REPORTE MENSUAL

RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA

OC124016

OCTUBRE 2024

ifx Networks | CARE Centro de Atención Regional

Contenido

INFORMACIÓN TÉCNICA DEL INFORME

Nombre	Informe de disponibilidad de servidores y recursos de **RAMA JUDICIAL – CONSEJO SUPERIOR DE LA JUDICATURA** alojados en Infraestructura IFX
Descripción	En el presente informe se visualiza la disponibilidad de los servidores y recursos contratados por **RAMA JUDICIAL – CONSEJO SUPERIOR DE LA JUDICATURA,** en el acuerdo marco Nube Privada IV OC 124016.
Finalidad	El informe presentado, se puede utilizar para evaluar la disponibilidad de los servidores y recursos contratados, bajo el acuerdo marco.
Parámetros	**Rango de fechas** Período del informe: mensual Fecha de inicio: 1 de OCTUBRE de 2024 Fecha de final: 31 de OCTUBRE 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**

1. ALOJAMIENTO DE INFRAESTRUCTURA

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

		64GB y128GB - U_Mes - Cantidad: 2						
30	2082020	npn04--IaaS Seguridad - Appliance Anti Ddos - AltaCapacidad - Oro - Hostingfísico - Rol de Inspección - 50Gbps - Paquetes PorSegundo (MPPS) - 45000000- Mes - Cantidad: 2	DDOS DC Torre central	FORTIDDOS FORTINET 2000E/PPLA	2000E	SN: FI2KETB20000015	31-32	32
30	2082021	npn04--IaaS Seguridad - Appliance Anti Ddos - AltaCapacidad - Oro - Hostingfísico - Rol de Inspección - 50Gbps - Paquetes PorSegundo (MPPS) - 45000000- Mes - Cantidad: 2	DDOS DC Torre central	FORTIDDOS FORTINET 2000E/BK	2000E	SN: FI2KE581900004 9	35-36	32
31	2082016	npn04--IaaS Seguridad - Firewall Nueva Generación - Media Capacidad - Oro - Hosting físico - Rol deFirewall - 40 Gbps - SesionesConcurrentes - 15000000 -Mes - Cantidad: 2	FIREWALL	PALACIO - PPLA	FortiGate 900G	SN: FG9H0GTB23900205	N/A	N/A
31	2082017	npn04--IaaS Seguridad - Firewall Nueva Generación - Media Capacidad - Oro - Hosting físico - Rol deFirewall - 40 Gbps - SesionesConcurrentes - 15000000 -Mes - Cantidad: 2	FIREWALL	PALACIO - BK	FortiGate 900G	SN: FG9H0GTB23900440	N/A	N/A
32	2082018	npn04--IaaS Seguridad - Firewall Nueva Generación - Alta Capacidad - Oro - Hosting físico - Rol deFirewall - 500 Gbps - Sesiones Concurrentes - 150000000 - Mes - Cantidad:2	FIREWALL DC Torre central	DATACENTER - BK	FORTIGATE-4400F	SN: FG440FTK21900183	27-30	32

32	2082019	npn04--IaaS Seguridad - Firewall Nueva Generación - Alta Capacidad - Oro - Hosting físico - Rol deFirewall - 500 Gbps - Sesiones Concurrentes - 150000000 - Mes - Cantidad:2	FIREWALL DC Torre central	DATA CENTER - PPLA	FORTIGATE-4400F	SN: FG440FTK21900184	5-8	32
33	2082013	npn04--IaaS Seguridad - WebAplication Firewall - AltaCapacidad - Oro - Hostingfísico - Desempeño WAF(Gbps) - 10 - Mes - Cantidad:3	WAF DC Torre central	DATACENTER - PPLA	KEMP LM-X25	SN: TSCC82005608	14	31
33	2082014	npn04--IaaS Seguridad - WebAplication Firewall - AltaCapacidad - Oro - Hostingfísico - Desempeño WAF(Gbps) - 10 - Mes - Cantidad:3	WAF DC Torre central	DATACENTER - BK	KEMP LM-X25	SN: TSCB72000545	13	31
33	2082015	npn04--IaaS Seguridad - WebAplication Firewall - AltaCapacidad - Oro - Hostingfísico - Desempeño WAF(Gbps) - 10 - Mes - Cantidad:3	WAF	SEDE CAN	KEMP LM-X25	SN: TSCC82005629	N/A	N/A

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

1. ALMACENAMIENTO

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

9	2081813	IaaS almacenamiento - Backup de Datos - Alta - Capacidad: 100TB a <200TB - Almacenamiento SAN - Semanal - GB/Mes - Cantidad: 185000
47	2082100	npn04--IaaS almacenamiento- Almacenamiento SAN AltoRendimiento - Oro - Alta -Nube Privada - Capacidad 100TB a <200TB - FC >= 8Gbps - SSD - RAID: 5 - IOPSREAD 72000 / WRITE 30000- GB/Mes - Cantidad: 100000
48	2082101	npn04--IaaS almacenamiento- Almacenamiento SAN AltoRendimiento - Oro - Alta -Nube Privada - Capacidad 100TB a <200TB - FC >= 8Gbps - SSD - RAID: 5 - IOPSREAD 72000 / WRITE 30000- GB/Mes - Cantidad: 100000
49	2082102	npn04--IaaS almacenamiento- Almacenamiento SAN AltoRendimiento - Oro - Alta -Nube Privada - Capacidad:100TB a <200TB - FC >= 8Gbps - SSD - RAID: 5 - IOPSREAD 72000 / WRITE 30000- GB/Mes - Cantidad: 150000

El almacenamiento total aprovisionado en la infraestructura contratada, de conformidad con las solicitudes de la Entidad, a corte 31 de octubre de 2024 es de: **3732580(GB)**

El almacenamiento total presentado adicional es de: **3607703 (GB)**

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

A corte 31 de octubre 2024 la entidad cuenta con un almacenamiento disponible de 22297 (GB)

(Remitirse al anexo "**Inventario_Servicios_CSJ_OCTUBRE_2024.xls**" para ver el detalle)

2. BACKUPS

No	ARTICULO	SIDOC124016
7	npn04--IaaS almacenamiento- Backup de Datos - Alta - Capacidad: 200TB a <300TB- Disco Duro Externo -Mensual - GB/Mes -Cantidad: 250000	2081814
8	npn04--IaaS almacenamiento- Backup de Datos - Alta - Capacidad: 100TB a <200TB- Almacenamiento SAN -Diaria - GB/Mes - Cantidad:165000	2081812
9	npn04--IaaS almacenamiento- Backup de Datos - Alta - Capacidad: 100TB a <200TB- Almacenamiento SAN - Semanal - GB/Mes -Cantidad: 185000	2081813

El almacenamiento backup total usado en la infraestructura contratada, según el cuadro de la página 20 del documento "veeam backup CSJ_PDF", donde se resta la sumatoria de la columna 1 "CAPACIDAD", menos la sumatoria de la columna 2, "ESPACIO,ESPACIO LIBRE", de conformidad con las solicitudes de la Entidad, a corte 31 de octubre, está utilizando, una capacidad de **1.306.600 GB** en almacenamiento físico total, pero la entidad actualmente tiene contratado, el siguiente almacenamiento en sus órdenes de compra y se desglosa de la siguiente manera:

• Total, contratado de Almacenamiento BK de datos diario y semanal
350000 GB

• A la fecha la entidad, está consumiendo 281900 GB de almacenamiento de BK diario y semanal, los cuales se sacan de la sumatoria de la columna "CAPACIDAD" menos "ESPACIO", de la tabla "DIARIO-SEMANAL OC 124016".

• **Acorde a la información suministrada con anterioridad y realizando la resta entre lo consumido, menos el almacenamiento contratado la entidad no supera, el almacenamiento BK de datos diario y semanal.**

• Para los Backus Mensuales la entidad tiene contratado un espacio de Almacenamiento físico en NAS mensual de: **250000 GB**

• A la fecha la entidad, está consumiendo 188.200 GB de almacenamiento de BK Mensual, los cuales se sacan de la sumatoria de la columna "CAPACIDAD" menos "ESPACIO LIBRE", de la tabla "MENSUAL BACKUP SAN OC 124016"

• Acorde a la información suministrada con anterioridad y realizando la resta entre lo consumido, menos el almacenamiento contratado, la entidad no supera el almacenamiento BK MENSUAL.

• Para los Backus Mensuales la entidad tiene contratado un espacio de **Almacenamiento físico en SAN** con retención de 6 meses que se utilizan de los ítems de producción: 370.000 GB

• A la fecha la entidad, está consumiendo 353300 GB de almacenamiento de BK Mensual en SAN, los cuales se sacan de la sumatoria de la columna "CAPACIDAD" menos "ESPACIO LIBRE", de la tabla "MENSUALES JULIO - NOVIEMBRE 2024 - OC 100980"

• Acorde a la información suministrada con anterioridad y realizando la resta entre lo consumido, menos el almacenamiento contratado la entidad no supera el almacenamiento BK MENSUAL.

• Para los Backus Mensuales anteriores a Julio de 2024 la entidad tiene ocupado un espacio de Almacenamiento físico en SAN con retención de 12 meses: 483.200 GB

• A la fecha la entidad está copiando esta información a AWS tiene como fecha de entrega el 10 de noviembre de 2024, los cuales se sacan de la sumatoria de la columna "CAPACIDAD" menos "ESPACIO LIBRE", de la tabla "MENSUALES ANTES DE JULIO - COPIA HACIA AWS -PTE AUTORIZACIÓN DE DEPURACIÓN OC 100980"

• Acorde a la información suministrada con anterioridad y realizando la resta entre lo consumido, menos el almacenamiento contratado la entidad supera el almacenamiento de BK en 483.200 GB.

Los backups se ejecutan de la siguiente manera:

Diarios: De domingo a viernes 20:00pm Semanales: Todos los sábados 20:00pm

Mensuales: Último domingo de cada mes 22:00pm

NOTA: Por motivos de seguridad, no es viable remitir fotografías de los backups ejecutados

DIARIOS-SEMANALES OC 124016			
REPOSITORIO	**CAPACIDAD (TB)**	**ESPACIO LIBRE (TB)**	**ESPACIO USADO (TB)**
UNIDAD 1	80	10,3	206,4
UNIDAD 2	80	12,2	206,8
UNIDAD 3	78,2	23,8	160,4
UNIDAD 4	110	20	207
SUMATORIAS	348,2	66,3	780,6
ESPACIO CONSUMIDO DIARIO - SEMANAL			281,90
DIFERENCIA DE LO CONTRATADO			68,10

MENSUALES ANTES DE JULIO - COPIA HACIA AWS -PTE AUTORIZACIÓN DE			
REPOSITORIO	**CAPACIDAD (TB)**	**ESPACIO LIBRE (TB)**	**ESPACIO USADO (TB)**
UNIDAD 1	90	8,5	9,1
UNIDAD 2	90	6,1	26,9
UNIDAD 3	90	0,0001	13,4
UNIDAD 4	90	6,3	11,7
UNIDAD 5	100	16,4	175,1
UNIDAD 6	100	39,5	94,1
SUMATORIAS	560	76,8001	330,3
ESPACIO CONSUMIDO JULIO COPIA AWS			483,20
DIFERENCIA DE LO CONTRATADO			-483,20

MENSUALES JULIO - NOVIEMBRE 2024 - OC 100980			
REPOSITORIO	**CAPACIDAD (TB)**	**ESPACIO LIBRE (TB)**	**ESPACIO USADO (TB)**
UNIDAD 1	130	11,5	139,5
UNIDAD 2	120	1,2	118,6
UNIDAD 3	130	14	115,1
SUMATORIAS	380	26,7	373,2
ESPACIO CONSUMIDO JULIO			353,30
DIFERENCIA DE LO CONTRATADO			16,70

MENSUAL BACKUP SAN OC 124016			
REPOSITORIO	**CAPACIDAD (TB)**	**ESPACIO LIBRE (TB)**	**ESPACIO USADO (TB)**
NAS	250	61,8	169,8
ESPACIO CONSUMIDO JULIO NAS OC 124016			188,20
DIFERENCIA DE LO CONTRATADO			61,80

ESPACIO CONSUMIDO TOTAL	1306,60
DIFERENCIA TOTAL VS LO CONTRATADO	-336,60

NOTA: Por favor tener en cuenta, que las dos primeras columnas, hacen referencia al espacio físico, tanto usado como libre, la tercera columna, hace referencia al especio que nos muestra la herramienta que consume en el espacio libre disponible (espacio total team sin de duplicación).
Tener en cuenta que el documento veeam backup CSJ.PDF, no se modifica porque son los valores que nos genera la herramienta, al momento de extraer los datos, pero si son la base para realizar los cálculos de los espacios a la fecha de corte.

(Remitirse al anexo "**Inventario_Servicios_CSJ_OCTUBRE_2024.xls**" para ver el detalle)

3. 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 31 de octubre 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_OCTUBRE_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

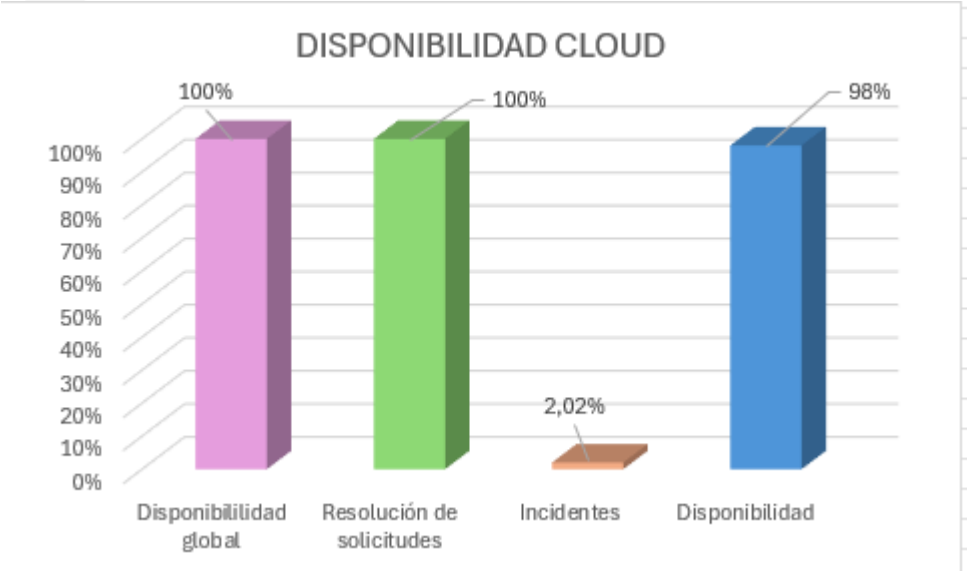
- **core-impact:** Línea de OC 12
- **Efinomina:** Líneas de OC 14,18,26,27,38 y 39
- **Fuse:** Línea OC 17
- **Gestión grabaciones:** Líneas de OC 12,13, 14,15,17,19,20,22,23,25,28,35,36 y 38
- **InsightVM console:** línea OC 27
- **InsightVM scan:** línea OC 27
- **Insightappsec scan:** línea OC 25
- **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_OCTUBRE_2024.xls**" para ver el detalle "maquinas")

7.DISPONIBILIDAD GLOBAL CLOUD DEL MES DE OCTUBRE

Disponibilidad Global mes de OCTUBRE	Numero de tickets mes de OCTUBRE	Imputabilidad por ANS
	132 solicitudes	**0 solicitudes**
	1 incidentes	**0 incidentes**
100%	Total 133 tickets	0 tickets



CONTROL DOCUMENTAL

ELABORADO POR

Fecha	Autor	Ingeniero
03-10-2024	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 octubre a31 de octubre del 2024.

CONSUMO TOTAL HORAS MES DE OCTUBRE	
• Casos Reportados Netsuite	97
Sesiones de Seguimiento	10
Sesiones de Trabajo	0
Casos Escalados Medio Digital - Whatsapp	7
Horas Disponibilidad del Recurso Fines de Semana	286
Total Horas Consumidas de las 300 - Experto Master	400

2.INDICADORES DEL CENTRO CONSOLIDADO DE SERVICIOS

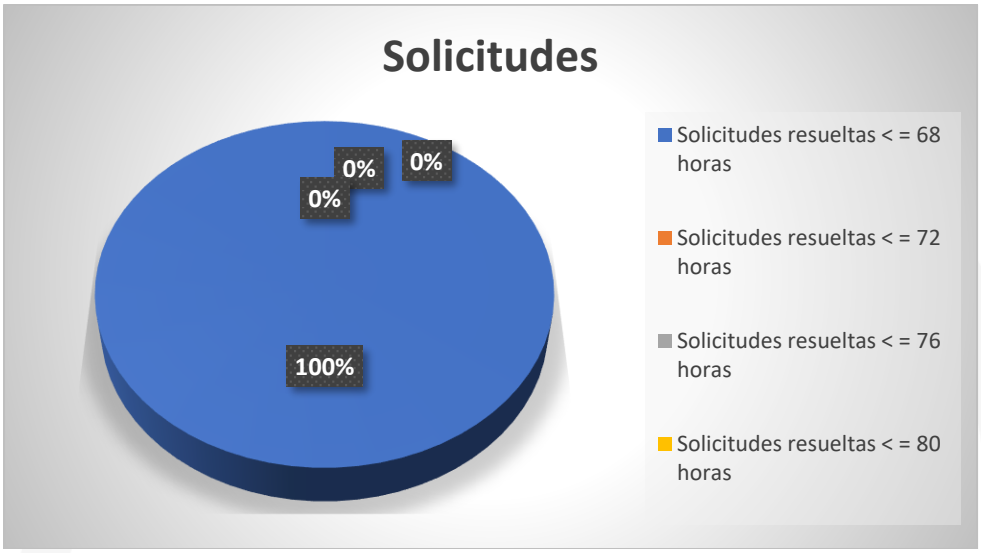
Con base en la información provista por el sistema de Netsuite, se elaboró el presente reporte el cual muestra el comportamiento de los problemas y requerimientos con enfoque en los días 01 enero a 31 de octubre, para el **Consejo Superior de la Judicatura**. Estas mediciones se basan en el número de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

	Volumen en 1 octubre a
Casos Reportados	22
Solicitudes	22
Incidencias	0
WA – AF	0

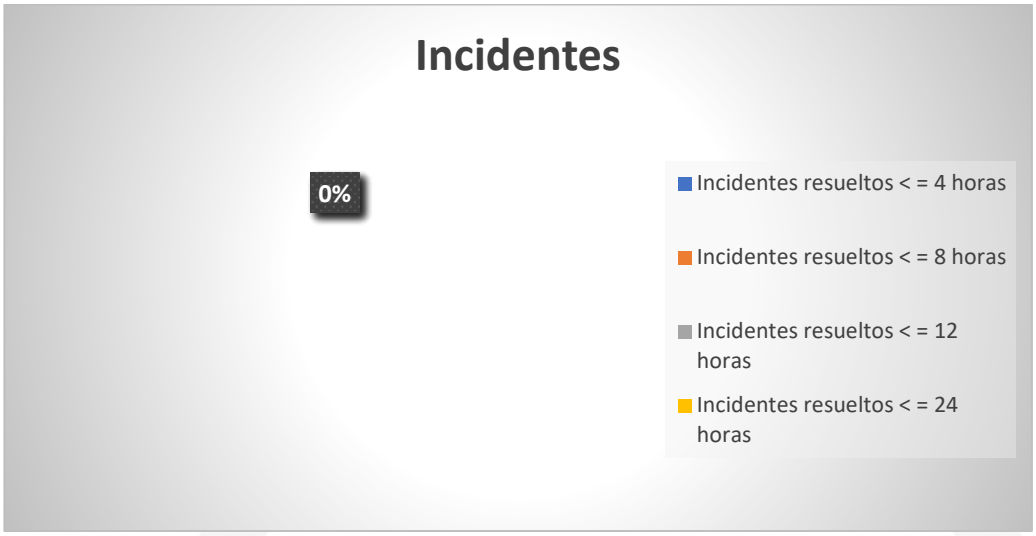
2.1 TASA DE RESOLUCIÓN DE PROBLEMAS

Tiempo de Gestión	Solicitudes
Solicitudes resueltas < = 68 horas	22
Solicitudes resueltas < = 72 horas	0
Solicitudes resueltas < = 76 horas	0
Solicitudes resueltas < = 80 horas	0

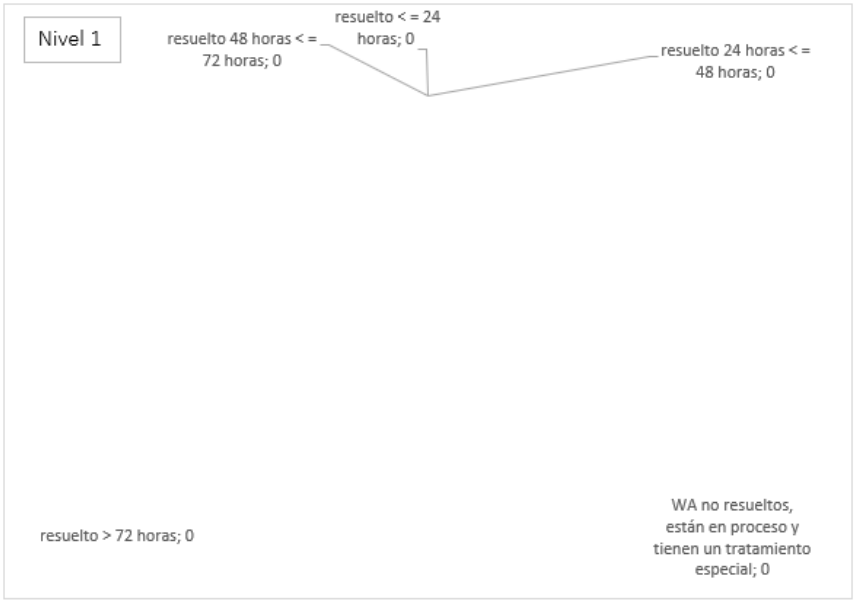
Solicitudes no resueltas > 80 horas, están en proceso y/o tienen un tratamiento especial	0
Total	22

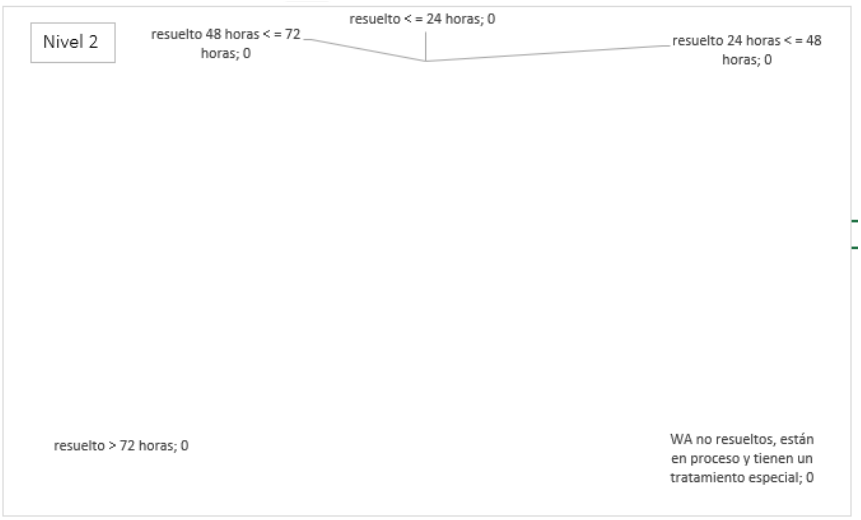


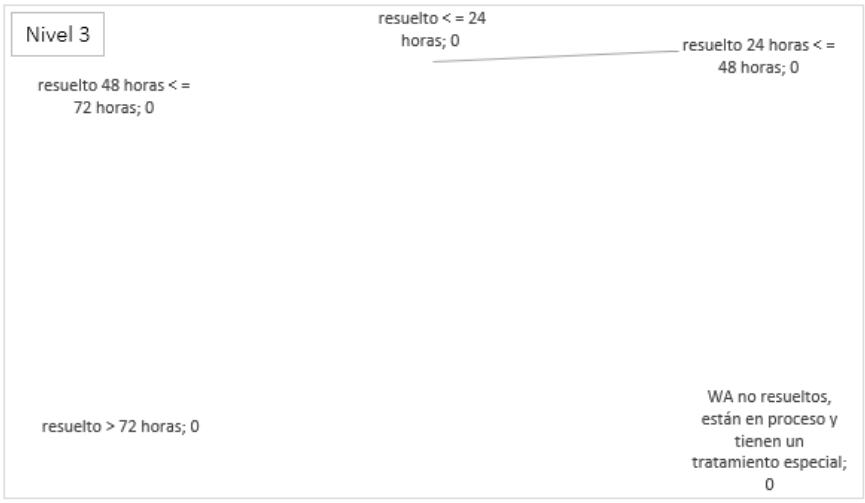
Tiempo de Gestión	Incidentes Penalizados
Incidentes resueltos < = 4 horas	0
Incidentes resueltos < = 8 horas	0
Incidentes resueltos <= 12 horas	0
Incidentes No resueltos < 24 horas	0
Total	0

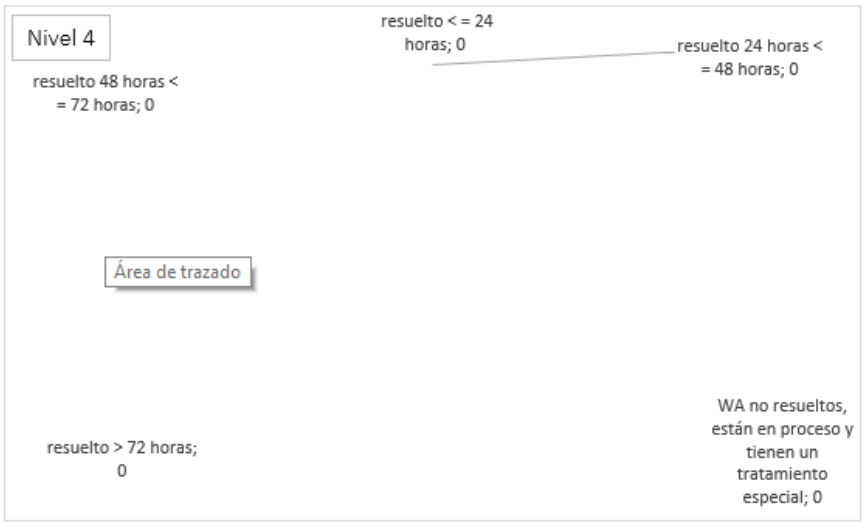


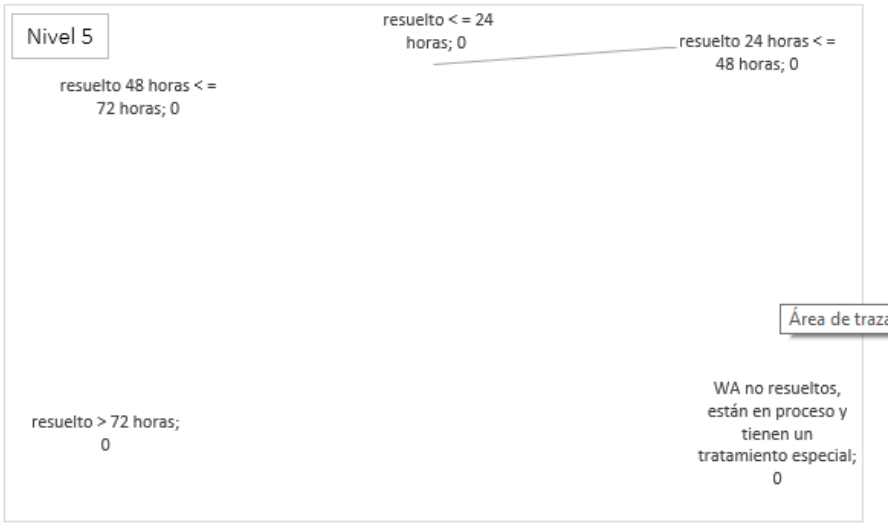
WA (Ajustes Funcionales)					
Tiempo de Gestión	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
resuelto < = 24 horas	0	0	0	0	0
resuelto 24 horas < = 48 horas	0	0	0	0	0
resuelto 48 horas < = 68 horas	0	0	0	0	0
resuelto > 68 horas	0	0	0	0	0
WA no resueltos, están en proceso y tienen un tratamiento especial	0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


Nivel 1
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 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





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 octubre a 31 de octubre 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&mobile

redirect=true" los cuales contienen la información detallada de cada uno desde el 1 de octubre a 31 de octubre 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 octubre 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	114	400	286
2024	114		
Solicitud	114		
Incidencia	0		
Total Horas Casos Reportados Netsuite	114	400	286
		286	286
		286	286
		286	286
		286	286
Horas consumidasde las 400 - Exp	400	400	0

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

Etiquetas de fila	Suma de Horas Hombre	Horas Presupuesto	Horas Disponibles
CASO	0	100	100
2024	0		
WA	0		
MF	0		
Total Horas Casos Reportados Netsuite	0	100	100
Total Horas Consumidas de las 100 - Exp	0	100	100

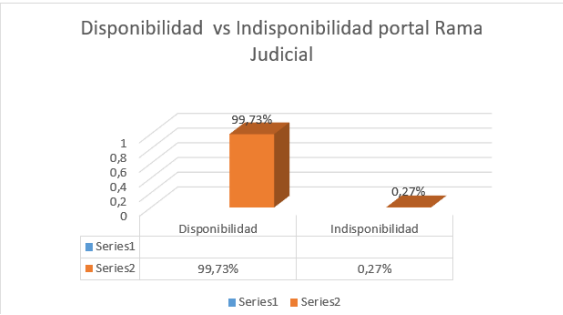
3. *DISPONIBILIDAD E INDISPONIBILIDAD DE LOS SERVICIOS DE HOSTING*

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:

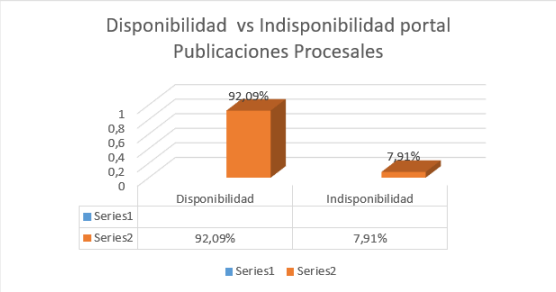
Portal Rama Judicial

Item	Aplicación	Disponibilidad	Indisponibilidad	Tiempo de duracion (Caida en horas)	Tiempo de duracion			
					Dias	Horas	Minutos	Segundos
1	Portal de la Rama Judicial	99,73%	0,27%	2,038333333	0	2	2	18
	Totales	99,73%	0,27%	2,038333333	**0**	2	2	18



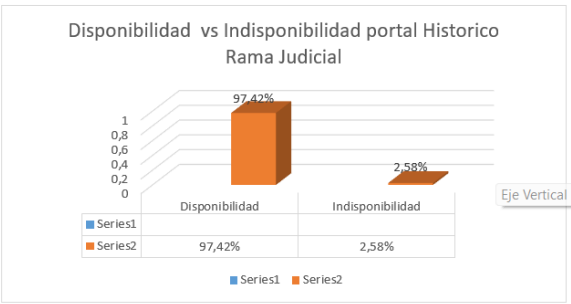
Portal Publicaciones Procesales

Item	Aplicación	Disponibilidad	Indisponibilidad	Tiempo de duracion (Caida en horas)	Tiempo de duracion			
					Dias	Horas	Minutos	Segundos
1	Publicaciones Procesales	92,09%	7,91%	58,83555556	2	10	50	8
	Totales	92,09%	7,91%	58,83555556	**2**	10	50	8



Portal Histórico Rama Judicial

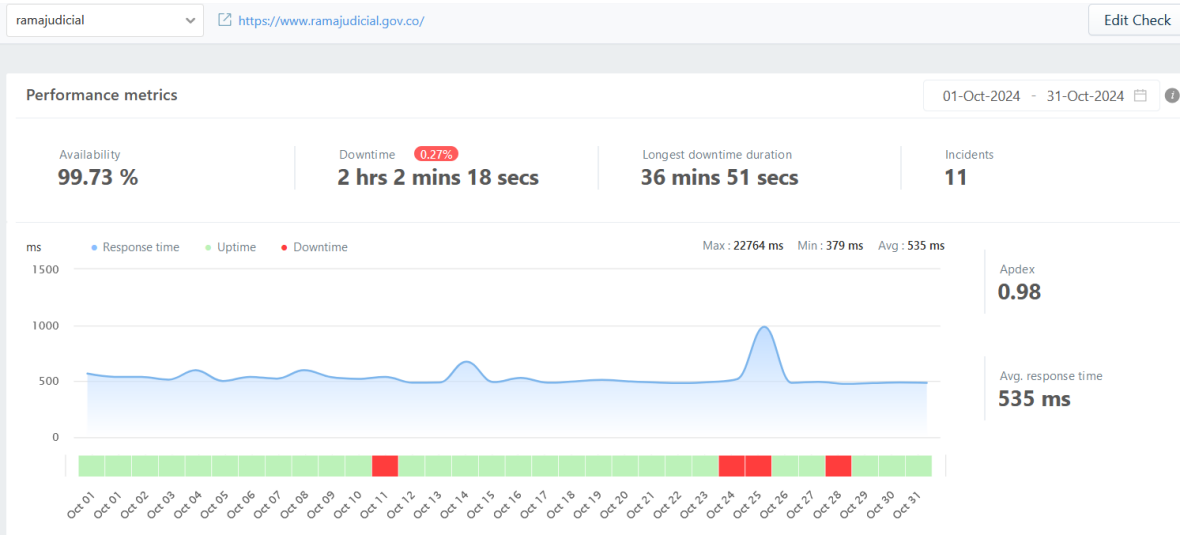
Item	Aplicación	Disponibilidad	Indisponibilidad	Tiempo de duracion (Caida en horas)	Tiempo de duracion			
					Dias	Horas	Minutos	Segundos
1	Portal Historico	97,42%	2,58%	19,16388889	0	19	9	50
	Totales	97,42%	2,58%	19,16388889	**0**	19	9	50



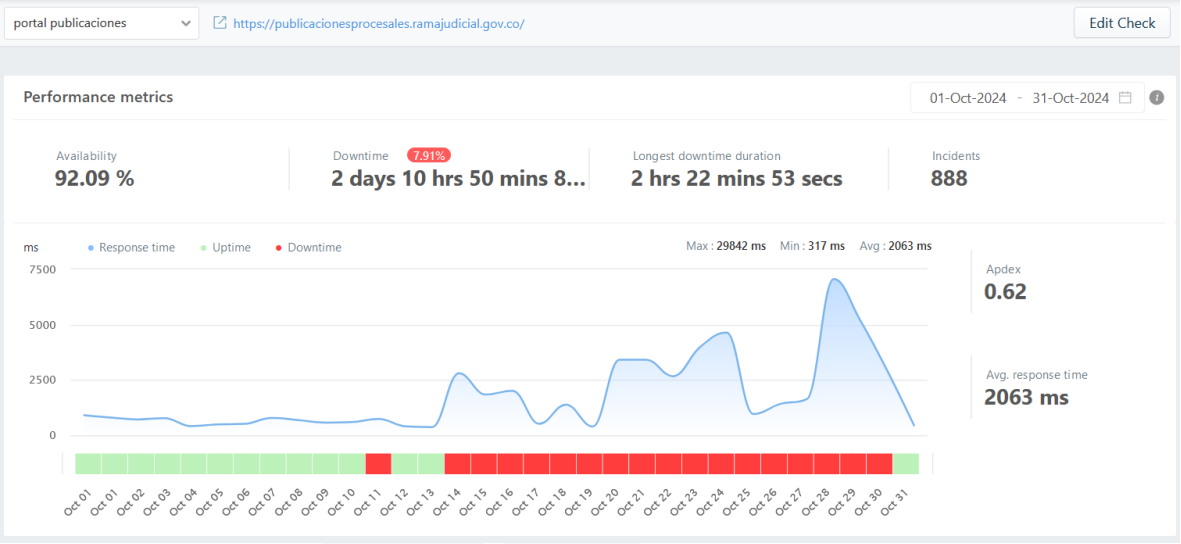
3.2 PORTAL DE LA RAMA JUDICIAL

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

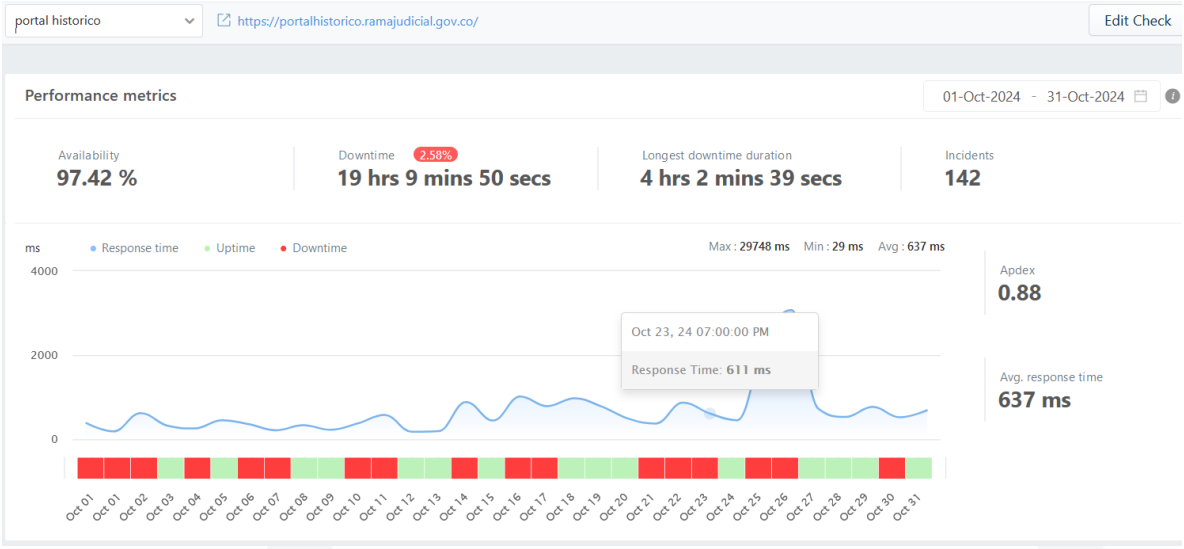
Portal Rama Judicial



Portal Publicaciones Procesales



Portal Histórico Rama Judicial



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	Tunning en datasources y balanceador	31/10/2024		Desarrollo IFX, SoftManagement
2	Generación de índices en tablas de usuarios, elasticsearch	31/10/2024		Desarrollo IFX
3	Validacion capa de seguridad	31/10/2024		Desarrollo IFX, Residente de seguridad

3.2.2 CRECIMIENTO DE LA BASE DE DATOS – INSTANCIA CSJPORTALDB01

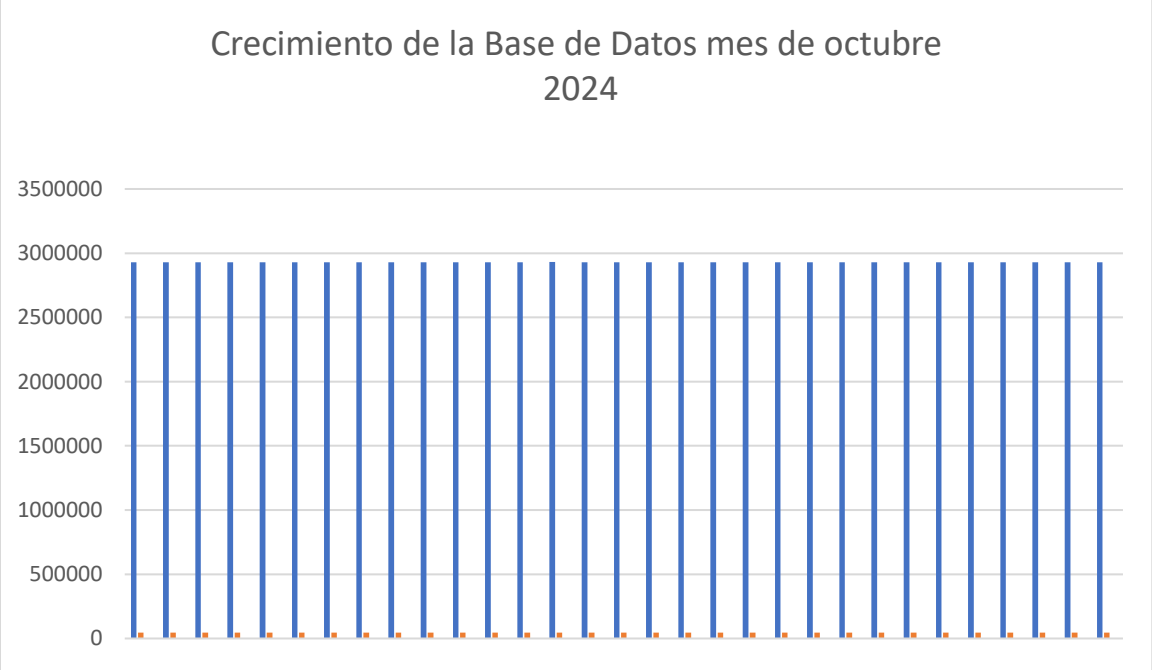
De acuerdo con la solicitud escalada en el **caso TT520553 RV: Crecimiento de la BD de la maquina CSJPORTALDB01** del portal de rama judicial, se agrega el presente informe consolidado del crecimiento que tuvo la BD en el mes de octubre.

BASE DE DATOS lportalramaprod

TAMAÑO (MB0	FECHA	AUMENTO TAMAÑO (MB) POR DIA
2928998 MB	2024-10-01	0
2928998 MB	2024-10-02	0
2928998 MB	2024-10-03	0
2928998 MB	2024-10-04	0
2928998 MB	2024-10-05	0
2928998 MB	2024-10-06	0
2928998 MB	2024-10-07	0
2928998 MB	2024-10-08	0
2928998 MB	2024-10-09	0
2928998 MB	2024-10-10	0
2928998 MB	2024-10-11	0
2928998 MB	2024-10-12	0
2928998 MB	2024-10-13	0
2932172 MB	2024-10-14	3174
2930022 MB	2024-10-15	-2150
2930022 MB	2024-10-16	0
2930022 MB	2024-10-17	0
2930022 MB	2024-10-18	0
2930022 MB	2024-10-19	0
2930022 MB	2024-10-20	0
2930022 MB	2024-10-21	0
2930022 MB	2024-10-22	0
2930022 MB	2024-10-23	0
2930022 MB	2024-10-24	0
2930022 MB	2024-10-25	0
2930022 MB	2024-10-26	0
2930022 MB	2024-10-27	0

2930022 MB	2024-10-28	0
2930022 MB	2024-10-29	0
2930022 MB	2024-10-30	0
2930022 MB	2024-10-31	0

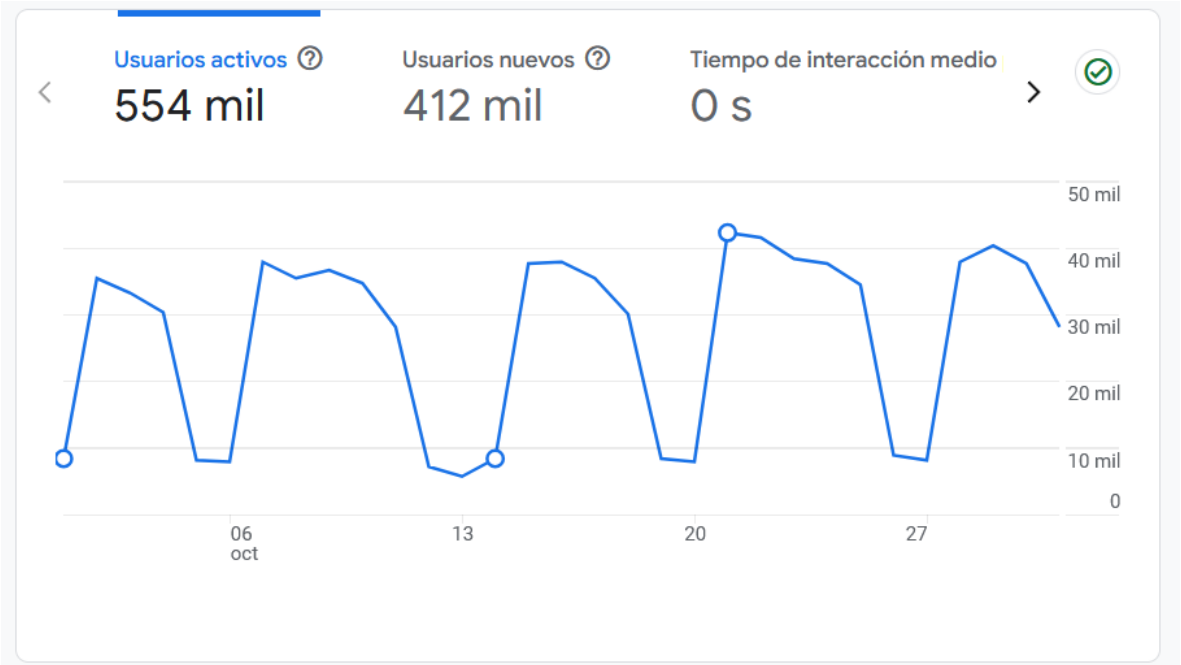
Grafica del crecimiento de la BD Iportalramaprod de la INSTANCIA CSJPORTALB01



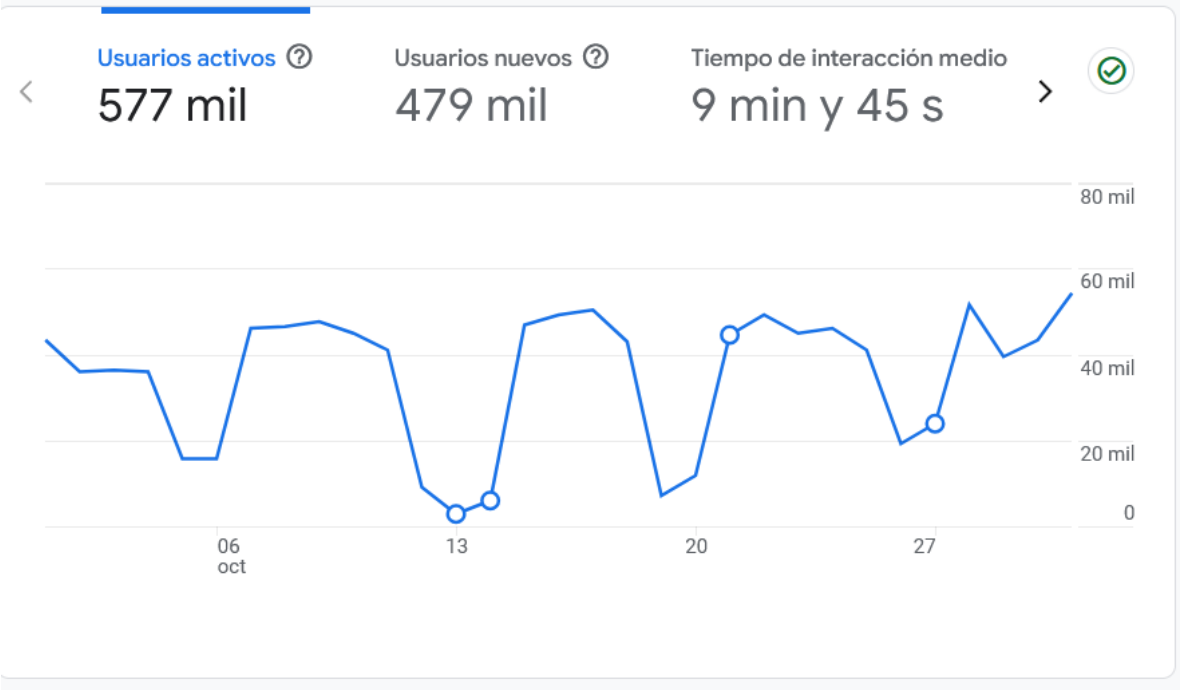
4. ESTADISTICAS PORTAL DE LA RAMA JUDICIAL

4.1 RESUMEN DEL PORTAL

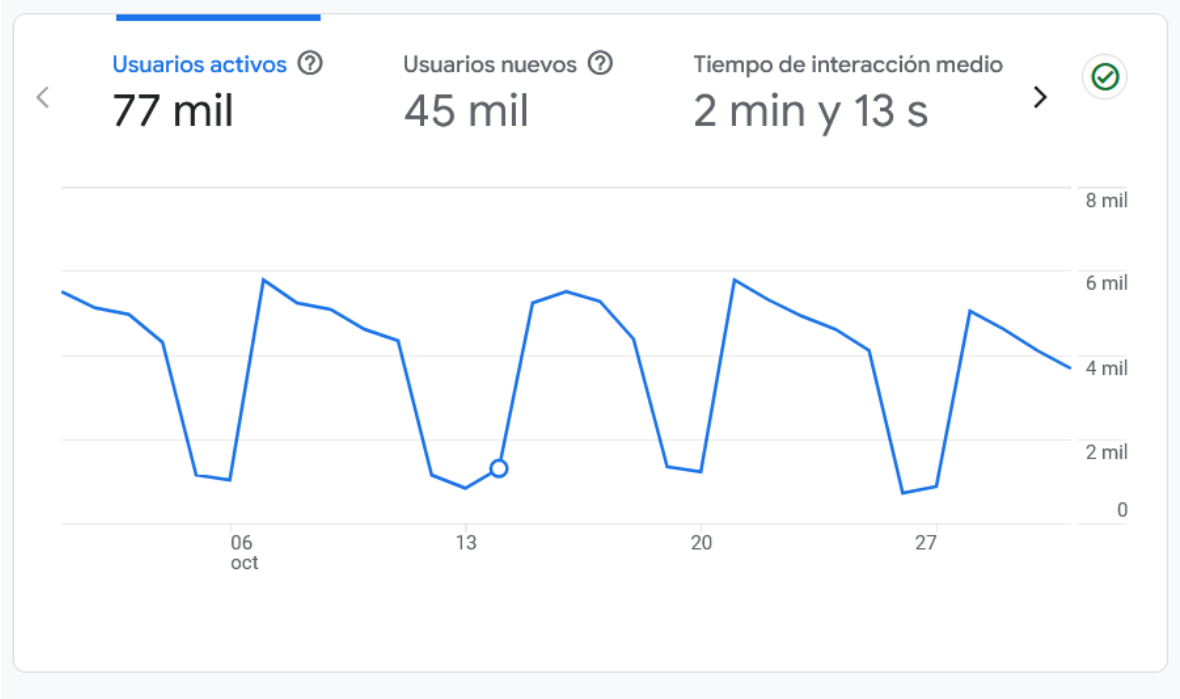
En la respectiva grafica se observa un comportamiento constante durante el mes de octubre para el portal Rama Judicial.



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



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



8. ESQUEMA DE SEGURIDAD

OC	SID	DESCRIPCIÓN	SUBTIPO	NOMBRE DEL EQUIPO	MODELO	SERIAL	UNIDAD DE RACK	RACK
11	2081817	npn04--IaaS Procesamiento -Balanceador de Carga AltaCapacidad - Oro - HostingNube Privada - SesionesCapa L4 (entre 36 y 100Millones) - RAM entre 64GB y128GB - U_Mes - Cantidad: 2	Balanceador DC Torre central	FORTI/PPLA	ADC-2200F	SN: FAD22FT2210000028	10	32
11	2081818	npn04--IaaS Procesamiento -Balanceador de Carga AltaCapacidad - Oro - HostingNube Privada - SesionesCapa L4 (entre 36 y 100Millones) - RAM entre 64GB y128GB - U_Mes - Cantidad: 2	Balanceador DC Torre central	FORTI/BK	ADC-2200F	SN: FAD22FT2210000027	9	32
30	2082020	npn04--IaaS Seguridad - Appliance Anti Ddos - AltaCapacidad - Oro - Hostingfísico - Rol de Inspección - 50Gbps - Paquetes PorSegundo (MPPS) - 45000000- Mes - Cantidad: 2	DDOS DC Torre central	FORTIDDOS FORTINET 2000E/PPLA	2000E	SN: FI2KETB20000015	31-32	32
30	2082021	npn04--IaaS Seguridad - Appliance Anti Ddos - AltaCapacidad - Oro - Hostingfísico - Rol de Inspección - 50Gbps - Paquetes PorSegundo (MPPS) - 45000000- Mes - Cantidad: 2	DDOS DC Torre central	FORTIDDOS FORTINET 2000E/BK	2000E	SN: FI2KE581900004 9	35-36	32
31	2082016	npn04--IaaS Seguridad - Firewall Nueva Generación - Media Capacidad - Oro - Hosting físico - Rol deFirewall - 40 Gbps - SesionesConcurrentes - 15000000 -Mes - Cantidad: 2	FIREWALL	PALACIO - PPLA	FortiGate 900G	SN: FG9H0GTB23900205	N/A	N/A
31	2082017	npn04--IaaS Seguridad - Firewall Nueva Generación - Media Capacidad - Oro - Hosting físico - Rol deFirewall - 40 Gbps - SesionesConcurrentes -	FIREWALL	PALACIO - BK	FortiGate 900G	SN: FG9H0GTB23900440	N/A	N/A

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

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

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

Edward Wilman Sierra Leon
Jose Luis Cardenas Rozo
Victor Hugo Galvis Botia

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

Ingeniero Residente:	Edward Wilman Sierra leon				
Item	**Fecha y Hora de inicio**	**Fecha y Hora de finalización**	**Cantidad de Horas**	**Tipo de Hora extra**	**Actividad Realizada**
1	10/11/2024 18:50	10/11/2024 19:10	1	Diurna	TT910551 RV: Solicitud de apertura Redes sociales 14 al 18 de octubre
2	10/11/2024 19:40	10/11/2024 20:42	2	Diurna	TT910568 RE: Acompañamiento migración ; TT910569 RE: cambio de VLAN
3	10/12/2024 10:00	10/12/2024 16:07	6	Diurna	TT910608 Fwd: Acompañamiento migración; TT910743 Alarma proactiva: SID_2082015_CSJ_KEMP_-WAF-CAN | SID_0_CSJ_www.cortesuprema.gov.co
4	10/15/2024 18:00	10/15/2024 18:53	1	Diurna	TT912018 Acompañamiento para activaciones
Total horas Extras			10		

Ingeniero Residente:	Jose Luis Cardenas				
Item	**Fecha y Hora de inicio**	**Fecha y Hora de finalización**	**Cantidad de Horas**	**Tipo de Hora extra**	**Actividad Realizada**
1	10/6/2024 10:00	10/6/2024 12:00	2	Diurna	Corte de energia en la sede Palacio de Justicia.
2	10/10/2024 18:00	10/10/2024 19:00	1	Nocturno	TT909949 RV: Sesión entreceibas
3	10/10/2024 15:25:00 PM	10/10/2024 16:25:00 PM	1	Diurna	Activación de servicio - CSJ - 50 Cundinamarca,Bogotá; Sede Judicial del CAN,// 1440 8639663 - 8639684 Meta,Villavicencio
4	26/10/2024 07:30:00 AM	26/10/2024 11:30:00 AM	4	Diurna	Mantenimiento de sistemas de trasferencia de planta de energia - Palacio de Justicia
5	26/10/2024 10:00:00 AM	26/10/2024 04:00:00 PM	6	Diurna	TT918685 Activación de servicio - CSJ - 1890 Cundinamarca, Bogotá; Calle 11 # 9-24, Escuela Judicial (Juzgados de Ejecución de Penas)
6	28/10/2024 06:00:00 PM	28/10/2024 07:00:00 PM	1	Nocturno	TT919633 RV: Activación de servicio - CSJ - 884 8661363 Huila,Neiva; Calle 11 # 2-55 -Migracion SDWAN
7	28/10/2024 07:00:00 PM	28/10/2024 08:00:00 PM	1	Nocturno	TT919780 RV: CSJ - SAN ANDRÉS Y PROVIDENCIA - SAN ANDRÉS PALACIO DE JUSTICIA AV LOS LIBERTADORES 2A-106
8	29/10/2024 06:00:00 PM	29/10/2024 09:00:00 PM	3	Nocturno	TT920456 RV: CSJ 11 - Antioquia Medellín; Calle 41 # 52-28 edificio Edatel
9	31/10/2024 06:00:00 PM	31/10/2024 07:00:00 PM	1	Nocturno	TT920996 RV: VENTANA DE MANTENIMIENTO - MIGRACION A CORE NUEVO HMM || DSAJB
Total horas Extras			20		

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	11/10/2024 22:00	12/10/2024 5:00	7	Hora Nocturna	Migración SW core CSJ
2	19/10/2024 11:00:00 AM	19/10/2024 2:00:00 PM	3	Diurna	TT914715 RE: Activación de servicio - CSJ - 1483 - DKO 8639621 - Meta,Villavicencio; Calle 5 # 22-75 Dirección Seccional
3	20/10/2024 06:00:00 PM	20/10/2024 09:00:00 PM	3	Diurna	TT915527 RV: Activación de servicio - CSJ - 61 Nariño,Pasto; Calle 19 # 23-00, Palacio de Justicia - Cesar Ruiz
4	21/10/2024 07:00:00 PM	21/10/2024 08:00:00 PM	1	Diurna	Activación internet para parchado
5	24/10/2024 06:00:00 PM	24/10/2024 09:00:00 PM	3	Diurna	RV: Activación de servicio - CSJ - NARIÑO, PASTO JUZGADO CIVIL MUNICIPAL CALLE 19 - cambo de tecnologia
6	29/10/2024 06:00:00 PM	29/10/2024 08:00:00 PM	2	Diurna	Problemas de acceso VPN y caida de pagians WEB surf.cndj.gov.co por inconvenietes de canales Cirion
Total horas Extras			19		

14.2. Inventario de equipos de seguridad perimetral.

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

#	Descripción	Hostname	Serial	SID	Ubicación	Version Firmware
1	FortiGate-4400F HA	FTG_CSJ_DC_TC_MASTER	FG440FTK21900184	2082019	DC IFX	v7.0.14
		FTG_CSJ_DC_TC_SLAVE	FG440FTK21900183	2082018	DC IFX	v7.0.14
2	FORTIADC 2200F HA	FADC_CSJ_TC_MASTER	FAD22FT221000027	2081818	DC IFX	v6.1.3
		FADC_CSJ_TC_SLAVE	FAD22FT221000028	2081817	DC IFX	v6.1.3
3	WAF KEMP Loadmaster x25 HA	WAF_TORRRE_CENTRAL	TSCC82005608	2082013	DC IFX	7.2.59.3.22368
		WAF_TORRRE_CENTRAL	TSCC8200529	2082014	DC IFX	7.2.59.3.22368
4	Fortigate 900G HA	FGT_900G_CSJ_PALACIO_M	FG9H0GTB23900440	2082016	PALACIO	V7.2.6
		FGT_900G_CSJ_PALACIO_S	FG9H0GTB23900205	2082017	PALACIO	V7.2.6

5	WAF KEMP Loadmaster x25	WAF_CAN	TSCC82005629	2082015	CAN	7.2.59.3.22368
6	FortiDDos 2000E HA	CSJ_FDDoS_MASTER	FI-2KE5819000049	2082020	DC IFX	v6.3.3
		CSJ_FDDoS_SLAVE	FI-2KETB2000015	2082021	DC IFX	v6.3.3

14.3. Actualización de firmware.

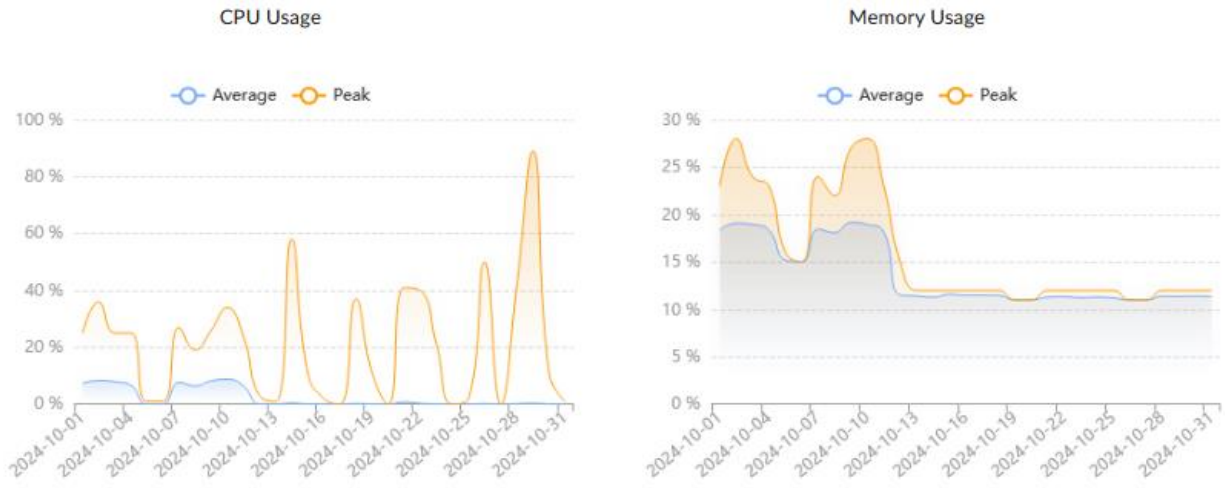
El plan de trabajo para la actualización del firmware será compartido, presentado y ejecutado con la autorización de los ingenieros Datacenter del CONSEJO SUPERIOR DE LA JUDICATURA.

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

WAF_CAN KEMP	7.2.59.3.22368	Actualizado	N/A
CSJ_FDDoS_MASTER	V5.7.3	Actualizado	N/A
CSJ_FDDoS_SLAVE	V5.7.3	Actualizado	N/A

15. FIREWALL PERIMETRAL

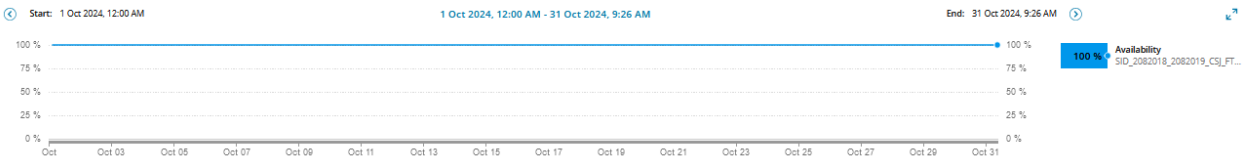
Durante octubre, el consumo promedio de CPU y memoria (traza azul) en el firewall perimetral estuvieron dentro de sus valores de operación normal.



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

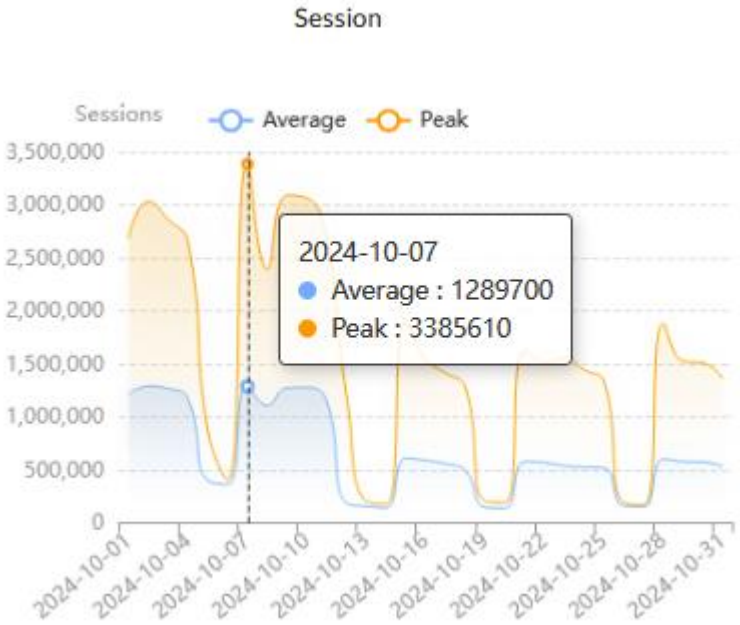
15.1. Disponibilidad mensual firewall perimetral.

Durante octubre se obtuvo 100% de disponibilidad en el firewall perimetral.



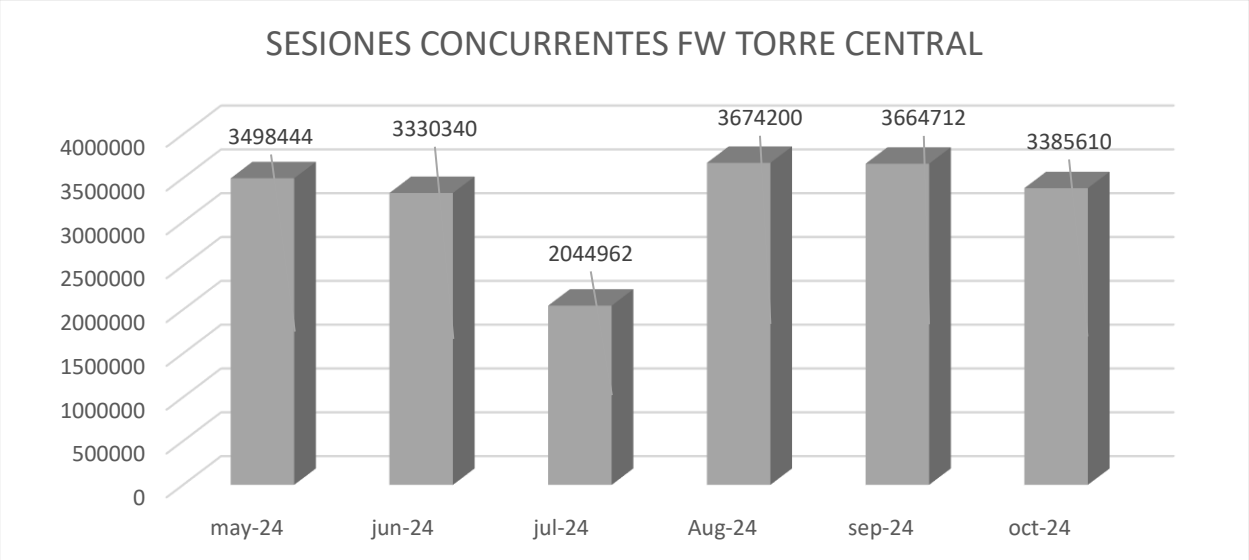
15.2. Cantidad de sesiones firewall perimetral.

Durante octubre se presentó un máximo de 3385610 sesiones TCP concurrentes, cantidad que se encuentra dentro del rango máximo soportado por el appliance Fortinet FG- 4400F cuyo valor es de 210 millones.



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

Durante los últimos 3 meses las sesiones en el FW perimetral se han mantenido constantes:



MES	SESIONES
may-24	3498444
jun-24	3330340
jul-24	2044962
Aug-24	3674200
sep-24	3664712
oct-24	3385610

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

HTTPS fue la aplicación con mayor consumo de ancho de banda durante octubre:

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	HTTPS			344.03 TB
2	Microsoft.SharePoint			90.02 TB
3	SSL			43.06 TB
4	Microsoft.Teams			39.43 TB
5	OneDrive			28.33 TB
6	Microsoft.365.Portal			22.68 TB
7	Microsoft.Portal			22.38 TB
8	Microsoft.Outlook			21.73 TB
9	TCP/9443			16.56 TB
10	WhatsApp			15.99 TB

HTTPS, DNS y SMB fueron las aplicaciones con mayor consumo durante octubre:

Top Applications by Sessions

#	Application	Sessions
1	HTTPS	4,085,070,455
2	DNS	3,201,841,703
3	SMB	2,086,536,603
4	TCP/5508	804,169,515
5	SSL	756,873,924
6	Microsoft.365.Portal	682,807,914
7	Microsoft.Portal	584,531,150
8	Microsoft.Windows.Update	503,782,482
9	HTTP	443,850,149
10	ESET-Eset.Service	434,018,711

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

172.16.182.85 (PC de la sede Valle, Cali; Palacio de Justicia) consumió la mayor cantidad de ancho de banda durante octubre:

Top Bandwidth IP

#	IP	Bandwidth
1	172.16.182.85	6.36 TB
2	10.101.100.114	5.05 TB
3	10.101.100.38	4.36 TB
4	10.101.101.14	2.25 TB
5	10.101.100.34	1.75 TB
6	10.101.101.54	1.43 TB
7	10.101.102.138	1.17 TB
8	10.101.102.6	1.13 TB
9	10.101.100.134	1.12 TB
10	10.101.100.170	1.01 TB

15.6. Top de destinos web por sesiones firewall perimetral.

8.243.164.21 (CTL Colombia) y 172.28.107.71 (Microsoft) fueron los destinos más consultados durante octubre.

Top Destinations by Sessions

#	Hostname(or IP)	Sessions
1	8.243.164.21	536,398,546
2	172.28.107.71	401,694,328
3	8.243.164.19	394,014,581
4	172.28.107.58	391,594,817
5	172.28.107.61	388,152,842
6	192.168.213.94	263,453,917
7	microsoft.com	257,474,290
8	4.175.87.197	184,694,022
9	windowsupdate.com	155,723,111
10	172.16.182.100	150,415,213

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

172.16.235.99 de la sede Edificio Kaiser II Torre Central, presentó la mayor cantidad de peticiones bloqueadas durante octubre:

Top Web Users by Blocked Requests

#	User (or IP)	Hostname	Requests
1	172.16.235.99	172.16.235.99	6,069,463
2	172.16.156.78	172.16.156.78	2,484,670
3	172.16.33.29	172.16.33.29	1,590,233
4	172.28.86.90	172.28.86.90	1,542,386
5	172.16.156.57	172.16.156.57	1,242,736
6	172.16.32.154	172.16.32.154	1,146,730
7	172.28.121.167	172.28.121.167	1,112,957
8	172.16.35.145	172.16.35.145	1,091,897
9	172.29.182.95	172.29.182.95	918,562
10	172.16.120.46	172.16.120.46	901,433

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

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

Streaming Media and Download fue la categoría con mayor cantidad de bloqueos durante octubre.

Top Blocked Web Categories

#	Category	Requests
1	Streaming Media and Download	41,407,987
2	Social Networking	12,323,674
3	Proxy Avoidance	3,662,967
4	Unrated	2,908,814
5	Games	2,201,544
6	Internet Radio and TV	1,525,980
7	Entertainment	529,597
8	IOC_Blacklist_Domains_Cyber	366,561
9	Information Technology	311,579
10	Society and Lifestyles	281,756

15.9. Top de IP más activos Firewall Perimetral

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

Top Web IP by Allowed Requests

#	IP	Requests
1	10.101.100.38	17,530,406
2	10.101.100.114	15,975,211
3	10.101.100.34	7,724,704
4	10.101.101.54	6,879,482
5	10.101.101.246	5,179,538
6	10.101.100.170	5,091,068
7	10.101.100.230	5,025,180
8	10.101.102.138	4,934,243
9	10.101.101.50	4,830,735
10	10.101.100.134	4,822,752

15.10. Top de categorías más visitadas Firewall Perimetral

La categoría más visitada durante octubre fue Information Technology:

Top Allowed Web Categories

#	Category	Requests
1	Information Technology	524,079,809
2	Overrride_permitidas	364,612
3	Unrated	2

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

172.28.107.87 de traspaso de información de TX_400TB-AWS, presentó el mayor consumo de ancho de banda durante octubre:

Top IP by Bandwidth

#	IP	Bandwidth	Sent	Received
1	172.28.107.87		261.79 TB	
2	172.27.177.3		8.12 TB	
3	172.17.201.251		7.27 TB	
4	172.16.182.85		6.67 TB	
5	172.28.107.91		6.17 TB	
6	10.101.100.114		6.10 TB	
7	10.101.100.38		5.52 TB	
8	172.27.64.14		4.55 TB	
9	10.101.101.14		2.89 TB	
10	10.1.1.2		2.55 TB	

16. TRÁFICO VPN FIREWALL PERIMETRAL

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

#	Usuario_VPN	devname	Tipo de conexión	Ultima Conexión	fv_dtime_tz_conv_e_time_t	IPs de origen de la conexión	Cantidad de conexiones	Duración	Consumo	traffic_in	traffic_out
1	Ecoralb	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-10-31 23:59:11	1730419151	186.154.96.194	183	690:44:12	31.16 GB	3949098506	29512228466
2	lbarrerf	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-10-31 22:11:57	1730412717	186.155.111.38;186.155.130.167;186.155.137.25;191.156.225.171;191.156.227.119;191.156.227.200;191.156.236.73;200.119.51.5	95	424:46:36	58.68 GB	3149249709	59858969078
3	pfajardg	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-10-31 23:53:14	1730418794	186.81.100.20	70	422:40:57	9.92 GB	1102508934	9553742576
4	vperezg	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-11-01 00:00:04	1730419204	129.222.203.208;129.222.203.254;129.222.203.36;138.84.40.105;138.84.40.3;138.84.40.49;138.84.40.92;138.84.41.148;138.84.41.185;138.84.41.6;138.84.41.61;172.29.55.3;186.102.17.147;186.102.63.197;186.145.248.181;191.156.229.206;200.189.27.108;200.189.27.125;200.189.27.38;200.189.27.7;200.189.27.92;200.189.27.94	415	420:29:14	594.37 MB	425715632	197522156

5	lmarinmo	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-10-31 06:32:17	1730356337	181.136.237.173	122	403:49:59	7.45 GB	771881926	7223954616
6	lcardenas	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-10-31 22:47:24	1730414844	181.49.225.42;191.108.24.149;200.118.63.31;201.184.87.194	186	391:55:58	54.53 GB	4783271334	53765051210
7	rgutierm	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-10-31 23:58:13	1730419093	179.19.7.255;181.59.148.17;181.59.2.210;181.59.2.27;181.59.3.218;181.59.3.226;181.59.3.249;181.59.3.83;190.255.246.111;190.66.141.113;191.107.1.6;191.107.12.120;191.107.24.4;191.107.3.56;191.107.5.4;191.107.6.227	100	388:26:27	2.28 GB	184753939	2267189021
8	cvillam	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-11-01 00:02:12	1730419332	181.55.51.20	120	369:21:33	5.77 GB	526141952	5669904116
9	jariasu	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2024-10-31 23:53:13	1730418793	181.137.8.129	1024	366:47:17	1.50 GB	161253637	1452003844

10	csichaca	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel;ssl-web	2024-10-31 14:13:14	1730383994	132.255.23.26;181.234.187.150;186.102.109.84;186.102.117.84;186.102.146.81;186.102.211.113;186.102.221.64;186.102.236.3;186.102.235.84;186.114.147.143;186.114.177.184;186.114.214.121.187;186.114.226.168;186.114.96.18;186.114.96.73;186.114.99.138;186.168.232.236;186.168.235.217;190.102.123.66;190.102.123.6;190.102.132.123.66	124	349:49:35	9.68 GB	891978274	9505241717

16.1. VPN IPSEC Site To Site Firewall Perimetral

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

Site-to-Site IPsec Tunnel	Initiating FortiGate	Terminating FortiGate	Duration	Bytes (Sent/Received)
VPN_AZURE	190.217.24.4 Bogota, Colombia	52.240.53.161 Potomac Falls, United States	31d 1h 12m 13s	30.8 TB/2.5 TB
VPN_ORACLE	190.217.80.4 Barrancabermeja, Colombia	129.213.6.36 Ashburn, United States	31d 1h 12m 52s	206.2 GB/2.5 TB
VPN_SIUG_AWS-2	190.217.24.4 Bogota, Colombia	34.224.152.152 Ashburn, United States	31d 1h 11m 10s	329.9 GB/177.1 GB
VPN_SIUG_AWS	190.217.24.4 Bogota, Colombia	34.194.187.190 Ashburn, United States	31d 1h 1m 55s	222.9 GB/257.3 GB
VPN_AZURE-ANALY	190.217.24.4 Bogota, Colombia	20.124.34.235 Potomac Falls, United States	31d 1h 12m 03s	196.5 GB/6.6 GB
VPN_Tierras	190.217.24.4 Bogota, Colombia	181.225.76.196 Anserma, Colombia	31d 0h 35m 39s	1.7 GB/61.4 GB
VPN_Linktic	190.217.24.4 Bogota, Colombia	3.222.171.115 Ashburn, United States	30d 23h 42m 08s	67.3 MB/792.5 MB
VPN_REGISTRADU	190.217.24.4 Bogota, Colombia	201.232.123.20 Medellin, Colombia	30d 23h 48m 31s	319.4 MB/538.2 MB
VPN_INPEC	190.217.19.156 Bogota, Colombia	190.25.112.10 Bogota, Colombia	30d 23h 24m 04s	140.8 MB/695.4 MB
VPN_FISCALIA	190.217.24.4 Bogota, Colombia	190.157.218.66 Bogota, Colombia	31d 1h 2m 45s	1.5 MB/28.6 MB
VPN_AZURE-VWAN2	190.217.24.4 Bogota, Colombia	4.153.117.131 Redmond, United States	31d 0h 52m 21s	12.1 KB/0.0 KB
VPN_AZURE-VWAN	190.217.24.4 Bogota, Colombia	4.153.117.133 Redmond, United States	31d 0h 52m 50s	0.0 KB/11.7 KB

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

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

Top Attacks

#	Attack Name	Severity	CVE-ID	Counts
1	tcp_syn_flood	Critical		108,762
2	Spring.Framework.SerializationUtils.Insecure.Deserialization	Critical	CVE-2022-22965	107,781
3	tcp_src_session	Critical		28,499
4	ip_dst_session	Critical		25,064
5	Apache.Log4j.Error.Log.Remote.Code.Execution	Critical	CVE-2021-4104,CVE-2021-44228,CVE-2021-45046	22,024
6	Adobe.ColdFusion.Multiple.Vulnerabilities	Critical	CVE-2013-0625,CVE-2013-0629,CVE-2013-0631,CVE-2013-0632	21,786
7	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	Critical	CVE-2017-11317,CVE-2017-11357,CVE-2019-18935	14,515
8	HTTP.URI.Java.Expression.Language.Code.Injection	Critical	CVE-2021-22053,CVE-2022-26134	14,271
9	Ivanti.EPMM.CVE-2023-35082.Authentication.Bypass	Critical	CVE-2023-35082	14,109
10	tcp_dst_session	Critical		13,921

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

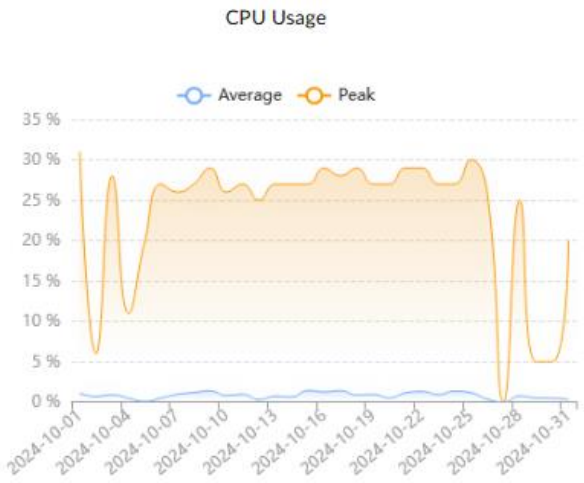
Top Intrusion Victims

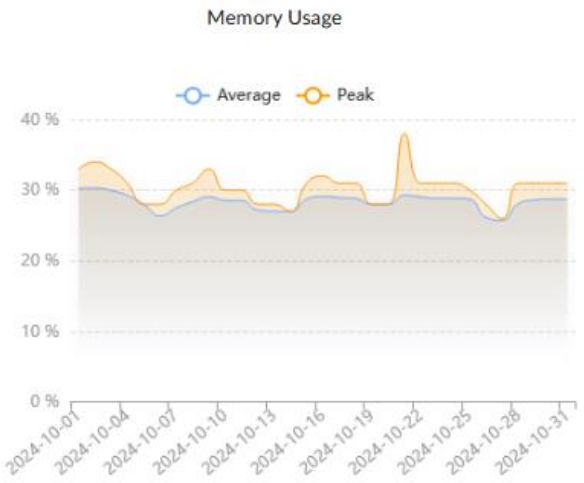
#	Attack Victim	Counts	Critical	High	Medium	Percent of Total Attacks
1	172.17.201.6				1,542,975	30.01%
2	172.17.202.151				1,540,844	29.97%
3	172.17.202.30				1,539,764	29.95%
4	172.17.201.13				161,349	3.14%
5	172.17.201.52				87,515	1.70%
6	190.217.24.175				56,064	1.09%
7	190.217.24.176				53,517	1.04%
8	163.70.152.60				33,265	0.65%
9	172.17.202.141				28,115	0.55%
10	172.17.201.100				27,140	0.53%

Los hosts 172.17.201.X, 172.17.202.X, son aplicaciones web protegidas por los WAF Torre Central y el WAF CAN. Se debe verificar los demás hosts con software antivirus

17. FIREWALL SEDE PALACIO

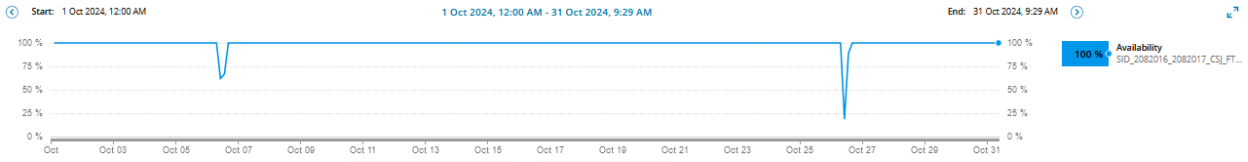
Durante octubre, el consumo de CPU y memoria en el Firewall de Palacio se mantuvo dentro de sus valores de operación normal.





17.1. Disponibilidad Mensual Firewall Palacio

El evento del 6 de octubre hace referencia a un corte de energía en la sede Palacio de Justicia al que referencia el caso TT907000= Incidencia Proactiva: SID_2082016_2082017_CSJ_FTG_900G_PALACIO y el evento del 26 de octubre hace referencia a un mantenimiento de sistemas de trasferencia de planta de energía en Palacio de Justicia por parte del cliente CSJ.



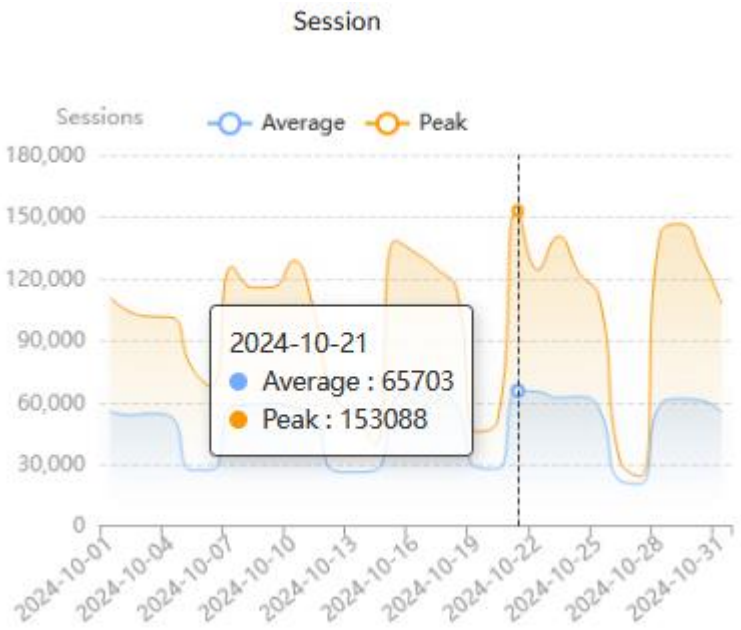
A pesar de los cortes de energía, la disponibilidad durante octubre fue de 99,302%:

Availability Statistics

PERIOD	AVAILABILITY
Today	100,000 %
Yesterday	100,000 %
Last 7 Days	98,358 %
Last 30 Days	99,302 %

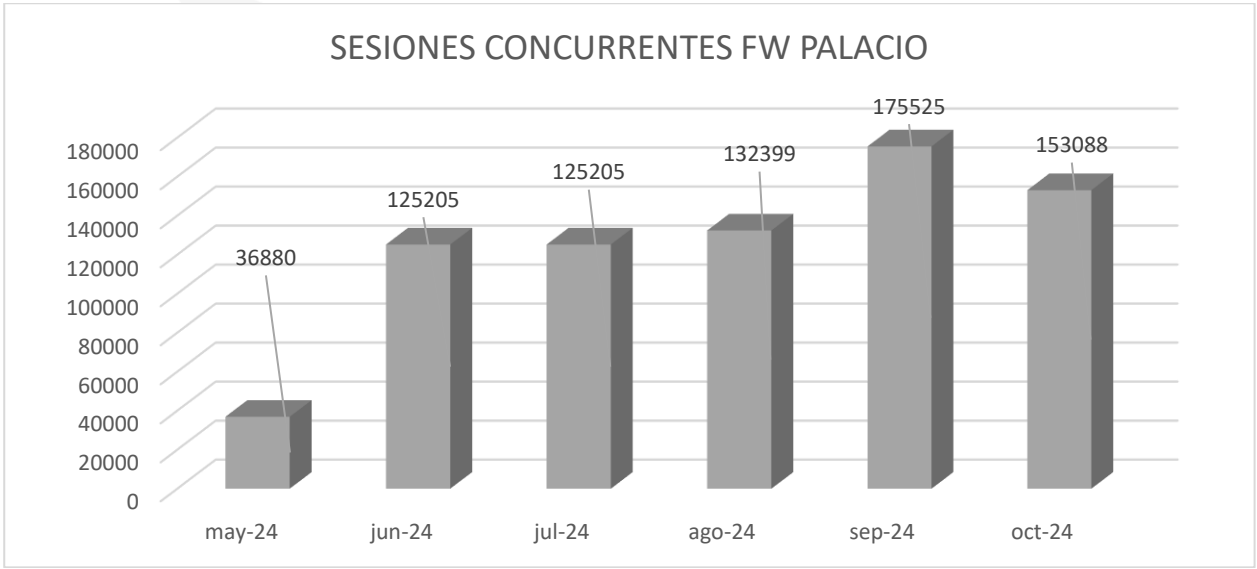
17.2. Cantidad de Sesiones Firewall Palacio

Durante octubre se presentó un máximo de 153088 sesiones concurrentes que están dentro del rango de sesiones soportadas por el equipo Fortigate 900G de 16 Millones.



17.3. Histórico de Sesiones Últimos 6 meses Firewall Palacio

Durante octubre la cantidad de conexiones disminuyeron levemente respecto al mes anterior de septiembre:



MES	SESIONES
may-24	36880
jun-24	125205
jul-24	125205
ago-24	132399
sep-24	175525
oct-24	153088

17.4. Aplicaciones y protocolos por ancho de banda firewall Palacio

Microsoft.Portal consumió la mayor cantidad de ancho de banda durante octubre:

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	Microsoft.Portal			8.05 TB
2	HTTPS.BROWSER			6.17 TB
3	Microsoft.SharePoint			6.08 TB
4	OneDrive			3.99 TB
5	SSL			3.06 TB
6	Microsoft.365.Portal			1.32 TB
7	Microsoft.Outlook			1.09 TB
8	Microsoft.Teams			1,004.78 GB
9	Microsoft.Windows.Update			557.77 GB
10	WhatsApp			526.06 GB

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

Top Applications by Sessions

#	Application	Sessions
1	SMB	744,558,680
2	DNS	62,268,937
3	HTTP.BROWSER	50,836,878
4	Microsoft.365.Portal	38,032,908
5	SSL	31,677,146
6	Microsoft.Windows.Update	31,389,062
7	Rapid7.Insight.Agent	31,231,182
8	HTTPS.BROWSER	29,928,202
9	Microsoft.Portal	26,551,948
10	tcp/44345	17,980,551

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

172.28.93.2 de la Comisión Nacional de Disciplina Judicial consumió la mayor cantidad de ancho de banda durante octubre:

Top Bandwidth IP

#	IP	Bandwidth
1	172.28.93.2	3.23 TB
2	172.29.154.19	620.96 GB
3	172.16.4.70	570.31 GB
4	172.28.92.31	511.77 GB
5	172.16.5.33	495.82 GB
6	172.16.2.59	486.63 GB
7	172.28.92.36	466.56 GB
8	172.28.92.23	451.16 GB
9	172.28.92.26	346.26 GB
10	172.17.114.88	312.84 GB

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

Eset.com fue el destino más visitado durante octubre:

Top Destinations by Sessions

#	Hostname(or IP)	Sessions
1	eset.com	48,007,897
2	rapid7.com	15,841,752
3	8.243.200.3	12,016,618
4	microsoft.com	11,782,142
5	windowsupdate.com	9,371,226
6	8.243.164.19	9,269,087
7	8.8.8.8	9,264,316
8	172.28.107.71	7,805,788
9	172.28.107.58	7,743,050
10	200.31.13.169	6,514,905

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

172.16.5.3 (Corte Suprema de Justicia - Comunicaciones-Deaj) y 172.16.6.68 (host de la LAN Palacio) presentaron la mayor cantidad de conexiones bloqueadas durante octubre.

Top Web Users by Blocked Requests

#	User (or IP)	Hostname	Requests
1	172.16.5.3	172.16.5.3	402,104
2	172.16.6.68	172.16.6.68	307,459
3	172.16.6.161	172.16.6.161	149,596
4	172.16.6.55	172.16.6.55	137,125
5	172.16.2.8	172.16.2.8	115,871
6	172.16.6.56	172.16.6.56	112,551
7	172.16.2.15	172.16.2.15	111,857
8	172.16.4.144	172.16.4.144	100,503
9	172.16.6.183	172.16.6.183	74,834
10	172.29.108.21	172.29.108.21	70,994

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

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

Las categorías más bloqueadas durante octubre en el firewall Palacio fueron Unrated (las desconocidas, las no clasificadas):

Top Blocked Web Categories

#	Category	Requests
1	Unrated	7,437,881
2	Social Networking	862,286
3	Proxy Avoidance	526,928
4	Streaming Media and Download	430,977
5	Games	188,086
6	Malicious Websites	155,776
7	Society and Lifestyles	55,917
8	Entertainment	54,898
9	Newly Observed Domain	21,696
10	Remote Access	7,320

17.9. Top de IP más activas Firewall Palacio

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

Top Web IP by Allowed Requests

#	IP	Requests
1	172.16.4.90	25,942,043
2	172.28.54.20	18,310,001
3	172.16.2.99	569,520
4	192.168.8.18	564,727
5	192.168.2.16	438,816
6	172.16.2.230	412,460
7	172.16.6.121	411,139
8	172.17.114.35	398,339
9	172.16.4.205	394,775
10	172.17.114.118	390,878

17.10. Top de las categorías más visitadas firewall Palacio.

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

Top Allowed Web Categories

#	Category	Requests
1	Information Technology	39,966,352
2	Search Engines and Portals	3,970,790
3	Business	1,825,975
4	Information and Computer Security	655,745
5	Web Analytics	542,089
6	Web-based Applications	162,277
7	Overrride_permitidas	116,391
8	Finance and Banking	88,977
9	Online Meeting	38,527
10	Secure Websites	37,605

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

172.29.154.58 y 172.28.93.2 (hosts de la Comisión Nacional de Disciplina Judicial) presentaron la mayor cantidad de conexiones durante octubre:

Top IP by Bandwidth

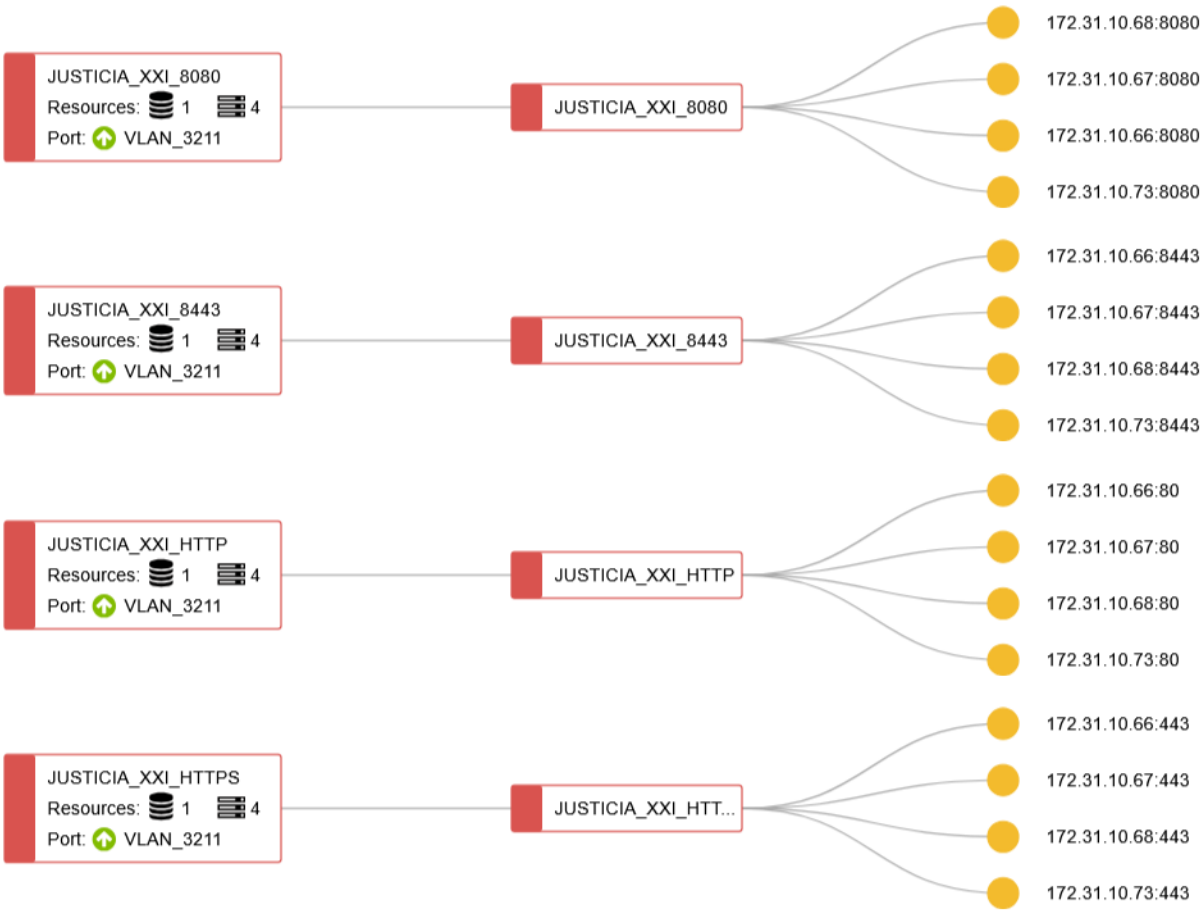
#	IP	Bandwidth	Sent	Received
1	172.29.154.58			3.26 TB
2	172.28.93.2			3.24 TB
3	172.16.6.92			1.19 TB
4	172.28.92.15			681.20 GB
5	172.29.154.19			617.98 GB
6	172.16.4.70			582.43 GB
7	172.16.2.59			513.57 GB
8	172.29.65.72			506.96 GB
9	172.28.92.31			504.05 GB
10	172.16.5.33			494.90 GB

18. BALANCEADOR DE CARGA FORTIADC

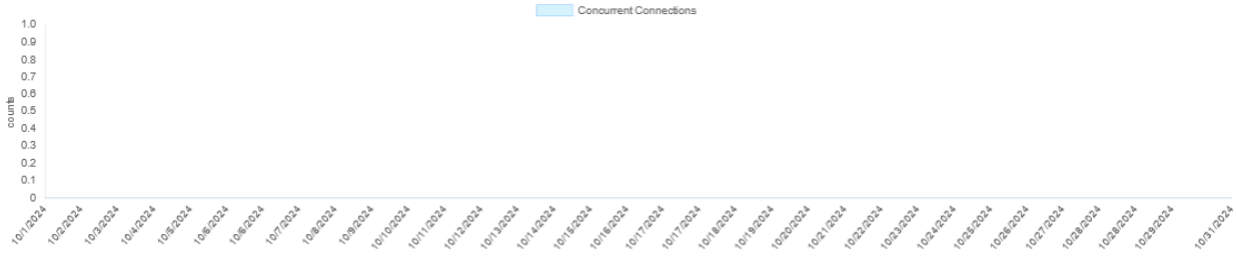
A continuación, se observan los diferentes servicios balanceados.

18.1. Justicia XXI

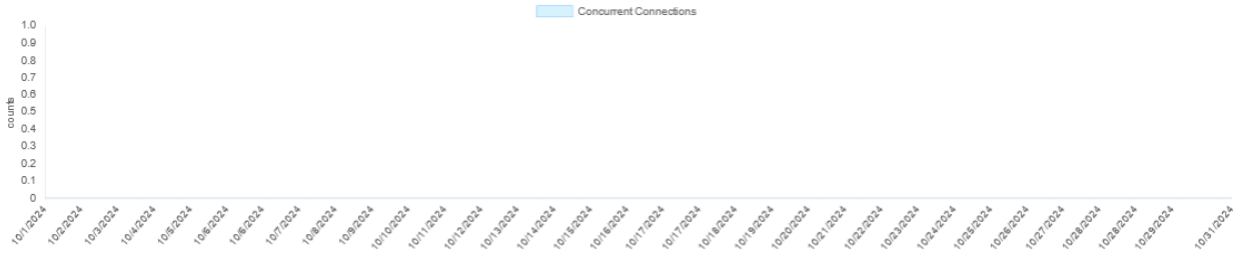
Se encuentra balanceado en el FortiADC:



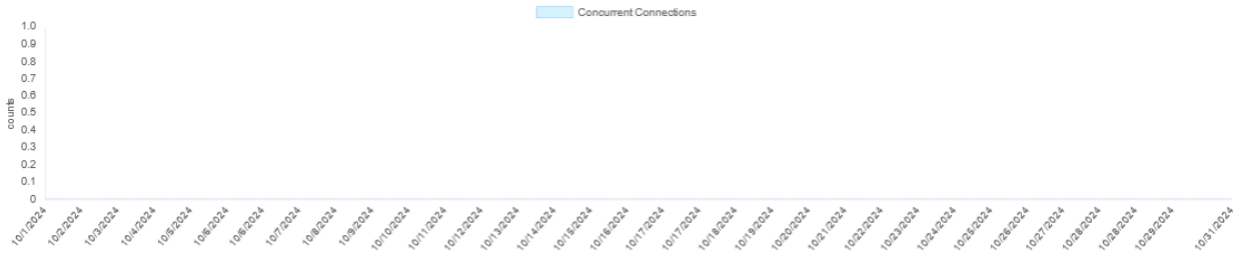
Durante octubre no se presentó tráfico por el puerto 8080:



Conexiones concurrentes por el puerto 8443:



Conexiones concurrentes por el puerto 443:

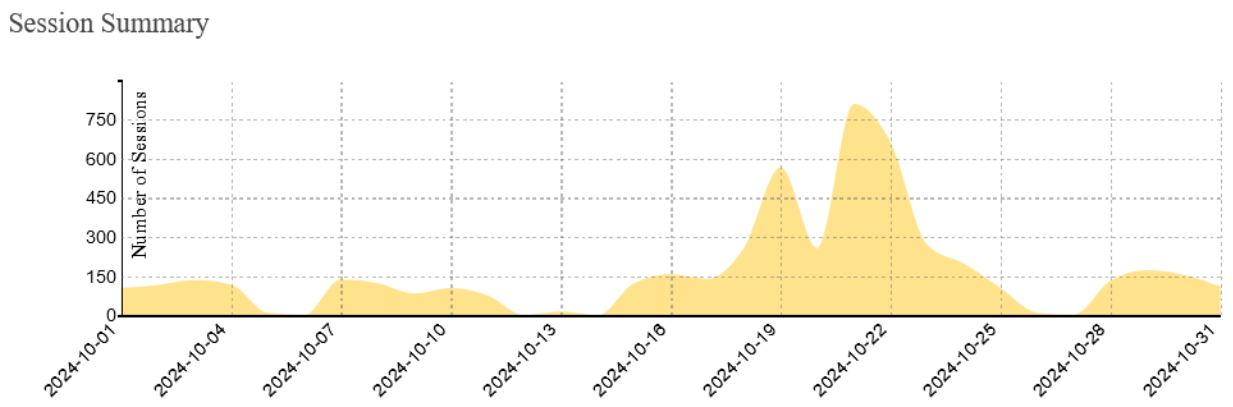


18.2. Kactus RDP

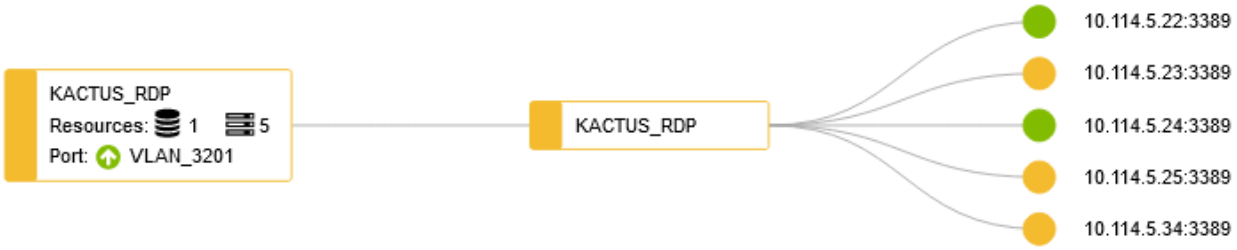
Esta aplicación se encuentra en el Firewall utilizando la siguiente configuración:

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

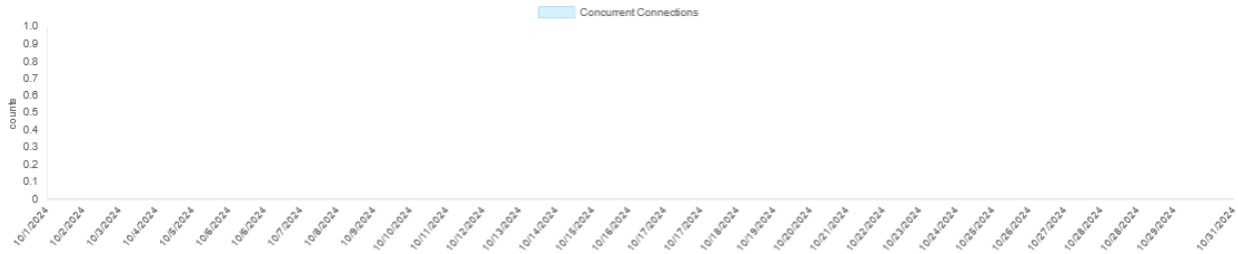
A continuación, se observa el número de sesiones concurrentes para este aplicativo.



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

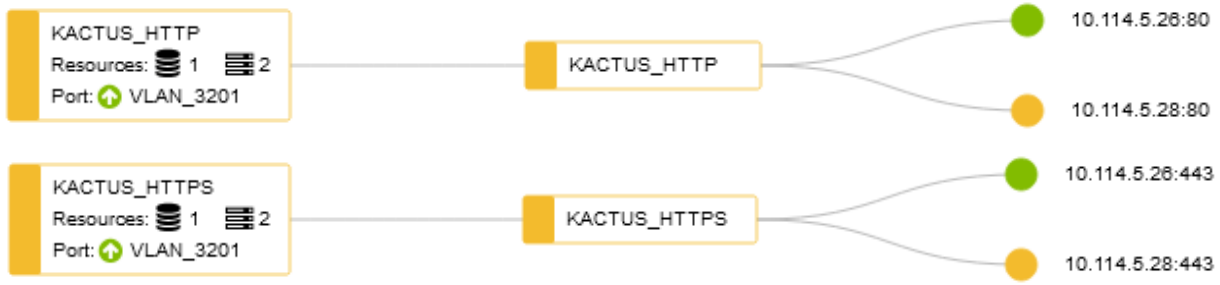


En el FortiADC no se observan sesiones concurrentes:

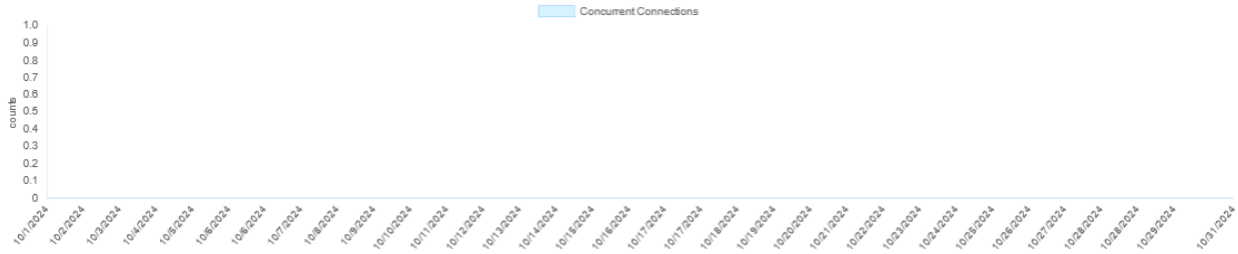


18.3. Kactus WEB

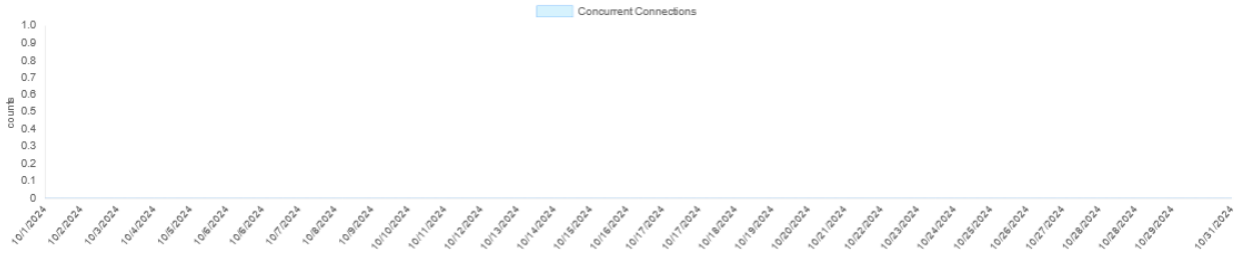
Se encuentra balanceado en el FortiADC:



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



Por HTTPS se observan las siguientes conexiones del mes:



18.4. SIRNA

Este servicio se encuentra balanceado en el FortiGate perimetral:

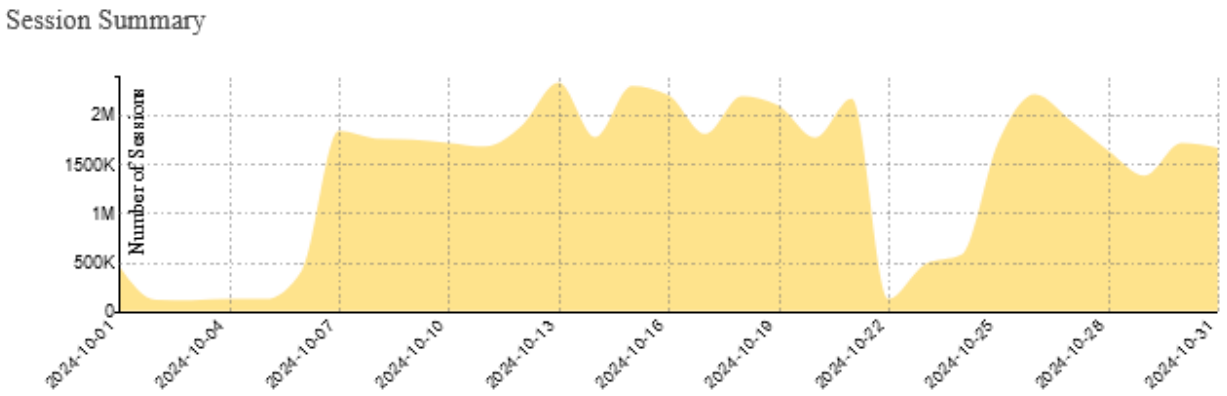
Configuración de balanceo de CRM en el Firewall.

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

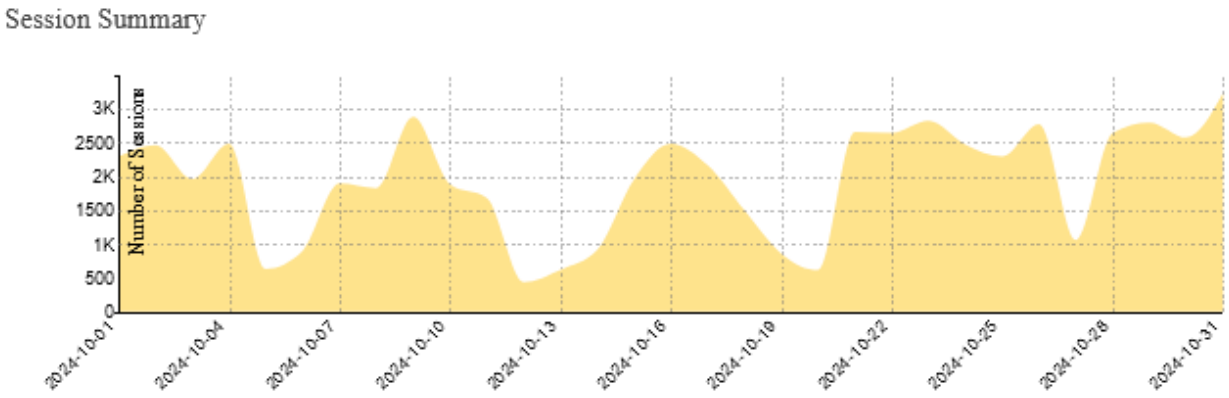
Configuración de balanceo de Sharepoint en el firewall perimetral.

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

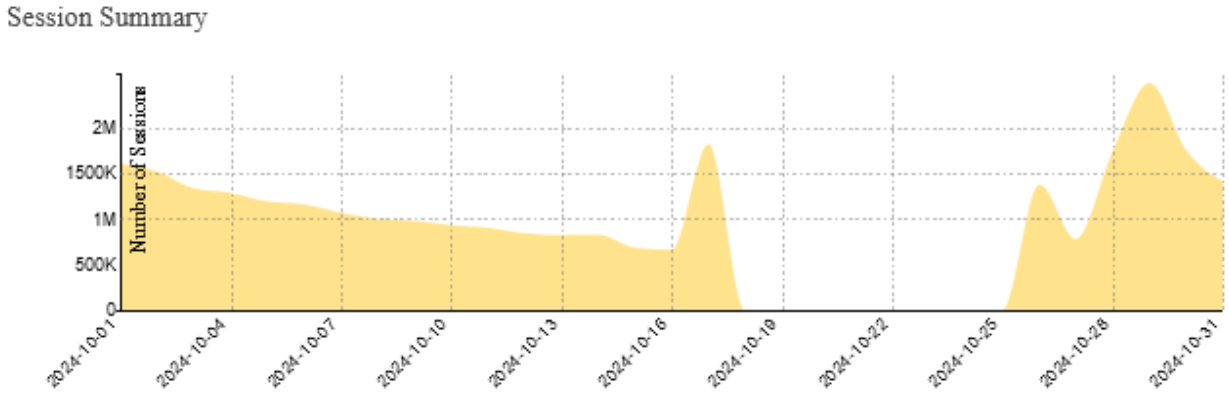
Las sesiones en el firewall para SIRNA 443 fueron:



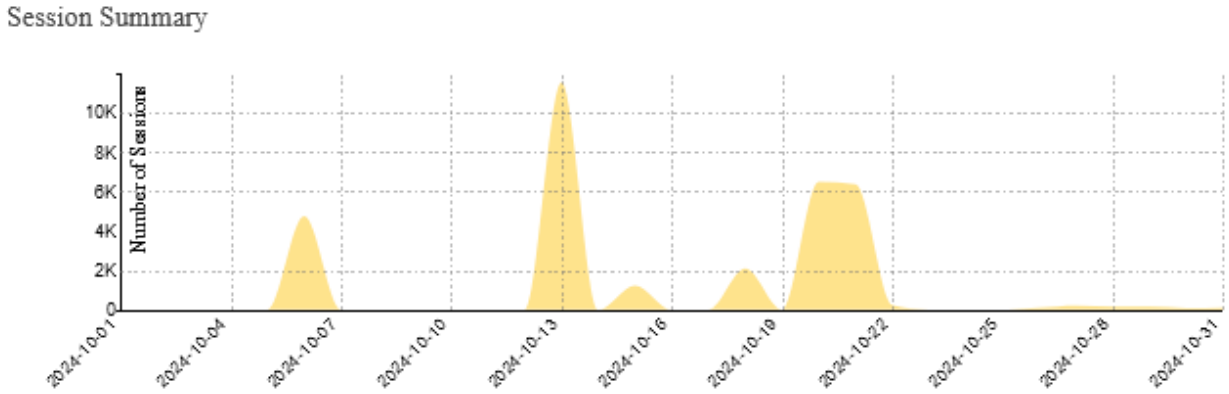
Las sesiones en el firewall para SIRNA 4443 fueron:



Las sesiones en el firewall para CRM 443 fueron:



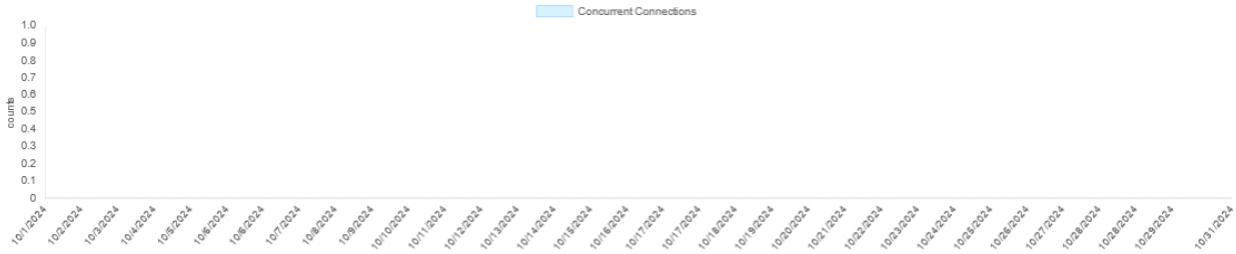
Las sesiones en el firewall para Sharepoint 444 fueron:



18.5. Convocatoria Peritos.

Este servicio se encuentra balanceado en el FortiADC:

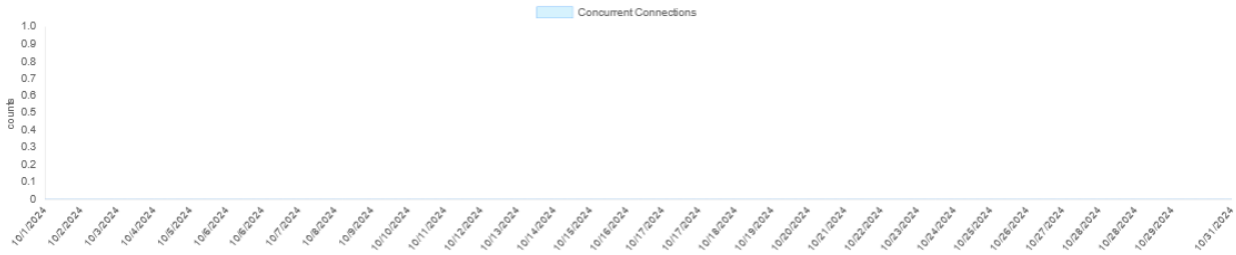
Durante octubre, no se observan sesiones concurrentes de esta aplicación:



18.6. SIERJU

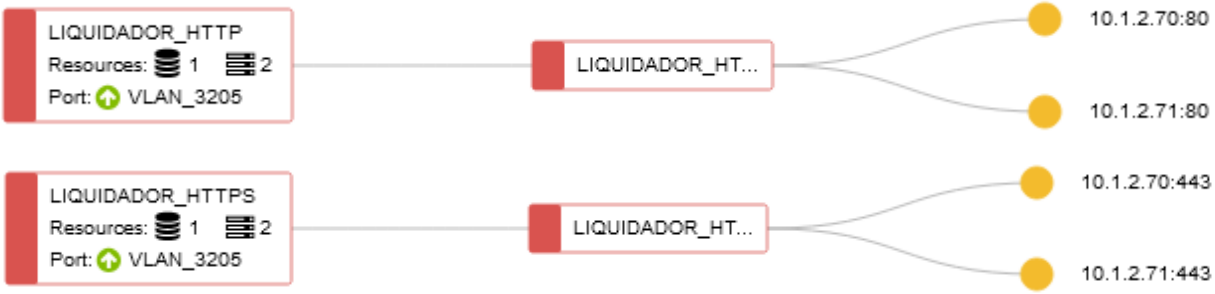
La configuración de balanceo para esta aplicación en el balanceador FortiADC es:

Durante octubre no se observan conexiones concurrentes para este aplicativo:

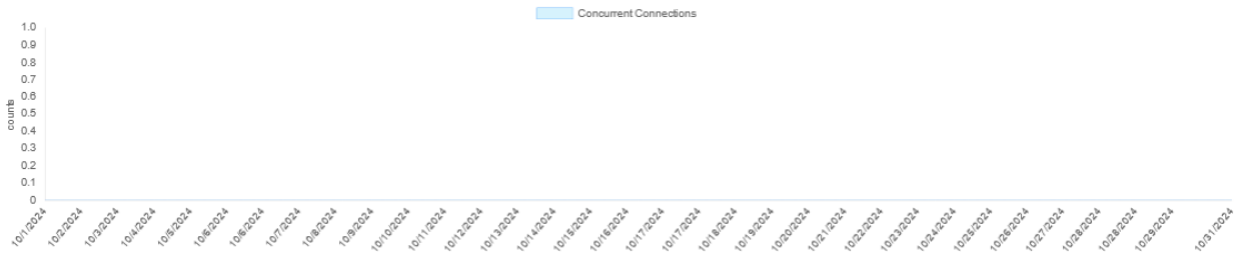


18.7. Liquidador de Sentencias

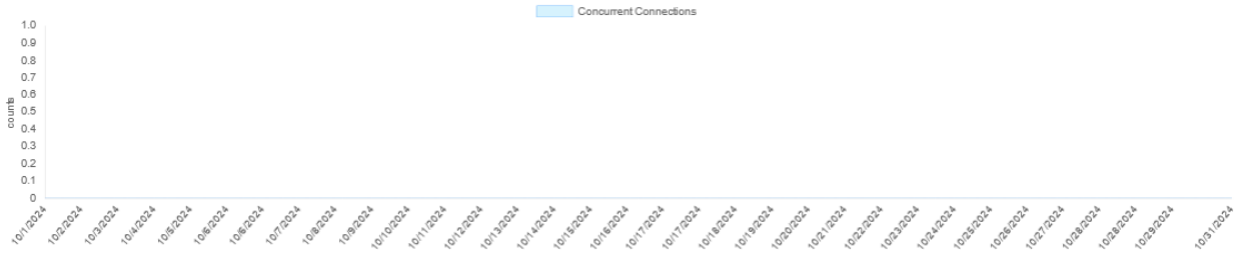
Virtual server Liquidador de Sentencias balanceador FortiADC



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



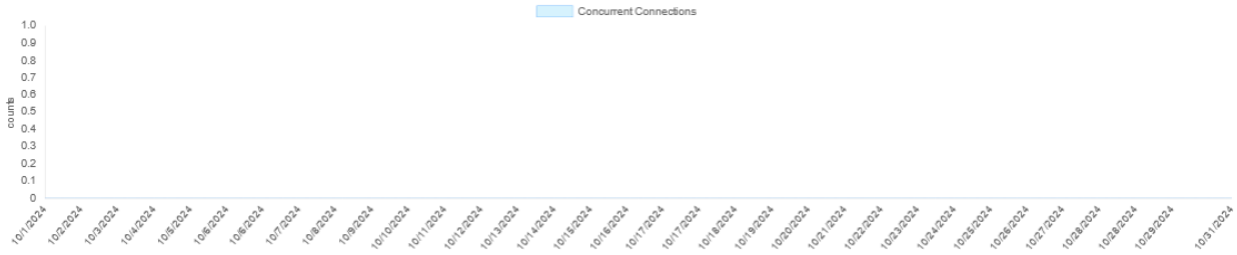
Las sesiones concurrentes por HTTPS fueron:



18.8. Consulta Jurisprudencia

Virtual server Consulta Jurisprudencia se encuentra en el balanceador FortiADC.

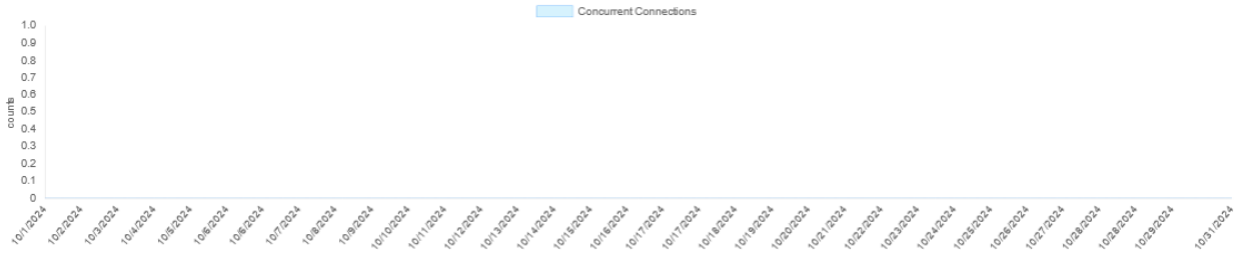
Durante octubre no se observan conexiones concurrentes para este aplicativo:



18.9. API Gestión de Audiencias

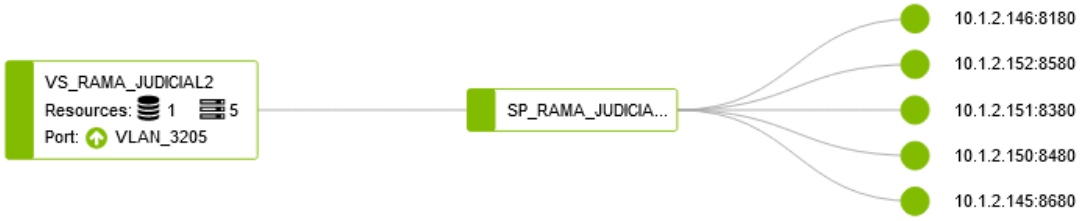
Virtual server API Gestión de Audiencias balanceador FortiADC.

Las sesiones concurrentes por HTTPS para este aplicativo:

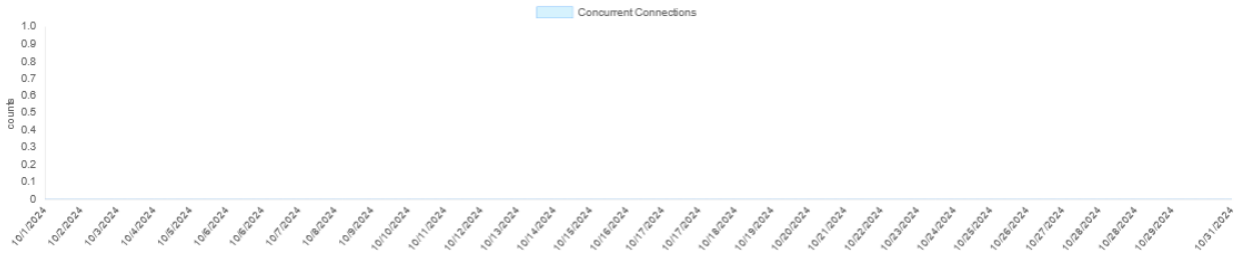


18.10. Portal Alterno de la Rama Judicial

Se encuentran balanceado en el FortiADC:

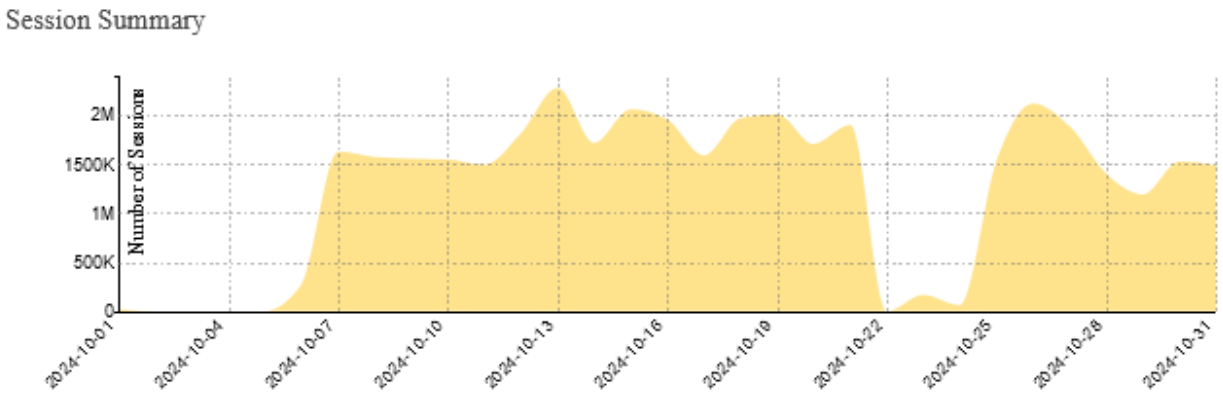


Durante octubre no se observan conexiones concurrentes para este aplicativo:



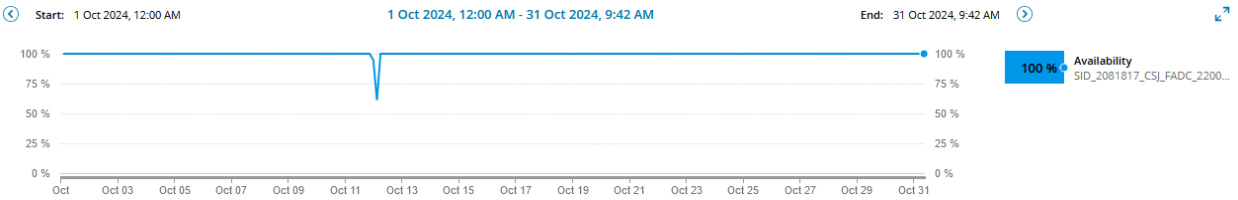
18.11. Portal de la Rama Judicial

Las sesiones Historico_Portal Rama Judicial fueron:



18.12. Disponibilidad y performance.

El evento del 12 de octubre corresponde a la migración del SW core en el datacenter Torre Central autorizada por el cliente CSJ.

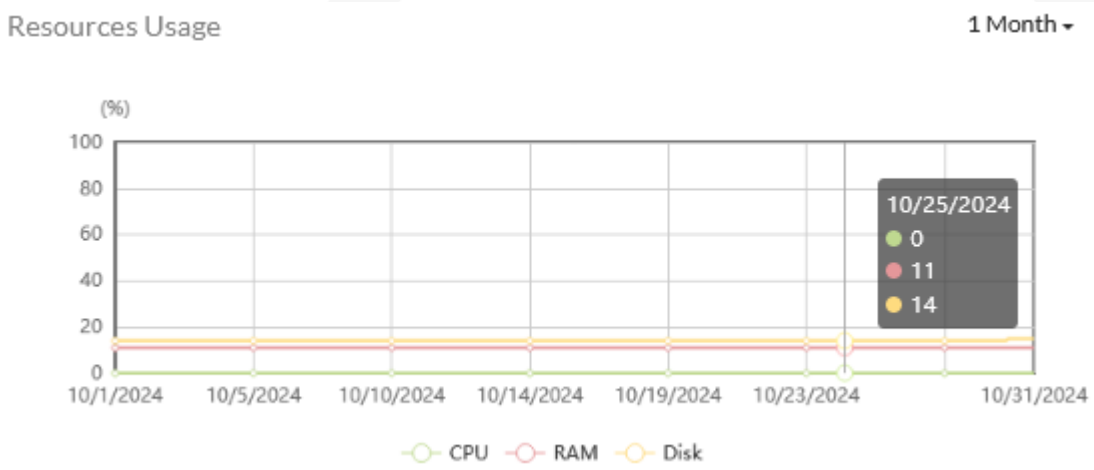


La disponibilidad durante octubre fue de 99,817%:

Availability Statistics

PERIOD	AVAILABILITY
Today	100,000 %
Yesterday	100,000 %
Last 7 Days	100,000 %
Last 30 Days	99,817 %

Durante octubre se observa consumo de CPU del 0%, memoria 11% y disco 14%:



19. 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:

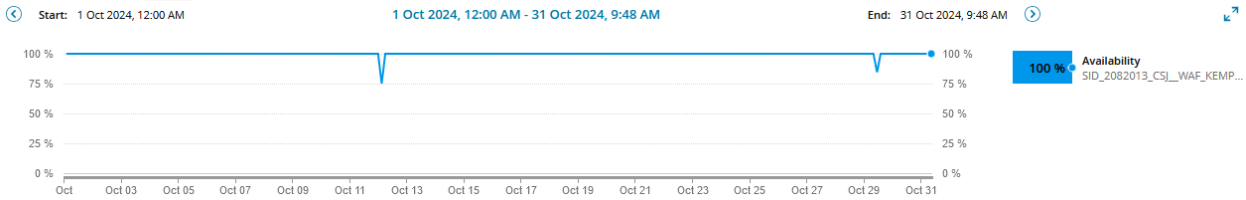
Item	Solución WAF	Cantidad de políticas de servidores
1	WAF TORRE CENTRAL	162
2	WAF CAN	74

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

19.1. Web application firewall datacenter principal IFX.

El evento del 12 de octubre corresponde a la migración del SW core en el datacenter Torre Central autorizada por el cliente CSJ.

El evento del 29 de octubre corresponde a Problemas de acceso VPN y caída de páginas WEB surf.cndj.gov.co por inconvenientes de canales Cirion.



Durante octubre la disponibilidad del WAF Torre central fue de 99.823%

Availability Statistics

PERIOD	AVAILABILITY
Today	100,000 %
Yesterday	100,000 %
Last 7 Days	99,728 %
Last 30 Days	99,823 %

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

La aplicación web más consultada durante octubre fue publicacionesprocesales.ramajudicial.gov.co (172.17.201.100:443) con 9137463 sesiones web correspondiente al 44,10%

#	Política	Virtual IP Address	Total Conns	% del total
1	publicacionesprocesales.ramajudicial.gov.co - 190.217.24.175	172.17.201.100:443	9137463	44,10%
2	nuevoportal.ramajudicial.gov.co Y cndj.gov.co 190.217.24.176	172.17.201.101:443	5699166	27,50%
3	siicor.corteconstitucional.gov.co - 190.217.24.62	172.17.201.13:443	2214837	10,69%
4	consejodeestado.gov.co - 190.217.24.60	172.17.201.52:443	1178569	5,69%
5	apigestionaudiencias1.ramajudicial.gov.co	172.17.201.42:443	474183	2,29%
6	sirna.ramajudicial.gov.co	172.17.201.28:443	365004	1,76%
7	sistemaaudiencias.ramajudicial.gov.co	172.17.201.44:443	294043	1,42%
8	consultajurisprudencial.ramajudicial.gov.co 8080	172.17.201.110:8080	274418	1,32%
9	seccionalescsj.ramajudicial.gov.co-intrajud.ramajudicial.gov.co	172.17.201.8:443	123158	0,59%
10	videoteca.ramajudicial.gov.co Holocausto_lector_videoteca_sidn_443	172.17.201.54:443	117296	0,57%
	Otros		**843869**	4,07%
	Total		**20722006**	100,00%

19.3. Top de peticiones por país WAF principal IFX.

Durante octubre, el país desde donde se recibieron más peticiones de conexión fue Colombia, Private hace referencia a las consultas que provienen desde la red corporativa del CSJ:

Top 10 Countries

Total

Country	Requests	Blocked
Private	2815815	746183
Colombia	7483992	453134
United States	2264572	109767
IPrep	22019	22019
Argentina	112621	9527
Poland	9866	8522
Brazil	48456	3667
Costa Rica	22220	2339
Singapore	7591	1905
Panama	23351	1887

19.4. Top de ataques por política WAF principal IFX.

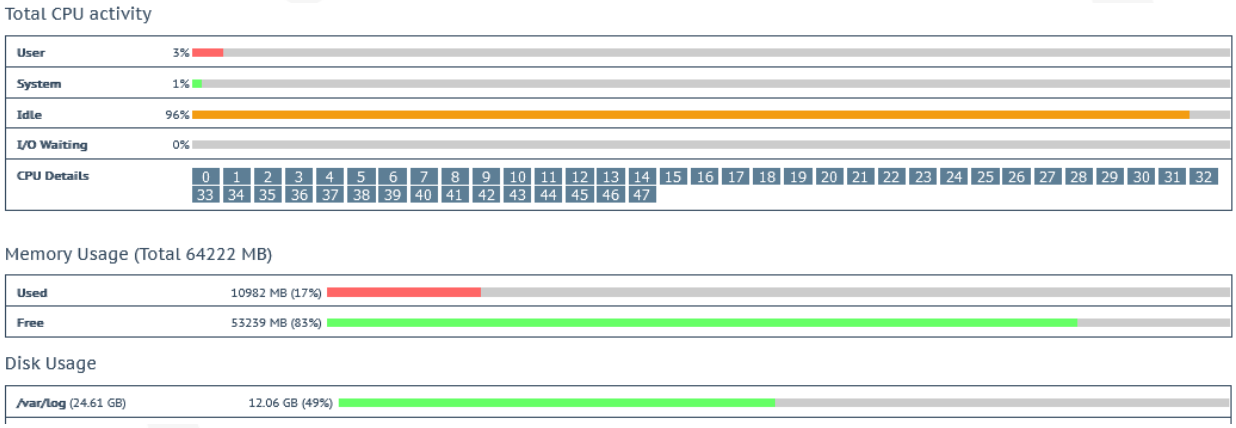
La siguiente tabla muestra el top 10 de las reglas o virtual services que proporcionaron mayor protección contra ataques a las aplicaciones web durante octubre. Sobre la aplicación *publicacionesprocesales.ramajudicial.gov.co* han sido prevenidas la mayor cantidad de ataques durante el mes:

#	Política	Virtual IP Address	Total Events	% del total
1	publicacionesprocesales.ramajudicial.gov.co - 190.217.24.175	172.17.201.100:443	1241074	90,16%
2	nuevoportal.ramajudicial.gov.co Y cndj.gov.co 190.217.24.176	172.17.201.101:443	122541	8,90%
3	siicor.corteconstitucional.gov.co - 190.217.24.62	172.17.201.13:443	2036	0,15%
4	consejodeestado.gov.co - 190.217.24.60	172.17.201.52:443	1916	0,14%
5	iedoc.consejodeestado.gov.co 448	172.17.201.60:448	1228	0,09%
6	videoteca.ramajudicial.gov.co Holocausto_lector_videoteca_sidn_443	172.17.201.54:443	853	0,06%
7	sistemaaudiencias.ramajudicial.gov.co	172.17.201.44:443	396	0,03%

8	peygi.ramajudicial.gov.co_TT918287	172.17.201.223:443	384	0,03%
9	antecedentesdisciplinarios.cndj.gov.co	172.17.201.31:443	352	0,03%
#	SIRTIWEB - 190.217.24.52	172.17.201.19:80	339	0,02%
	Otros		**5352**	0,39%
	Total		**1376471**	100,00 %

19.5. Consumo de recursos WAF principal IFX.

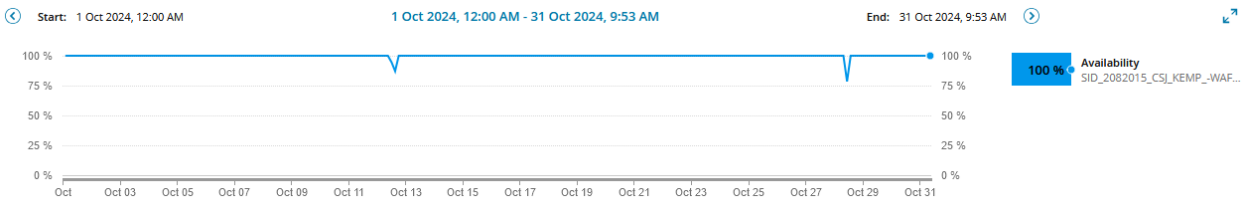
El WAF KEMP de Torre Central presentó consumo de CPU del 3%, memoria de 17% y disco en un 49%:



20. TRÁFICO DE WEB APPLICATION FIREWALL (WAF) CAN

20.1. Disponibilidad WAF CAN.

El evento del 12 de octubre corresponde a la migración del SW core en el datacenter Torre Central autorizada por el cliente CSJ.
El evento del 29 de octubre corresponde a Problemas de acceso VPN y caída de páginas WEB surf.cndj.gov.co por inconvenientes de canales Cirion.



Durante octubre la disponibilidad del WAF CAN fue de 99,828%:

Availability Statistics

PERIOD	AVAILABILITY
Today	100,000 %
Yesterday	100,000 %
Last 7 Days	99,619 %
Last 30 Days	99,828 %

20.2. Uso de políticas de servidores WAF CAN.

La aplicación más consultada durante octubre fue cortesuprema.gov.co_Palacio con un 72,08% del total:

#	Política	Virtual IP Address	Total Conns	% del total
1	cortesuprema.gov.co_Palacio	172.17.202.239:443	1530591	72,08%
2	tesauro.ramajudicial.gov.co[1]	172.17.202.110:8888	198426	9,35%
3	sso.cortesuprema.gov.co	172.17.202.141:443	101026	4,76%
4	linkce.consejodeestado.gov.co	172.17.202.42:443	40777	1,92%
5	samairj.consejodeestado.gov.co	172.17.202.38:443	34354	1,62%
6	restituciontierras.ramajudicial.gov.co	172.17.202.37:443	34144	1,61%
7	cortesuprema_Palacio Redirect	172.17.202.239:80	32767	1,54%

8	sso.cortesuprema.gov.co Redirect	172.17.202.141:80	20382	0,96%
9	capacitacion.ramajudicial.gov.co 443	172.17.202.13:443	14730	0,69%
#	serviciopdf.ramajudicial.gov.co	172.17.202.7:443	14352	0,68%
	Otros		**101766**	4,79%
	Total		**2123315**	100,00 %

20.3. 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	581805	1968
IPrep	1469	1469
Singapore	9286	710
China	1910	455
Private	212287	367
Germany	24937	117
Bulgaria	7551	89
Brazil	4274	67
Indonesia	777	49
Malaysia	110	41

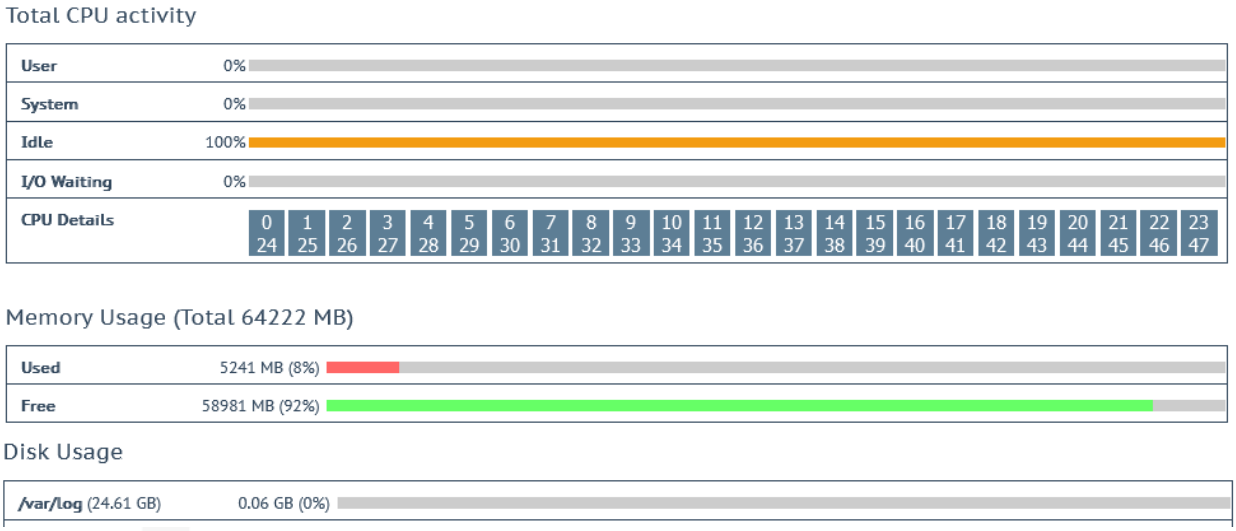
20.4. Top de ataques por política WAF CAN.

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

#	Política	Virtual IP Address	Total Events	% del total
1	tesauro.ramajudicial.gov.co[1]	172.17.202.110:8888	1561	28,27%
2	cortesuprema.gov.co_Palacio	172.17.202.239:443	1092	19,78%
3	sivoto.ramajudicial.gov.co-SiVotoWeb	172.17.202.44:443	421	7,62%
4	www.siedp.cndj.gov.co 443	172.17.202.15:443	319	5,78%
5	predesarchive.ramajudicial.gov.co	172.17.202.53:443	278	5,03%
6	convocatorias.consejodeestado.gov.co	172.17.202.147:443	250	4,53%
7	serviciopdf.ramajudicial.gov.co	172.17.202.7:443	244	4,42%
8	siapoas.ramajudicial.gov.co	172.17.202.43:443	226	4,09%
9	samairj.consejodeestado.gov.co	172.17.202.38:443	213	3,86%
10	efinominapruebas.ramajudicial.gov.co	172.17.202.45:443	172	3,11%
	Otros		**746**	13,51%
	Total		**5522**	100,00 %

20.5. Consumo de recursos WAF CAN.

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



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

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

Otros certificados digitales presentan las siguientes vigencias:

Identifier	Common Name(s)
ComisionNacional_2024	*.cndj.gov.co [Expires: Jan 24 23:59:59 2025 GMT]
Corteconstitucional2024_2025	*.corteconstitucional.gov.co [Expires: Oct 2 23:59:59 2025 GMT]
consejodeestado_ULTIMO	*.consejodeestado.gov.co [Expires: Oct 7 23:59:59 2025 GMT]
cortesuprema.gov.co_2024_2025	*.cortesuprema.gov.co [Expires: Oct 1 23:59:59 2025 GMT]

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

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

20.7. Intentos login fallidos a Firewalls

Durante octubre se presentaron los siguientes intentos de ingreso administrativo hacia los firewall perimetrales. El acceso administrativo se encuentra protegido controles de "Restrict login to trusted hosts",

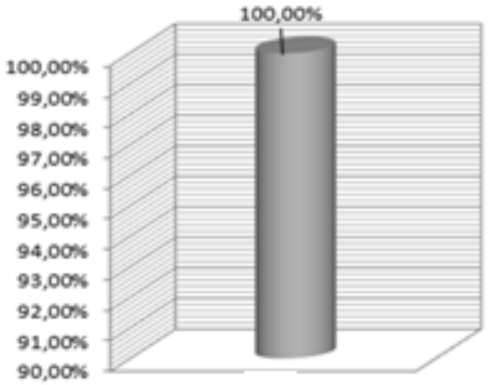
#	Login Source	User Name	Total Number of Failed Logins
1	https(172.16.54.215)	victor.galvis	22
2	ssh(185.11.61.88)	admin	19
3	ssh(62.122.184.252)	admin	18
4	https(190.60.96.34)	victor.galvis	14
5	ssh(185.11.61.88)	root	13
6	ssh(62.122.184.252)	root	9
7	ssh(185.11.61.88)	test	4
8	ssh(62.122.184.252)	test	3
9	ssh(185.11.61.88)	ftpuser	3
10	ssh(185.11.61.88)	ubnt	2

21. DISPONIBILIDAD SEGURIDAD GLOBAL DEL MES DE OCTUBRE

La disponibilidad del servicio de IFX durante el mes de octubre fue del 100%

DISPONIBILIDAD GLOBAL	NUMERO DE TICKETS POR IMPUTABILIDAD	
	RESPONSABILIDAD IFX (NUMERO TICKETS)	RESPONSABILIDAD CLIENTE (NUMERO TICKETS)
100.00%	0	1

MES	DISPONIBILIDAD (%)
OCTUBRE	100%



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

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

9. CONSUMO MOTORES BASES DE DATOS

A continuación, se desglosas los motores bases de datos contratados bajo acuerdo marco:

- CPU
- Memoria RAM
- Disco

(Remitirse al documento "**Anexo consumo motores base de datos**" para ver el detalle)

10. GESTIÓN FINANCIERA

19.1 Tabla información Gestión financiera

Fecha de inicio	5-feb-24
Fecha de finalización	4-dic-24
Valor inicial	$ 15.516.011.530,00
Plazo	10 meses
Items de la Orden de Compra	49 lineas - SID
AMP	Nube Privada IV - CEE-308-AMP-2022- # Proceso CCENEG-061-1-2022
Valor facturado a la fecha	$ 12.011.345.192,02
% Valor facturado	77,41%
Valor pagado a la fecha	$ 10.473.475.679,02
% Valor pagado	67,50%

19.2 Tabla Facturación

FACTURA	FECHA EMISIÓN	VALOR (IVA incluido)	PERIODO FACTURADO	FECHA DE PAGO	ESTADO
IFXC-402862	miércoles, 3 de abril de 2024	$ 1.318.151.327,59	05 al 29 de Febrero 2024	jueves, 18 de abril de 2024	Pagada
IFXC-403030	viernes, 19 de abril de 2024	$ 1.530.871.522,52	01 al 31 de Marzo 2024	lunes, 6 de mayo de 2024	Pagada
IFXC-405204	martes, 28 de mayo de 2024	$ 1.510.877.833,00	01 al 30 de Abril 2024	miércoles, 5 de junio de 2024	Pagada
IFXC-407246	martes, 18 de junio de 2024	$ 1.520.031.300,36	01 al 31 de Mayo 2024	jueves, 27 de junio de 2024	Pagada
IFXC-409336	martes, 16 de julio de 2024	$ 1.527.092.873,00	01 al 30 de Junio 2024	lunes, 29 de julio de 2024	Pagada
IFXC - 411473	viernes, 16 de agosto de 2024	$ 1.529.127.888,86	01 al 31 de Julio 2024	viernes, 20 de septiembre de 2024	Pagada
IFXC-413631	lunes, 16 de septiembre de 2024	$ 1.537.322.933,70	01 al 30 de Agosto 2024	martes, 1 de octubre de 2024	Pagada
IFXC-415782	miércoles, 16 de octubre de 2024	$ 1.537.869.513,00	01 al 30 de Septiembre 2024		Pendiente

19.3 Tabla ANS

ANS (sin IVA incluido)	
05 al 29 de Febrero 2024	No se generaron ANS durante el periodo
01 al 31 de Marzo 2024	$ 6.034.935,00
01 al 30 de Abril 2024	$ 9.379.680,00
01 al 31 de Mayo 2024	No se generaron ANS durante el periodo
01 al 30 de Junio 2024	$ 1.703.940,00
01 al 31 de Julio 2024	No se generaron ANS durante el periodo
Descuento SID 2081861 "Disponibilidad del servicio en instalaciones DC" - 05 de Febrero 2024 al 31 de julio de 2024	$ 469.024,14

01 al 30 de Agosto 2024	No se generaron ANS durante el periodo
01 al 30 de Septiembre2024	No se generaron ANS durante el periodo
Total ANS	**$ 17.587.579,14**

11. 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.