INFORME DE GESTIÓN MENSUAL

RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA

OC147451- CCE

JULIO 2025

ifx Networks | CARE Centro de Atención Regional

1 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 147451.
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: 01 de julio 2025 Fecha de final: 31 de julio 2025
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. Infraestructura

Linea OC	SID Anterior	SID Nuevo	Articulo	EQUIPO	SERIAL	DIRECCIÓN
1	2081796	2498144	Alojamiento de infraestructura - Housing - Cross Conexión - Oro - Puntos de red: 4 - Capacidad de energía: 1 KVA - Capacidad en unidades: 4 U - Rack/M - Cantidad: 10			DATA CENTER PRINCIPAL IFX
1	2081797	2498145	Alojamiento de infraestructura - Housing - Cross Conexión - Oro - Puntos de red: 4 - Capacidad de energía: 1 KVA - Capacidad en unidades: 4 U - Rack/M - Cantidad: 10			DATA CENTER PRINCIPAL IFX
1	2081798	2498146	Alojamiento de infraestructura - Housing - Cross Conexión - Oro - Puntos de red: 4 - Capacidad de energía: 1 KVA - Capacidad en unidades: 4 U - Rack/M - Cantidad: 10			DATA CENTER PRINCIPAL IFX
1	2081799	2498147	Alojamiento de infraestructura - Housing - Cross Conexión - Oro - Puntos de red: 4 - Capacidad de energía: 1 KVA - Capacidad en unidades: 4 U - Rack/M - Cantidad: 10			DATA CENTER PRINCIPAL IFX
1	2081800	2498148	Alojamiento de infraestructura - Housing - Cross Conexión - Oro - Puntos de red: 4 - Capacidad de energía: 1 KVA - Capacidad en unidades: 4 U - Rack/M - Cantidad: 10			DATA CENTER PRINCIPAL IFX
1	2081801	2498149	Alojamiento de infraestructura - Housing - Cross Conexión - Oro - Puntos de red: 4 - Capacidad de energía: 1 KVA - Capacidad en unidades: 4 U - Rack/M - Cantidad: 10			DATA CENTER PRINCIPAL IFX
1	2081802	2498150	Alojamiento de infraestructura - Housing - Cross Conexión - Oro - Puntos de red: 4 - Capacidad de energía: 1 KVA - Capacidad en unidades: 4 U - Rack/M - Cantidad: 10			DATA CENTER PRINCIPAL IFX
1	2081803	2498151	Alojamiento de infraestructura - Housing - Cross Conexión - Oro - Puntos de red: 4 - Capacidad de energía: 1 KVA - Capacidad en unidades: 4 U - Rack/M - Cantidad: 10			DATA CENTER PRINCIPAL IFX
1	2383100	2498152	Alojamiento de infraestructura - Housing - Cross Conexión - Oro - Puntos de red: 4 - Capacidad de energía: 1 KVA - Capacidad en unidades: 4 U - Rack/M - Cantidad: 10			DATA CENTER PRINCIPAL IFX
1	2383101	2498153	Alojamiento de infraestructura - Housing - Cross Conexión - Oro - Puntos de red: 4 - Capacidad de energía: 1 KVA -			DATA CENTER

			Capacidad en unidades: 4 U - Rack/M - Cantidad: 10			PRINCIPAL IFX
2	2081804	2498154	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			DATA CENTER PRINCIPAL IFX
2	2081805	2498155	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			DATA CENTER PRINCIPAL IFX
10	2082020	2498162	IaaS Seguridad - Appliance Anti Ddos - Alta Capacidad - Oro - Hosting físico - Rol de Inspección - 28 Gbps - Paquetes Por Segundo (MPPS) - 25000000 - Mes - Cantidad: 2	DDOS	FI-2KETB20000015	DATA CENTER PRINCIPAL IFX
10	2082021	2498163	IaaS Seguridad - Appliance Anti Ddos - Alta Capacidad - Oro - Hosting físico - Rol de Inspección - 28 Gbps - Paquetes Por Segundo (MPPS) - 25000000 - Mes - Cantidad: 2	DDOS	FI-2KE5819000049	DATA CENTER PRINCIPAL IFX
11	2082018	2498164	IaaS Seguridad - Firewall Nueva Generación - Alta Capacidad - Oro - Hosting físico - Rol de Firewall - 500 Gbps - Sesiones Concurrentes - 100000000 - Mes - Cantidad: 2	FIREWALL FORTI 4400F	FG440FTK21900184	DATA CENTER PRINCIPAL IFX
11	2082019	2498165	IaaS Seguridad - Firewall Nueva Generación - Alta Capacidad - Oro - Hosting físico - Rol de Firewall - 500 Gbps - Sesiones Concurrentes - 100000000 - Mes - Cantidad: 2	FIREWALL FORTI 4400F	FG440FTK21900183	DATA CENTER PRINCIPAL IFX
12	2082016	2498166	IaaS Seguridad - Firewall Nueva Generación - Media Capacidad - Oro - Hosting físico - Rol de Firewall - 40 Gbps - Sesiones Concurrentes - 15000000 - Mes - Cantidad: 2	FIREWALL FORTI 900G	FG9H0GTB23900440	PALACIO
12	2082017	2498167	IaaS Seguridad - Firewall Nueva Generación - Media Capacidad - Oro - Hosting físico - Rol de Firewall - 40 Gbps - Sesiones Concurrentes - 15000000 - Mes - Cantidad: 2	FIREWALL FORTI 900G	FG9H0GTB23900205	PALACIO
13	2082013	2498168	IaaS Seguridad - Web Aplication Firewall - Alta Capacidad - Oro - Hosting físico - Desempeño WAF (Gbps) - 10 - Mes - Cantidad: 2	KEMP LM-X25	TSCC82005608	DATA CENTER PRINCIPAL IFX
13	2082014	2498169	IaaS Seguridad - Web Aplication Firewall - Alta Capacidad - Oro - Hosting físico - Desempeño WAF (Gbps) - 10 - Mes - Cantidad: 2	KEMP LM-X25	TSCB72000545	DATA CENTER PRINCIPAL IFX

2. *IaaS almacenamiento- Almacenamiento SAN Alto Rendimiento*

OC	SID Anterior	SID Nuevo	ARTICULO	GB
3	2350068	2254344	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: 3650000	3650000
4	2081812	2498156	IaaS almacenamiento - Crecimiento capacidad de almacenamiento - Oro - Alta - Nube Privada - Capacidad : 100GB - GB/Mes - Cantidad: 150000	150000
TOTAL ALMACENAMIENTO CONTRATADO DE ALTO RENDIMIENTO				**3800000**

El almacenamiento total aprovisionado en la infraestructura contratada, de conformidad con las solicitudes de la Entidad, a corte 31 de Julio de 2025 es de: **4068576 (GB)**

Total, contratado de Almacenamiento SAN alto rendimiento: **3800000(GB)**

NOTA: La entidad y el contratista se encuentran en verificación, dado que unidades de IFX se están usando para recuperación de la información y otras no están en uso por parte de la entidad y se ejecutará depuración para llegar a los limites contratados, bajo la OC 147451.

(Remitirse al anexo "**Inventario de servicios OC147451_ Julio**" para ver el detalle)

3 IaaS almacenamiento - Backup de Datos – Alta

3.1 Backup de Datos OC-147451

OC	SID Anterior	SID Nuevo	ARTICULO
5	2081813	2498158	IaaS almacenamiento - Backup de Datos - Alta - Capacidad: 100TB a <200TB - Almacenamiento SAN - Diaria - GB/Mes - Cantidad: 150000
6	2362326	2498157	IaaS almacenamiento - Backup de Datos - Alta - Capacidad: 100TB a <200TB - Almacenamiento SAN - Mensual - GB/Mes - Cantidad: 200000
7	2081814	2498159	IaaS almacenamiento - Backup de Datos - Alta - Capacidad: 50TB a <100TB - Disco Duro Externo - Diaria - GB/Mes - Cantidad: 100000
			450000 GB

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 Julio, está utilizando, una capacidad de **450,000 GB**en almacenamiento físico total, pero la entidad actualmente tiene contratado, elsiguiente almacenamiento en sus órdenes de compra y se desglosa de la siguiente manera:

- Para los Backups Diarios la entidad tiene contratado un espacio de Almacenamiento en SAN mensual de: 150.000 GB, donde se almacenan 30 puntos de retención diarios.

- A la fecha la entidad, está consumiendo 146.600 GB de almacenamiento de BK diario, los cuales se sacan de la sumatoria de la columna "CAPACIDAD" menos "ESPACIO", de la tabla "DIARIOS OC 147451".

- 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.

- Para los Backups Mensuales la entidad tiene contratado un espacio de Almacenamiento físico en SAN mensual de: 250.000 GB, donde se almacenan 6 puntos de retención mensuales.

- A la fecha la entidad, está consumiendo 247.700 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 NAS OC 147451".

- 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 Backups Mensuales la entidad tiene contratado un espacio de Almacenamiento físico en NAS mensual de: 100.000 GB, donde se almacenan 3 puntos de retención mensuales.

- A la fecha la entidad, está consumiendo 244.700 GB de almacenamiento de BK Mensual en NAS, los cuales se sacan de la sumatoria de la columna "CAPACIDAD" menos "ESPACIO LIBRE", de la tabla "MENSUALES OC 147451"

- Acorde a la información suministrada con anterioridad y realizando la resta entre lo consumido, menos el almacenamiento contratado la entidad supera el almacenamiento BK MENSUAL NAS en 144.700 GB

Los backups se ejecutan de la siguiente manera:

Diarios: De domingo a viernes 20:00pm
Mensuales: Último domingo de cada mes 22:00pm

DIARIOS OC 147451			
REPOSITORIO	CAPACIDAD (TB)	ESPACIO LIBRE (TB)	ESPACIO USADO (TB)
UNIDAD 1	75,5	3,1	309,4
UNIDAD 2	75,5	1,3	163,7
SUMATORIAS	151	4,4	473,1
ESPACIO CONSUMIDO DIARIO			146,6
DIFERENCIA DE LO CONTRATADO			4,4

MENSUALES OC 147451			
REPOSITORIO	CAPACIDAD (TB)	ESPACIO LIBRE (TB)	ESPACIO USADO (TB)
UNIDAD 1	100	1,2	120,1
UNIDAD 2	100	1	98,3
SUMATORIAS	200	2,2	218,4
ESPACIO CONSUMIDO MENSUAL			197,8
DIFERENCIA DE LO CONTRATADO			2,2

MENSUAL BACKUP NAS OC 124016			
REPOSITORIO	CAPACIDAD (TB)	ESPACIO LIBRE (TB)	ESPACIO USADO (TB)
NAS	250	5,3	203,9
ESPACIO CONSUMIDO			244,7
DIFERENCIA DE LO CONTRATADO			-144,7

ESPACIO CONSUMIDO TOTAL	451
DIFERENCIA TOTAL VS LO CONTRATADO	-138,1

3.2 Backup de Datos OC_124016

NOTA: Se mantienen los almacenamientos de la orden de compra anterior de la siguiente manera: de Almacenamiento BK de datos diario y semanal: 350.000 GB y Almacenamiento de Backup Mensual: 430.000 GB, que del espacio de Almacenamiento físico en SAN con retención de 6 meses que se utilizan de los ítems de producción: (Item 7) de los cuales 180.000 GB + corresponden al Item 51 250.000. - Orden de compra anterior, se mantiene el espacio hasta cumplir retención de los backups Mensuales.

DIARIOS-SEMANALES OC 124016			
REPOSITORIO	**CAPACIDAD (TB)**	**ESPACIO LIBRE (TB)**	**ESPACIO USADO (TB)**
UNIDAD 1	80	7.2	321.4
UNIDAD 2	80	8.1	175.7
UNIDAD 3	78	4.4	181.3
UNIDAD 4	110	4.6	349.6
SUMATORIAS	348	24.3	1028
ESPACIO CONSUMIDO DIARIO - SEMANAL			323.7
DIFERENCIA DE LO CONTRATADO			26.3

MENSUALES SAN - OC 100980			
REPOSITORIO	**CAPACIDAD (TB)**	**ESPACIO LIBRE (TB)**	**ESPACIO USADO (TB)**
UNIDAD 1	130	1.3	128.1
UNIDAD 2	150	8.7	135.3
UNIDAD 3	150	5.9	138.1
SUMATORIAS	430	15.9	401.5
ESPACIO CONSUMIDO MENSUAL			414.1
DIFERENCIA DE LO CONTRATADO			15.9

NOTA: Estamos a la espera de la confirmación de depuración de espacio de las máquinas que no requieren backups para poder ejecutar los backups mensuales.

(Remitirse al anexo "**Inventario_Servicios_CSJ_JULIO 2025.xls**" para ver el detalle)

4 Iaas almacenamiento – Replicación Local de Datos

Linea OC	SID Anterior	SID Nuevo	Articulo
9	2081816	2498161	IaaS almacenamiento - Replicación Local de Datos - Oro - Alta - Nube Privada - Capacidad: 900TB a <1000TB - 10 Gbps - Restauración: 10TB / hora - GB/Mes - Cantidad: 3750000

La replicación total usada, de conformidad con las solicitudes de la Entidad, a corte 31 de Julio 2025 es de: **2549792,35 (GB)**

Unidad	Fecha	Cantidad de archivos registrados	Diferencia entre cantidad de archivos registrados	Cantidad de archivos	total capacidad GB	% de uso	Espacio usado en GB
botrpa22	2025-07-14	60930	937618	998548	204799	63	129023,37
botrpa08	2025-07-16	132	1567353	1567485	189439	89	168600,71
botrpa03	2025-07-16	1	374211	374212	81919	68	55704,92
botrpa02	2025-07-16	0	2118049	2118049	240639	96	231013,44
botrpa11	2025-07-16	0	867566	867566	127999	95	121599,05
botrpa00	2025-07-16	0	1205697	1205697	182271	95	173157,45
botrpa05	2025-07-16	0	520843	520843	51199	94	48127,06
botrpa09	2025-07-16	0	921151	921151	122879	94	115506,26
botrpa21	2025-07-16	0	1034478	1034478	153599	94	144383,06
botrpa10	2025-07-16	0	784227	784227	112639	92	103627,88
botrpa07	2025-07-16	0	1057408	1057408	146431	92	134716,52
botrpa18	2025-07-16	0	863209	863209	112639	92	103627,88
botrpa19	2025-07-16	0	652451	652451	112639	92	103627,88
botrpa12	2025-07-16	0	998955	998955	112639	91	102501,49
botrpa06	2025-07-16	0	766449	766449	97279	91	88523,89
botrpa17	2025-07-16	0	842793	842793	102399	88	90111,12
botrpa13	2025-07-16	0	1144764	1144764	143359	87	124722,33
botrpa14	2025-07-16	0	1346542	1346542	153599	87	133631,13
botrpa15	2025-07-16	0	905745	905745	143359	82	117554,38
botrpa04	2025-07-16	0	353180	353180	133119	80	106495,2
botrpa16	2025-07-16	0	1172023	1172023	153599	69	105983,31
botrpa20	2025-07-16	0	318084	318084	88063	54	47554,02
				TOTAL	**2966506**		**2549792,35**

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 máquinas alternas.

En anexo "**Inventario de servicios OC147451_ Julio**" se encontrarán más detalles de las ejecuciones mencionadas.

5 Servicios por aplicación_ Servidores

A continuación, se resumen las principales actividades en la provisión de los servicios y aplicaciones para Consejo Superior de la Judicatura:

Item OC	2025 SID OC147451	Grupos _APP
14	2498189	Agendamiento y Portal Grabaciones
15	2498187	Libre
15	2498188	Libre
16	2498186	Agendamiento y Portal Grabaciones
17	2498182	Agendamiento y Portal Grabaciones
17	2498184	Almacenamiento (BOTRPA)
17	2498185	Almacenamiento (BOTRPA)
17	2498183	Almacenamiento (BOTRPA)
18	2498181	Almacenamiento (BOTRPA)
19	2498180	Gestión de Grabaciones
20	2498179	Almacenamiento (BOTRPA)
21	2498178	Libre
22	2498206	Catalogación
22	2498207	Catalogación
22	2498208	Catalogación
22	2498172	Catalogación
22	2498173	Catalogación
22	2498174	Gestión de Grabaciones
22	2498175	Catalogación
22	2498176	Catalogación
22	2498177	Catalogación
22	2498201	Catalogación
22	2498202	Catalogación
22	2498203	Catalogación

22	2498204	Catalogación
22	2498205	Catalogación
22	2498170	Gestión de Grabaciones
22	2498171	Almacenamiento (BOTRPA)
23	2498214	Disponible/apagada
23	2498213	Almacenamiento (BOTRPA)
23	2498215	Libre
24	2498212	Gestión de Grabaciones
25	2498210	Catalogación
25	2498211	Catalogación
26	2498191	Agendamiento y Portal Grabaciones (Base de datos)
26	2498190	Libre
27	2498197	Agendamiento y Portal Grabaciones
27	2498195	Almacenamiento (BOTRPA)
27	2498196	Almacenamiento (BOTRPA)
28	2498198	Agendamiento y Portal Grabaciones
28	2498199	Agendamiento y Portal Grabaciones
28	2498200	Agendamiento y Portal Grabaciones

(Remitirse al anexo "**Inventario de servicios OC147451_ Julio**" para ver el detalle "maquinas")

6 *Disponibilidad Servidor de Uso Básico*

6.1 Inventario gestión de grabaciones

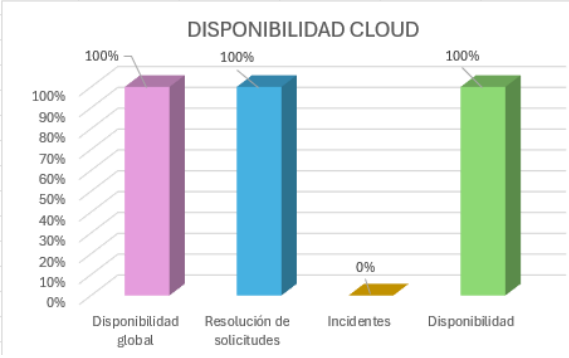
Item OC	2025 SID OC147451	Nombre de la máquina	Grupos _APP	LINEA BASE // CCE			APROVISIONADO		
				CPU	RAM	DISCO	CPU	RAM	DISCO
14	2498189	SO1HST-GGLOG03	Agendamiento y Portal Grabaciones	24	192	960	16	96	196
15	2498187	Libre 1	Libre	24	128	480	16	96	0
15	2498188	Libre 2	Libre	24	128	480	16	96	0
16	2498186	S01HST-GGLOG02	Agendamiento y Portal Grabaciones	16	96	480	16	96	195

17	2498182	S01HST-GGAPP04	Agendamiento y Portal Grabaciones	16	64	960	8	32	799
17	2498184	S01HST-GGCS03	Almacenamiento (BOTRPA)	16	64	960	16	64	312319
17	2498185	S01HST-GGCS02	Almacenamiento (BOTRPA)	16	96	960	16	64	468933
17	2498183	S01HST-GGCS04	Almacenamiento (BOTRPA)	16	96	960	16	64	883639
18	2498181	S01HST-GGCAPP06	Almacenamiento (BOTRPA)	16	32	960	16	32	433277
19	2498180	S01HST-GGBOTRP	Gestión de Grabaciones	16	32	480	16	32	11239
20	2498179	S01001-CS01	Almacenamiento (BOTRPA)	8	64	960	6	64	337495
21	2498178	Libre 3	Libre	8	32	960	0	0	0
22	2498206	S01HST-VWCATA13	Catalogación	8	16	480	8	16	479
22	2498207	S01HST-VWCATA14	Catalogación	8	16	480	8	16	479
22	2498208	S01HST-VWCATA15	Catalogación	8	16	480	8	16	479
22	2498172	S01HST-VWCATA02	Catalogación	8	16	480	8	16	479
22	2498173	S01HST-VWCATA03	Catalogación	8	16	480	8	16	479
22	2498174	S01HST-VWCATA04	Gestión de Grabaciones	8	16	480	8	16	479
22	2498175	S01HST-VWCATA05	Catalogación	8	16	480	8	16	479
22	2498176	S01HST-VWCATA06	Catalogación	8	16	480	8	16	479
22	2498177	S01HST-VWCATA07	Catalogación	8	16	480	8	16	479
22	2498201	S01HST-VWCATA08	Catalogación	8	16	480	8	16	479
22	2498202	S01HST-VWCATA09	Catalogación	8	16	480	8	16	479
22	2498203	S01HST-VWCATA10	Catalogación	8	16	480	8	16	479
22	2498204	S01HST-VWCATA11	Catalogación	8	16	480	8	16	479
22	2498205	S01HST-VWCATA12	Catalogación	8	16	480	8	16	479
22	2498170	S01HST-GGRBOT2	Gestión de Grabaciones	8	16	480	8	16	11619
22	2498171	S01HST-VWCATA01	Almacenamiento (BOTRPA)	8	16	480	8	16	256479
23	2498214	S01HST-GGPRULI	Disponible/apagada	4	32	480	4	16	448
23	2498213	S01HST-VMPRBOT	Almacenamiento (BOTRPA)	4	32	480	8	32	501215
23	2498215	Libre 5	Libre	4	32	480	0	0	0
24	2498212	S01HST-GGPRUBD	Gestión de Grabaciones	4	16	240	4	16	1319
25	2498210	CSJStream2	Catalogación	4	8	240	2	8	0
25	2498211	S01HST- SAMES01	Catalogación	4	8	240	4	8	289
26	2498191	CT-CTLOGPLUS-BDSERVER	Agendamiento y Portal Grabaciones (Base de datos)	24	256	960	24	256	2999
26	2498190	Libre 4	Libre	24	256	960	24	256	960
27	2498197	S01HST-GGAPP03	Agendamiento y Portal Grabaciones	16	96	960	8	32	1099
27	2498195	S01HST-GGCS06	Almacenamiento (BOTRPA)	16	96	960	8	32	371058
27	2498196	S01HST-GGCS07	Almacenamiento (BOTRPA)	16	96	960	8	32	463799
28	2498198	S01HST-GGAPP02	Agendamiento y Portal Grabaciones	16	96	960	8	32	1149
28	2498199	S01HST-GGAPP01	Agendamiento y Portal Grabaciones	16	96	960	8	32	1149

28	2498200	SO1HST-GGLOG01	Agendamiento y Portal Grabaciones	16	96	960	16	96	196

7.DISPONIBILIDAD GLOBAL CLOUD DEL MES DE JULIO

Disponibilidad Global mes de JULIO	Numero de tickets mes de JULIO	Imputabilidad por ANS
	68 solicitudes	**0 solicitudes**
	0 incidentes	**0 incidentes**
100%	Total 68 tickets	0 tickets



8 ESQUEMA DE SEGURIDAD

Linea OC	SID Anterior	SID Nuevo	Articulo	EQUIPO	SERIAL	DIRECCIÓN
10	2082020	2498162	IaaS Seguridad - Appliance Anti Ddos - Alta Capacidad - Oro - Hosting físico - Rol de Inspección - 28 Gbps - Paquetes Por Segundo (MPPS) - 25000000 - Mes - Cantidad: 2	DDOS	FI-2KETB20000015	DATA CENTER PRINCIPAL IFX
10	2082021	2498163	IaaS Seguridad - Appliance Anti Ddos - Alta Capacidad - Oro - Hosting físico - Rol de Inspección - 28 Gbps - Paquetes Por Segundo (MPPS) - 25000000 - Mes - Cantidad: 2	DDOS	FI-2KE5819000049	DATA CENTER PRINCIPAL IFX
11	2082018	2498164	IaaS Seguridad - Firewall Nueva Generación - Alta Capacidad - Oro - Hosting físico - Rol de Firewall - 500 Gbps - Sesiones Concurrentes - 100000000 - Mes - Cantidad: 2	FIREWALL FORTI 4400F	FG440FTK21900184	DATA CENTER PRINCIPAL IFX
11	2082019	2498165	IaaS Seguridad - Firewall Nueva Generación - Alta Capacidad - Oro - Hosting físico - Rol de Firewall - 500 Gbps - Sesiones Concurrentes - 100000000 - Mes - Cantidad: 2	FIREWALL FORTI 4400F	FG440FTK21900183	DATA CENTER PRINCIPAL IFX

12	2082016	2498166	IaaS Seguridad - Firewall Nueva Generación - Media Capacidad - Oro - Hosting físico - Rol de Firewall - 40 Gbps - Sesiones Concurrentes - 15000000 - Mes - Cantidad: 2	FIREWALL FORTI 900G	FG9H0GTB23900440	PALACIO
12	2082017	2498167	IaaS Seguridad - Firewall Nueva Generación - Media Capacidad - Oro - Hosting físico - Rol de Firewall - 40 Gbps - Sesiones Concurrentes - 15000000 - Mes - Cantidad: 2	FIREWALL FORTI 900G	FG9H0GTB23900205	PALACIO
13	2082013	2498168	IaaS Seguridad - Web Aplication Firewall - Alta Capacidad - Oro - Hosting físico - Desempeño WAF (Gbps) - 10 - Mes - Cantidad: 2	KEMP LM-X25	TSCC82005608	DATA CENTER PRINCIPAL IFX
13	2082014	2498169	IaaS Seguridad - Web Aplication Firewall - Alta Capacidad - Oro - Hosting físico - Desempeño WAF (Gbps) - 10 - Mes - Cantidad: 2	KEMP LM-X25	TSCB72000545	DATA CENTER PRINCIPAL IFX

8.1 Horas experto del item 29 y esquema de compensación.

Los servicios horas experto son prestados por los siguientes especialistas, bajo las líneas contratadas en la OC 147451:

Linea OC	SID Anterior	SID Nuevo	Articulo	Expertos
29	2082108	2498194	Servicios Complementarios - Experto Master - Región 1 - Hora/M - Cantidad: 480	Victor Hugo Galvis Edwar Wilmar Sierra Jose Luis Cardenas Rozo
30	2082099	2498192	Servicios Complementarios - Servicios de Preparación para Migración - Oro - Alta - Hora/M - Cantidad: 480	
31	Nuevo	2498193	Servicios Complementarios - Experto en soporte para migración - Alta - Región 1 - Hora/M - Cantidad: 320	

NOTA: Los ítems 30 y 31 no fueron ofertados por IFX, teniendo en cuenta que se daría uso de estos ítems, si la entidad migraba con otro proveedor

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 01 al 31 de julio 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	7/3/2025 18:00	7/3/2025 19:13	1	Nocturna	validacion bastion azure CE , CNDJ
2	7/11/2025 19:00	7/11/2025 19:15	1	Nocturna	TT1091725 RV: Permisos Conectividad Azure equipo Contratista URT
3	7/16/2025 19:00	7/16/2025 19:30	1	Nocturna	validacion bastion azure CE , CNDJ
4	7/18/2025 18:00	7/18/2025 19:29	2	Nocturna	TT1096939 RV: Solicitud de Permisos de Navegación para 25 de julio 2025 | TT1096966 RV: Formulario de permisos
Total horas Extras			5		

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	7/6/2025 12:00	7/6/2025 13:00	1	Diurna	TT1085721 RV: Solicitud información VPN INPEC-CSdJ TT1087098 RV: Solicitud de priorización de direcciones IP Auditorio del Palacio de Justicia de Riohacha RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA
2	7/8/2025 22:00	7/9/2025 3:00	5	Nocturna	TT1088675 CSJ | Actualización equipo Firewall 4400F versión 7.2.10 y armado HA
	7/29/2025 18:00	7/29/2025 19:00	1	Diurna	TT1105269 RV: Permisos On Premise Bus de Interoperabilidad Contrato 215 de 2024 Soaint RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA TT1105268 RV: Permisos On Premise Bus de Interoperabilidad Contrato 215 de 2024 Soaint RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA TT1105239 RV: Solicitud permisos conectividad transferencia FTP Barranquilla RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA TT1105225 RV: Listado de VPN para agregar a FW LDAP 29072025j1 RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA
Total horas Extras			7		

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	7/3/2025 18:00	7/3/2025 20:00	2	Diurna	validacion bastion azure CE , CNDJ
2	7/3/2025 23:00	7/4/2025 6:00	7	Nocturna	TT1085799 Creado: RV: CSJ | Actualización Firewall segunda parte 4400F 7.2.10
3	7/8/2025 22:00	7/9/2025 3:00	5	Nocturna	TT1088675 CSJ | Actualización equipo Firewall 4400F versión 7.2.10 y armado HA
TOTAL			14		

8.2 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	2498164	DC IFX	v7.2.10
		FTG_CSJ_DC_TC_SLAVE	FG440FTK21900183	2498165	DC IFX	v7.2.10
2	WAF KEMP Loadmaster x25 HA	WAF_TORRRE_CENTRAL	TSCC82005608	2498168	DC IFX	7.2.59.3.22368
		WAF_TORRRE_CENTRAL	TSCC8200529	2498169	DC IFX	7.2.59.3.22368
3	Fortigate 900G HA	FGT_900G_CSJ_PALACIO_M	FG9H0GTB23900440	2498165	PALACIO	V7.6.3
		FGT_900G_CSJ_PALACIO_S	FG9H0GTB23900205	2498166	PALACIO	V7.6.3
4	FortiDDos 2000E HA	CSJ_FDDoS_MASTER	FI-2KE5819000049	2498164	DC IFX	V5.7.4
		CSJ_FDDoS_SLAVE	FI-2KETB20000015	2498165	DC IFX	V5.7.4

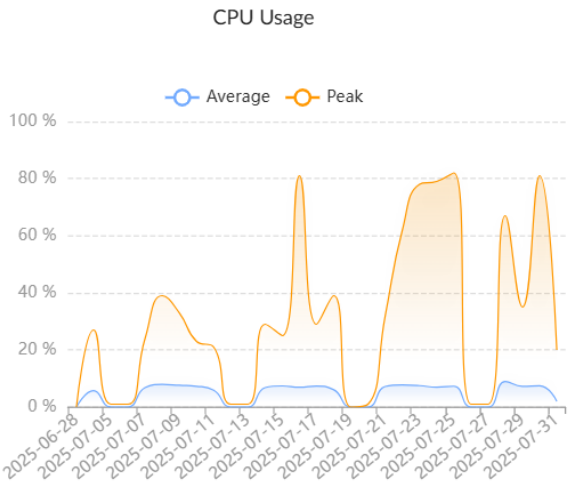
8.3 Actualización de firmware.

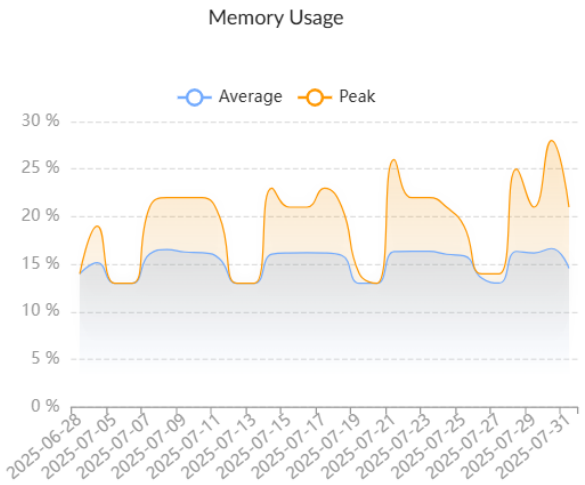
El plan de trabajo para la actualización del firmware será compartido, presentado y ejecutado con la autorización de los ingenieros Datacenter del CONSEJO SUPERIOR DE LA JUDICATURA.

Equipos	Versión Firmware	Fecha de Ejecucion	Versión Por Actualizar
FTG_CSJ_DC_TC_MASTER	V7.2.10	Actualizado	N/A
FTG_CSJ_DC_TC_SLAVE	v7.2.10	Actualizado	N/A
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	V7.6.3	Actualizado	N/A
FGT_900G_CSJ_PALACIO_S	V7.6.3	Actualizado	N/A
CSJ_FDDoS_MASTER	V5.7.4	Actualizado	N/A
CSJ_FDDoS_SLAVE	V5.7.4	Actualizado	N/A

9 FIREWALL PERIMETRAL

Durante el 01 al 31 de julio, el consumo promedio de CPU y memoria (traza azul) en el firewall perimetral estuvieron dentro de sus valores de operación normal.

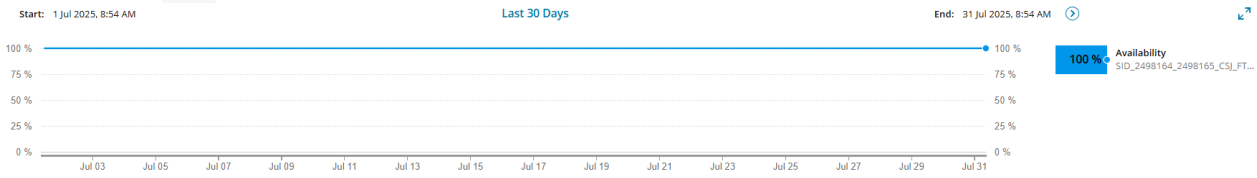




En la gráfica de rendimiento "CPU Usage", la curva color naranja muestra los picos de consumo de una o varias de las 160 CPUs del appliance FortiGate-4400F, cuando estos picos ocurren las tareas que generan estos picos son desbordadas a las otras CPUs por lo que la curva color azul se muestra el consumo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

9.1 Disponibilidad mensual firewall perimetral.

Durante el 01 al 31 de julio se obtuvo 100% de disponibilidad en el firewall perimetral.



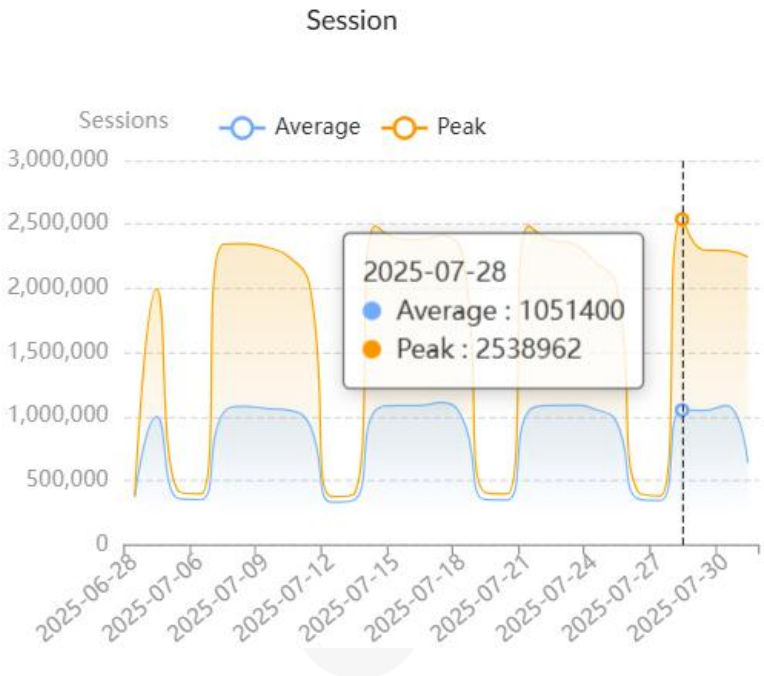
Durante julio la disponibilidad del firewall Principal IFX fue de 100%

Availability Statistics

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

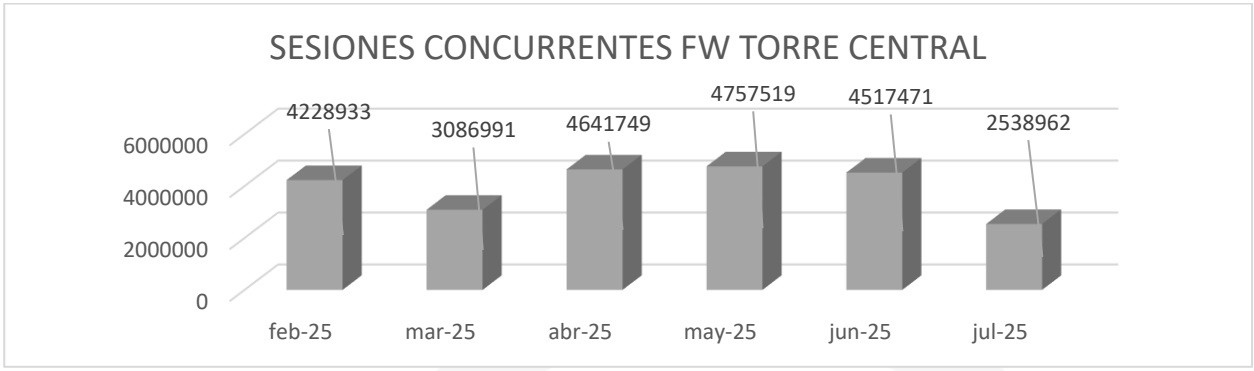
9.2 Cantidad de sesiones firewall perimetral.

Durante el 01 al 31 de julio se presentó un máximo de 2538962 sesiones TCP concurrentes, cantidad que se encuentra dentro del rango máximo soportado por el appliance Fortinet FG- 4400F cuyo valor es de 210 millones.



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

Durante el 01 al 31 de julio las sesiones en el FW central se mantuvieron en el rango menor, respecto al mes anterior:



MES	SESIONES
feb-25	4228933
mar-25	3086991
abr-25	4641749
may-25	4757519
jun-25	4517471
jul-25	**2538962**

9.4 Aplicaciones y protocolos por ancho de banda firewall perimetral.

HTTPS, Microsoft.SharePoint y Microsoft-Azure fueron las aplicaciones con mayor consumo de ancho de banda durante el 01 al 31 de julio:

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	HTTPS			93.99 TB
2	Microsoft.SharePoint			87.12 TB
3	Microsoft-Azure			84.77 TB
4	Microsoft.Teams			40.66 TB
5	Google-Web			35.37 TB
6	Microsoft-Azure.AD			30.78 TB
7	SSL			30.63 TB
8	Akamai-CDN			24.13 TB
9	STUN			21.86 TB
10	Microsoft.Windows.Update			13.88 TB

DNS, Microsoft-Azure y SMB fueron las aplicaciones con mayor consumo de sesiones durante 01 al 31 de julio:

Top Applications by Sessions

#	Application	Sessions
1	DNS	2,088,395,214
2	Microsoft-Azure	1,605,128,119
3	SMB	781,137,000
4	SSL	767,824,275
5	HTTPS	579,508,582
6	ESET-Eset.Service	388,156,414
7	HTTP	377,864,488
8	Google.Services	335,971,294
9	Akamai-CDN	271,827,876
10	Google-Web	258,820,504

9.5 Top de IP por ancho de banda firewall perimetral.

10.101.100.34, SDWAN LUMEN VLAN_2007 presentó la mayor cantidad de consumo de ancho de banda durante el 01 al 31 de julio:

Top Bandwidth IP

#	IP	Bandwidth
1	10.101.100.34	2.04 TB
2	10.101.101.78	1.91 TB
3	10.101.101.198	1.27 TB
4	10.101.100.42	1.04 TB
5	10.101.101.130	913.08 GB
6	10.101.101.94	881.53 GB
7	10.101.100.250	842.36 GB
8	10.101.101.34	836.45 GB
9	10.101.102.146	815.14 GB
10	10.101.101.62	804.82 GB

9.6 Top de destinos web por sesiones firewall perimetral.

Los destinos en Internet con mayor cantidad de sesiones durante el 01 al 31 de julio fueron 8.243.164.21, 8.243.164.19 (CTL Colombia) y gvt1.com

Top Destinations by Sessions

#	Hostname(or IP)	Sessions
1	8.243.164.21	787,062,942
2	8.243.164.19	579,633,769
3	172.29.130.220	206,615,783
4	8.8.8.8	200,253,721
5	rapid7.com	192,955,334
6	8.243.200.3	125,796,069
7	172.28.146.154	119,708,108
8	gvt1.com	95,846,201
9	microsoft.com	73,176,541
10	msftconnecttest.com	68,807,612

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

172.29.74.156 de la sede "Cundinamarca, Facatativá; Carrera 1 # 1e 27", 172.16.85.197 de la sede " Quindío, Armenia; Palacio de Justicia" y 172.27.91.82 de la sede "Cordoba, Monteria; Cra 6 # 61-44 Edificio Elite", presentaron la mayor cantidad de peticiones hacia Internet bloqueadas durante el 01 al 31 de julio:

Top Web Users by Blocked Requests

#	User (or IP)	Hostname	Requests
1	172.29.74.156	172.29.74.156	3,108,511
2	172.16.85.197	172.16.85.197	2,926,745
3	172.27.91.82	172.27.91.82	2,766,544
4	172.27.22.81	172.27.22.81	2,493,768
5	192.168.58.196	192.168.58.196	2,335,957
6	192.168.58.214	192.168.58.214	2,245,692
7	172.27.91.15	172.27.91.15	1,648,577
8	172.27.91.88	172.27.91.88	1,628,212
9	192.168.58.46	192.168.58.46	1,457,117
10	172.27.22.85	172.27.22.85	1,395,414

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

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

Streaming Media and Download, Proxy Avoidance y Overrride_bloqueadas fueron las categorías con mayor cantidad de bloqueos durante el 01 al 31 de julio:

Top Blocked Web Categories

#	Category	Requests
1	Streaming Media and Download	49,579,446
2	Proxy Avoidance	32,714,901
3	Overrride_bloqueadas	16,060,482
4	Unrated	15,892,399
5	Social Networking	10,967,268
6	Games	3,599,161
7	Internet Radio and TV	2,796,182
8	Gambling	1,019,541
9	Entertainment	948,481
10	Malicious Websites	569,196

9.9 Top de IP más activos Firewall Perimetral

Los hosts con mayor cantidad de peticiones durante el 01 al 31 de julio fueron los dispositivos de la red 10.101.101.0/24 correspondientes a Deaj UTDI - Div- ST y breakout de Cirion "SDWAN LUMEN":

Top Web IP by Allowed Requests

#	IP	Requests
1	10.101.101.50	5,436,911
2	10.101.101.94	5,233,843
3	10.101.100.34	4,656,983
4	10.101.101.62	3,850,575
5	10.101.100.42	3,576,908
6	10.101.101.54	3,346,224
7	10.101.101.130	3,345,524
8	10.101.101.118	3,240,091
9	10.101.101.78	3,198,586
10	10.101.101.30	3,160,049

9.10 Top de categorías más visitadas Firewall Perimetral

La categoría más visitada durante el 01 al 31 de julio fue Information Technology:

Top Allowed Web Categories

#	Category	Requests
1	Information Technology	489,026,326
2	Overrride_permitidas	312,343

9.11 Top de consumo ancho de banda por usuario Firewall Perimetral

Las maquinas con IP 172.27.64.14 que corresponde a RED_CICERO, presentó el mayor consumo de ancho de banda durante el 01 al 31 de julio:

Top IP by Bandwidth

#	IP	Bandwidth	Sent	Received
1	172.27.64.14			30.78 TB
2	172.27.64.110			29.80 TB
3	172.16.182.85			5.44 TB
4	10.101.100.34			3.69 TB
5	10.101.101.78			3.22 TB
6	192.168.209.92			2.99 TB
7	10.101.100.42			2.16 TB
8	172.27.64.19			1.83 TB
9	192.168.213.68			1.82 TB
10	10.101.101.198			1.77 TB

10 TRÁFICO VPN FIREWALL PERIMETRAL

El top 10 de los usuarios conectados a la VPN SSL durante el 01 al 31 de julio 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	cvillam	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2025-08-01 00:02:32	1754006552	181.55.51.20	364	699:48:57	8.85 GB	867754518	8637838364
2	Ecoralb	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2025-07-31 23:57:15	1754006235	186.102.2.108;186.102.91.244;186.102.97.205;186.30.132.138;190.27.152.172;190.27.178.188	95	561:32:21	11.47 GB	1231189278	11080213844
3	rgutierm	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2025-07-31 23:58:08	1754006288	181.59.2.226;181.59.3.143;181.59.3.222;181.59.3.235;181.59.3.84;186.113.150.213;190.255.159.42;191.107.33.50;191.107.9.5	101	443:45:48	2.88 GB	217869020	2877165545
4	gcardeng	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2025-07-31 22:49:31	1754002171	200.118.63.31	148	404:51:22	35.05 GB	3139024365	34493105634
5	VpnTSA	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2025-07-31 23:55:10	1754006110	172.27.90.236	75	366:08:09	118.94 MB	44922209	7979541 6
6	jsanabrl	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2025-07-31 22:41:55	1754001715	181.61.246.255;181.61.246.45;181.61.246.66;186.85.240.14;186.85.240.175;191.156.50.241;191.156.53.241;191.156.55.137;191.156.61.138	83	337:28:18	34.48 GB	1910412518	35112537742

7	MMoraleH	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2025-07-27 02:09:38	1753582178	179.32.238.39;186.112.101.247;186.112.105.212;186.112.125.79;186.118.228.97;186.118.243.148;190.66.100.236;190.66.108.193;190.67.146.241;190.67.146.95;190.67.156.119;190.67.158.129;190.67.205.104	65	330:02:00	8.56 GB	795667745	8390672776
8	lmortizh	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2025-07-31 22:02:39	1753999359	186.30.114.210;190.255.40.238	53	327:37:52	87.06 GB	1721542112	91757048866
9	jramiren	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2025-07-31 23:27:33	1754004453	181.63.116.3;186.86.110.255;191.156.124.198;191.156.152.166;191.156.152.48;191.156.53.241	82	316:48:41	14.34 GB	1026184857	14375050978
10	GOsorioD	CSJ_FTG_DC_TC_FG4400_	ssl-tunnel	2025-07-31 06:43:59	1753944239	179.32.226.102;179.32.237.162;179.32.237.254;186.112.105.252;186.112.99.149;186.118.244.75;186.170.77.250;186.170.77.27;186.170.85.248;190.67.154.235;190.67.155.205	81	310:21:09	30.29 GB	1752527382	30776146575

10.1 VPN IPSEC Site To Site Firewall Perimetral

El consumo de ancho de banda de las VPN IPSec Site to Site durante el 01 al 31 de julio fue el siguiente:

CSJ_FTG_DC_TC_FG4400_ Custom ... 2025-07-01 00:00:00 - 2025-07-31 23:59:00 Refr

Site-to-Site IPsec

Add Filter

Site-to-Site IPsec Tunnel	Initiating FortiGate	Terminating FortiGate	Duration	Bytes (Sent/Received)
VPN_AZURE	190.217.24.4 Bogota, Colombia	52.240.53.161 Potomac Falls, United States	30d 12h 0m 03s	26.0 TB/4.0 TB
VPN_SIUG_AWS	190.217.24.4 Bogota, Colombia	34.194.187.190 Ashburn, United States	30d 11h 59m 31s	21.9 TB/233.5 GB
VPN_ORACLE	190.217.80.4 Barrancabermeja, Colombia	129.213.6.36 Ashburn, United States	30d 11h 55m 47s	187.5 GB/2.6 TB
VPN_SIUG_AWS-2	190.217.24.4 Bogota, Colombia	34.224.152.152 Ashburn, United States	30d 11h 37m 23s	1.4 TB/142.6 GB
Prueba2	10.101.250.4	10.1.1.2	27d 0h 47m 58s	626.3 GB/698.1 GB
VPN_Tierras	190.217.24.4 Bogota, Colombia	181.225.76.196 Anserma, Colombia	30d 9h 39m 03s	2.3 GB/71.8 GB
VPN_AZURE-ANALY	190.217.24.4 Bogota, Colombia	20.124.34.235 Potomac Falls, United States	30d 12h 0m 02s	37.8 MB/933.1 MB
VPN_INPEC	190.217.19.156 Bogota, Colombia	181.225.69.10 Pereira, Colombia	30d 11h 15m 14s	160.9 MB/703.3 MB
VPN_REGISTRADU	190.217.24.4 Bogota, Colombia	201.232.123.20 Medellin, Colombia	30d 12h 0m 02s	26.3 MB/90.7 MB
VPN_ALPOPULAR_M	190.217.24.4 Bogota, Colombia	190.144.184.24 Colombia	26d 23h 15m 26s	2.2 MB/94.3 MB
VPN_FISCALIA	190.217.24.4 Bogota, Colombia	190.157.218.66 Bogota, Colombia	30d 11h 59m 32s	5.3 MB/32.8 MB
OCI_EXADATA_FAB	190.217.24.4 Bogota, Colombia	150.136.25.96 Ashburn, United States	30d 11h 59m 51s	12.9 MB/0.0 KB
VPN_Linktic	190.217.24.4 Bogota, Colombia	3.222.171.115 Ashburn, United States	30d 11h 59m 52s	352.2 KB/314.0 KB

10.2 Top de intrusiones detectadas por el IPS del firewall perimetral

Las intrusiones detectadas y bloqueadas por los perfiles IPS del FortiGate durante el 01 al 31 de julio fueron los siguientes:

Top Attacks

#	Attack Name	Severity	CVE-ID	Counts
1	ip_dst_session	Critical		214,256
2	ip_src_session	Critical		140,036
3	icmp_flood	Critical		99,770
4	tcp_src_session	Critical		83,789
5	tcp_port_scan	Critical		75,245
6	tcp_dst_session	Critical		66,883
7	udp_scan	Critical		57,875
8	udp_src_session	Critical		29,794
9	udp_dst_session	Critical		29,072
10	Hikvision.Products.SDK.Web Language.Tag.Command.Injection	Critical	CVE-2021-36260	8,602

Las víctimas de intrusión detectadas en el firewall central durante el 01 al 31 de julio fueron los siguientes hosts:

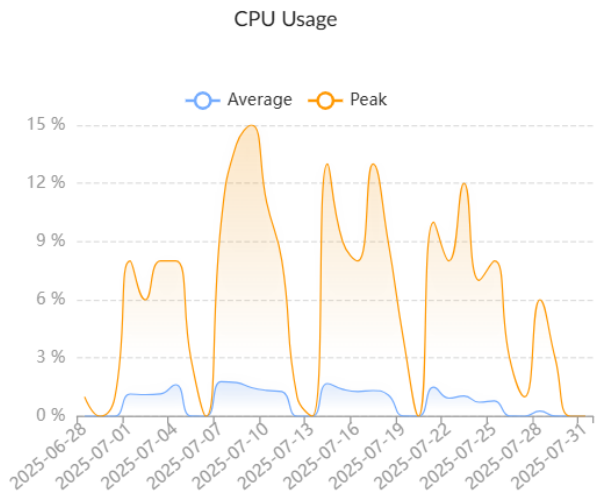
Top Intrusion Victims

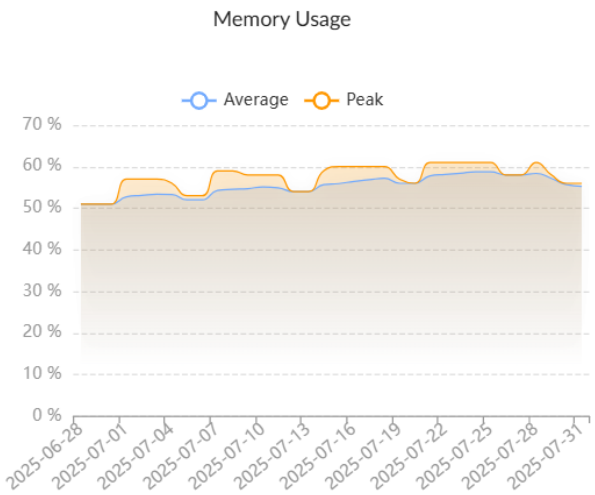
#	Attack Victim	Counts	Critical	High	Medium	Percent of Total Attacks
1	163.70.152.60				435,758	43.25%
2	57.144.115.32				304,643	30.24%
3	172.17.201.52				80,812	8.02%
4	65.20.83.65				62,804	6.23%
5	157.240.197.60				35,573	3.53%
6	66.70.227.25				10,504	1.04%
7	192.168.213.94				10,211	1.01%
8	172.17.201.13				8,995	0.89%
9	172.17.201.10				7,605	0.75%
10	172.17.201.8				6,227	0.62%
11	172.17.201.95				5,732	0.57%
12	172.17.201.84				5,387	0.53%
13	172.17.201.48				5,006	0.50%
14	172.17.201.89				4,771	0.47%
15	172.28.108.87				4,445	0.44%
16	172.17.201.57				4,373	0.43%
17	172.17.201.7				4,099	0.41%
18	172.17.201.50				3,650	0.36%
19	172.28.108.92				3,458	0.34%
20	172.17.201.88				3,393	0.34%

Los hosts 172.17.201.X, son aplicaciones web protegidas por los WAF PRINCIPAL IFX. Se debe verificar los demás hosts con software antivirus debido a que se encuentran comprometidos con algún malware.

11 FIREWALL SEDE PALACIO

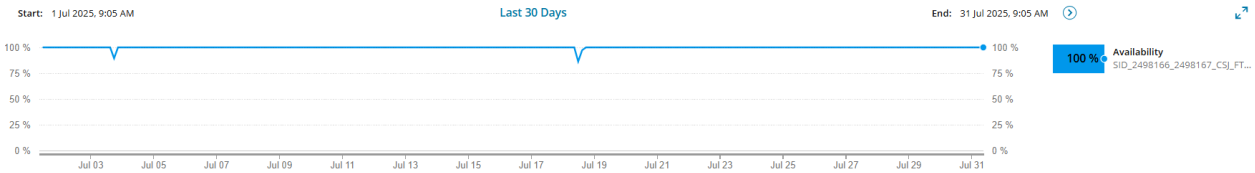
Durante el 1 al 31 de julio, el consumo de CPU y memoria en el Firewall de Palacio se mantuvo dentro de sus valores de operación normal.



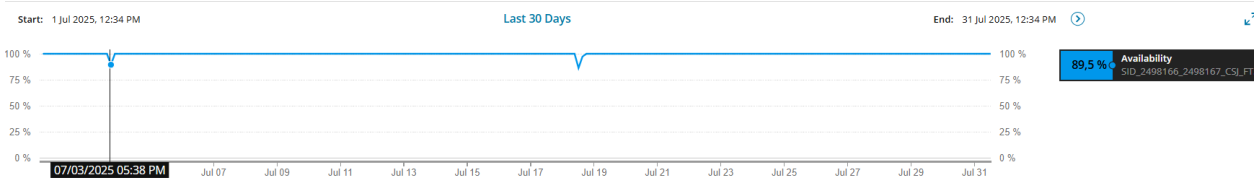


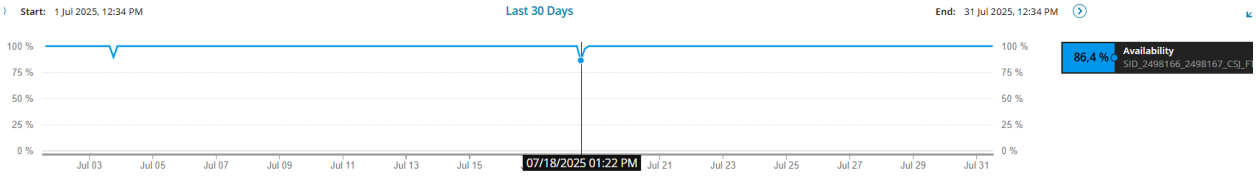
11.2 Disponibilidad Mensual Firewall Palacio

Durante el 01 al 31 de julio se obtuvo 100% de disponibilidad en el firewall perimetral Palacio.



Los eventos presentados del 03 y 18 de julio, es relacionado a una un cambio de direccionamiento IP en la interface de internet del firewall de Palacio "VLAN_80_INTERN" por el proveedor claro, este cambio es debido a un posible bloqueo que se tenía en el bastion de azure.



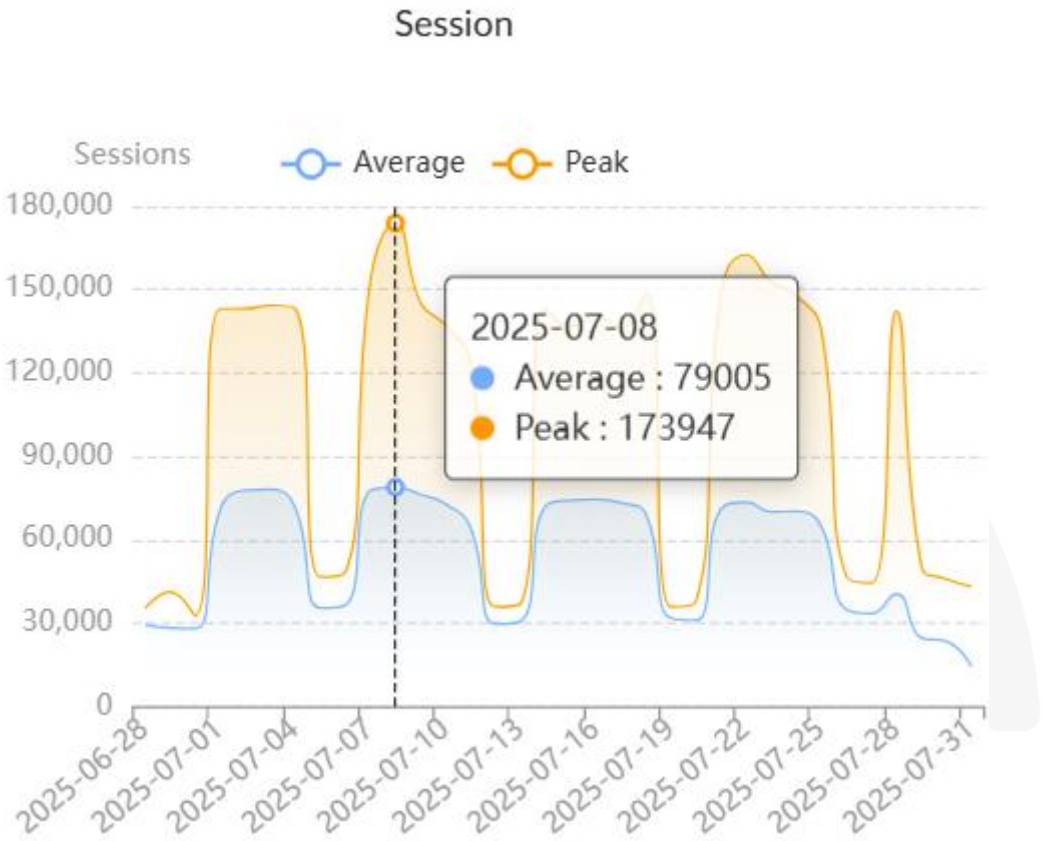


Availability Statistics

PERIOD	AVAILABILITY
Today	100.000 %
Yesterday	100.000 %
Last 7 Days	100.000 %
Last 30 Days	99.874 %
This Month	99.874 %

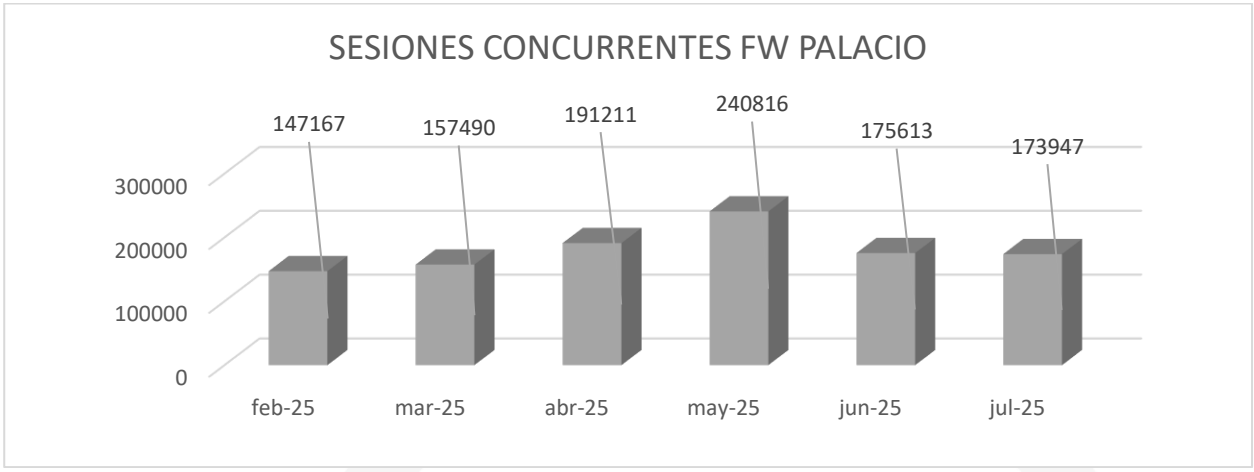
11.3 Cantidad de Sesiones Firewall Palacio

Durante el 01 al 31 de julio se presentó un máximo de 173947 sesiones concurrentes que están dentro del rango de sesiones soportadas por el equipo Fortigate 900G de 16 Millones.



11.4 Histórico de Sesiones Últimos 6 meses Firewall Palacio

Durante el 01 al 31 de julio las sesiones en el FW Palacio se mantuvieron en el rango promedio, respecto al mes anterior:



MES	SESIONES
feb-25	147167
mar-25	157490
abr-25	191211
may-25	240816
jun-25	175613
jul-25	**173947**

11.5 Aplicaciones y protocolos por ancho de banda firewall Palacio

Durante el 01 al 31 de julio las aplicaciones que consumieron la mayor cantidad de ancho de banda fueron Microsoft.SharePoint, OneDrive y Microsoft.Portal:

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	Microsoft.SharePoint			7.19 TB
2	OneDrive			6.95 TB
3	Microsoft.Portal			5.59 TB
4	Microsoft.Azure.Blob.Storage			4.21 TB
5	HTTPS.BROWSER			3.02 TB
6	HTTPS			2.80 TB
7	Microsoft.Teams			2.75 TB
8	Microsoft.Windows.Update			2.00 TB
9	SSL			1.78 TB
10	Microsoft-Azure			1.55 TB

SMB, DNS y Microsoft.365.Portal fueron las aplicaciones con mayor consumo de sesiones durante el 01 al 31 de julio:

Top Applications by Sessions

#	Application	Sessions
1	SMB	693,864,261
2	DNS	163,526,388
3	Microsoft.365.Portal	43,517,242
4	Microsoft.Portal	42,539,024
5	Rapid7.Insight.Agent	36,200,930
6	SSL	34,077,309
7	HTTPS.BROWSER	33,756,019
8	Microsoft.Teams	21,804,769
9	HTTP.BROWSER	21,759,220
10	Microsoft.Outlook	21,007,813

11.6 Top de IP por ancho de banda firewall Palacio.

172.28.93.2 de la "Comisión Nacional de Disciplina Judicial" y 172.28.92.15 de la red de "Digitalizacion Palacio de Justicia de Bogotá Corte Suprema" fueron los host que consumieron la mayor cantidad de ancho de banda durante 01 al 31 de julio:

Top Bandwidth IP

#	IP	Bandwidth
1	172.28.93.2	5.21 TE
2	172.28.92.15	2.85 TE
3	172.16.4.177	1.14 TE
4	172.28.92.36	963.40 GE
5	172.28.92.11	507.70 GE
6	172.16.2.59	325.89 GE
7	172.28.92.20	314.10 GE
8	192.168.8.42	301.60 GE
9	172.29.154.86	290.49 GE
10	172.17.114.228	286.53 GE

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

57.150.106.102, 13.107.136.10 y 13.107.138.10 (Microsoft) fueron destinos más visitados durante el 01 al 31 de julio:

Top Websites and Category by Bandwidth

#	Site	Category	Bytes
1	57.150.106.102		4.67 TB
2	13.107.136.10		3.17 TB
3	13.107.138.10		2.92 TB
4	backupaudienciascsj.blob.core.windows.net		1.61 TB
5	1d.tlu.dl.delivery.mp.microsoft.com		1.02 TB
6	20.209.74.1		854.10 GB
7	20.60.220.129		755.06 GB
8	cndjdisciplinaenlinea.file.core.windows.net		577.27 GB
9	57.151.50.164		500.84 GB
10	57.150.223.65		444.08 GB

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

172.29.99.52 y 172.29.99.73 (hosts de la LAN Palacio) presentaron la mayor cantidad de conexiones bloqueadas durante el 01 al 31 de julio.

Top Web Users by Blocked Requests

#	User (or IP)	Hostname	Requests
1	172.29.99.52	172.29.99.52	437,775
2	172.29.99.73	172.29.99.73	349,052
3	172.29.99.46	172.29.99.46	311,396
4	172.16.4.250	172.16.4.250	309,730
5	172.16.4.209	172.16.4.209	288,142
6	192.168.8.133	192.168.8.133	278,352
7	172.16.4.111	172.16.4.111	261,026
8	172.29.99.25	172.29.99.25	246,229
9	172.16.4.217	172.16.4.217	243,977
10	192.168.8.229	192.168.8.229	233,327

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.

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

Las categorías más bloqueadas durante julio en el firewall Palacio fueron Streaming Media and Download y las Unrated:

Top Blocked Web Categories

#	Category	Requests
1	Streaming Media and Download	8,228,857
2	Unrated	4,506,031
3	Overrride_bloqueadas	3,038,272
4	Proxy Avoidance	2,786,111
5	Social Networking	524,756
6	Games	141,076
7	Society and Lifestyles	134,440
8	Newly Observed Domain	80,776
9	Entertainment	77,013
10	Gambling	14,437

11.10 Top de IP más activas Firewall Palacio

172.28.54.20 ("Consejo de Estado Palacio de Justicia De Bogota") y 172.29.97.120 ("PROYECTO ESPECIAL DE REDES WIFI ARUBA Palacio de Justicia de Bogotá Corte Constitucional") presentaron la mayor cantidad de conexiones durante el 01 al 31 de julio:

Top Web IP by Allowed Requests

#	IP	Requests
1	172.28.54.20	8,169,720
2	172.29.97.120	724,386
3	172.16.4.101	635,617
4	172.16.2.168	606,762
5	172.16.6.121	587,074
6	172.28.93.54	522,693
7	172.16.2.95	475,292
8	172.28.93.121	468,184
9	192.168.2.43	448,723
10	172.17.114.232	442,898

11.11 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	55,241,352
2	Search Engines and Portals	4,208,329
3	Business	1,932,943
4	Information and Computer Security	796,052
5	Web Analytics	680,554
6	Finance and Banking	264,275
7	Web-based Applications	173,053
8	Online Meeting	101,770
9	Overrride_permitidas	87,709
10	Secure Websites	41,546

11.12 Top de consumo ancho de banda por usuario Firewall Palacio

172.28.93.2 y 172.28.92.15 (hosts de la LAN Palacio) presentaron la mayor cantidad de conexiones durante el 01 al 31 de julio:

Top IP by Bandwidth

#	IP	Bandwidth	Sent	Received
1	172.28.93.2			5.25 TB
2	172.28.92.15			2.91 TB
3	172.28.92.36			1.12 TB
4	172.16.4.177			1.12 TB
5	172.29.65.72			730.52 GB
6	172.28.92.11			627.09 GB
7	172.28.92.20			386.31 GB
8	172.16.2.59			342.99 GB
9	172.28.92.19			334.25 GB
10	192.168.8.42			327.54 GB

12 TRÁFICO DE WEB APPLICATION FIREWALL (WAF) PRINCIPAL IFX

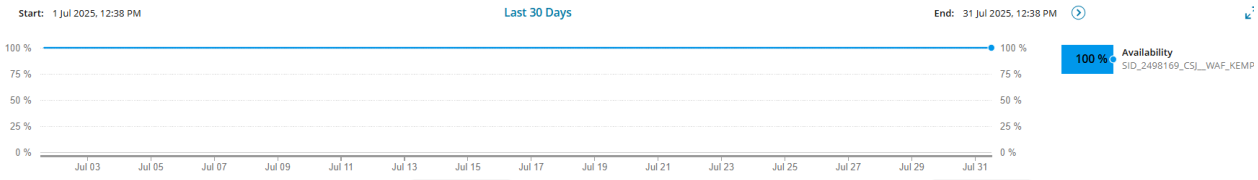
Para la protección de las aplicaciones web se tienen configuradas las siguientes políticas en los Firewall de Aplicaciones Web:

Item	Solución WAF	Cantidad de políticas de servidores
1	WAF PRINCIPAL IFX	212

A continuación, se muestran las estadísticas del WAF PRINCIPAL IFX.

12.2 Web application firewall datacenter principal IFX.

Durante el 01 al 31 de julio se obtuvo disponibilidad del 100 % en el Kemp de PRINCIPAL IFX.



Durante julio la disponibilidad del WAF Principal IFXfue de 100%

Availability Statistics

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

12.3 Uso de políticas de los servidores en el WAF principal PRINCIPAL IFX.

La aplicación web más consultada durante el 01 al 31 de julio fue GestionIPPublicaCorteConstitucional correspondiente al 59,7% del total:

#	Name	Virtual IP Address	Total Conns	% del total
1	GestionIPPublicaCorteConstitucional - 190.217.24.188	172.17.201.10:443	41757949	59,7%
2	cortesuprema.gov.co_Palacio	172.17.201.95:443	6766683	9,7%
3	apigestionaudiencias1.ramajudicial.gov.co	172.17.201.42:443	4665420	6,7%
4	capacitacion.ramajudicial.gov.co	172.17.201.197:443	3026492	4,3%
5	siicor.corteconstitucional.gov.co - 190.217.24.62	172.17.201.13:443	2594306	3,7%
6	sistemaaudiencias.ramajudicial.gov.co	172.17.201.44:443	1999704	2,9%
7	seccionalescsj.ramajudicial.gov.co-intrajud.ramajudicial.gov.co	172.17.201.8:443	1386589	2,0%
8	GestionIPPublicaCorteConstitucional - Redirect- 190.217.24.188	172.17.201.10:80	1095621	1,6%
9	sso.cortesuprema.gov.co	172.17.201.89:443	504587	0,7%
10	cortesuprema_Palacio Redirect	172.17.201.95:80	453804	0,6%
	Otras aplicaciones		5747807	8,2%
	Total		69998962	100,0%

12.4 Top de peticiones por país WAF principal IFX.

Durante el 01 al 31 de julio, el país desde donde se recibieron más peticiones de conexión fue Switzerland:

Top 10 Countries

Total

Country	Requests	Blocked
IPrep	193556	193558
Switzerland	388591	72142
United States	10685009	65305
Japan	158787	18789
Romania	48831	9453
Private	8747364	7186
United Kingdom	125501	5142
Singapore	41830	3642
Spain	401109	2504
Russia	184934	1959

12.5 Top de ataques por política WAF principal IFX.

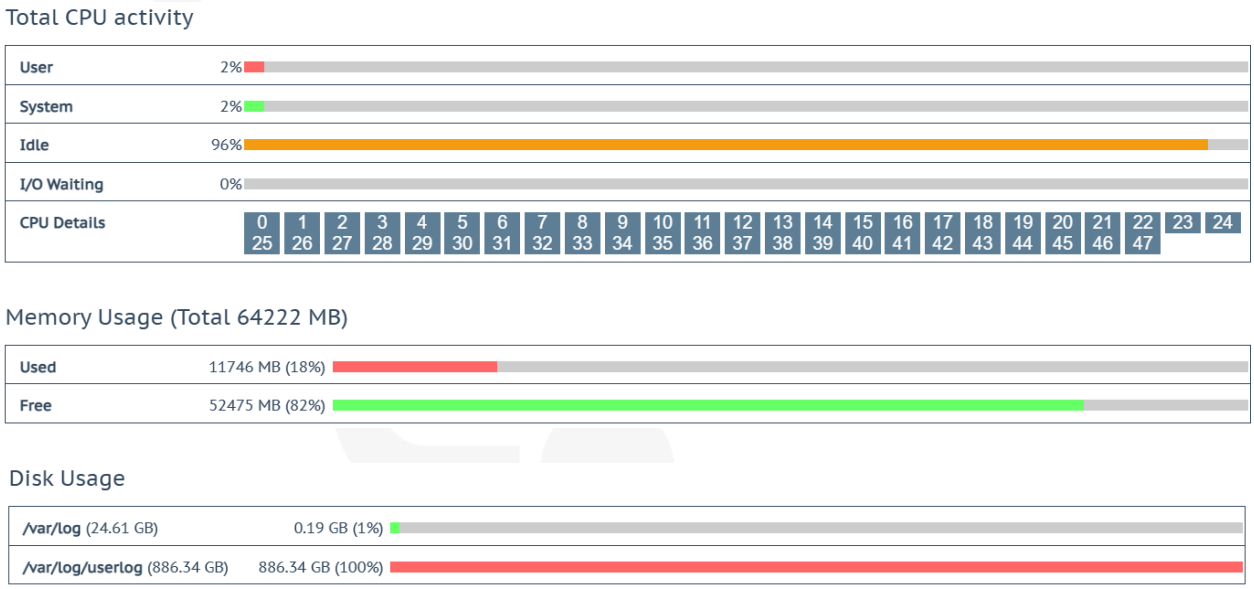
La siguiente tabla muestra el top 10 de las reglas o virtual services que proporcionaron mayor protección contra ataques a las aplicaciones web durante el 01 al 31 de julio. Sobre la aplicación GestionIPPublicaCorteConstitucional y

apigestionaudiencias1.ramajudicial.gov.co fueron prevenidas la mayor cantidad de ataques:

#	Name	Virtual IP Address	Total Conns	% del total
1	GestionIPPublicaCorteConstitucional - 190.217.24.188	172.17.201.10:443	277080193	74,2%
2	apigestionaudiencias1.ramajudicial.gov.co	172.17.201.42:443	23238418	6,2%
3	cortesuprema.gov.co_Palacio	172.17.201.95:443	19189614	5,1%
4	capacitacion.ramajudicial.gov.co	172.17.201.197:443	12197176	3,3%
5	sicofcsj_compras.ramajudicial.gov.co_Oracle	172.17.201.51:8443	11673833	3,1%
6	siicor.corteconstitucional.gov.co - 190.217.24.62	172.17.201.13:443	10313600	2,8%
7	seccionalescsj.ramajudicial.gov.co-intrajud.ramajudicial.gov.co	172.17.201.8:443	4624883	1,2%
8	sistemaaudiencias.ramajudicial.gov.co	172.17.201.44:443	4104367	1,1%
9	iedoc.consejodeestado.gov.co 448	172.17.201.60:448	2468585	0,7%
10	servicios.consejodeestado.gov.co	172.17.201.7:443	1626474	0,4%
	Otras aplicaciones		6894852	1,8%
	Total		373411995	100,0%

12.6 Consumo de recursos WAF principal IFX.

El WAF KEMP de Principal IFXpresentó consumo de CPU del 2%, memoria de 18% y disco en un 1%:



Certificados digitales del CSJ presentan las siguientes vigencias:

Corteconstitucional2024_2025	*.corteconstitucional.gov.co [Expires: Oct 2 23:59:59 2025 GMT]
Ramajudicial.gov.co_2025_2026	*.ramajudicial.gov.co [Expires: Mar 25 16:41:00 2026 GMT]
cndj_2025-2026	*.cndj.gov.co [Expires: Jan 3 20:03:53 2026 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 digitales se encuentran instalados en los siguientes dispositivos para autenticar y cifrar el tráfico hacia las aplicaciones.

N°	Descripción	Hostname	Ubicación	Versión Firmware
1	**FortiGate-4400F HA**	FTG_CSJ_DC_TC_MASTER	DC IFX	V7.2.10
		FTG_CSJ_DC_TC_SLAVE	DC IFX	V7.2.10
3	**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

12.7 Intentos login fallidos a Firewalls

Durante el 01 al 31 de julio se presentaron los siguientes intentos de ingreso administrativos fallidos hacia los firewalls perimetrales. Estos accesos administrativos se encuentran protegidos por los controles "Restrict login to trusted hosts":

Top 100 Failed Admin Logins

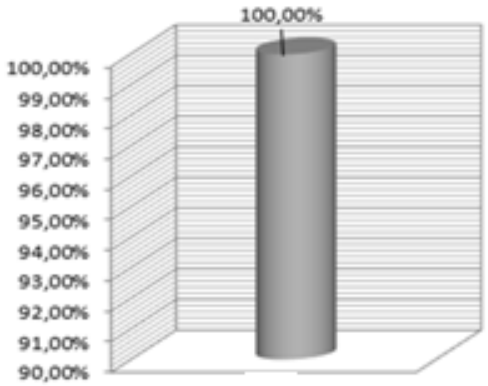
#	Login Source	User Name	Total Number of Failed Logins
1	ssh(172.16.54.86)	jose.cardenas	13
2	ssh(172.16.54.215)	victor.galvis	4
3	https(172.16.73.146)	dasarmiento	3
4	https(172.16.54.78)	jose.cardenas	2
5	https(10.0.0.1)	jose.cardenas	2
6	https(10.0.0.24)	victor.galvis	2
7	ssh(172.16.54.103)	esierra	1
8	https(10.0.0.143)	esierra	1
9	ssh(172.16.54.114)	esierra	1
10	https(10.0.0.96)	jose.cardenas	1

13 DISPONIBILIDAD SEGURIDAD GLOBAL DEL 01 AL 31 DE JULIO.

La disponibilidad del servicio de IFX durante el 01 al 31 de julio fue del 100%

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

MES	DISPONIBILIDAD (%)
01 al 31 de julio	100%



13.2 Anexo de las solicitudes e incidentes de seguridad reportadas.

Se adjunta documento "Anexo CSJ-Consolidado casos julio 2025", con los casos que se presentaron durante el 01 al 31 de julio.

14 CONSUMO MOTORES BASES DE DATOS

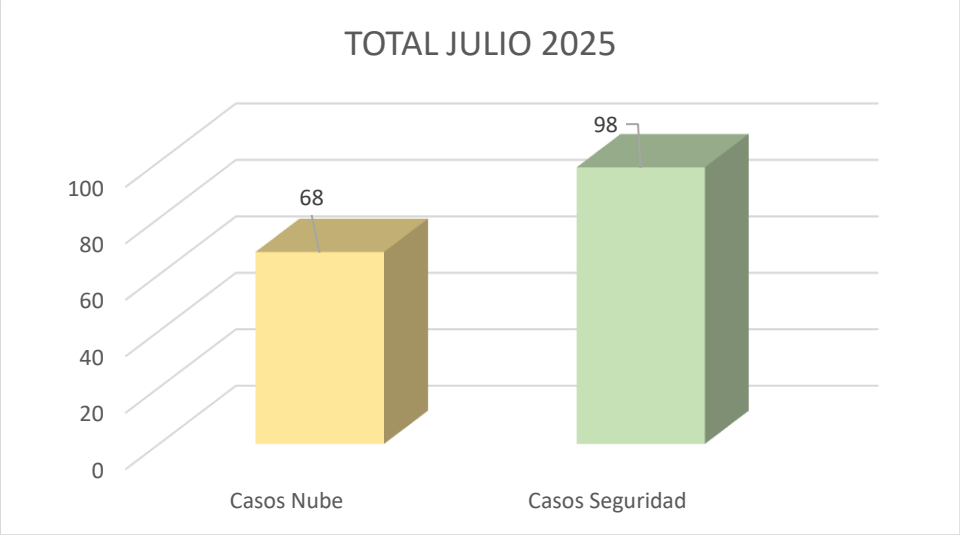
A continuación, se desglosas los motores bases de datos contratados bajo acuerdo marco:

- CPU
- Memoria RAM
- Disco

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

15 CONSOLIDADO-CASOS DE SERVICIO-ATENDIDOS JULIO 2025

SOLICITUDES	TICKETS
Casos Nube	68
Casos Seguridad	98
TOTAL	**166**



Se aclara a la entidad que las solicitudes internas y eventos reportados no aplican para imputabilidad de ANS, durante el mes de Julio 2025 se reportan las siguientes cantidades por grupo:

Solicitudes internas Cloud: 12
Eventos Cloud: 0

Solicitudes internas Seguridad:2
Eventos Seguridad: 0

Alarmas Proactivas (Solicitudes/eventos): 0

16 GESTIÓN FINANCIERA

- ***Tabla información Gestión financiera***

Fecha de inicio	16-jun-25
Fecha de finalización	31-dic-25
Valor inicial	$ 7.501.871.975,00
PLAZO	6,5 meses
Items de la Orden de Compra	31 lineas - SID
AMP	Nube Privada IV - CEE-308- AMP-2022- # Proceso CCENEG-061-1-2022
Valor facturado a la fecha	$ 1.719.955.725,00
% Valor facturado	22,93%
Valor pagado a la fecha	$ 0,00
% Valor pagado	0,00%

- ***Tabla Facturación***

FACTURA	FECHA EMISIÓN	VALOR (IVA incluido)	PERIODO FACTURADO	FECHA DE PAGO	ESTADO
VALOR PROYECTADO 16-30 JUNIO 2025		$ 573.318.575,00			
VALOR PROYECTADO 01-31 JULIO 2025		1.146.637.150			
Total proyectado ejecución financiera OC 147451		$ 1.719.955.725,00			

- ***Tabla ANS***

ANS (sin IVA incluido)	
16 al 30 de Junio 2025	No se generaron ANS durante el periodo
1 al 31 de Julio 2025	No se generaron ANS durante el periodo
Total ANS	

17 RECOMENDACIONES

- Depurar las políticas y objetos que no se estén usando en los dispositivos de seguridad. Esta depuración se debe programar en conjunto con los ingenieros del CSJ para determinar si 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 sesiones 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 no se están utilizando. Esta depuración se debe revisar en

conjunto con los ingenieros del CSJ para determinar si las políticas y estos objetos no se van a volver a utilizar.