REPORTE MENSUAL

RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA

FEBRERO 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	Este informe visualiza la disponibilidad de los servidores y recursos contratados por **RAMA JUDICIAL – CONSEJO SUPERIOR DE LA JUDICATURA** en Cloud
Finalidad	Puede utilizar este informe para evaluar la disponibilidad de los servidores y recursos
Parámetros	**Rango de fechas** Período del informe; Mes de FEBRERO de 2023 Fecha de inicio: 1 de FEBRERO de 2023 Fecha de final: 29 de FEBRERO 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

ITEM OC	DESCRIPCIÓN	Ubicación /Observación
1,1	npn03--Alojamiento de infraestructura - Housing - Cross Conexión - Oro - Puntos de red: 1 - Capacidad de energía: 1 KVA - Capacidad en unidades: 4 U - Rack/M - Cantidad: 3	Rack 69
1,2	npn03--Alojamiento de infraestructura - Housing - Cross Conexión - Oro - Puntos de red: 1 - Capacidad de energía: 1 KVA - Capacidad en unidades: 4 U - Rack/M - Cantidad: 3	Rack 31
1,3	npn03--Alojamiento de infraestructura - Housing - Cross Conexión - Oro - Puntos de red: 1 - Capacidad de energía: 1 KVA - Capacidad en unidades: 4 U - Rack/M - Cantidad: 3	Rack 69
2,1	npn03--Alojamiento de infraestructura - Housing - Cross Conexión - Oro - Puntos de red: 1 - Capacidad de energía: 1 KVA - Capacidad en unidades: 4 U - Rack/M - Cantidad: 2	Rack 31
2,2	npn03--Alojamiento de infraestructura - Housing - Cross Conexión - Oro - Puntos de red: 1 - Capacidad de energía: 1 KVA - Capacidad en unidades: 4 U - Rack/M - Cantidad: 2	Rack 31
9	npn03--Alojamiento de infraestructura - Housing - Full Rack - Oro - Puntos de red: 4 - Capacidad de energía: 4 KVA - Capacidad en unidades: 42 U - Rack/M - Cantidad: 1	Rack 31
10,1	npn03--Alojamiento de infraestructura - Housing - Full Rack - Oro - Puntos de red: 4 - Capacidad de energía: 4 KVA - Capacidad en unidades: 42 U - Rack/M - Cantidad: 2	Rack 29
10,2	npn03--Alojamiento de infraestructura - Housing - Full Rack - Oro - Puntos de red: 4 - Capacidad de energía: 4 KVA - Capacidad en unidades: 42 U - Rack/M - Cantidad: 2	Rack 30
11	npn03--Alojamiento de infraestructura - Housing - Full Rack - Oro - Puntos de red: 4 - Capacidad de energía: 4 KVA - Capacidad en unidades: 42 U - Rack/M - Cantidad: 1	Rack 32
12	npn03--Alojamiento de infraestructura - Housing - Full Rack - Oro - Puntos de red: 4 - Capacidad de energía: 4 KVA - Capacidad en unidades: 42 U - Rack/M - Cantidad: 1	Rack 73

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) y la infraestructura de Oracle (oracle), se encuentra en calidad de collocation y la Entidad de acuerdo con las necesidades ha contratado energía y puntos de red adicionales para el funcionamiento de la misma.

3. ALMACENAMIENTO

ITEM	SERVICIO	DETALLE	PRESENTACIÓN Y/O UTILIZACION	TIEMPO
13	1726655	npn03--IaaS almacenamiento - Almacenamiento SAN Alto Rendimiento - Oro - Alta - Nube Privada - Capacidad: 200TB a <500TB - FC >= 8 Gbps - SSD - RAID: 5 - IOPS READ 72000 / WRITE 30000 - GB/Mes - Cantidad: 500000	500000	7,5
14	1726656	npn03--IaaS almacenamiento - Almacenamiento SAN Alto Rendimiento - Oro - Alta - Nube Privada - Capacidad: 200TB a <500TB - FC >= 8 Gbps - SSD - RAID: 5 - IOPS READ 72000 / WRITE 30000 - GB/Mes - Cantidad: 500000	500000	7,5
15	1726657	npn03--IaaS almacenamiento - Almacenamiento SAN Alto Rendimiento - Oro - Alta - Nube Privada - Capacidad: 200TB a <500TB - FC >= 8 Gbps - SSD - RAID: 5 - IOPS READ 72000 / WRITE 30000 - GB/Mes - Cantidad: 500000	500000	7,5
16	1726658	npn03--IaaS almacenamiento - Almacenamiento SAN Alto Rendimiento - Oro - Alta - Nube Privada - Capacidad: 200TB a <500TB - FC >= 8 Gbps - SSD - RAID: 5 - IOPS READ 72000 / WRITE 30000 - GB/Mes - Cantidad: 500000	500000	7,5
17	1726659	npn03--IaaS almacenamiento - Almacenamiento SAN Alto Rendimiento - Oro - Alta - Nube Privada - Capacidad: 200TB a <500TB - FC >= 8 Gbps - SSD - RAID: 5 - IOPS READ 72000 / WRITE 30000 - GB/Mes - Cantidad: 500000	500000	7,5
18	1855654	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	150000	7,5
19	1855655	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	150000	6,5
20	1855656	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	150000	5,5
21	1855657	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	150000	4,5
22	1855658	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	150000	3,5
23	1855659	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	150000	2,5
24	1855660	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	150000	1,5
25	1855661	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	150000	7,5

El almacenamiento total presentado a las Máquinas Virtuales de conformidad con las solicitudes de la Entidad, con corte a 20 de FEBRERO de 2024 es de: **3700000 TERAS.**

La información se encuentra detallada en el anexo "**Inventario_ServiciosCSJ_FEBRERO_2023.xls**" hoja **"ALMACENAMIENTO"**

4. BACKUPS

ITEM OC	DESCRIPCIÓN
32	npn03--IaaS almacenamiento - Backup de Datos - Alta - Capacidad: 50TB a <100TB - Almacenamiento SAN - Diaria - GB/Mes - Cantidad: 65000
33	npn03--IaaS almacenamiento - Backup de Datos - Alta - Capacidad: 50TB a <100TB - Almacenamiento SAN - Semanal - GB/Mes - Cantidad: 85000
34	npn03--IaaS almacenamiento - Backup de Datos - Alta - Capacidad: 200TB a <500TB - Almacenamiento SAN - Mensual - GB/Mes - Cantidad: 350000

Actualmente de las 179 máquinas virtuales, de las cuales se encuentran disponibles en estado de producción 179 y cuatro se encuentran en estado off. Los Backups se ejecutan sobre 179 máquinas virtuales

(Remitirse al anexo "**Inventario_Servicios_CSJ_FEBRERO_2023.xls**" para ver el detalle) Para las tomas de Backups de las máquinas virtuales de grabaciones se encuentran excluidas las copias de respaldo de las unidades de almacenamiento que contienen formatos de video (gestión de grabaciones) los mismos están incluidos en el ítem 32 33 y 34 que corresponden a la actividad de replicación local; Las demás máquinas virtuales tienen respaldos que se ejecutan con periodicidad diaria, semanal y mensual y que atienden a las diferentes políticas acordadas entre la Entidad e IFX.

Los reportes de los Backups diarios están configurados para generar un informe a los correos electrónicos de los funcionarios de la entidad, tal cual como se definió en el momento de la entrega de este servicio.

5. REPLICACIÓN

ITEM	SERVICIO	DETALLE	PRESENTACIÓN Y/O UTILIZACION
26	1726660	npn03--IaaS almacenamiento - Replicación Local de Datos - Oro - Alta - Nube Privada - Capacidad: 200TB a <500TB - 10 Gbps - Restauración: 10TB / hora - GB/Mes - Cantidad: 410000	Replicación como contingencia a gestión de grabaciones.
27	1726661	npn03--IaaS almacenamiento - Replicación Local de Datos - Oro - Alta - Nube Privada - Capacidad: 200TB a <500TB - 10 Gbps - Restauración: 10TB / hora - GB/Mes - Cantidad: 500000	
28	1726662	npn03--IaaS almacenamiento - Replicación Local de Datos - Oro - Alta - Nube Privada - Capacidad: 200TB a <500TB - 10 Gbps - Restauración: 10TB / hora - GB/Mes - Cantidad: 500000	
29	1726663	npn03--IaaS almacenamiento - Replicación Local de Datos - Oro - Alta - Nube Privada - Capacidad: 200TB a <500TB - 10 Gbps - Restauración: 10TB / hora - GB/Mes - Cantidad: 500000	
30	1726664	npn03--IaaS almacenamiento - Replicación Local de Datos - Oro - Alta - Nube Privada - Capacidad: 200TB a <500TB - 10 Gbps - Restauración: 10TB / hora - GB/Mes - Cantidad: 500000	
31	1855653	npn03--IaaS almacenamiento - Replicación Local de Datos - Oro - Alta - Nube Privada - Capacidad: 200TB a <500TB - 10 Gbps - Restauración: 10TB / hora - GB/Mes - Cantidad: 500000	

Los detalles de la ejecución de las réplicas se encuentran a continuación:

1337771_VWSQRA04	1424279_1337776_CSJSIRNA_02 (1)	DC-IFX TC	Meeting SLA	8 sec
1337835_VWSHRA01	1424279_1337776_CSJSIRNA_01 (4)	DC-IFX TC	Meeting SLA	8 sec
1337751_VWSHRA02	1424279_1337776_CSJSIRNA_01 (4)	DC-IFX TC	Meeting SLA	8 sec
1337749_VWCRRA01	1424279_1337776_CSJSIRNA_01 (4)	DC-IFX TC	Meeting SLA	8 sec
1337750_VWCRRA02	1424279_1337776_CSJSIRNA_01 (4)	DC-IFX TC	Meeting SLA	8 sec
1337739_CSJPROC02	1424279_CSJ_PROC_03 (4)	DC-IFX TC	Meeting SLA	8 sec
1337729_CSJNGINX01	1424279_CSJ_PORTALWEB_01 (3)	DC-IFX TC	Meeting SLA	8 sec
1337753_VM-J21WAP...	1424279_1337776_CSJXXIAPP_01 (2)	DC-IFX TC	Meeting SLA	8 sec
1337766_CSJPROCRS...	1424279_CSJ_PROC_03 (4)	DC-IFX TC	Meeting SLA	8 sec
1337768_CSJPROCD...	1424279_CSJ_PROC_03 (4)	DC-IFX TC	Meeting SLA	8 sec
1337779_CSJPROCD...	1424279_CSJ_PROC_01 (4)	DC-IFX TC	Meeting SLA	8 sec
1337777_CSJPROCD...	1424279_CSJ_PROC_01 (4)	DC-IFX TC	Meeting SLA	8 sec
1337776_CSJPROCD...	1424279_CSJ_PROC_01 (4)	DC-IFX TC	Meeting SLA	8 sec
1337778_CSJPROCD...	1424279_CSJ_PROC_01 (4)	DC-IFX TC	Meeting SLA	8 sec
1337783_EFINOMINA...	1424279_CSJ_EFINOMINA (2)	DC-IFX TC	Meeting SLA	8 sec
1337767_CSJJURISD...	1424279_CSJ_PORTALDB_01 (2)	DC-IFX TC	Meeting SLA	8 sec
1337793_CSJPROCW...	1424279_CSJ_PROC_02 (2)	DC-IFX TC	Meeting SLA	8 sec
1337794_CSJPROCW...	1424279_CSJ_PROC_02 (2)	DC-IFX TC	Meeting SLA	8 sec
1337746_CSJCLUSTE...	1424279_CSJ_PROC_03 (4)	DC-IFX TC	Meeting SLA	8 sec
1337846_EFINOMINA...	1424279_CSJ_EFINOMINA (2)	DC-IFX TC	Meeting SLA	8 sec
1337765_CSJPORTAL...	1424279_CSJ_PORTALDB_01 (2)	DC-IFX TC	Meeting SLA	8 sec
1337752_VMC-JXXIW...	1424279_1337776_CSJXXIAPP_01 (2)	DC-IFX TC	Meeting SLA	8 sec

1337799_CSJLIQSET...	1424279_CSJ_01 (1)	DC-IFX TC	Meeting SLA	7 sec
1337754_CSJ-CXV-CE...	1424279_CSJ_CXVWEB_01 (1)	DC-IFX TC	Meeting SLA	7 sec
1337728_CSJ-CXV-RE...	1424279_CSJ_PORTALWEB_01 (3)	DC-IFX TC	Meeting SLA	7 sec
1337747_CSJPORTAL...	1424279_CSJ_PORTALWEB_01 (3)	DC-IFX TC	Meeting SLA	7 sec
1337790_CSJPORTAL...	1424279_CSJ_PORTALWEB_03 (2)	DC-IFX TC	Meeting SLA	7 sec
1337789_CSJPORTAL...	1424279_CSJ_PORTALWEB_03 (2)	DC-IFX TC	Meeting SLA	7 sec
1337788_CSJPORTAL...	1424279_CSJ_PORTALWEB_02 (2)	DC-IFX TC	Meeting SLA	7 sec
1337787_CSJPORTAL...	1424279_CSJ_PORTALWEB_02 (2)	DC-IFX TC	Meeting SLA	7 sec
1337772_VWSQRA05	1424279_1337776_CSJSIRNA_03 (1)	DC-IFX TC	RPO Not Meeting SLA	2 hours

En anexo "**Inventario_Servicios_CSJ_FEBRERO_2023.xls**" se encontrarán más detalles de las ejecuciones mencionadas.

6.SERVICIOS POR APLICACIÓN

6.1 Portal Web y Aplicaciones Conexas

ITEM OC	DESCRIPCIÓN	HOSTNAME
37	npn03--IaaS Procesamiento - Servidor de Uso Básico - Oro - Alta - Hosting Nube Privada - 4 - Según ficha técnica - 8 GB - 240 GB - Ser/M - Cantidad: 1	CSJ-CXV-RELAY01
44	npn03--IaaS Procesamiento - Servidor de Uso Básico - Oro - Alta - Hosting Nube Privada - 4 - Según ficha técnica - 8 GB - 240 GB - Ser/M - Cantidad: 1	CSJNGINX01
59	npn03--IaaS Procesamiento - Servidor de Uso Básico - Oro - Alta - Hosting Nube Privada - 8 - Según ficha técnica - 16 GB - 480 GB - Ser/M - Cantidad: 1	CSJEVENTOSWEB01
72	npn03--IaaS Procesamiento - Servidor de Uso Básico - Oro - Alta - Hosting Nube Privada - 8 - Según ficha técnica - 8 GB - 240 GB - Ser/M - Cantidad: 1	CSJPROC02
74	npn03--IaaS Procesamiento - Servidor de Uso Básico - Oro - Alta - Hosting Nube Privada - 8 - Según ficha técnica - 8 GB - 480 GB - Ser/M - Cantidad: 1	CSJRPSAIDOJWEB01
92	npn03--IaaS Procesamiento - Servidor de Uso Estandar - Oro - Alta - Hosting Nube Privada - 16 - Según ficha técnica - 32 GB - 960 GB - Ser/M - Cantidad: 1	CSJCLUSTER03
102	npn03--IaaS Procesamiento - Servidor de Uso Estandar - Oro - Alta - Hosting Nube Privada - 16 - Según ficha técnica - 64 GB - 960 GB - Ser/M - Cantidad: 5	CSJPORTALREP01

119	npn03--PaaS - Internet Information Server - Oro - Alta - Servidor de Uso Básico - Hosting físico - PaaS/M - Cantidad: 1	CSJLIQSETWEB01
120	npn03--PaaS - Internet Information Server - Oro - Alta - Servidor de Uso Básico - Hosting físico - PaaS/M - Cantidad: 1	CSJLIQSETWEB02
121	npn03--PaaS - SQL Sobre Windows - Oro - Alta - Servidor de Uso Intermedio - Hosting físico - SQL Server 2012 R2 o superior - PaaS/M - Cantidad: 1	CSJPROCDB01
124	npn03--PaaS - SQL Sobre Windows - Oro - Alta - Servidor de Uso Intermedio - Hosting físico - SQL Server 2012 R2 o superior - PaaS/M - Cantidad: 1	CSJPROCDBHA
125	servidor fisico BD portal web	Servidor físico (host) SQL Sobre Windows 40 Cores físicos 256 de RAM 960 de Gb Almacenamiento SSD
127	npn03--PaaS - SQL Sobre Windows - Oro - Alta - Servidor de Uso Básico - Nube privada - SQL Server 2012 R2 o superior - PaaS/M - Cantidad: 1	CSJPROCRS01
132	npn03--PaaS - SQL Sobre Windows - Oro - Alta - Servidor de Uso Estandar - Nube privada - SQL Server 2012 R2 o superior - PaaS/M - Cantidad: 1	CSJPORTALAUDI
133	npn03--PaaS - SQL Sobre Windows - Oro - Alta - Servidor de Uso Estandar - Nube privada - SQL Server 2012 R2 o superior - PaaS/M - Cantidad: 1	CSJJURISDB01
134	npn03--PaaS - SQL Sobre Windows - Oro - Alta - Servidor de Uso Estandar - Nube privada - SQL Server 2012 R2 o superior - PaaS/M - Cantidad: 1	CSJJURISWEB01
137	npn03--PaaS - SQL Sobre Windows - Oro - Alta - Servidor de Uso Estandar - Nube privada - SQL Server 2012 R2 o superior - PaaS/M - Cantidad: 1	CSJLIQSETDB01
138	npn03--PaaS - SQL Sobre Windows - Oro - Alta - Servidor de Uso Estandar - Nube privada - SQL Server 2012 R2 o superior - PaaS/M - Cantidad: 1	CSJPROCDB05
140	npn03--PaaS - SQL Sobre Windows - Oro - Alta - Servidor de Uso Estandar - Nube privada - SQL Server 2012 R2 o superior - PaaS/M - Cantidad: 1	CSJPROCDB04
142	npn03--PaaS - SQL Sobre Windows - Oro - Alta - Servidor de Uso Estandar - Nube privada - SQL Server 2012 R2 o superior - PaaS/M - Cantidad: 1	CSJPROCDB03
143	npn03--PaaS - SQL Sobre Windows - Oro - Alta - Servidor de Uso Estandar - Nube privada - SQL Server 2012 R2 o superior - PaaS/M - Cantidad: 1	CSJPROCDB02
151	npn03--PaaS - SQL Sobre Windows - Oro - Alta - Servidor de Uso Estandar - Nube privada - SQL Server 2012 R2 o superior - PaaS/M - Cantidad: 1	CSJPORTALDB01
156	npn03--PaaS - Internet Information Server - Oro - Alta - Servidor de Uso Estandar - Nube privada - PaaS/M - Cantidad: 1	CSJPROCWEB01
157	npn03--PaaS - Internet Information Server - Oro - Alta - Servidor de Uso Estandar - Nube privada - PaaS/M - Cantidad: 1	CSJPROCWEB02
159	npn03--PaaS - Internet Information Server - Oro - Alta - Servidor de Uso Estandar - Nube privada - PaaS/M - Cantidad: 1	CSJPORTALWEB06
161	npn03--PaaS - Internet Information Server - Oro - Alta - Servidor de Uso Estandar - Nube privada - PaaS/M - Cantidad: 1	CSJPORTALWEB05
171	npn03--PaaS - Tomcat - Oro - Alta - Servidor de Uso Estandar - Nube privada - 6.0x o superior - PaaS/M - Cantidad: 1	CSJPORTALWEB01
172	npn03--PaaS - Tomcat - Oro - Alta - Servidor de Uso Estandar - Nube privada - 6.0x o superior - PaaS/M - Cantidad: 1	CSJPORTALWEB02

173	npn03--PaaS - Tomcat - Oro - Alta - Servidor de Uso Estandar - Nube privada - 6.0x o superior - PaaS/M - Cantidad: 1	CSJPORTALWEB03
174	npn03--PaaS - Tomcat - Oro - Alta - Servidor de Uso Estandar - Nube privada - 6.0x o superior - PaaS/M - Cantidad: 1	CSJPORTALWEB04

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 febrero a 29 de febrero del 2024.

CONSUMO TOTAL HORAS MES DE FEBRERO	
• Casos Reportados Netsuite	72
Sesiones de Seguimiento	6
Sesiones de Trabajo	0
Casos Escalados Medio Digital - Whatsapp	4
Horas Disponibilidad del Recurso Fines de Semana	--
Total Horas Consumidas de las 400 - Experto Master	**318**

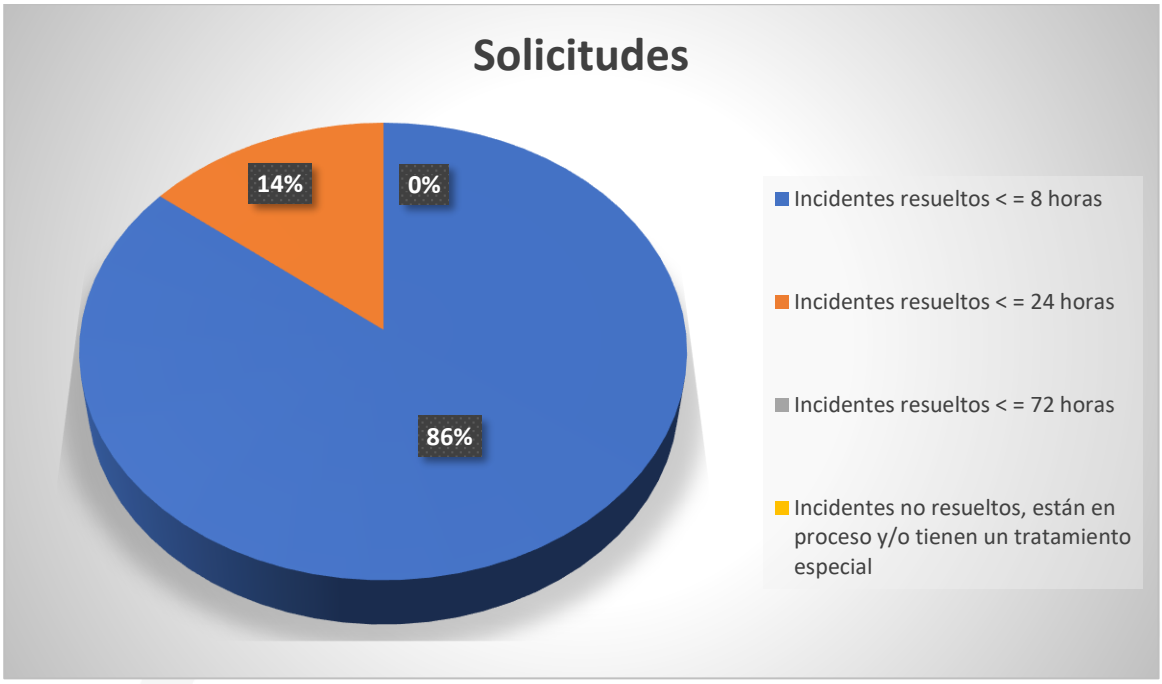
2. INDICADORES DEL CENTRO CONSOLIDADO DE SERVICIOS

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

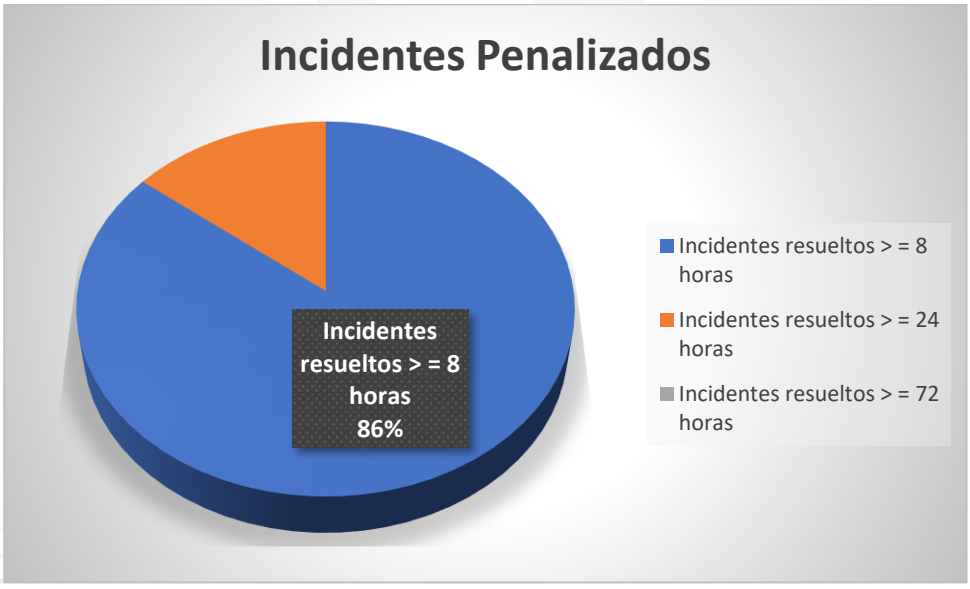
	Volumen en 1 febrero a 29 de febrero
Casos Reportados	14
Solicitudes	14
Incidencias	0
WA - AF	0

2.1 TASA DE RESOLUCIÓN DE PROBLEMAS

Tiempo de Gestión	Solicitudes
Solicitudes resueltas < = 8 horas	13
Solicitudes resueltas < = 24 horas	1
Solicitudes resueltas < = 72 horas	0
Solicitudes no resueltas, están en proceso y/o tienen un tratamiento especial	0
Total	**14**

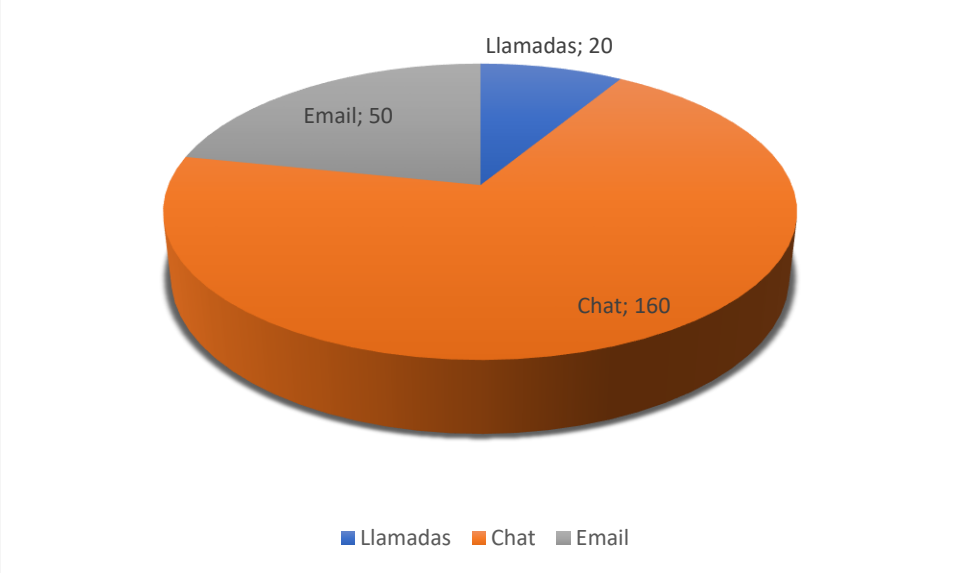


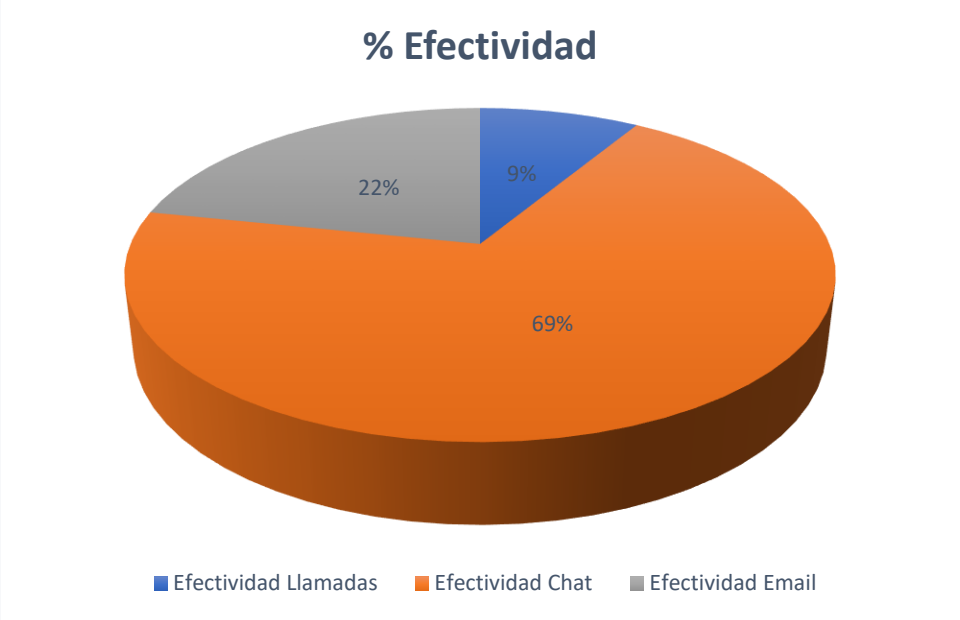
Tiempo de Gestión	Incidentes Penalizados
Incidentes resueltos > = 8 horas	0
Incidentes resueltos > = 24 horas	0
Incidentes resueltos > = 72 horas	0
Total	**0**



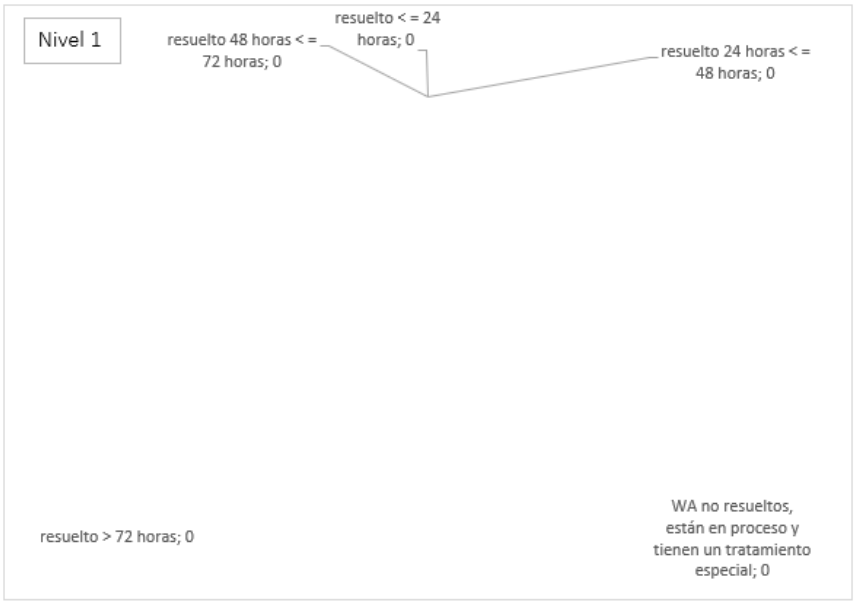
Canales de Atención	Cantidad
Llamadas	20
Chat	160
Email	50
Total	230
Efectividad	**%**
Efectividad Llamadas	8,70
Efectividad Chat	69,57
Efectividad Email	21,74
Efectividad Total en Canales de Atención	100

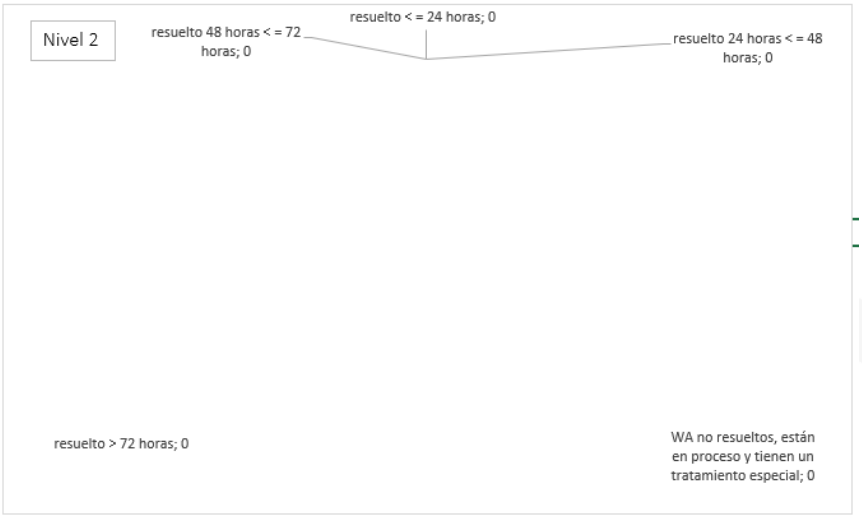
No conformidad	0

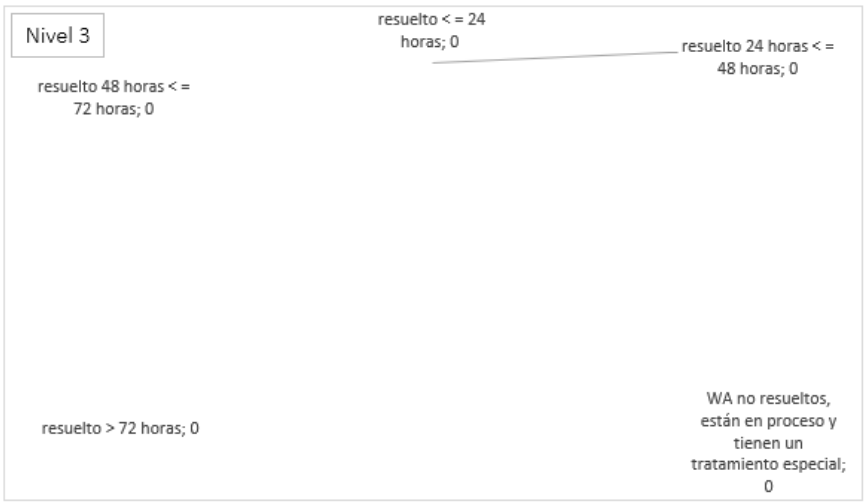


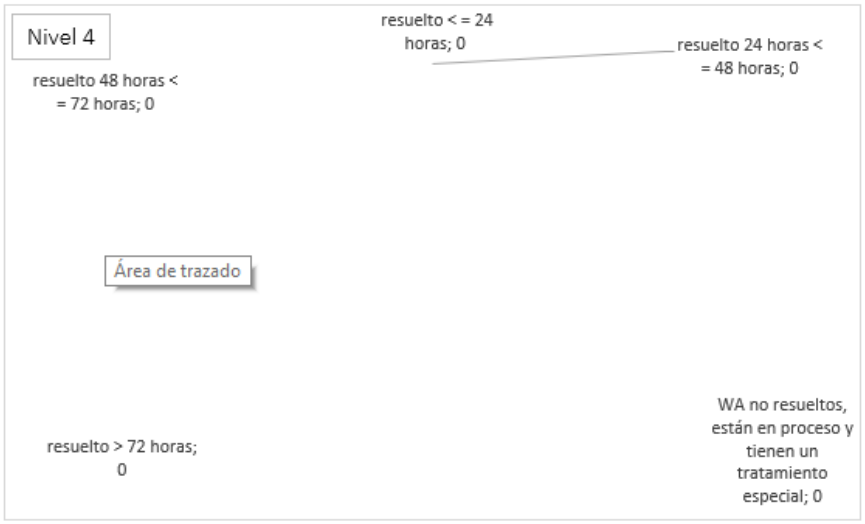


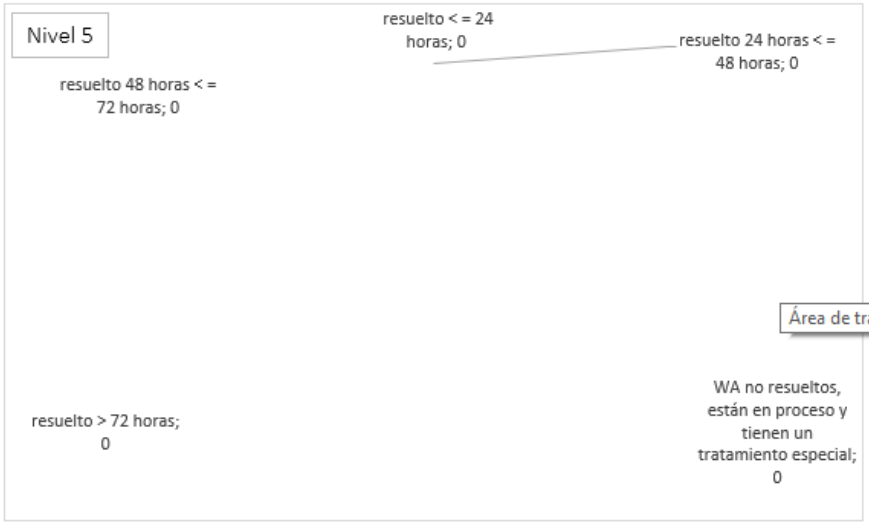
WA (Ajustes Funcionales)					
Tiempo de Gestión	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
resuelto < = 24 horas	0	0	0	0	0
resuelto 24 horas < = 48 horas	0	0	0	0	0
resuelto 48 horas < = 72 horas	0	0	0	0	0
resuelto > 72 horas	0	0	0	0	0
WA no resueltos, están en proceso y tienen un tratamiento especial	0	0	0	0	0
Total	**0**	**0**	**0**	**0**	**0**




Nivel 2
resuelto 48 horas < = 72 horas; 0
resuelto < = 24 horas; 0
resuelto 24 horas < = 48 horas; 0
resuelto > 72 horas; 0
WA no resueltos, están en proceso y tienen un tratamiento especial; 0


Nivel 3
resuelto < = 24 horas; 0
resuelto 24 horas < = 48 horas; 0
resuelto 48 horas < = 72 horas; 0
resuelto > 72 horas; 0
WA no resueltos, están en proceso y tienen un tratamiento especial; 0


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



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 febrero a 29 de febrero 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 febrero a 29 de febrero 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 29 de febrero 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	82	400	318
2024	82		
Solicitud	82		
Incidencia	0		
Total Horas Casos Reportados Netsuite	82	400	318
		318	318
		318	318
		318	318
		318	318
Horas consumidasde las 400 - Exp	400	400	0

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

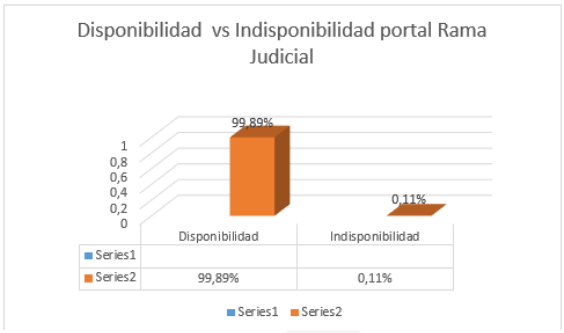
Etiquetas de fila	Suma de Horas Hombre	Horas Presupuesto	Horas Disponibles
CASO	0	100	100
2023	0		
WA	0		
MF	0		
Total Horas Casos Reportados Netsuite	0	100	100
Total Horas Consumidas de las 100 - Exp	0	100	100

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

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

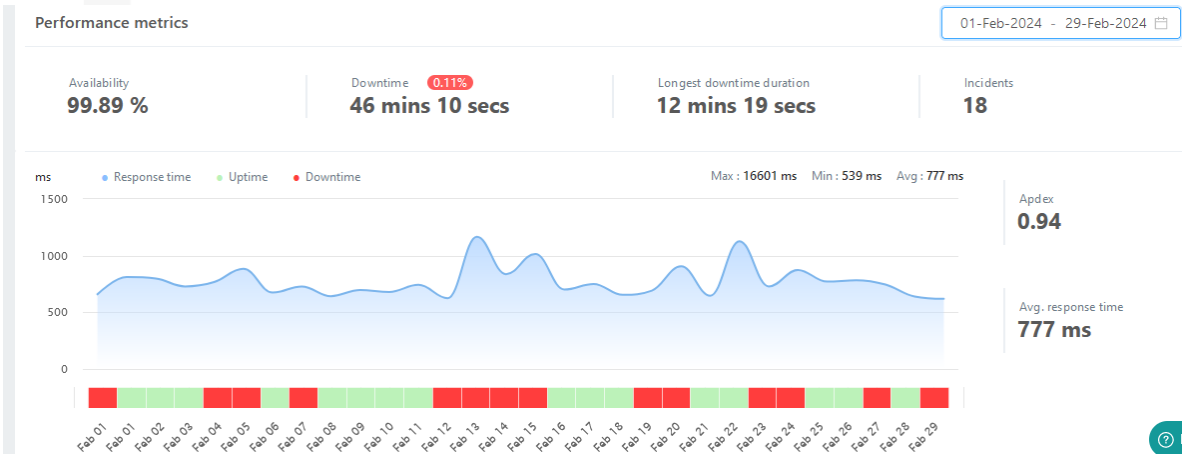
Se visualiza a través de la siguiente matriz los datos de disponibilidad, indisponibilidad y tiempo de caída de las aplicaciones que están soportadas al Consejo Superior de la Judicatura:

Item	Aplicación	Disponibilidad	Indisponibilidad	Tiempo de duracion (Caida en horas)	Tiempo de duracion			
					Dias	Horas	Minutos	Segundos
1	Portal de la Rama Judicial	99,89%	0,11%	0,769444444	0	0	46	10
	Totales	99,89%	0,11%	0,769444444	**0**	0	46	10



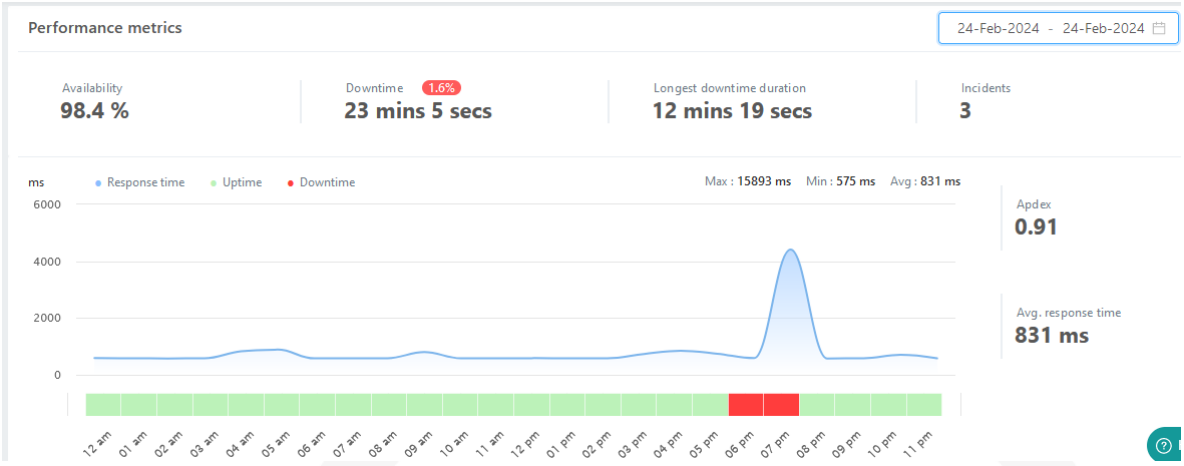
3.2 PORTAL DE LA RAMA JUDICIAL

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



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

% de Disponibilidad: 99,89%
% de Indisponibilidad: 0,11%
Tiempo total de eventos del mes: 46 minuto 10 segundos
Promedio en el tiempo de respuesta que tuvo el portal: 777 ms



Fecha: sábado 24 de febrero
% de Disponibilidad: 98,4%
% de Indisponibilidad: 1,6%
Numero de eventos: 3
Tiempo total de eventos: 23 minuto 5 segundos
Promedio en el tiempo de respuesta que tuvo el portal: 831 ms
Se produjeron 3 eventos durante el sábado 24 de febrero, pero el mismo tubo un restablecimiento automático, sin generar afectación a los usuarios.

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

A través del presente drive https://drive.google.com/drive/folders/1kZx3eIpxxGU_0HqLd7aqEiZ3ie4En1CD?usp=sharing se cargan las certificaciones y están ubicadas las del mes de febrero 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

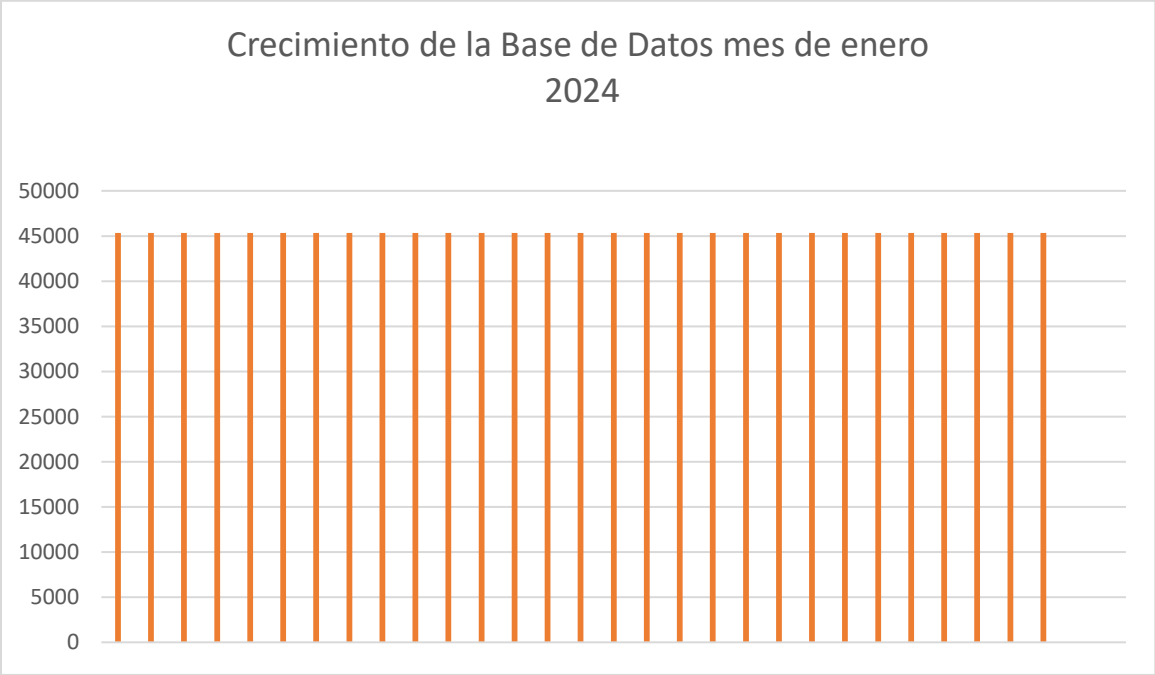
De acuerdo con la solicitud escalada en el **caso TT520553 RV: Crecimiento de la BD de la maquina CSJPORTALDB01** del portal de rama judicial, se agrega el presente informe consolidado del crecimiento que tuvo la BD en el mes de febrero.

BASE DE DATOS lportalramaprod

TAMAÑO (MB0	FECHA	AUMENTO TAMAÑO (MB) POR DIA
3091309 MB	2024-02-01	0
3091309 MB	2024-02-02	0
3091309 MB	2024-02-03	0
3091309 MB	2024-02-04	0
3091309 MB	2024-02-05	0
3091309 MB	2024-02-06	0
3091309 MB	2024-02-07	0
3091309 MB	2024-02-08	0
3091309 MB	2024-02-09	0
3091309 MB	2024-02-10	0
3091309 MB	2024-02-11	0
3091309 MB	2024-02-12	0
3091309 MB	2024-02-13	0
3091309 MB	2024-02-14	0
3091309 MB	2024-02-15	0
3091309 MB	2024-02-16	0
3091309 MB	2024-02-17	0
3091309 MB	2024-02-18	0
3091309 MB	2024-02-19	0
3091309 MB	2024-02-20	0
3091309 MB	2024-02-21	0
3091309 MB	2024-02-22	0
3091309 MB	2024-02-23	0
3091309 MB	2024-02-24	0
3091309 MB	2024-02-25	0
3091309 MB	2024-02-26	0

3091309 MB	2024-02-27	0
3091309 MB	2024-02-28	0
3091309 MB	2024-02-29	0

Grafica del crecimiento de la BD Iportalramaprod de la INSTANCIA CSJPORTALB01



4. ESTADISTICAS PORTAL DE LA RAMA JUDICIAL

4.1 RESUMEN DEL PORTAL

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

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

A continuación, encontrará una explicación más detallada de los términos que suelen ser objeto de confusión.

- Clics y visitas
- Visitas y usuarios y usuarios únicos absolutos
- Visitas de página y visitas de página únicas

Clics y visitas

Existe una importante diferencia entre clics (como los que se recogen en el informe "Campañas de AdWords") y visitas (como las que se reflejan en los informes "Motores de búsqueda" y "Usuarios"). La columna "clics" de sus informes indica las veces que los usuarios han hecho clic en sus publicaciones, mientras que la columna "visitas" señala las sesiones únicas que han iniciado los usuarios. Existen varios motivos por los que tal vez no coincidan estas dos cantidades:

•Un usuario puede hacer clic en su publicación varias veces. Cuando esto sucede dentro de la misma sesión, AdWords registra varios clics, mientras que Google Analytics identifica las distintas visitas de página como una sola visita.

Esto ocurre con frecuencia entre los usuarios que comparan los productos que van a comprar.

• Un usuario puede hacer clic en una publicación y, más tarde, durante una sesión diferente, volver directamente al sitio a través de un marcador. En este caso, se guardará la información de referencia de la visita original, de manera que el clic se convertirá en varias visitas.

• Un usuario puede hacer clic en su publicación, pero impedir que la página se cargue por completo si decide acceder a otra página o pulsar el botón "Detener" del navegador. En este caso, el código de seguimiento de Google Analytics es incapaz de ejecutar o enviar datos de seguimiento a los servidores de Google. Sin embargo, AdWords registrará un clic.

• Para poder garantizar una facturación más exacta, AdWords de Google filtra automáticamente los clics de sus informes que no son válidos. Sin embargo, los informes de Google Analytics incluyen estos clics como visitas realizadas a su sitio web para mostrar todo el conjunto de datos de tráfico.

Visitas y usuarios y usuarios únicos absolutos

Google Analytics realiza un recuento tanto de las visitas como de los usuarios en su cuenta. Las visitas representan el número de sesiones individuales iniciadas por todos los usuarios para llegar a su sitio web. Si un usuario permanece inactivo en su sitio durante al menos 30 minutos, toda actividad posterior se atribuirá a una nueva sesión. Los usuarios que abandonen su sitio y vuelvan en menos de 30 minutos se considerarán como parte de la sesión inicial.

El usuario es un término utilizado para definir con la máxima precisión el número de personas distintas y reales que visitan un sitio web. Evidentemente, no existe modo alguno de saber si dos personas comparten un equipo desde la perspectiva del sitio web, pero un buen sistema de seguimiento de usuarios puede aproximarse mucho a la cifra real. Los sistemas más precisos normalmente emplean cookies para realizar el recuento de usuarios diferentes.

Los "usuarios" representan el número diario de usuarios únicos que visitan su sitio web. Todas las sesiones de un mismo usuario iniciadas durante un mismo día se agregarán a un usuario único, aunque pueden representar dos o más visitas diferentes.

En el informe "Usuario único absoluto", se añadirán todas las visitas del mismo usuario realizadas en el intervalo de tiempo activo completo que haya seleccionado, de manera que se contabilizarán como un usuario único

absoluto, independientemente del número de días que haya visitado su sitio y las veces que lo haya hecho cada día.

Visitas de página y visitas de página únicas

Una visita de página hace referencia a la visualización de una página de su sitio web que el código de seguimiento de Google Analytics está controlando. Si un usuario vuelve a cargar la página después de que se haya cargado completamente, esto contará como una visita de página adicional. Si un usuario navega a una página diferente y más tarde vuelve a la página original, se registrará también una segunda visita de página.

Una visita de página única, tal y como aparece en el informe "Contenido principal", integra las visitas de páginas que genera el mismo usuario durante la misma sesión. Una visita de página única representa el número de sesiones durante las cuales se ha visitado esa página al menos una vez.

Porcentaje de rebote

El porcentaje de rebote el porcentaje de visitas a una sola página o visitas en las que el usuario ha abandonado su sitio desde la página de acceso (destino).

Use este indicador para evaluar la calidad de las visitas; En caso de presentar un porcentaje elevado, significa que los usuarios no valoran como relevantes las páginas de acceso al sitio.

Cuanto más atractivas resulten las páginas de destino, más usuarios permanecerán en el sitio y se convertirán en clientes. Para lograr reducir el porcentaje de rebote, intente adaptar las páginas de destino a cada una de las palmayas clave y las publicaciones que publica. Estas páginas deberían proporcionar la información y los servicios mencionados en el texto del anuncio.

5. ESQUEMA DE SEGURIDAD

ITEM OC	DESCRIPCIÓN	SEDE DE UBICACIÓN
27	npn03--IaaS Procesamiento - Balanceador de Carga Media Capacidad - Oro - Hosting Físico - RAM entre 16GB y 32GB - U_Mes - Cantidad: 1	Jupiter Data
28	npn03--IaaS Procesamiento - Balanceador de Carga Media Capacidad - Oro - Hosting Físico - - RAM entre 16GB y 32GB - U_Mes - Cantidad: 1	Jupiter Data
95	npn03--IaaS Seguridad - Appliance Anti Ddos - Alta Capacidad - Oro - Hosting físico - Rol de Inspección - 30 Gbps - Paquetes Por Segundo (MPPS) - 25000000 - Mes - Cantidad: 1	Jupiter Data
96	npn03--IaaS Seguridad - Appliance Anti Ddos - Alta Capacidad - Oro - Hosting físico - Rol de Inspección - 30 Gbps - Paquetes Por Segundo (MPPS) - 25000000 - Mes - Cantidad: 1	Jupiter Data
97	npn03--IaaS Seguridad - Web Aplication Firewall - Alta Capacidad - Oro - Hosting físico - Desempeño WAF (Gbps) - 10 - Mes - Cantidad: 1	Jupiter Data
98	npn03--IaaS Seguridad - Web Aplication Firewall - Alta Capacidad - Oro - Hosting físico - Desempeño WAF (Gbps) - 10 - Mes - Cantidad: 1	Jupiter Data

99	npn03--IaaS Seguridad - Web Aplication Firewall - Alta Capacidad - Oro - Hosting físico - Desempeño WAF (Gbps) - 10 - Mes - Cantidad: 1	Datacenter CAN
100	npn03--IaaS Seguridad - Firewall Nueva Generación - Alta Capacidad - Oro - Hosting físico - Rol de Firewall - 500 Gbps - Sesiones Concurrentes - 100000000 - Mes - Cantidad: 1	Jupiter Data
101	npn03--IaaS Seguridad - Firewall Nueva Generación - Alta Capacidad - Oro - Hosting físico - Rol de Firewall - 500 Gbps - Sesiones Concurrentes - 100000000 - Mes - Cantidad: 1	Jupiter Data
154	npn03--Servicios Complementarios - Experto Master - Región 1 - Hora/M - Cantidad: 160	Transversales a servicios de SP
155	npn03--Servicios Complementarios - Experto Senior - Región 1 - Hora/M - Cantidad: 160	Transversales a servicios de SP
158	npn03--IaaS Seguridad - Firewall Nueva Generación - Media Alta Capacidad - Oro - Hosting físico - 100 Gbps - Sesiones Concurrentes - 45000000 - Mes - Cantidad: 1	Palacio de Justicia
159	npn03--IaaS Seguridad - Firewall Nueva Generación - Media Alta Capacidad - Oro - Hosting físico - 100 Gbps - Sesiones Concurrentes - 45000000 - Mes - Cantidad: 1	Palacio de Justicia

14.1. Horas experto de los ítems 154, 155 y esquema de compensación.

El servicio de experto es prestado por los siguientes dos 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	2/21/2024 21:00	2/21/2024 22:00	1:00:00	Diurna ordinaria	TT798550 PARCHADOS MES DE FEBRERO
2					
3					
Total horas Extras			1:00:00		

Ingeniero Residente:	Victor Galvis				
Item	**Fecha y Hora de inicio**	**Fecha y Hora de finalización**	**Cantidad de Horas**	**Tipo de Hora extra**	**Actividad Realizada**
1	10/2/2024 20:00	10/2/2024 12:00	4:00:00 AM	Nocturna	TT793558 Ventana de reinicio Hub's Meraki
2	15/2/2024 9:00:00 PM	15/2/2024 11:00:00 PM	2:00:00 AM	Nocturna	Ventana Router de Datos Palacio de Justicia
3	16/2/2024 6:00:00 PM	16/2/2024 7:00:00 PM	1:00:00 AM	Diurna	SALIDA A PRODUCCION CPNU - AZURE
4	24/2/2024 5:00:00 PM	24/2/2024 9:00:00 PM	4:00:00 AM	Diurna	Actualización Firewall TC Verssion 7.0.14
8					
Total horas Extras			11:00:00		

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	24/2/2024 5:00:00 PM	24/2/2024 9:00:00 PM	4:00:00 AM	Diurna	Actualización Firewall TC Verssion 7.0.14
2	24/2/2024 9:00:00 PM	24/2/2024 11:00:00 PM	2:00:00 AM	Nocturna	Revision Fallas de Monitoreo de Equipos despues de Actualizacion de Firewall de Torre Central
3	24/2/2024 11:00:00 PM	24/2/2024 12:00:00 PM	1:00:00 AM	Nocturna	TT800487 RV: Solicitud de Permisos de Navegación RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA TT800489 RV: SOLICITUD PERMISOS DE NAVEGACIÓN SANTIAGO HERNÁN RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA TT800491 RV: SOLICITUD PERMISOS DE NAVEGACIÒN RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA
4	26/2/2024 6:00:00 PM	26/2/2024 8:00:00 PM	2:00:00 AM	Nocturna	Verificación de fallas del aplicativo: https://tierrasv3-test.ramajudicial.gov.co/#/
5	27/2/2024 8:00:00 PM	27/2/2024 12:00:00 PM	4:00:00 AM	Nocturna	TT793558 Ventana de reinicio Hub's Meraki
5	28/2/2024 11:00:00 PM	28/2/2024 12:00:00 PM	1:00:00 AM	Nocturna	TT802298: alarma proactivo: multiples alarmas RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA
5	29/2/2024 11:00:00 PM	29/2/2024 12:00:00 PM	1:00:00 AM	Nocturna	TT802298: alarma proactivo: multiples alarmas RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA
Total horas Extras			15:00:00		

14.2. Inventario de equipos de seguridad perimetral.

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

Nº	Descripción	Hostname	Serial	SID	Ubicación	Version Firmware
1	FortiGate-4400F HA	FTG_CSJ_DC_TC_MASTER	FG440FTK21900184	2082019	DC IFX	v7.0.14
		FTG_CSJ_DC_TC_SLAVE	FG440FTK21900183	2082018	DC IFX	v7.0.14
2	FORTIADC 2200F HA	FADC_CSJ_TC_MASTER	FAD22FT221000027	2081818	DC IFX	v6.1.3
		FADC_CSJ_TC_ SLAVE	FAD22FT221000028	2081817	DC IFX	v6.1.3
3	WAF KEMP Loadmaster x25 HA	WAF_TORRRE_CENTRAL	TSCC82005608	2082013	DC IFX	V7.2.59.0.22007
		WAF_TORRRE_CENTRAL	TSCC8200529	2082014	DC IFX	V7.2.59.0.22007
4	Fortigate 3500F HA	FGT_3500F_CSJ_PALACIO_M	FG3K5FTB21900137	2082016	PALACIO	V7.2.6
		FGT_3500F_CSJ_PALACIO_S	FG3K5FTB21900138	2082017	PALACIO	V7.2.6
5	WAF KEMP Loadmaster x25	WAF_CAN	TSCC82005629	2082015	CAN	V7.2.59.0.22007
6	FortiDDos 1500F HA	CSJ_FDDoS_MASTER	FI1K5FTE20000012	2082020	DC IFX	v6.3.3
		CSJ_FDDoS_SLAVE	FI1K5FTE20000011	2082021	DC IFX	v6.3.3

14.3. Actualización de firmware.

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

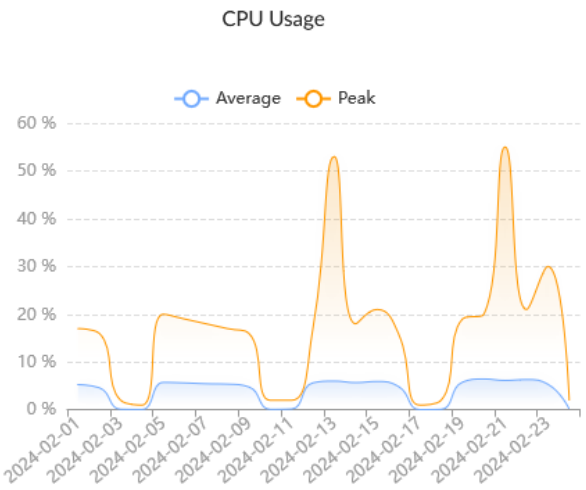
Equipos	Versión Firmware	Fecha de Ejecucion	Versión Por Actualizar
FTG_CSJ_DC_TC_MASTER	V7.0.14	Actualizado	N/A
FTG_CSJ_DC_TC_SLAVE	v7.0.14	Actualizado	N/A
FADC_CSJ_TC_MASTER	V6.1.3	Por definir	V7.1.0
FADC_CSJ_TC_MASTER	V6.1.3	Por definir	V7.1.0
WAF_TORRRE_CENTRAL KEMP	V7.2.59.0.22007	Actualizado	N/A
WAF_TORRRE_CENTRAL KEMP	V7.2.59.0.22007	Actualizado	N/A
FGT_3500F_CSJ_PALACIO_M	V7.2.6	Actualizado	N/A
FGT_3500F_CSJ_PALACIO_S	V7.2.6	Actualizado	N/A
WAF_CAN KEMP	V7.2.59.0.22007	Actualizado	N/A
CSJ_FDDoS_MASTER	V6.3.3	Actualizado	N/A
CSJ_FDDoS_SLAVE	v6.3.3	Actualizado	N/A

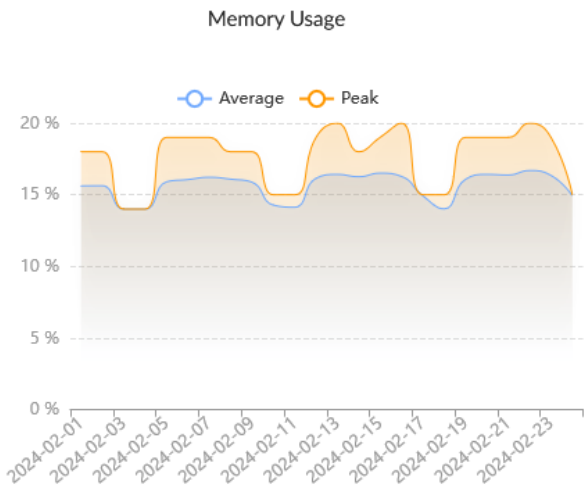
6. FIREWALL PERIMETRAL

Durante febrero, el consumo promedio de CPU y memoria en el Firewall perimetral se mantuvieron dentro de los valores de operación normal. El día 24 de febrero se

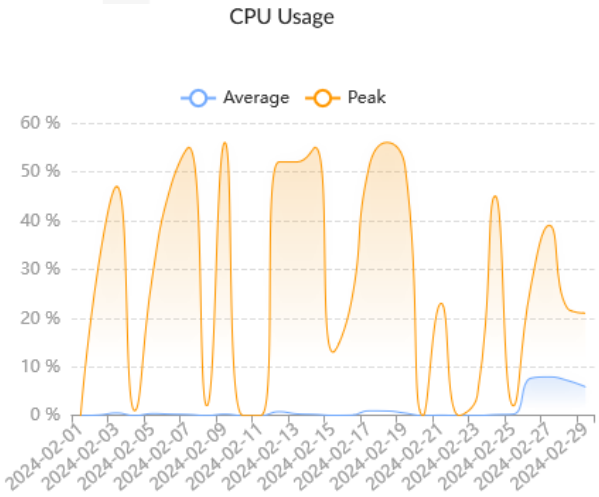
realizó actualización del firewall de Torre Central y se realizó conmutación de equipo Activo, del Esclavo al Maestro:

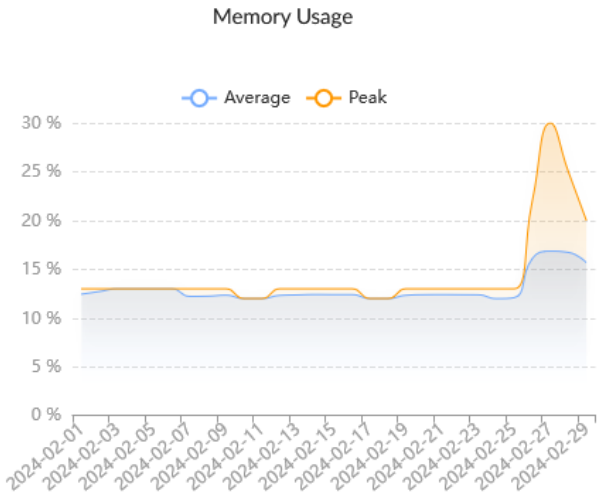
Equipo Esclavo: FG440FTK21900183





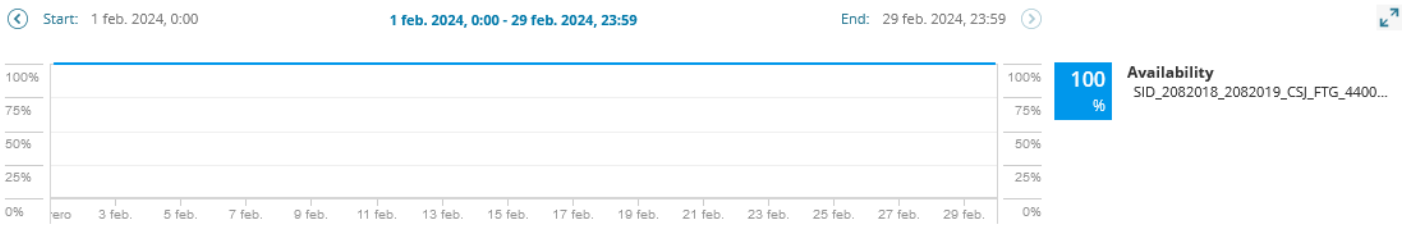
Equipo Maestro: FG440FTK21900184





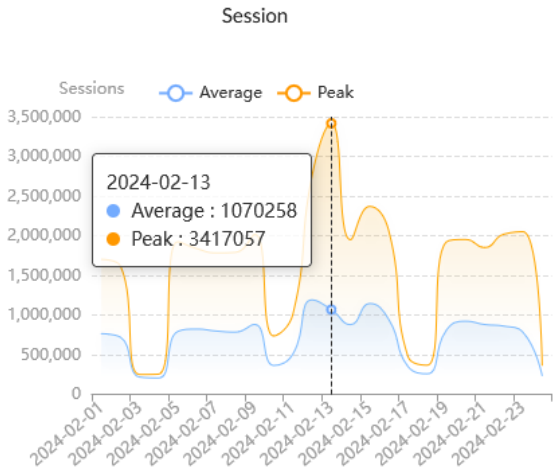
15.1. Disponibilidad mensual firewall perimetral.

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



15.2. Cantidad de sesiones firewall perimetral.

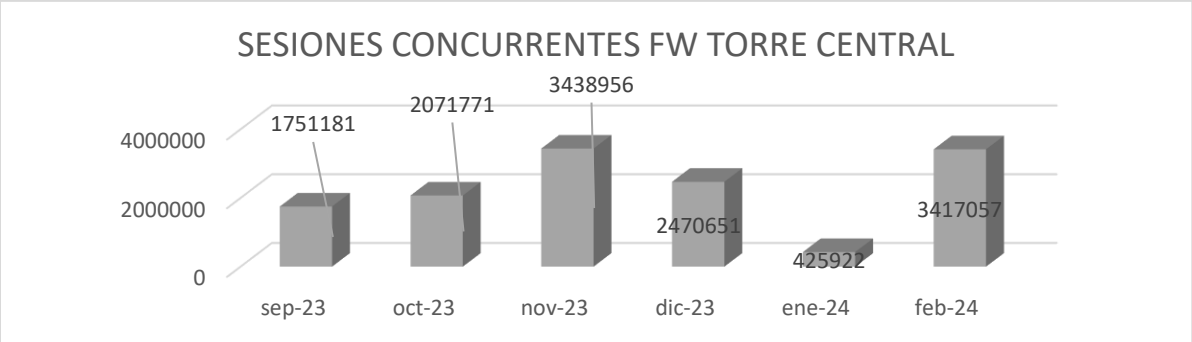
Durante febrero se presentó un máximo de 3.417.057 sesiones concurrentes TCP, cantidad que se encuentra dentro del rango máximo soportado por el equipo Fortinet FG- 4400F cuyo valor es de 210 millones.



MES	SESIONES
sep-23	1751181
oct-23	2071771
nov-23	3438956
dic-23	2470651
ene-24	425922
feb-24	3417057

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

En el último mes se presentó aumento en las sesiones en el FW perimetral:



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

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

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	HTTPS			249.15 TB
2	Microsoft.SharePoint			59.72 TB
3	DTLS			47.87 TB
4	SMB			45.63 TB
5	SSL			40.93 TB
6	Microsoft.Portal			29.22 TB
7	TCP/9443			25.53 TB
8	Microsoft.365.Portal			23.35 TB
9	Amazon-AWS			17.18 TB
10	Akamai-CDN			15.93 TB

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

Top Applications by Sessions

#	Application	Sessions
1	SMB	2,826,820,404
2	DNS	2,512,644,615
3	HTTPS	1,596,350,562
4	SSL	797,973,347
5	Microsoft.Windows.Update	673,697,829
6	HTTP	539,067,263
7	NTP	513,599,440
8	Microsoft.Portal	489,956,161
9	Microsoft-Office365	401,133,550
10	TCP/448	353,056,328

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

La IP 10.101.100.38 de la sede Popayán Palacio de Justicia tuvo la mayor cantidad de sesiones:

Top Bandwidth IP

#	IP	Bandwidth
1	10.101.100.38	2.27 TB
2	10.101.100.114	2.01 TB
3	10.101.100.34	1.93 TB
4	10.101.100.182	1.51 TB
5	10.101.100.122	1.29 TB
6	10.101.100.70	1.12 TB
7	10.101.100.134	930.95 GB
8	10.101.100.110	828.40 GB
9	10.101.101.178	805.69 GB
10	10.101.100.138	779.10 GB

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

Los destinos en Internet con mayor consumo de ancho de banda durante febrero fueron 8.243.164.19 (rns1co.cirion.live), microsoft.com y 190.217.24.155 (HoneyPot2):

Top Destinations by Sessions

#	Hostname(or IP)	Sessions
1	8.243.164.19	528,169,674
2	microsoft.com	392,881,969
3	190.217.24.155	314,865,200
4	200.31.13.169	266,606,927
5	rapid7.com	231,006,898
6	192.168.213.94	209,517,712
7	8.243.164.21	208,477,808
8	190.217.24.69	200,917,949
9	40.68.123.157	191,300,507
10	windowsupdate.com	178,686,811

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

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

Top Web Users by Blocked Requests

#	User (or IP)	Hostname	Requests
1	172.16.155.37	172.16.155.37	12,454,766
2	172.26.176.6	172.26.176.6	6,425,262
3	172.16.228.170	172.16.228.170	5,949,813
4	192.168.125.26	192.168.125.26	5,631,052
5	192.168.125.17	192.168.125.17	5,232,271
6	192.168.208.128	192.168.208.128	4,838,817
7	172.27.90.208	172.27.90.208	4,202,546
8	192.168.199.21	192.168.199.21	4,198,132
9	192.168.221.40	192.168.221.40	3,864,425
10	192.168.66.79	192.168.66.79	3,751,050

Se recomienda verificar los equipos en lista para que no continúen intentando conexiones a destinos bloqueados por el firewall perimetral y se descarte software malicioso instalado intentando hacer estas conexiones.

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

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

Top Blocked Web Categories

#	Category	Requests
1	Internet Radio and TV	135,323,213
2	Streaming Media and Download	6,338,768
3	Social Networking	3,959,620
4	Information Technology	3,690,034
5	Proxy Avoidance	2,998,267
6	Games	2,843,826
7	Malicious Websites	999,078
8	Entertainment	971,570
9	Unrated	684,055
10	Hacking	264,753

15.9. Top de IP más activos Firewall Perimetral

Los hosts con mayor cantidad de peticiones durante febrero fueron del host con ip 172.16.23.85:

Top Web IP by Allowed Requests

#	IP	Requests
1	172.16.23.85	17,865,215
2	172.16.181.39	13,814,079
3	10.101.100.114	5,972,744
4	172.17.132.228	5,621,577
5	172.27.121.163	5,612,238
6	10.101.100.38	5,469,332
7	192.168.74.54	5,445,708
8	10.101.100.34	4,559,626
9	192.168.32.223	4,184,378
10	10.101.100.122	3,906,558

15.10. Top de categorías más visitadas Firewall Perimetral

La categoría más visitada durante febrero fueron Information Technology:

Top Allowed Web Categories

#	Category	Requests
1	Information Technology	567,382,100
2	Overrride_permitidas	71,515,109
3	Streaming Media and Download	105
4	Unrated	7

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

172.17.201.251 (WAF de Torre Central) y usrsigobius, 172.27.64.17 (Servidor de grabaciones) presentaron el mayor consumo de ancho de banda durante febrero:

Top IP by Bandwidth

#	IP	Bandwidth	Sent	Received
1	172.17.201.251			89.69 TB
2	172.27.64.17			32.39 TB
3	10.244.2.239			13.81 TB
4	172.17.201.252			11.99 TB
5	erubianr			9.39 TB
6	172.16.120.18			8.74 TB
7	usrsigobius			8.51 TB
8	172.27.64.61			7.77 TB
9	172.25.201.6			5.30 TB
10	190.60.84.6			4.29 TB

7. TRÁFICO VPN FIREWALL PERIMETRAL

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

#	f_user	devname	vpn_type_group	end_time	fv_dtime_tz_conv_e_time_t	remip	connections	Duration	bandwidth	traffic_in	traffic_out
1	cvillam	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-03-02 23:58:47	1709423927	181.55.51.20	51	1134407	3273886090	381833187	2892052903
2	jariasu	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-03-02 22:10:18	1709417418	181.137.8.129	46	1055894	1094146830	181617683	912529147
3	lmarinmo	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-03-01 06:19:53	1709273993	191.91.108.168	49	1043689	649401965	64519792	584882173
4	msantamm	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel;ssl-web	2024-03-02 23:27:13	1709422033	179.15.132.52;191.95.46.72	60	780863	180786830	14700483	166086347
5	Ecoralb	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-03-02 23:57:56	1709423876	186.28.24.209;186.30.82.109;190.26.174.34	1029	756918	183434	98982	84452
6	j01epenladorada@cendoj.ramajudicial.gov.co	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-03-03 00:00:18	1709424018	172.25.26.146	56	746183	14999614	11689832	3309782
7	ssuareza	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-03-02 23:59:00	1709423940	181.58.39.159;181.58.39.249;181.58.39.30;181.58.39.86	106	703824	14019726883	933531339	13086195544

#	f_user	devname	vpn_type_group	end_time	fv_dtime_tz_conv_e_time_t	remip	connections	Duration	bandwidth	traffic_in	traffic_out
8	csichaca	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-03-02 23:52:58	1709423578	186.102.22.30;186.102.24.240;186.102.3.89;186.102.35.95;186.102.37.136;186.102.67.217;186.114.103.237;186.84.22.195	66	687145	5800209649	54479269	5255416959
9	fleonc	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel;ssl-web	2024-03-02 20:46:22	1709412382	186.29.168.99;186.30.79.217	52	680769	20255689	0	20255689
10	omunozch	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-03-02 17:34:24	1709400864	181.235.135.114;181.235.141.196;181.235.193.98	39	635659	28304521088	930001329	27374519759

16.1. VPN IPSEC Site To Site Firewall Perimetral

El consumo de ancho de banda de las VPN IPSec Site to Site durante febrero 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	2405120	40551659018142	5574656195364	34977002822778
2	VPN_ORACLE	129.213.6.36	190.217.80.4	2403624	2167796664462	2076779632565	91017031897
3	VPN_ORACLE	129.213.7.34	190.217.80.4	2404767	2091135545169	2089946404979	1189140190
4	VPN_AZURE-ANALY	20.124.34.235	190.217.24.4	2405175	509636436147	8968437433	500667998714
5	VPN_Tierras	181.225.76.196	190.217.24.4	2400508	24798727357	24068039358	730687999
6	VPN_INPEC	190.25.112.10	190.217.19.156	2400308	884256883	740880156	143376727
7	VPN_REGISTRADU	201.232.123.20	190.217.24.4	2406359	769310401	328572099	440738302
8	VPN_SIUG_AWS	34.194.187.190	190.217.24.4	1516936	556404432	314339600	242064832
9	VPN_SIUG_AWS-2	34.224.152.152	190.217.24.4	1516360	556088992	314203096	241885896
10	VPN_Linktic	3.222.171.115	190.217.24.4	2405431	529562748	295114119	234448629
11	OCI_EXADATA_FAB	150.136.25.96	190.217.24.4	2403753	103986584	0	103986584
12	VPN_FISCALIA	190.157.218.66	190.217.24.4	2400851	84986527	81347844	3638683

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

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

Top Attacks

#	Attack Name	Severity	CVE-ID	Counts
1	tcp_syn_flood	Critical		306,590
2	tcp_src_session	Critical		305,461
3	tcp_port_scan	Critical		83,794
4	ip_src_session	Critical		61,230
5	tcp_dst_session	Critical		13,609
6	Spring.Framework.SerializationUtils.Insecure.Deserialization	Critical	CVE-2022-22965	6,983
7	Apache.Log4j.Error.Log.Remote.Code.Execution	Critical	CVE-2021-4104,CVE-2021-44228,CVE-2021-45046	5,174
8	Andromeda.Botnet	Critical		4,329
9	Andromeda	Critical		2,983
10	Backdoor.DoublePulsar	Critical		2,422

Las víctimas de intrusión fueron los siguientes hosts:

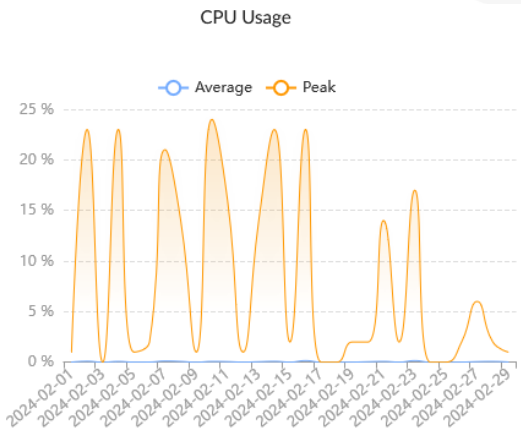
Top Intrusion Victims

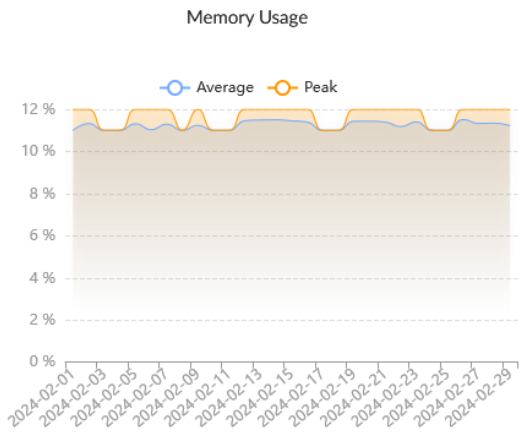
#	Attack Victim	Counts (Critical / High / Medium)	Percent of Total Attacks
1	190.217.24.69	204,552	20.01%
2	172.17.201.26	198,934	19.46%
3	172.17.201.52	178,667	17.48%
4	172.17.201.68	152,553	14.93%
5	190.217.24.172	148,323	14.51%
6	190.217.24.149	37,572	3.68%
7	172.17.201.25	31,673	3.10%
8	161.18.255.202	21,143	2.07%
9	181.131.217.74	16,648	1.63%
10	185.196.10.85	9,645	0.94%
11	172.17.201.7	2,899	0.28%
12	172.16.2.15	2,887	0.28%
13	190.67.192.234	2,754	0.27%
14	181.55.68.10	2,577	0.25%
15	172.17.201.54	2,009	0.20%
16	186.144.72.156	1,989	0.19%
17	186.118.229.60	1,938	0.19%
18	181.140.165.34	1,838	0.18%
19	192.169.69.26	1,724	0.17%
20	192.168.213.110	1,713	0.17%

Los hosts 190.217.24.69,172.17.201.x y 172.17.202.x son las aplicaciones web, sin embargo, están siendo protegidas por los WAF de Torre Central y del CAN.

8. FIREWALL SEDE PALACIO

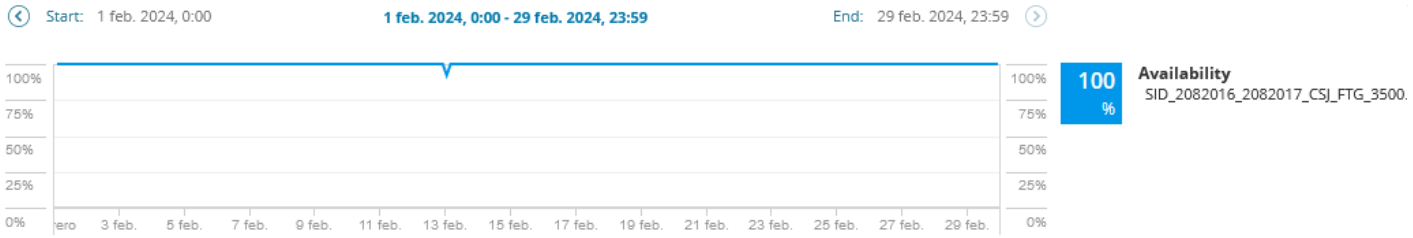
Durante febrero, el Consumo de CPU y memoria en el Firewall de Palacio se mantuvieron dentro de los valores de operación normal.





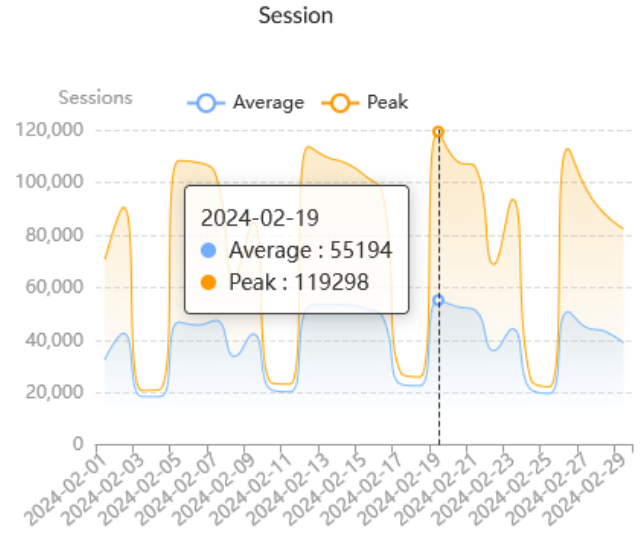
8.1 Disponibilidad Mensual Firewall Palacio

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



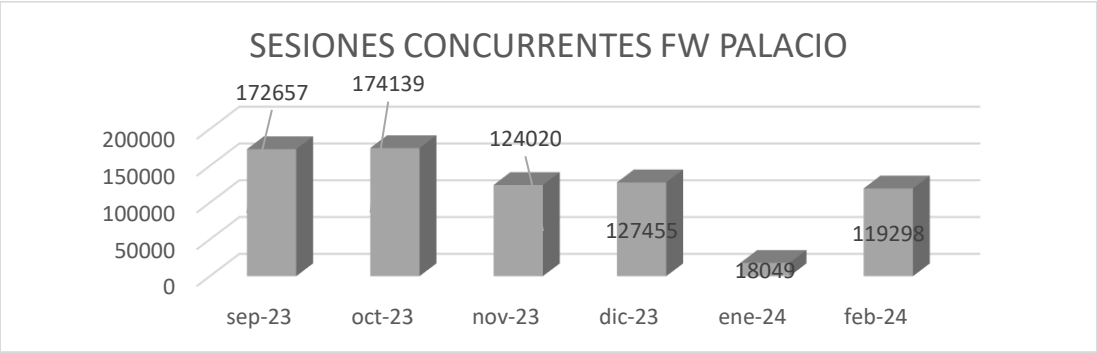
8.2 Cantidad de Sesiones Firewall Palacio

Durante febrero se presentó un máximo de 119298 sesiones concurrentes que están dentro del rango de sesiones soportadas por el equipo Fortigate 3500F de 160 Millones.



8.3 Histórico de Sesiones Últimos 6 meses Firewall Palacio

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



MES	SESIONES
sep-23	172657
oct-23	174139
nov-23	124020

dic-23	127455
ene-24	18049
feb-24	119298

8.4 Aplicaciones y protocolos por ancho de banda firewall Palacio

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

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	Microsoft.Portal			10.31 TB
2	HTTPS			9.07 TB
3	Microsoft.SharePoint			4.71 TB
4	OneDrive			3.23 TB
5	HTTPS.BROWSER			3.17 TB
6	Lifesize			3.12 TB
7	SMB			2.86 TB
8	SSL			2.13 TB
9	MSSQL			1.88 TB
10	HTTP			1.75 TB

Por sesiones las aplicaciones con mayor consumo fue SMB:

Top Applications by Sessions

#	Application	Sessions
1	SMB	1,069,934,900
2	DNS	175,590,115
3	Microsoft.Windows.Update	44,924,336
4	other	42,373,804
5	SQUID	34,324,207
6	tcp/5508	33,288,055
7	HTTP.BROWSER	33,142,242
8	Microsoft.Portal	32,751,301
9	SSL	27,839,972
10	HTTP	26,486,690

8.5 Top de IP por ancho de banda firewall Palacio.

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

Top Bandwidth IP

#	IP	Bandwidth
1	172.28.93.2	6.70 TB
2	172.16.2.59	1.31 TB
3	172.16.4.53	739.26 GB
4	172.17.114.19	709.06 GB
5	172.28.93.202	304.49 GB
6	172.28.93.203	257.94 GB
7	172.16.4.193	253.07 GB
8	172.16.4.246	242.72 GB
9	172.28.93.180	238.45 GB
10	172.16.4.80	217.33 GB

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

El destino web más visitado durante febrero fue 20.60.0.104 (Microsoft Corporation):

Top Websites and Category by Bandwidth

#	Site	Category	Bytes
1	20.60.0.104		4.01 TB
2	13.107.136.10		2.86 TB
3	13.107.138.10		2.58 TB
4	cndjdisciplinaenlinea.file.core.windows.net		1.50 TB
5	20.60.62.8		1.19 TB
6	172.190.220.253		884.69 GB
7	52.104.3.39		882.44 GB
8	20.60.128.228		844.37 GB
9	20.168.235.216		429.81 GB
10	20.209.74.225		389.41 GB

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

Top Web Users by Blocked Requests

#	User (or IP)	Hostname	Requests
1	172.17.74.43	172.17.74.43	295,731
2	172.16.6.155	172.16.6.155	223,637
3	172.16.6.75	172.16.6.75	123,161
4	172.16.5.230	172.16.5.230	96,241
5	172.16.4.40	172.16.4.40	71,676
6	172.16.4.162	172.16.4.162	64,033
7	172.16.6.76	172.16.6.76	53,709
8	172.28.93.142	172.28.93.142	28,706
9	192.168.6.12	192.168.6.12	19,219
10	172.16.6.51	172.16.6.51	19,198

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

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

Top Blocked Web Categories

#	Category	Requests
1	Streaming Media and Download	877,396
2	Proxy Avoidance	576,125
3	Unrated	538,596
4	Malicious Websites	283,895
5	Social Networking	251,397
6	Games	72,854
7	Entertainment	49,964
8	Society and Lifestyles	10,855
9	Phishing	7,364
10	Spam URLs	4,141

8.9 Top de IP más activas Firewall Palacio

172.28.54.20, 172.16.4.90 (Servidor_AV) y 172.16.5.80 presentaron la mayor cantidad de conexiones durante febrero:

#	IP	Requests
1	172.28.54.20	13,097,429
2	172.16.4.90	10,548,645
3	172.16.5.80	1,441,894
4	172.16.4.43	1,225,484
5	172.16.4.246	794,316
6	172.28.93.45	681,719
7	172.17.114.240	363,572
8	172.28.93.90	356,312
9	172.17.114.75	350,993
10	172.16.6.121	345,719

8.10 Top de las categorías más visitadas firewall Palacio.

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

Top Allowed Web Categories

#	Category	Requests
1	Information Technology	38,737,195
2	Search Engines and Portals	6,338,708
3	Business	1,578,363
4	Information and Computer Security	580,287
5	Web Analytics	480,008
6	Web-based Applications	147,745
7	Finance and Banking	89,403
8	Online Meeting	88,076
9	Overrride_permitidas	27,465
10	Web Hosting	19,199

8.11 Top de consumo ancho de banda por usuario Firewall Palacio

172.17.201.251 (WAF Torre Central), 172.28.93.2, 10.101.250.4 (NAT en el Fw Torre Central para aplicaciones web) y 172.16.2.7 presentaron la mayor cantidad de tráfico durante febrero:

Top IP by Bandwidth

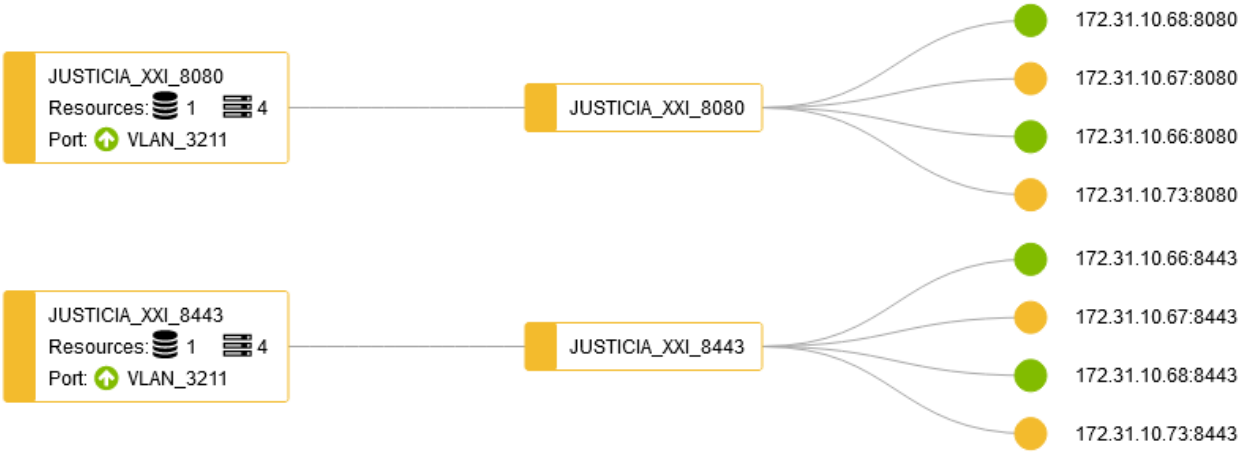
#	IP	Bandwidth	Sent	Received
1	172.17.201.251			6.87 TB
2	172.28.93.2			6.64 TB
3	10.101.250.4			2.63 TB
4	172.16.2.7			2.12 TB
5	172.16.4.121			1.56 TB
6	172.17.202.250			1.54 TB
7	172.16.2.59			1.42 TB
8	172.17.201.252			910.47 GB
9	172.16.4.162			793.91 GB
10	172.16.6.9			751.77 GB

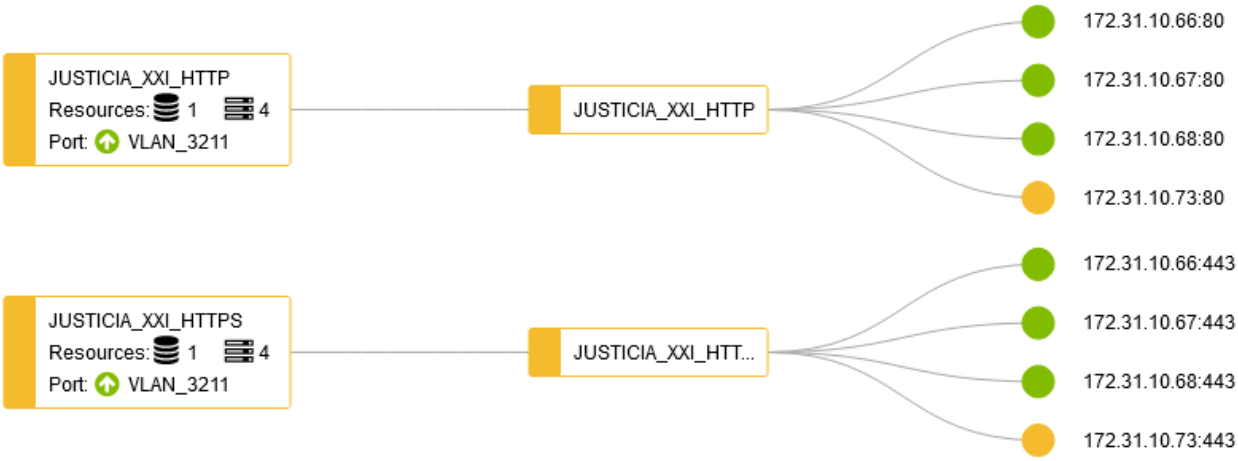
9. BALANCEADOR DE CARGA FORTIADC

A continuación, se observan los diferentes servicios balanceados.

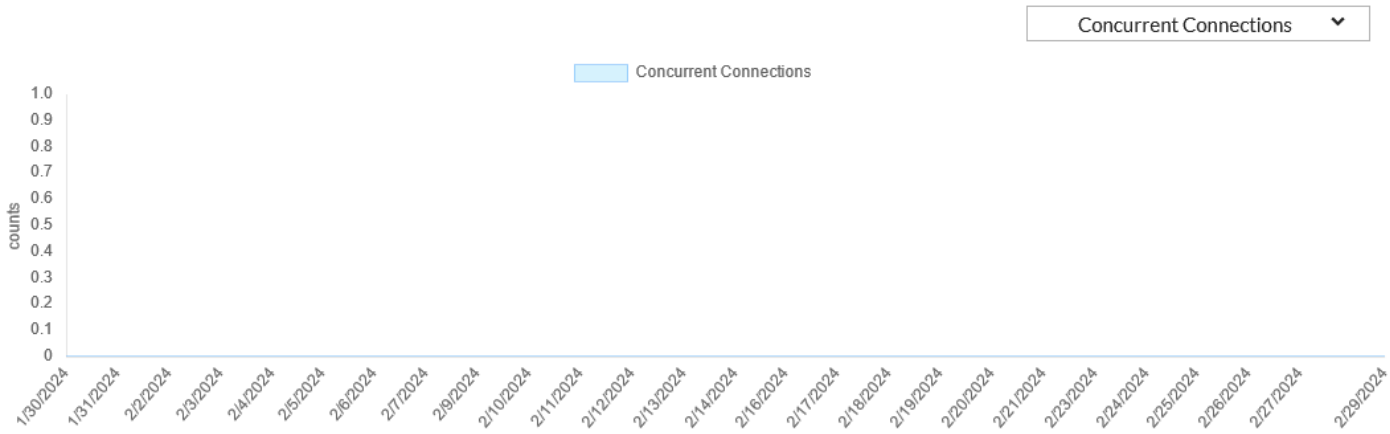
9.1 Justicia XXI

Se encuentra balanceado en el FortiADC:

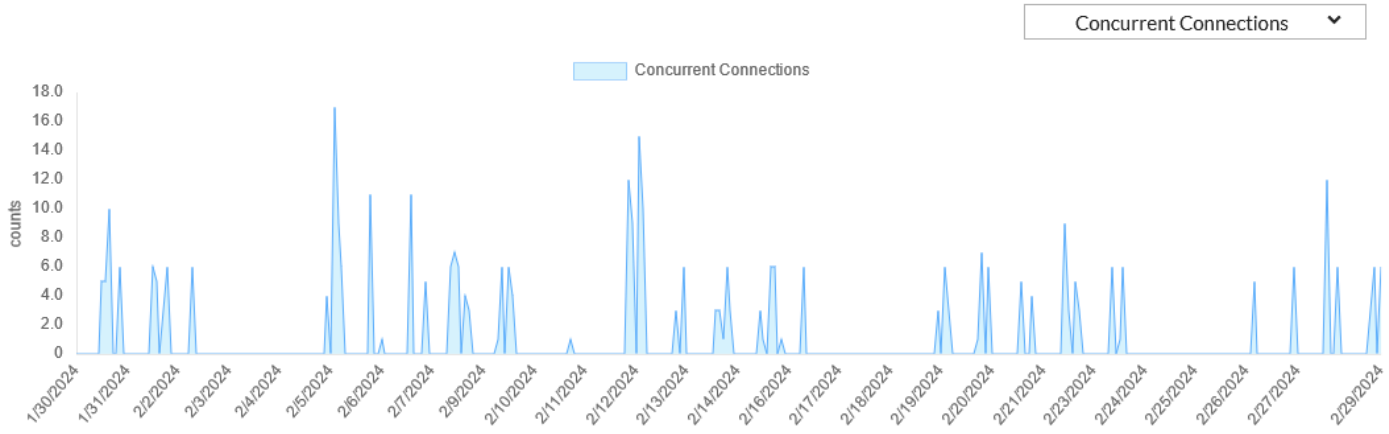




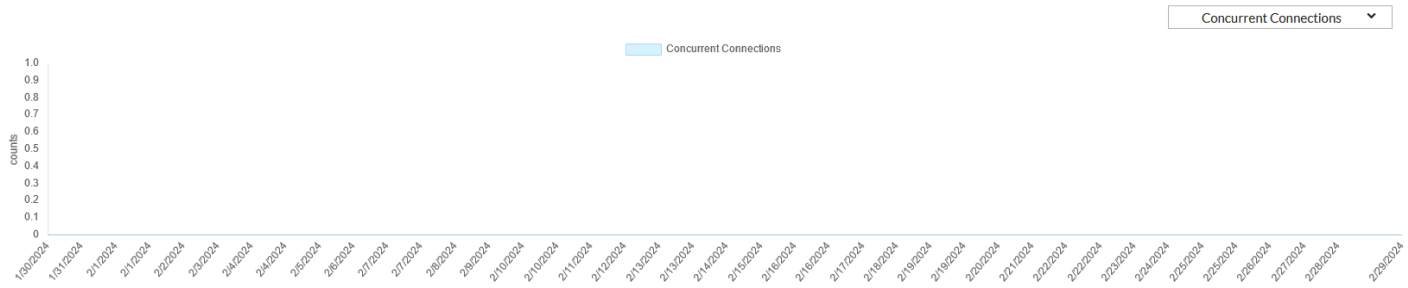
Durante febrero no se presentó tráfico por el puerto 8080:



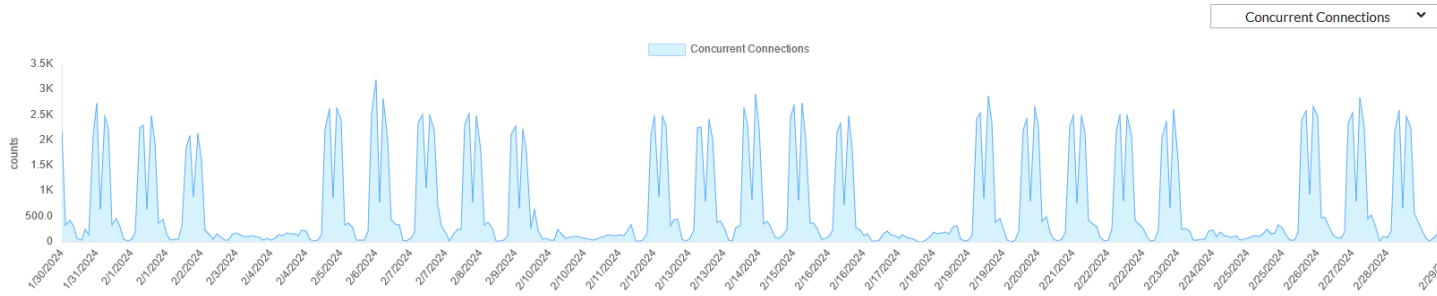
Conexiones concurrentes Virtual Server Justicia XXI con el puerto 8443:



Durante febrero no se presentó tráfico por el puerto 80:



Conexiones concurrentes Virtual Server Justicia XXI por el puerto 443:

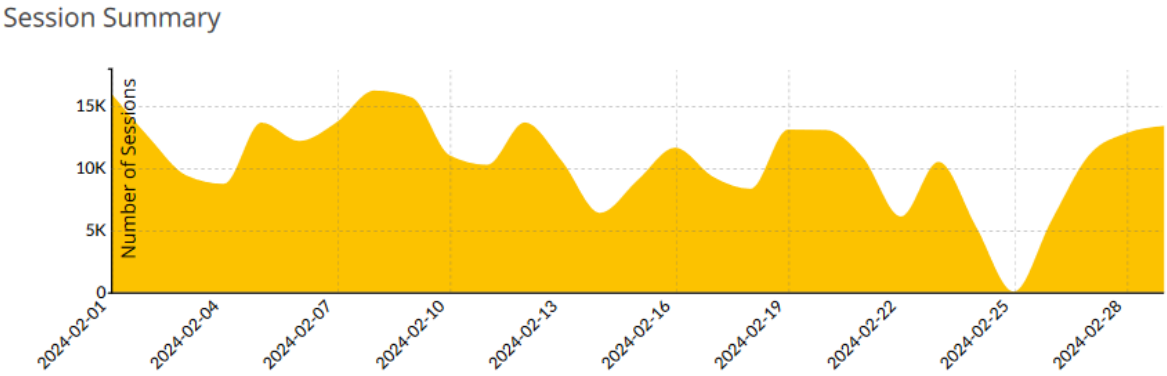


9.2 Kactus RDP

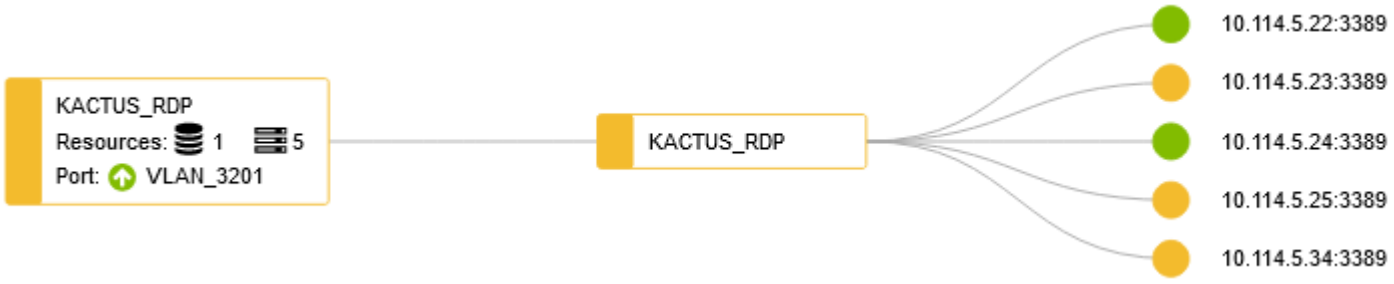
Esta aplicación se encuentra en el Firewall utilizando la siguiente configuración:

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

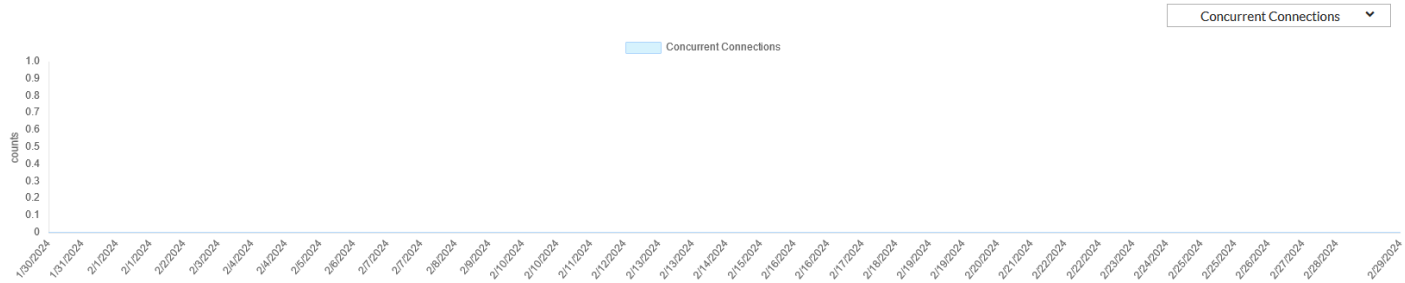
A continuación, se observa el número de sesiones concurrentes para este aplicativo.



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

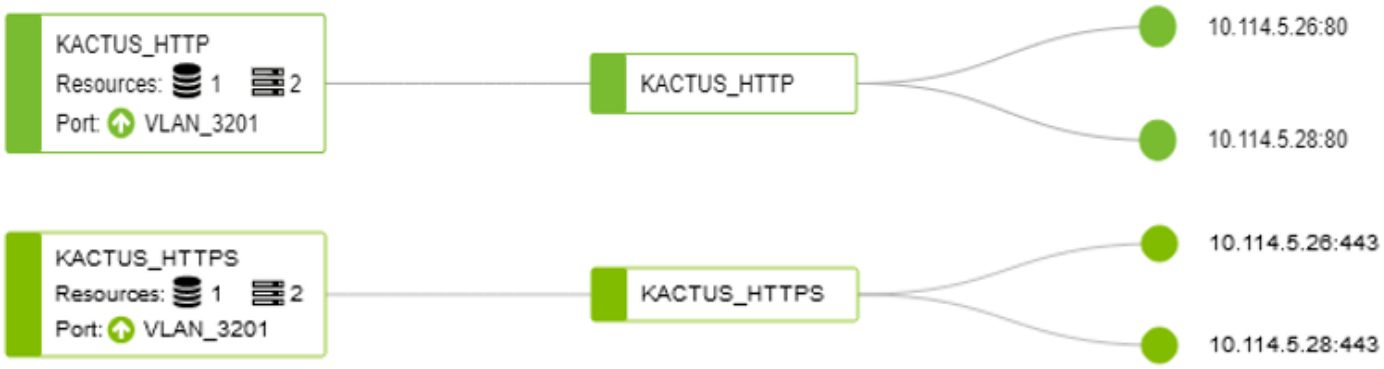


En el FortiADC no se observan sesiones concurrentes:

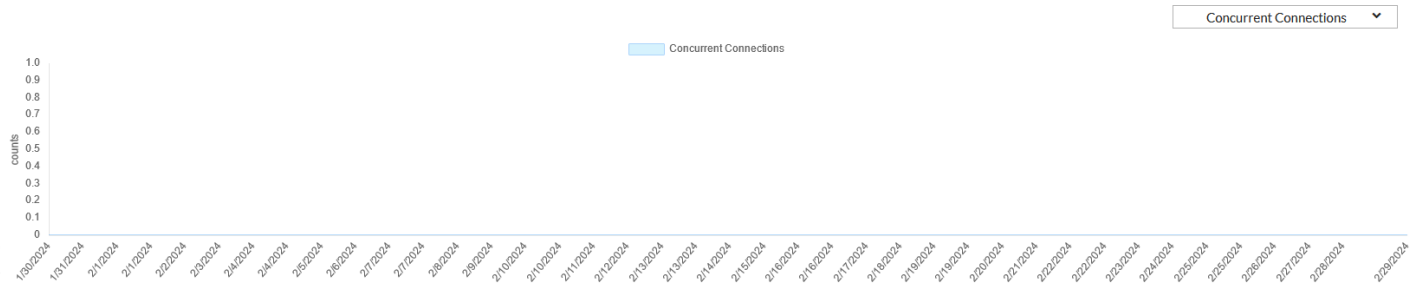


9.3 Kactus WEB

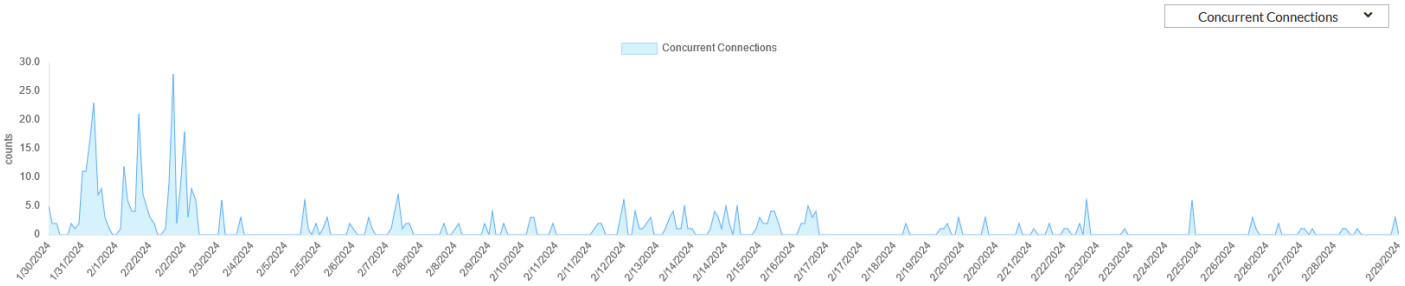
Se encuentra balanceado en el FortiADC:



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



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



9.4 SIRNA

Estos servidores se encuentran balanceados en el Fortigate perimetral:

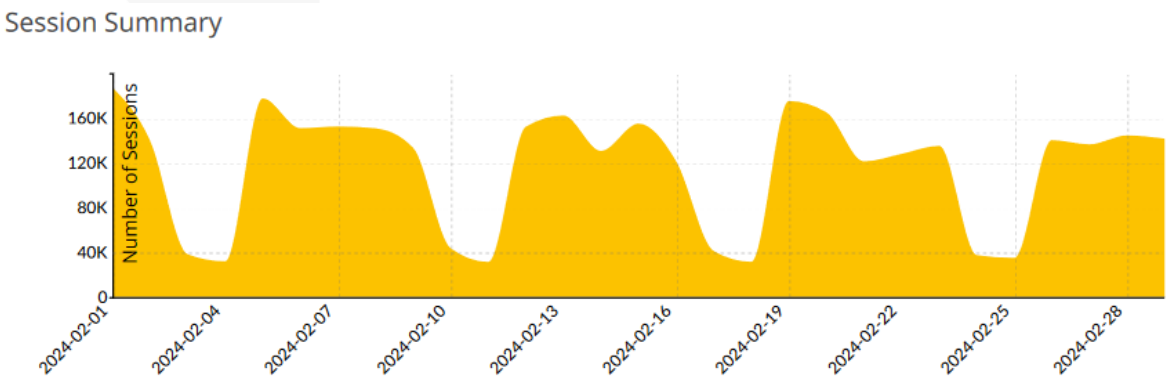
Configuración de balanceo de CRM en el Firewall.

Name	Type	Virtual Server IP	Load Balancing Method	Real Servers	Interface
IPv4 Virtual Server 1/4					
CRM_HTTP_HTTPS_4...	IP	10.244.2.236:0-65535	Round Robin	10.244.2.226 10.244.2.227	P6.3210

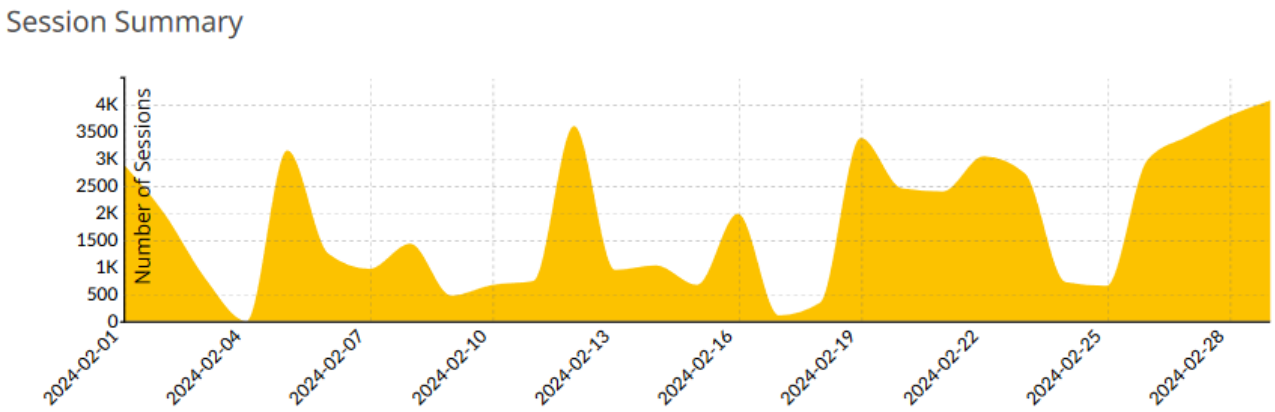
Configuración de balanceo de Sharepoint en el firewall perimetral.

Name	Type	Virtual Server IP	Load Balancing Method	Real Servers	Interface
IPv4 Virtual Server 1/4					
SHAREPOINT	IP	10.244.2.237:0-65535	Round Robin	10.244.2.229 10.244.2.228	any

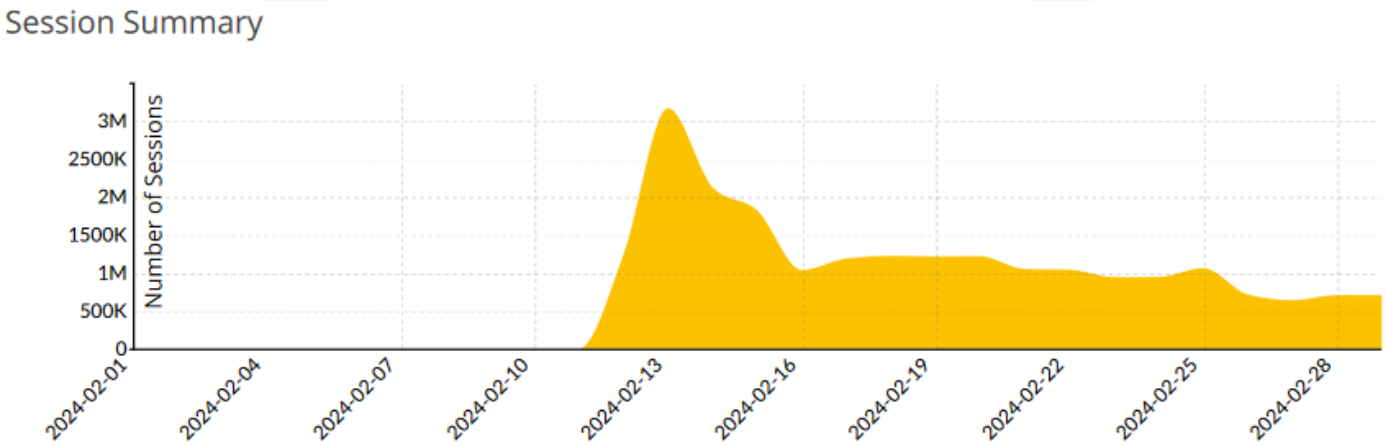
Las sesiones en el firewall para SIRNA 443 fueron:



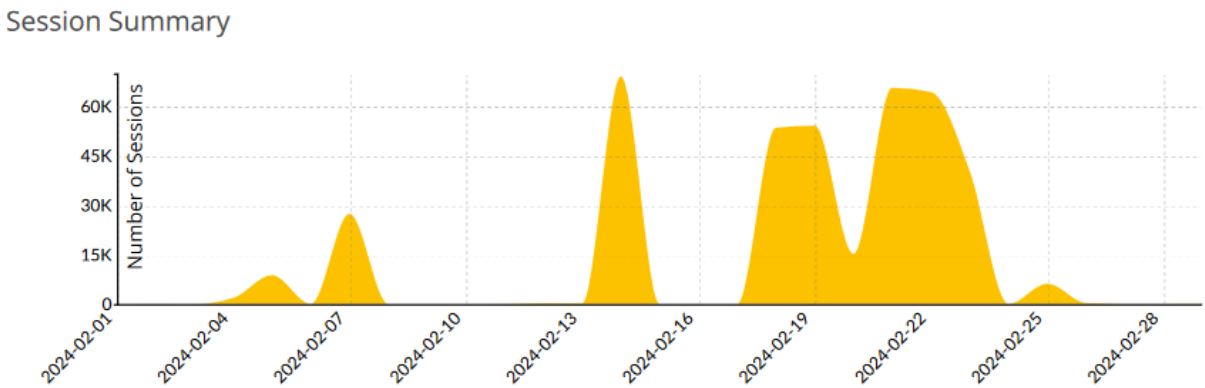
Las sesiones en el firewall para SIRNA 4443 fueron:



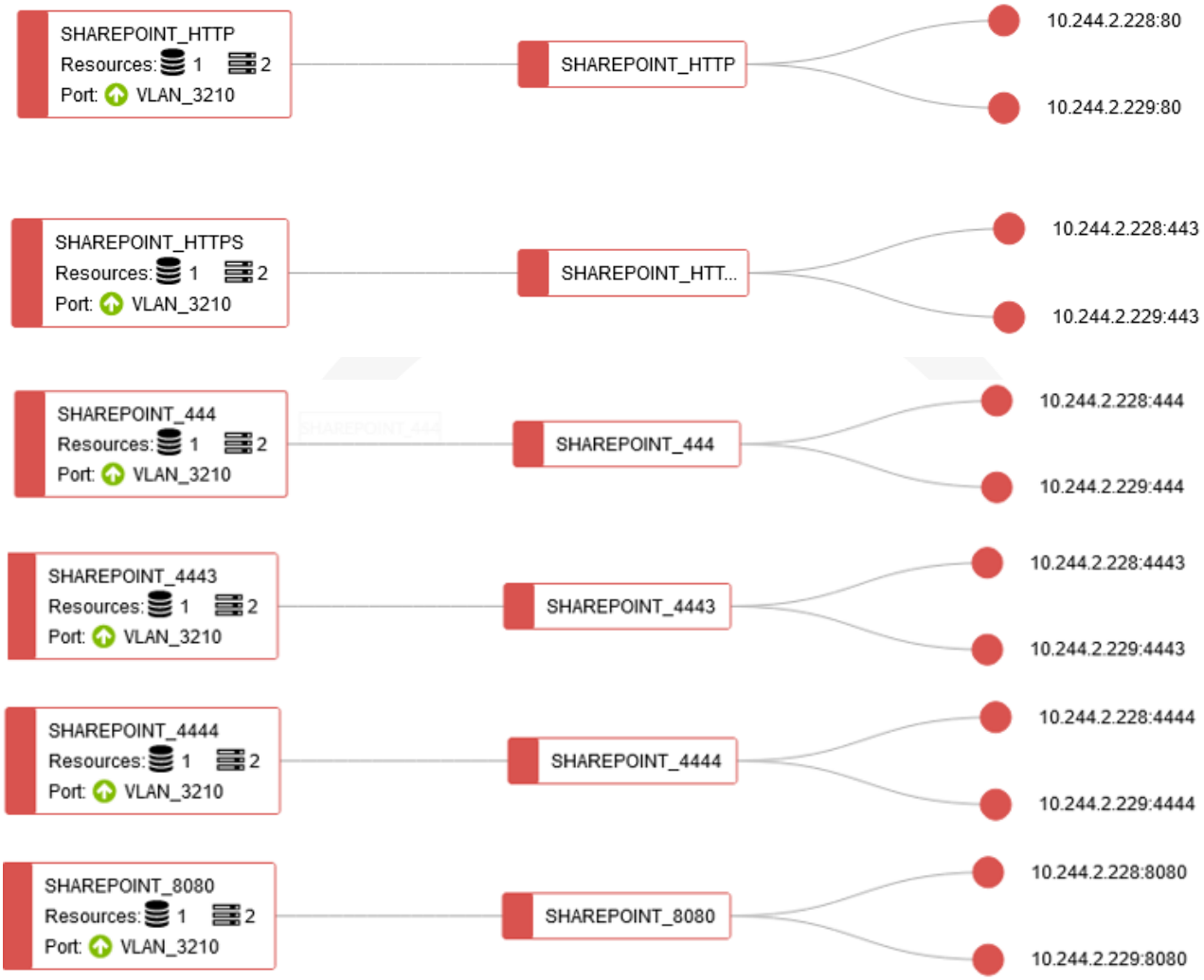
Las sesiones en el firewall para CRM 443 fueron:



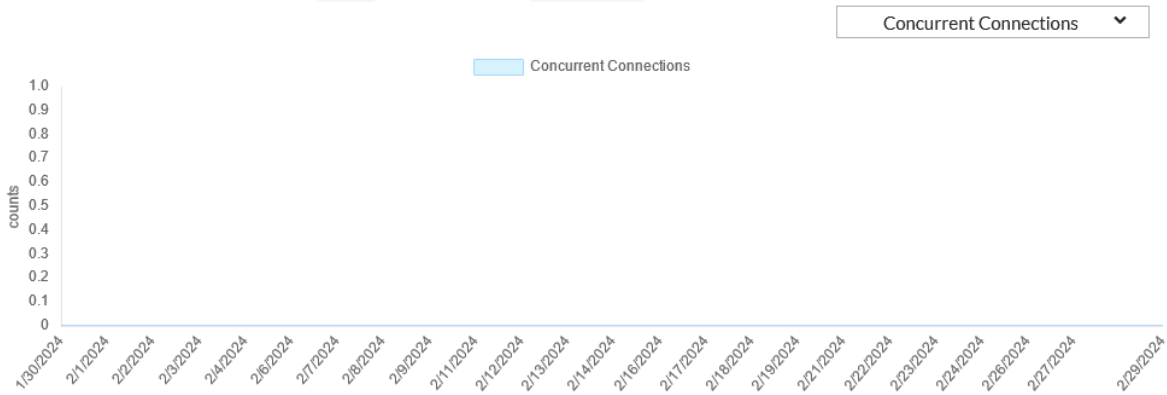
Las sesiones en el firewall para Sharepoint 444 fueron:



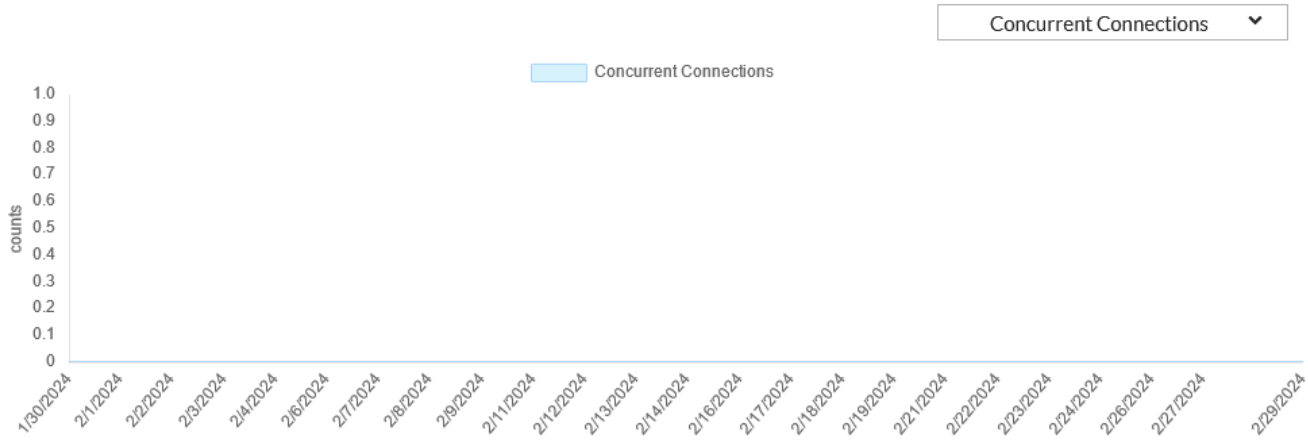
Y se encuentran balanceados en el FortiADC de Torre Central de la siguiente manera:



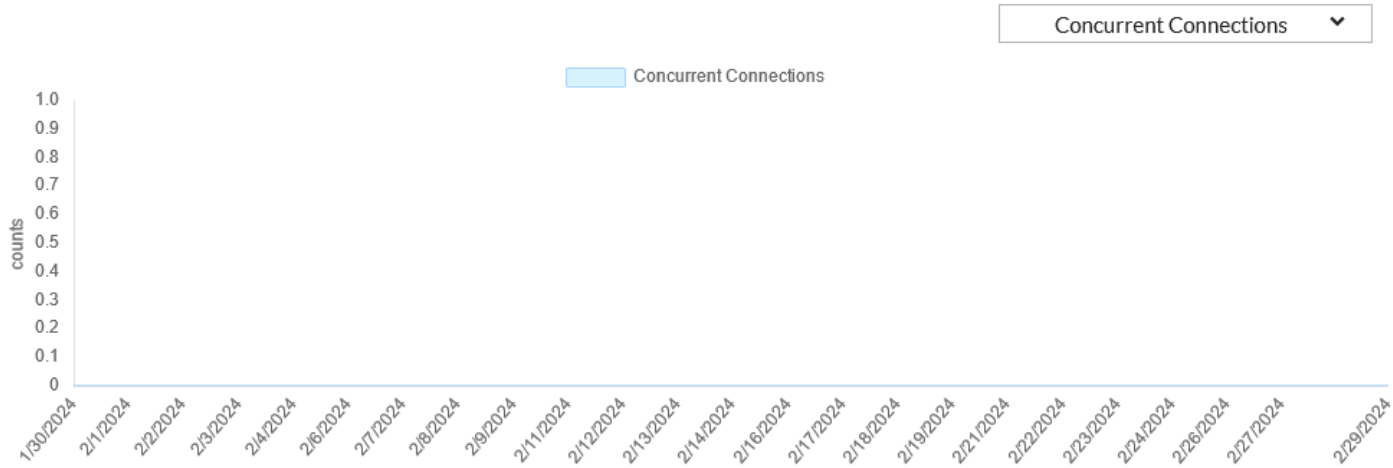
No se presentaron sesiones concurrentes por HTTP:



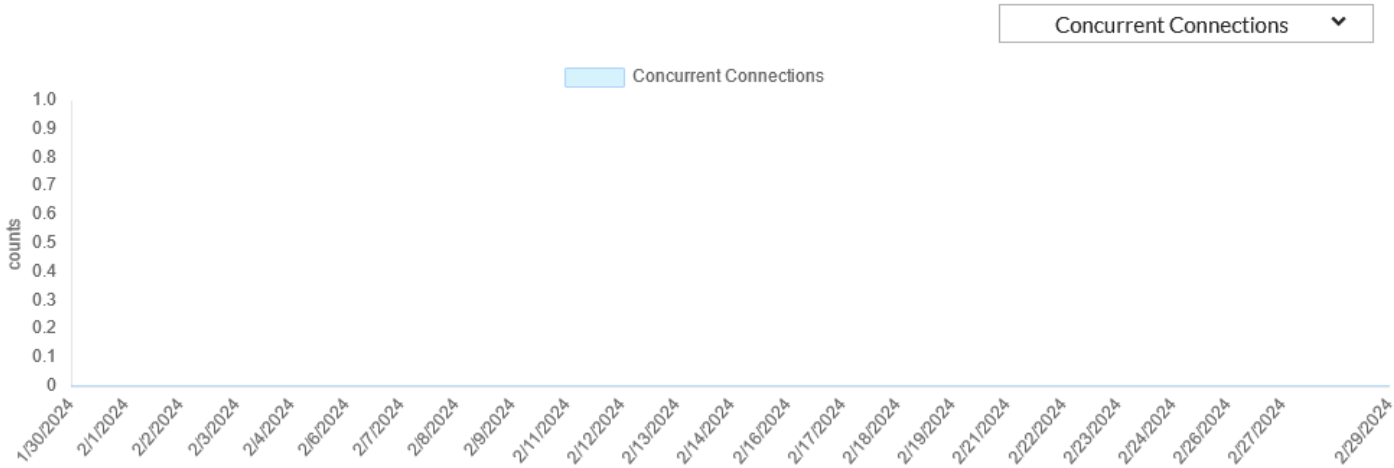
No se presentaron sesiones concurrentes por HTTPS:



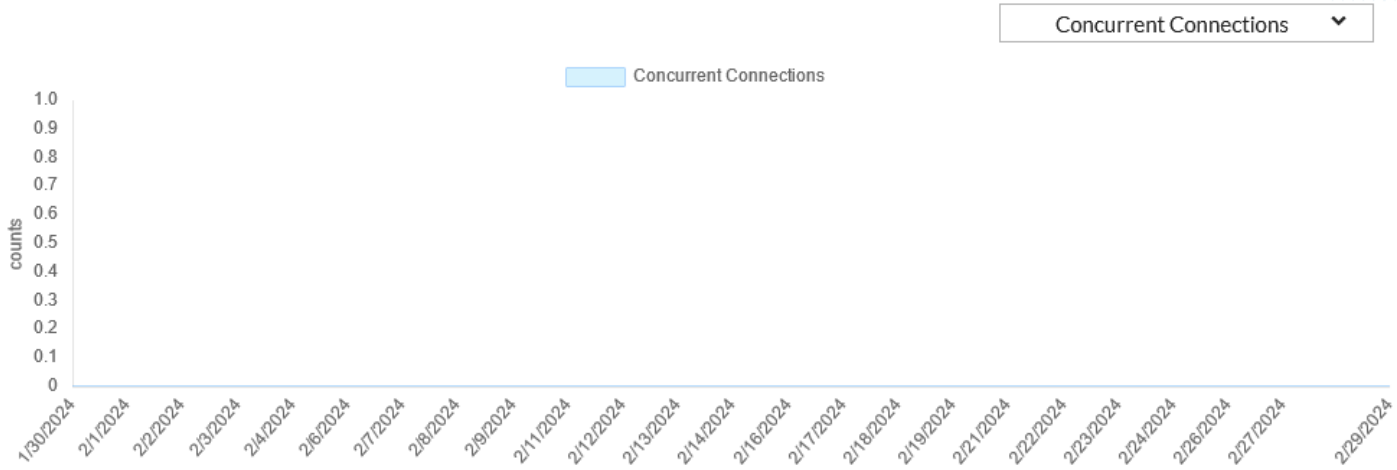
No se tuvieron sesiones concurrentes por el puerto 444:



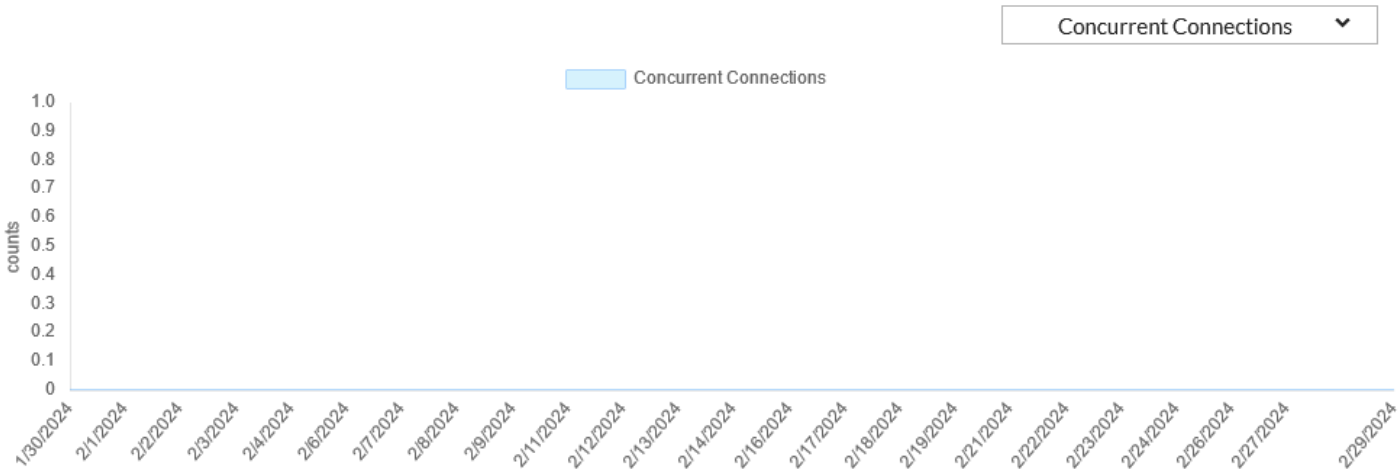
No se tuvieron sesiones concurrentes por el puerto 4443:



No se tuvieron sesiones concurrentes por el puerto 4444:



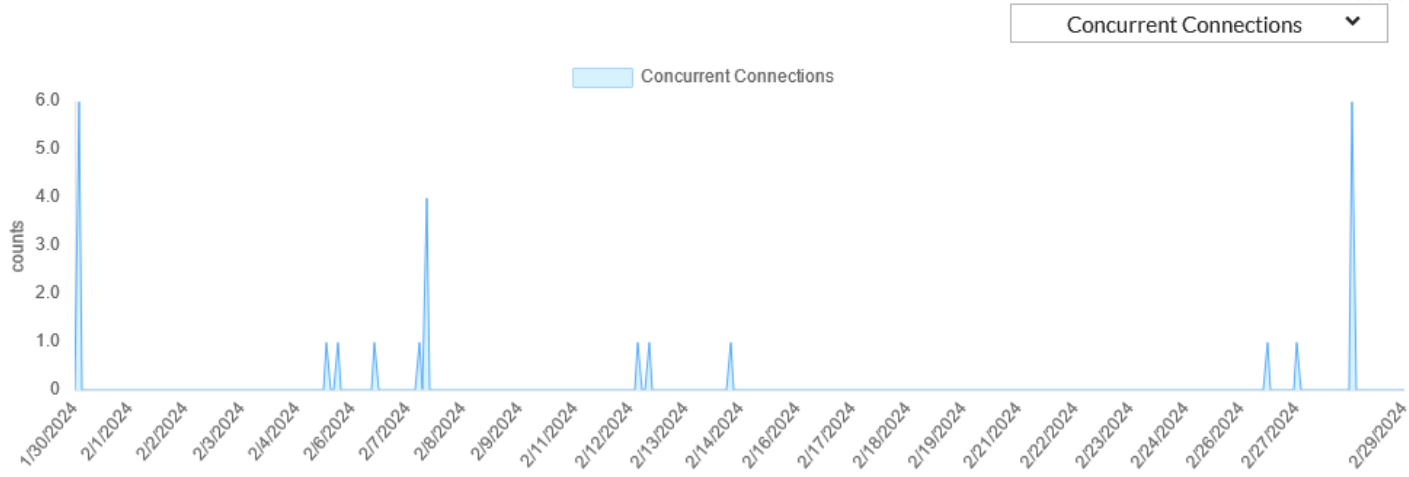
No se tuvieron sesiones concurrentes por el puerto 8080:



9.5 Convocatoria Peritos.

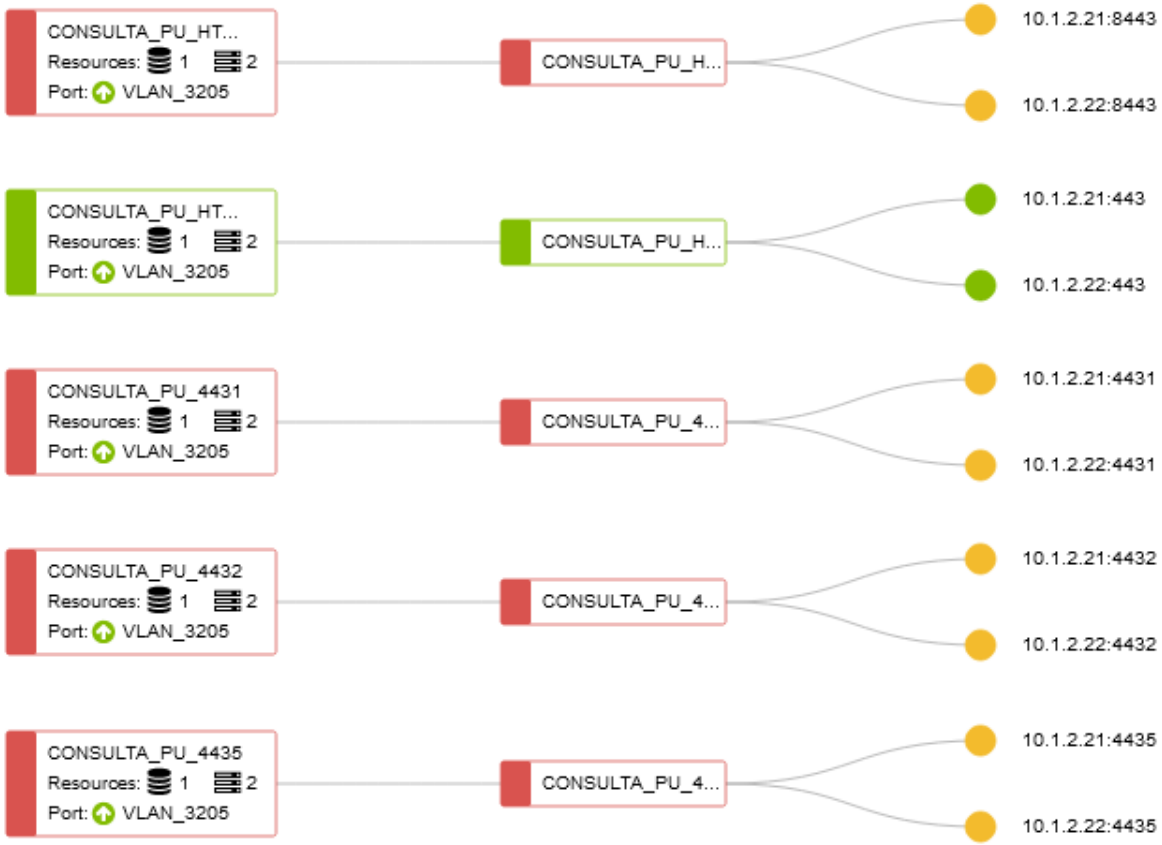
Este servicio se encuentra balanceado en el FortiADC:

Las sesiones concurrentes son las siguientes:

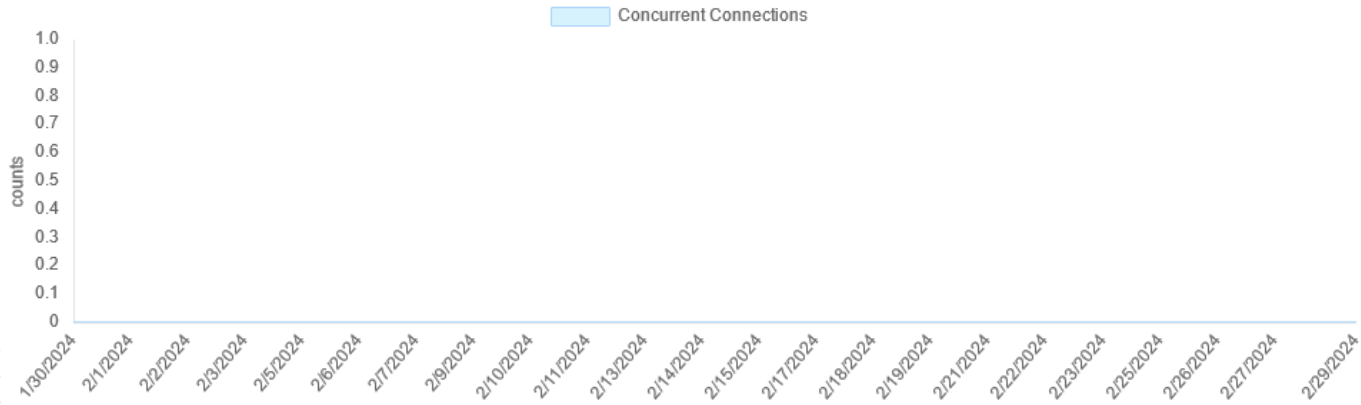


9.6 Consulta De Procesos Nacional Unificada (CPNU)

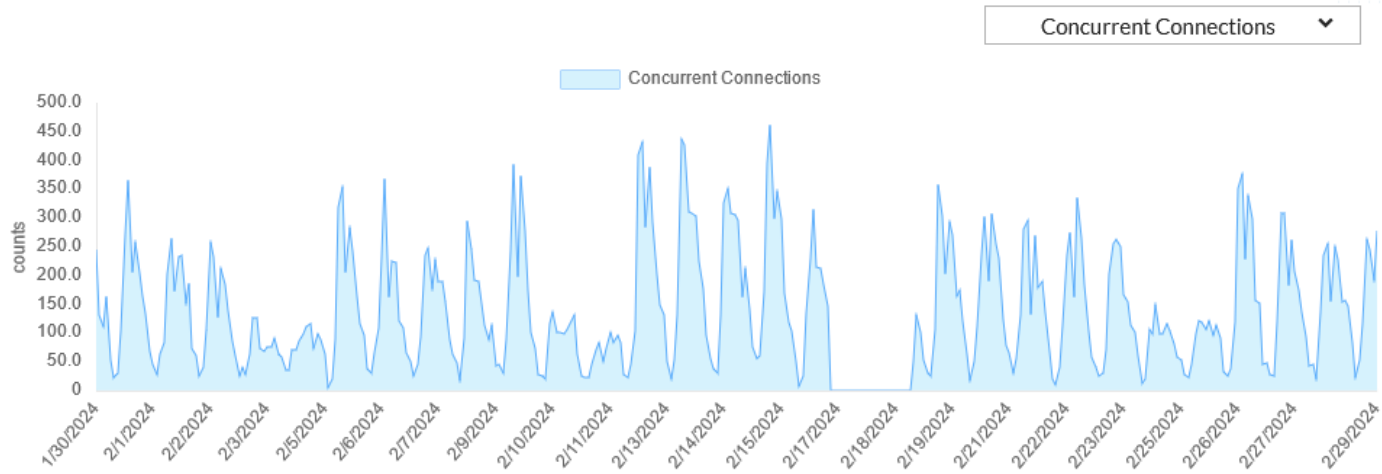
A continuación, se muestra la configuración de balanceo para esta aplicación en el FortiADC:



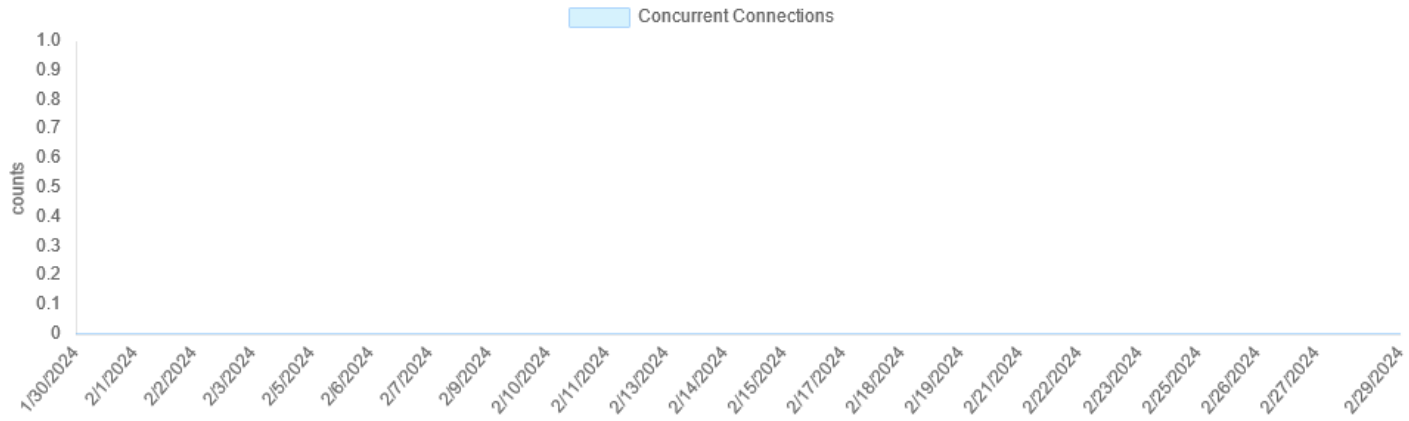
Durante febrero no se tuvieron sesiones concurrentes por el puerto HTTP:



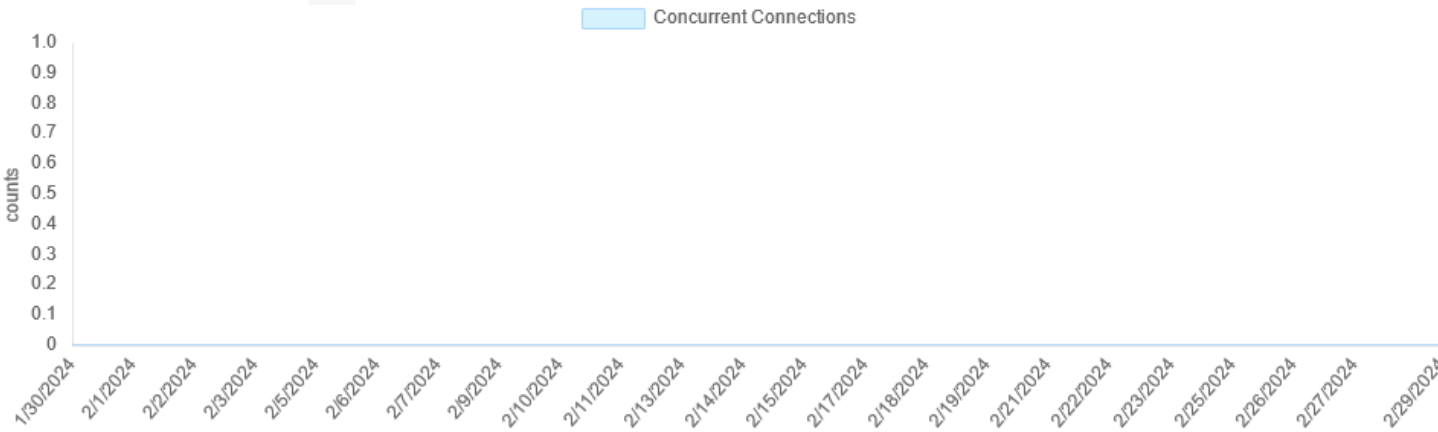
Las sesiones concurrentes por HTTPS fueron:



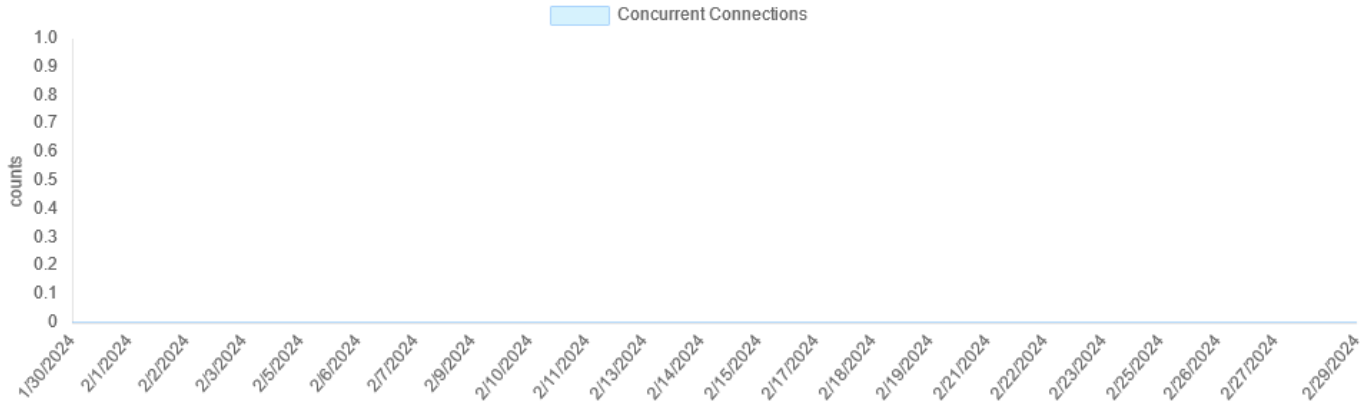
No se tuvieron sesiones concurrentes por el puerto 4431:



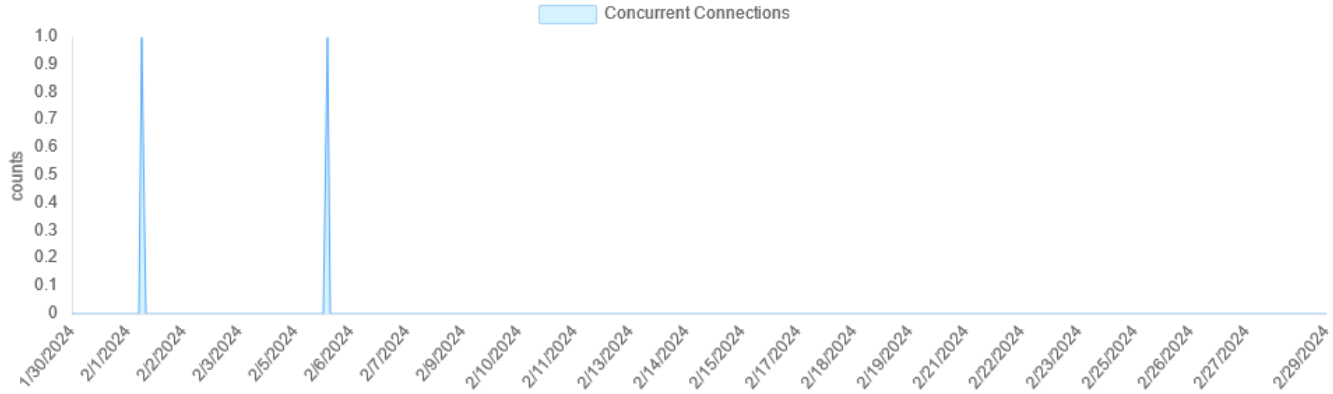
No se tuvieron sesiones concurrentes por el puerto 4432:



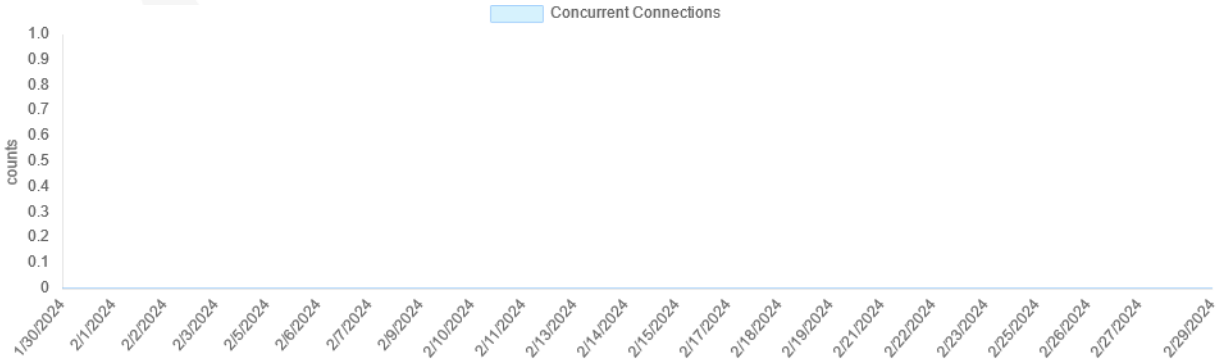
No se tuvieron sesiones concurrentes por el puerto 4435:



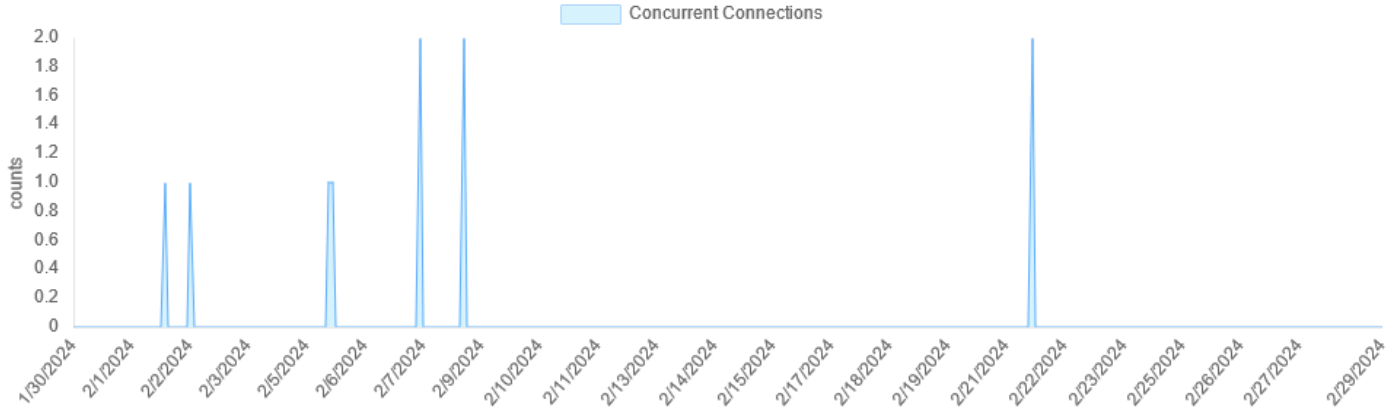
Las sesiones concurrentes por puerto 4436 fueron:



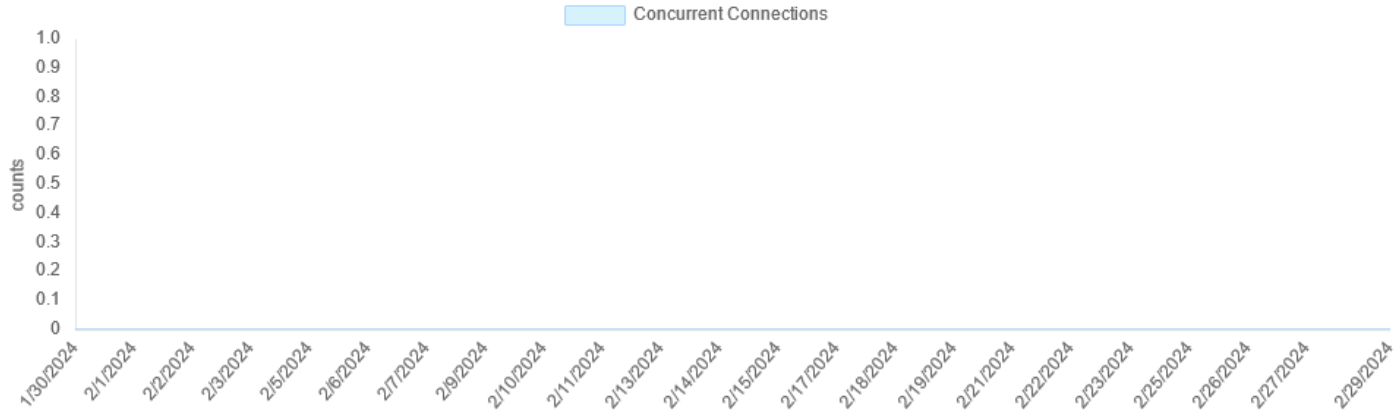
No se tuvieron sesiones concurrentes por el puerto 444:



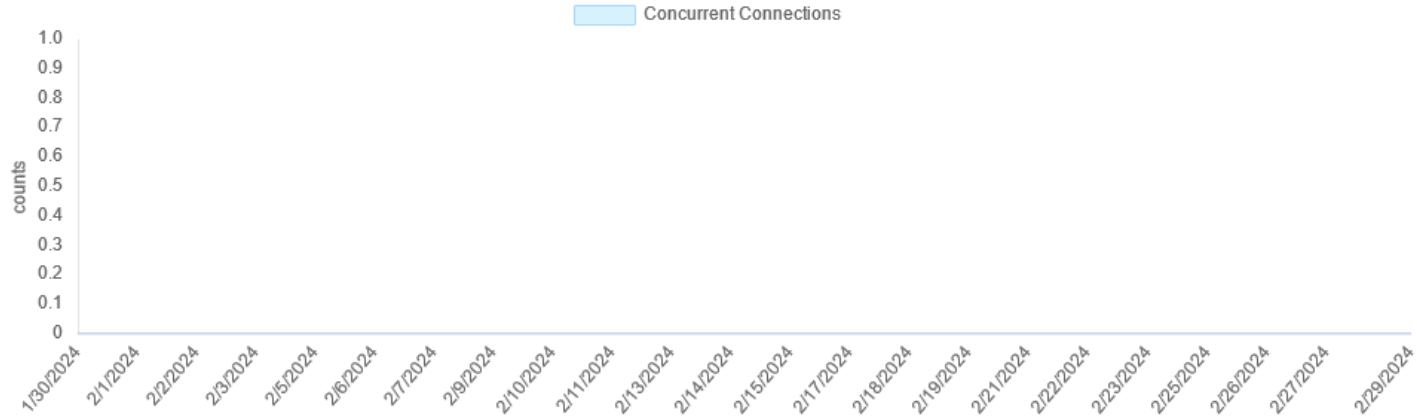
Las sesiones concurrentes por 448 fueron:



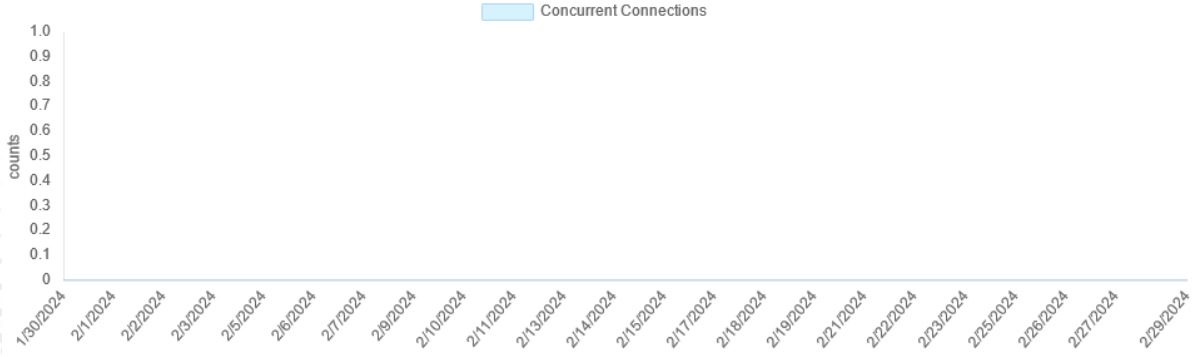
No se tuvieron sesiones concurrentes por el puerto 449:



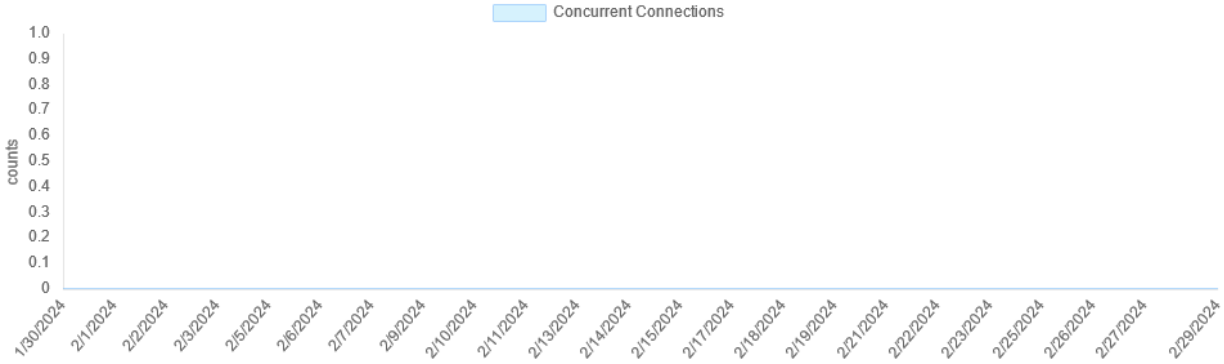
No se tuvieron sesiones concurrentes por el puerto 8085:



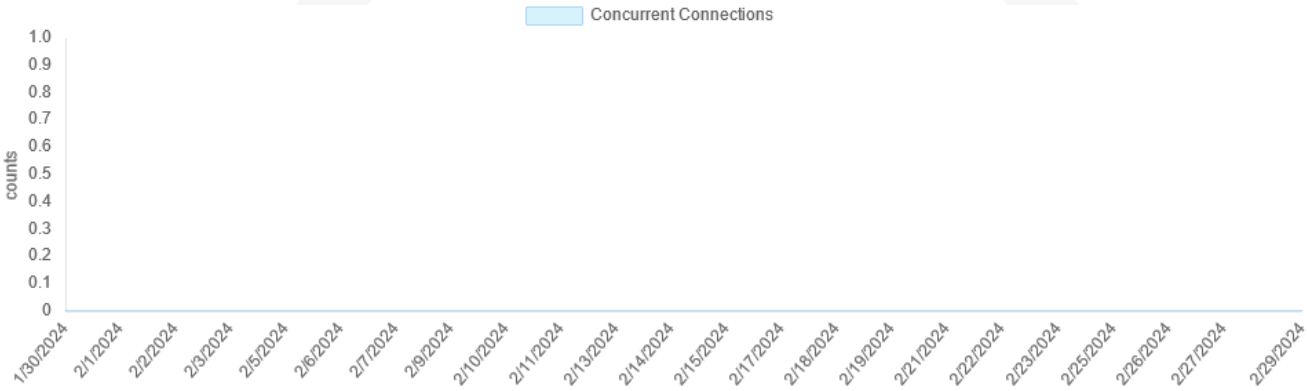
No se tuvieron sesiones concurrentes por el puerto 90:



No se tuvieron sesiones concurrentes por el puerto 9085:



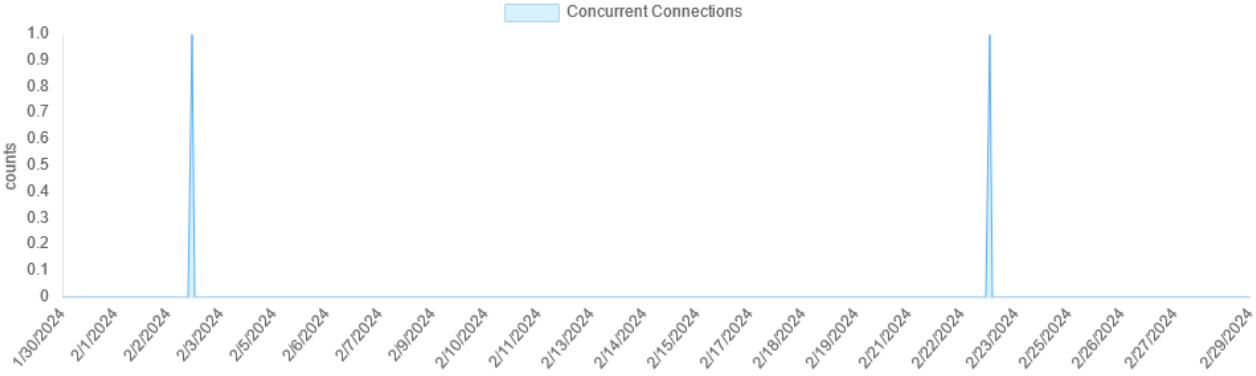
No se tuvieron sesiones concurrentes por el puerto 8643:



9.7 SIERJU

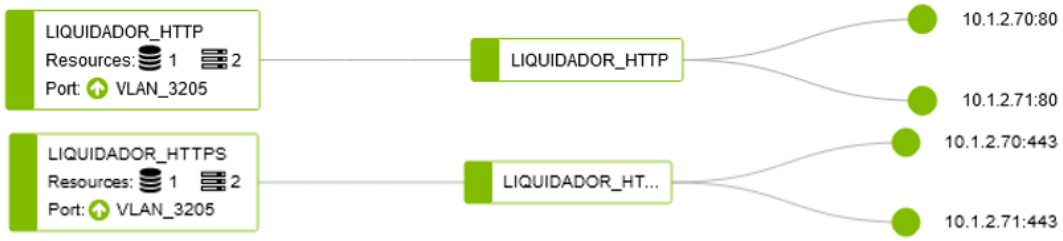
La configuración de balanceo para esta aplicación en el balanceador FortiADC es:

Las sesiones concurrentes para este aplicativo fueron:

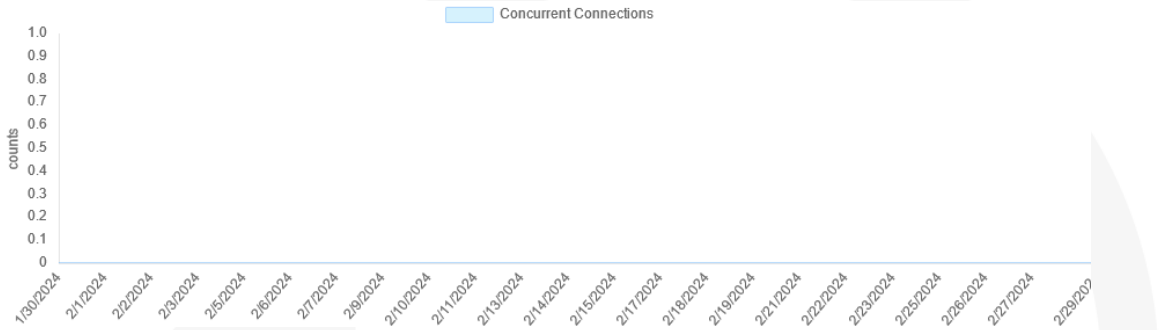


9.8 Liquidador de Sentencias

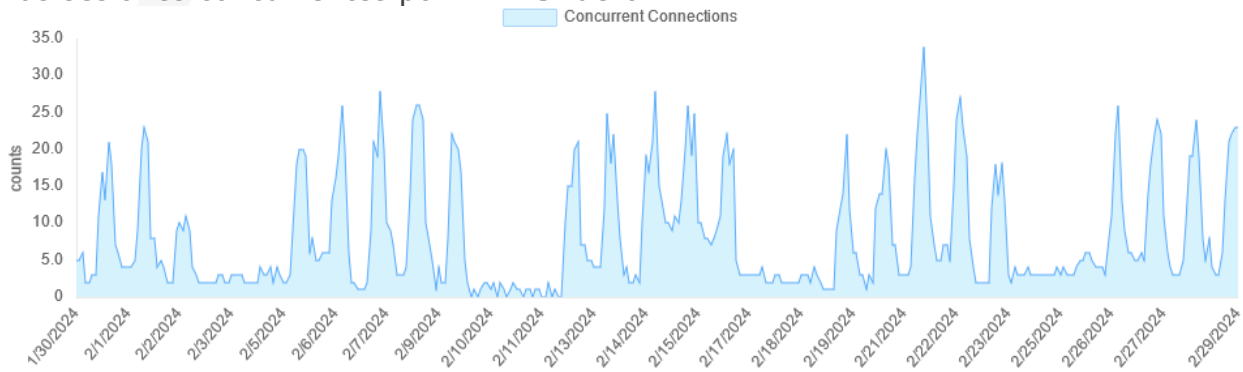
Virtual server Liquidador de Sentencias balanceador FortiADC



Las sesiones concurrentes por HTTP fueron:



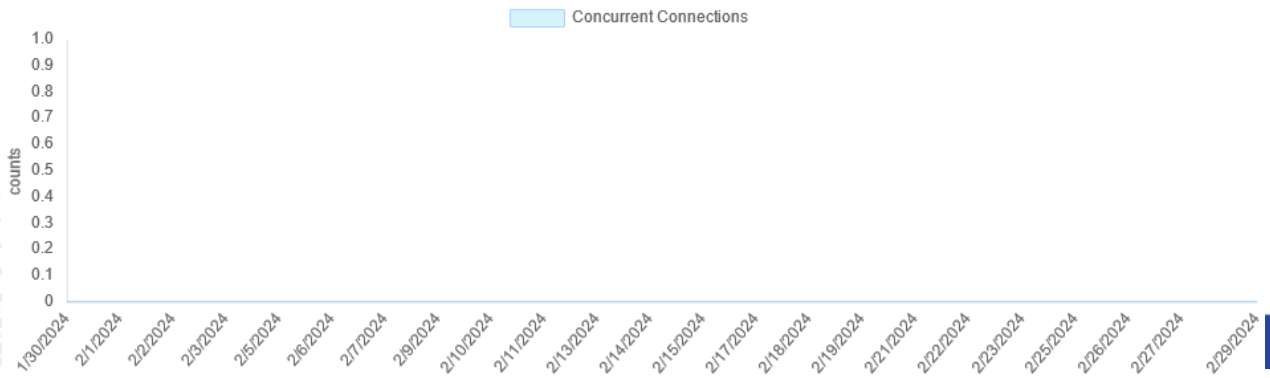
Las sesiones concurrentes por HTTPS fueron:



9.9 Consulta Jurisprudencia

Virtual server Consulta Jurisprudencia se encuentra en el balanceador FortiADC.

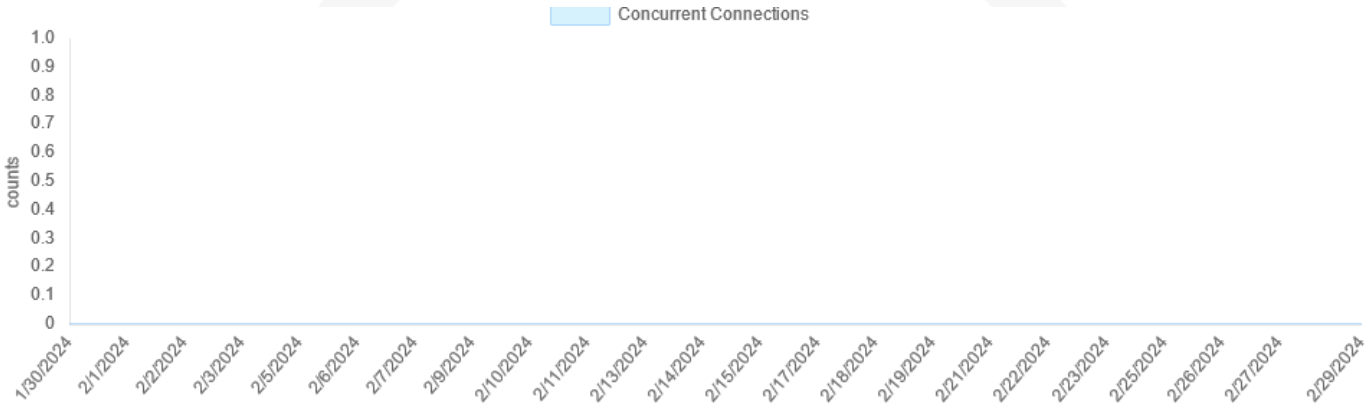
Las sesiones concurrentes para este aplicativo fueron:



9.10 API Gestión de Audiencias

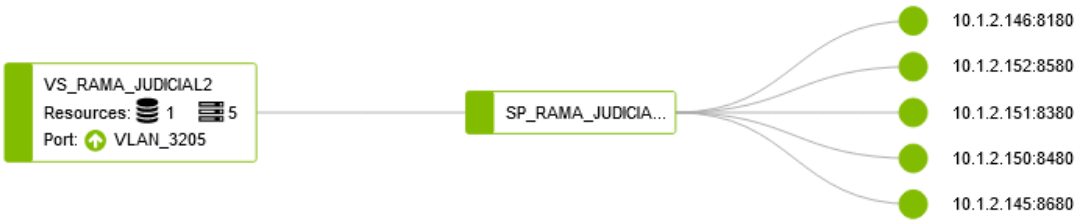
Virtual server API Gestión de Audiencias balanceador FortiADC.

Las sesiones concurrentes para este aplicativo fueron:

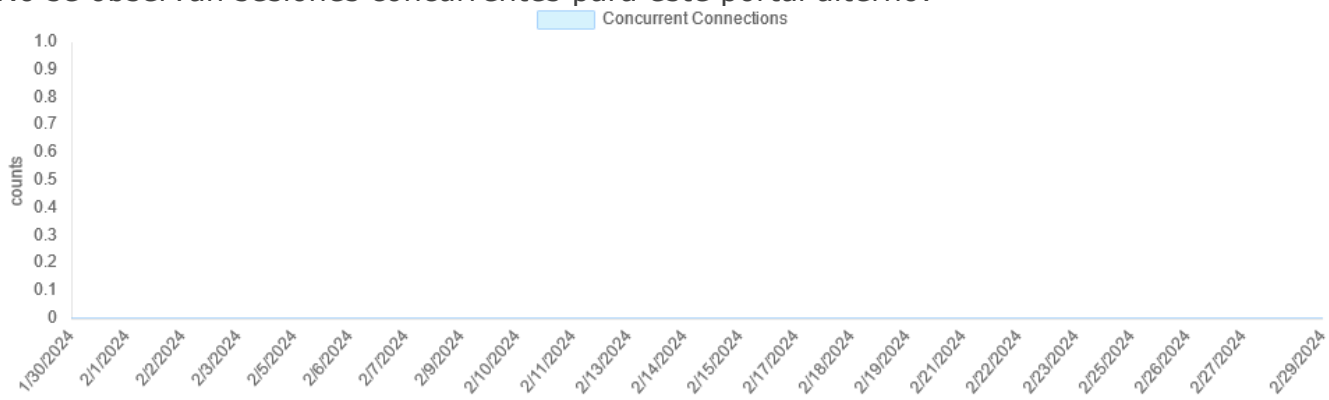


9.11 Portal Alterno de la Rama Judicial

Se encuentran balanceado en el FortiADC:

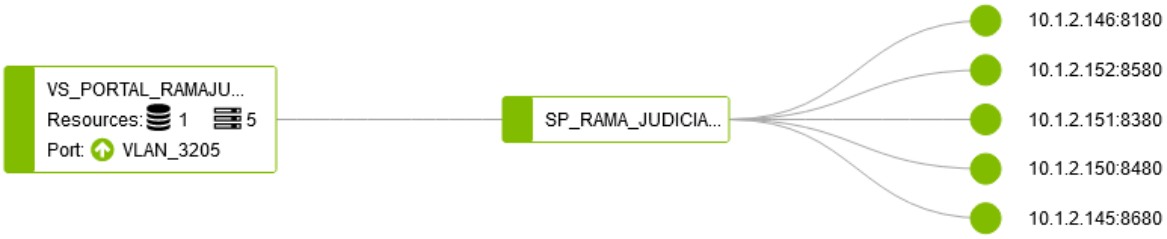


No se observan sesiones concurrentes para este portal alterno:

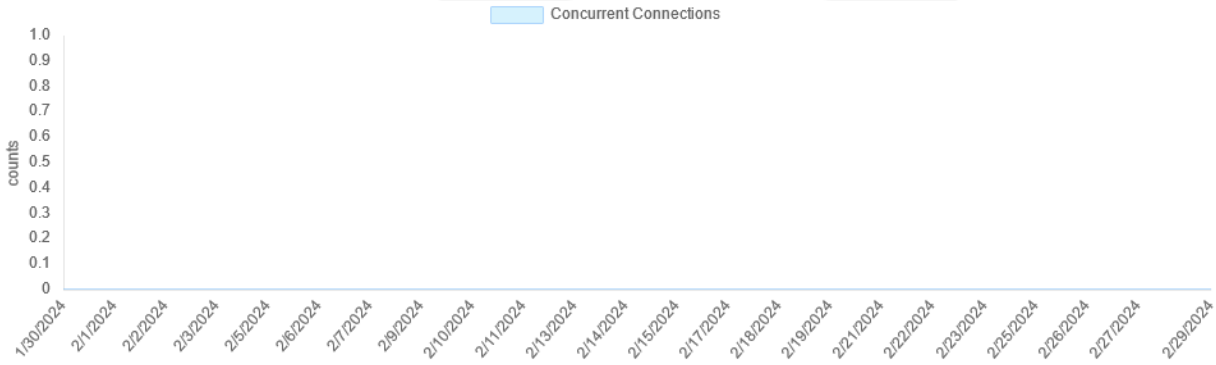


9.12 Portal de la Rama Judicial

Se encuentran balanceado en el FortiADC:

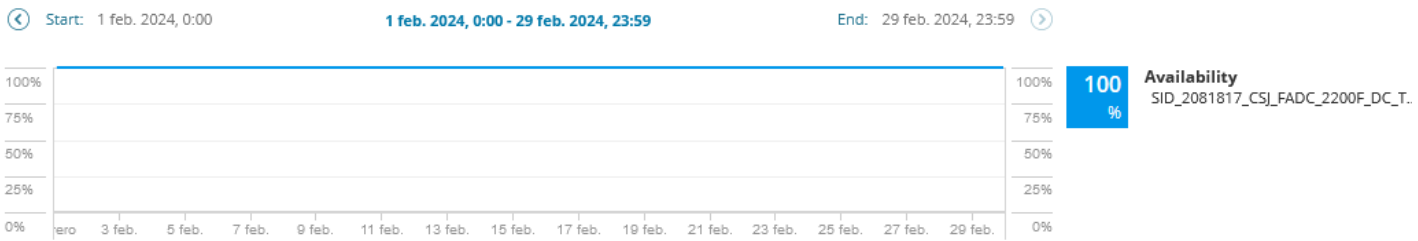


No se observan sesiones concurrentes para este portal:

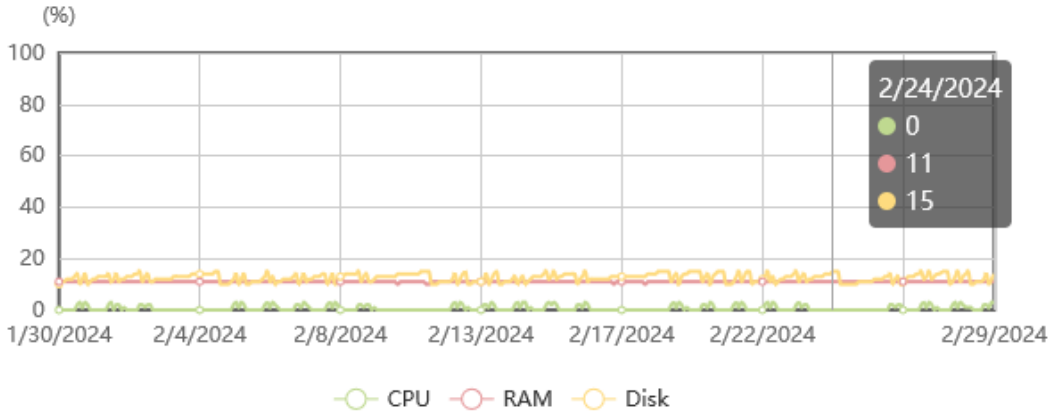


9.13 Disponibilidad y performance.

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



Durante febrero se observa que el consumo de CPU es del 1%, memoria 11% y disco 15%.



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

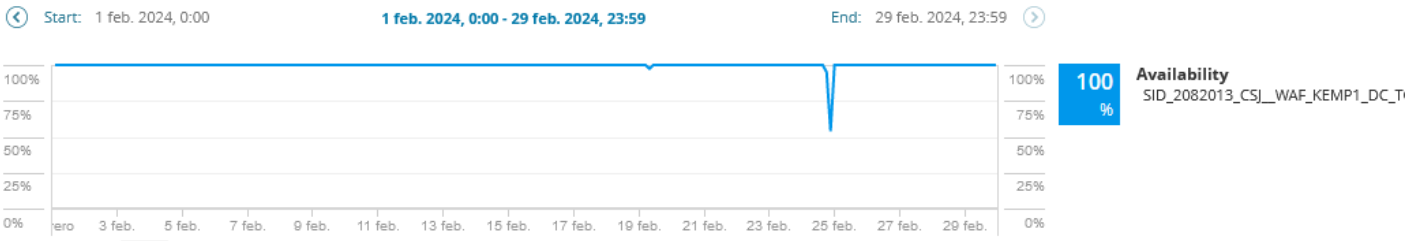
Para la protección de las aplicaciones web se tienen configuradas las siguientes políticas en los Firewall de Aplicaciones Web:

Item	Solución WAF	Cantidad de políticas de servidores
1	WAF TORRE CENTRAL	159
2	WAF CAN	69

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

10.1 Web application firewall datacenter principal IFX.

Durante febrero se obtuvo una disponibilidad del 100 % para el Kemp de Torre Central:



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

Las aplicaciones más consultadas durante el mes de febrero fueron consultaprocesos.ramajudicial.gov.co - 448:

#	Name	Virtual IP Address	Total Conns	% del Total
1	consultaprocesos.ramajudicial.gov.co - 448	172.17.201.68:448	74342576	47.59%
2	www.ramajudicial.gov.co	172.17.201.25:443	26484771	16.96%
3	procesojudicial.ramajudicial.gov.co TYBA PRUEBAS	172.17.201.249:443	25329612	16.22%
4	consultaprocesos.ramajudicial.gov.co - 443	172.17.201.68:443	7925423	5.07%
5	consejodeestado.gov.co	172.17.201.52:443	7272046	4.66%
6	www.corteconstitucional.gov.co	172.17.201.13:443	6128065	3.92%
7	consultajurisprudencial.ramajudicial.gov.co 8080	172.17.201.110:8080	1090957	0.70%
8	sirna.ramajudicial.gov.co	172.17.201.28:443	1077756	0.69%
9	antecedentesdisciplinarios.ramajudicial.gov.co	172.17.201.31:443	738129	0.47%
10	apigestionaudiencias1.ramajudicial.gov.co	172.17.201.42:443	651630	0.42%
	Otros		5161928	3.30%
	System Total Conns		156202893	100.00%

10.3 Top de peticiones por país WAF principal IFX.

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

Top 10 Countries

Total

Country	Requests	Blocked
United States	55678931	607100
Colombia	70171261	151132
Brazil	991469	11590
Argentina	23019182	9959
Taiwan	7265	2774
IPrep	2320	2320
Germany	658031	2221
Singapore	10710	1842
Netherlands	1653339	1276
China	26192	1075

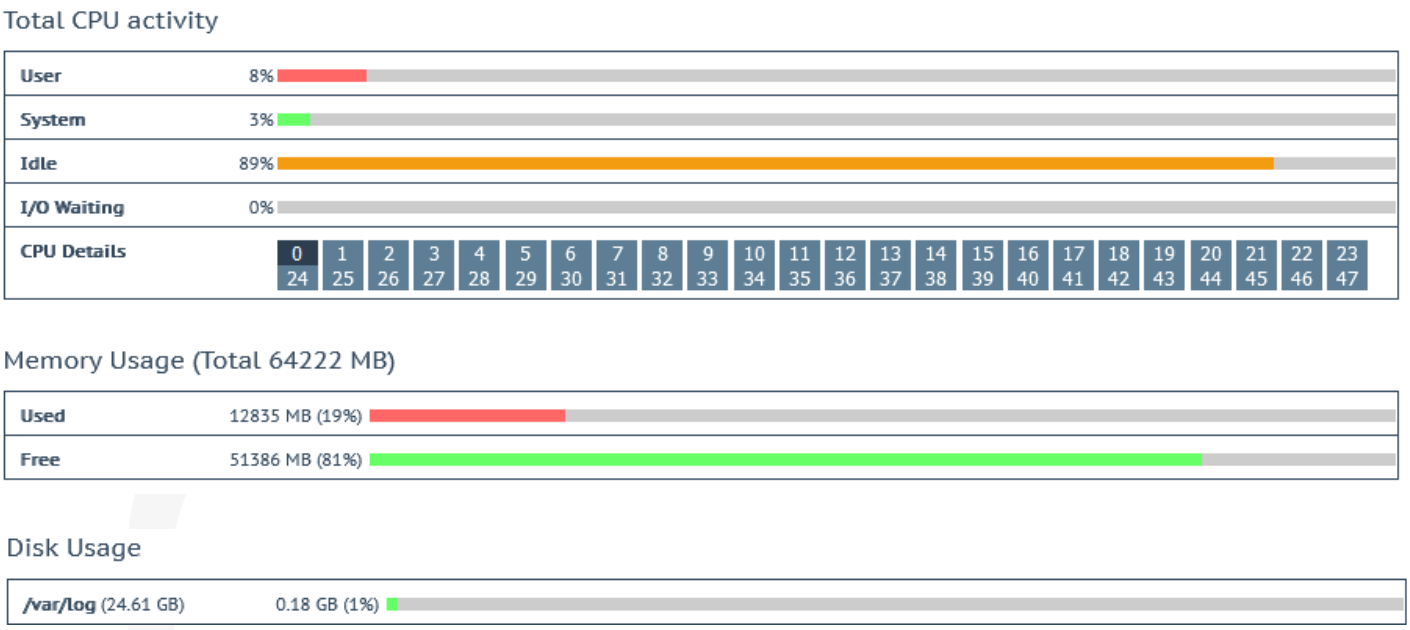
10.4 Top de ataques por política WAF principal IFX.

Sobre las aplicaciones consejodeestado.gov.co y procesos.ramajudicial.gov.co_procesoscs CONSULTA AZUL han sido prevenidas la mayor cantidad de ataques:

#	Name	Virtual IP Address	Total Events	% del Total
1	consejodeestado.gov.co	172.17.201.52:443	493113	62.37%
2	procesos.ramajudicial.gov.co_procesoscs CONSULTA AZUL	172.17.201.26:8443	174109	22.02%
3	consultaprocesos.ramajudicial.gov.co - 448	172.17.201.68:448	93513	11.83%
4	jurisprudencia.ramajudicial.gov.co - ayudajurisprudencia.ramajudicial.gov.co	172.17.201.29:443	7181	0.91%
5	saidoj.ramajudicial.gov.co	172.17.201.69:443	6770	0.86%
6	iedoc.consejodeestado.gov.co 448	172.17.201.60:448	2368	0.30%
7	www.corteconstitucional.gov.co	172.17.201.13:443	1989	0.25%
8	www.ramajudicial.gov.co	172.17.201.25:443	1955	0.25%
9	PS_relatoriaconsejoestado Redirect	172.17.201.57:443	1005	0.13%
10	procesojudicial.ramajudicial.gov.co TYBA PRUEBAS	172.17.201.249:443	923	0.12%
	Otros		7654	0.97%
	WAF enabled VS Total		790580	100.00%

10.5 Consumo de recursos WAF principal IFX.

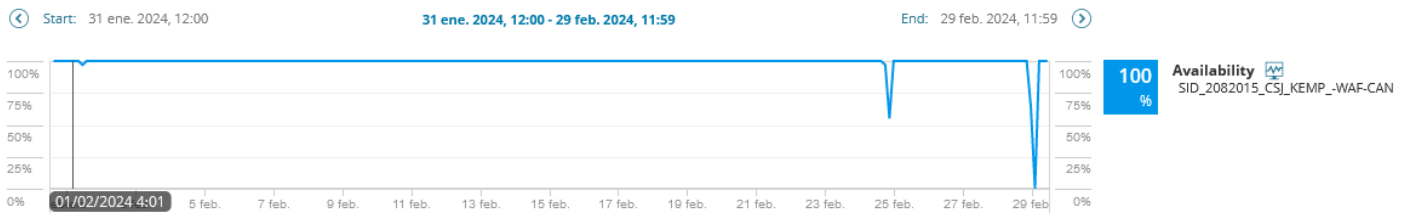
El WAF KEMP de Torre Central presentó consumo de CPU del 8%, memoria de 19% y disco en un 1%.



11. TRÁFICO DE WEB APPLICATION FIREWALL (WAF) CAN

11.1 Disponibilidad WAF CAN.

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



11.2 Uso de políticas de servidores WAF CAN.

La aplicación más consultada durante febrero fue cortesuprema.gov.co_Palacio:

#	Name	Virtual IP Address	Total Conns	% del Total
1	cortesuprema.gov.co_Palacio	172.17.202.239:443	6083292	60.46%
2	restituciontierras.ramajudicial.gov.co	172.17.202.37:443	1555219	15.46%
3	samairj.consejodeestado.gov.co	172.17.202.38:443	440046	4.37%
4	sso.cortesuprema.gov.co	172.17.202.141:443	396386	3.94%

5	restituciontierras.ramajudicial.gov.co redirect	172.17.202.37:80	346634	3.44%
6	cortesuprema_Palacio Redirect	172.17.202.239:80	299794	2.98%
7	convocatorias.consejodeestado.gov.co	172.17.202.147:443	154980	1.54%
8	linkce.consejodeestado.gov.co	172.17.202.42:443	134124	1.33%
9	sso.cortesuprema.gov.co redirect	172.17.202.141:80	88800	0.88%
10	sigobius.consejodeestado.gov.co_443	172.17.202.29:443	76233	0.76%
	Otros		486646	4.84%
	System Total Conns		10062154	100.00%

11.3 Top de peticiones por país WAF CAN.

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

Top 10 Countries

Total

Country	Requests	Blocked
Brazil	40127	3753
United States	1126976	2227
Netherlands	12468	1089
Taiwan	2930	1002
IPrep	575	575
Singapore	4712	431
Ireland	50151	353
Switzerland	5653	316
United Kingdom	27087	314
Private	906248	208

11.4 Top de ataques por política WAF CAN.

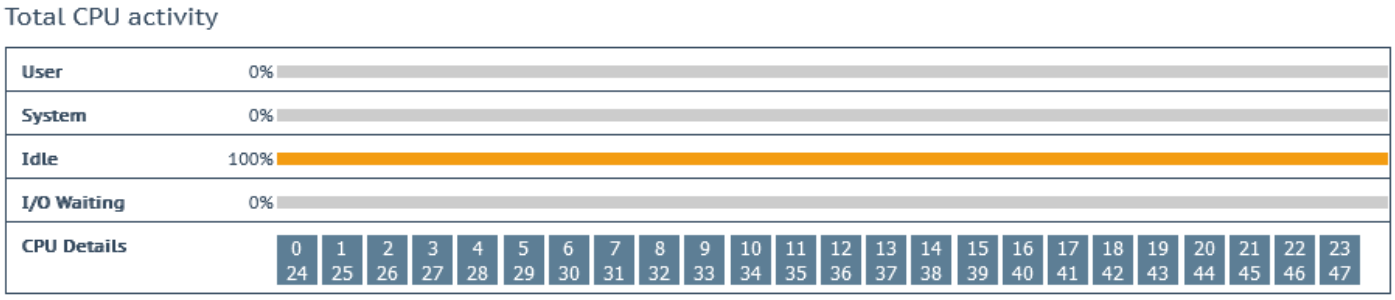
Sobre la aplicación restituciontierras.ramajudicial.gov.co ha sido prevenida la mayor cantidad de ataques:

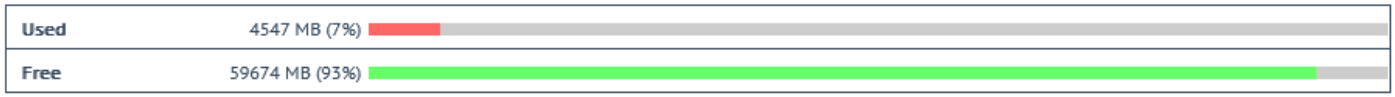
#	Name	Virtual IP Address	Total Events	% del Total
1	restituciontierras.ramajudicial.gov.co	172.17.202.37:443	3573	31.56%
2	cortesuprema.gov.co_Palacio	172.17.202.239:443	2139	18.89%
3	pruebasportal.ability.com.co_Portal pruebas	172.17.202.47:80	1683	14.87%
4	sivehl.ramajudicial.gov.co	172.17.202.145:443	876	7.74%

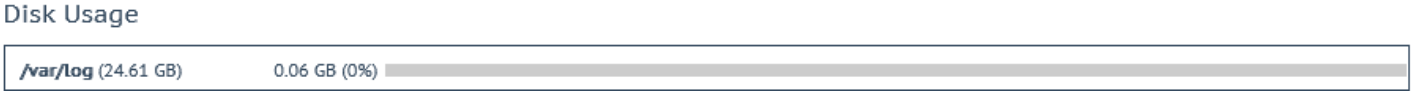
5	samairj.consejodeestado.gov.co	172.17.202.38:443	721	6.37%
6	capacitacion.ramajudicial.gov.co 443	172.17.202.13:443	304	2.69%
7	convocatorias.consejodeestado.gov.co	172.17.202.147:443	267	2.36%
8	SP_WIKI_NUEVA_443 - 190.217.24.27 - sin servicio productivo	172.17.202.30:443	192	1.70%
9	pre_interoperabilidad.ramajudicial.gov.co	172.17.202.51:443	182	1.61%
10	efinominapruebas.ramajudicial.gov.co	172.17.202.45:443	156	1.38%
	Otros		1228	10.85%
	WAF enabled VS Total		11321	100.00%

11.5 Consumo de recursos WAF CAN.

El WAF KEMP del CAN presentó consumo de CPU del 0%, memoria de 7% y disco en un 10%.







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

Este certificado tiene vigencia hasta el 24 de octubre de 2024, como se puede observar en la siguiente imagen:

Nombre del asunto

País	CO
Localidad	Bogota
Organización	Direccion Ejecutiva de Administración judicial
Nombre común	*.ramajudicial.gov.co

Nombre del emisor

País	US
Organización	DigiCert Inc
Nombre común	DigiCert Global G2 TLS RSA SHA256 2020 CA1

Validez

No antes	Thu, 30 Mar 2023 00:00:00 GMT
No después	Wed, 24 Apr 2024 23:59:59 GMT

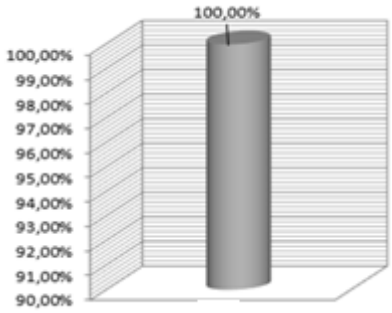
Este certificado se encuentra instalado en los siguientes dispositivos para cifrar el tráfico hacia las aplicaciones.

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 3500F HA**	FGT__CSJ_PALACIO_M	PALACIO	V7.2.6
		FGT_3500F_CSJ_PALACIO_S	PALACIO	V7.2.6
4	**KEMP Loadmaster x25 HA**	WAF_TORRRE_CENTRAL_MASTER	DC IFX	V7.2.59.0.22007
		WAF_TORRRE_CENTRAL_SLAVE	DC IFX	V7.2.59.0.22007
6	**KEMP Loadmaster x25**	WAF_CAN	DC CAN	V7.2.59.0.22007

12. DISPONIBILIDAD SEGURIDAD GLOBAL DEL MES DE FEBRERO

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

MES	DISPONIBILIDAD (%)
FEBRERO	100%



12.1 Anexo de las solicitudes e incidentes de seguridad reportadas.

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

13. 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.