



## REPORTE MENSUAL

RAMA JUDICIAL CONSEJO  
SUPERIOR DE LA JUDICATURA

OC124016

MARZO  
2024



## CONTENIDO

1. INFORMACIÓN TÉCNICA DEL INFORME.....	5
2. ALOJAMIENTO DE INFRAESTRUCTURA.....	6
3. ALMACENAMIENTO.....	8
4. BACKUPS.....	9
5. REPLICACIÓN.....	10
6.SERVICIOS POR APLICACIÓN.....	10
• Capacitación SST: líneas de OC 16 y 38.....	10
• Cobro coactivo: líneas de OC 17 y 38.....	10
• core-impact: Línea de OC 12.....	10
• Efinomina: Líneas de OC 14,18,26,27,38 y 39.....	10
• Fuse: Línea OC 17.....	10
• Gestión grabaciones: Líneas de OC 12,13, 14,15,17,19,20,22,23,25,28,35,36 y 38.....	10
• InsightVM console: línea OC 27.....	10
• InsightVM scan: línea OC 27.....	10
• Insightappsec scan: línea OC 25.....	10
• Isigthwm scan: línea OC 26.....	11
• Ivanti: Líneas de OC 17,18,20,21,22,28,38 y 42.....	11
7.DISPONIBILIDAD GLOBAL CLOUD DEL MES DE MARZO.....	12
1. INTRODUCCIÓN.....	13
2. INDICADORES DEL CENTRO CONSOLIDADO DE SERVICIOS.....	13
2.1 TASA DE RESOLUCIÓN DE PROBLEMAS.....	13
2.2 LISTADO DE CASOS REPORTADOS.....	18
2.3 BOLSA DE HORAS SEGÚN CONTRATO.....	19
2.4 ESTADO DE LAS HORAS CONSUMIDAS DE LOS CASOS REPORTADOS.....	19
3. DISPONIBILIDAD E INDISPONIBILIDAD DE LOS SERVICIOS DE HOSTING.....	20
3.1. DISPONIBILIDAD GLOBAL DEL MES DE MARZO.....	20
3.2 PORTAL DE LA RAMA JUDICIAL.....	21
24	
4. ESTADÍSTICAS PORTAL DE LA RAMA JUDICIAL.....	25
4.1 RESUMEN DEL PORTAL.....	25
5. ESQUEMA DE SEGURIDAD.....	28

14.1.	Horas experto del ítem 44 y esquema de compensación.....	30
14.2.	Inventario de equipos de seguridad perimetral.....	31
14.3.	Actualización de firmware.....	31
6.	FIREWALL PERIMETRAL.....	32
15.1.	Disponibilidad mensual firewall perimetral. ....	32
15.2.	Cantidad de sesiones firewall perimetral.....	32
15.3.	Histórico de sesiones de los últimos 6 meses en el firewall perimetral.....	33
15.4.	Aplicaciones y protocolos por ancho de banda firewall perimetral. ....	34
15.5.	Top de IP por ancho de banda firewall perimetral.....	34
15.6.	Top de destinos web por ancho de banda firewall perimetral. ....	35
15.7.	Top de usuarios con peticiones bloqueadas por el firewall perimetral.....	35
15.8.	Top de las categorías más bloqueadas por el firewall perimetral.....	36
15.9.	Top de IP más activos Firewall Perimetral.....	36
15.10.	Top de categorías más visitadas Firewall Perimetral .....	36
15.11.	Top de consumo ancho de banda por usuario Firewall Perimetral .....	37
7.	TRÁFICO VPN FIREWALL PERIMETRAL.....	37
16.1.	VPN IPSEC Site To Site Firewall Perimetral.....	39
16.2.	Top de intrusiones detectadas por el IPS del firewall perimetral .....	39
8.	FIREWALL SEDE PALACIO.....	41
8.1	Disponibilidad Mensual Firewall Palacio .....	41
8.2	Cantidad de Sesiones Firewall Palacio .....	41
8.3	Histórico de Sesiones Últimos 6 meses Firewall Palacio.....	42
8.4	Aplicaciones y protocolos por ancho de banda firewall Palacio.....	43
8.5	Top de IP por ancho de banda firewall Palacio. ....	44
8.6	Top de destinos web por ancho de banda Firewall Palacio. ....	44
8.7	Top de usuarios con peticiones bloqueadas por el Firewall Palacio.....	44
8.8	Top de las categorías más bloqueadas por el Firewall Palacio. ....	45
8.9	Top de IP más activas Firewall Palacio.....	45
8.10	Top de las categorías más visitadas firewall Palacio.....	45
8.11	Top de consumo ancho de banda por usuario Firewall Palacio.....	46
9.	BALANCEADOR DE CARGA FORTIADC.....	47
9.1	Justicia XXI .....	47
9.2	Kactus RDP .....	48
9.3	Kactus WEB.....	49
9.4	SIRNA.....	50

9.5	Convocatoria Peritos.....	52
9.6	Consulta De Procesos Nacional Unificada (CPNU).....	52
9.7	SIERJU.....	57
9.8	Liquidador de Sentencias.....	57
9.9	Consulta Jurisprudencia.....	58
9.10	API Gestión de Audiencias.....	58
9.11	Portal Alterno de la Rama Judicial.....	59
9.12	Portal de la Rama Judicial.....	59
9.13	Disponibilidad y performance.....	59
10.	TRÁFICO DE WEB APPLICATION FIREWALL (WAF) TORRE CENTRAL.....	60
10.1	Web application firewall datacenter principal IFX.....	60
10.2	Uso de políticas de los servidores en el WAF principal Torre Central.....	61
10.3	Top de peticiones por país WAF principal IFX.....	61
10.4	Top de ataques por política WAF principal IFX.....	62
10.5	Consumo de recursos WAF principal IFX.....	63
11.	TRÁFICO DE WEB APPLICATION FIREWALL (WAF) CAN.....	63
11.1	Disponibilidad WAF CAN.....	63
11.2	Uso de políticas de servidores WAF CAN.....	64
11.3	Top de peticiones por país WAF CAN.....	64
11.4	Top de ataques por política WAF CAN.....	65
11.5	Consumo de recursos WAF CAN.....	65
11.6	Certificado wildcard Rama Judicial *.ramajudicial.gov.co.....	66
12.	DISPONIBILIDAD SEGURIDAD GLOBAL DEL MES DE MARZO.....	67
12.1	Anexo de las solicitudes e incidentes de seguridad reportadas.....	67
13.	CONSUMO MOTORES BASES DE DATOS.....	68
14.	GESTIÓN FINANCIERA.....	68
15.	RECOMENDACIONES.....	69

## 1. INFORMACIÓN TÉCNICA DEL INFORME

Nombre	Informe de disponibilidad de servidores y recursos de <b>RAMA JUDICIAL – CONSEJO SUPERIOR DE LA JUDICATURA</b> alojados en Infraestructura IFX
Descripción	En el presente informe se visualiza la disponibilidad de los servidores y recursos contratados por <b>RAMA JUDICIAL – CONSEJO SUPERIOR DE LA JUDICATURA</b> , 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	<b>Rango de fechas</b> Período del informe: mensual Fecha de inicio: 1 de MARZO de 2024 Fecha de final: 31 de MARZO de 2024
Atributos de entrada	<ul style="list-style-type: none"><li>• Estado, % Memory Used, CPU LOAD, DISK SPACE USED, Top de Usados.</li></ul>
Tablas vistas o utilizadas	Reporte Mensual <b>RAMA JUDICIAL – CONSEJO SUPERIOR DE LA JUDICATURA</b>
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 <b>RAMA JUDICIAL – CONSEJO SUPERIOR DE LA JUDICATURA</b>



## 2. ALOJAMIENTO DE INFRAESTRUCTURA

OC	SID	DESCRIPCIÓN	SUBTIPO	NOMBRE DEL EQUIPO	MODELO	SERIAL	UNIDAD DE RACK	RACK
1	2081796	npn04--Alojamiento de infraestructura - Housing - Cross Conexión - Oro - Puntos de red: 4 - Capacidad de 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 de infraestructura - Housing - Full Rack - Oro - Puntos de red: 4 - Capacidad de energía: 4 KVA - Capacidad en 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 de infraestructura - Housing/Collocation - Energía Adicional KVA - Oro - KVA/Mes - Cantidad: 4	Energía Adicional DC Torre central	Disponibile para uso de la unidad				
4	2081810	npn04--Alojamiento de infraestructura - Housing/Collocation - Punto de 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 Alta Capacidad - Oro - Hosting Nube Privada - Sesiones Capa L4 (entre 36 y 100 Millones) - RAM entre 64GB y 128GB - U_Mes - Cantidad: 2	Balanceador DC Torre central	FORTI/PPLA	ADC-2200F	SN: FAD22F T221000 028	10	32
11	2081818	npn04--IaaS Procesamiento - Balanceador de Carga Alta Capacidad - Oro - Hosting Nube Privada - Sesiones Capa L4 (entre 36 y 100 Millones) - RAM entre 64GB y 128GB - U_Mes - Cantidad: 2	Balanceador DC Torre central	FORTI/BK	ADC-2200F	SN: FAD22F T221000 027	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 2000001 5	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 1900004 9	35-36	32
31	2082016	npn04--IaaS Seguridad - Firewall Nueva Generación - Media Capacidad - Oro - Hosting físico - Rol deFirewall - 40 Gbps - SesionesConcurrentes - 15000000 -Mes - Cantidad: 2	FIREWALL	PALACIO - PPLA	FortiGate 900G	SN: FG9H0G TB2390 0205	N/A	N/A
31	2082017	npn04--IaaS Seguridad - Firewall Nueva Generación - Media Capacidad - Oro - Hosting físico - Rol deFirewall - 40 Gbps - SesionesConcurrentes - 15000000 -Mes - Cantidad: 2	FIREWALL	PALACIO - BK	FortiGate 900G	SN: FG9H0G TB2390 0440	N/A	N/A
32	2082018	npn04--IaaS Seguridad - Firewall Nueva Generación - Alta Capacidad - Oro - Hosting físico - Rol deFirewall - 500 Gbps - Sesiones Concurrentes - 150000000 - Mes - Cantidad:2	FIREWALL DC Torre central	DATACENTE R - BK	FORTIGAT E-4400F	SN: FG440FT K219001 83	27-30	32
32	2082019	npn04--IaaS Seguridad - Firewall Nueva Generación - Alta Capacidad - Oro - Hosting físico - Rol deFirewall - 500 Gbps - Sesiones Concurrentes - 150000000 - Mes - Cantidad:2	FIREWALL DC Torre central	DATA CENTER - PPLA	FORTIGAT E-4400F	SN: FG440FT K219001 84	5-8	32
33	2082013	npn04--IaaS Seguridad - WebApplication Firewall - AltaCapacidad - Oro - Hostingfísico - Desempeño WAF(Gbps) - 10 - Mes - Cantidad:3	WAF DC Torre central	DATACENTE R - PPLA	KEMP LM- X25	SN: TSCC820 05608	14	31

33	2082014	npn04--IaaS Seguridad - WebApplication Firewall - AltaCapacidad - Oro - Hostingfísico - Desempeño WAF(Gbps) - 10 - Mes - Cantidad:3	WAF DC Torre central	DATACENTE R - BK	KEMP LM- X25	SN: TSCB720 00545	13	31
33	2082015	npn04--IaaS Seguridad - WebApplication Firewall - AltaCapacidad - Oro - Hostingfísico - Desempeño WAF(Gbps) - 10 - Mes - Cantidad:3	WAF	SEDE CAN	KEMP LM- X25	SN: TSCC820 05629	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 presentado en la infraestructura contratada, de conformidad con las solicitudes de la Entidad, a corte 30 de MARZO de 2024 es de: **4787962 (P)**

Del monto anterior se descuentan **610000 GB**, de propiedad IFX, para un total **4177962 (P)**

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

**Acorde a la información suministrada con anterioridad, a la fecha la entidad supera en 27962 GB, el almacenamiento contratado**

(Remitirse al anexo "**Inventario\_Servicios\_CSJ\_MARZO\_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 MARZO de 2024 es de: **688000 GB**

Total, contratado de Almacenamiento BK de datos: **600000 GB**

**Acorde a la información suministrada con anterioridad, a la fecha la entidad supera en 88000 GB, el almacenamiento BK de datos contratados.**

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

**Diarios:** De domingo a viernes 20:00pm

**Semanales:** Todos los sábados 20:00pm

**Mensuales:** Ultimo 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\_MARZO\_2024.xls** y **Protección Maquinas virtuales RAMA CSJ** " 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 MARZO 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\_MARZO\_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:

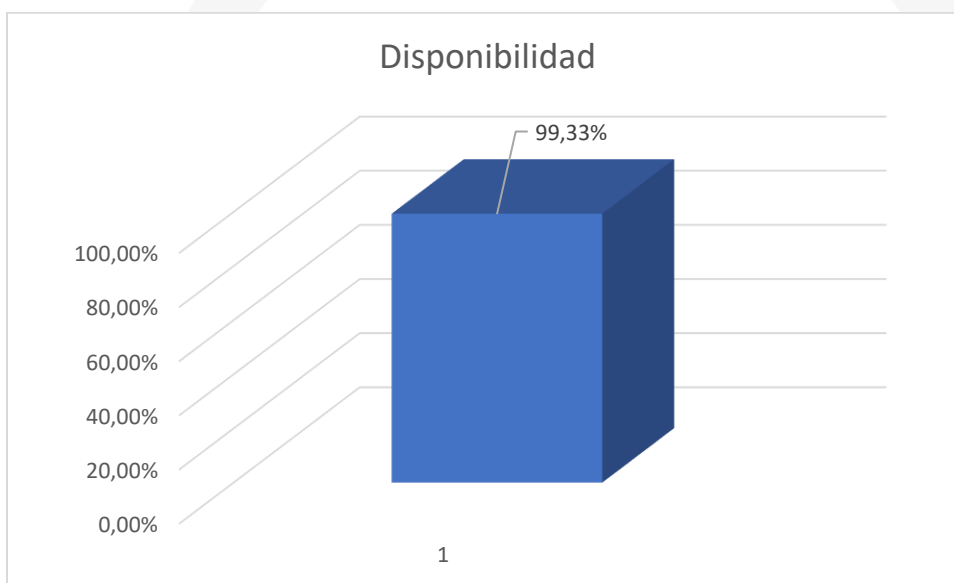
- **Capacitación SST:** líneas de OC 16 y 38
- **Cobro coactivo:** líneas de OC 17 y 38
- **core-impact:** Línea de OC 12
- **Efinomina:** Líneas de OC 14,18,26,27,38 y 39
- **Fuse:** Línea OC 17
- **Gestión grabaciones:** Líneas de OC 12,13, 14,15,17,19,20,22,23,25,28,35,36 y 38
- **InsightVM console:** 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\_MARZO\_2024.xls**" para ver el detalle "maquinas")

## 7.DISPONIBILIDAD GLOBAL CLOUD DEL MES DE MARZO

Disponibilidad Global	Número de tickets por Imputabilidad	
	Responsabilidad IFX	Responsabilidad cliente
	(Número de tickets)	(Número de tickets)
99,33%	6 (1 Incidente y 5 solicitudes)	6 (incidentes)



CONTROL DOCUMENTAL

ELABORADO POR

Fecha	Autor	Ingeniero
03-04-2024	IFX Networks	Juan Carlos Romero

## REVISADO POR

Fecha	Autor	Ingeniero
	IFX Networks	

**1. INTRODUCCIÓN**

El presente documento resume las principales actividades en la provisión de los servicios de Soporte técnico para **Consejo Superior de la Judicatura** durante el periodo 1 marzo a 31 de marzo del 2024.

CONSUMO TOTAL HORAS MES DE MARZO	
• Casos Reportados Netsuite	118
Sesiones de Seguimiento	8
Sesiones de Trabajo	0
Casos Escalados Medio Digital - Whatsapp	6
Horas Disponibilidad del Recurso Fines de Semana	282
Total Horas Consumidas de las 400 - 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 MARZO a 31 de marzo, para el **Consejo Superior de la Judicatura**. Estas mediciones se basan en el número de casos reportados por la aplicación.

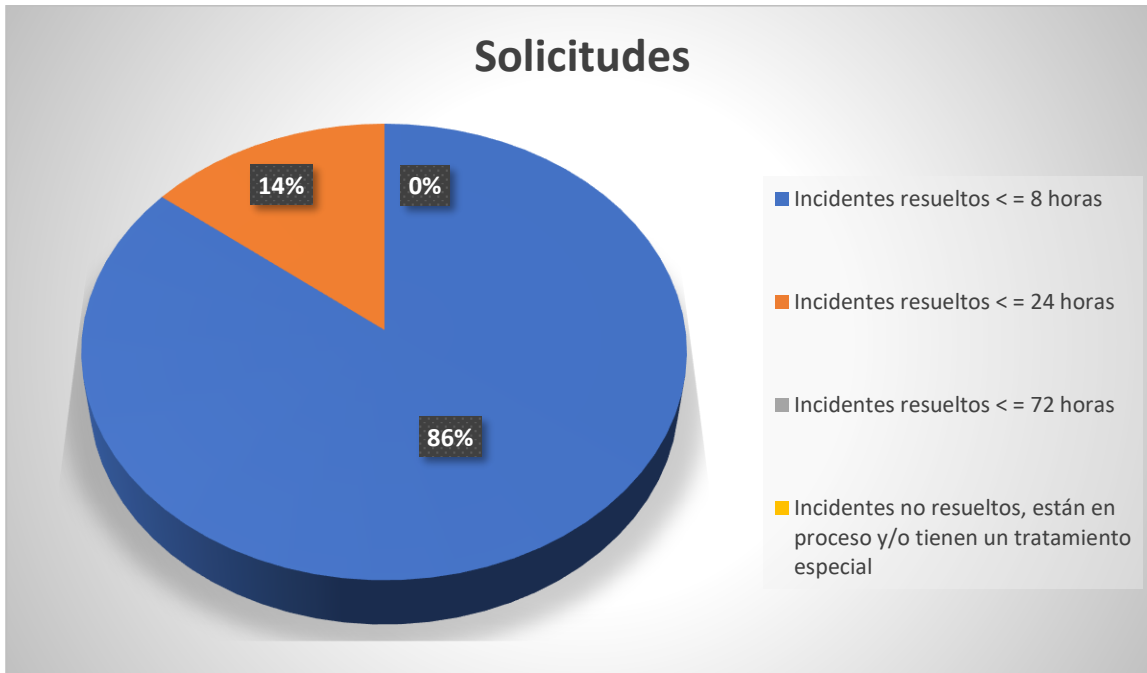
	Volumen en 1 marzo a 31 de marzo
Casos Reportados	14
Solicitudes	12
Incidencias	2
WA - AF	0

**2.1 TASA DE RESOLUCIÓN DE PROBLEMAS**

Tiempo de Gestión	Solicitudes
Solicitudes resueltas < = 4 horas	11
Solicitudes resueltas < = 20 horas	1

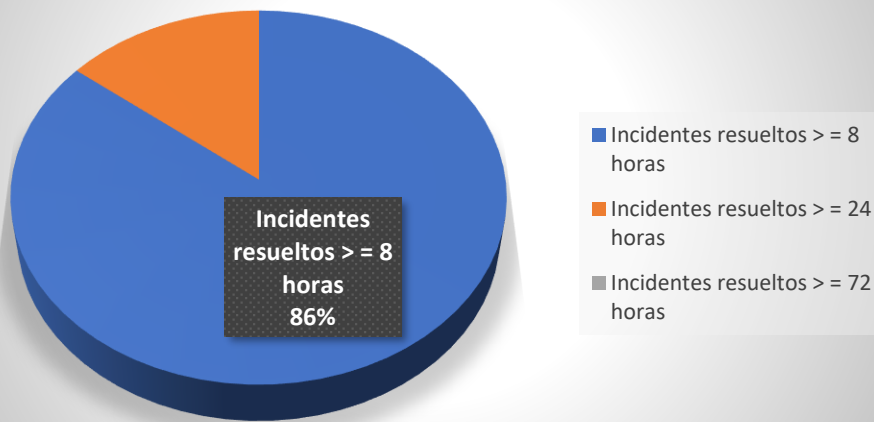


Solicitudes resueltas < = 68 horas	0
Solicitudes no resueltas, están en proceso y/o tienen un tratamiento especial	0
<b>Total</b>	<b>14</b>

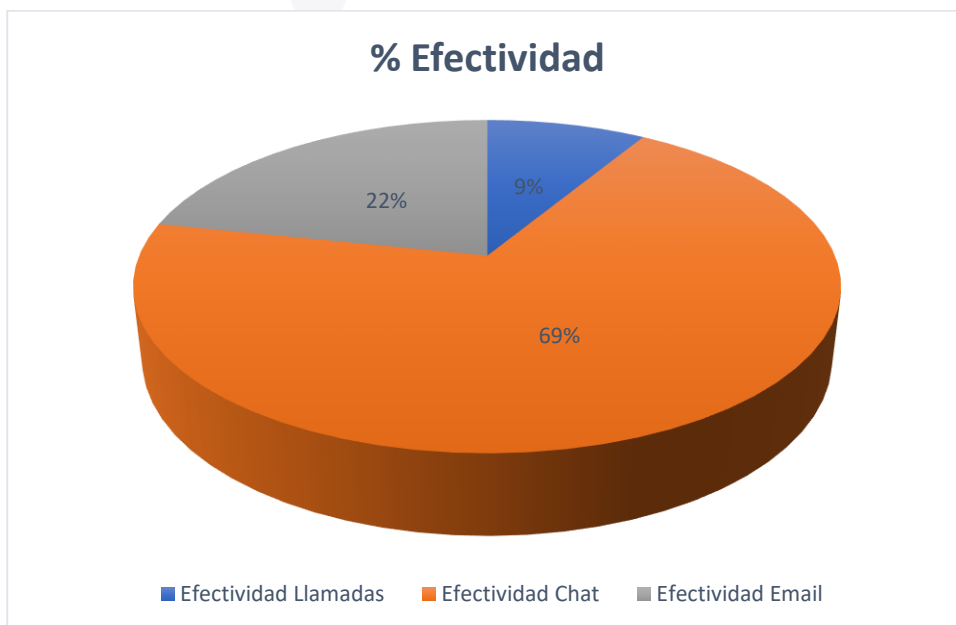
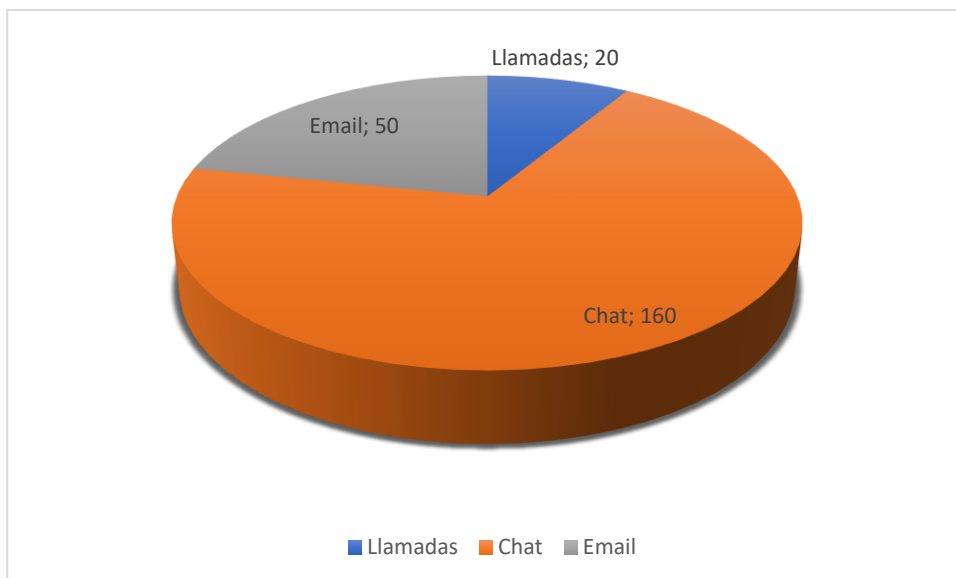


Tiempo de Gestión	Incidentes Penalizados
Incidentes resueltos > = 4 horas	2
Incidentes resueltos > = 20 horas	0
Incidentes resueltos > = 68 horas	0
<b>Total</b>	<b>2</b>

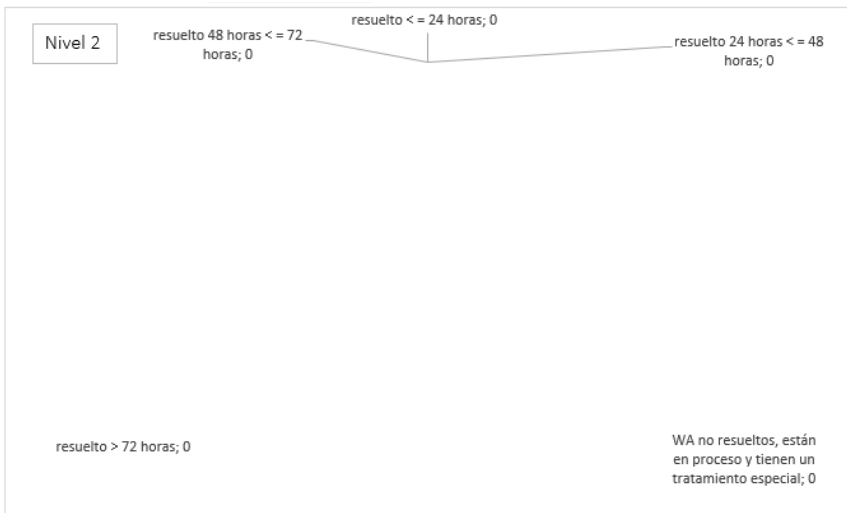
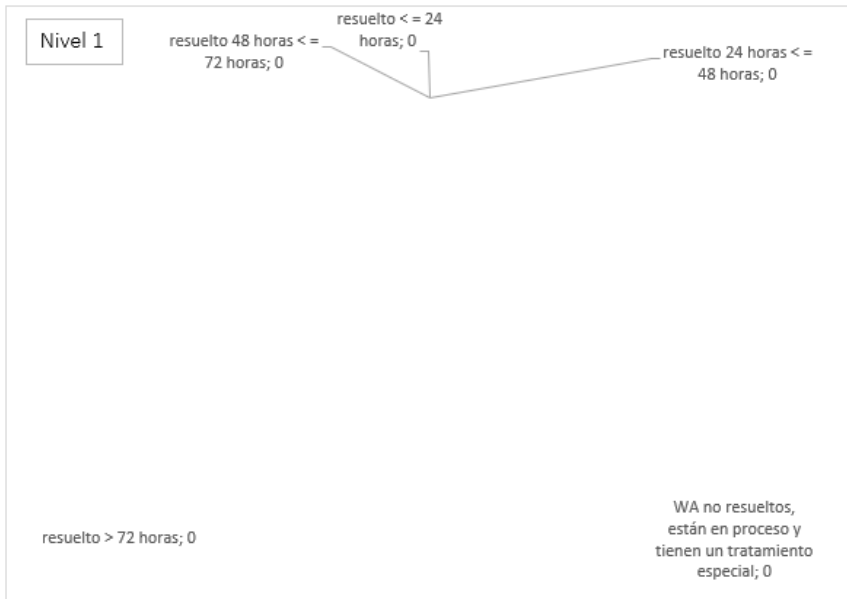
## Incidentes Penalizados

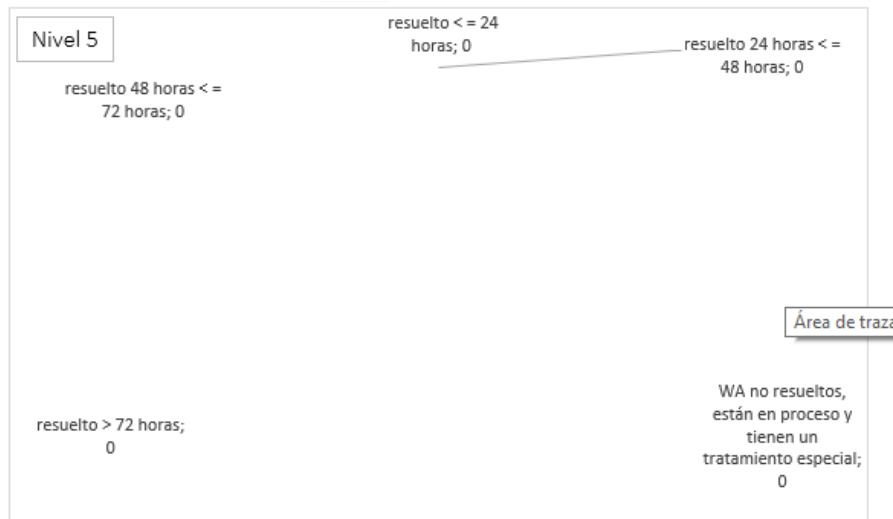
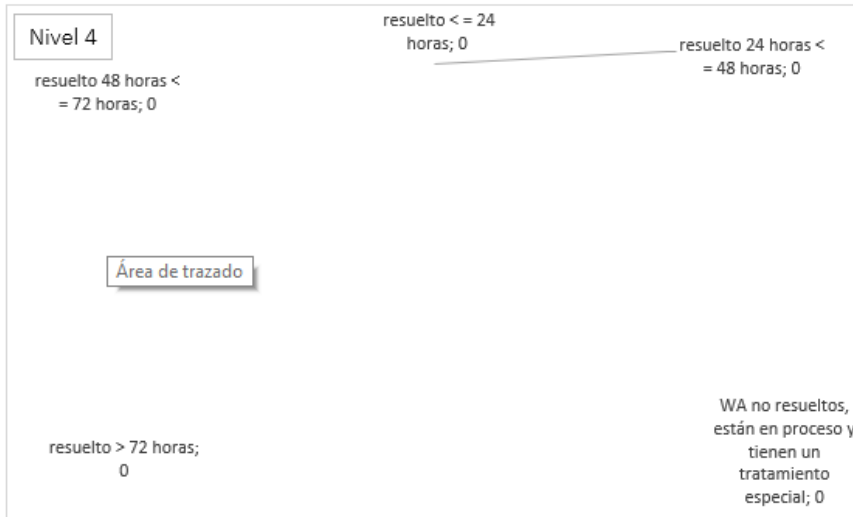


Canales de Atención	Cantidad
Llamadas	20
Chat	160
Email	50
<b>Total</b>	<b>230</b>
<b>Efectividad</b>	<b>%</b>
Efectividad Llamadas	8,70
Efectividad Chat	69,57
Efectividad Email	21,74
<b>Efectividad Total en Canales de Atención</b>	<b>100</b>
<b>No conformidad</b>	<b>0</b>



WA (Ajustes Funcionales)					
Tiempo de Gestión	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
resuelto <= 4 horas	0	0	0	0	0
resuelto 4 horas <= 20 horas	0	0	0	0	0
resuelto 20 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
<b>Total</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>





## 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 marzo a 31 de marzo 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://ifxusamy.sharepoint.com/:x:/r/personal/desarrollocs\\_j\\_ifxcorp\\_com/\\_layouts/15/Doc.aspx?sourcedoc=%7B69A6AAC0-913F-491D-866B-DB9F5BCDDAEE%7D&file=casos%20reportados%20por%20medio%20digital.xlsx&action=default&mobileredirect=true](https://ifxusamy.sharepoint.com/:x:/r/personal/desarrollocs_j_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 marzo a 31 de marzo 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 marzo 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	132	400	268
☑ 2024	132		
☑ Solicitud	129		
☑ Incidencia	3		
<b>Total Horas Casos Reportados Netsuite</b>	<b>132</b>	<b>400</b>	<b>268</b>
		268	268
		268	268
		268	268
		268	268
<b>Horas consumidas de las 400 - Exp</b>	<b>400</b>	<b>400</b>	<b>0</b>

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

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

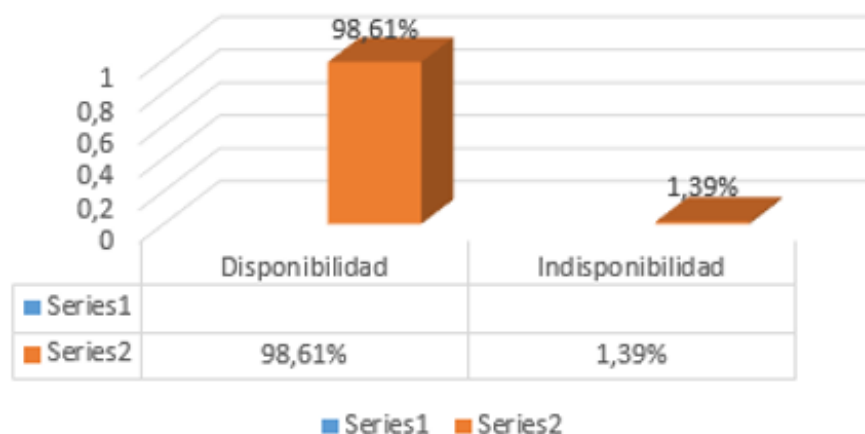
### 3. DISPONIBILIDAD E INDISPONIBILIDAD DE LOS SERVICIOS DE HOSTING

#### 3.1. DISPONIBILIDAD GLOBAL DEL MES DE MARZO

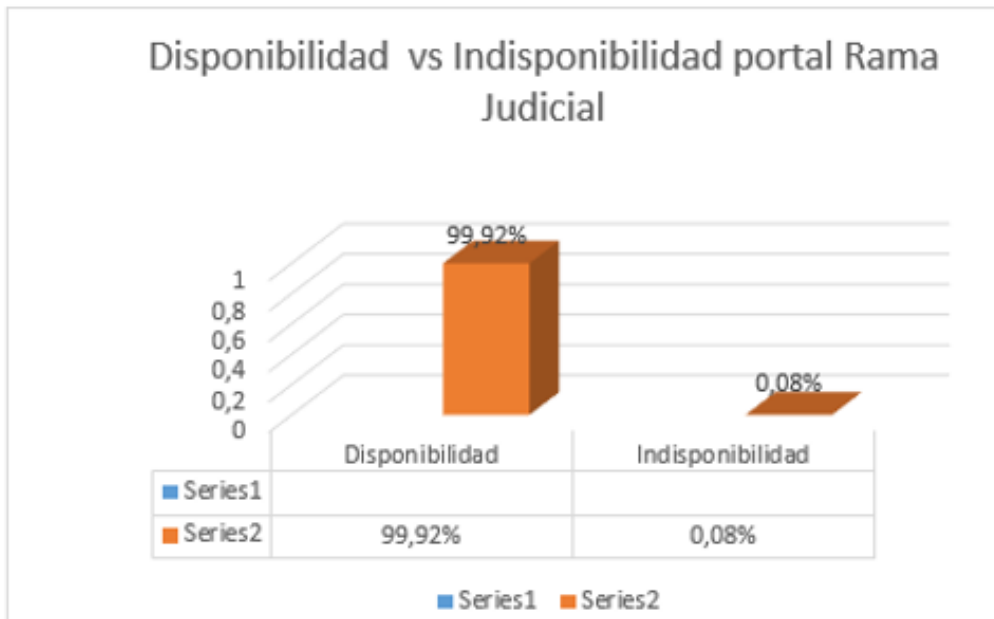
Se visualiza a través de la siguiente matriz los datos de disponibilidad, indisponibilidad y tiempo de caída de las aplicaciones que están soportadas al Consejo Superior de la Judicatura, antes y después de sesión conciliación:

Item	Aplicación	Disponibilidad	Indisponibilidad	Tiempo de duracion (Caída en horas)	Tiempo de duracion			
					Dias	Horas	Minutos	Segundos
1	Portal de la Rama Judicial	98,61%	1,39%	10,33916667	0	10	20	21
	<b>Totales</b>	98,61%	1,39%	10,33916667	0	10	20	21

#### Disponibilidad vs Indisponibilidad portal Rama Judicial

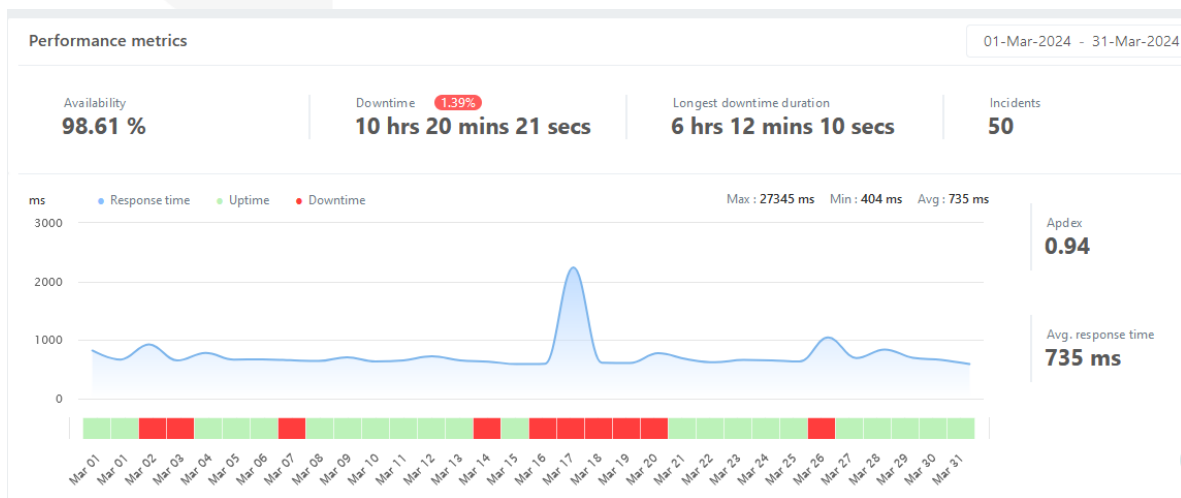


Item	Aplicación	Disponibilidad	Indisponibilidad	Tiempo de duracion (Caída en horas)	Tiempo de duracion			
					Dias	Horas	Minutos	Segundos
1	Portal de la Rama Judicial	99,92%	0,08%	0,562777778	0	1	-26	-14
	<b>Totales</b>	99,92%	0,08%	0,562777778	<b>0</b>	<b>1</b>	<b>-26</b>	<b>-14</b>



### 3.2 PORTAL DE LA RAMA JUDICIAL

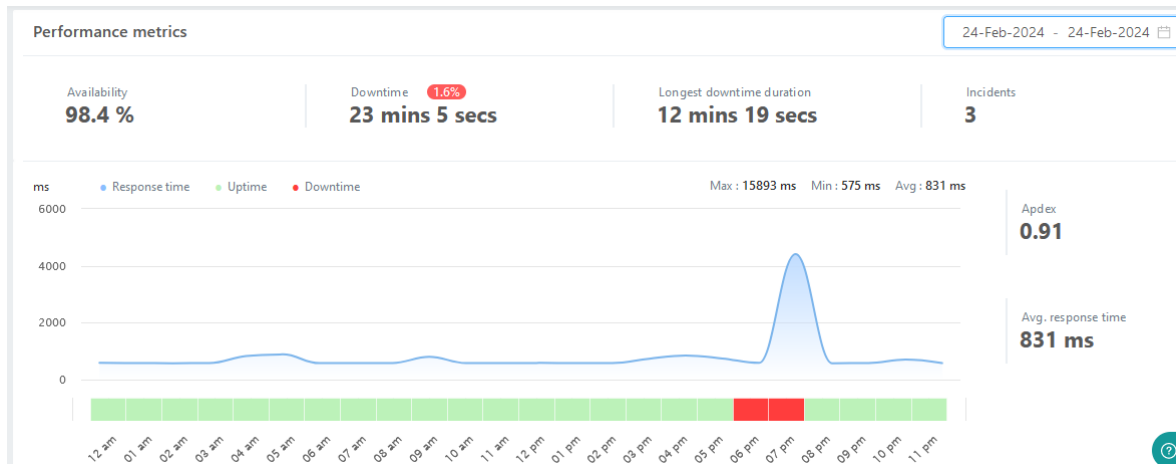
Grafica de la información consolidada de disponibilidad e indisponibilidad del portal del mes de marzo



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

- % de Disponibilidad: 99,89%
- % de Indisponibilidad: 1.39%

Tiempo total de eventos del mes: 10 horas 20 minutos 21 segundos  
Promedio en el tiempo de respuesta que tuvo el portal: 735 ms



Fecha: sábado 24 de marzo

% 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 marzo, 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](https://drive.google.com/drive/folders/1kZx3eIpxxGU_0HqLd7aqEiZ3ie4En1CD?usp=sharing) se cargan las certificaciones y están ubicadas las del mes de marzo 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 marzo.

**BASE DE DATOS**

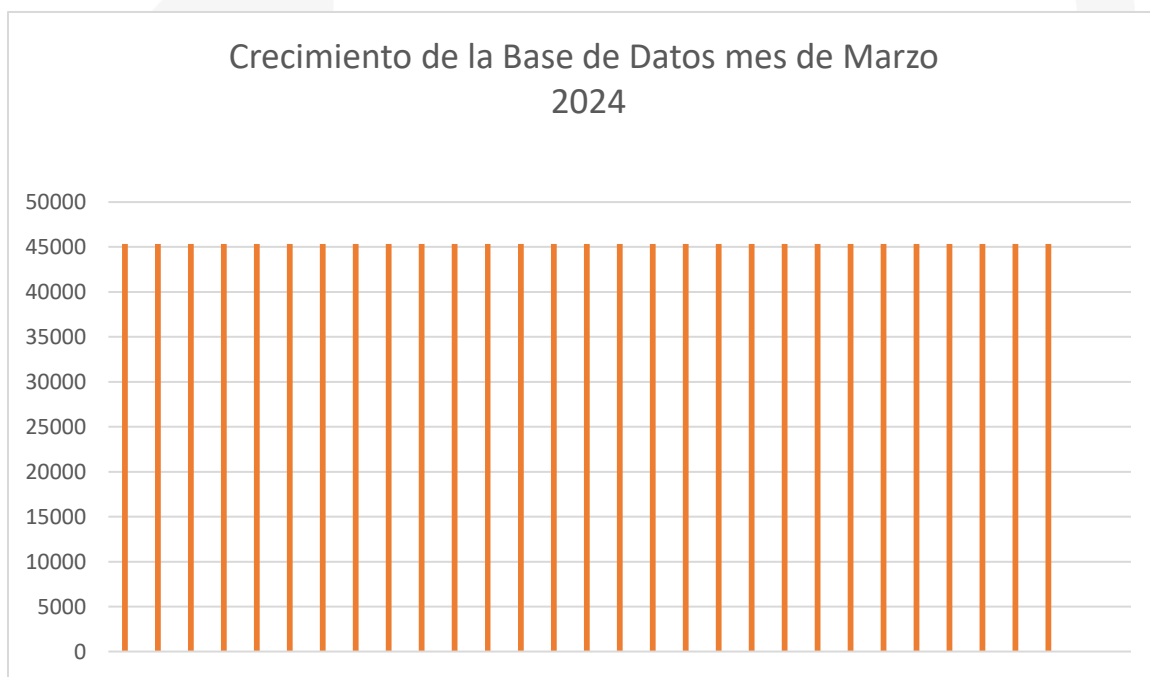
**lportalramaprod**

TAMAÑO (MBO)	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. ESTADÍSTICAS PORTAL DE LA RAMA JUDICIAL

### 4.1 RESUMEN DEL PORTAL



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

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](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 palmas 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

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: FAD22F T221000 028	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: FAD22F T221000 027	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: F12KETB 2000001 5	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: F12KE58 1900004 9	35-36	32
31	2082016	npn04--IaaS Seguridad - Firewall Nueva Generación - Media Capacidad - Oro - Hosting físico - Rol deFirewall - 40 Gbps - SesionesConcurrentes - 15000000 -Mes - Cantidad: 2	FIREWALL	PALACIO - PPLA	FortiGate 900G	SN: FG9H0G TB2390 0205	N/A	N/A
31	2082017	npn04--IaaS Seguridad - Firewall Nueva Generación - Media Capacidad - Oro - Hosting físico - Rol deFirewall - 40 Gbps - SesionesConcurrentes - 15000000 -Mes - Cantidad: 2	FIREWALL	PALACIO - BK	FortiGate 900G	SN: FG9H0G TB2390 0440	N/A	N/A



32	2082018	npn04--IaaS Seguridad - Firewall Nueva Generación - Alta Capacidad - Oro - Hosting físico - Rol de Firewall - 500 Gbps - Sesiones Concurrentes - 150000000 - Mes - Cantidad:2	FIREWALL DC Torre central	DATACENTE R - BK	FORTIGAT E-4400F	SN: FG440FT K219001 83	27-30	32
32	2082019	npn04--IaaS Seguridad - Firewall Nueva Generación - Alta Capacidad - Oro - Hosting físico - Rol de Firewall - 500 Gbps - Sesiones Concurrentes - 150000000 - Mes - Cantidad:2	FIREWALL DC Torre central	DATA CENTER - PPLA	FORTIGAT E-4400F	SN: FG440FT K219001 84	5-8	32
33	2082013	npn04--IaaS Seguridad - WebApplication Firewall - AltaCapacidad - Oro - Hostingfísico - Desempeño WAF(Gbps) - 10 - Mes - Cantidad:3	WAF DC Torre central	DATACENTE R - PPLA	KEMP LM- X25	SN: TSCC820 05608	14	31
33	2082014	npn04--IaaS Seguridad - WebApplication Firewall - AltaCapacidad - Oro - Hostingfísico - Desempeño WAF(Gbps) - 10 - Mes - Cantidad:3	WAF DC Torre central	DATACENTE R - BK	KEMP LM- X25	SN: TSCB720 00545	13	31
33	2082015	npn04--IaaS Seguridad - WebApplication Firewall - AltaCapacidad - Oro - Hostingfísico - Desempeño WAF(Gbps) - 10 - Mes - Cantidad:3	WAF	SEDE CAN	KEMP LM- X25	SN: TSCC820 05629	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 del ítem 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	14/03/2024 18:00	14/03/2024 19:03	1:00:00	Ordinaria diurna	TT809089 VPN Proyecto Calltech 3430, TT809099 RV: HABILITACIÓN DE PÁGINAS INSTITUCIONALE Policía Nacional, TT809106 RV: 2024-0238523: APOYO PARA TRANSMISION DE EVENTO EN VIVO PALACIO DE JUSTICIA DE TURBACO
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	1/03/2024 19:00	1/03/2024 23:00	4:00:00	Diurna/Nocturna	Ventana actualización y armado HA
2	2/03/2024 17:00	2/03/2024 21:00	4:00:00	Diurna	Ventana actualización y armado HA
3	16/03/2024 17:00	16/03/2024 18:00	1:00:00	Diurna	Servicio de parcheo TT808203
4	17/03/2024 16:00	18/03/2024 0:00	8:00:00	Diurna/Nocturna/Dominical	Ventana paso a produccion Portal WEB
5	18/03/2024 6:00	18/03/2024 8:00	2:00:00	Diurna	Ventana paso a produccion Portal WEB
6	20/03/2024 19:30	21/03/2024 0:00	4:30:00	Nocturna	Cambio DDoS 3000E
7	23/03/2024 14:00	23/03/2024 17:00	3:00:00	Diurna	Problema WAF KEMP CAN - Incidente
8	24/03/2024 11:00	25/03/2024 12:00	1:00:00	Diurna/dominical	Caso TT813188
9	25/03/2024 9:00	25/03/2024 13:00	4:00:00	Diurna/dominical	Problema WAF KEMP CAN - Incidente
10	28/03/2024 15:00	28/03/2024 18:00	3:00:00	Diurna/dominical	TT815012,TT815007,TT814976,TT814970,TT814966,TT814962,TT814949
Total horas Extras			34:30:00		

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	13/03/2024 17:00	13/03/2024 18:00	1:00:00	Diurna	Reunion: Sesion cambiar IPv, Convocada por Leonel Torres
2	15/03/2024 23:00	16/03/2024 00:00	1:00:00	Nocturna	Ventana paso a produccion Portal WEB
3	16/03/2024 17:00	16/03/2024 19:00	2:00:00	Nocturna	Ventana de migracion de FortiDDoS (Cancelada)
4	17/03/2024 11:00	17/03/2024 13:00	2:00:00	Diurna/Nocturna/Dominical	Ventana paso a produccion Portal WEB
5	17/03/2024 15:00	17/03/2024 17:00	2:00:00	Diurna/Nocturna/Dominical	Ventana paso a produccion Portal WEB
6	17/03/2024 20:00	17/03/2024 21:00	1:00:00	Diurna/Nocturna/Dominical	Ventana paso a produccion Portal WEB/Caso: TT810065,TT810074
7	18/03/2024 00:00	18/03/2024 02:00	2:00:00	Nocturna	Llamada del ingeniero Leonel Torres por caída del portal: <a href="https://www.ramajudicial.gov.co/">https://www.ramajudicial.gov.co/</a>
8	20/03/2024 19:00	21/03/2024 01:00	6:00:00	Nocturna	Ventana de migracion de FortiDDoS
Total horas Extras			17:00:00		

## 14.2. Inventario de equipos de seguridad perimetral.

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

Nº	Descripción	Hostname	Serial	SID	Ubicación	Version Firmware
1	FortiGate-4400F HA	FTG_CSJ_DC_TC_MASTER	FG440FTK21900184	2082019	DC IFX	v7.0.14
		FTG_CSJ_DC_TC_SLAVE	FG440FTK21900183	2082018	DC IFX	v7.0.14
2	FORTIADC 2200F HA	FADC_CSJ_TC_MASTER	FAD22FT221000027	2081818	DC IFX	v6.1.3
		FADC_CSJ_TC_SLAVE	FAD22FT221000028	2081817	DC IFX	v6.1.3
3	WAF KEMP Loadmaster x25 HA	WAF_TORRRE_CENTRAL	TSCC82005608	2082013	DC IFX	7.2.59.3.22368
		WAF_TORRRE_CENTRAL	TSCC8200529	2082014	DC IFX	7.2.59.3.22368
4	Fortigate 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	7.2.59.3.22368
6	FortiDDoS 1500F HA	CSJ_FDDoS_MASTER	FI1K5FTE20000012	2082020	DC IFX	v6.3.3
		CSJ_FDDoS_SLAVE	FI1K5FTE20000011	2082021	DC IFX	v6.3.3

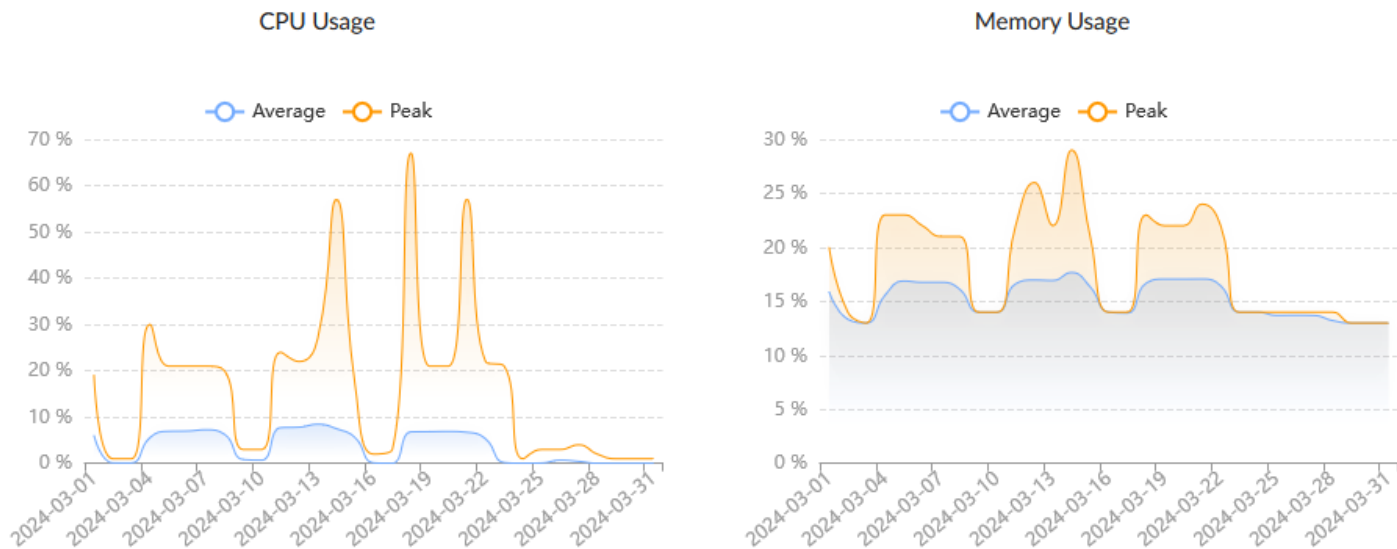
## 14.3. Actualización de firmware.

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_SLAVE	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_3500F_CSJ_PALACIO_M	V7.2.6	Actualizado	N/A
FGT_3500F_CSJ_PALACIO_S	V7.2.6	Actualizado	N/A
WAF_CAN KEMP	7.2.59.3.22368	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 marzo, el consumo promedio de CPU y memoria en el firewall perimetral estuvo dentro de sus valores de operación normal.



### 15.1. Disponibilidad mensual firewall perimetral.

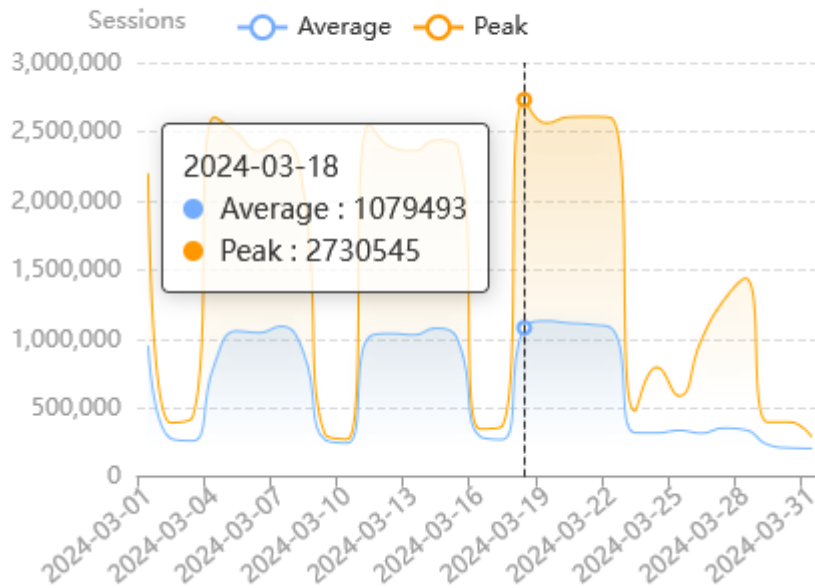
Durante marzo se obtuvo una disponibilidad del 100 % en el firewall perimetral. El evento del 1 de marzo corresponde a una falla en el sistema de Gestión Orión con el caso IFX TT802944 y el 5 de marzo se presentó falla de conectividad con la gestión Orión que fue solucionada desactivando la policy route 23 en el fortigate Torre Central. Ninguno de estos eventos ocasionó afectación de los servicios productivos del CSJ:



### 15.2. Cantidad de sesiones firewall perimetral.

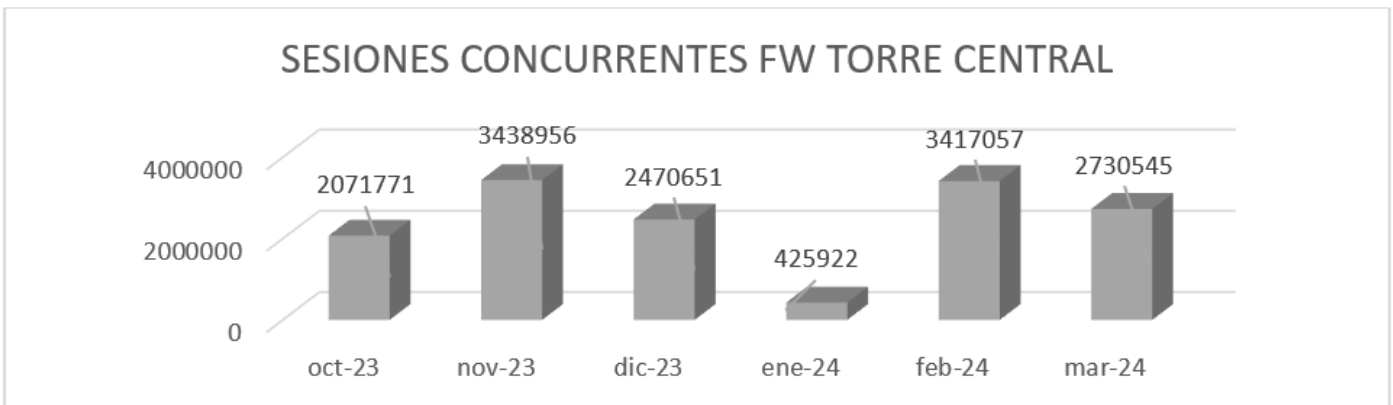
Durante marzo se presentó un máximo de 2'730.545 sesiones TCP concurrentes, cantidad que se encuentra dentro del rango máximo soportado por el equipo Fortinet FG- 4400F cuyo valor es de 210 millones.

### Session



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

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



MES	SESIONES
oct-23	2071771
nov-23	3438956
dic-23	2470651
ene-24	425922
feb-24	3417057
mar-24	2730545

## 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			341.56 TB
2	Microsoft.Portal			106.55 TB
3	Microsoft.SharePoint			59.75 TB
4	Microsoft.365.Portal			32.29 TB
5	SSL			31.10 TB
6	TCP/9443			27.22 TB
7	DTLS			26.02 TB
8	Akamai-CDN			21.95 TB
9	Microsoft.Outlook			21.48 TB
10	SMB			20.89 TB

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

Top Applications by Sessions

#	Application	Sessions
1	SMB	2,551,246,269
2	HTTPS	1,534,609,536
3	DNS	1,134,625,199
4	SSL	504,472,054
5	Microsoft.Windows.Update	452,536,343
6	Microsoft.Portal	380,762,902
7	Microsoft-Web	357,969,186
8	Microsoft.365.Portal	328,965,141
9	TCP/448	327,274,946
10	ESET-Eset.Service	295,753,909

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

El servidor de la CPNU 172.31.10.41 en IFX presentó la mayor cantidad de sesiones:

Top Bandwidth IP

#	IP	Bandwidth
1	172.31.10.41	70.16 TB
2	172.31.10.43	4.85 TB
3	10.101.100.114	2.66 TB
4	10.101.100.38	1.86 TB
5	10.101.100.182	1.68 TB
6	10.114.5.26	1.03 TB
7	10.101.100.34	1.00 TB
8	10.101.100.134	976.79 GB
9	10.101.100.122	921.12 GB
10	10.101.101.70	784.83 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 marzo 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	348,560,715
2	microsoft.com	251,849,184
3	190.217.24.69	186,466,278
4	8.243.164.21	148,284,113
5	190.217.24.155	145,789,735
6	200.31.13.169	136,975,498
7	windowsupdate.com	115,448,978
8	rapid7.com	105,728,240
9	172.28.146.154	97,200,394
10	172.28.107.58	95,862,563

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

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

Top Web Users by Blocked Requests

#	User (or IP)	Hostname	Requests
1	192.168.125.26	192.168.125.26	11,377,145
2	172.16.56.165	172.16.56.165	9,550,193
3	172.27.90.88	172.27.90.88	6,200,493
4	192.168.199.35	192.168.199.35	4,843,828
5	172.17.97.87	172.17.97.87	4,573,135
6	172.26.176.6	172.26.176.6	3,980,562
7	192.168.125.17	192.168.125.17	3,591,906
8	172.16.128.102	172.16.128.102	3,559,946
9	172.27.90.208	172.27.90.208	3,264,535
10	192.168.208.128	192.168.208.128	2,618,014

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.

Teniendo en cuenta que son IPs bloqueadas, no se obtiene información del consumo ancho de banda.



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

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

### Top Blocked Web Categories

#	Category	Requests
1	Internet Radio and TV	99,003,354
2	Streaming Media and Download	4,788,263
3	Social Networking	4,534,087
4	Proxy Avoidance	3,158,095
5	Games	1,670,130
6	Information Technology	1,632,654
7	Entertainment	863,757
8	Unrated	807,456
9	IOC_Blacklist_Domains_Cyber	297,052
10	Gambling	98,728

## 15.9. Top de IP más activos Firewall Perimetral

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

### Top Web IP by Allowed Requests

#	IP	Requests
1	10.101.100.38	9,561,417
2	10.101.100.114	7,893,862
3	10.101.100.34	5,988,987
4	10.101.100.110	5,335,071
5	10.101.100.194	4,986,379
6	10.101.100.122	4,720,303
7	10.101.100.138	4,619,441
8	10.101.100.70	4,099,185
9	10.101.100.134	3,964,574
10	10.101.100.170	3,946,681

## 15.10. Top de categorías más visitadas Firewall Perimetral

La categoría más visitada durante marzo fueron Information Technology:

### Top Allowed Web Categories

#	Category	Requests
1	Information Technology	367,362,306
2	Override_permitidas	10,994,478

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

172.31.10.41 (servidor de la CPNU), 172.17.201.251 (WAF de Torre Central) y 172.17.202.251 (WAF CAN) presentaron el mayor consumo de ancho de banda durante marzo:

#### Top IP by Bandwidth

#	IP	Bandwidth	Sent	Received
1	172.31.10.41			76.35 TB
2	172.17.201.251			51.87 TB
3	172.17.201.252			49.44 TB
4	172.28.146.83			34.60 TB
5	172.28.146.82			30.85 TB
6	172.27.64.17			30.76 TB
7	172.28.146.79			27.40 TB
8	10.244.2.239			10.62 TB
9	172.27.64.61			9.25 TB
10	erubianr			6.21 TB

## 7. TRÁFICO VPN FIREWALL PERIMETRAL

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

#	f_user	devname	vpn_type_group	end_time	fv_dtime_tz_conv_e_time_tremip	connections	Duration	bandwidth	traffic_in	traffic_out
1	jsierr adear	CSJ_FT G_DC_ TC_FG 4400_	ssl-tunnel	2024-0 3-27 21: 49:45	1711576185 181.71.242.139	67	105389 4	78165300 541	2048148 414	76117152 127
2	nroja sb	CSJ_FT G_DC_ TC_FG 4400_	ssl-tunnel	2024-0 3-31 16: 51:05	1711903865 181.135.215.17	35	239207	65089118 757	2850312 769	62238805 988
3	Mfor eroP	CSJ_FT G_DC_ TC_FG 4400_	ssl-tunnel	2024-0 3-31 22: 47:40	1711925260 177.93.52.219;1 81.234.181.32;1 81.234.186.103; 181.234.190.47; 186.102.7.128;1 86.114.127.35;1 86.119.198.26;1 86.168.233.218; 186.169.11.248; 186.169.8.88	67	791613	50966533 621	1230587 177	49735946 444
4	lvca mpos	CSJ_FT G_DC_ TC_FG 4400_	ssl-tunnel	2024-0 3-27 17: 35:11	1711560911 186.30.178.167; 186.30.18.80	38	612862	47834275 889	1306991 986	46527283 903
5	rgarc iav	CSJ_FT G_DC_ TC_FG 4400_	ssl-tunnel	2024-0 3-24 17: 21:57	1711300917 181.128.165.18 4;181.128.18.20 0;181.128.221.6 4;181.128.52.5 9;181.128.53.14 6;181.128.79.7; 181.128.95.201	15	251215	47704968 933	2317220 751	45387748 182

6	asar miev	CSJ_FT G_DC_ TC_FG 4400_	ssl-tunnel	2024-0 3-27 16: 45:56	1711557956	181.59.148.108; 181.59.148.124; 181.59.148.151; 181.59.148.46;1 81.59.148.58;18 1.59.148.71;18 1.59.148.74;18 1.59.148.78;18 1.59.2.104;181. 59.2.126;181.5 9.2.185;181.59. 2.241;181.59.3. 165;181.59.3.20 0;181.59.3.209; 186.102.108.17 9;186.102.18.6 4;186.102.20.8 1;186.102.39.23 2;186.102.44.8 8;186.102.51.23 0;186.102.70.1 1;186.102.70.17 9;186.102.91.1	110	862839	43840578 183	1433925 945	42406652 238
						9;186.102.94.8 0;186.102.96.20 5;191.156.145.1 23;191.156.146. 168;191.156.14 7.135;191.156.1 51.24;191.156.1 52.145;191.156. 158.185;191.15 6.178.5;191.15 6.181.205;191.1 56.225.186;191. 156.238.3;191.1 56.48.52;191.15 6.50.88;191.15 6.52.49;191.15 6.52.91;191.15 6.53.22;191.15 6.54.1;191.156. 54.171;191.156. 58.117;191.156. 60.104;191.156. 60.222;191.156. 61.5					
7	amor acr	CSJ_FT G_DC_ TC_FG 4400_	ssl-tunnel	2024-0 3-27 17: 51:40	1711561900	186.84.88.119;1 86.84.90.29;19 0.26.3.205	77	846165	43087902 149	1796495 273	41291406 876
8	yanan gul	CSJ_FT G_DC_ TC_FG 4400_	ssl-tunnel	2024-0 3-22 16: 39:31	1711125571	186.28.128.11;1 86.30.136.51;18 6.30.74.86	28	543508	39829141 482	7545456 61	39074595 821

9	vcaroal	CSJ_FT G_DC TC_FG 4400_	ssl-tunnel	2024-03-27 19:22:03	1711567323	152.204.136.86; 80 181.206.98.91;1 81.237.235.102; 181.237.251.11 4;181.32.216.17 6;181.59.3.233; 190.128.105.64; 191.104.112.47	722486	34314591 192	1427214 575	32887376 617
10	lvelozam	CSJ_FT G_DC TC_FG 4400_	ssl-tunnel	2024-03-08 17:00:28	1709917228	190.248.102.12 13 3	199296	33308605 624	1682295 882	31626309 742

## 16.1. VPN IPSEC Site To Site Firewall Perimetral

El consumo de ancho de banda de las VPN IPsec Site to Site durante marzo fue el siguiente:

CSJ\_FTG\_DC\_TC\_FG4400\_ Custom ... Mar 01 2024 - Mar 31 2024 Dark Mode

Site-to-Site IPsec Top: 100 Lite

#	Site-to-Site IPsec Tunnel	Initiating FortiGate	Terminating FortiGate	Bytes (Sent/Received)
1	VPN_AZURE	190.217.24.4 Bogota Colombia	52.240.53.161 Potomac Falls Unite	27.3 TB/1019.9 GB
2	VPN_ORACLE	190.217.80.4 Barrancabermeja	129.213.6.36 Ashburn United Stat	54.2 GB/890.5 GB
3	VPN_ORACLE	190.217.80.4 Barrancabermeja	129.213.7.34 Ashburn United Stat	979.9 MB/572.6 GB
4	VPN_AZURE-ANALY	190.217.24.4 Bogota Colombia	20.124.34.235 Potomac Falls Unite	298.6 GB/7.9 GB
5	VPN_Tierras	190.217.24.4 Bogota Colombia	181.225.76.196 Anserma Colombi	2.3 GB/40.5 GB
6	VPN_SIUG_AWS-2	190.217.24.4 Bogota Colombia	34.224.152.152 Ashburn United St	408.7 MB/531.0 MB
7	VPN_SIUG_AWS	190.217.24.4 Bogota Colombia	34.194.187.190 Ashburn United St	408.7 MB/530.3 MB
8	VPN_INPEC	190.217.19.156 Bogota Colom	190.25.112.10 Bogota Colombia	102.3 MB/515.3 MB
9	VPN_REGISTRADU	190.217.24.4 Bogota Colombia	201.232.123.20 Medellin Colombi	199.8 MB/213.1 MB
10	VPN_Linktic	190.217.24.4 Bogota Colombia	3.222.171.115 Ashburn United Sta	142.0 MB/167.0 MB
11	OCI_EXADATA_FAB	190.217.24.4 Bogota Colombia	150.136.25.96 Ashburn United Sta	69.6 MB/0.0 KB
12	VPN_FISCALIA	190.217.24.4 Bogota Colombia	190.157.218.66 Bogota Colombia	2.0 MB/36.5 MB

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

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

## Top Attacks

#	Attack Name	Severity	CVE-ID	Counts
1	tcp_syn_flood	Critical		456,603
2	tcp_src_session	Critical		392,450
3	tcp_port_scan	Critical		128,921
4	ip_src_session	Critical		35,677
5	Spring.Framework.SerializationUtils.Insecure.Deserialization	Critical	CVE-2022-22965	35,282
6	tcp_dst_session	Critical		9,668
7	Apache.Log4j.Error.Log.Remote.Code.Execution	Critical	CVE-2021-4104,CVE-2021-44228,CVE-2021-45046	8,780
8	Adobe.ColdFusion.Multiple.Vulnerabilities	Critical	CVE-2013-0625,CVE-2013-0629,CVE-2013-0631,CVE-2013-0632	6,773
9	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	Critical	CVE-2017-11317,CVE-2017-11357,CVE-2019-18935	4,626
10	Remote.CMD.Shell	Critical		4,603

Las víctimas de intrusión fueron los siguientes hosts:

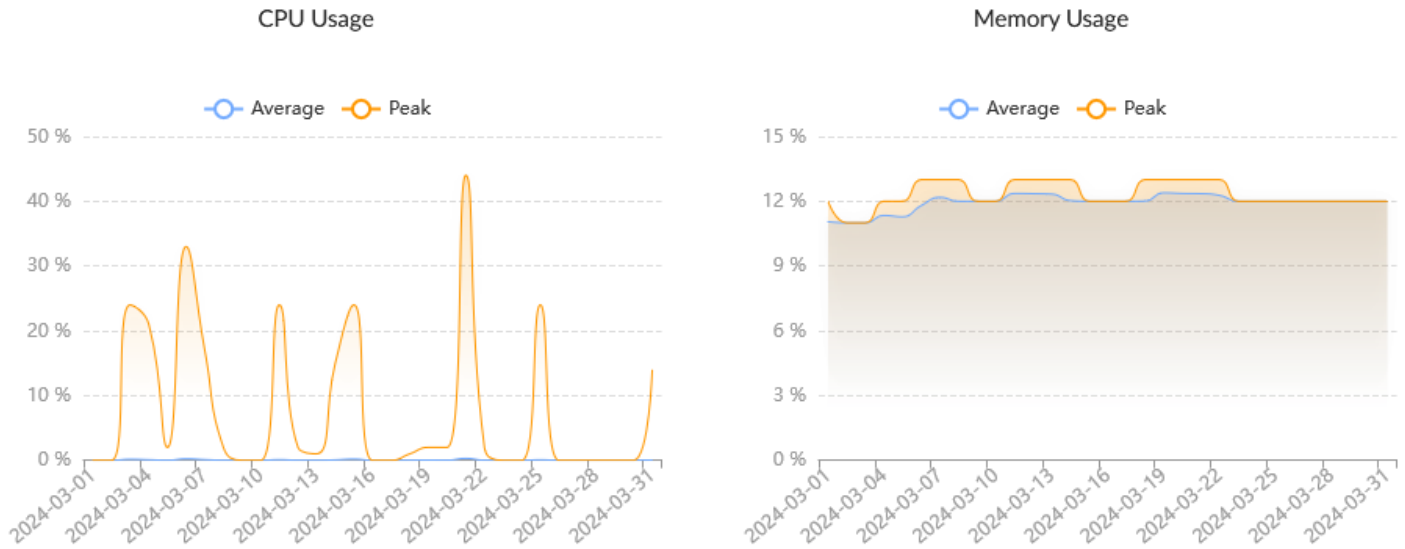
## Top Intrusion Victims

#	Attack Victim	Counts	■ Critical ■ High ■ Medium	Percent of Total Attacks
1	190.217.24.172			284,863 25.33%
2	190.217.24.69			278,489 24.76%
3	172.17.201.26			221,391 19.69%
4	172.17.201.68			197,795 17.59%
5	172.17.201.25			42,492 3.78%
6	190.217.24.149			22,172 1.97%
7	161.18.255.202			19,702 1.75%
8	185.196.10.85			7,985 0.71%
9	34.29.85.190			6,075 0.54%
10	172.17.201.101			4,940 0.44%
11	192.168.89.28			4,388 0.39%
12	172.17.201.52			4,090 0.36%
13	172.28.108.94			4,089 0.36%
14	172.17.201.249			3,950 0.35%
15	34.80.59.191			3,931 0.35%
16	192.168.213.229			3,846 0.34%
17	172.17.201.28			3,716 0.33%
18	172.17.201.88			3,707 0.33%
19	172.17.201.54			3,501 0.31%
20	172.17.201.31			3,452 0.31%

Los hosts 190.217.24.69, 172.17.201.x y 172.17.202.x son las aplicaciones web, sin embargo, están siendo contenidos por el firewall central y no alcanzan a llegar a los WAF de Torre Central y del CAN.

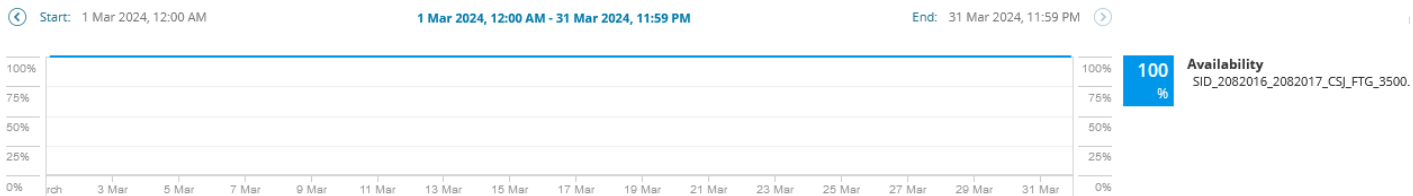
## 8. FIREWALL SEDE PALACIO

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



### 8.1 Disponibilidad Mensual Firewall Palacio

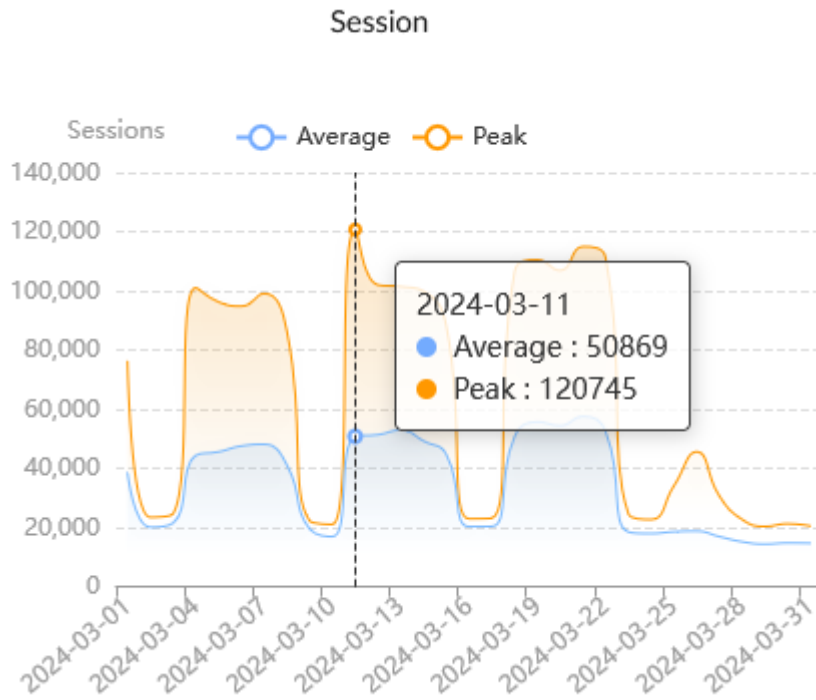
Durante marzo se obtuvo una disponibilidad del 100 % en el firewall de Palacio.



### 8.2 Cantidad de Sesiones Firewall Palacio

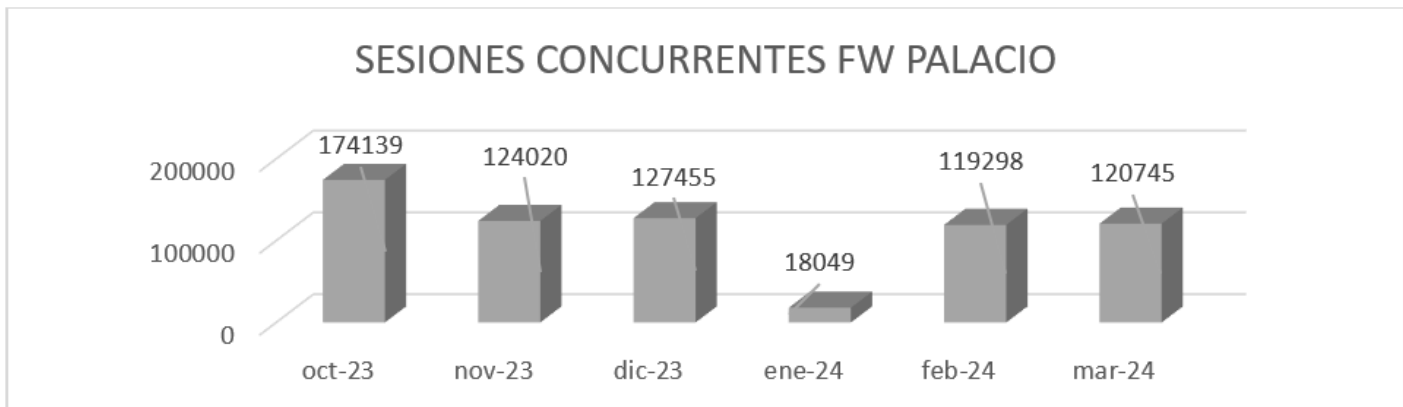
Durante marzo se presentó un máximo de 120.745 sesiones concurrentes que están dentro del rango de sesiones soportadas por el equipo Fortigate 3500F de 160 Millones.





### 8.3 Histórico de Sesiones Últimos 6 meses Firewall Palacio

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



MES	SESIONES
oct-23	174139
nov-23	124020
dic-23	127455
ene-24	18049
feb-24	119298
mar-24	120745



## 8.4 Aplicaciones y protocolos por ancho de banda firewall Palacio

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

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	HTTPS		24.93 TB	
2	Microsoft.Portal		6.82 TB	
3	Microsoft.SharePoint		4.64 TB	
4	OneDrive		2.97 TB	
5	HTTPS.BROWSER		2.78 TB	
6	Microsoft.365.Portal		1.73 TB	
7	Akamai-CDN		1.62 TB	
8	HTTP		1.47 TB	
9	SMB		1.46 TB	
10	MS-SQL		1.39 TB	

Por sesiones las aplicaciones con mayor consumo fue SMB:








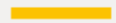












Top Applications by Sessions

#	Application	Sessions
1	SMB	1,137,680,100
2	DNS	189,730,654
3	Microsoft.Windows.Update	44,540,644
4	HTTP.BROWSER	41,804,314
5	HTTPS	39,404,671
6	SQUID	36,236,067
7	Microsoft.Portal	29,018,274
8	SSL	28,576,264
9	HTTP	25,945,546
10	Rapid7.Insight.Agent	23,783,153

## 8.5 Top de IP por ancho de banda firewall Palacio.

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





















Top Bandwidth IP

#	IP	Bandwidth
1	 172.28.93.2	 3.12 TB
2	 172.16.2.59	 1.01 TB
3	 172.17.114.19	 677.16 GB
4	 172.16.5.80	 611.52 GB
5	 172.16.5.113	 305.16 GB
6	 172.16.4.195	 303.49 GB
7	 172.29.154.38	 299.74 GB
8	 172.29.154.19	 223.19 GB
9	 172.16.4.193	 210.63 GB
10	 172.29.154.13	 184.79 GB

## 8.6 Top de destinos web por ancho de banda Firewall Palacio.





















Los destinos más visitados durante marzo fueron 20.60.0.104, 13.107.136.10, 13.107.138.10 y 52.104.3.39 (Microsoft Corporation):

Top Websites and Category by Bandwidth

#	Site	Category	Bytes
1	20.60.0.104		 2.82 TB
2	13.107.136.10		 2.33 TB
3	13.107.138.10		 2.27 TB
4	52.104.3.39		 1.71 TB
5	20.209.75.97		 638.25 GB
6	20.60.128.228		 635.40 GB
7	20.209.52.65		 583.81 GB
8	172.190.220.253		 562.43 GB
9	20.168.235.216		 433.90 GB
10	20.209.74.225		 314.23 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	 172.28.93.142	172.28.93.142	 94,324
2	 192.168.8.100	192.168.8.100	 48,601
3	 172.16.5.53	172.16.5.53	 43,033
4	 172.16.4.227	172.16.4.227	 33,944
5	 172.16.5.230	172.16.5.230	 30,806
6	 172.16.4.190	172.16.4.190	 30,070
7	 172.16.5.69	172.16.5.69	 26,456
8	 172.17.74.96	172.17.74.96	 23,320
9	 172.29.154.61	172.29.154.61	 15,677
10	 172.17.74.59	172.17.74.59	 12,776

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

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

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

Top Blocked Web Categories

#	Category	Requests
1	Unrated	961,969
2	Streaming Media and Download	453,297
3	Proxy Avoidance	350,655
4	Social Networking	199,167
5	Games	74,159
6	Entertainment	73,010
7	Dating	36,875
8	Malicious Websites	8,915
9	Society and Lifestyles	8,422
10	Phishing	5,565

## 8.9 Top de IP más activas Firewall Palacio

172.28.54.20 y 172.16.4.90 (Servidores de antivirus) presentaron la mayor cantidad de conexiones durante marzo:

Top Web IP by Allowed Requests

#	IP	Requests
1	172.28.54.20	19,651,587
2	172.16.4.90	14,033,626
3	172.28.93.45	1,366,807
4	172.16.4.30	1,313,597
5	172.16.4.246	496,387
6	172.28.93.101	377,611
7	172.16.7.96	348,562
8	172.17.114.77	342,083
9	172.28.93.176	332,769
10	172.29.154.22	331,955

## 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	35,611,450
2	Search Engines and Portals	5,252,988
3	Business	1,241,557
4	Information and Computer Security	466,669
5	Web Analytics	367,839
6	Web-based Applications	139,803
7	Online Meeting	83,441
8	Finance and Banking	73,494
9	Override permitidas	31,920
10	Government and Legal Organizations	31,258

## 8.11 Top de consumo ancho de banda por usuario Firewall Palacio

192.168.2.71 (Servidor Web de la Corte Constitucional) presento la mayor cantidad de conexiones durante marzo:

## Top IP by Bandwidth

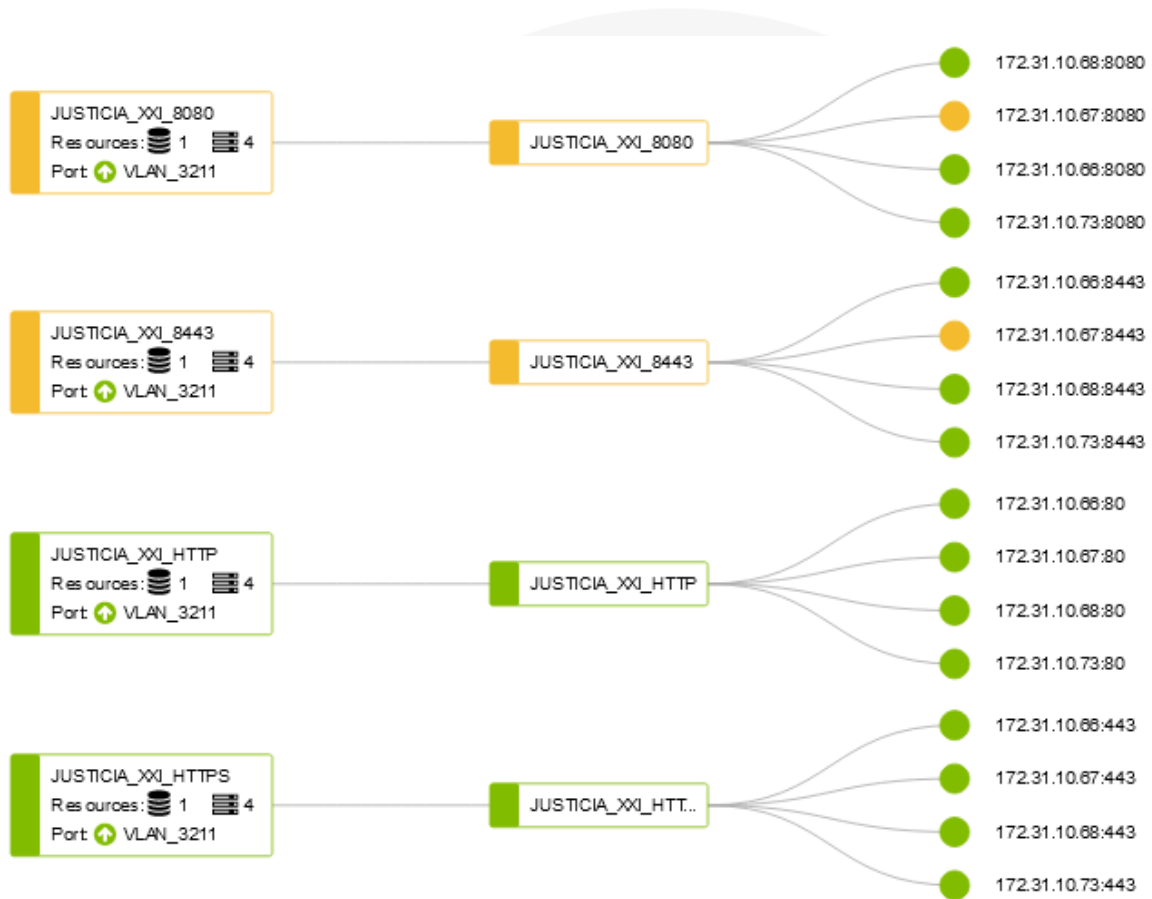
#	IP	Bandwidth	Sent	Received
1	192.168.2.71	15.01 TB		
2	172.17.201.251	4.67 TB		
3	172.17.201.252	4.57 TB		
4	172.28.93.2	3.14 TB		
5	10.101.250.4	2.23 TB		
6	172.16.4.121	1.36 TB		
7	172.17.202.250	1.35 TB		
8	172.16.2.59	1.12 TB		
9	172.17.114.19	686.10 GB		
10	172.28.107.59	639.52 GB		

## 9. BALANCEADOR DE CARGA FORTIADC

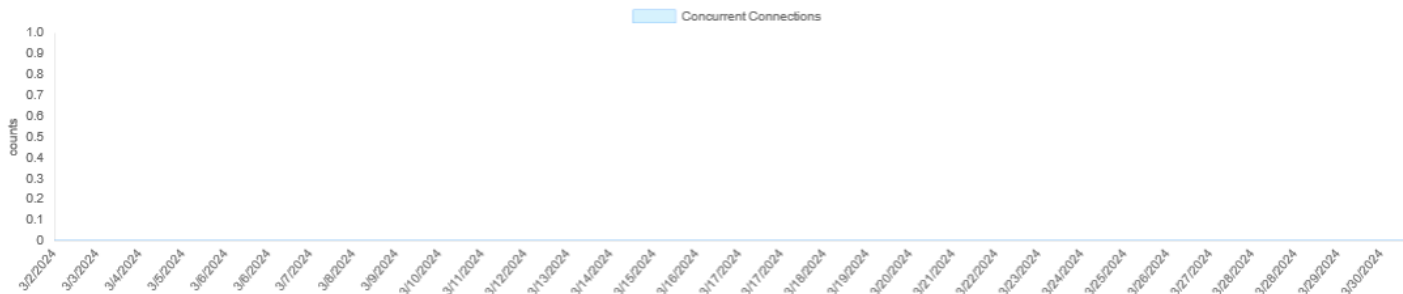
A continuación, se observan los diferentes servicios balanceados.

### 9.1 Justicia XXI

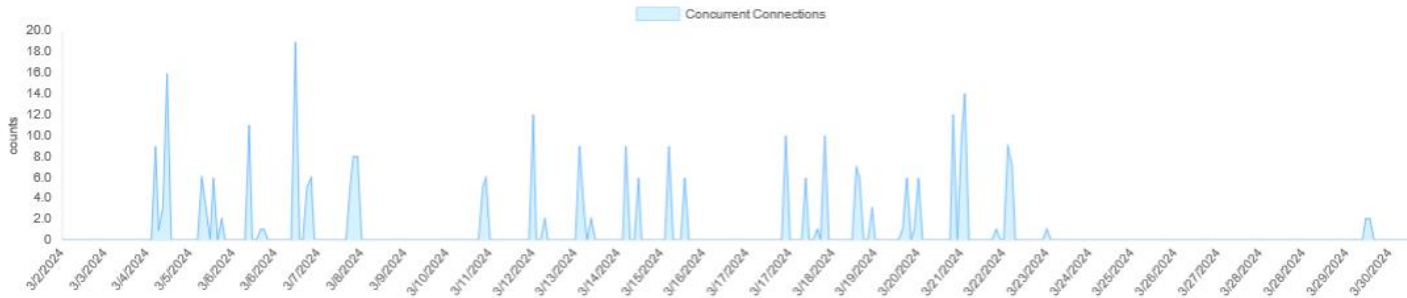
Se encuentra balanceado en el FortiADC:



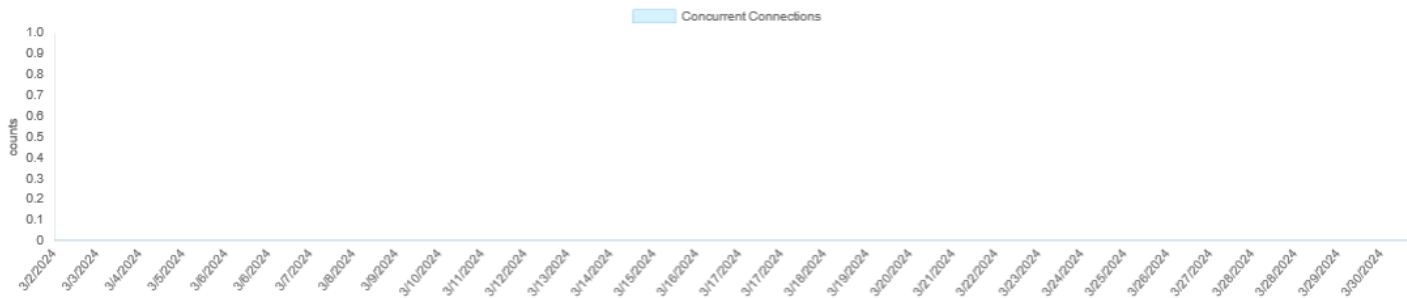
Durante marzo no se presentó tráfico por el puerto 8080:



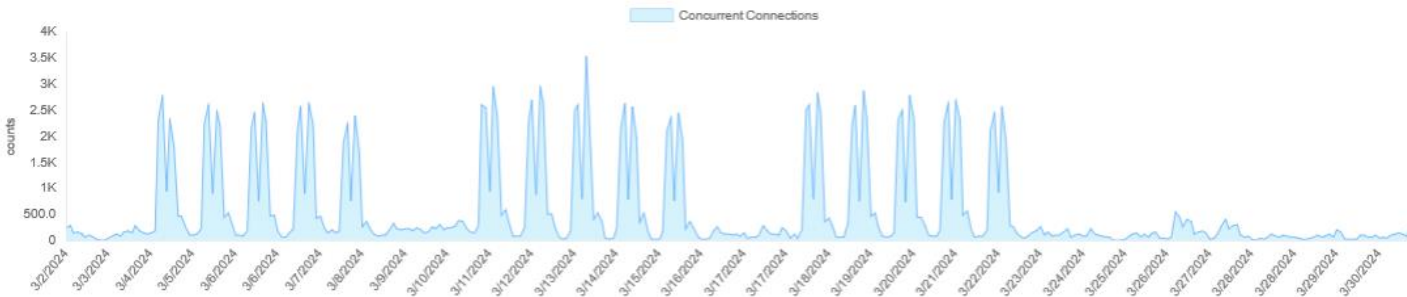
Conexiones concurrentes Virtual Server Justicia XXI con el puerto 8443:



Durante marzo no se presentó tráfico por el puerto 80:



Conexiones concurrentes Virtual Server Justicia XXI por el puerto 443:



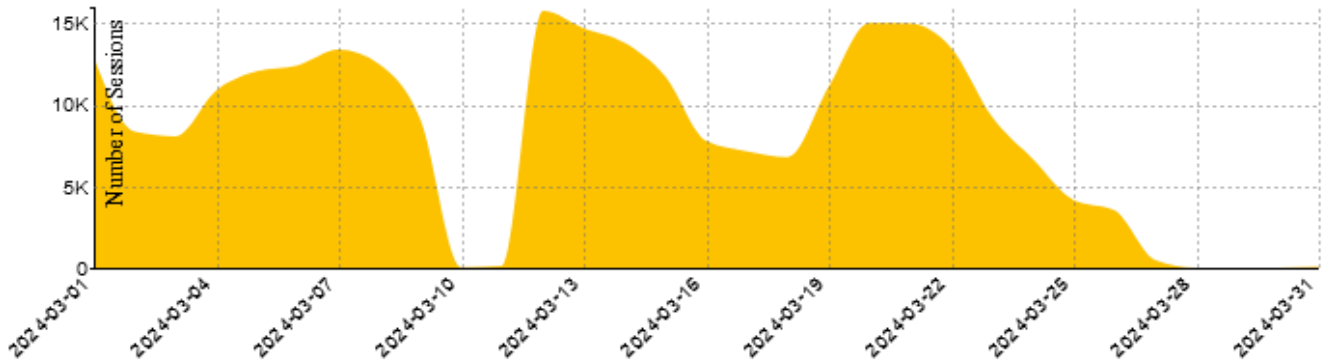
## 9.2 Kactus RDP

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

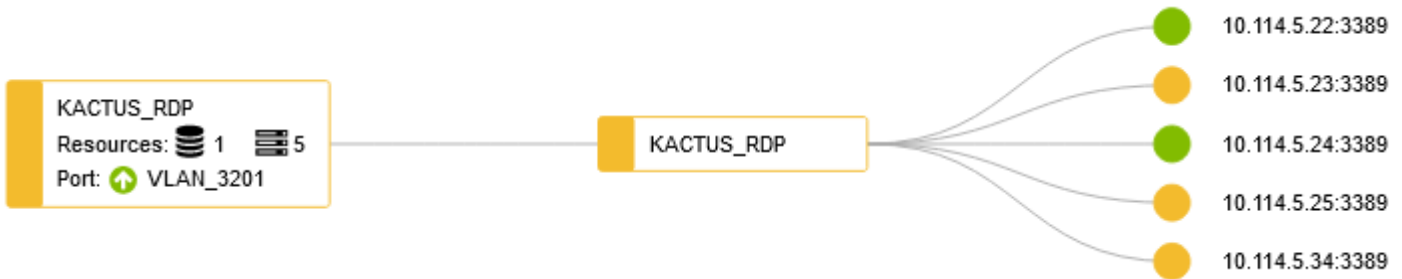
Name	Type	Virtual Server IP	Load Balancing Method	Real Servers	Interface
IPv4 Virtual Server 1/4					
KACTUS_RDP	TCP	10.114.5.38:3389	Static	10.114.5.24 10.114.5.22	Vlan_2000

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

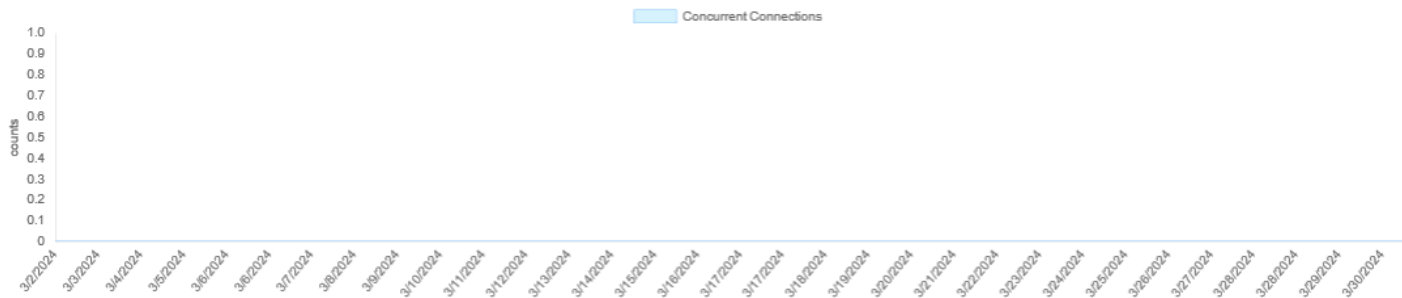
### Session Summary



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

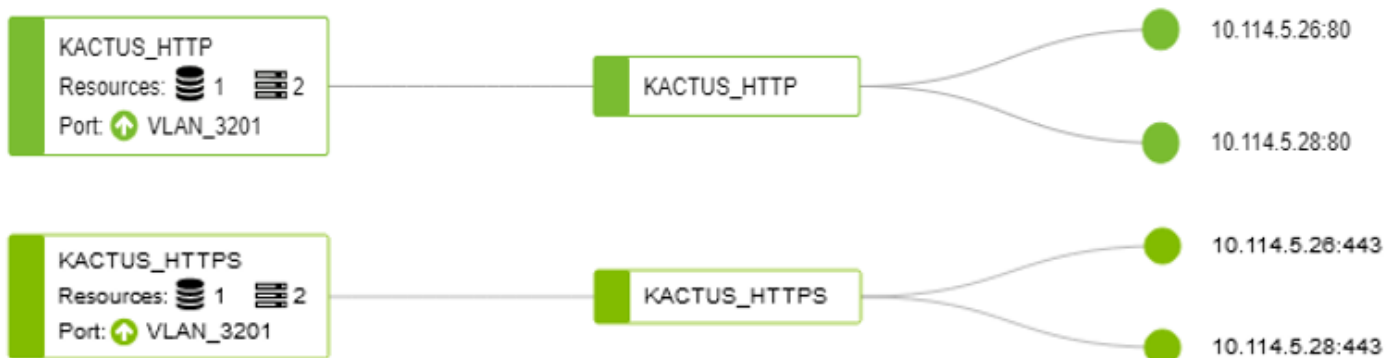


En el FortiADC no se observan sesiones concurrentes:



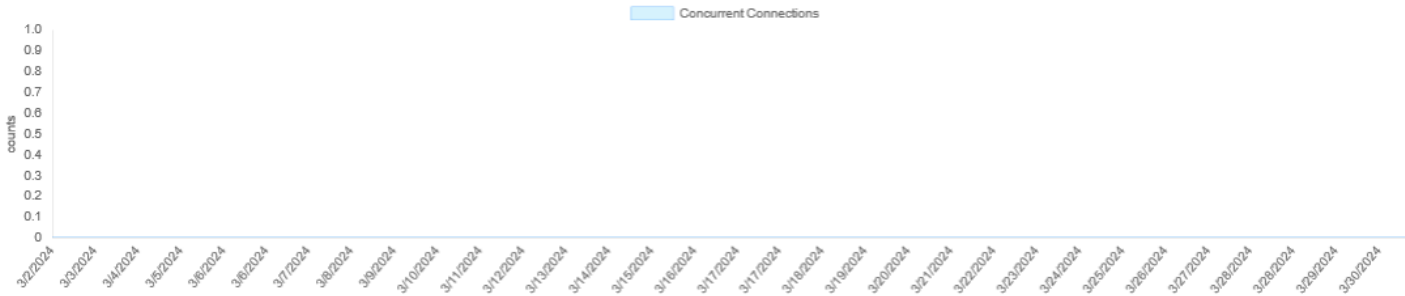
### 9.3 Kactus WEB

Se encuentra balanceado en el FortiADC:

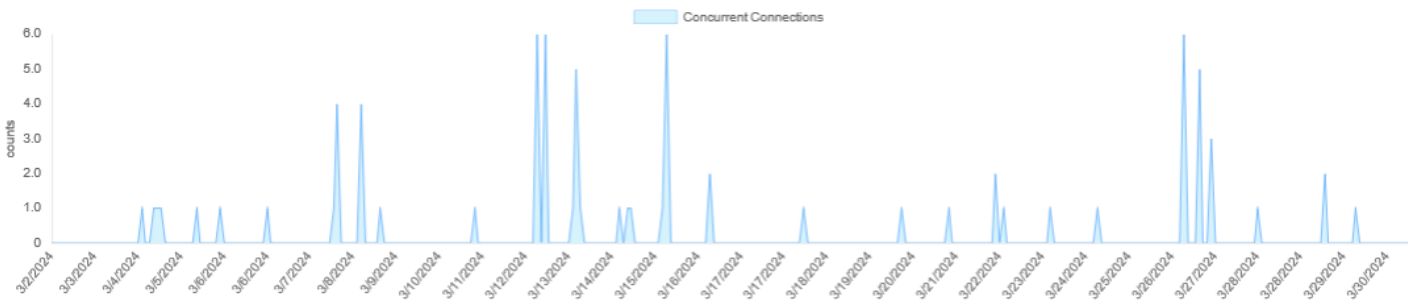




En el FortiADC no se observan sesiones concurrentes por el puerto 80.



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



### 9.4 SIRNA

Este servicio se encuentra balanceado en el Fortigate perimetral:

Configuración de balanceo de CRM en el Firewall.

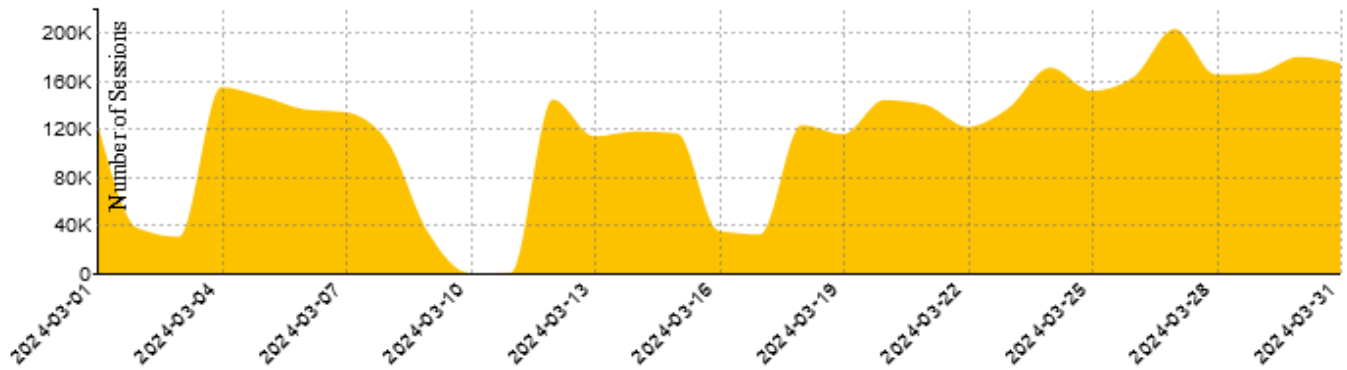
Name	Type	Virtual Server IP	Load Balancing Method	Health Check	Real Servers
<b>IPv4 Virtual Server 4</b>					
CRM_HTTP_HTTPS_444	IP	10.244.2.236:0-65535	Round Robin	Health_CRM_HTTP_HTTPS_444	10.244.2.226 10.244.2.227

Configuración de balanceo de Sharepoint en el firewall perimetral.

Name	Type	Virtual Server IP	Load Balancing Method	Health Check	Real Servers
<b>IPv4 Virtual Server 1/4</b>					
SHAREPOINT	IP	10.244.2.237:0-65535	Round Robin	HLTCK_443	10.244.2.229 10.244.2.228

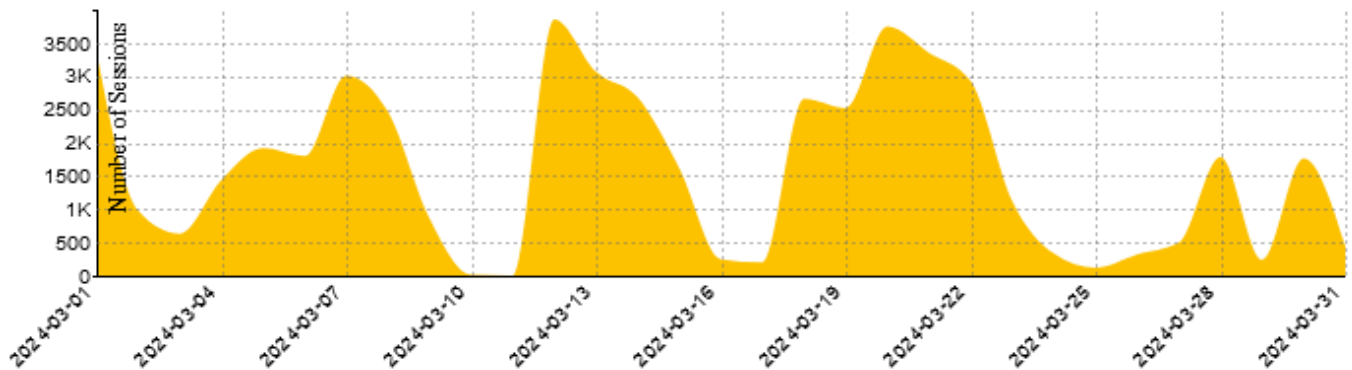
Las sesiones en el firewall para SIRNA 443 fueron:

### Session Summary



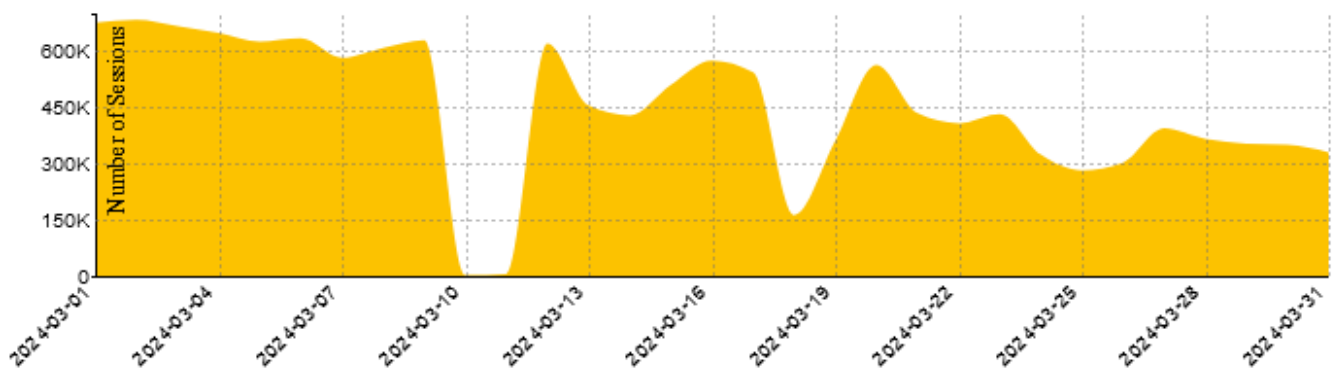
Las sesiones en el firewall para SIRNA 4443 fueron:

### Session Summary



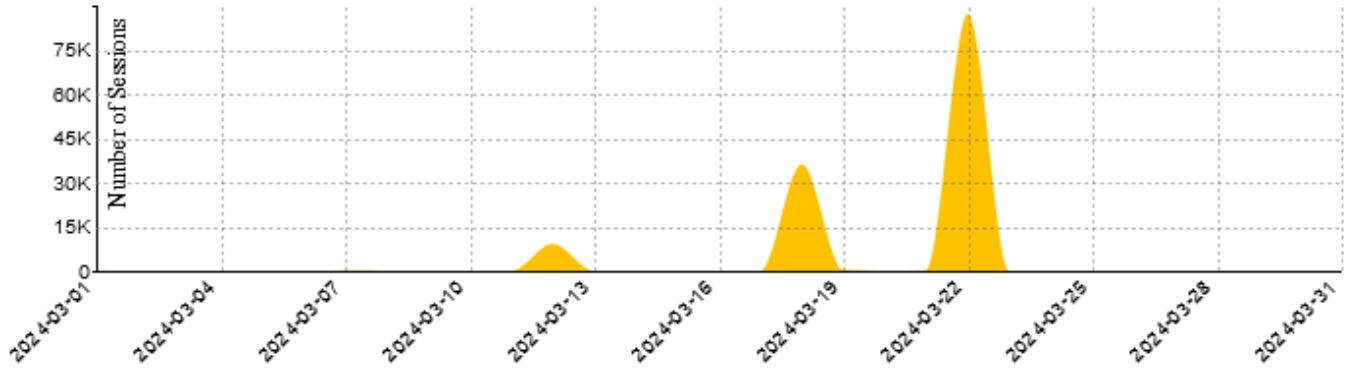
Las sesiones en el firewall para CRM 443 fueron:

### Session Summary



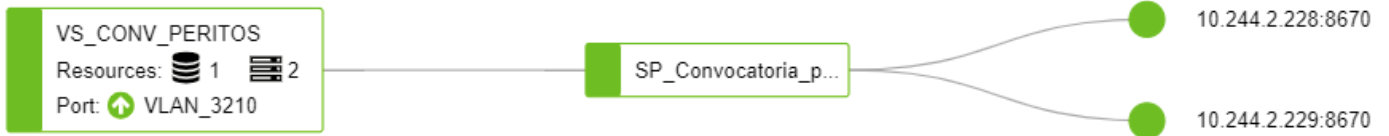
Las sesiones en el firewall para Sharepoint 444 fueron:

### Session Summary

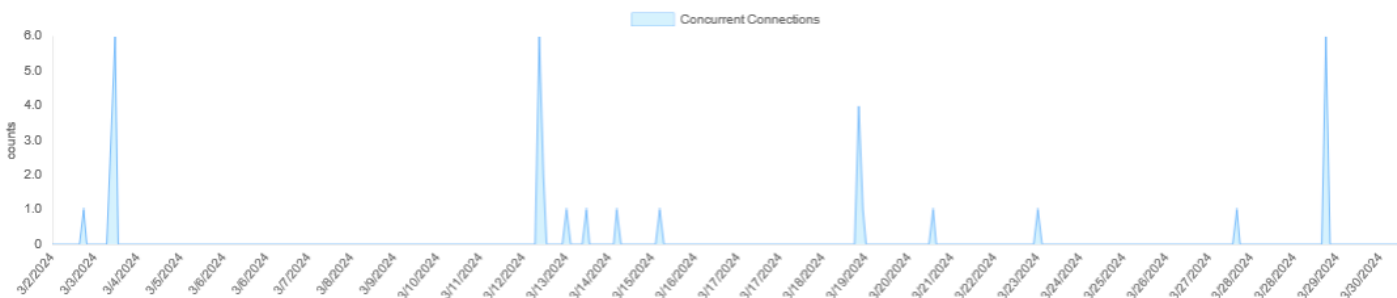


### 9.5 Convocatoria Peritos.

Este servicio se encuentra balanceado en el FortiADC:

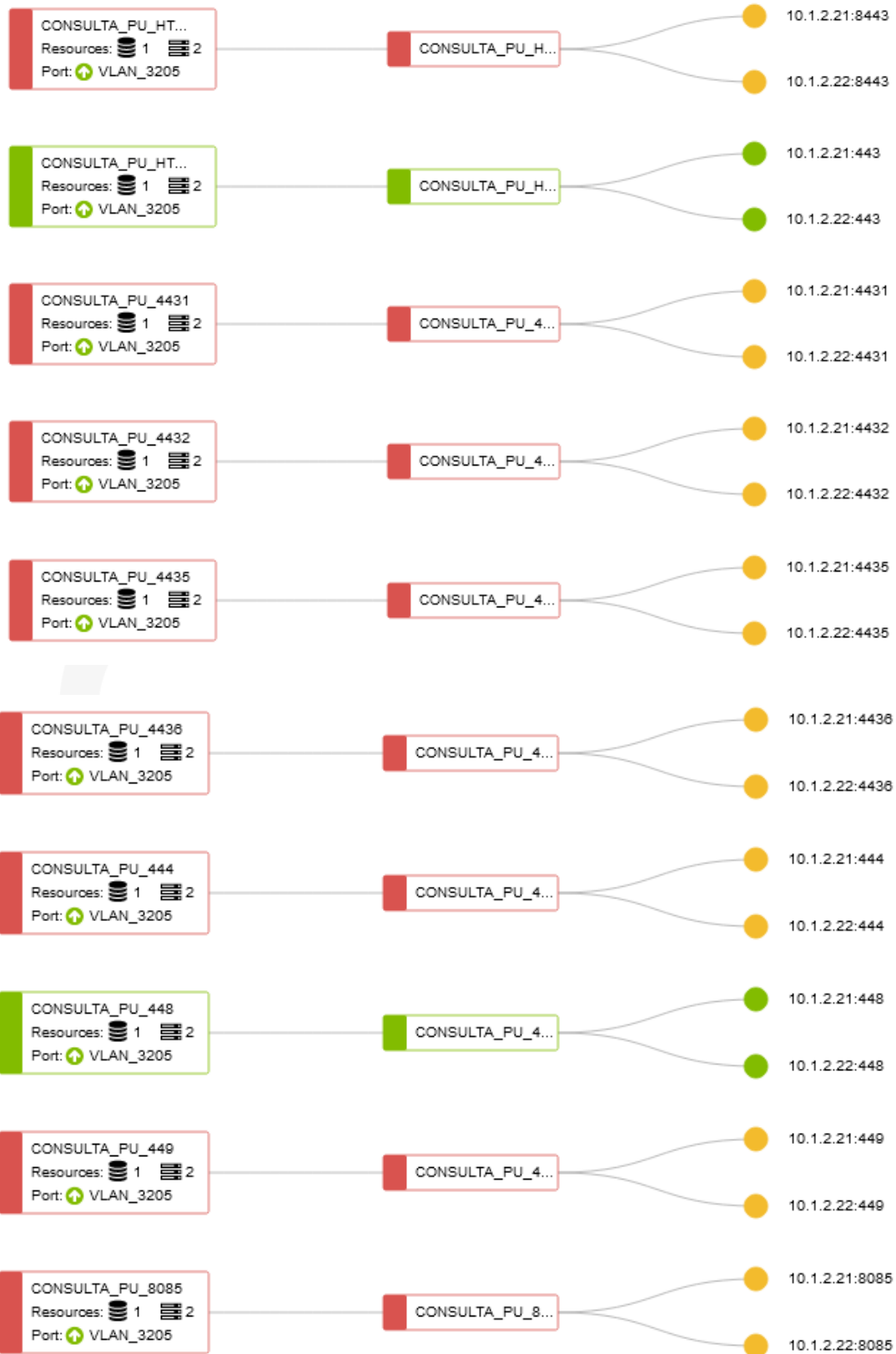


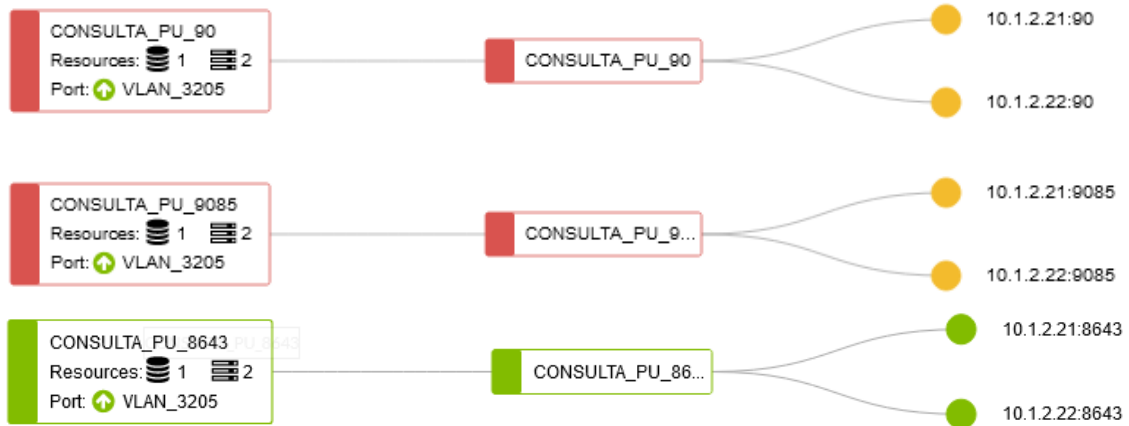
Las sesiones concurrentes fueron las siguientes:



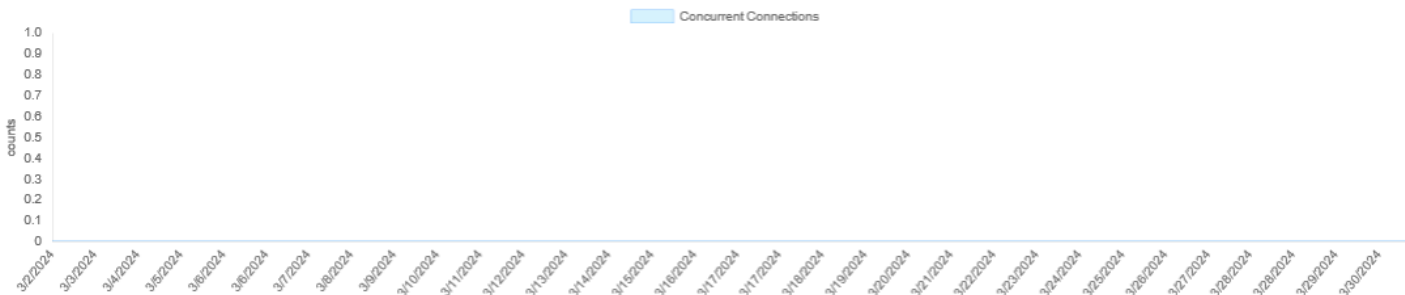
### 9.6 Consulta De Procesos Nacional Unificada (CPNU)

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

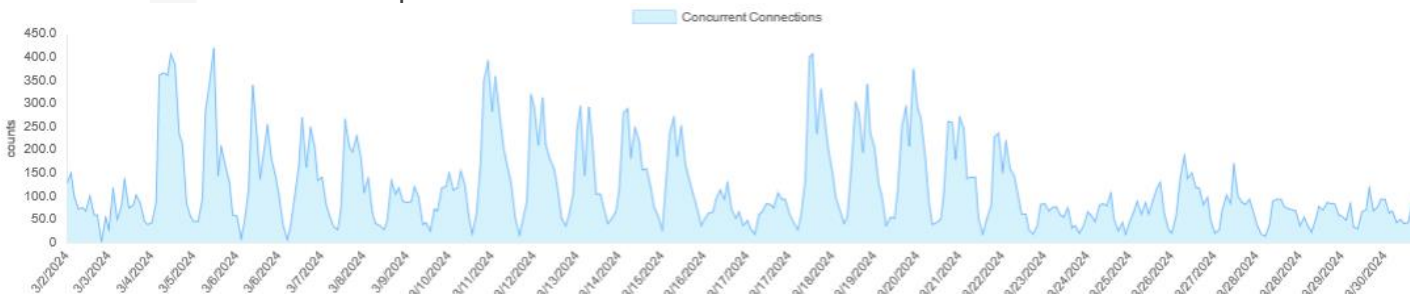




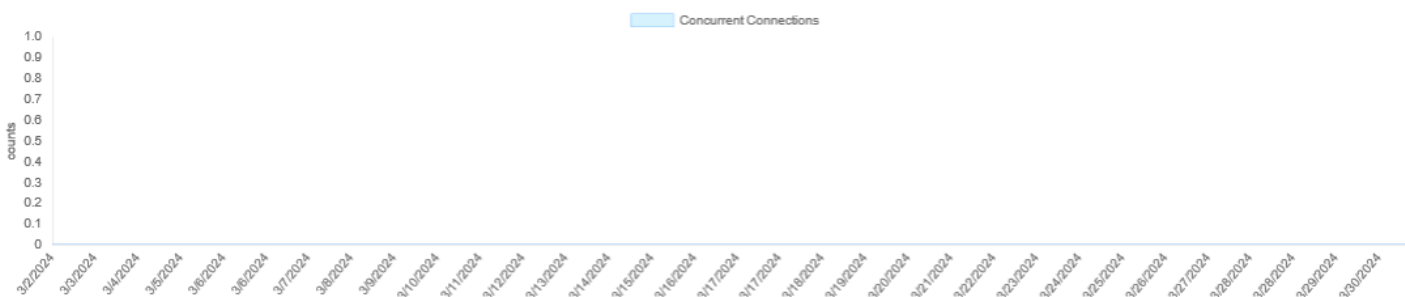
Durante marzo no se tuvieron sesiones concurrentes por el puerto HTTP:



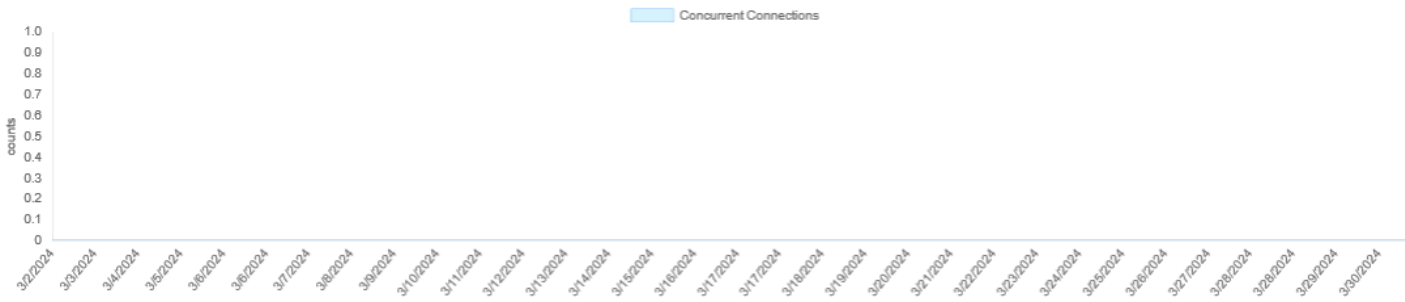
Las sesiones concurrentes por HTTPS fueron:



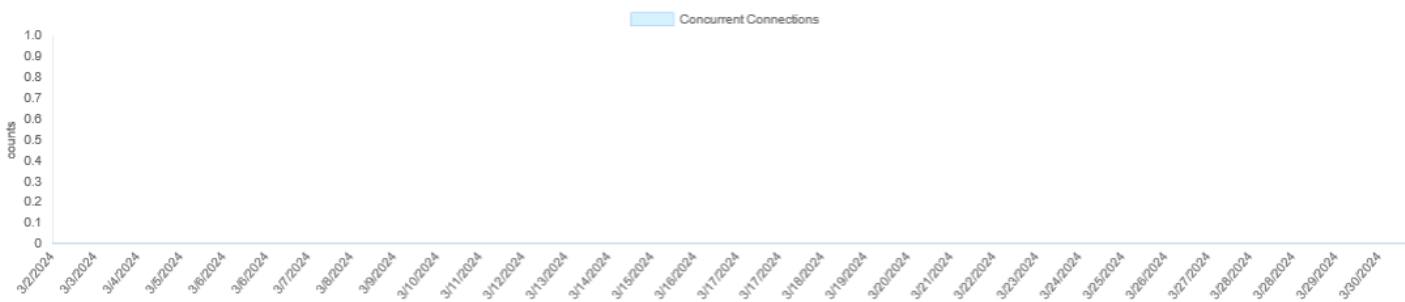
No se tuvieron sesiones concurrentes por el puerto 4431:



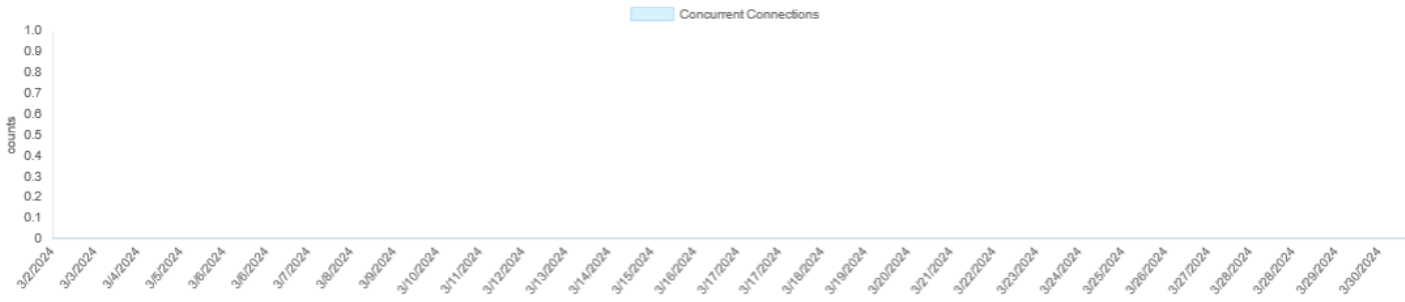
No se tuvieron sesiones concurrentes por el puerto 4432:



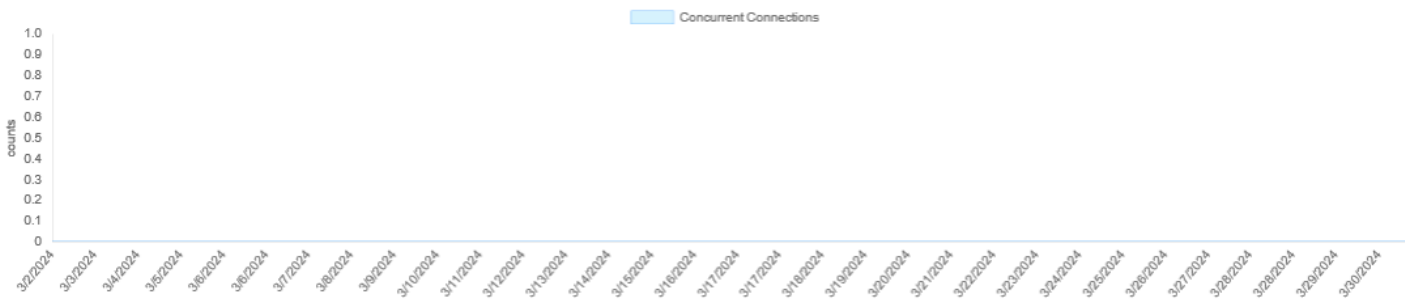
No se tuvieron sesiones concurrentes por el puerto 4435:



Las sesiones concurrentes por puerto 4436 fueron:



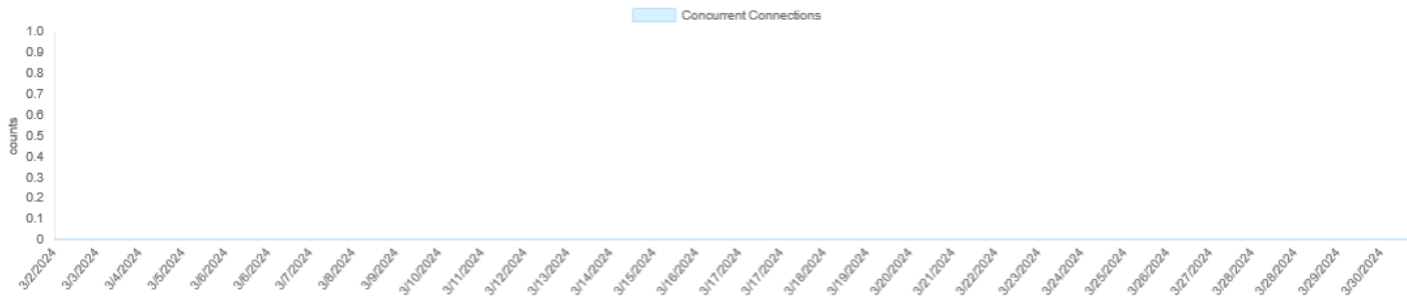
No se tuvieron sesiones concurrentes por el puerto 444:



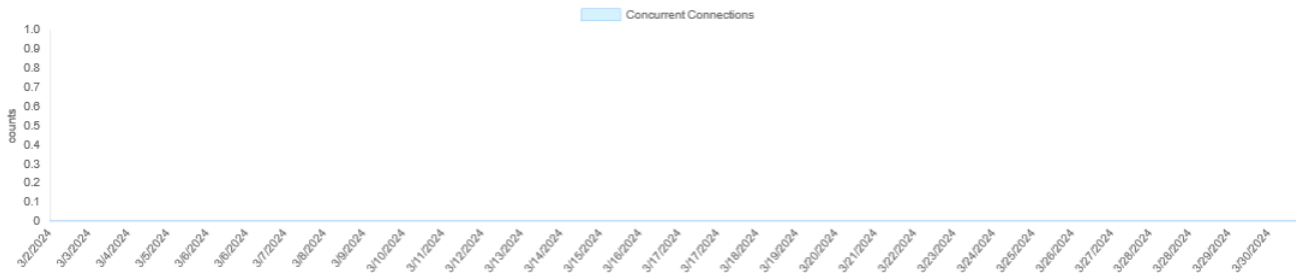
Las sesiones concurrentes por 448 fueron:



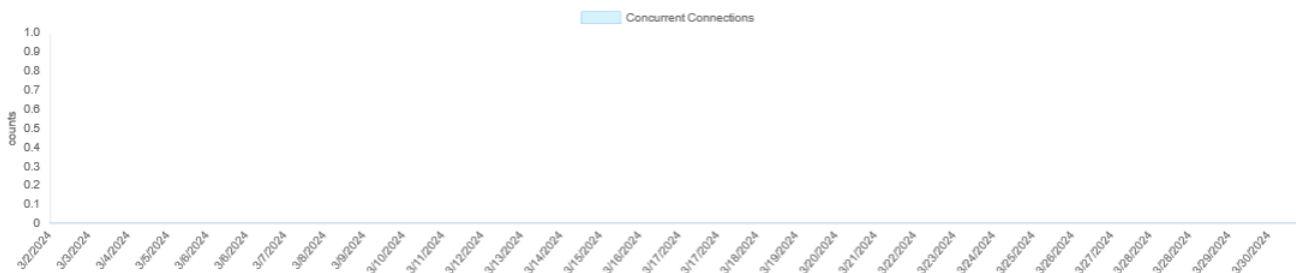
No se tuvieron sesiones concurrentes por el puerto 449:



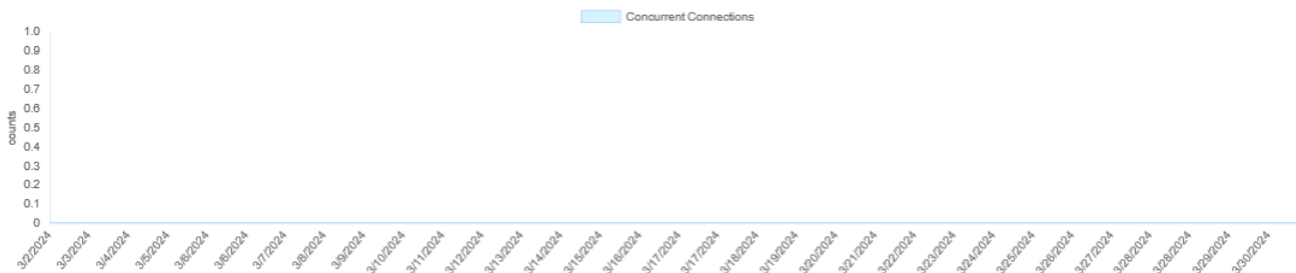
No se tuvieron sesiones concurrentes por el puerto 8085:



No se tuvieron sesiones concurrentes por el puerto 90:

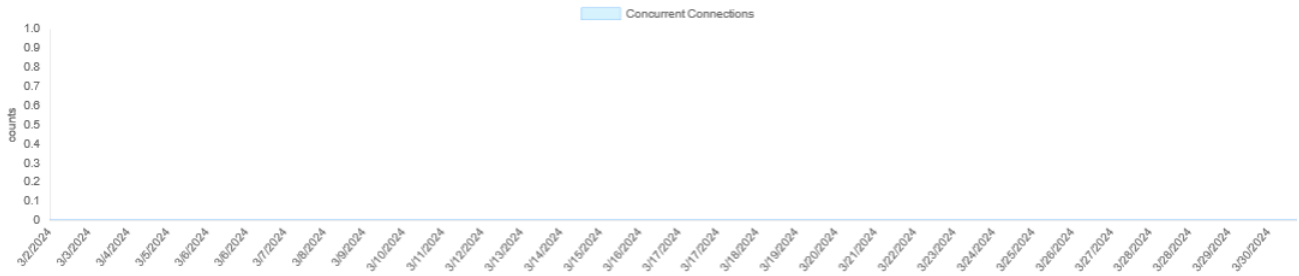


No se tuvieron sesiones concurrentes por el puerto 9085:



No se tuvieron sesiones concurrentes por el puerto 8643:



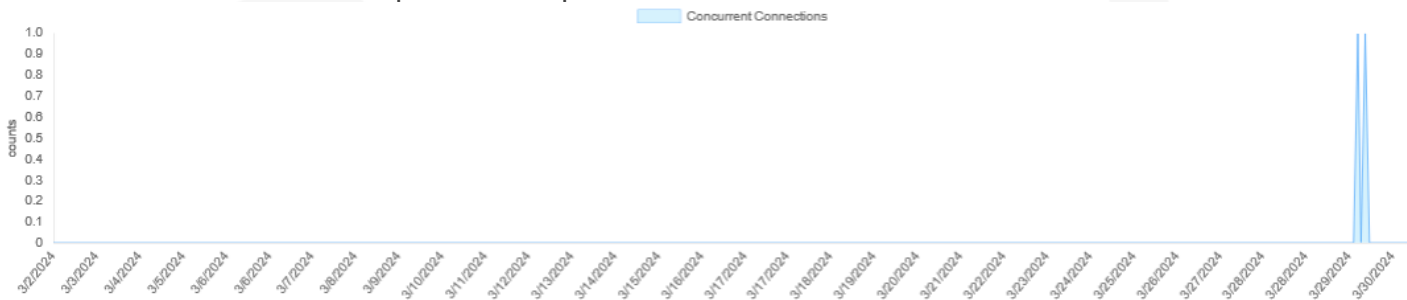


### 9.7 SIERJU

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

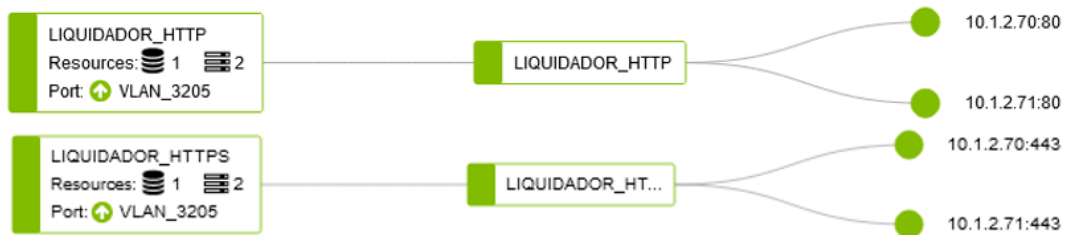


Las sesiones concurrentes para este aplicativo fueron:

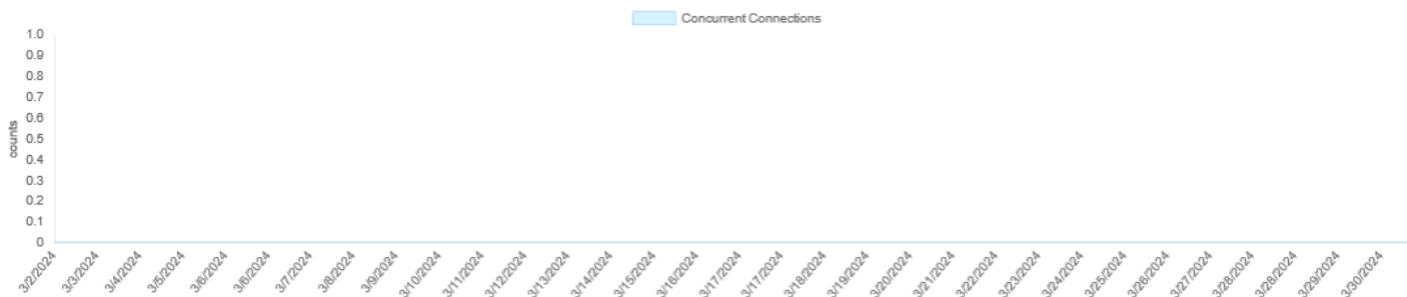


### 9.8 Liquidador de Sentencias

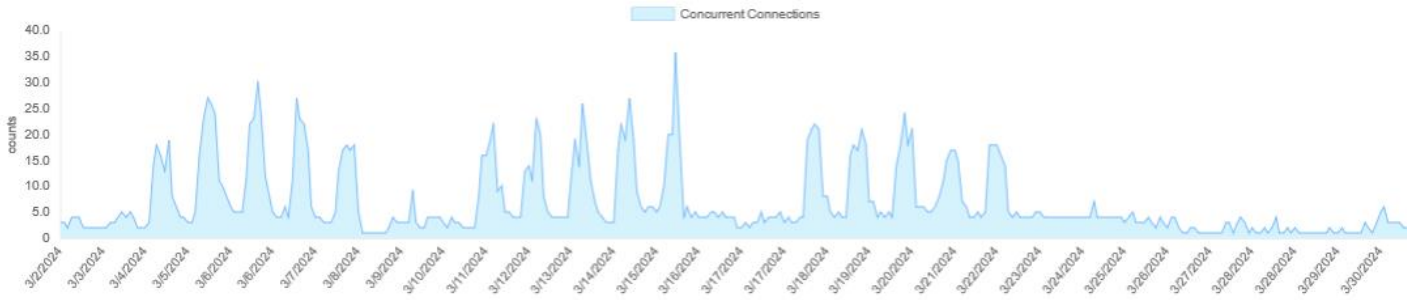
Virtual server Liquidador de Sentencias balanceador FortiADC



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:

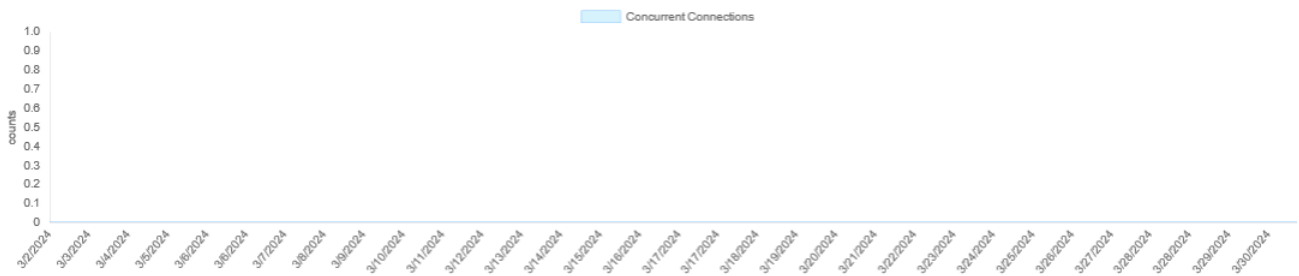


### 9.10 API Gestión de Audiencias

Virtual server API Gestión de Audiencias balanceador FortiADC.

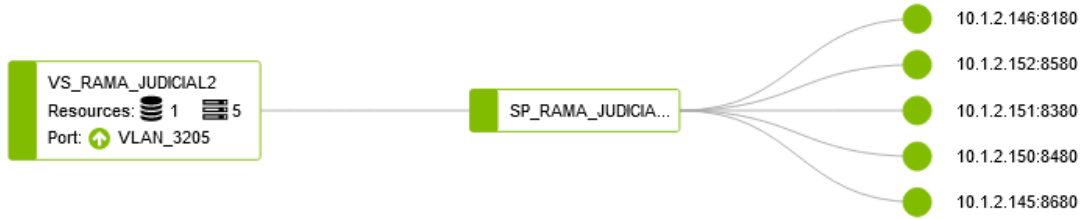


Las sesiones concurrentes para este aplicativo fueron:

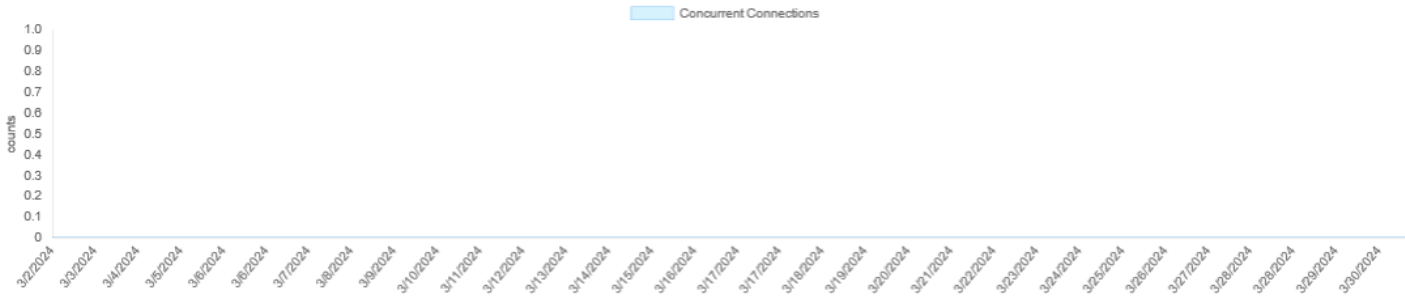


### 9.11 Portal Alterno de la Rama Judicial

Se encuentran balanceado en el FortiADC:



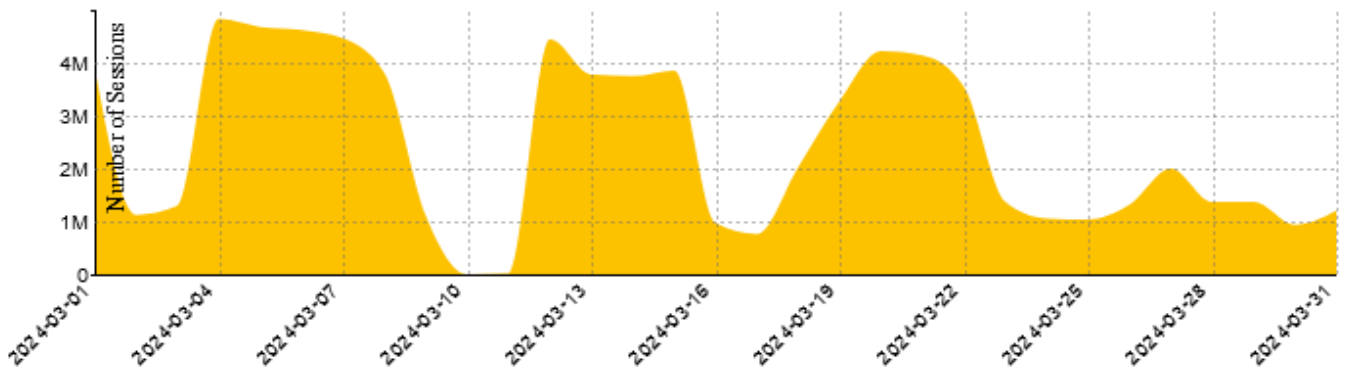
No se observan sesiones concurrentes para este portal alternativo:



### 9.12 Portal de la Rama Judicial

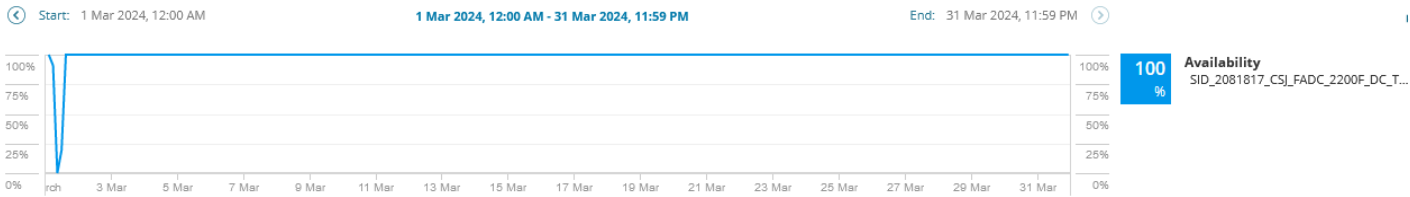
Las sesiones para este portal fueron:

Session Summary



### 9.13 Disponibilidad y performance.

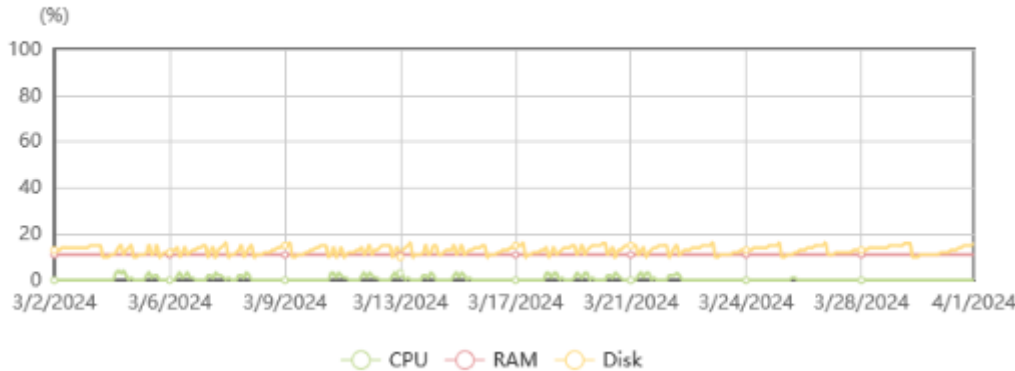
Durante marzo se obtuvo un 100% de disponibilidad en el FortiADC de Torre Central. El evento del 1 de marzo corresponde a una falla en el sistema de Gestión Orión con el caso IFX TT802944 que no ocasionó afectación de los servicios productivos del CSJ:



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

Resources Usage

1 Month ▾



## 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	155
2	WAF CAN	66

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

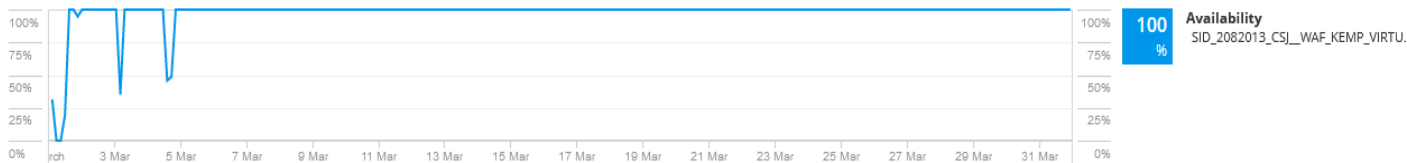
### 10.1 Web application firewall datacenter principal IFX.

Durante marzo se obtuvo una disponibilidad del 100 % en el Kemp de Torre Central. Los eventos del 1 y 3 de marzo corresponden a una incidencia en el sistema de Gestión Orión TT802944 que no afectaron los servicios productivos del CSJ y el 5 de marzo se presentaron fallas de conectividad con la gestión Orión que fue solucionada desactivando la policy route 23 en el fortigate Torre Central:

Start: 1 Mar 2024, 12:00 AM

1 Mar 2024, 12:00 AM - 31 Mar 2024, 11:59 PM

End: 31 Mar 2024, 11:59 PM



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

La aplicación web más consultada durante marzo fue `consultaprosesos.ramajudicial.gov.co-448`:

#	Name	Virtual IP Address	Total Conns	% del Total
1	<code>consultaprosesos.ramajudicial.gov.co - 448</code>	172.17.201.68:448	67900164	41,05%
2	<code>procesos.ramajudicial.gov.co_procesoscs CONSULTA AZUL</code>	172.17.201.26:8443	29157392	17,63%
3	<code>www.ramajudicial.gov.co</code>	172.17.201.25:443	23658756	14,30%
4	<code>procesojudicial.ramajudicial.gov.co TYBA PRUEBAS</code>	172.17.201.249:443	18855480	11,40%
5	<code>consultaprosesos.ramajudicial.gov.co - 443</code>	172.17.201.68:443	7632428	4,61%
6	<code>www.corteconstitucional.gov.co</code>	172.17.201.13:443	6592395	3,99%
7	<code>consejodeestado.gov.co</code>	172.17.201.52:443	2154640	1,30%
8	<code>consultajurisprudencial.ramajudicial.gov.co 8080</code>	172.17.201.110:8080	1244460	0,75%
9	<code>sirna.ramajudicial.gov.co</code>	172.17.201.28:443	952698	0,58%
10	<code>antecedentesdisciplinarios.ramajudicial.gov.co</code>	172.17.201.31:443	810174	0,49%
	Otros		6458413	3,90%
16	System Total Conns		165417000	100,00%

## 10.3 Top de peticiones por país WAF principal IFX.

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

## Top 10 Countries

## Total

Country	Requests	Blocked
United States	45577458	221415
Colombia	61624335	67069
IPrep	36594	36594
Private	6553318	3740
Germany	915170	1027
Australia	33932	1018
China	35667	792
Argentina	13856521	674
Netherlands	2674430	636
Brazil	799680	553

## 10.4 Top de ataques por política WAF principal IFX.

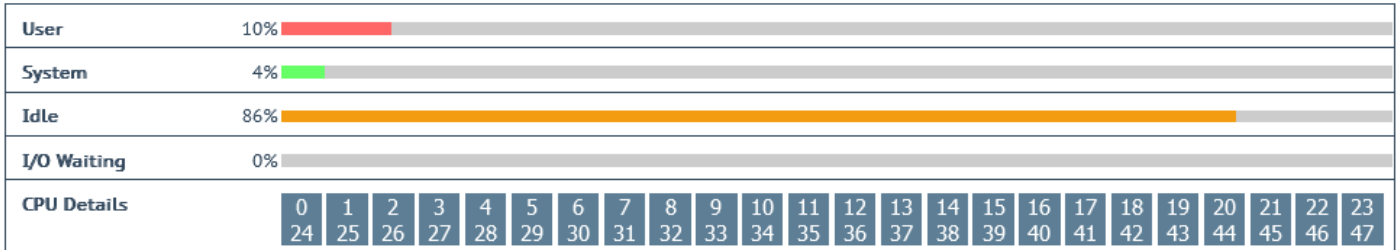
Sobre las aplicaciones procesos.ramajudicial.gov.co\_procesoscs CONSULTA AZUL y consultaprocesos.ramajudicial.gov.co – 448 han sido prevenidas la mayor cantidad de ataques:

#	Name	Virtual IP Address	Total Events	% del Total
1	procesos.ramajudicial.gov.co_procesoscs CONSULTA AZUL	172.17.201.26:8443	100756242	19,81%
2	consultaprocesos.ramajudicial.gov.co - 448	172.17.201.68:448	87081540	17,12%
3	www.corteconstitucional.gov.co	172.17.201.13:443	15669297	3,08%
4	jurisprudencia.ramajudicial.gov.co - ayudajurisprudencia.ramajudicial.gov.co _ 8446	172.17.201.29:8446	80822	0,02%
5	Nuevo portal Rama[1]	172.17.201.101:443	1257536	0,25%
6	consejodeestado.gov.co	172.17.201.52:443	3036260	0,60%
7	jurisprudencia.ramajudicial.gov.co - ayudajurisprudencia.ramajudicial.gov.co	172.17.201.29:443	769173	0,15%
8	SP_ACC_PORTAL_ADMINS	172.17.201.78:443	2331720	0,46%
9	Holocausto_lector_videoteca_sidn_443	172.17.201.54:443	1109488	0,22%
10	portaljudicial_IntranetRama_prueba	172.17.201.88:443	34240	0,01%
	Otros		296569333	58,30%
94	WAF enabled VS Total		508695651	100,00%

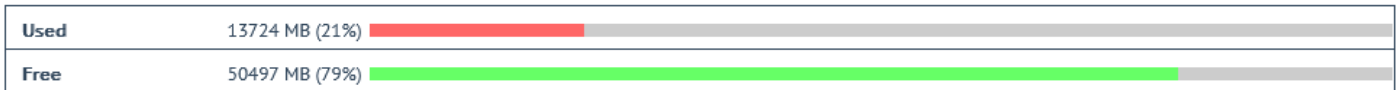
## 10.5 Consumo de recursos WAF principal IFX.

El WAF KEMP de Torre Central presentó consumo de CPU del 10%, memoria de 21% y disco en un 1%.

### Total CPU activity



### Memory Usage (Total 64222 MB)



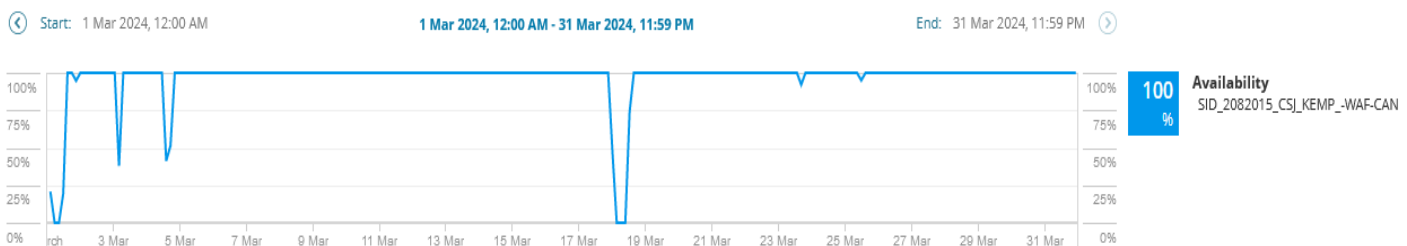
### Disk Usage



## 11. TRÁFICO DE WEB APPLICATION FIREWALL (WAF) CAN

### 11.1 Disponibilidad WAF CAN.

Durante marzo se obtuvo una disponibilidad del 100 % en el WAF de CAN. El evento del 1 de marzo corresponde a una falla en el sistema de Gestión Orión con el caso IFX TT802944 y el 5 de marzo se presentó falla de conectividad con la gestión Orión que fue solucionada desactivando la policy route 23 en el fortigate Torre Central, ninguno de estos eventos ocasionó afectación de los servicios productivos del CSJ. El 18 de marzo se presentó falla de energía en el Datacenter CAN por falla en el sector del proveedor de energía del cliente.





## 11.2 Uso de políticas de servidores WAF CAN.

La aplicación más consultada durante marzo fue cortesuprema.gov.co\_Palacio:

#	Name	Virtual IP Address	Total Conns	% del Total
1	cortesuprema.gov.co_Palacio	172.17.202.239:443	835499	51,31%
2	restituciontierras.ramajudicial.gov.co	172.17.202.37:443	91534	5,62%
3	cortesuprema_Palacio Redirect	172.17.202.239:80	77342	4,75%
4	sso.cortesuprema.gov.co	172.17.202.141:443	67851	4,17%
5	pruebasportal.ability.com.co_Portal pruebas	172.17.202.47:80	40653	2,50%
6	sso.cortesuprema.gov.co	172.17.202.141:80	34866	2,14%
7	samairj.consejodeestado.gov.co	172.17.202.38:443	34741	2,13%
8	siapoas.ramajudicial.gov.co	172.17.202.43:443	30858	1,90%
9	restituciontierras.ramajudicial.gov.co redirect	172.17.202.37:80	28696	1,76%
10	pre_interoperabilidad.ramajudicial.gov.co	172.17.202.51:443	21951	1,35%
	Otros		364236	22,37%
66	System Total Conns		1628227	100,00%

## 11.3 Top de peticiones por país WAF CAN.

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

### Top 10 Countries

#### Total

Country	Requests	Blocked
United States	406619	44510
Private	83735	6748
Russia	9499	148
IPrep	22	22
India	1857	11
United Kingdom	1380	5
Colombia	393284	4
Brazil	4459	4
Romania	272	3
France	30700	2

## 11.4 Top de ataques por política WAF CAN.

Sobre la aplicación cortesuprema.gov.co\_Palacio ha sido prevenida la mayor cantidad de ataques:

#	Name	Virtual IP Address	Total Events	% del Total
1	cortesuprema.gov.co_Palacio	172.17.202.239:443	2979533	78,01%
2	restituciontierras.ramajudicial.gov.co	172.17.202.37:443	222667	5,83%
3	sso.cortesuprema.gov.co	172.17.202.141:443	158060	4,14%
4	siapoas.ramajudicial.gov.co	172.17.202.43:443	100245	2,62%
5	pruebasportal.ability.com.co_Portal pruebas	172.17.202.47:80	47618	1,25%
6	serviciopdf.ramajudicial.gov.co	172.17.202.7:443	31152	0,82%
7	predivprocesos.ramajudicial.gov.co	172.17.202.153:80	26207	0,69%
8	samairj.consejodeestado.gov.co	172.17.202.38:443	25917	0,68%
9	pre_interoperabilidad.ramajudicial.gov.co	172.17.202.51:443	18999	0,50%
10	relatoriacndj.ramajudicial.gov.co	172.17.202.66:443	17010	0,45%
	Otros		192029	5,03%
45	WAF enabled VS Total		3819437	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 7%.

### Total CPU activity

User	0%	<div style="width: 0%;"></div>																																																																													
System	1%	<div style="width: 1%;"></div>																																																																													
Idle	99%	<div style="width: 99%;"></div>																																																																													
I/O Waiting	0%	<div style="width: 0%;"></div>																																																																													
CPU Details	<table border="1"> <tbody> <tr> <td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td> </tr> <tr> <td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td><td>32</td><td>33</td><td>34</td><td>35</td><td>36</td><td>37</td><td>38</td><td>39</td> </tr> <tr> <td>40</td><td>41</td><td>42</td><td>43</td><td>44</td><td>45</td><td>46</td><td>47</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> </tbody> </table>																			0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47												
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19																																																												
20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39																																																												
40	41	42	43	44	45	46	47																																																																								

### Memory Usage (Total 64222 MB)

Used	4779 MB (7%)	<div style="width: 7%;"></div>
Free	59442 MB (93%)	<div style="width: 93%;"></div>

### Memory Usage (Total 64222 MB)

Used	4779 MB (7%)	<div style="width: 7%;"></div>
------	--------------	--------------------------------

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

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

### Nombre del asunto

País	CO
Localidad	Bogota
Organización	Dirección 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

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]

?ramajudicial.gov.co  
[Expires: Apr 24 23:59:59  
2024 GMT]

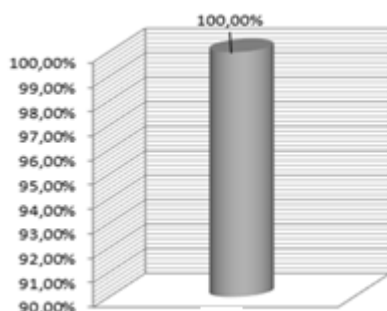
Estos certificados se encuentran instalados en los siguientes dispositivos para cifrar el tráfico hacia las aplicaciones.

N°	Descripción	Hostname	Ubicación	Versión Firmware
1	<b>FortiGate-4400F HA</b>	FTG_CSJ_DC_TC_MASTER	DC IFX	V7.0.14
		FTG_CSJ_DC_TC_SLAVE	DC IFX	v6.4.11
2	<b>FORTIADC</b>	FADC_CSJ_TC_MASTER	DC IFX	v6.1.3
		FADC_CSJ_TC_SLAVE	DC IFX	v6.1.3
3	<b>FortiGate 3500F HA</b>	FGT_CSJ_PALACIO_M	PALACIO	V7.2.6
		FGT_3500F_CSJ_PALACIO_S	PALACIO	V7.2.6
4	<b>KEMP Loadmaster x25 HA</b>	WAF_TORRRE_CENTRAL_MASTER	DC IFX	V7.2.59.0.22007
		WAF_TORRRE_CENTRAL_SLAVE	DC IFX	V7.2.59.0.22007
6	<b>KEMP Loadmaster x25</b>	WAF_CAN	DC CAN	V7.2.59.0.22007

## 12. DISPONIBILIDAD SEGURIDAD GLOBAL DEL MES DE MARZO

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

MES	DISPONIBILIDAD (%)
MARZO	100%



### 12.1 Anexo de las solicitudes e incidentes de seguridad reportadas.

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

### 13. CONSUMO MOTORES BASES DE DATOS

A continuación, se desglosa 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)

### 14. 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 líneas - SID
AMP	Nube Privada IV - CEE-308- AMP-2022- # Proceso CCENEG-061-1-2022
Valor facturado a la fecha	\$ 1.318.151.327,59
% Valor facturado	8,50%
Valor pagado a la fecha	\$ -
% Valor pagado	0%

ANS	
05 al 29 de Febrero 2024	No se generaron ANS durante el periodo
01 al 31 de Marzo 2024	En proceso de conciliación

FACTURA	VALOR	PERIODO FACTURADO	ESTADO
IFXC-402862	\$ 1.318.151.327,59	05 al 29 de Febrero 2024	Pendiente de pago
A la fecha no se ha generado la facturación	\$ -	01 al 31 de Marzo 2024	

## 15. 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 utilizando 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.