REPORTE MENSUAL

RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA

OC124016

MAYO 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 MAYO de 2024 Fecha de final: 31 de MAYO 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 31 de MAYO de 2024 es de: **3803320 (GB)**

El almacenamiento total presentado adicional es de: **3689407 (GB)**

Total, contratado de Almacenamiento SAN alto rendimiento: **3900000 (3.9GB)**

A corte 31 de mayo 2024 la entidad cuenta con un almacenamiento disponible de **210593 (GB)**

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

Ítem 48 de la Orden de compra 100000 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: 100000

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

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_MAYO_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 MAYO de 2024 es de **1036200 GB** y se desglosa de la siguiente manera:

- Total, contratado de Almacenamiento BK de datos diario y semanal: **350000 GB**
- A la fecha la entidad ha dado uso de 553200 GB de almacenamiento de BK mensual
- **Acorde a la información suministrada con anterioridad, a la fecha la entidad supera en 203200 GB, el almacenamiento BK de datos diario y semanal.**
- Total, contratado de Almacenamiento BK de datos mensual: 250000 GB
- A la fecha la entidad ha dado uso de 483000 GB de almacenamiento de BK mensual
- **Acorde a la información suministrada con anterioridad, a la fecha la entidad supera en 233000 GB, el almacenamiento BK de datos mensual.**

Actualmente la entidad cuenta con 208 máquinas virtuales y 2 máquinas físicas en producción y estado ON. Desde el día 10 de mayo una de las máquinas se encuentra en desuso por solicitud de la entidad, pero en estado ON (disponible). En la sesión ejecutada el día 05-06-2024 con el especialista del portal, se evidenció que las máquinas se encuentran encendidas. Actualmente se encuentra en uso una de las máquinas para el nuevo portal.

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.

(Remitirse al anexo "**Inventario_Servicios_CSJ_MAYO_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 MAYO 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_MAYO_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:

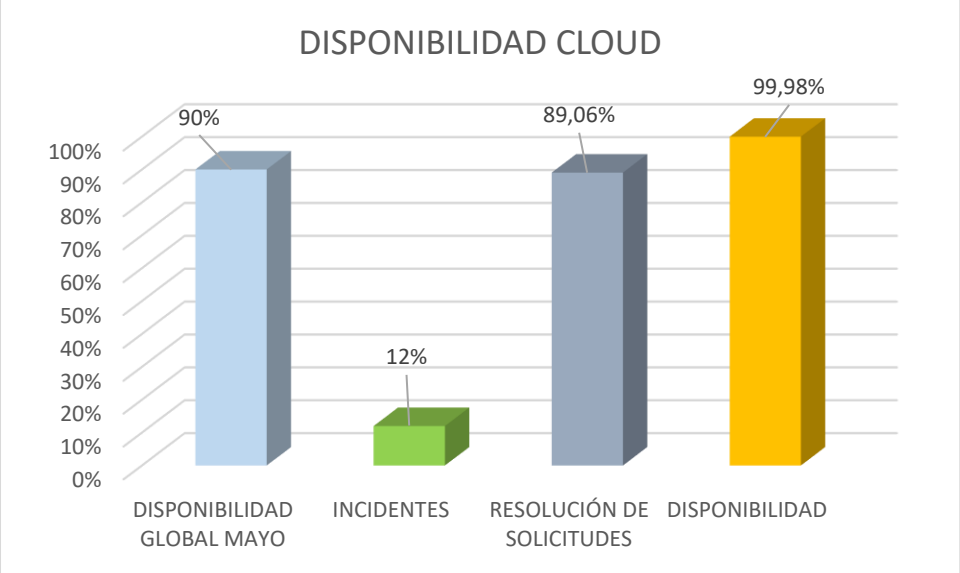
- **Capacitación SST:** líneas de OC 16 y 38
- **Cobro coactivo:** líneas de OC 17 y 38
- **core-impact:** Línea de OC 12
- **Efinomina:** Líneas de OC 14,18,26,27,38 y 39
- **Fuse:** Línea OC 17
- **Gestión grabaciones:** Líneas de OC 12,13, 14,15,17,19,20,22,23,25,28,35,36 y 38
- **InsightVM console:** 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_MAYO_2024.xls**" para ver el detalle "maquinas")

7.DISPONIBILIDAD GLOBAL CLOUD DEL MES DE MAYO

Disponibilidad Global mes de MAYO	Numero de tickets mes de MAYO	Imputabilidad por ANS
	57 solicitudes	**0 solicitudes**
	7 incidentes	**0 incidentes**
90%	Total 64 tickets	0 tickets



CONTROL DOCUMENTAL

ELABORADO POR

Fecha	Autor	Ingeniero
06-06-2024	IFX Networks	Juan Carlos Romero

REVISADO POR

Fecha	Autor	Ingeniero
	IFX Networks	

CONTENIDO

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 mayo a31 de mayo del 2024.

CONSUMO TOTAL HORAS MES DE MAYO	
• Casos Reportados Netsuite	135
Sesiones de Seguimiento	5
Sesiones de Trabajo	0
Casos Escalados Medio Digital - Whatsapp	1
Horas Disponibilidad del Recurso Fines de Semana	259
Total Horas Consumidas de las 300 - Experto Master	400

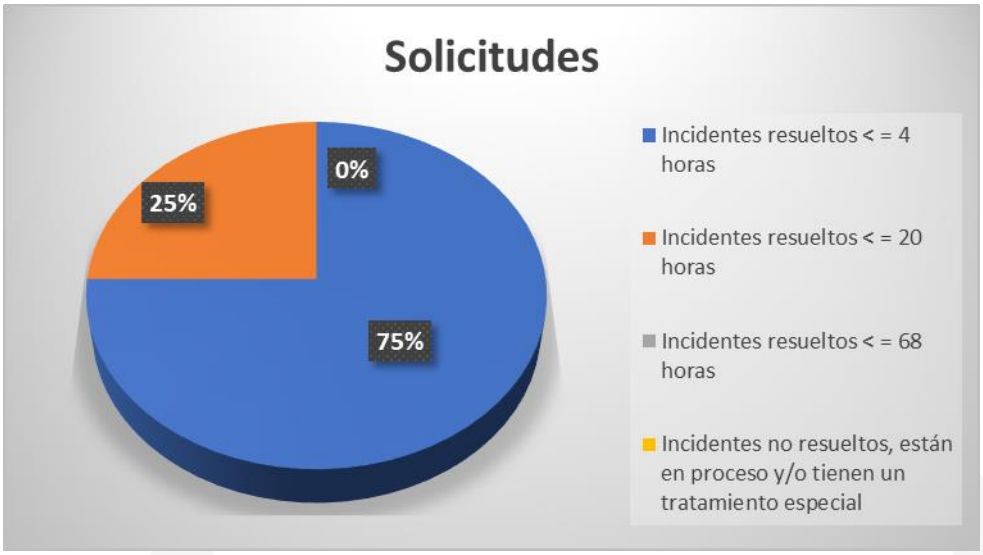
2. INDICADORES DEL CENTRO CONSOLIDADO DE SERVICIOS

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

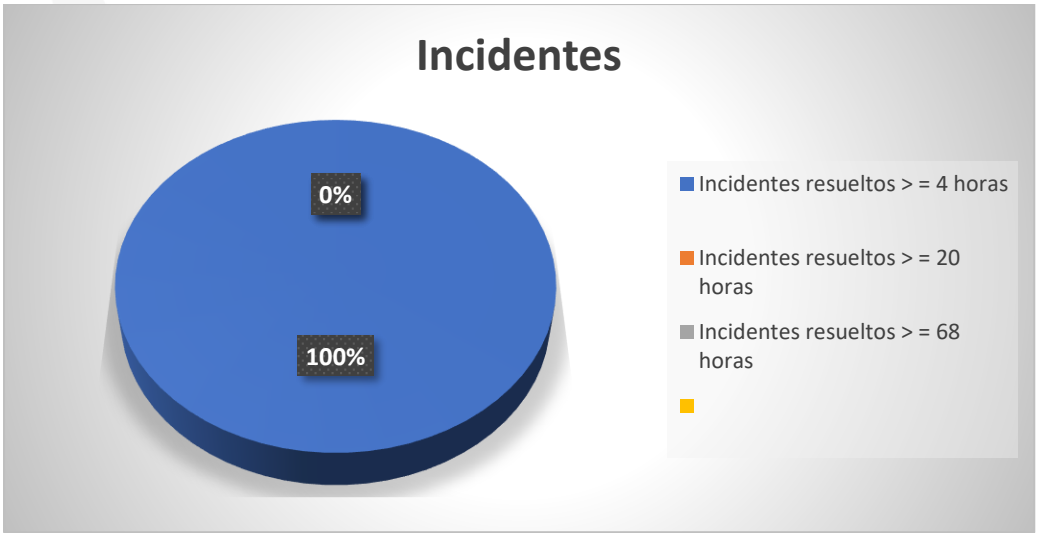
	Volumen en 1 mayo a
Casos Reportados	13
Solicitudes	12
Incidencias	1
WA - AF	0

2.1 TASA DE RESOLUCIÓN DE PROBLEMAS

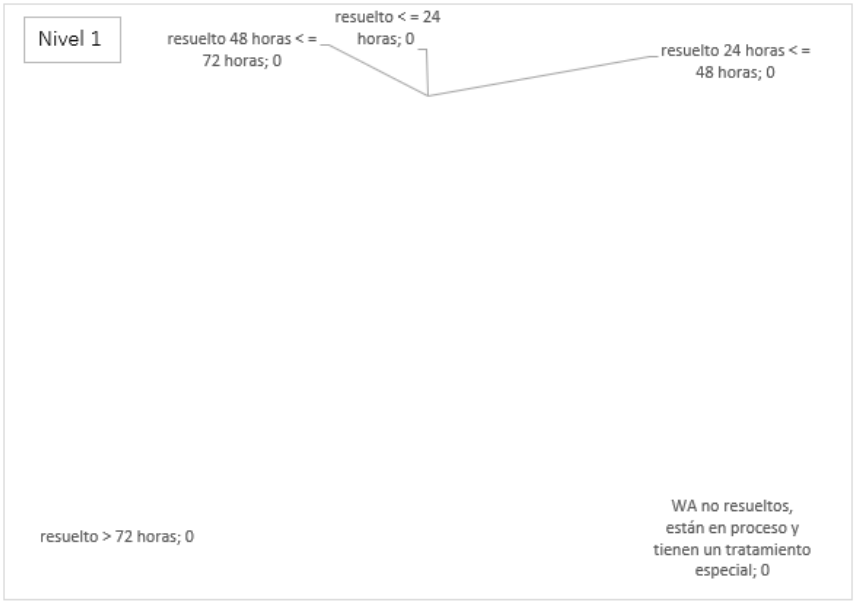
Tiempo de Gestión	Solicitudes
Solicitudes resueltas < = 4 horas	9
Solicitudes resueltas < = 20 horas	3
Solicitudes resueltas < = 68 horas	0
Solicitudes no resueltas, están en proceso y/o tienen un tratamiento especial	0
Total	**12**

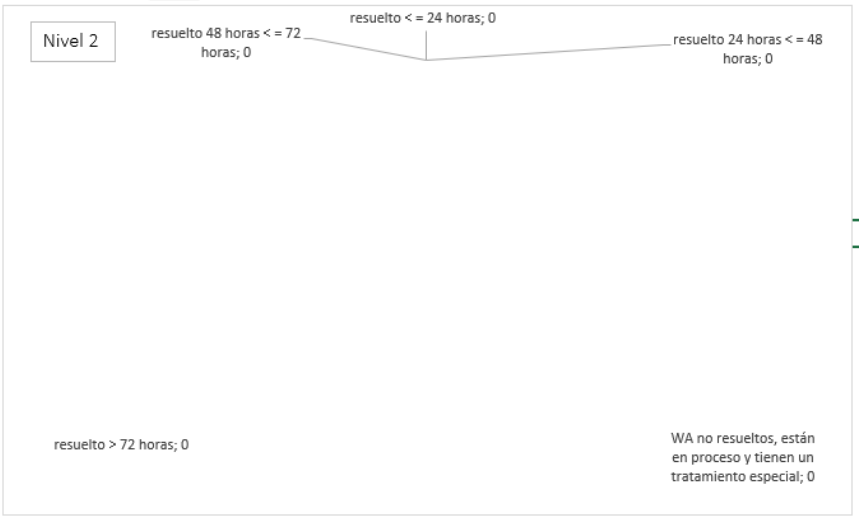


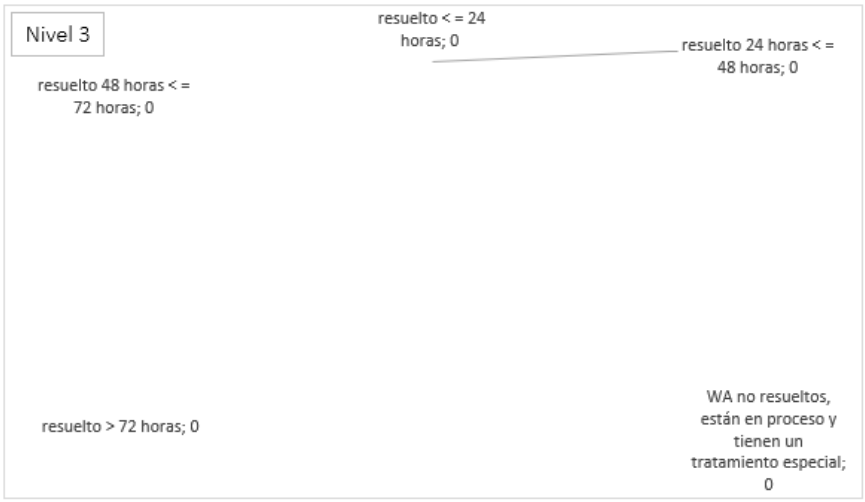
Tiempo de Gestión	Incidentes Penalizados
Incidentes resueltos > = 4 horas	1
Incidentes resueltos > = 20 horas	0
Incidentes resueltos > = 68 horas	0
Total	0

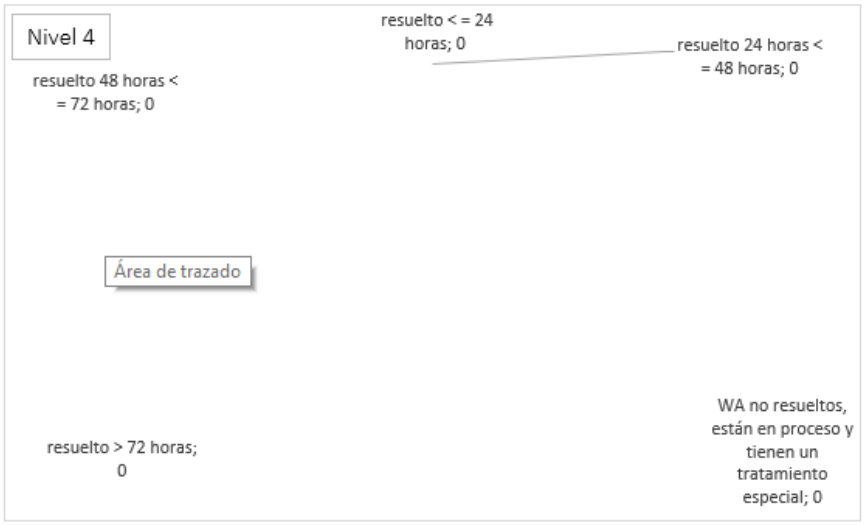


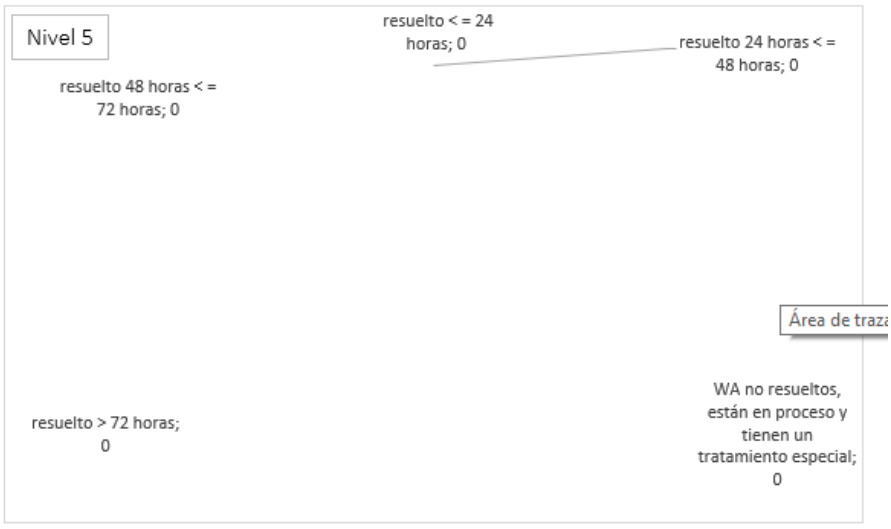
WA (Ajustes Funcionales)					
Tiempo de Gestión	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
resuelto < = 24 horas	0	0	0	0	0
resuelto 24 horas < = 48 horas	0	0	0	0	0
resuelto 48 horas < = 68 horas	0	0	0	0	0
resuelto > 68 horas	0	0	0	0	0
WA no resueltos, están en proceso y tienen un tratamiento especial	0	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 mayo a 31 de mayo 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 mayo a 31 de mayo del 2024.

2.3 BOLSA DE HORAS SEGÚN CONTRATO

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

2.4 ESTADO DE LAS HORAS CONSUMIDAS DE LOS CASOS REPORTADOS

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

Etiquetas de fila	Suma de Horas Hombre	Horas Presupuesto	Horas Disponible
Caso	141	400	259
2024	141		
Solicitud	138		
Incidencia	3		
Total Horas Casos Reportados Netsuite	141	400	259
		259	259
		259	259
		259	259
		259	259
Horas consumidasde las 400 - Exp	400	400	0

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

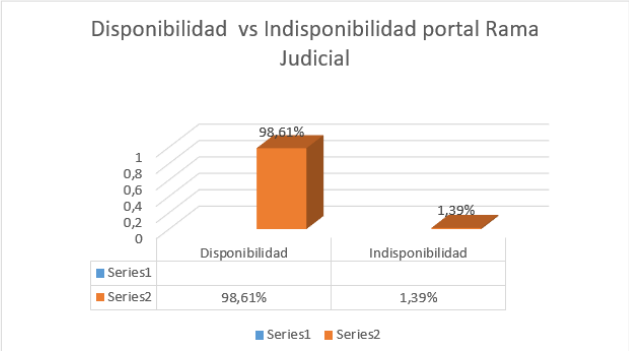
3.1. GRÁFICO DE DISPONIBILIDAD E INDISPONIBILIDAD DE LOS SERVICIOS DEL PORTAL DE RAMA JUDICIAL

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:

Nota: para el mes de mayo 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

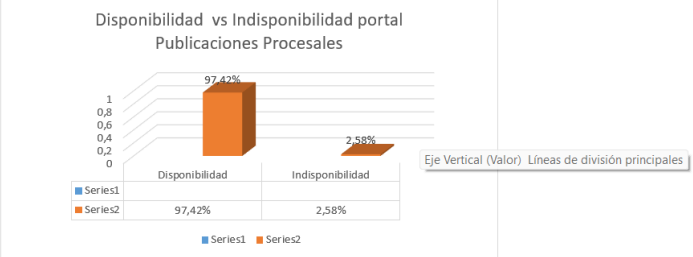
Portal Rama Judicial

Item	Aplicación	Disponibilidad	Indisponibilidad	Tiempo de duracion (Caida en horas)	Tiempo de duracion			
					Dias	Horas	Minutos	Segundos
1	Portal de la Rama Judicial	98,61%	1,39%	10,33861111	0	10	20	19
	Totales	98,61%	1,39%	10,33861111	**0**	10	20	19



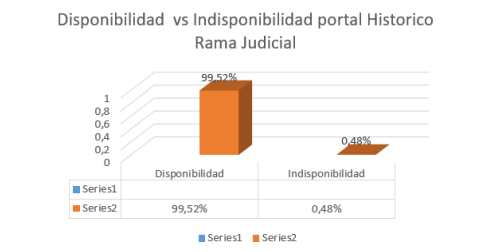
Portal Publicaciones Procesales

Item	Aplicación	Disponibilidad	Indisponibilidad	Tiempo de duracion (Caida en horas)	Tiempo de duracion			
					Dias	Horas	Minutos	Segundos
1	Portal de la Rama Judicial	97,42%	2,58%	19,22166667	0	19	13	18
	Totales	97,42%	2,58%	19,22166667	**0**	19	13	18



Portal Histórico 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	99,52%	0,48%	3,581944444	0	3	34	55
	Totales	99,52%	0,48%	3,581944444	**0**	3	34	55



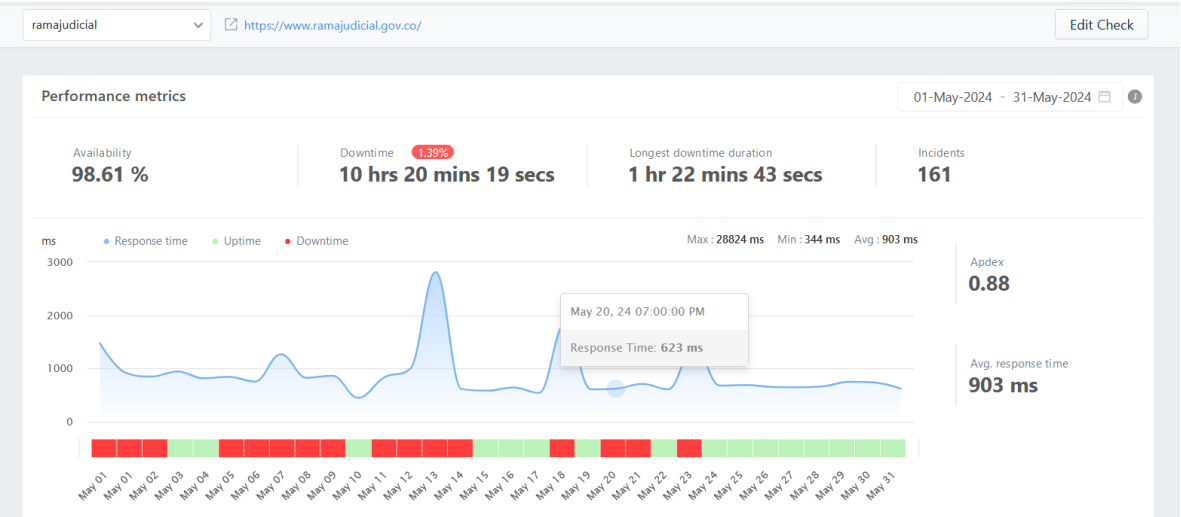
3.2 PORTAL DE LA RAMA JUDICIAL

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

Nota: para el mes de mayo 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

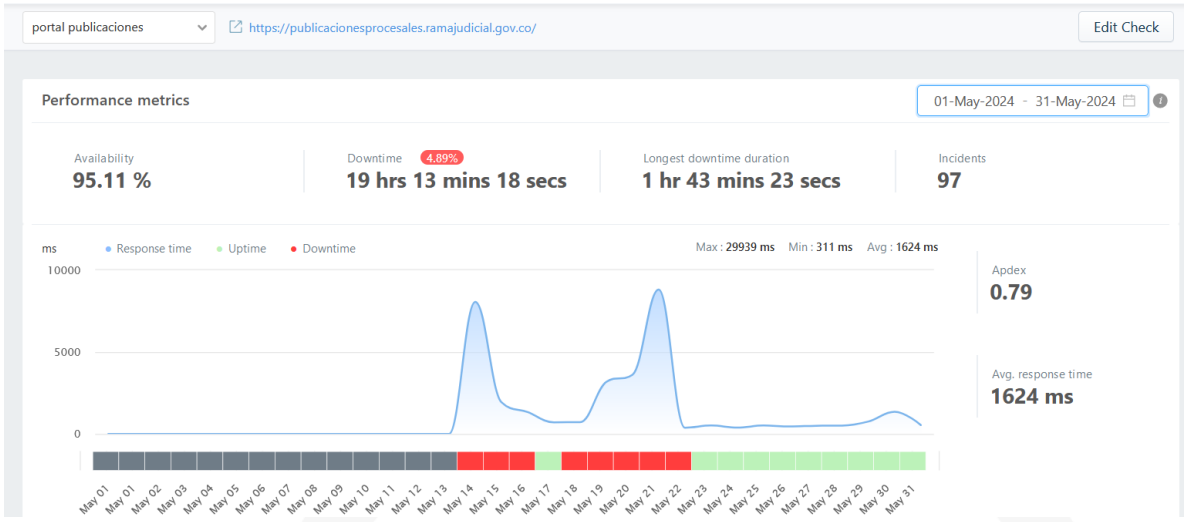
Portal Rama Judicial

Para el portal de la Rama Judicial del mes de mayo, se tienen los datos recopilados por el portal anterior Liferay 6.1 hasta la fecha 14 de mayo, posteriormente se encuentra recopilando los datos del portal Liferay 7.1 recientemente puesto en producción.



Portal Publicaciones Procesales

El monitor fue configurado a partir del 15 de mayo, posterior a la puesta en producción del portal publicaciones procesales



Portal Histórico Rama Judicial

El monitor fue configurado a partir del 15 de mayo, posterior a la puesta en producción del portal histórico

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

A través del presente drive https://drive.google.com/drive/folders/1Wuye3jPq_https://etbcsj.sharepoint.com/sites/DivisiondeSistemasdeinformacinyComunicaciones/Documentos%20compartidos/Forms/AllItems.aspx?ga=1&id=%2Fsites%2FDivisiondeSistemasdeinformacinyComunicaciones%2FDocumentos%20compartidos%2FGeneral%2FBackup%20%2D%20Gmail%20Contrato%20Portal%2FContrato%20Portal%20y%20Aplicaciones%20Conexas%2FAdicci%C3%B3n%20No%2E%203%20Contrato%20Portal%20Rama%20Judicial%2F2022%2F01012022%20al%2031072022%2F1%2E%20Casos%2FTT544033%20RV%20Certificaciones%20disponibilidad%20portal%20Rama%20Judicial%20a%C3%B1o%202022%2F00%2E%20A%C3%B1o%202024&viewid=a04a0a92%2D12c0%2D48b6%2D857d%2Dbad74c62a8ae certificaciones y están ubicadas las del mes de MAYO de acuerdo con que la rama judicial mediante la herramienta NOC solicita si se tiene alguna información adicional

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

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

ITEM	ACTIVIDAD	FECHA DE EJECUCION	TRABAJO REALIZADO (OPCIONAL)	AREA ENCARGADA
1				

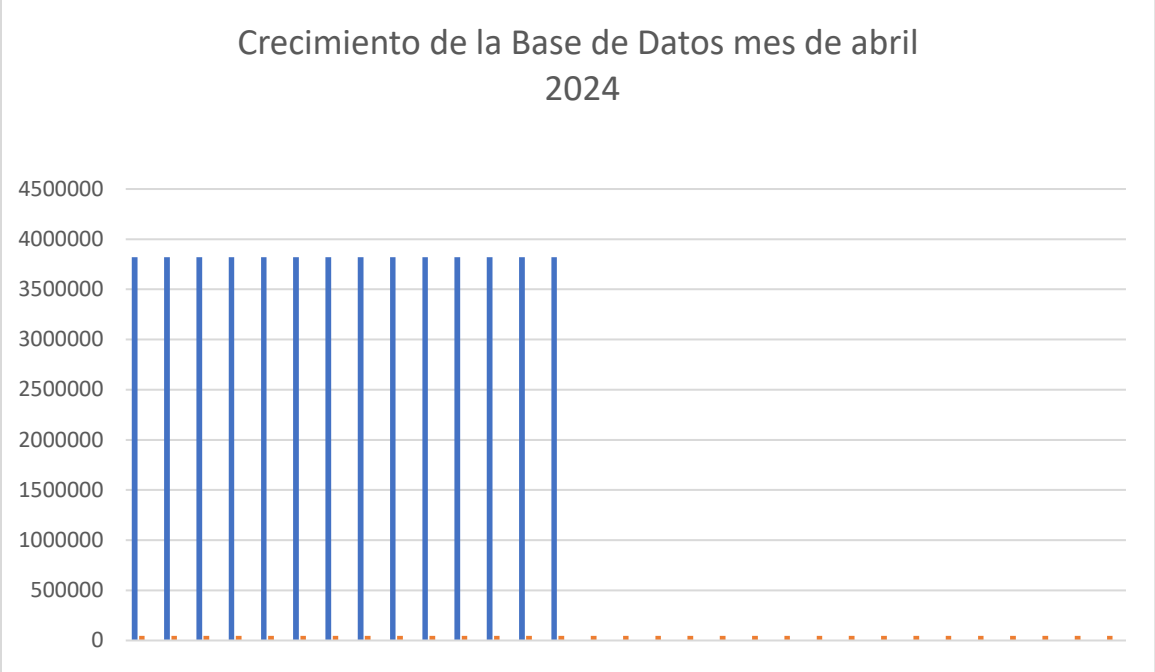
3.2.2 CRECIMIENTO DE LA BASE DE DATOS – INSTANCIA CSJPORTALDB01

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 mayo.

BASE DE DATOS lportalramaprod

TAMAÑO (MB0	FECHA	AUMENTO TAMAÑO (MB) POR DIA
3821324 MB	2024-05-01 00:00:00.547	0
3821324 MB	2024-05-02 00:00:01.120	0
3821324 MB	2024-05-03 00:00:00.370	0
3821324 MB	2024-05-04 00:00:00.573	0
3821324 MB	2024-05-05 00:00:00.507	0
3821324 MB	2024-05-06 00:00:00.570	0
3821324 MB	2024-05-07 00:00:00.663	0
3821324 MB	2024-05-08 00:00:00.713	0
3821324 MB	2024-05-09 00:00:00.657	0
3821324 MB	2024-05-10 00:00:01.003	0
3821324 MB	2024-05-11 00:00:00.753	0
3821324 MB	2024-05-12 00:00:01.077	0
3821324 MB	2024-05-13 00:00:00.263	0
3821324 MB	2024-05-14 00:00:00.563	0

Grafica del crecimiento de la BD Iportalramaprod de la INSTANCIA CSJPORTALB01



1. ESTADISTICAS PORTAL DE LA RAMA JUDICIAL

4.1 RESUMEN DEL PORTAL

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

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

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

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: FAD22FT221000028	10	32
11	2081818	npn04--IaaS Procesamiento -Balanceador de Carga AltaCapacidad - Oro - HostingNube Privada - SesionesCapa L4 (entre 36 y 100Millones) - RAM entre 64GB y128GB - U_Mes - Cantidad: 2	Balanceador DC Torre central	FORTI/BK	ADC-2200F	SN: FAD22FT221000027	9	32
30	2082020	npn04--IaaS Seguridad - Appliance Anti Ddos - AltaCapacidad - Oro - Hostingfísico - Rol de Inspección - 50Gbps - Paquetes PorSegundo	DDOS DC Torre central	FORTIDDOS FORTINET 2000E/PPLA	2000E	SN: FI2KETB20000015	31-32	32

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

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

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	10/05/2024 18:00	10/05/2024 22:00	4	Diurna	TT834251 RV: Replica controlador nube AWS; TT834261 RV: seguimiento a vocabulario controlado; TT834262 RV: seguimiento a vocabulario controlado CORECCION MARTES 14 DE MAYO A LAS 03 00 PM; TT834284 RV: registro dns relatoria cndj; TT834295 RV: Permisos de navegación Camilo Vargas | Ventana de mantenimiento - PASO A PRODUCCIÓN NUEVO PORTAL WEB
2	11/05/2024 12:00	11/05/2024 13:09	1	Diurna	TT834519 Urgente BK de VEEM de servidor | Ventana de mantenimiento - PASO A PRODUCCIÓN NUEVO PORTAL WEB
3	12/05/2024 13:57	12/05/2024 15:00	1	Dominical	Ventana de mantenimiento - PASO A PRODUCCIÓN NUEVO PORTAL WEB
4	13/05/2024 9:21	13/05/2024 22:09	13	Festiva Diurna	Ventana de mantenimiento - PASO A PRODUCCIÓN NUEVO PORTAL WEB
5	14/05/2024 7:00	14/05/2024 8:00	1	Diurna	Ventana de mantenimiento - PASO A PRODUCCIÓN NUEVO PORTAL WEB
6	14/05/2024 18:00	14/05/2024 22:00	4	Nocturna	TT835776 RV: [Alta] ID: 23729 - Varios inicios de sesión desde una misma IP en una ubicación poco habitual 189.203.181.34; TT835785 RV: [Alta] ID: 23520 - Varios inicios de sesión desde una misma IP en una ubicación poco habitual 208.115.224.165; TT835797 RV: Permisos de navegación Ingeniero Camilo; Sesión de soporte Ventana de mantenimiento - PASO A PRODUCCIÓN NUEVO PORTAL WEB
7	15/05/2024 18:00	15/05/2024 22:00	4	Diurna	TT836325 adicionar vpn para portal 7.1 | Ventana de mantenimiento - PASO A PRODUCCIÓN NUEVO PORTAL WEB
8	17/05/2024 18:00	15/05/2024 19:00	1	Diurna	Ventana de mantenimiento - PASO A PRODUCCIÓN NUEVO PORTAL WEB
9	31/05/2024 18:00	31/05/2024 19:00	1	Diurna	VENTANA MANTENIMIENTO SALIDA PRODUCCION CPNU AZURE
Total horas Extras			30		

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	3/05/2024 18:00	3/05/2024 22:30	4:30:00	Diurna/Nocturna	Migración Sigobius a Azure
2	4/05/2024 1:00	4/05/2024 2:00	1:00:00	Nocturna	Caida Puerto MPLS Cirion
3	4/05/2024 6:00	4/05/2024 12:30	6:30:00	Diurna	Apagado y Encendido Controlado de Equipos de Comunicaciones DataCenter Piso 10 CSJ
4	5/05/2024 4:00	5/05/2024 5:00	1:00:00	Nocturna/Dominical	Alerta caida WAF CAN - Problemas electricos cliente
5	5/05/2024 19:00	5/05/2024 23:00	4:00:00	Nocturna/Dominical	Casos TT831474 - TT831453 - Creacaion de politica-validacion WAF
6	5/08/2024 18:00	5/08/2024 19:00	1:00:00	Diurna	Validacion VPN SSL
7	25/5/2024 12:00:00	25/5/2024 14:00:00	2:00:00	Diurna	Migración VLAN 2000 a 2009 -ACTIVACION DE SERVICIOS - CSJ - CHOCÓ UNGUIA - DKO 8529929, 8529934 - Diego Mirquez
8	28/5/2024 19:00:00	28/5/2024 21:00:00	2:00:00	Diurna	TT843241 Revision Conexion VPN RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA
9					
10					
Total horas Extras			22:00:00		

Ingeniero Residente:	Camilo Calvo

Item	Fecha y Hora de inicio	Fecha y Hora de finalización	Cantidad de Horas	Tipo de Hora extra	Actividad Realizada
1	1/05/2024 9:00	1/05/2024 16:00	7	Nocturna/Dominical	Ventana de mantenimiento Portales
2	17/05/2024 18:00	15/05/2024 19:00	1	Diurna	TT837537 RV: Acompañamiento Migración Chocó TT837633 RV: Solicitud apertura YouTube eventos 20, 21, 23 y 24 de mayo TT837639 RV: Permisos de navegación Despacho Dr Chaverra
3	18/05/2024 22:00	19/05/2024 1:00	3	Nocturna	TT837611 RV: SOLICITUD ACOMPAÑAMIENTO Reinicio HUB's SDWAN MERAKI
4	20/05/2024 18:00	20/05/2024 19:00	1	Diurna	TT838645 RV: Acompañamiento migración RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA
5	21/05/2024 18:00	21/05/2024 19:00	1	Diurna	TT839238 RV: Migración Juradó RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA TT839288 RV: Migración Nuquí RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA
6	21/05/2024 19:00	21/05/2024 20:00	1	Diurna	TT839398 permisos VPN portal 7.1 RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA
7	22/05/2024 19:00	22/05/2024 20:00	1	Diurna	TT840070 permisos conectividad portal 7.1 RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA Permisos temporales de navegacion a la IP 10.1.2.156
Total horas Extras			15		

14.2. 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 Loadmast	WAF_CAN	TSCC82005629	2082015	CAN	7.2.59.3.22368

	er x25					
6	FortiDDos 2000E HA	CSJ_FDDoS_MASTER	FI-2KE5819000049	2082020	DC IFX	v6.3.3
		CSJ_FDDoS_SLAVE	FI-2KETB20000015	2082021	DC IFX	v6.3.3

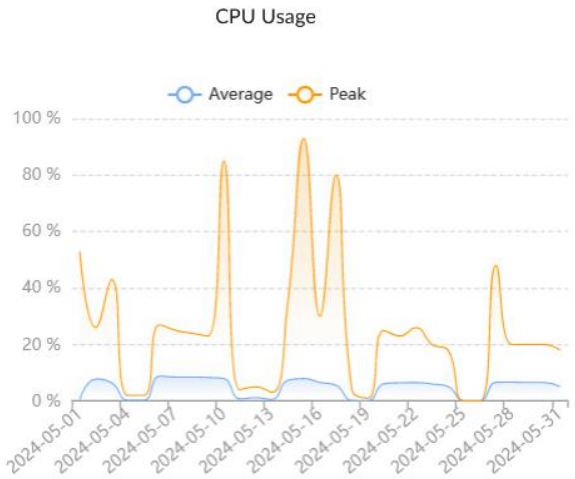
14.3. Actualización de firmware.

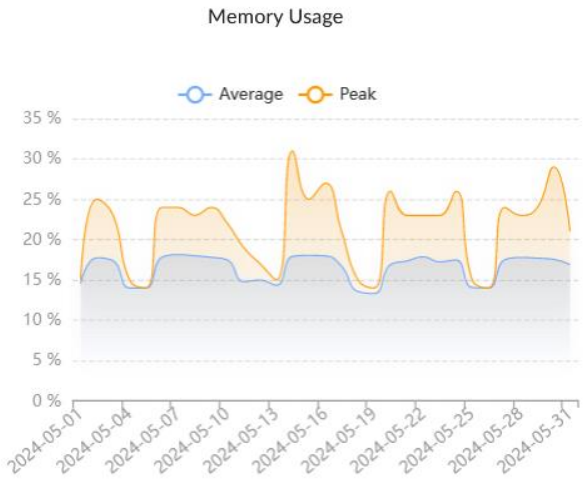
El plan de trabajo para la actualización del firmware será compartido, presentado y ejecutado con la autorización de los ingenieros Datacenter del CONSEJO SUPERIOR DE LA JUDICATURA.

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

14. FIREWALL PERIMETRAL

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

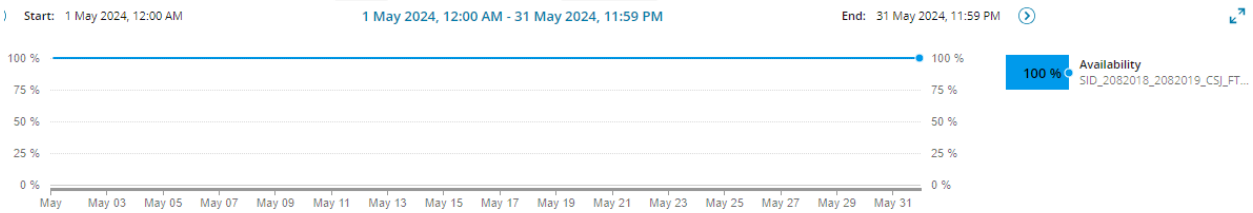




En la gráfica de rendimiento "CPU Usage", la curva color naranja muestra los picos de consumo de una o varias de las 160 CPUs del appliance FortiGate-4400F, cuando estos picos ocurren las tareas que los generan son desbordadas a las otras CPUs del appliance por lo que la curva color azul se muestra el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

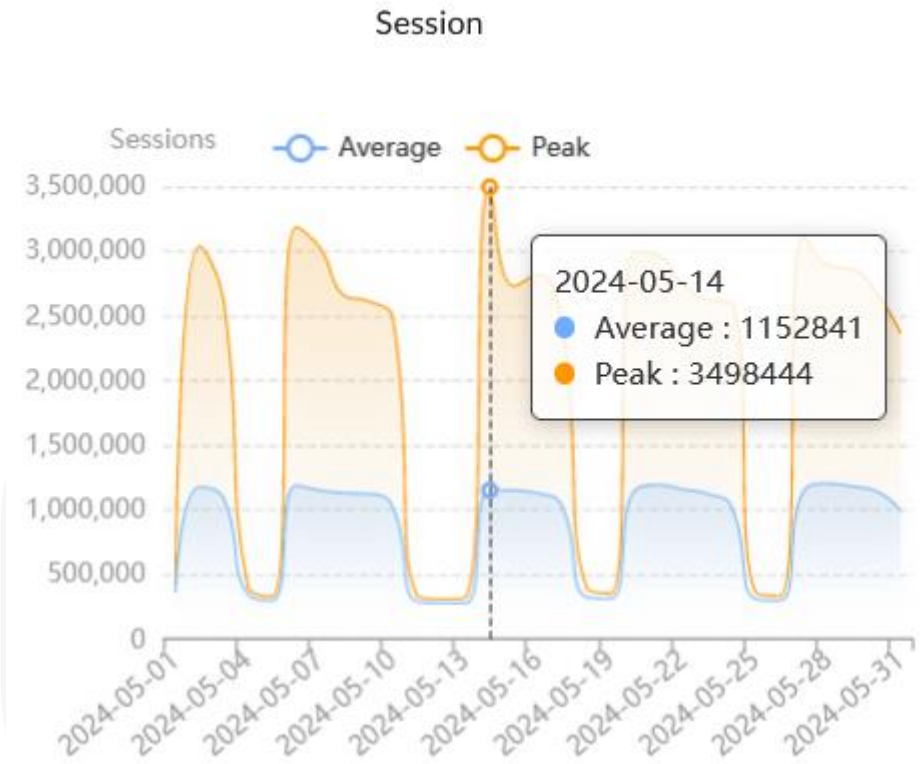
15.1. Disponibilidad mensual firewall perimetral.

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



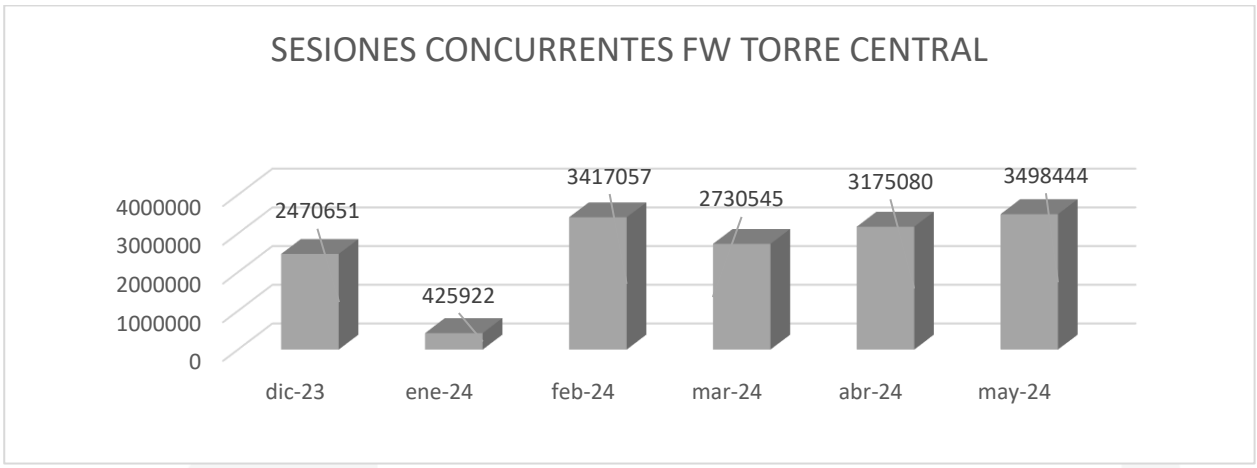
15.2. Cantidad de sesiones firewall perimetral.

Durante mayo se presentó un máximo de 3.498.444 sesiones TCP concurrentes, cantidad que se encuentra dentro del rango máximo soportado por el appliance Fortinet FG- 4400F cuyo valor es de 210 millones.



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

Durante mayo se presentó aumento en las sesiones en el FW perimetral correspondientes a 3’498.444 de sesiones:



MES	SESIONES
dic-23	2470651
ene-24	425922
feb-24	3417057
mar-24	2730545
abr-24	3175080
may-24	3498444

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

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

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	HTTPS			309.29 TB
2	SSL			121.39 TB
3	Microsoft.SharePoint			66.49 TB
4	SMB			35.60 TB
5	DTLS			28.24 TB
6	TCP/9443			24.87 TB
7	Akamai-CDN			24.10 TB
8	Microsoft.365.Portal			23.52 TB
9	Microsoft.Portal			22.40 TB
10	Google-Web			21.17 TB

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

Top Applications by Sessions

#	Application	Sessions
1	SMB	2,250,965,994
2	HTTPS	1,811,978,401
3	DNS	1,412,692,402
4	SSL	640,456,336
5	Microsoft.Windows.Update	619,007,679
6	Microsoft.Portal	482,768,675
7	Microsoft.365.Portal	468,913,621
8	TCP/448	435,507,647
9	Akamai-CDN	399,379,578
10	Google-Web	389,021,145

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

8.243.164.19 (CTL Colombia), microsoft.com, 190.217.24.69 (sede Palacio) y 8.243.164.21 (CTL Colombia) presentaron la mayor cantidad de consumo de ancho de banda durante mayo:

Top Bandwidth IP

#	Hostname(or IP)	Sessions
1	8.243.164.19	455,164,407
2	microsoft.com	261,637,008
3	190.217.24.69	255,730,918
4	8.243.164.21	246,315,640
5	172.28.107.71	206,367,343
6	windowsupdate.com	200,684,446
7	spotify.com	139,409,546
8	8.243.200.3	116,550,919
9	172.28.146.154	112,002,068
10	172.28.107.58	104,963,822

15.6. Top de destinos web por sesiones firewall perimetral.

Los destinos en Internet con mayor cantidad de sesiones durante mayo fueron 8.243.164.19 (rns1co.cirion.live), 190.217.24.69 (IP pública de la sede Palacio), 8.243.164.21 (rns1co.cirion.live), 35.186.224.25 (Google LLC) y 8.243.200.3 (CTL LATAM= Cirion).

Top Destination by Sessions

#	Destination	Sessions
1	8.243.164.19	394703287
2	190.217.24.69	226796485
3	8.243.164.21	210612087
4	35.186.224.25	144256338
5	8.243.200.3	112182610
6	10.1.2.21	96278045
7	10.1.2.22	94068690
8	190.217.24.172	82588617
9	172.28.146.154	79237083
10	8.8.8.8	78621974

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

172.16.33.29 (host de Cundinamarca, Bogota; Edificio Nemqueteba) y 172.16.56.165 (Valle, Cali; Entreceibas) presentaron la mayor cantidad de peticiones bloqueadas durante mayo:

Top Web Users by Blocked Requests

#	User (or IP)	Hostname	Requests
1	172.16.33.29	172.16.33.29	22,720,370
2	172.16.56.165	172.16.56.165	10,694,309
3	172.27.91.49	172.27.91.49	7,317,079
4	192.168.46.197	192.168.46.197	3,601,286
5	192.168.140.20	192.168.140.20	3,254,050
6	192.168.34.220	192.168.34.220	2,950,337
7	192.168.125.26	192.168.125.26	2,841,814
8	192.168.66.79	192.168.66.79	2,828,823
9	172.25.57.147	172.25.57.147	2,676,463
10	172.29.6.18	172.29.6.18	2,653,181

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

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

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

Top Blocked Web Categories

#	Category	Requests
1	Internet Radio and TV	150,371,388
2	Proxy Avoidance	8,317,077
3	Streaming Media and Download	8,043,110
4	Social Networking	3,712,582
5	Games	3,403,123
6	Unrated	1,541,195
7	Information Technology	1,204,966
8	Malicious Websites	413,088
9	Entertainment	309,249
10	Society and Lifestyles	282,567

15.9. Top de IP más activos Firewall Perimetral

Los hosts con mayor cantidad de peticiones durante mayo 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	14,951,214
2	10.101.100.38	9,658,191
3	10.101.100.194	9,459,023
4	10.101.100.34	8,968,791
5	10.101.100.122	6,385,841
6	10.101.100.134	5,457,147
7	10.101.100.170	5,287,343
8	10.101.100.70	5,013,552
9	10.101.100.138	4,669,067
10	10.101.101.246	4,130,971

15.10. Top de categorías más visitadas Firewall Perimetral

La categoría más visitada durante mayo fue Information Technology:

Top Allowed Web Categories

#	catdesc	requests
1	Information Technology	451562683
2	Overrride_permitidas	703306
3	Unrated	2

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

El WAF del Datacenter CAN 172.17.201.252 y la aplicación 172.31.10.41 (Árbol tutela Justicia_XXI_DB) en IFX presentaron consumieron la mayor cantidad de ancho de banda durante mayo:

Top IP by Bandwidth

#	IP	Bandwidth	Sent	Received
1	172.17.201.252			94.75 TB
2	172.31.10.41			90.02 TB
3	172.17.201.251			32.84 TB
4	172.27.64.17			31.68 TB
5	10.244.2.239			17.45 TB
6	172.28.146.83			16.58 TB
7	172.27.64.61			15.83 TB
8	172.28.108.48			12.02 TB
9	172.28.108.51			10.66 TB
10	erubianr			8.88 TB

15. TRÁFICO VPN FIREWALL PERIMETRAL

El top 10 de los usuarios conectados a la VPN SSL durante mayo 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	2024-06-01 00:01:15	186.28.44.62;186.31.186.194	294	708:35:13	17.42 GB	3698633577	15005726702
2	cvillam	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-05-31 23:53:29	181.55.51.20	76	479:55:56	5.54 GB	600576176	5352391117
3	jariasu	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-05-31 23:58:35	181.137.8.129	63	356:55:37	1.70 GB	185962014	1641444436
4	froaga	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-05-31 23:44:43	12.219.56.114;181.59.148.142;181.59.3.152;181.59.3.252;186.28.62.72;186.29.217.213;190.27.128.224	73	334:26:15	63.36 GB	27503087701	40531020717
5	pfajardg	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-06-01 00:01:41	186.81.100.20	108	333:19:06	20.78 GB	1089746642	21227069645
6	lbarrerf	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-05-31 22:46:40	191.156.51.94;191.156.53.249;201.244.129.88;201.244.161.87	62	315:27:46	35.99 GB	1826750354	36821215887
7	Fcaldert	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-05-31 23:29:21	186.31.144.110;186.31.144.128;186.31.147.29;186.31.147.88;186.31.148.148;186.31.148.151;186.31.148.46;186.31.148.61;186.31.148.8;186.31.152.182;186.31.152.251;186.31.153.146;186.31.153.161;186.31.153.177;186.31.153.18;186.31.153.211;186.31.153.74;186.31.153.84;186.31.208.230;186.31.210.26;186.31.213.42;186.31.215.147;186.31.216.244;186.31.216.32;186.31.217.89;186.31.218.94;186.31.219.228;191.108.140.23;191.108.141.68;191.108.150.79;191.108.169.48;191.108.188.0;191.108.191.101;191.108.200.223;191.108.203.139;191.108.205.50;191.156.251.190	205	293:07:17	2.55 GB	161066051 8	1125084711

8	jmartinm	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-05-31 15:25:24	186.121.28.199;186.121.43.86;186.121.7.176;186.121.8.122;200.118.220.133	129	288:48:47	21.06 GB	1608303483	2100747018 6
9	LPineroSe	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-05-31 23:48:25	45.238.181.215;45.238.181.252;45.238.182.131;45.238.182.2;45.238.182.25;45.238.182.54;45.238.182.62;45.238.183.70;45.238.183.79	59	285:45:53	52.50 GB	1635180556	5473659117 7
10	omunozch	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-05-31 18:51:07	152.204.239.180;152.204.249.195;152.204.254.253;181.235.159.142;181.235.168.6;181.235.181.205;181.235.202.27;181.235.218.54	60	284:34:23	6.82 GB	2670146967	4649637529

16.1. VPN IPSEC Site To Site Firewall Perimetral

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

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

#	vpnname	remip	locip	Duration	bandwidth	traffic_in	traffic_out
1	VPN_AZURE	52.240.53.161	190.217.24.4	2677803	31691048782154	2949146521355	28741902260799
2	VPN_AZURE-VWAN2	4.153.117.131	190.217.24.4	2676102	291271959336	27008970734	264262988602
3	VPN_ORACLE	129.213.6.36	190.217.80.4	2677803	216847364328	185292217645	31555146683
4	VPN_AZURE-ANALY	20.124.34.235	190.217.24.4	2677803	160508038740	7916480163	152591558577
5	VPN_Tierras	181.225.76.196	190.217.24.4	2677798	54873134231	53223403701	1649730530
6	VPN_SIUG_AWS	34.194.187.190	190.217.24.4	2677710	8432829677	2495716347	5937113330
7	VPN_SIUG_AWS-2	34.224.152.152	190.217.24.4	2677704	4402273825	1963944336	2438329489
8	VPN_AZURE-VWAN	4.153.117.133	190.217.24.4	2676036	984727187	984502158	225029
9	VPN_REGISTRADU	201.232.123.20	190.217.24.4	2677803	906141521	482350175	423791346
10	VPN_Linktic	3.222.171.115	190.217.24.4	2677786	751159834	456705988	294453846
11	VPN_INPEC	190.25.112.10	190.217.19.156	2677798	694481750	581778067	112703683
12	OCI_EXADATA_FAB	150.136.25.96	190.217.24.4	2677709	76161072	0	76161072
13	VPN_FISCALIA	190.157.218.66	190.217.24.4	2677803	46633424	44565920	2067504

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

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

Top Attacks

#	Attack Name	Severity	CVE-ID	Counts
1	tcp_syn_flood	Critical		525,253
2	tcp_src_session	Critical		467,029
3	tcp_port_scan	Critical		196,943
4	Tofsee	Critical		32,736
5	Apache.Log4j.Error.Log.Remote.Code.Execution	Critical	CVE-2021-4104,CVE-2021-44228,CVE-2021-45046	6,016
6	tcp_dst_session	Critical		4,402
7	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	Critical	CVE-2017-9841	4,225
8	Andromeda.Botnet	Critical		3,764
9	Amadey.Botnet	Critical		3,088
10	Andromeda	Critical		1,256

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

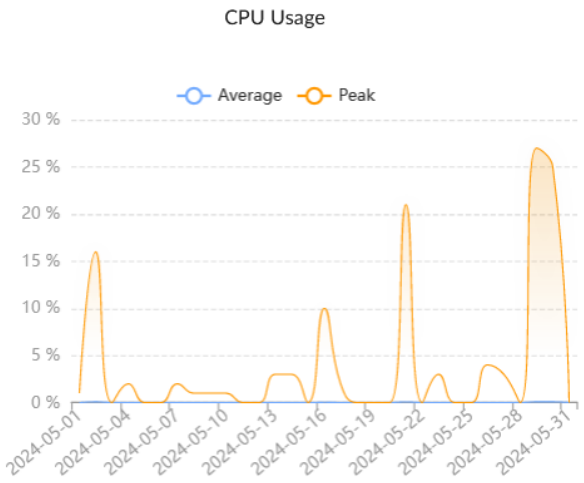
Top 20 Intrusion Victims

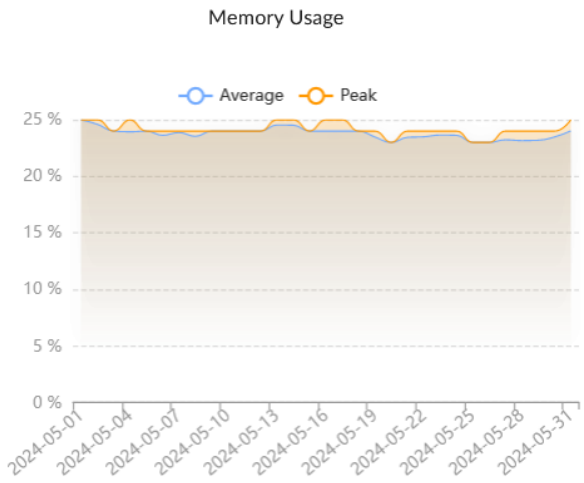
#	Attack Victim	Counts (Critical / High / Medium)	Percent of Total Attacks
1	190.217.24.172	326,618	21.36%
2	190.217.24.69	319,911	20.93%
3	172.17.201.68	231,613	15.15%
4	172.17.201.26	204,516	13.38%
5	172.17.201.13	143,764	9.40%
6	172.17.201.52	90,761	5.94%
7	190.217.24.176	44,508	2.91%
8	172.17.201.25	33,105	2.17%
9	190.217.24.149	31,154	2.04%
10	93.95.230.126	23,000	1.50%
11	172.17.201.101	12,348	0.81%
12	34.16.47.102	11,443	0.75%
13	172.111.159.74	8,681	0.57%
14	176.113.115.84	8,580	0.56%
15	176.113.115.135	8,578	0.56%
16	34.29.85.190	8,272	0.54%
17	80.66.75.11	6,238	0.41%
18	45.74.46.61	6,029	0.39%
19	45.74.46.83	5,377	0.35%
20	172.17.201.45	4,326	0.28%

Los hosts 190.217.24.172, 190.217.24.69 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.

16. FIREWALL SEDE PALACIO

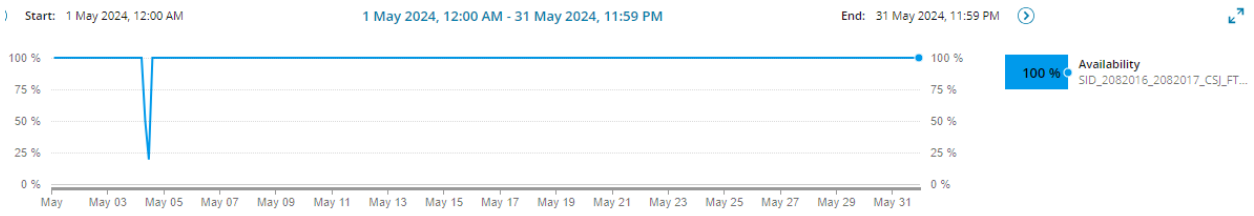
Durante mayo, el consumo de CPU y memoria en el Firewall de Palacio se mantuvo dentro de sus valores de operación normal.





16.1 Disponibilidad Mensual Firewall Palacio

Durante mayo 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%.

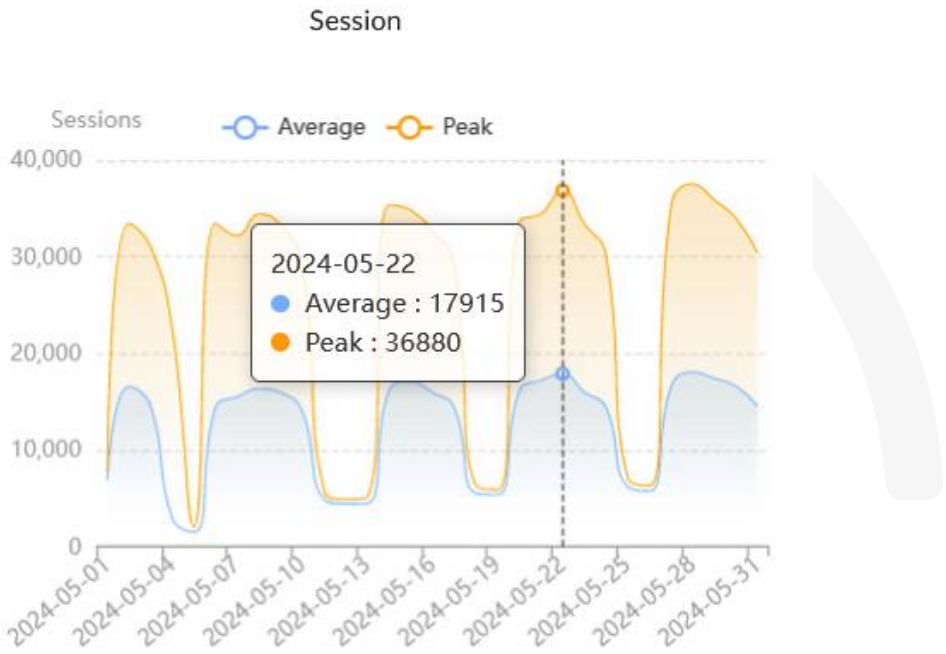
Nota: El evento del sábado 4 de mayo en la mañana se debe a las incidencias con imputabilidad a cliente CSJ "Caída Puerto MPLS Cirion" y "Apagado y Encendido Controlado de Equipos de Comunicaciones Datacenter Piso 10 CSJ". Debido a este evento, la medición de disponibilidad sin redondear para alcanzar el appliance desde la herramienta de monitoreo es del 99.444% imputable a cliente:

Availability Statistics

PERIOD	AVAILABILITY
Today	100.000 %
Yesterday	100.000 %
Last 7 Days	100.000 %
Last 30 Days	100.000 %
This Month	100.000 %
Last Month	99.444 %

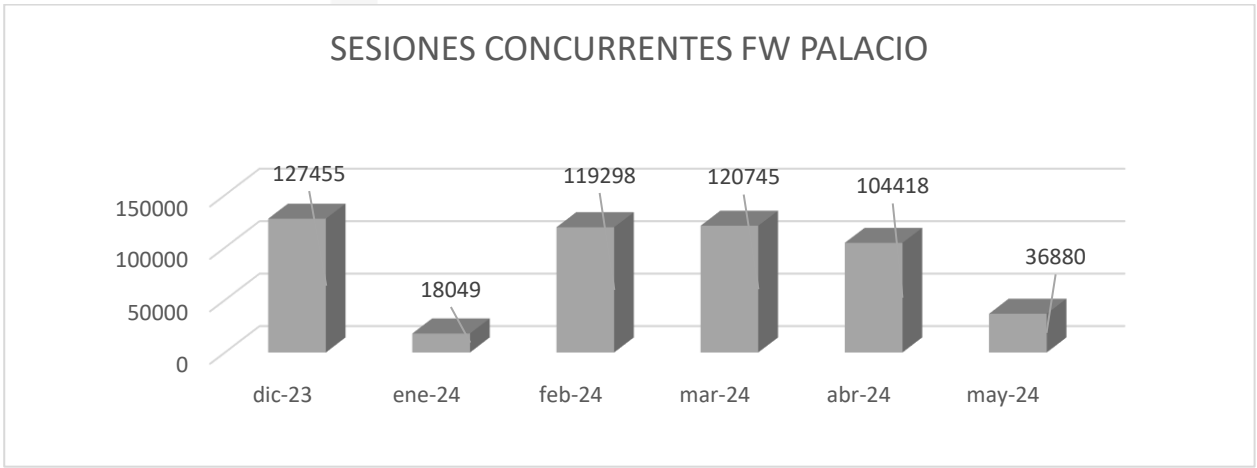
16.2 Cantidad de Sesiones Firewall Palacio

Durante mayo se presentó un máximo de 36.880 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 reducción en la cantidad de las sesiones del firewall de Palacio:



MES	SESIONES
dic-23	127455
ene-24	18049
feb-24	119298
mar-24	120745
abr-24	104418
may-24	36880

16.4 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 mayo:

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	Microsoft.Portal			11.73 TB
2	HTTPS			10.36 TB
3	Microsoft.SharePoint			6.79 TB
4	OneDrive			4.19 TB
5	SSL			3.28 TB
6	HTTPS.BROWSER			2.96 TB
7	SMB			2.89 TB
8	MS-SQL			2.11 TB
9	HTTP			1.73 TB
10	Akamai-CDN			1.47 TB

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

Top Applications by Sessions

#	Application	Sessions
1	SMB	771,540,365
2	DNS	274,299,163
3	HTTP.BROWSER	48,832,321
4	Microsoft.Windows.Update	46,211,175
5	HTTPS	41,806,729
6	HTTP	38,529,782
7	TCP-3000	37,001,577
8	Microsoft.365.Portal	33,266,517
9	SQUID	33,031,200
10	Microsoft.Portal	31,778,529

16.5 Top de IP por ancho de banda firewall Palacio.

172.28.93.2 (host de la Comisión Nacional de Disciplina Judicial) consumió la mayor cantidad de ancho de banda durante mayo:

Top Bandwidth IP

#	IP	Bandwidth
1	172.28.93.2	6.08 TB
2	172.16.4.184	1,019.30 GB
3	172.28.92.15	810.87 GB
4	172.28.92.23	670.83 GB
5	172.16.2.59	637.50 GB
6	172.16.5.33	615.51 GB
7	172.16.4.186	407.56 GB
8	172.28.92.34	403.44 GB
9	172.16.5.17	384.30 GB
10	172.17.114.139	375.74 GB

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

20.60.0.104, 13.107.138.10 y 13.107.136.10, todas en Microsoft Corporation, fueron destinos más visitados durante mayo:

Top Websites and Category by Bandwidth

#	Site	Category	Bytes
1	20.60.0.104		5.76 TB
2	13.107.138.10		4.34 TB
3	13.107.136.10		4.05 TB
4	172.190.220.253		1.25 TB
5	52.104.3.39		1.14 TB
6	52.239.171.228		750.02 GB
7	20.209.52.65		668.91 GB
8	20.60.128.228		605.50 GB
9	20.168.235.216		601.27 GB
10	20.209.74.225		530.67 GB

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

172.16.5.243 (host de la LAN Palacio), 172.28.93.142 (host de la Comisión Nacional de Disciplina Judicial) y 172.29.136.22 (host de la RED WIFI CISCO Palacio de Justicia de Bogotá Comisión Nacional de Disciplina Judicial) presentan la mayor cantidad de conexiones bloqueadas durante mayo.

Top Web Users by Blocked Requests

#	User (or IP)	Hostname	Requests
1	172.16.5.243	172.16.5.243	205,023
2	172.28.93.142	172.28.93.142	174,513
3	172.29.136.22	172.29.136.22	105,716
4	172.16.4.182	172.16.4.182	74,044
5	192.168.8.25	192.168.8.25	70,888
6	172.29.136.73	172.29.136.73	68,627
7	172.16.5.57	172.16.5.57	67,582
8	172.16.4.227	172.16.4.227	63,130
9	172.16.5.40	172.16.5.40	39,341
10	172.29.136.91	172.29.136.91	31,840

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.

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

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

Top Blocked Web Categories

#	Category	Requests
1	Unrated	1,572,566
2	Streaming Media and Download	987,513
3	Social Networking	854,412
4	Proxy Avoidance	613,778
5	Games	93,464
6	Society and Lifestyles	31,356
7	Entertainment	28,144
8	Phishing	7,988
9	Newsgroups and Message Boards	5,869
10	Remote Access	5,510

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 mayo:

Top Web IP by Allowed Requests

#	IP	Requests
1	172.16.4.90	23,713,114
2	172.28.54.20	18,232,605
3	172.28.93.87	1,201,977
4	192.168.6.66	518,023
5	192.168.2.16	466,147
6	172.16.4.67	444,796
7	172.28.93.101	435,892
8	172.16.2.99	414,329
9	192.168.8.25	399,831
10	172.16.2.230	386,548

16.10 Top de las categorías más visitadas firewall Palacio.

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

Top Allowed Web Categories

#	Category	Requests
1	Information Technology	32,072,300
2	Search Engines and Portals	6,643,343
3	Business	1,750,230
4	Information and Computer Security	545,299
5	Web Analytics	505,538
6	Web-based Applications	171,262
7	Finance and Banking	87,653
8	Online Meeting	77,111
9	Overrride_permitidas	61,242
10	Government and Legal Organizations	30,098

16.11 Top de consumo ancho de banda por usuario Firewall Palacio

172.17.201.252 (WAF del Datacenter CAN) y 172.28.93.2 (host de la Comisión Nacional de Disciplina Judicial) presentaron la mayor cantidad de conexiones durante mayo:

Top IP by Bandwidth

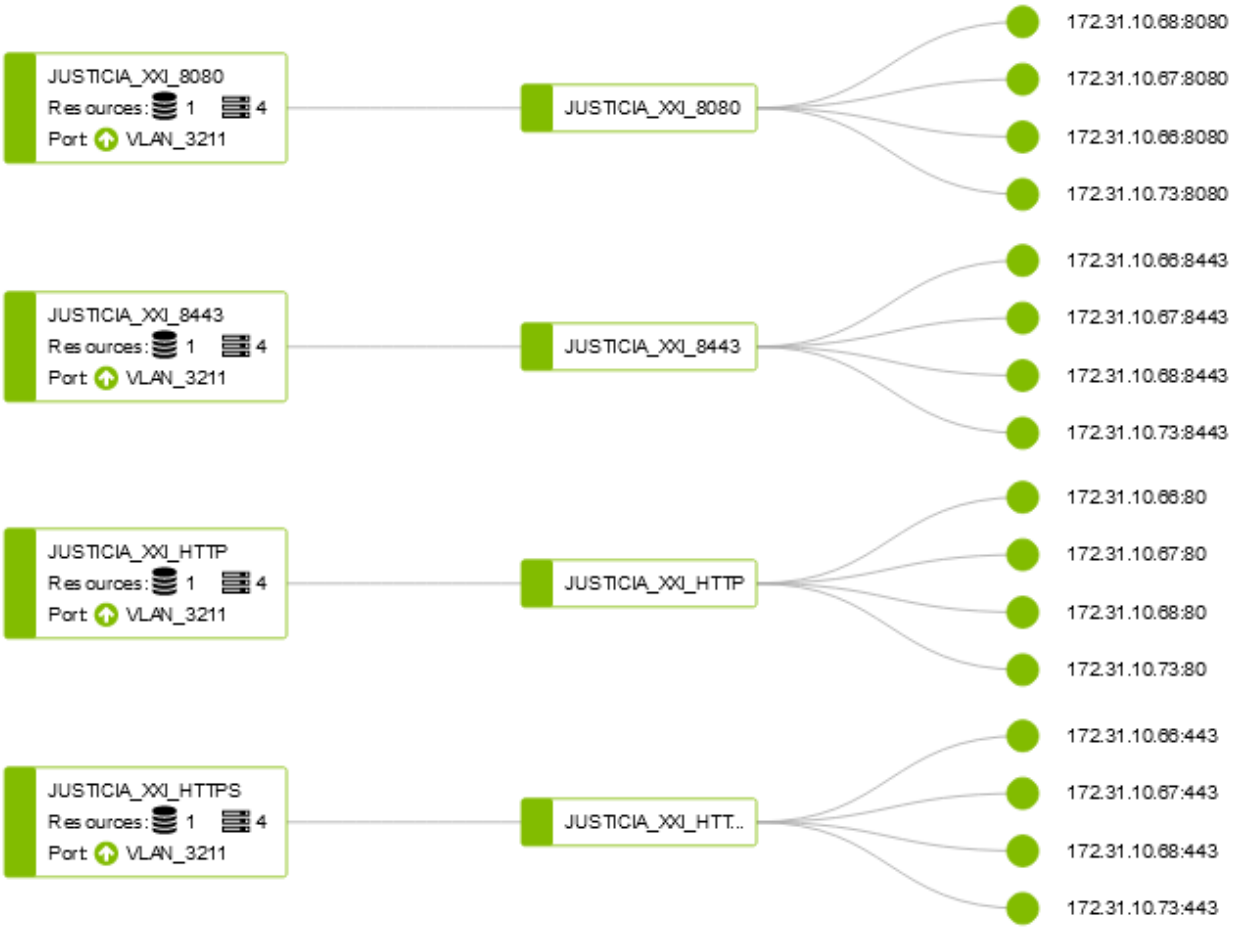
#	IP	Bandwidth	Sent / Received
1	172.17.201.252		6.17 TB
2	172.28.93.2		6.12 TB
3	10.101.250.4		2.45 TB
4	172.29.154.58		2.39 TB
5	172.17.201.251		2.21 TB
6	172.17.202.250		1.66 TB
7	172.16.4.121		1.66 TB
8	172.16.4.184		1.00 TB
9	172.16.4.186		965.38 GB
10	172.28.92.15		885.53 GB

17. BALANCEADOR DE CARGA FORTIADC

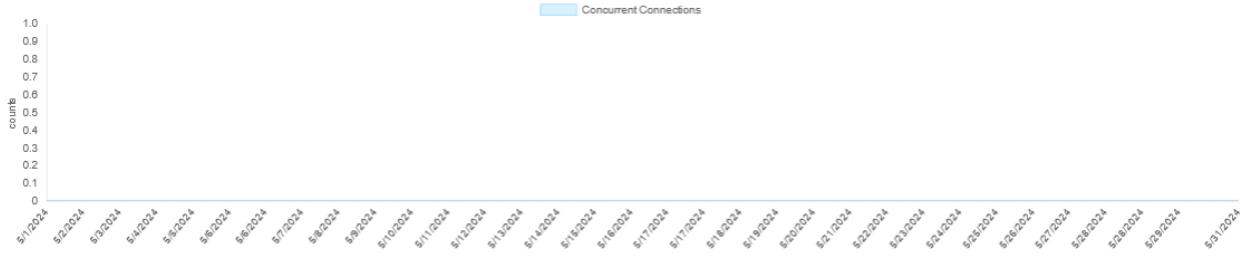
A continuación, se observan los diferentes servicios balanceados.

17.1 Justicia XXI

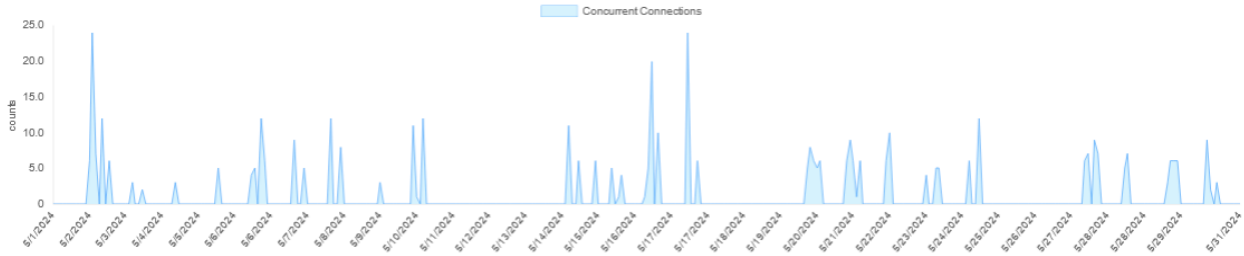
Se encuentra balanceado en el FortiADC:



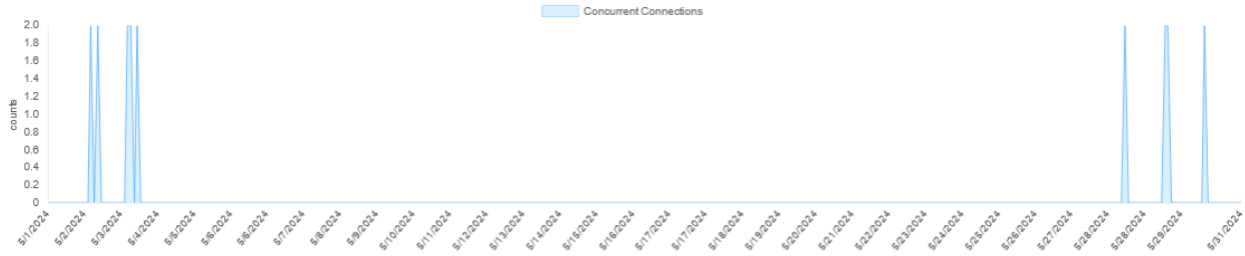
Durante mayo no se presentó tráfico por el puerto 8080:



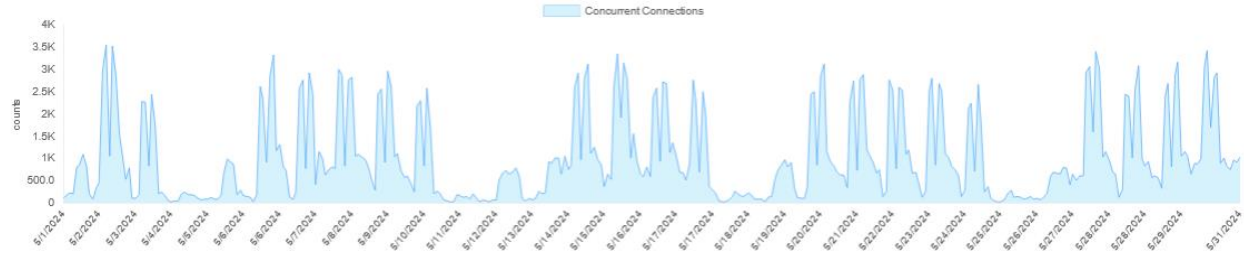
Conexiones concurrentes por el puerto 8443:



Conexiones concurrentes por el puerto 80:



Conexiones concurrentes por el puerto 443:

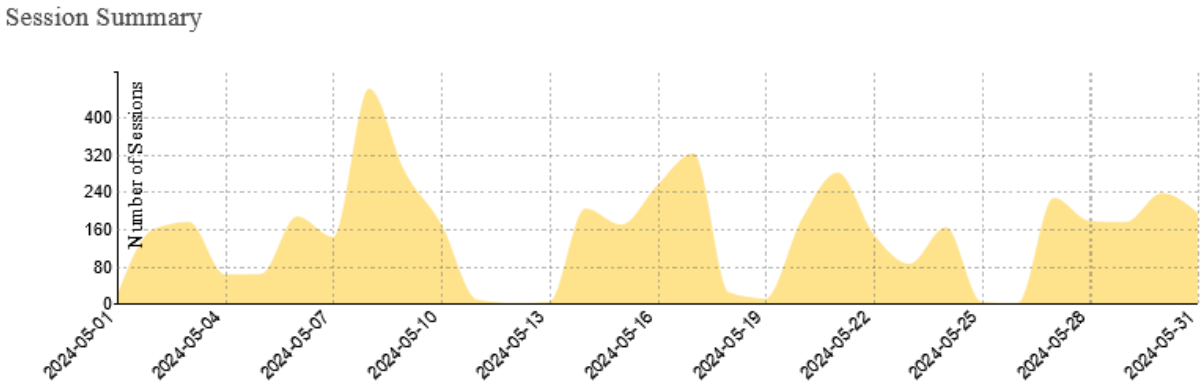


17.2 Kactus RDP

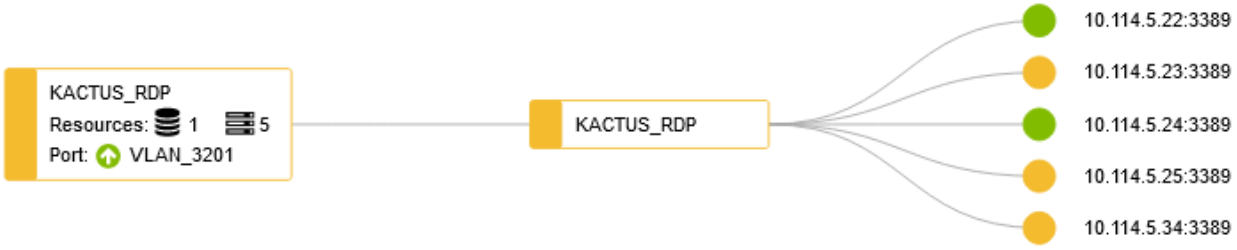
Esta aplicación se encuentra en el Firewall utilizando la siguiente configuración:

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

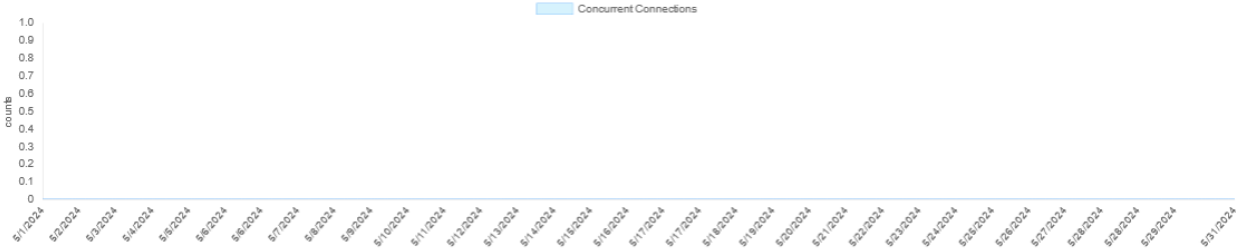
A continuación, se observa el número de sesiones concurrentes para este aplicativo.



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

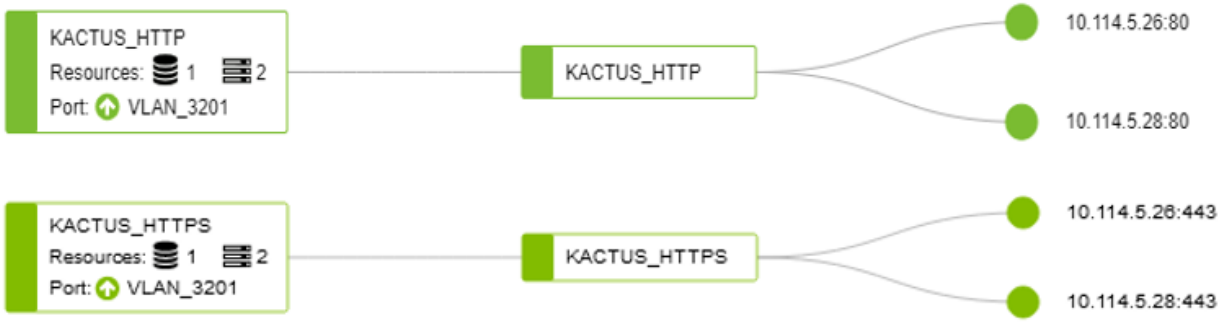


En el FortiADC no se observan sesiones concurrentes:

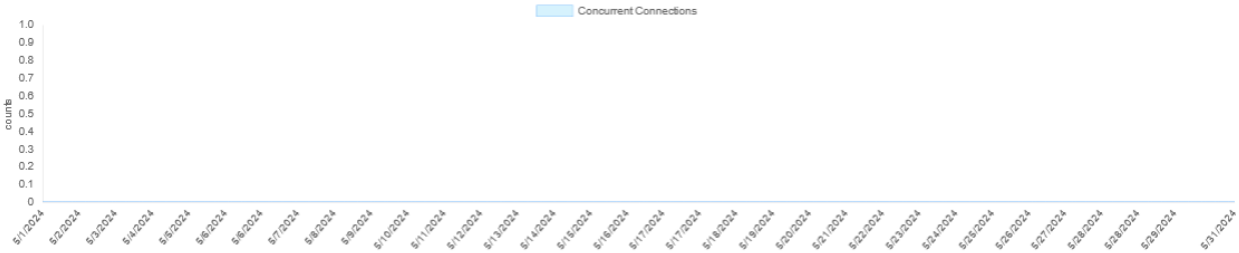


17.3 Kactus WEB

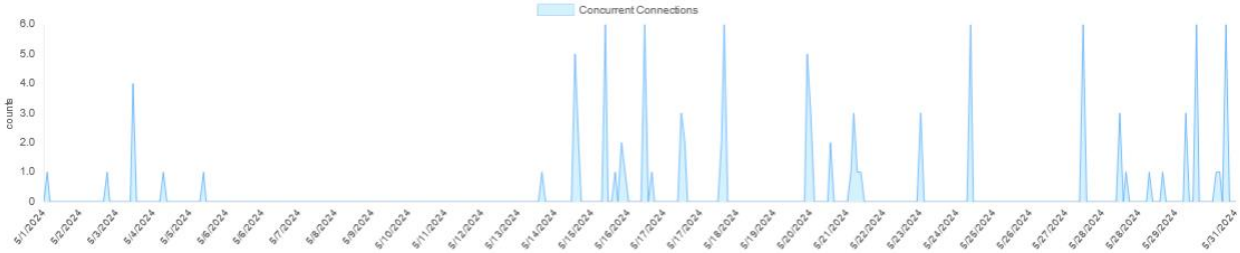
Se encuentra balanceado en el FortiADC:



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



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



17.4 SIRNA

Este servicio se encuentra balanceado en el Fortigate perimetral:

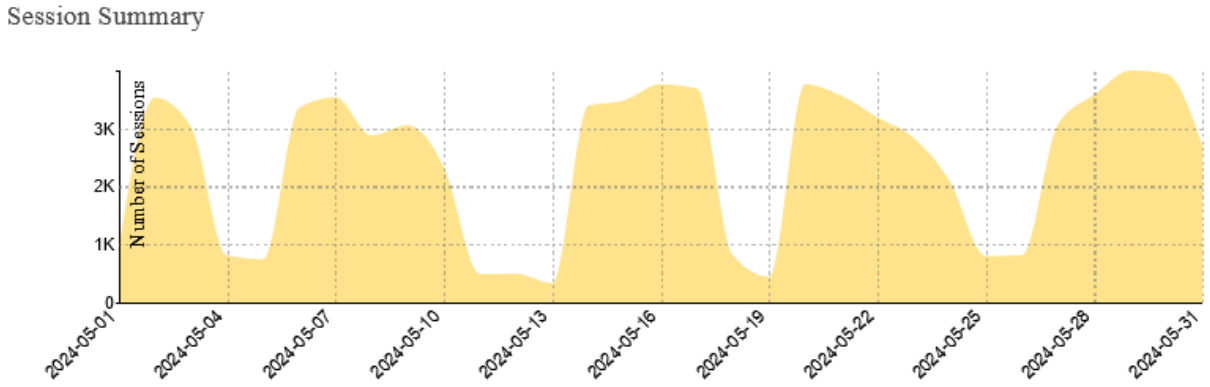
Configuración de balanceo de CRM en el Firewall.

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

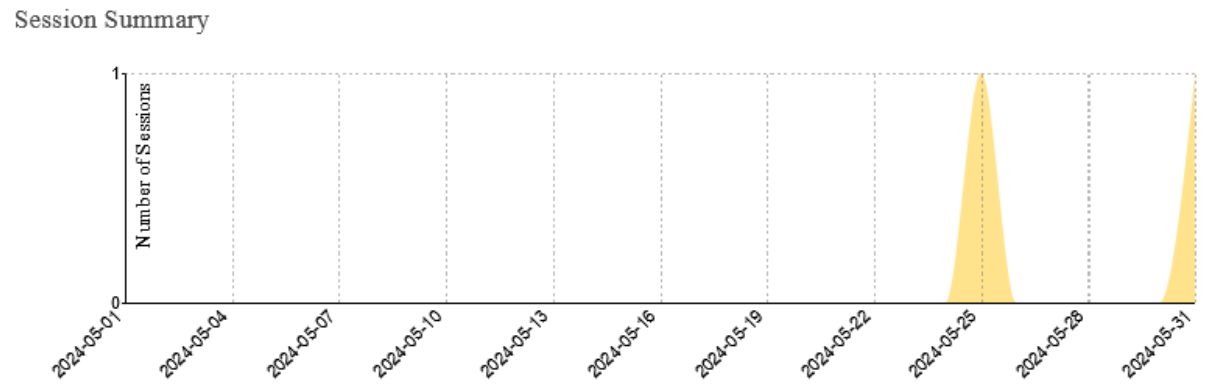
Configuración de balanceo de Sharepoint en el firewall perimetral.

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

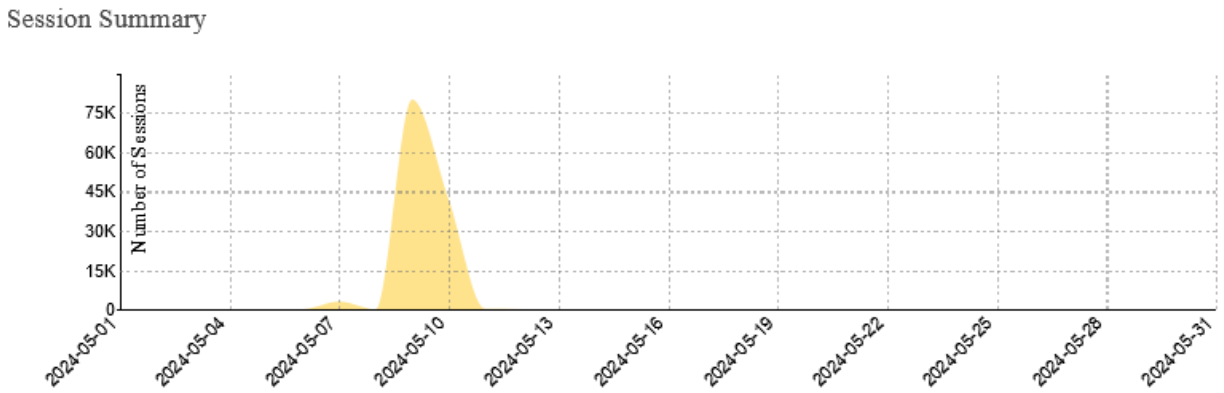
Las sesiones en el firewall para SIRNA 4443 fueron:



Las sesiones en el firewall para CRM 443 fueron:



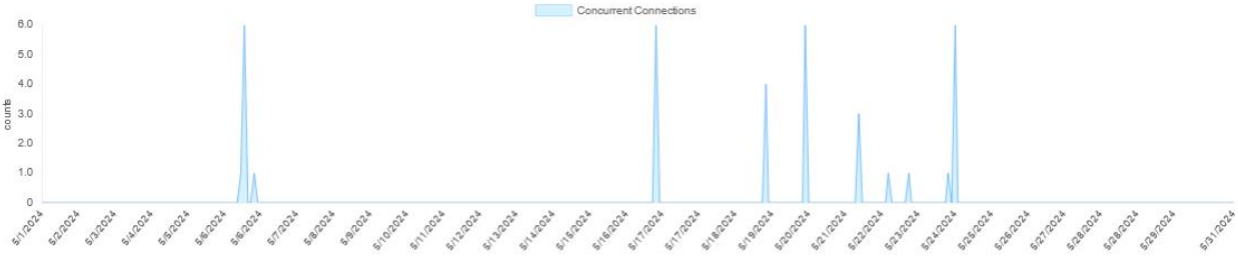
Las sesiones en el firewall para Sharepoint 444 fueron:



17.5 Convocatoria Peritos.

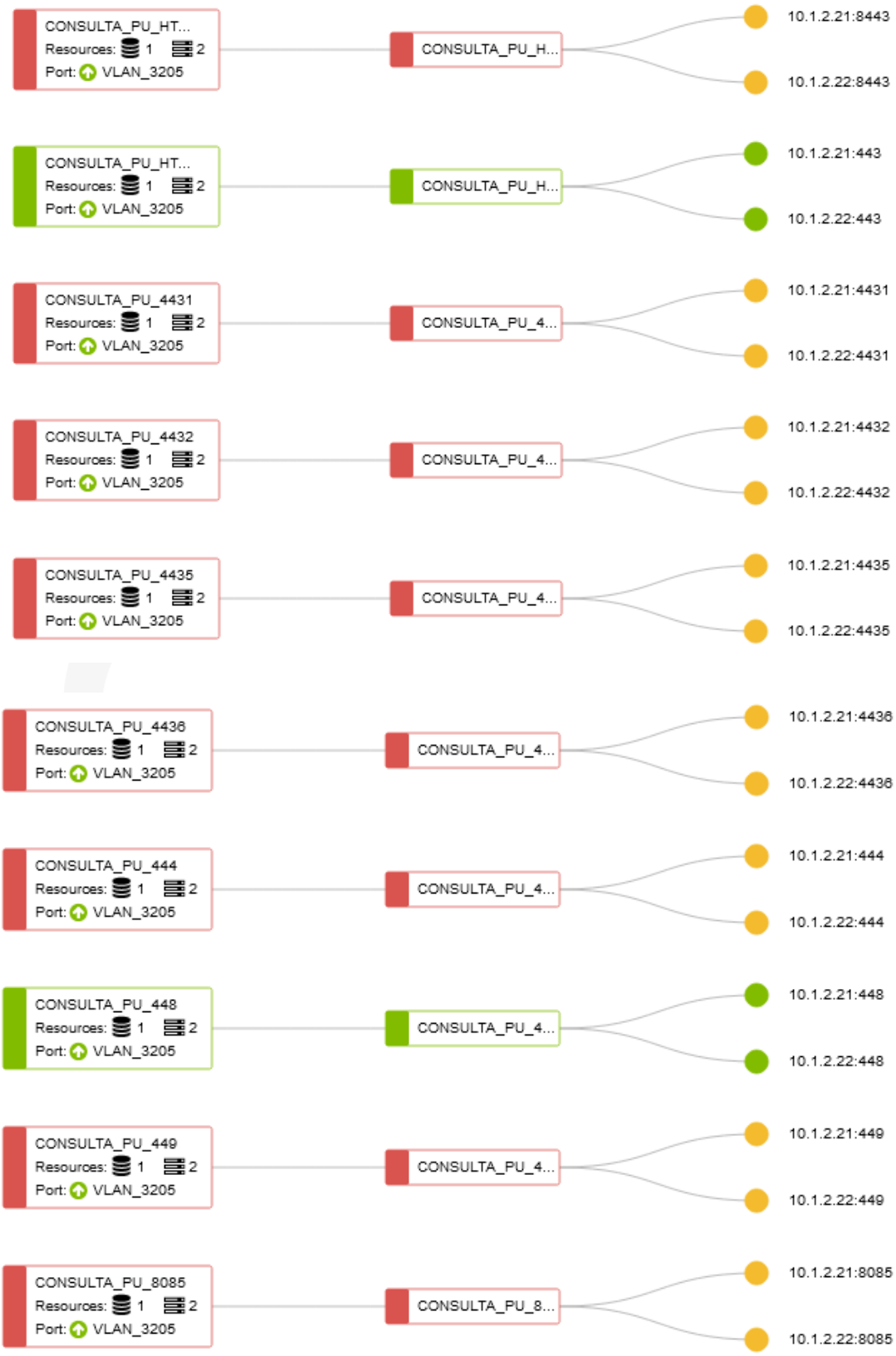
Este servicio se encuentra balanceado en el FortiADC:

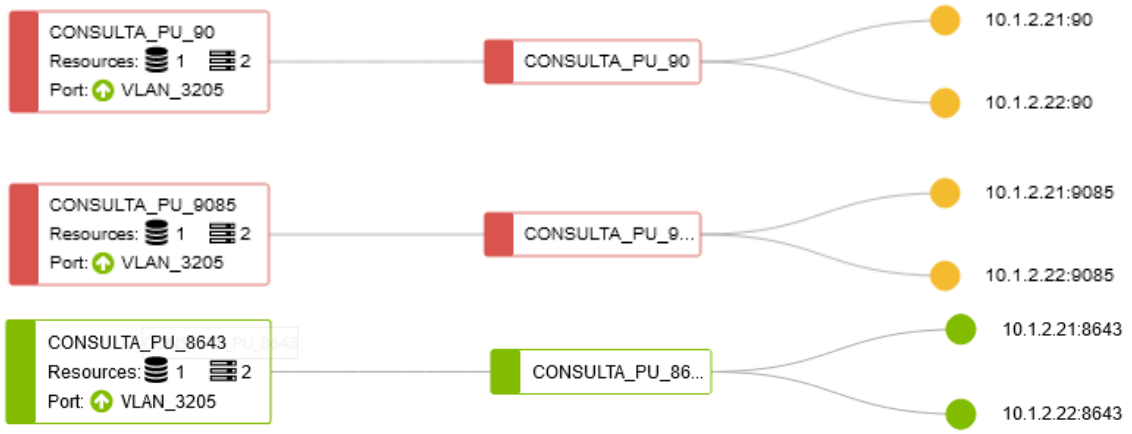
Las sesiones concurrentes fueron las siguientes:



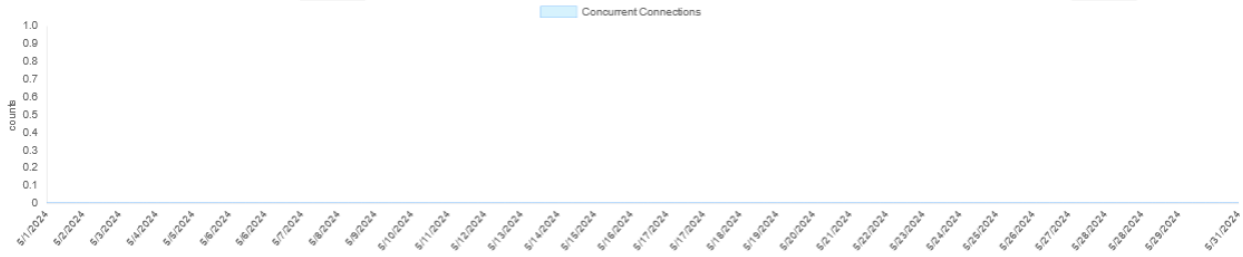
17.6 Consulta De Procesos Nacional Unificada (CPNU)

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

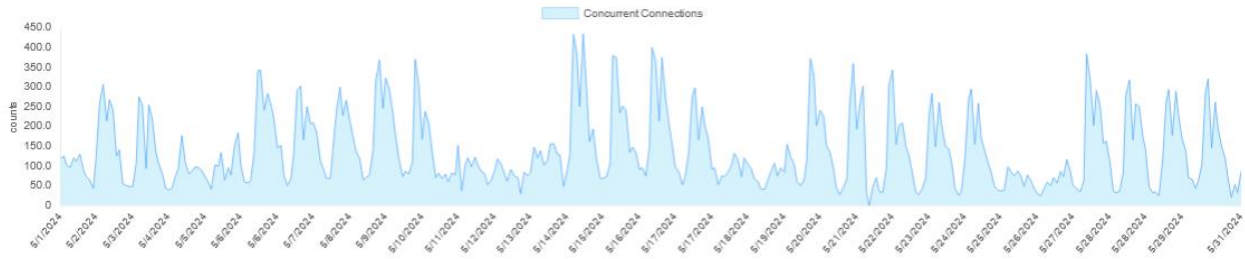

CONSULTA_PU_HT...
Resources: 1 2
Port: VLAN_3205
CONSULTA_PU_H...
10.1.2.21:8443
10.1.2.22:8443
CONSULTA_PU_HT...
Resources: 1 2
Port: VLAN_3205
CONSULTA_PU_H...
10.1.2.21:443
10.1.2.22:443
CONSULTA_PU_4431
Resources: 1 2
Port: VLAN_3205
CONSULTA_PU_4...
10.1.2.21:4431
10.1.2.22:4431
CONSULTA_PU_4432
Resources: 1 2
Port: VLAN_3205
CONSULTA_PU_4...
10.1.2.21:4432
10.1.2.22:4432
CONSULTA_PU_4435
Resources: 1 2
Port: VLAN_3205
CONSULTA_PU_4...
10.1.2.21:4435
10.1.2.22:4435
CONSULTA_PU_4436
Resources: 1 2
Port: VLAN_3205
CONSULTA_PU_4...
10.1.2.21:4436
10.1.2.22:4436
CONSULTA_PU_444
Resources: 1 2
Port: VLAN_3205
CONSULTA_PU_4...
10.1.2.21:444
10.1.2.22:444
CONSULTA_PU_448
Resources: 1 2
Port: VLAN_3205
CONSULTA_PU_4...
10.1.2.21:448
10.1.2.22:448
CONSULTA_PU_449
Resources: 1 2
Port: VLAN_3205
CONSULTA_PU_4...
10.1.2.21:449
10.1.2.22:449
CONSULTA_PU_8085
Resources: 1 2
Port: VLAN_3205
CONSULTA_PU_8...
10.1.2.21:8085
10.1.2.22:8085



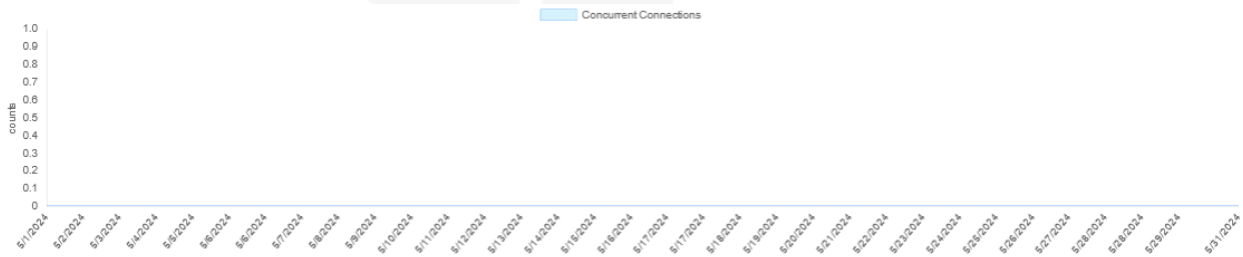
Durante mayo no se tuvieron sesiones concurrentes por el puerto HTTP:



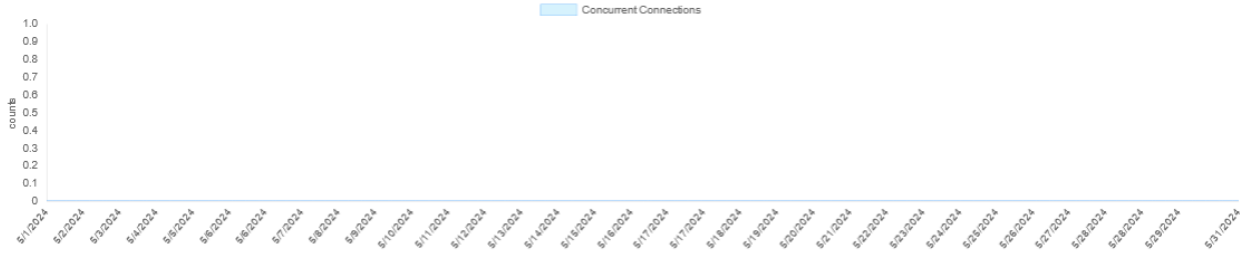
Las sesiones concurrentes por HTTPS fueron:



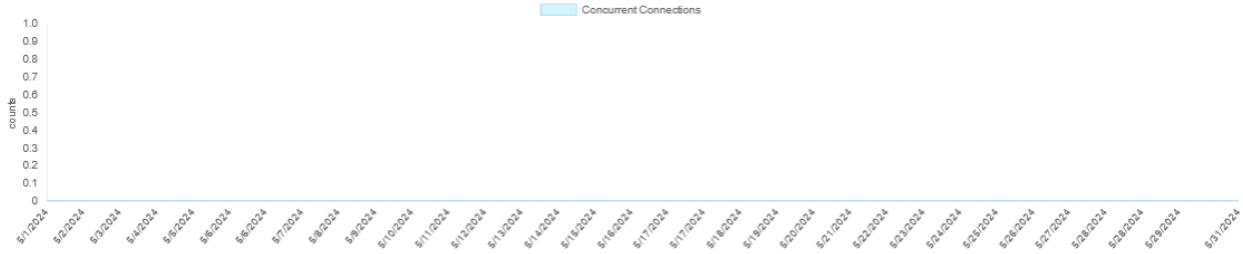
No se tuvieron sesiones concurrentes por el puerto 4431:



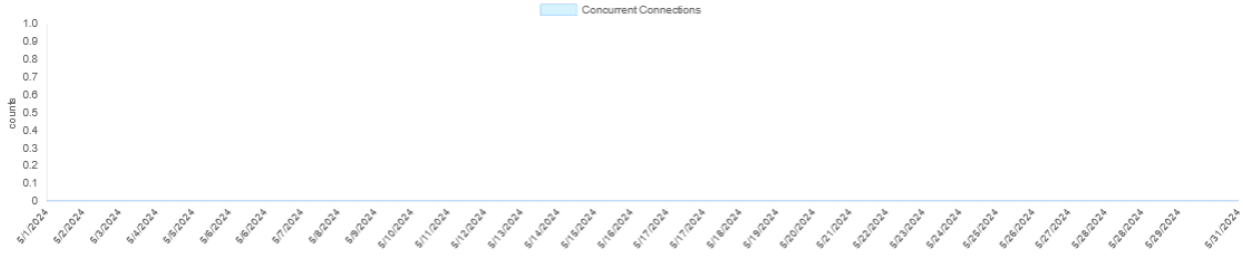
No se tuvieron sesiones concurrentes por el puerto 4432:



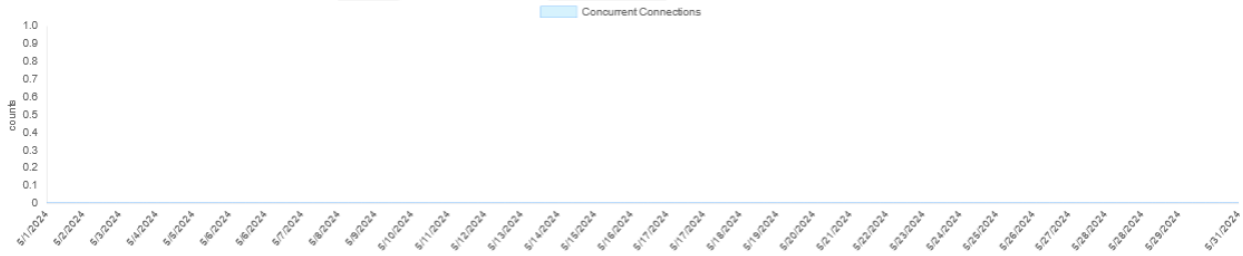
No se tuvieron sesiones concurrentes por el puerto 4435:



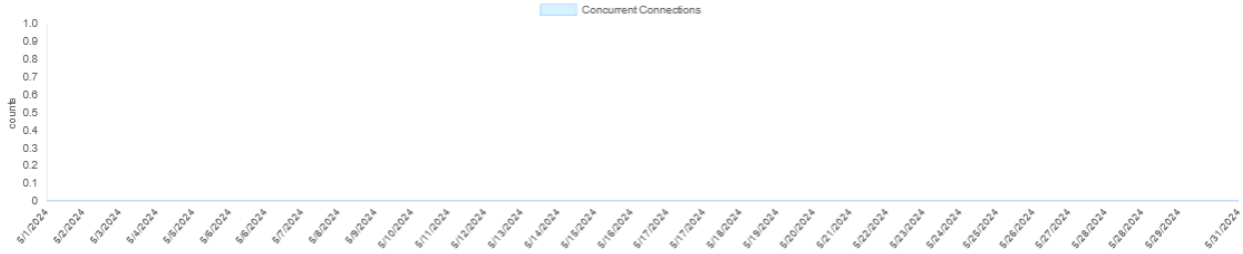
Las sesiones concurrentes por puerto 4436 fueron:



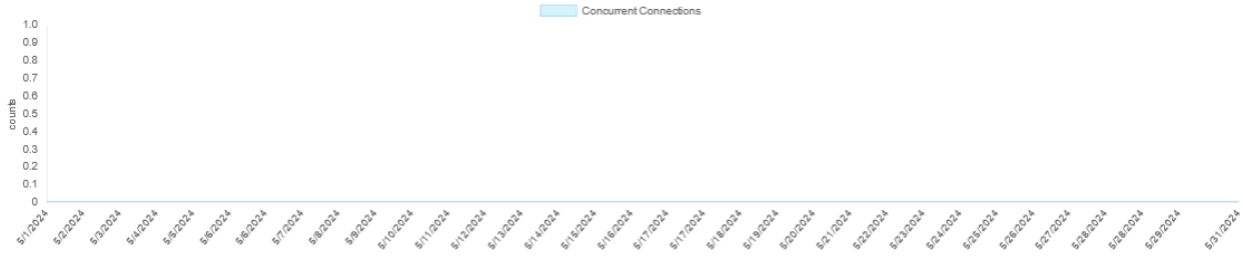
No se tuvieron sesiones concurrentes por el puerto 444:



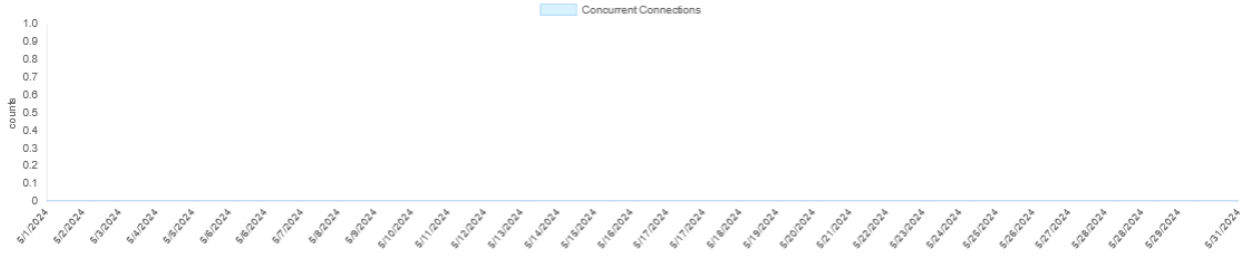
Las sesiones concurrentes por 448 fueron:



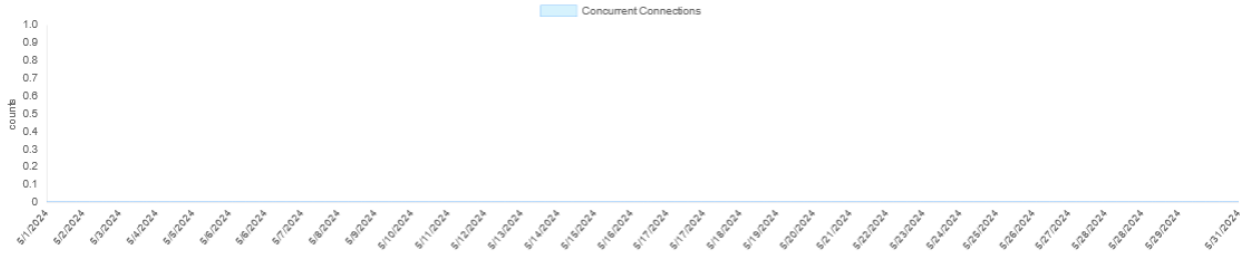
No se tuvieron sesiones concurrentes por el puerto 449:



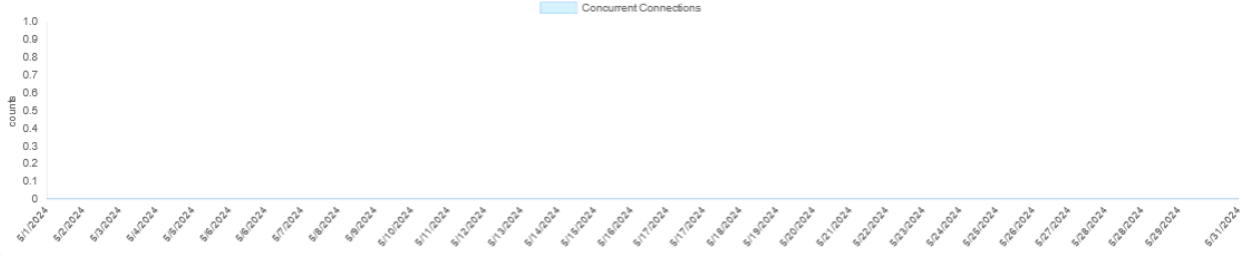
No se tuvieron sesiones concurrentes por el puerto 8085:



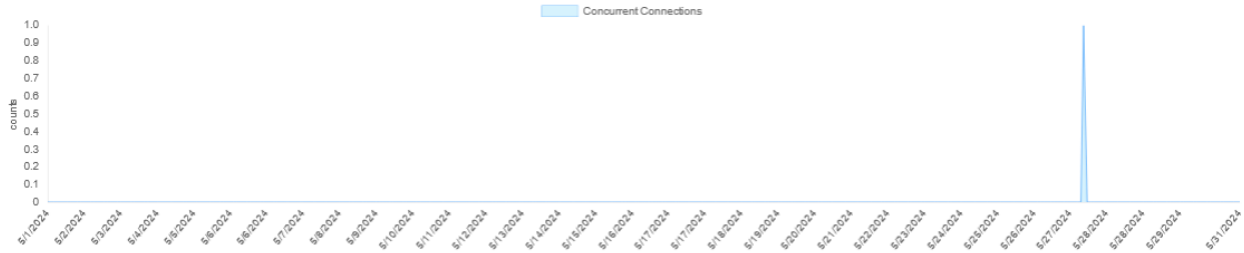
No se tuvieron sesiones concurrentes por el puerto 90:



No se tuvieron sesiones concurrentes por el puerto 9085:



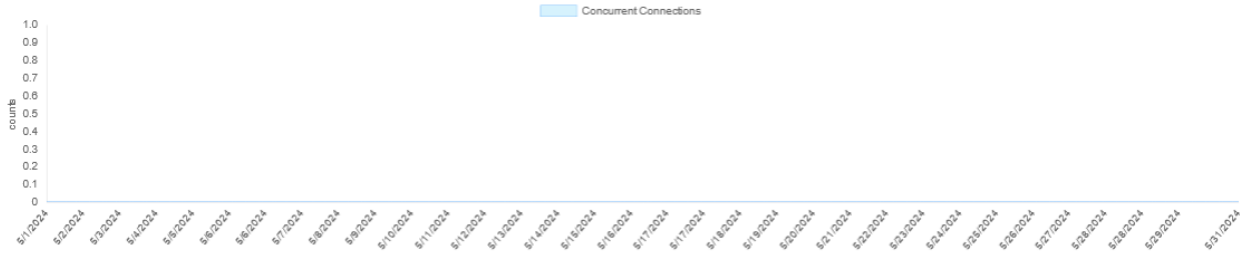
No se tuvieron sesiones concurrentes por el puerto 8643:



17.7 SIERJU

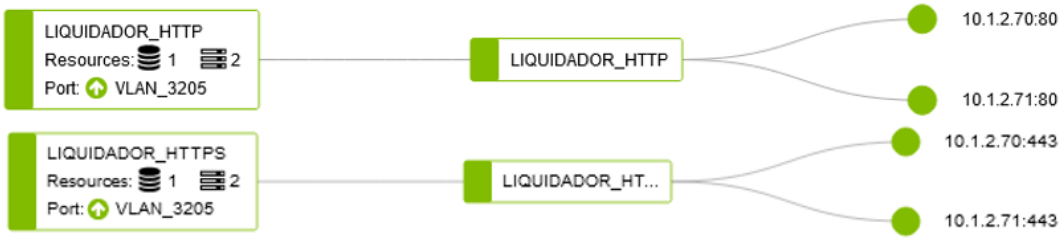
La configuración de balanceo para esta aplicación en el balanceador FortiADC es:

Durante mayo no se observan conexiones concurrentes para este aplicativo:

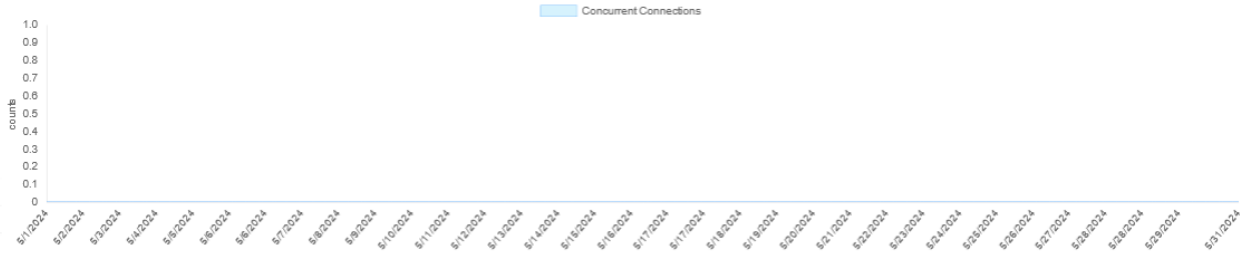


17.8 Liquidador de Sentencias

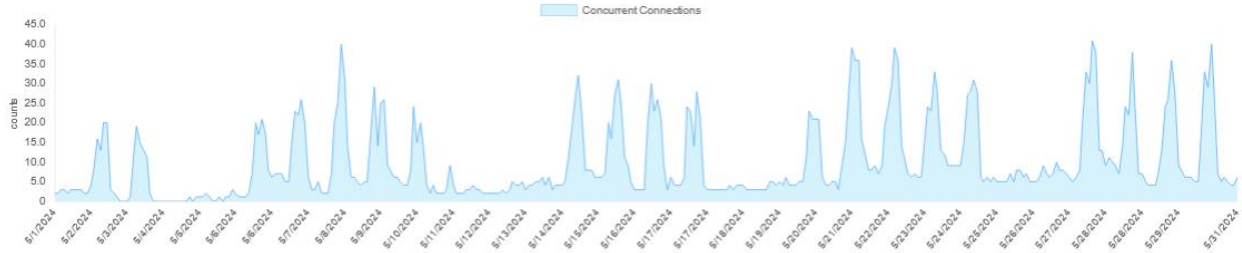
Virtual server Liquidador de Sentencias balanceador FortiADC



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



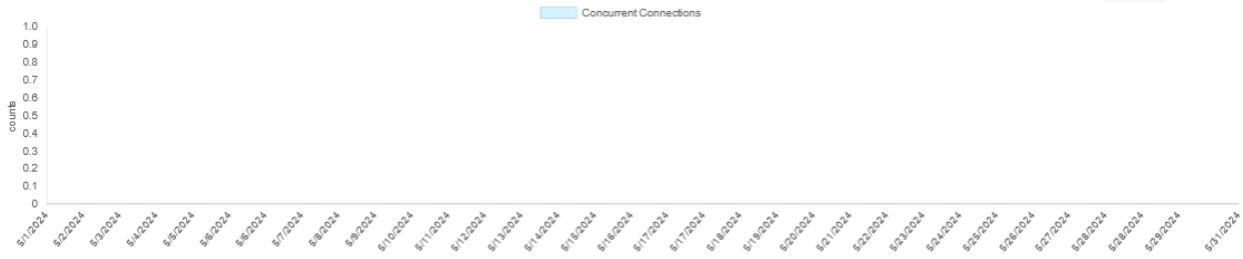
Las sesiones concurrentes por HTTPS fueron:



17.9 Consulta Jurisprudencia

Virtual server Consulta Jurisprudencia se encuentra en el balanceador FortiADC.

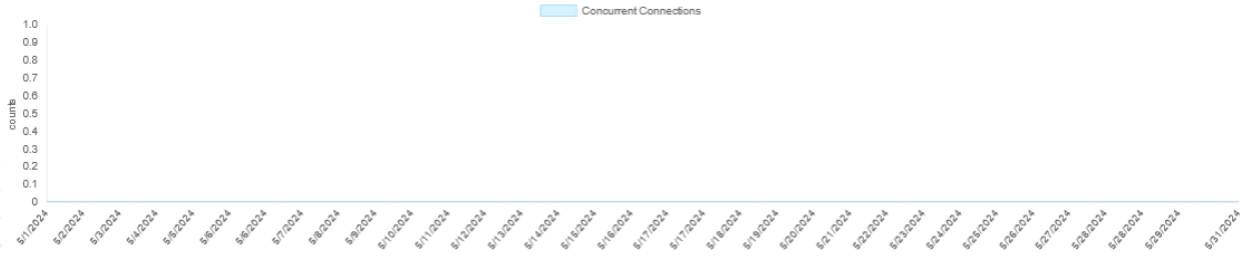
Durante mayo no se observan conexiones concurrentes para este aplicativo:



17.10 API Gestión de Audiencias

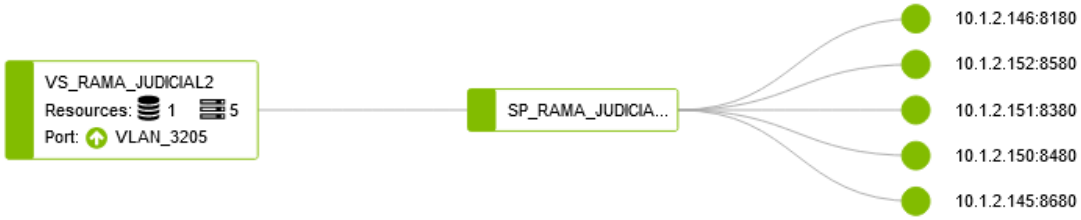
Virtual server API Gestión de Audiencias balanceador FortiADC.

Durante mayo no se observan conexiones concurrentes para este aplicativo:

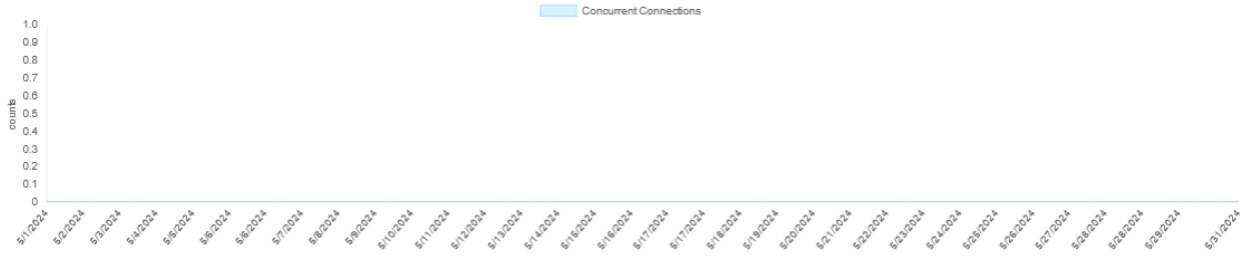


17.11 Portal Alterno de la Rama Judicial

Se encuentran balanceado en el FortiADC:

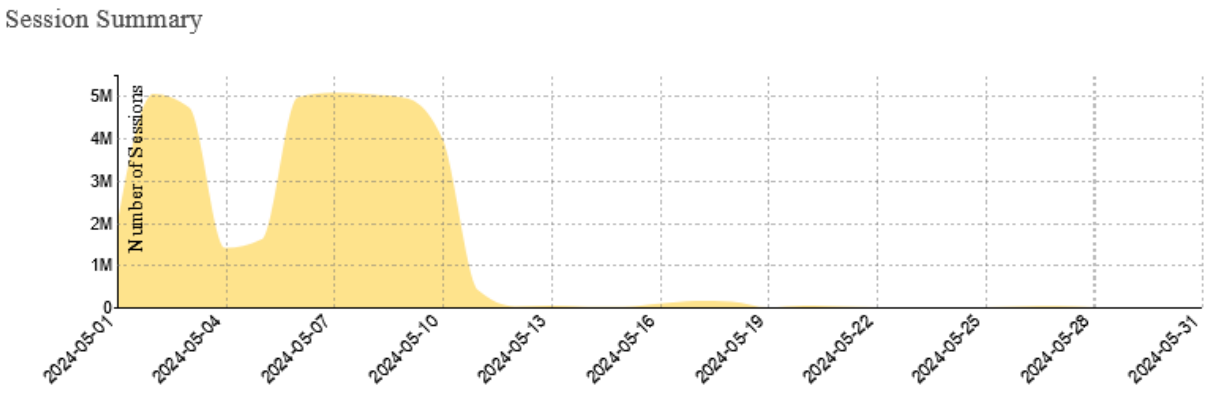


Durante mayo no se observan conexiones concurrentes para este aplicativo:



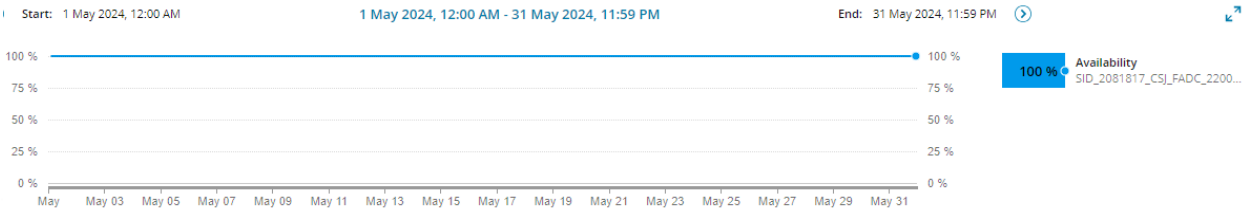
17.12 Portal de la Rama Judicial

Las sesiones Historico_Portal Rama Judicial fueron:

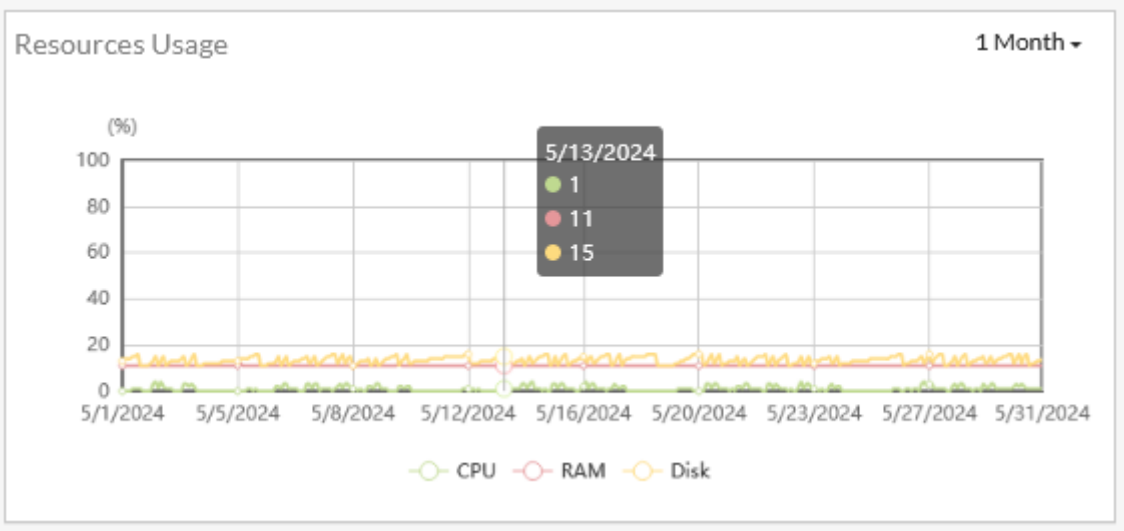


17.13 Disponibilidad y performance.

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



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



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

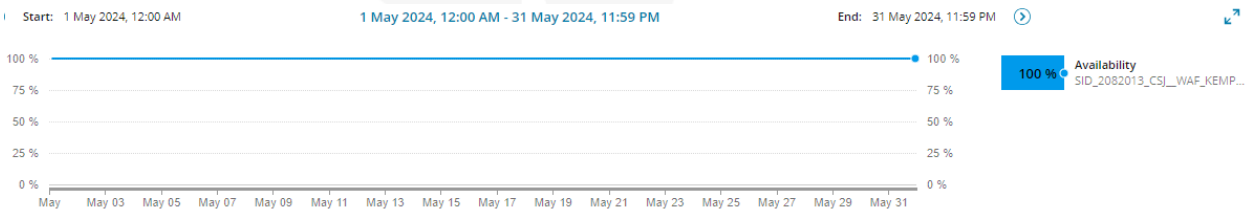
Para la protección de las aplicaciones web se tienen configuradas las siguientes políticas en los Firewall de Aplicaciones Web:

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 mayo se obtuvo una disponibilidad del 100 % en el Kemp de Torre Central.



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

La siguiente tabla muestra el top 10 de las reglas o virtual services que proporcionaron mayor protección contra ataques a las aplicaciones web durante mayo. Sobre las aplicaciones procesojudicial.ramajudicial.gov.co TYBA PRUEBAS, procesos.ramajudicial.gov.co_procesoscs CONSULTA AZUL, nuevoportal.ramajudicial.gov.co Y cndj.gov.co 190.217.24.176 han sido prevenidas la mayor cantidad de ataques durante mayo:

#	Name	Virtual IP Address	Total Events	% del total
1	procesojudicial.ramajudicial.gov.co TYBA PRUEBAS	172.17.201.249:443	11178418	32,81%
2	procesos.ramajudicial.gov.co_procesoscs CONSULTA AZUL	172.17.201.26:8443	7170294	21,04%
3	nuevoportal.ramajudicial.gov.co Y cndj.gov.co 190.217.24.176	172.17.201.101:443	4550456	13,35%
4	publicacionesprocesales.ramajudicial.gov.co - 190.217.24.175	172.17.201.100:443	3832206	11,25%
5	consejodeestado.gov.co - 190.217.24.60	172.17.201.52:443	2608623	7,66%
6	siicor.corteconstitucional.gov.co - 190.217.24.62	172.17.201.13:443	2205554	6,47%
7	judit.ramajudicial.gov.co - Ivanti - TT682978 - 190.217.24.141	172.17.201.141:443	360521	1,06%
8	sirna.ramajudicial.gov.co	172.17.201.28:443	341711	1,00%
9	jurisprudencia.ramajudicial.gov.co - ayudajurisprudencia.ramajudicial.gov.co -190.217.24.193-	172.17.201.29:443	325997	0,96%
10	saidoj.ramajudicial.gov.co	172.17.201.69:443	237341	0,70%
	Otras aplicaciones		1262032	3,70%
	Total		34073153	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.

18.3 Top de peticiones por país WAF principal IFX.

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

Top 10 Countries

Total

Country	Requests	Blocked
Colombia	5762846	1094365
United States	4378879	494466
Private	811305	228764
IPrep	14633	14633
Argentina	115928	11846
Spain	88535	8255
Brazil	76171	6945
Russia	49483	5458
Costa Rica	5898	1793
Bangladesh	29263	1503

18.4 Top de ataques por política WAF principal IFX.

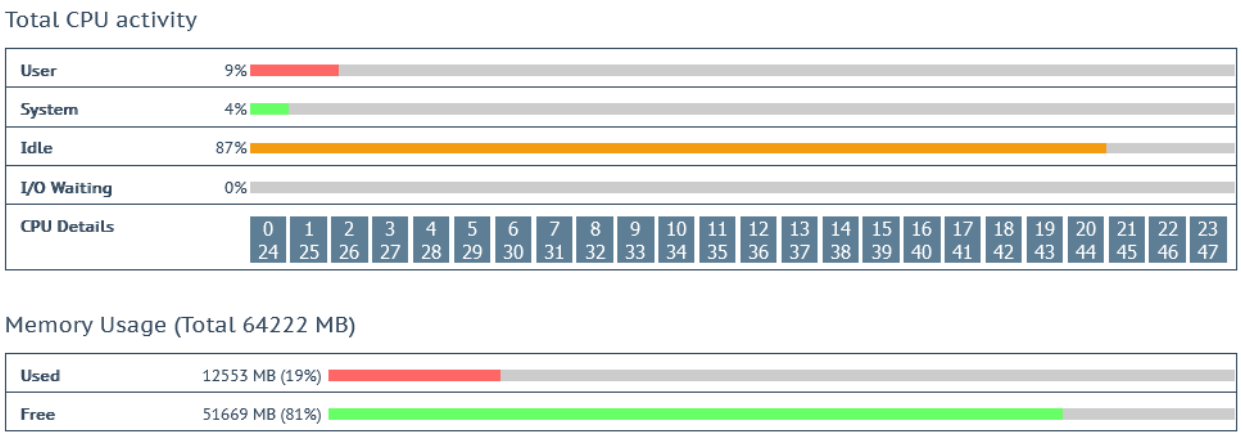
La siguiente tabla muestra el top 10 de las reglas o virtual services que proporcionaron mayor protección contra ataques a las aplicaciones web durante mayo. Sobre las aplicaciones procesojudicial.ramajudicial.gov.co TYBA PRUEBAS, procesos.ramajudicial.gov.co_procesoscs CONSULTA AZUL, nuevoportal.ramajudicial.gov.co Y cndj.gov.co 190.217.24.176 han sido prevenidas la mayor cantidad de ataques durante mayo:

#	Name	Virtual IP Address	Total Events	% del total
1	procesojudicial.ramajudicial.gov.co TYBA PRUEBAS	172.17.201.249:443	11178418	32,81%
2	procesos.ramajudicial.gov.co_procesoscs CONSULTA AZUL	172.17.201.26:8443	7170294	21,04%
3	nuevoportal.ramajudicial.gov.co Y cndj.gov.co 190.217.24.176	172.17.201.101:443	4550456	13,35%
4	publicacionesprocesales.ramajudicial.gov.co - 190.217.24.175	172.17.201.100:443	3832206	11,25%
5	consejodeestado.gov.co - 190.217.24.60	172.17.201.52:443	2608623	7,66%
6	siicor.corteconstitucional.gov.co - 190.217.24.62	172.17.201.13:443	2205554	6,47%
7	judit.ramajudicial.gov.co - Ivanti - TT682978 - 190.217.24.141	172.17.201.141:443	360521	1,06%
8	sirna.ramajudicial.gov.co	172.17.201.28:443	341711	1,00%
9	jurisprudencia.ramajudicial.gov.co - ayudajurisprudencia.ramajudicial.gov.co -190.217.24.193-	172.17.201.29:443	325997	0,96%
10	saidoj.ramajudicial.gov.co	172.17.201.69:443	237341	0,70%
	Otras aplicaciones		1262032	3,70%
	Total		34073153	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.

18.5 Consumo de recursos WAF principal IFX.

El WAF KEMP de Torre Central presentó consumo de CPU del 9%, memoria de 19% y disco en un 25%.



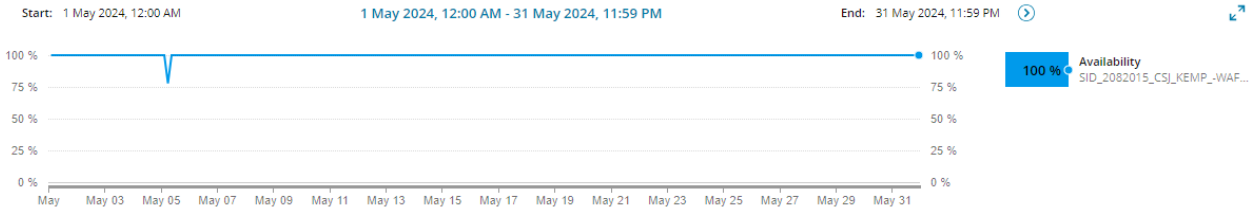
Disk Usage

/var/log (24.61 GB)	0.34 GB (1%)	
/var/log/ userlog (886.34 GB)	219.72 GB (25%)	

19. TRÁFICO DE WEB APPLICATION FIREWALL (WAF) CAN

19.1 Disponibilidad WAF CAN.

Durante mayo 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%.

Nota: El evento del domingo 5 de mayo a las 5am se debe a la incidencia imputable a cliente CSJ "Alerta caída WAF CAN - Problemas eléctricos cliente". Debido a este evento, la medición de disponibilidad sin redondear para alcanzar el appliance desde la herramienta de monitoreo es del 99.908% imputable a cliente:

Availability Statistics

PERIOD	AVAILABILITY
Today	100.000 %
Yesterday	100.000 %
Last 7 Days	100.000 %
Last 30 Days	99.930 %
This Month	99.845 %
Last Month	99.908 %

19.2 Uso de políticas de servidores WAF CAN.

La aplicación más consultada durante mayo fue cortesuprema.gov.co_Palacio con un 68,93% del total:

#	Name	Virtual IP Address	Total Conns	% del total
1	cortesuprema.gov.co_Palacio	172.17.202.239:443	7698421	68,93%
2	sso.cortesuprema.gov.co	172.17.202.141:443	489727	4,38%
3	convocatorias.consejodeestado.gov.co	172.17.202.147:443	408118	3,65%
4	cortesuprema_Palacio Redirect	172.17.202.239:80	345763	3,10%
5	restituciontierras.ramajudicial.gov.co	172.17.202.37:443	335308	3,00%
6	samairj.consejodeestado.gov.co	172.17.202.38:443	332268	2,97%
7	sso.cortesuprema.gov.co Redirect	172.17.202.141:80	299470	2,68%
8	linkce.consejodeestado.gov.co	172.17.202.42:443	138574	1,24%
9	serviciopdf.ramajudicial.gov.co	172.17.202.7:443	130053	1,16%
10	siapoas.ramajudicial.gov.co	172.17.202.43:443	120341	1,08%
	Otras aplicaciones		870992	7,80%
	Total		11169035	100,00%

19.3 Top de peticiones por país WAF CAN.

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

Top 10 Countries

Total

Country	Requests	Blocked
IPrep	12688	12688
Spain	22902	3262
China	22617	1207
United States	1410111	1016
Private	986800	960
Germany	70234	586
Lithuania	2618	413
Switzerland	5783	342
Romania	5632	326
Russia	45823	218

19.4 Top de ataques por política WAF CAN.

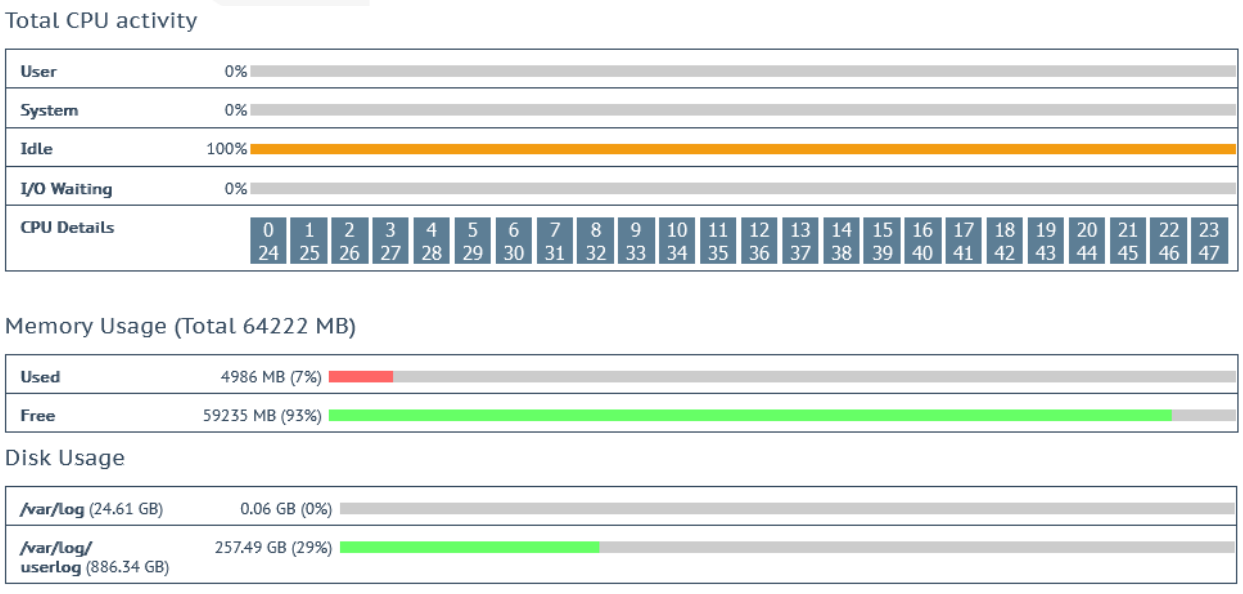
La siguiente tabla muestra el top 10 de las reglas o virtual services que proporcionaron mayor protección contra ataques a las aplicaciones web durante mayo. Sobre la aplicación cortesuprema.gov.co_Palacio ha sido prevenida la mayor cantidad de ataques durante mayo:

#	Name	Virtual IP Address	Total Events	% del total
1	cortesuprema.gov.co_Palacio	172.17.202.239:443	35259942	87,59%
2	sso.cortesuprema.gov.co	172.17.202.141:443	1126676	2,80%
3	restituciontierras.ramajudicial.gov.co	172.17.202.37:443	930068	2,31%
4	convocatorias.consejodeestado.gov.co	172.17.202.147:443	492592	1,22%
5	siapoas.ramajudicial.gov.co	172.17.202.43:443	422584	1,05%
6	linkce.consejodeestado.gov.co	172.17.202.42:443	407556	1,01%
7	capacitacion.ramajudicial.gov.co 443	172.17.202.13:443	324145	0,81%
8	samairj.consejodeestado.gov.co	172.17.202.38:443	225074	0,56%
9	efipruebas2.ramajudicial.gov.co	172.17.202.150:443	175584	0,44%
10	serviciopdf.ramajudicial.gov.co	172.17.202.7:443	172284	0,43%
	Otras aplicaciones		720689	1,79%
	Total		40257194	100,00%

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

19.5 Consumo de recursos WAF CAN.

El WAF KEMP del CAN presentó consumo de CPU del 0%, memoria de 7% y disco en un 29%.



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

Este certificado tiene vigencia hasta el 25 de mayo 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

Durante mayo se presentaron 788 intentos de login hacia los firewall perimetrales. El acceso administrativo se encuentra protegido con Token.

Usuario	Firewall Central	Firewall Palacio	Total de intentos fallidos
123		2	2
348934jt80gfj093jswerfg		1	1
academie		1	1
access		1	1
accounting		2	2
accountingar		1	1
accueil		1	1
achat		1	1
act		1	1
adm		1	1
admin		223	223
admin01		1	1
admin1		1	1
administrator		9	9
adsl		2	2
adtest		1	1
adv02		1	1
akustik		1	1

amministrazione	1	1
apc	1	1
archive	1	1
aruba	1	1
assessor	1	1
associations	1	1
audit	1	1
auditor	1	1
autocad	1	1
automate	1	1
backoffice	1	1
backup	1	1
backupexec	1	1
bailiff	1	1
barcode	1	1
bartender	1	1
bcpadmin	1	1
benefits	1	1
bernadette	1	1
bewerbung	1	1
bilancia	1	1
billing	1	1
blanchisserie	1	1
board	1	1
boardroom	1	1
booking	1	1
cad	1	1
cafeuser	1	1
callcenter	1	1
camera	1	1
canon	1	1
canonscan	1	1
careers	1	1
centralino	1	1
checkin	1	1
checkout	1	1
checkscan	1	1
class	1	1
cleanroom	1	1
cleanup	1	1
clerk	1	1
coffre	1	1
commercial	1	1
commercialcdm	1	1
commercialmp	1	1
communicatie	1	1

compass		1	1
compta		1	1
comptabilite		1	1
conditionnement		1	1
conf		1	1
confroom		1	1
construction		1	1
consultant		1	1
cooler		1	1
copier		2	2
copy		1	1
corenet		1	1
costar		1	1
court		1	1
credit		1	1
cristina		1	1
crlworkstation		1	1
crystal		1	1
csjud\\jrozor	1		1
csuser		1	1
ctest		1	1
cubiscan		1	1
cursist		1	1
customer		1	1
cybersecurity		1	1
dasarmiento		1	1
dataentry		1	1
db2admin		1	1
dbagent		1	1
design		1	1
despatch		1	1
detail		1	1
developer		2	2
dietary		1	1
director		1	1
dispatch		1	1
dispatch1		1	1
dispatch3		1	1
dispatcher		1	1
display		1	1
dozent		1	1
dsarmiento		2	2
durpc		1	1
ec		1	1
ediftp		1	1
elections		1	1

eleve	1	1
elisa	1	1
emcuser	1	1
empfang	1	1
enterprise	1	1
eqmuser	1	1
equitrac	1	1
es	1	1
esprit	1	1
etude	1	1
eval	1	1
events	1	1
eweek	1	1
ewsierra	2	2
exchange	1	1
executive	1	1
expedition	1	1
exservice	1	1
extern	1	1
fax	1	1
faxstar	1	1
finance	2	2
firepower	1	1
formation	1	1
forti	4	4
foscan	1	1
fotocopiatore	1	1
frontdesk	1	1
fssauzen	1	1
fsuser	1	1
fusion	1	1
gates	1	1
graphic	1	1
graphicdesign	1	1
guest	12	12
guest1	1	1
guest2	1	1
guest3	1	1
helpdesk	4	4
holzma	1	1
hotline	1	1
hr	2	2
hradmin	1	1
hrphoto	1	1
hutter	1	1
india	1	1

info		1	1
info2		1	1
inplant		1	1
insight		1	1
inspection		1	1
intelerad		1	1
interface		1	1
interim		1	1
intern		1	1
intsrv		1	1
intsrv1		1	1
inventory		1	1
ipad		1	1
isilog		1	1
it		2	2
it_helpdesk		2	2
itsupport		2	2
jcastrir	1		1
jessica		1	1
jrozor	7		7
jrozor@cendoj.ramajudicial.gov.co	1		1
kiosk		1	1
kitchen		1	1
konica		1	1
kyocera		1	1
lab		1	1
label		1	1
labels		1	1
labomp		1	1
lager		1	1
laptop		1	1
laser		1	1
ldap		1	1
library		1	1
livescan		1	1
locum		1	1
logistique		1	1
loic		1	1
mac		1	1
magasin		1	1
mail		1	1
mailroom		1	1
mailstore		1	1
maint		1	1
maintenance		1	1
management		1	1

manager		1	1
manager2		1	1
market		1	1
marketing		1	1
marquage		1	1
mde		1	1
mecano		1	1
media		1	1
meetingroom		1	1
mes		1	1
migwiz		1	1
misuser		1	1
mmarino	3		3
monitor		1	1
montage		1	1
multimedia		1	1
nasadmin		1	1
newsletter		1	1
noreply		1	1
nurse		1	1
office		2	2
officer		1	1
operations		2	2
operator		1	1
pack		1	1
parent		1	1
parking		1	1
pasa		1	1
paul		1	1
paxton		1	1
payroll		1	1
pcdocs		1	1
plot		1	1
portfolio		1	1
postgres		1	1
postmaster		1	1
praktikant		1	1
prep		1	1
prepa		1	1
presentation		1	1
presse		1	1
printer		1	1
printuser		1	1
privacy		1	1
procurement		1	1
prod		1	1

productie	1	1
production	1	1
program	1	1
public	1	1
pve	1	1
qa	1	1
qualite	1	1
radworks	1	1
reception	2	2
receptionist	1	1
recorder	1	1
recovery	1	1
redlands	1	1
release	1	1
remote	1	1
reports	1	1
research	1	1
returns	1	1
reunion	1	1
rfid	1	1
ricoh	1	1
root	50	50
sa	1	1
safety	1	1
sales	2	2
save	1	1
scan	2	2
scanner	1	1
scanner2	1	1
scans	1	1
scansione	1	1
scanuser	1	1
scheduler	1	1
schedusr	1	1
schulung	1	1
security	2	2
server	1	1
shipping	2	2
shipping2	1	1
shop	2	2
shopfloor1	1	1
shpda	1	1
siemens	1	1
smart	1	1
soft	1	1
sqladmin	1	1

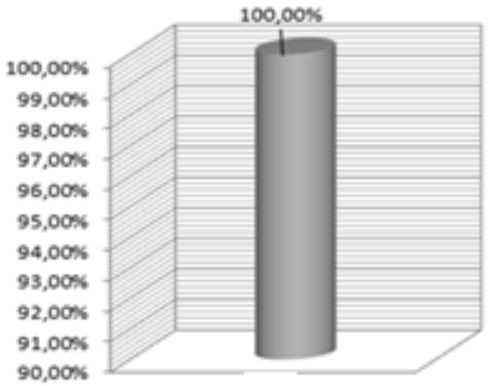
ssiad	1	1
staff	1	1
staff1	1	1
staff2	2	2
stage	1	1
stagenv	1	1
stagiaire	1	1
statements	1	1
student	1	1
super	6	6
support	14	14
surv	1	1
sylvie	1	1
symed	1	1
system	1	1
systems	1	1
taxsale	1	1
tcnote	1	1
teachers	1	1
tech	1	1
techline	1	1
technology	1	1
telecomadmin	3	3
temp	1	1
tempuser	1	1
test	5	5
test1	1	1
test2	1	1
tester	1	1
testerb	1	1
testloginapp	1	1
testmark	1	1
testrds	1	1
testuser	3	3
tfs	1	1
time	1	1
timeclock	1	1
top	1	1
toptools	1	1
toshiba	1	1
trackit	1	1
train	1	1
trainee	1	1
trainer	1	1
training	1	1
training1	1	1

training2		1	1
training3		1	1
travaux		1	1
treasurer		1	1
ubnt		3	3
uniflow		1	1
unknown	3		3
user		51	51
user1		2	2
user2		1	1
useradmin		3	3
vendor		1	1
vertscape		1	1
victor.galvis	4	1	5
video		1	1
videoconf		1	1
visio		1	1
vision		1	1
visit		1	1
visiteur		1	1
visitor		2	2
voicemail		1	1
volunteer		1	1
wang		1	1
warehouse		1	1
watchguard		1	1
webadmin		1	1
webinar		1	1
webtadmin		1	1
whatsup		1	1
whiteboard		1	1
wifi		1	1
workshop		1	1
xerox		1	1
xray		1	1
Total intentos	**20**	**768**	**788**

20. DISPONIBILIDAD SEGURIDAD GLOBAL DEL MES DE MAYO

DISPONIBILIDAD GLOBAL	NUMERO DE TICKETS POR IMPUTABILIDAD	
	RESPONSABILIDAD IFX (NUMERO TICKETS)	RESPONSABILIDAD CLIENTE (NUMERO TICKETS)
100,00%	0	0

MES	DISPONIBILIDAD (%)
MAYO	100%



20.1 Anexo de las solicitudes e incidentes de seguridad reportadas.

Se adjunta documento "Anexo CSJ-Consolidado casos mayo 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	$ 4.359.900.683,11
% Valor facturado	28,10%
Valor pagado a la fecha	$ 4.359.900.683,11
% Valor pagado	28,10%

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
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

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
01 al 30 de Abril 2024	$ 9.379.680,00

1. 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.