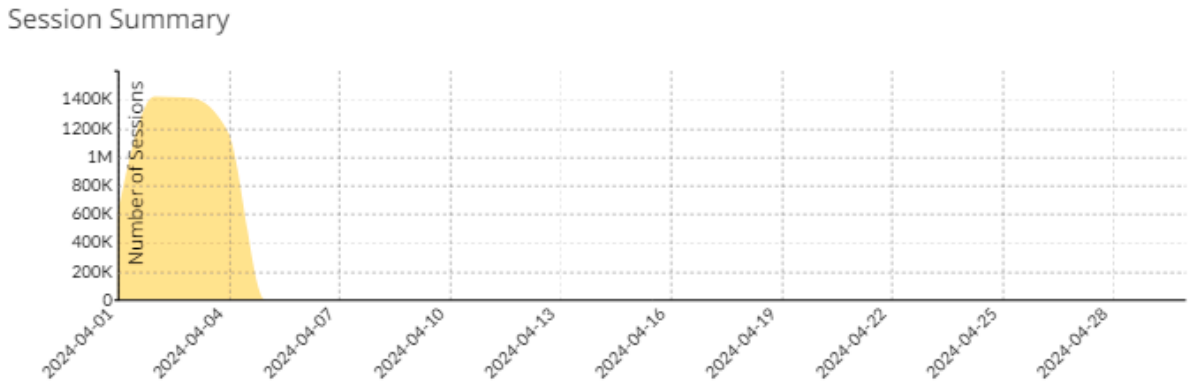
Configuración de balanceo de Sharepoint en el firewall perimetral.

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

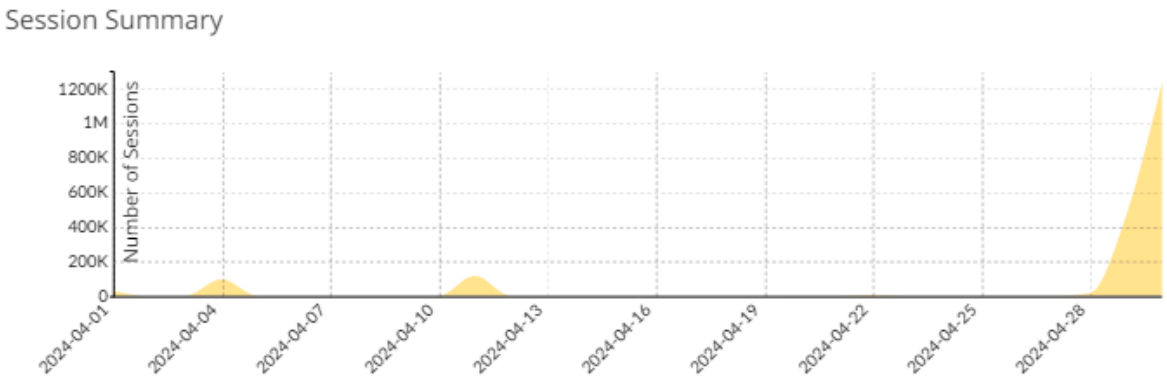
Las sesiones en el firewall para SIRNA 4443 fueron:



Las sesiones en el firewall para CRM 443 fueron:



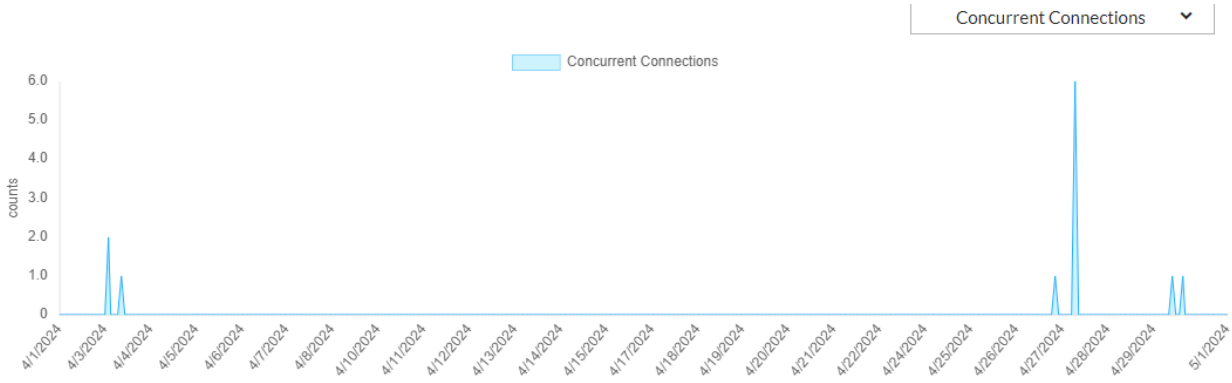
Las sesiones en el firewall para Sharepoint 444 fueron:



17.5 Convocatoria Peritos.

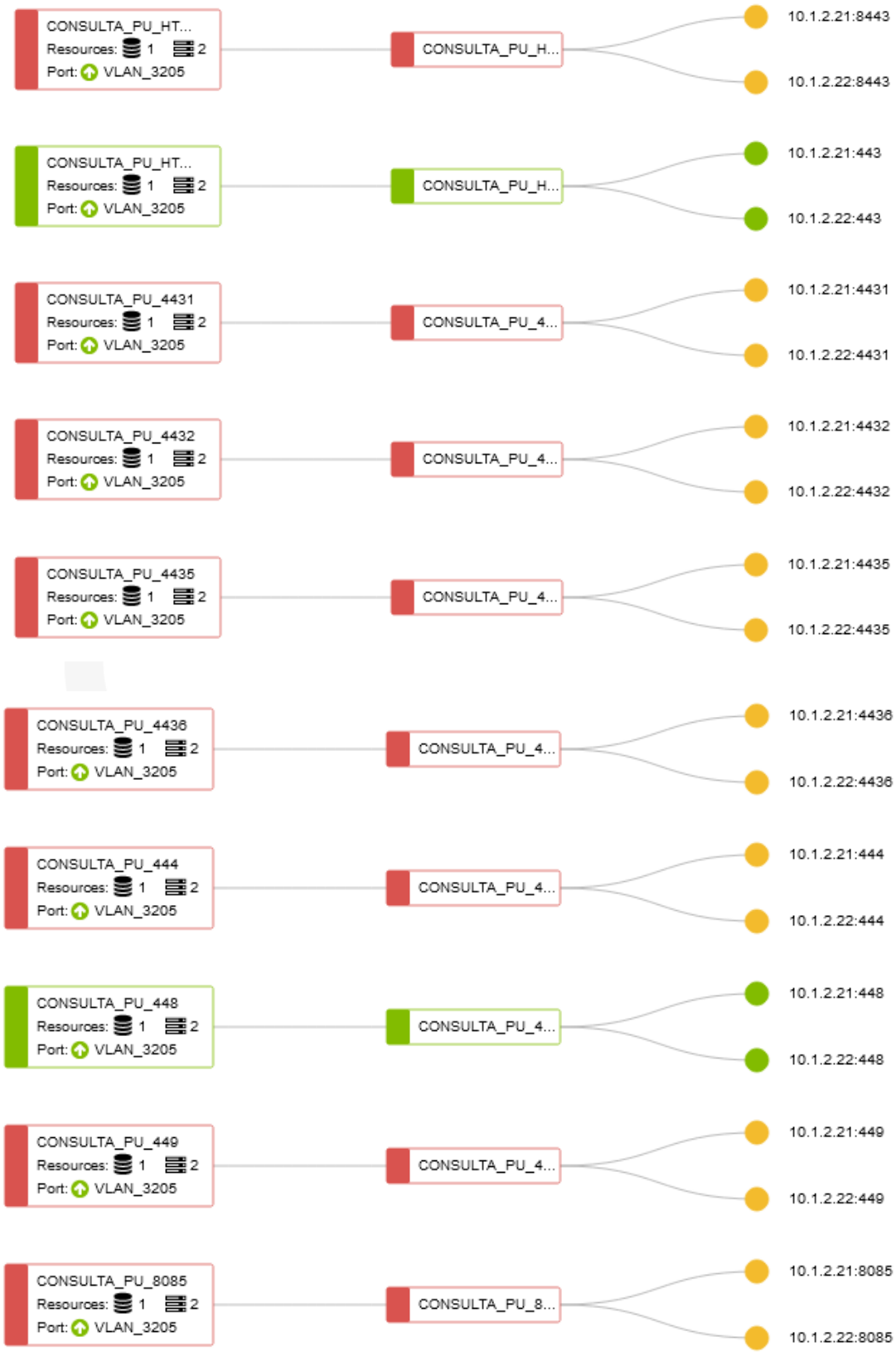
Este servicio se encuentra balanceado en el FortiADC:

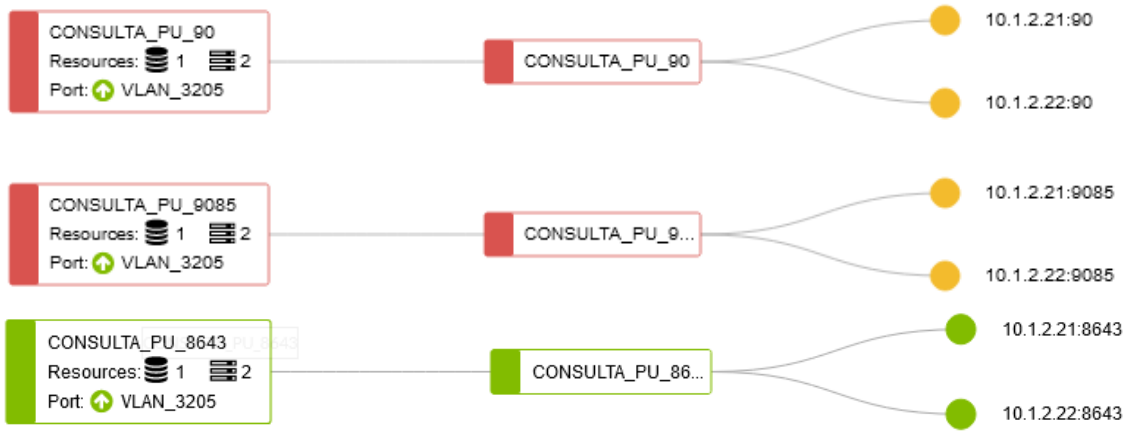
Las sesiones concurrentes fueron las siguientes:



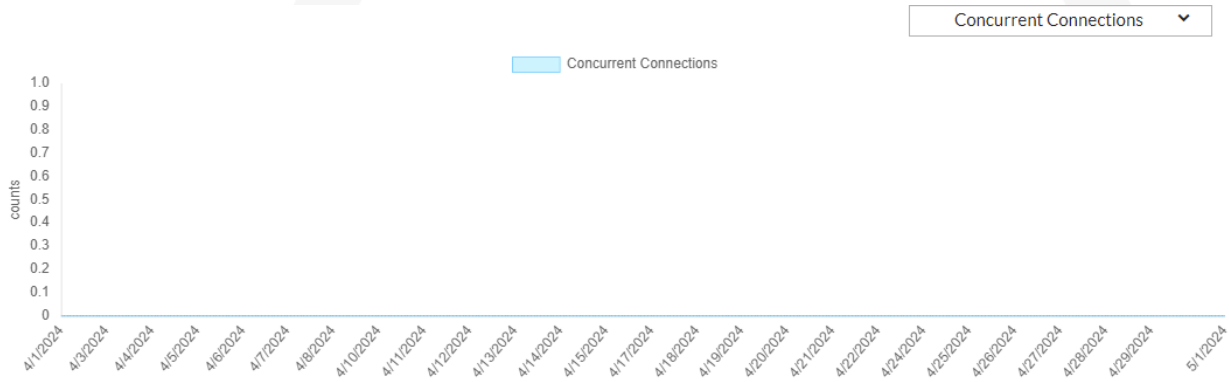
17.6 Consulta De Procesos Nacional Unificada (CPNU)

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

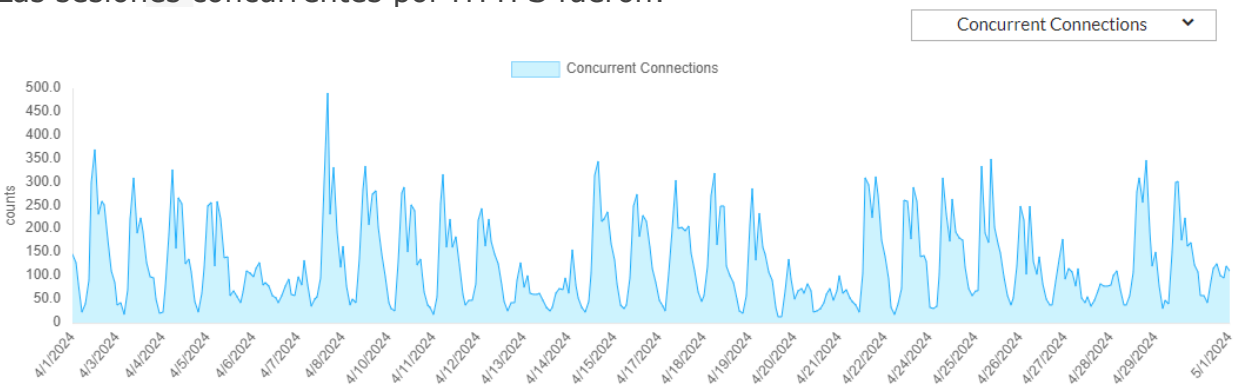




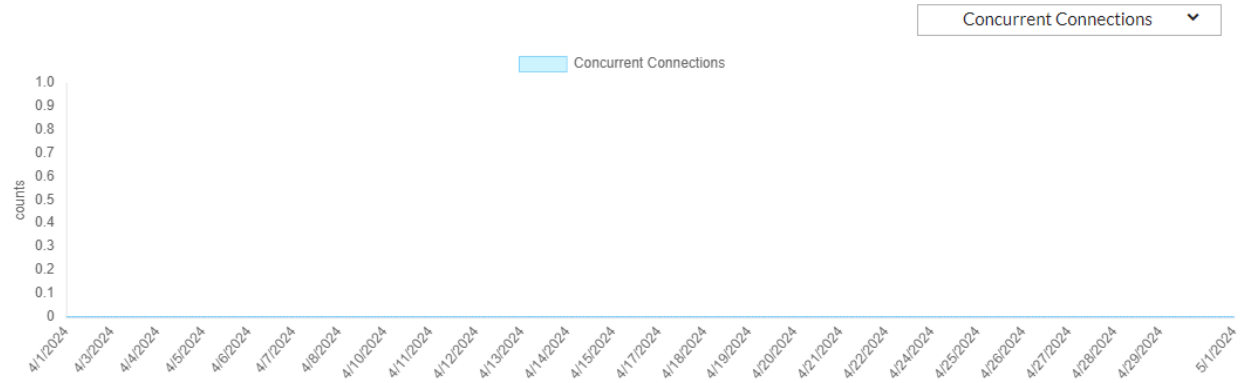
Durante abril no se tuvieron sesiones concurrentes por el puerto HTTP:



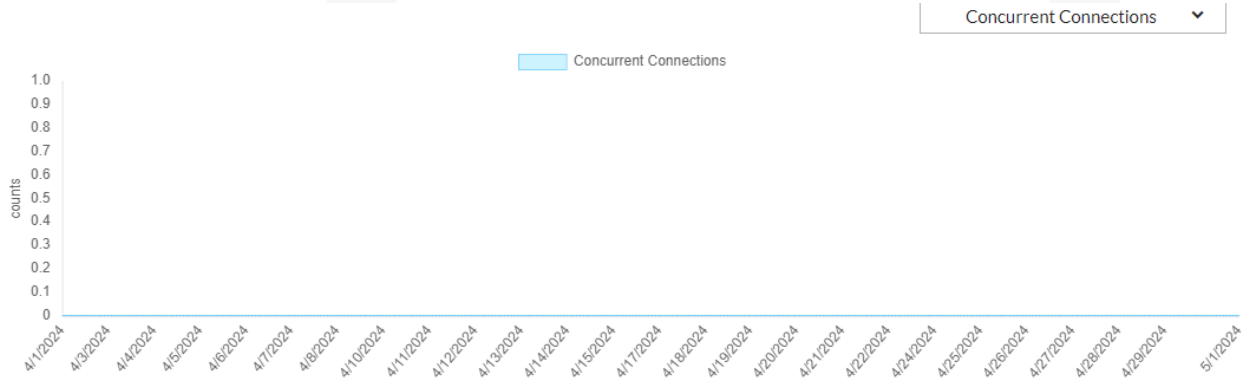
Las sesiones concurrentes por HTTPS fueron:



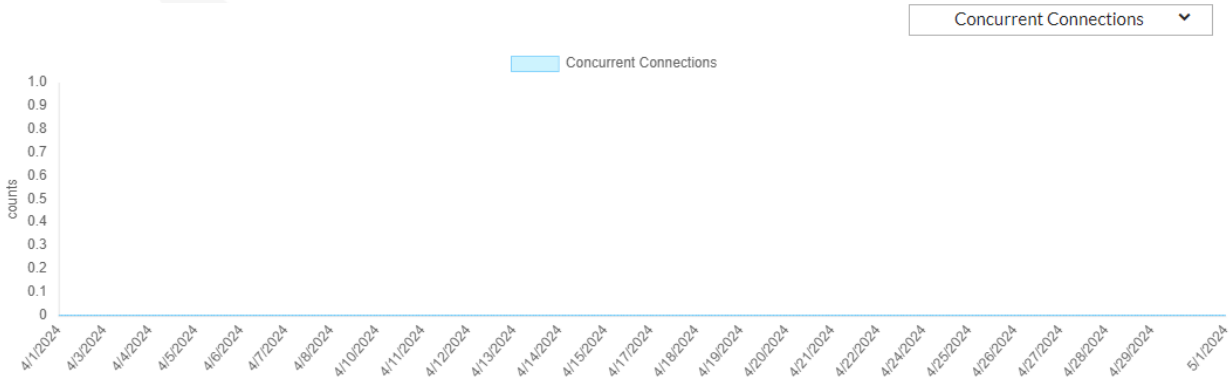
No se tuvieron sesiones concurrentes por el puerto 4431:



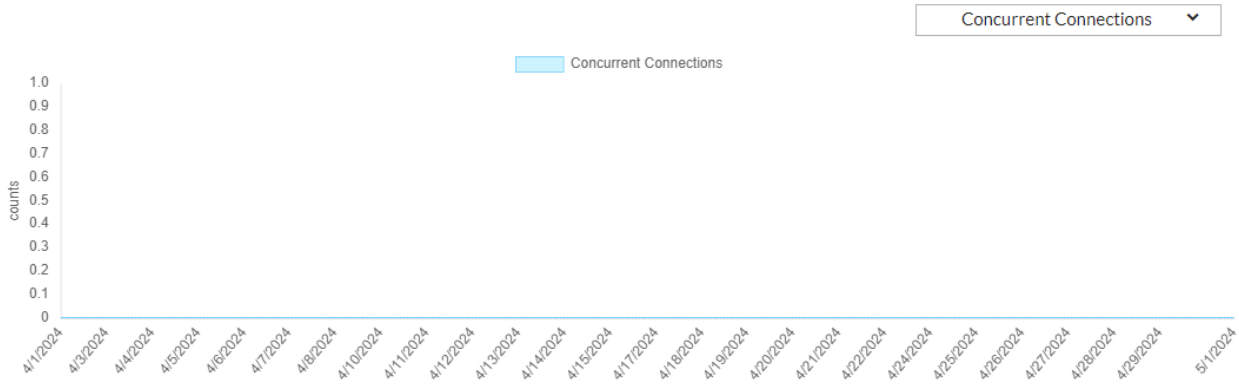
No se tuvieron sesiones concurrentes por el puerto 4432:



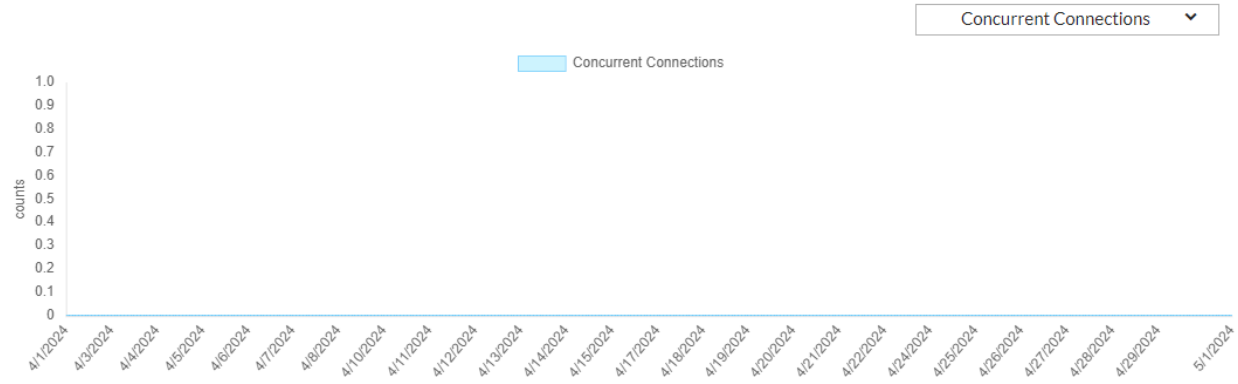
No se tuvieron sesiones concurrentes por el puerto 4435:



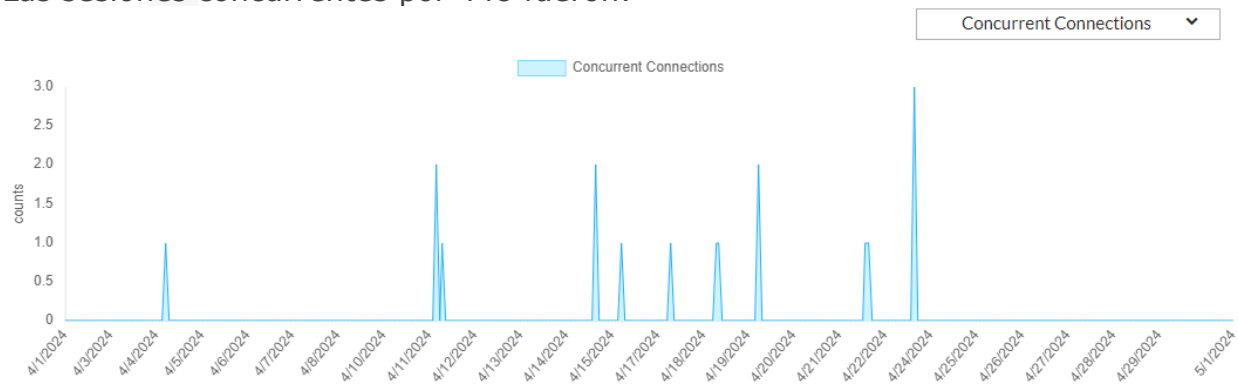
Las sesiones concurrentes por puerto 4436 fueron:



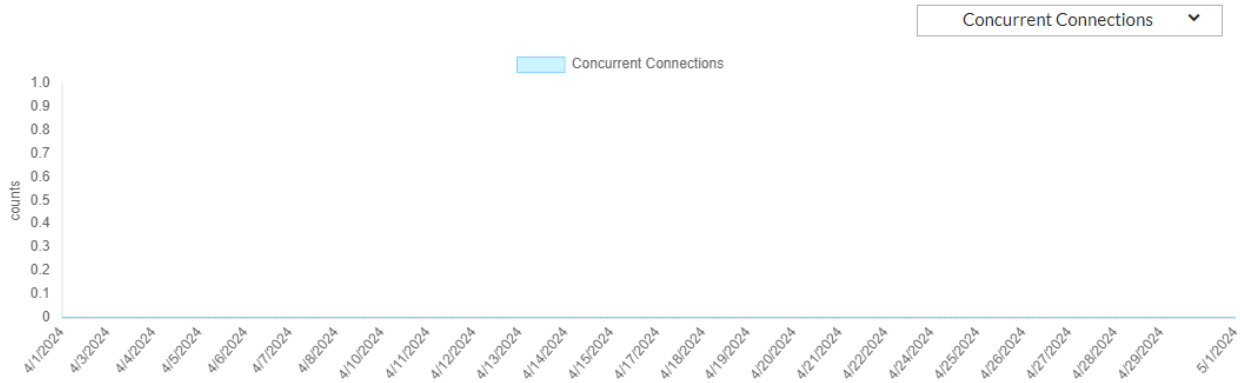
No se tuvieron sesiones concurrentes por el puerto 444:



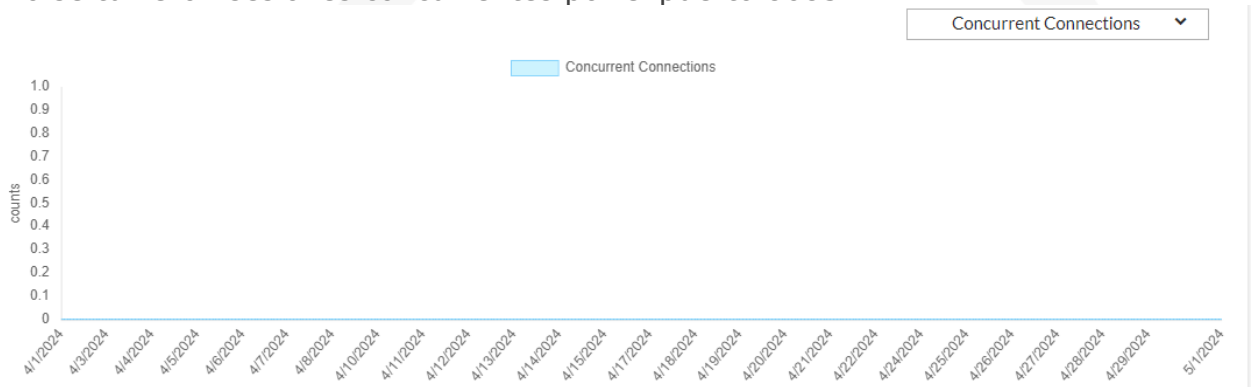
Las sesiones concurrentes por 448 fueron:



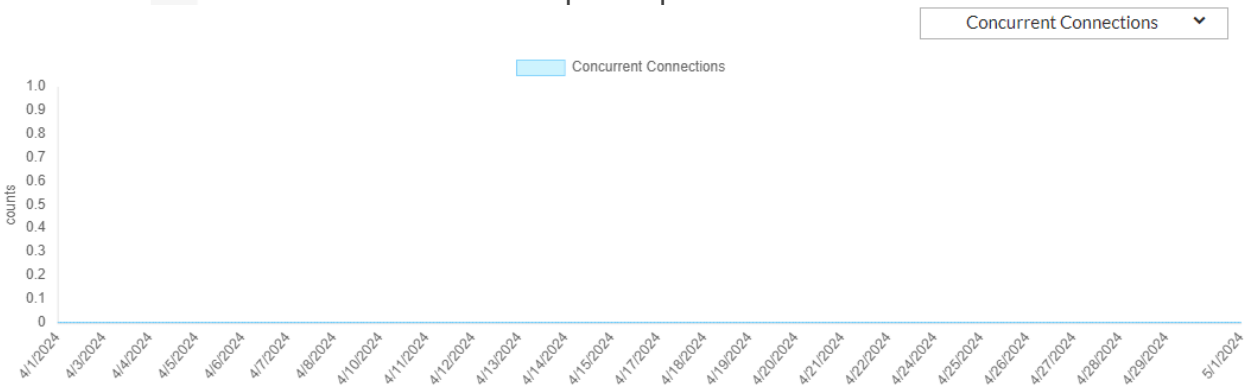
No se tuvieron sesiones concurrentes por el puerto 449:



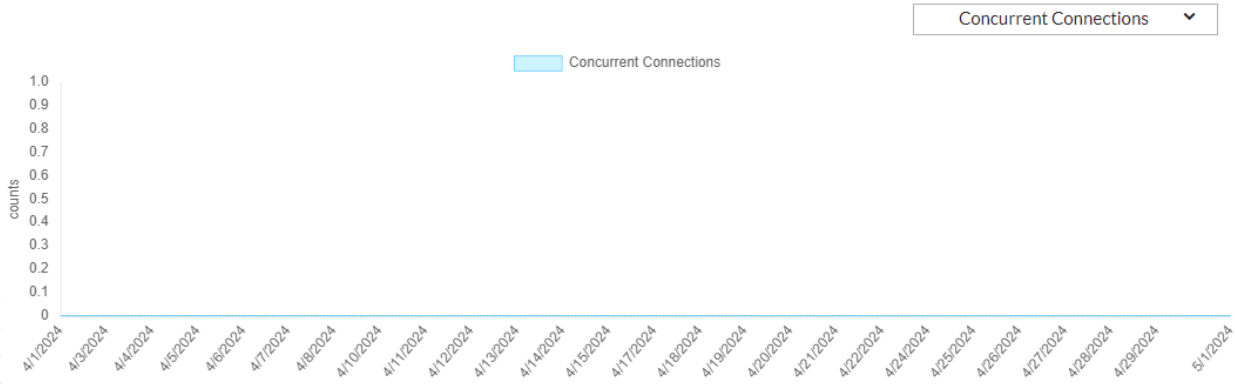
No se tuvieron sesiones concurrentes por el puerto 8085:



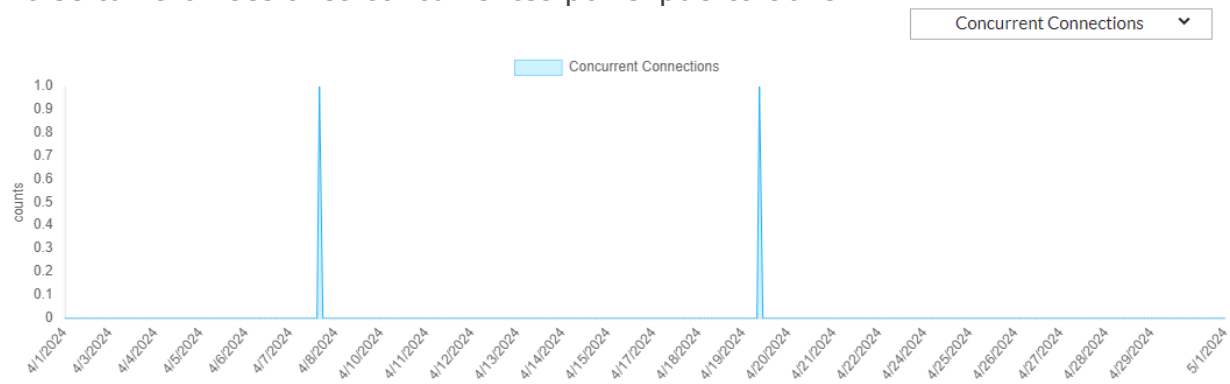
No se tuvieron sesiones concurrentes por el puerto 90:



No se tuvieron sesiones concurrentes por el puerto 9085:



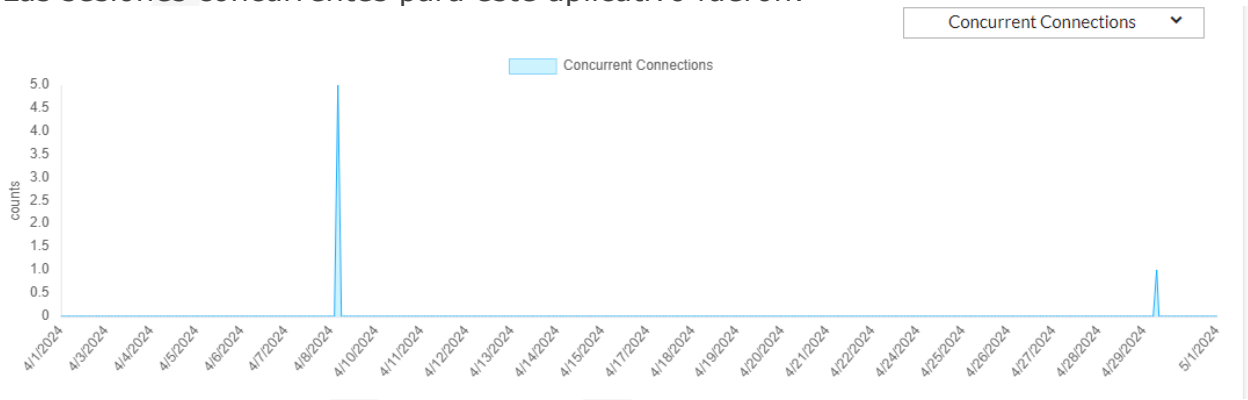
No se tuvieron sesiones concurrentes por el puerto 8643:



17.7 SIERJU

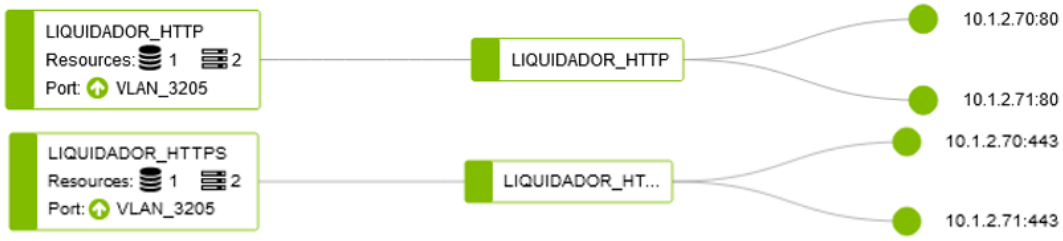
La configuración de balanceo para esta aplicación en el balanceador FortiADC es:

Las sesiones concurrentes para este aplicativo fueron:

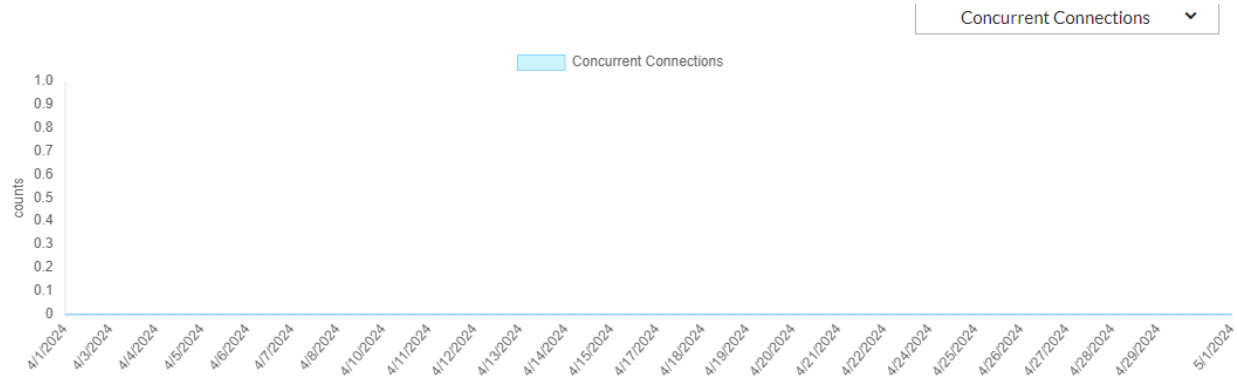


17.8 Liquidador de Sentencias

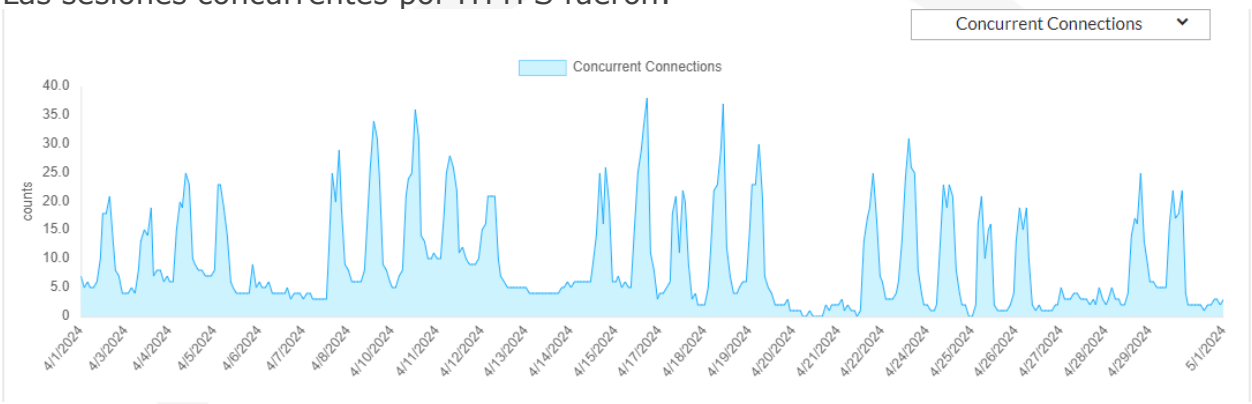
Virtual server Liquidador de Sentencias balanceador FortiADC



Las sesiones concurrentes por HTTP fueron:



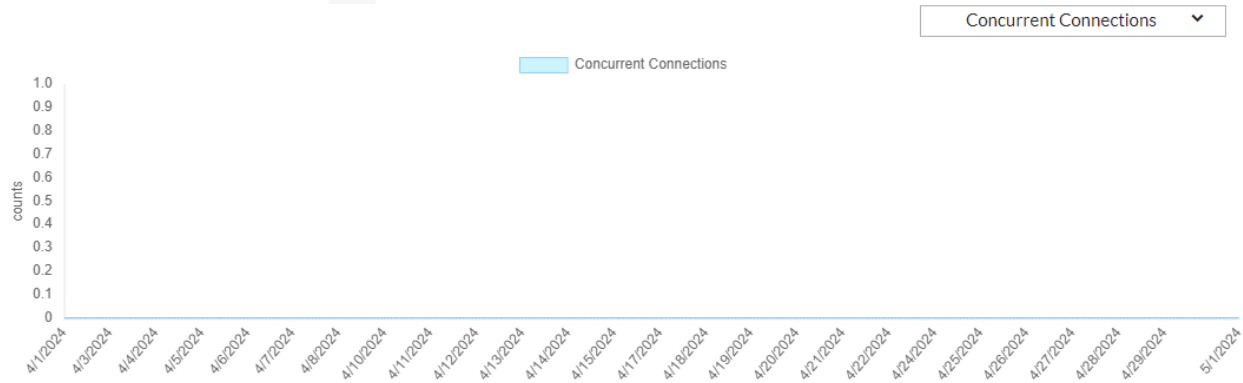
Las sesiones concurrentes por HTTPS fueron:



17.9 Consulta Jurisprudencia

Virtual server Consulta Jurisprudencia se encuentra en el balanceador FortiADC.

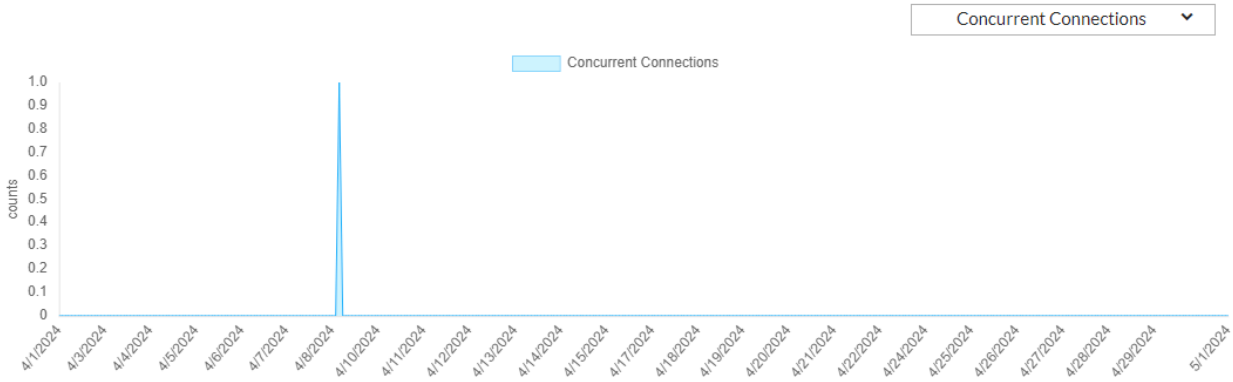
Las sesiones concurrentes para este aplicativo fueron:



17.10 API Gestión de Audiencias

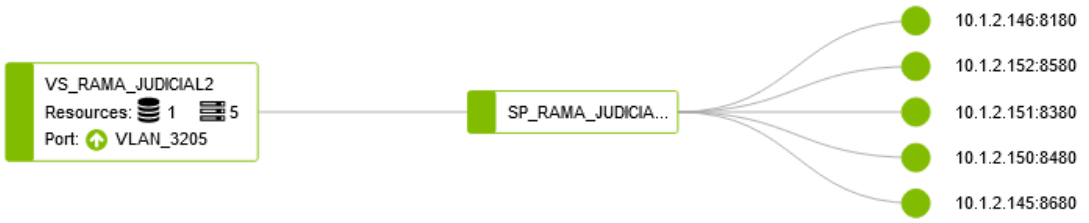
Virtual server API Gestión de Audiencias balanceador FortiADC.

Las sesiones concurrentes para este aplicativo fueron:

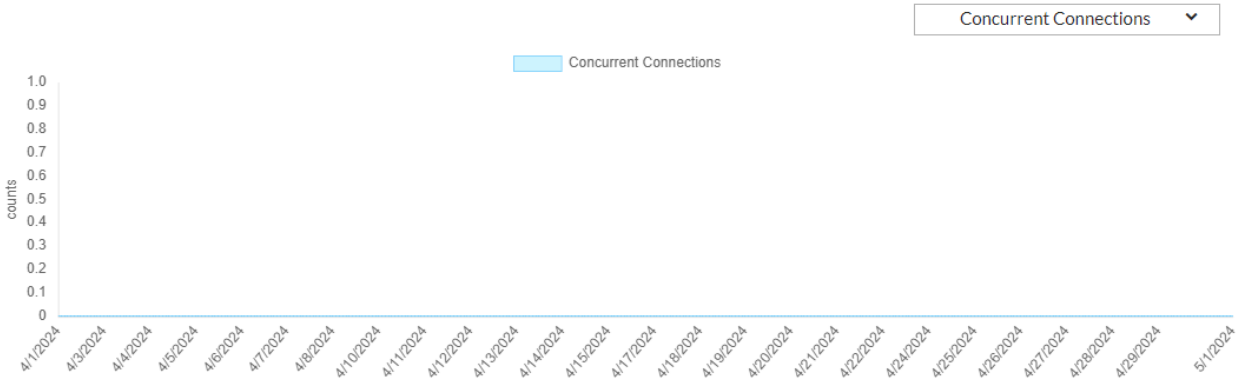


17.11 Portal Alterno de la Rama Judicial

Se encuentran balanceado en el FortiADC:

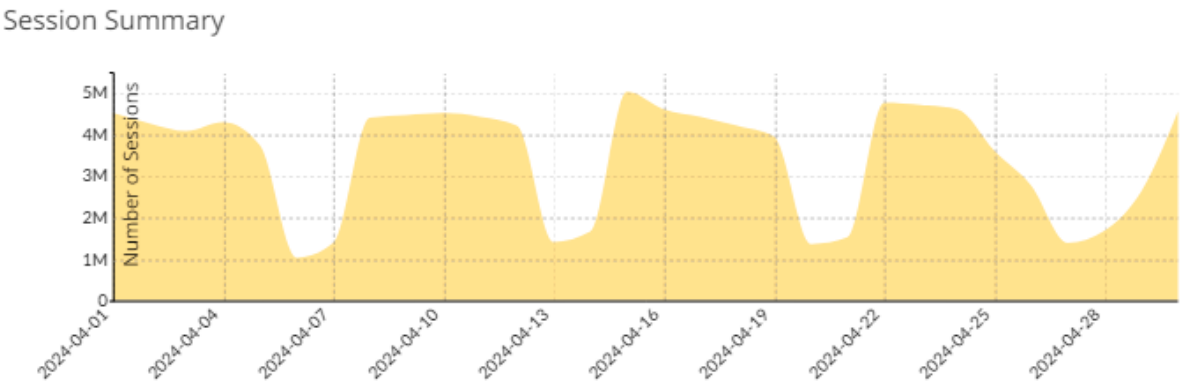


No se observan sesiones concurrentes para este portal alterno:



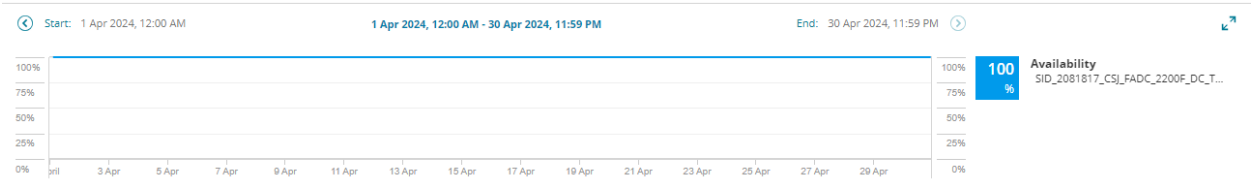
17.12 Portal de la Rama Judicial

Las sesiones para este portal fueron:

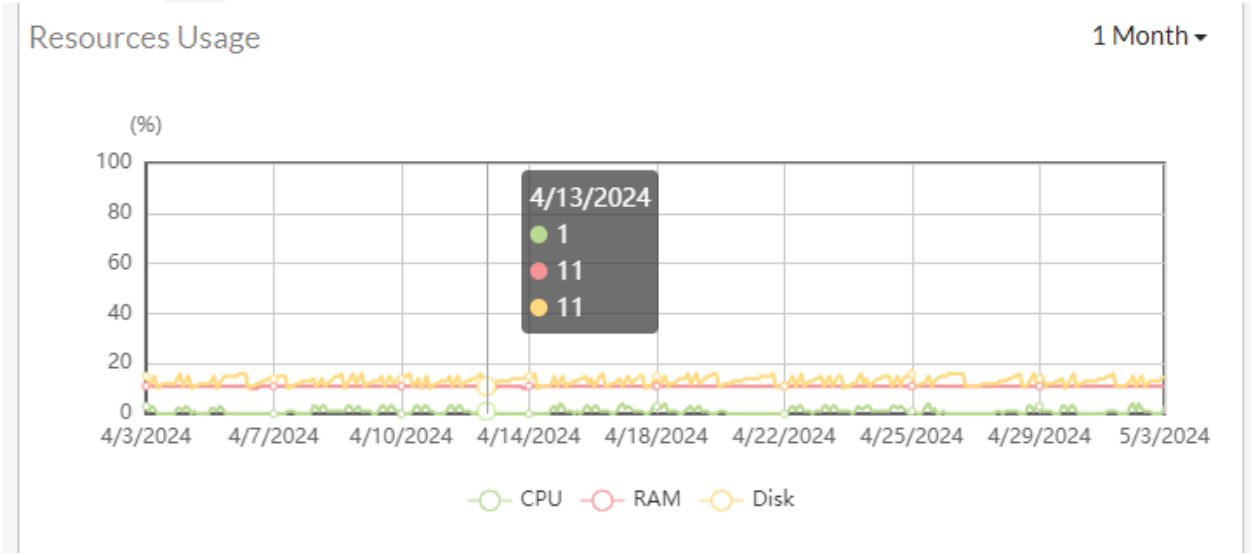


17.13 Disponibilidad y performance.

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



Durante abril se observa que el consumo de CPU es del 1%, memoria 11% y disco 11%.



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

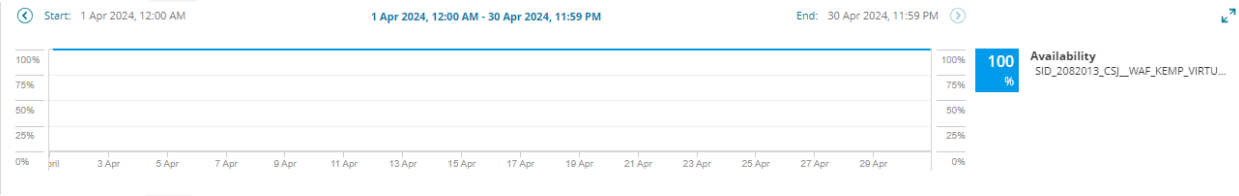
Para la protección de las aplicaciones web se tienen configuradas las siguientes políticas en los Firewall de Aplicaciones Web:

Item	Solución WAF	Cantidad de políticas de servidores
1	WAF TORRE CENTRAL	157
2	WAF CAN	67

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

18.1 Web application firewall datacenter principal IFX.

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



Es importante resaltar que los dispositivos KempX.25, no proporcionan información detallada como (picos de consumo, días y horarios específicos, entre otros).

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

La aplicación web más consultada durante abril fue consultaprocesos.ramajudicial.gov.co-448:

#	Name	Virtual IP Address	Total Events	% del total
1	consultaprocesos.ramajudicial.gov.co - 448	172.17.201.68:448	7305434	33%
2	consejodeestado.gov.co - 190.217.24.60	172.17.201.52:443	2249541	10%
3	procesos.ramajudicial.gov.co_procesoscs CONSULTA AZUL	172.17.201.26:8443	2190829	10%
4	procesos.ramajudicial.gov.co_procesoscs CONSULTA AZUL	172.17.201.26:8443	2190829	10%

5	www.ramajudicial.gov.co - 190.217.24.149	172.17.201.25:443	2034857	9%
6	www.ramajudicial.gov.co - 190.217.24.149	172.17.201.25:443	2034857	9%
7	procesojudicial.ramajudicial.gov.co TYBA PRUEBAS	172.17.201.249:443	1782442	8%
8	www.corteconstitucional.gov.co	172.17.201.13:443	878246	4%
9	consultaprocesos.ramajudicial.gov.co - 443	172.17.201.68:443	558042	3%
10	www.corteconstitucional.gov.co Redirect	172.17.201.13:80	124640	1%
	Otros		587803	3%
	Total		21937520	100%

Es importante resaltar que los dispositivos KempX.25, no proporcionan información detallada como (picos de consumo, días y horarios específicos, entre otros).

18.3 Top de peticiones por país WAF principal IFX.

En abril, el país desde donde se recibieron más peticiones de conexión fue Estados Unidos:

Top 10 Countries

Total

Country	Requests	Blocked
United States	6163876	275855
Colombia	5111658	28448
Private	667619	23354
IPrep	2559	2559
Brazil	91273	1557
Argentina	1971258	1104
Germany	60530	611
South Africa	2513	339
Albania	23180	72
Russia	421249	70

18.4 Top de ataques por política WAF principal IFX.

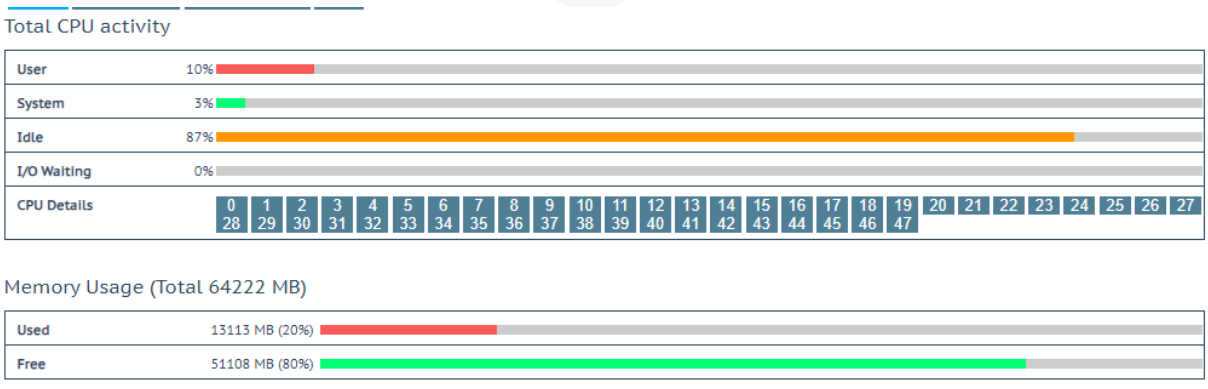
Sobre las aplicaciones www.ramajudicial.gov.co y procesojudicial.ramajudicial.gov.co TYBA PRUEBAS han sido prevenidas la mayor cantidad de ataques:

#	Name	Virtual IP Address	Total Events	% del total
1	www.ramajudicial.gov.co - 190.217.24.149	172.17.201.25:443	15804999	32%
2	procesojudicial.ramajudicial.gov.co TYBA PRUEBAS	172.17.201.249:443	9671248	20%
3	consultaprocesos.ramajudicial.gov.co - 448	172.17.201.68:448	8325620	17%
4	procesos.ramajudicial.gov.co_procesoscs CONSULTA AZUL	172.17.201.26:8443	7029026	14%
5	consejodeestado.gov.co - 190.217.24.60	172.17.201.52:443	2296957	5%
6	consultaprocesos.ramajudicial.gov.co - 443	172.17.201.68:443	1905598	4%
7	www.corteconstitucional.gov.co	172.17.201.13:443	1678883	3%
8	judit.ramajudicial.gov.co - Ivanti - TT682978 - 190.217.24.141	172.17.201.141:443	336880	1%
9	nuevoportal.ramajudicial.gov.co	172.17.201.101:443	335777	1%
10	sirna.ramajudicial.gov.co	172.17.201.28:443	327017	1%
	Otros		1479784	3%
	Total		49191789	100%

Es importante resaltar que los dispositivos KempX.25, no proporcionan información detallada como (picos de consumo, días y horarios específicos, entre otros).

18.5 Consumo de recursos WAF principal IFX.

El WAF KEMP de Torre Central presentó consumo de CPU del 10%, memoria de 20% y disco en un 22%.



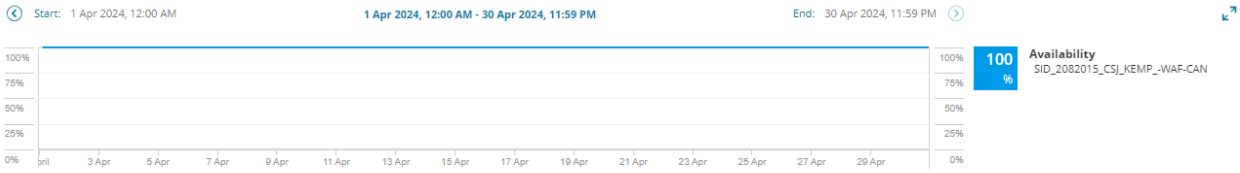
Disk Usage

/var/log (24.61 GB)	0.21 GB (1%)
/var/log/userlog (886.34 GB)	192.92 GB (22%)

19. TRÁFICO DE WEB APPLICATION FIREWALL (WAF) CAN

19.1 Disponibilidad WAF CAN.

Durante abril se obtuvo una disponibilidad del 100 % en el WAF de CAN.



Es importante resaltar que los dispositivos KempX.25, no proporcionan información detallada como (picos de consumo, días y horarios específicos, entre otros).

19.2 Uso de políticas de servidores WAF CAN.

La aplicación más consultada durante abril fue restituciontierras.ramajudicial.gov.co:

#	Name	Virtual IP Address	Total Events	% del total
1	restituciontierras.ramajudicial.gov.co	172.17.202.37:443	1669727	46%
2	samairj.consejodeestado.gov.co	172.17.202.38:443	420653	12%
3	restituciontierras.ramajudicial.gov.co redirect	172.17.202.37:80	374897	10%
4	linkce.consejodeestado.gov.co	172.17.202.42:443	184201	5%
5	serviciopdf.ramajudicial.gov.co	172.17.202.7:443	140434	4%
6	siapoas.ramajudicial.gov.co	172.17.202.43:443	129844	4%
7	capacitacion.ramajudicial.gov.co 443	172.17.202.13:443	122658	3%
8	sigobius.consejodeestado.gov.co_443	172.17.202.29:443	94668	3%
9	factor_calidad.ramajudicial.gov.co	172.17.202.34:443	64719	2%
10	pruebasportal.ability.com.co_Portal pruebas	172.17.202.47:80	56649	2%
	Otros		336576	9%
	Total		3595026	100%

19.3 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	3552703	319751
Private	1196854	7275
Brazil	67632	5129
India	10973	1240
Netherlands	32918	970
IPrep	895	895
Bangladesh	9100	837
Dominican Republic	4423	789
Hong Kong	3868	510
Germany	51333	423

19.4 Top de ataques por política WAF CAN.

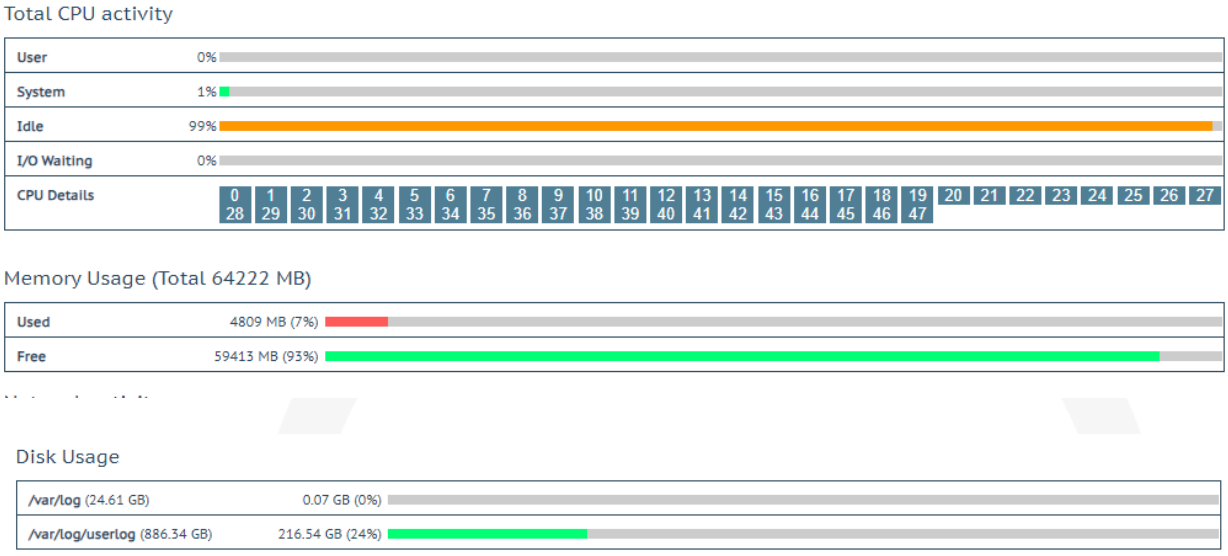
Sobre la aplicación cortesuprema.gov.co_Palacio ha sido prevenida la mayor cantidad de ataques:

#	Name	Virtual IP Address	Total Events	% del total
1	cortesuprema.gov.co_Palacio	172.17.202.239:443	38229186	80%
2	restituciontierras.ramajudicial.gov.co	172.17.202.37:443	3902870	8%
3	sso.cortesuprema.gov.co	172.17.202.141:443	1535417	3%
4	linkce.consejodeestado.gov.co	172.17.202.42:443	1054555	2%
5	siapoas.ramajudicial.gov.co	172.17.202.43:443	569852	1%
6	capacitacion.ramajudicial.gov.co 443	172.17.202.13:443	354765	1%
7	samairj.consejodeestado.gov.co	172.17.202.38:443	319536	1%
8	capacitacion.ramajudicial.gov.co 9443	172.17.202.13:9443	243229	1%
9	sigobius.consejodeestado.gov.co_443	172.17.202.29:443	217422	0%
10	serviciopdf.ramajudicial.gov.co	172.17.202.7:443	213702	0%
	Otros		1144414	2%
	Total		47784948	100%

Es importante resaltar que los dispositivos KempX.25, no proporcionan información detallada como (picos de consumo, días y horarios específicos, entre otros).

19.5 Consumo de recursos WAF CAN.

El WAF KEMP del CAN presentó consumo de CPU del 0%, memoria de 7% y disco en un 24%.



19.6 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]

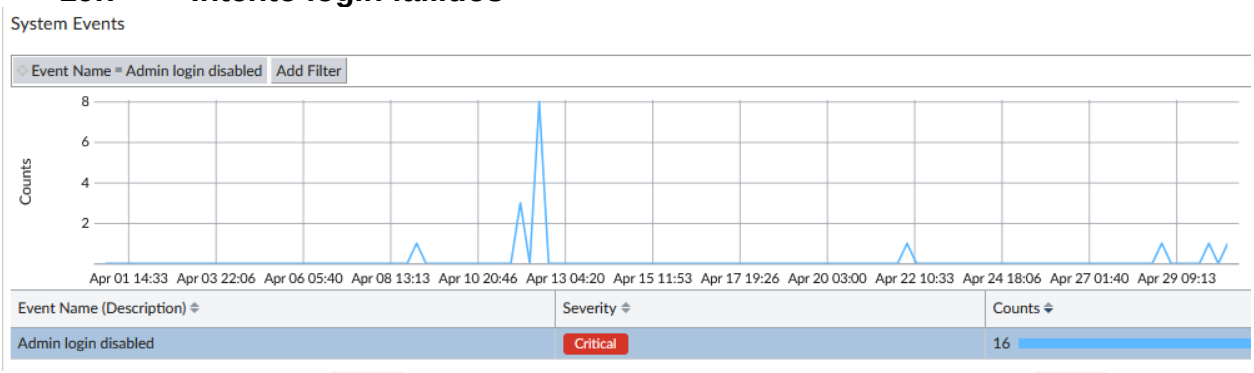
:corteconstitucional.gov.c
[Expires: Sep 30 23:59:59
2024 GMT]

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

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

19.7 Intento login fallidos

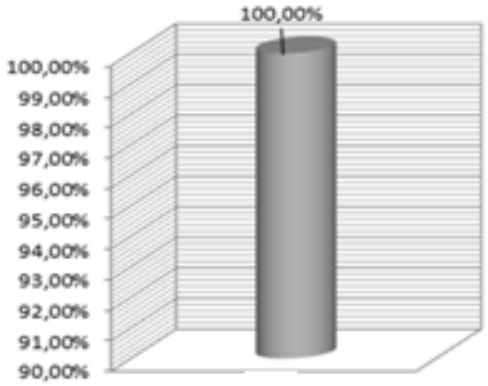


Usuario	Nombre de usuario que hace el intento	Firewall Central	Firewall Palacio	Total de eventos
1	"admin"		12	12
2	"adsl"		1	1
3	"anaranjoca"	1		1
4	"ctorresh"	1		1
5	"fsutab@cendoj.ramajudicial.gov.co"	1		1
6	"ipintop"	3		3
7	"lnanez"	6		6
8	"root"		2	2
9	"scanner"		1	1
10	"super"		1	1
11	"support"		1	1
12	"telecomadmin"		1	1
13	"ubnt"		1	1
14	"unknown"	3		3
15	"user"		2	2
16	"useradmin"		1	1
	Total de eventos	15	23	38

20. DISPONIBILIDAD SEGURIDAD GLOBAL DEL MES DE ABRIL

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

MES	DISPONIBILIDAD (%)
ABRIL	100%



20.1 Anexo de las solicitudes e incidentes de seguridad reportadas.

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

21. 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)

22. GESTIÓN FINANCIERA

22.1 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	$ 2.849.022.850,11
% Valor facturado	18,36%
Valor pagado a la fecha	$ 1.318.151.327,59
% Valor pagado	8,50%

22.2 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

22.3 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

23. 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.