Trabajo

Informe de Gestión Mensual Contrato 574 de 2023

Servicios Tecnológicos Informáticos para el Ministerio del Trabajo a Nivel Nacional

Unión Temporal
Gestión TIC 2023

Julio de 2026

DOCUMENTO/ ARCHIVO	
Código:	**Informe Gestión - Unión Temporal Gestión TIC 2023**
Nombre Archivo:	**Informe Gestión - Unión Temporal Gestión TIC 2023 – Julio 2026**
Fecha:	6/08/2026
Versión:	1

REGISTRO DE CAMBIOS			
Versión	**Páginas**	**Fecha Modificación**	**Motivo del cambio**
1	184	6/08/2026	Elaboración del documento

CONTROL DE DOCUMENTOS			
Versión	**PREPARADO**	**REVISADO**	**APROBADO**
1	**Equipo de Operación del Proyecto**	Paola Barrero Castro **Gestor ITIL Senior**	Diana Marcela Rueda **Gerente de Proyecto**

Índice

Introducción 10
Objetivo 10
Alcance 10
Definición de Siglas y Expresiones Técnicas 11
1 GERENCIA Y/O ADMINISTRACIÓN 12
2 LÍNEA DE GESTIÓN DE SERVICIOS 12
2.1. Gestión del Servicio 12
2.1.2. Prácticas ITIL 4 19
2.1.2.1. Práctica Acuerdos Niveles de Servicio (ANS) 20
2.1.2.2. Práctica Habilitación de Cambios 22
2.1.2.3. Práctica Gestión de Activos 23
2.1.2.4. Práctica Catálogo de servicios 25
2.1.2.5. Práctica de Problemas 29
2.1.2.6. Práctica de Incidentes 32
2.1.2.7. Práctica de Requerimientos 42
2.1.2.8. Práctica de Eventos 49
2.1.2.9. Práctica de Disponibilidad 67
2.1.2.10. Práctica de Implementación 70
2.2 Mesa de Servicios y Soporte en Sitio 71
3 LINEA DE SERVICIOS CENTRALES 80
3.1 Datacenter Principal 80
3.1.1 Datacenter Alterno y DRP 82
3.1.2 Procesamiento almacenamiento y respaldo Servicio Windows y Office 365. 88
3.1.3 Procesamiento, almacenamiento y respaldo - Nube Privada 93
3.1.4 Aplicaciones Especializadas 101
3.1.5 No aplica 111
3.1.6 Seguridad Informática 111
3.1.6.1 Firewalls de nueva generación 111
3.1.6.2 Sandbox – Amenazas día 0 118
3.1.6.3 SIEM - Solución de correlación de eventos de seguridad, disponibilidad y recursos 121
3.1.6.4 WAF - Servicio de tipo “Firewall de Aplicaciones Web” 124
3.1.6.5 Solución de Anti-DDoS 125
3.1.6.6 Casos atendidos de los servicios de seguridad 126
3.1.6.7 Análisis de riesgo 128
3.1.6.8 Políticas y procedimiento de seguridad 129
3.1.7 Licenciamiento 130
3.1.8 Administración, soporte y monitoreo 130
3.2 No aplica 131
3.3 Conectividad WAN, SDWAN e Internet 131
3.3.1 Canales WAN 131
3.3.1.1 Incidentes de Conectividad 133
3.3.1.2 Topología Actual 133
3.3.2 Canales SDWAN e Internet Dedicado 133
4 LINEA DE SERVICIOS EN SEDE 137
4.1.1.1 Equipos de Cómputo de usuario final 137
4.1.2 Equipos de Escritorio 143
4.1.3 Equipos Portátiles 143
4.2 Conectividad LAN y WLAN 143
4.2.1 Switch CORE Sede Principal 145
4.2.2 Switch para conexiones perimetrales (EDGE) en sede principal 145
4.2.3 Switch de acceso 24 puertos 145

4.2.4 Switch de acceso 48 puertos 145
4.2.5 Puntos de Acceso 146
4.3 Telefonía IP 147
4.3.1 Teléfono Gama Media 147
4.3.2 Teléfono Gama Baja 148
4.3.3 Troncales SIP 149
4.3.4 No Aplica 149
4.3.5 No Aplica 149
4.3.6 Módems 4G – Con plan de 50 Gbps 149
4.4 Energía Regulada UPS 155
4.4.1 UPS 10 kVA 155
4.4.2 UPS 15 kVA 156
4.4.3 UPS 20 kVA 156
4.5 No aplica 158
4.6 Outsourcing de Impresión 158
4.6.1 No aplica 162
4.6.2 Multifuncional B/N rango medio – Cargo fijo mensual 162
4.6.3 Impresora Color rango medio – Cargo fijo mensual 162
4.6.4 No aplica 162
4.6.5 Multifuncional B/N rango medio – Clic de impresión 162
4.6.6 Impresora Color rango medio – Clic de impresión 163
4.7 Antivirus 163
4.7.1 Instalaciones de antivirus en servidores 163
4.7.2 Instalación de antivirus PCs usuarios final 164
4.7.3 Top 10 Virus Detectados 164
4.7.4 Servicio de Vulnerabilidades 168
4.7.4.1 Inventario y licenciamiento 168
4.7.4.2 Escaneos programados 169
4.7.4.3 TOP 10 – Vulnerabilidades más explotables 170
4.7.4.4 Estrategia de remediación y/o mitigación 171
4.7.4.5 Resumen de mitigación efectuada 171
5 GESTIÓN DE CALIDAD DE INFORMACIÓN 174
5.1 Evaluación calidad documental de casos 175
5.2 Evaluación de calidad de llamadas 176
5.3 Práctica de Mejora 176
6 GESTION DE RIESGOS 179
7 BOLSA DE RECURSOS 181
8 MEDICIÓN DE ACUERDOS DE NIVEL DE SERVICIO 181
9 ANEXOS 184

Índice de Tablas

Tabla 1 Divulgación de información por SoporteMT 13
Tabla 2 Novedades de sedes 14
Tabla 3 Atención de solicitudes por Grupo de Especialista 20
Tabla 4 Medición Indicador Porcentaje de Cumplimiento de ANS 20
Tabla 5 Tipificación de los cambios 22
Tabla 6 Medición Indicador Porcentaje de Cambios Exitosos 23
Tabla 7 KPI Práctica de activos 25
Tabla 9 KPI Práctica Catálogo de Servicios 28
Tabla 10 Consolidado problemas identificados 30
Tabla 11 Categorización de Incidentes por Servicio 36
Tabla 11 Top 10 Incidentes 37
Tabla 13 Incidentes Suspendidos 38
Tabla 14 Incidentes mayores 39

Tabla 15 Medición de KPIs 39
Tabla 16 Estados de Requerimientos 42
Tabla 17 Estados de Tareas de requerimientos 43
Tabla 18 Seguimiento del Backlog Suspendidos 43
Tabla 19 Top 10 de Solicitudes 44
Tabla 20 Detalle de KIP Practica de Requerimientos 44
Tabla 21 Casos reabiertos 49
Tabla 22 Consolidado disponibilidad de servidores 68
Tabla 23 Consolidado disponibilidad de Directorio Activo 68
Tabla 24 Desagregado de Disponibilidad Directorio Activo 68
Tabla 25 Consolidado disponibilidad de equipos Datacenter principal 68
Tabla 26 Desagregado de Disponibilidad Datacenter Principal 68
Tabla 27 Consolidado disponibilidad de equipos Datacenter alterno 69
Tabla 28 Desagregado Disponibilidad de equipos Datacenter alterno 69
Tabla 29 Consolidado disponibilidad de equipos redes y conectividad 69
Tabla 30 Consolidado disponibilidad de equipos de seguridad 69
Tabla 31 Disponibilidad de equipos Seguridad de la Información 69
Tabla 32 Consolidado disponibilidad de equipos de telefonía 69
Tabla 33 Consolidado disponibilidad de plataforma antivirus 70
Tabla 34 Llamadas Atendida por la Mesa de Servicio 72
Tabla 36 casos suspendidos 73
Tabla 37 Casos Atendidos usuarios VIPS 76
Tabla 38 Casos Atendidos usuarios 76
Tabla 39 Visitas a sedes sin Soporte en Sitio 79
Tabla 40 Medición de ANS Mesa de servicios 80
Tabla 41 Pruebas realizadas 84
Tabla 42 Capacidades iniciales 98
Tabla 43 Capacidades modificatorio 98
Tabla 44 Total capacidades + servers desaprovisionamiento 98
Tabla 45 Total capacidades consumidas 99
Tabla 46 Total capacidades sin servers de pruebas 99
Tabla 47 Total capacidades ambientes pruebas 99
Tabla 48 Consumos totales 100
Tabla 49 *Suma Instancias* 106
Tabla 50 Total Docs 107
Tabla 51 Total Radicados 107
Tabla 52 Dimensionamiento Servers IBM - Virtualización Optima 108
Tabla 53 Apps & DDBB Oracle 111
Tabla 52 Tendencia de uso de ancho de banda 112
Tabla 53 usuarios con mayor consumo de ancho de banda 114
Tabla 54 Top de usuarios por sesiones 115
Tabla 57 Top de aplicaciones 116
Tabla 58 Consolidado de indicadores 117
Tabla 59 métricas EPS 122
Tabla 58 Tipos de incidentes 122
Tabla 61 Hosts e IPs Implicados 122
Tabla 60 Usuarios con Mayor Actividad de Riesgo 123
Tabla 61 Aplicaciones por Ancho de Banda 123
Tabla 62 Tipo de ataque 125
Tabla 63 Reporte de requerimientos junio 128
Tabla 66 Vulnerabilidades en la infraestructura 128
Tabla 67 Vulnerabilidades en la infraestructura 128
Tabla 68 ataques de phishing 128
Tabla 69 Licenciamiento 130
Tabla 70 Medición ANS Datacenter 131
Tabla 71 Medición ANS Nube Pública 131

Tabla 70 Incidentes de conectividad 133
Tabla 73 Medición de ANS Conectividad WAN e Internet 136
Tabla 72 Desagregado sedes con novedad un solo enlace 136
Tabla 73 Desagregado sedes con novedad con doble enlace 137
Tabla 74 Cantidades de equipos Contractual – Instalados - Almacén 137
Tabla 75 Cantidades de equipos asignados nivel nacional 138
Tabla 76 Cantidades de equipos por devolución nivel nacional 139
Tabla 77 Estado de casos de garantía. 139
Tabla 78 ANS casos de garantía. 139
Tabla 79 ANS Relación casos de garantía 140
Tabla 80 Equipos en siniestro 142
Tabla 81 Solicitudes de Equipos Usuario Final – Según Grupo Responsable 142
Tabla 82 Solicitudes de Equipos Usuario Final – Según Grupo Responsable 142
Tabla 83 Medición ANS Equipos de Usuario Final 143
Tabla 84 Top 5 de categorías en el Servicio de conectividad LAN-WLAN 144
Tabla 85 Distribución y Cantidades de switch 24 puertos 145
Tabla 86 Distribución y Cantidades de Switch 48 puertos 146
Tabla 87 Distribución de puntos de acceso 147
Tabla 88 Medición ANS LAN y WLAN 147
Tabla 89 Equipos gama media 148
Tabla 90 Sedes cerradas 148
Tabla 91 Consolidado de teléfonos gama baja 148
Tabla 92 Consolidado equipos MIFI 149
Tabla 93 Minutos, consumos 151
Tabla 94 Top llamadas nacionales 151
Tabla 95 Top 5 consumo de llamadas 152
Tabla 96 Top 5 llamadas LDI 152
Tabla 97 Top 5 llamadas Celular 153
Tabla 98 Top 5 llamadas locales 153
Tabla 99 Medición ANS Telefonía IP 155
Tabla 100 Inventario de UPS – 10kVA 156
Tabla 101 Inventario de UPS – 20Kva 156
Tabla 102 Casos gestionados – Energía Eléctrica Regulada UPS 157
Tabla 103 Medición ANS Energía Eléctrica UPS 158
Tabla 104 Inventario de impresoras para el servicio 158
Tabla 105 Consumo de impresiones y copias por usuario - Impresoras B/N 159
Tabla 106Top 10 de impresoras con mayor uso 160
Tabla 107 Top usuarios impresión a color 160
Tabla 108 Top oficinas 160
Tabla 109Top 10 impresoras más usadas del servicio de fotocopiado 161
Tabla 110 Ampliación de cuota de impresión 161
Tabla 111 Despacho de papel a sedes del Ministerio del Trabajo 162
Tabla 112Cargo mensual multifuncional rango medio 162
Tabla 113 Cargo mensual impresora color 162
Tabla 114 Clics de impresión de junio 2026 – Multifuncional B/N 162
Tabla 115 Tendencia de consumo de clics B/N 162
Tabla 116 Clics de Impresión – Impresora Color 163
Tabla 117Tendencia de consumo de clics color 163
Tabla 118 Medición ANS Outsourcing de Impresión 163
Tabla 119 Top 5 Equipos 166
Tabla 120 Medición de ANS Antivirus 174
Tabla 121 KPI Practica de Mejora 177
Tabla 122 Gestión de Riesgos 181
Tabla 123 Bolsa de Recursos 181
Tabla 124 Medición de Acuerdos de Niveles de Servicio 183

Índice de Ilustraciones

Ilustración 1 Estado final de casos al corte del período 19
Ilustración 2 Medición de KPI Activos 25
Ilustración 3 Estados Incidentes 33
Ilustración 4 Categorización de Incidentes por Servicio 34
Ilustración 5 Top 10 Incidentes 37
Ilustración 6 Efectividad de resolución de incidentes 40
Ilustración 7 Porcentaje de incidentes abiertos 41
Ilustración 8 KPI Efectividad de Resolución de Requerimientos de Servicio 45
Ilustración 9 Requerimientos de Reabiertos en el periodo 45
Ilustración 10 Resumen de incidentes ..... **¡Error! Marcador no definido.**
Ilustración 11 Top 10 Sedes afectadas por router ..... **¡Error! Marcador no definido.**
Ilustración 12 Causas de eventos generados por router ..... **¡Error! Marcador no definido.**
Ilustración 13 Casos suspendidos VS. Casos solucionados/Cerrados de Router **¡Error! Marcador no definido.**
Ilustración 14 Sedes afectadas por Switch ..... **¡Error! Marcador no definido.**
Ilustración 15 Causa de eventos generados por Switch ..... **¡Error! Marcador no definido.**
Ilustración 16 Casos suspendidos VS. Casos solucionados de Switch ..... **¡Error! Marcador no definido.**
Ilustración 17 Top 9 Sedes afectadas por Access Point ..... **¡Error! Marcador no definido.**
Ilustración 18 Causa de eventos generados por AP ..... **¡Error! Marcador no definido.**
Ilustración 19 Casos suspendidos VS. Casos solucionados de AP ..... **¡Error! Marcador no definido.**
Ilustración 20 Top 10 Sedes afectadas por Starlink ..... **¡Error! Marcador no definido.**
Ilustración 21 Causas de eventos generados por Starlink ..... **¡Error! Marcador no definido.**
Ilustración 22 Casos suspendidos VS. Casos solucionados de Starlink ..... **¡Error! Marcador no definido.**
Ilustración 23 Top 5 Sedes afectadas por FortiGate ..... **¡Error! Marcador no definido.**
Ilustración 24 Causas de eventos generados por FortiGate ..... **¡Error! Marcador no definido.**
Ilustración 25 Casos suspendidos VS. Casos solucionados de FortiGate ..... **¡Error! Marcador no definido.**
Ilustración 26 Estado de casos escalados a Proveedor ..... **¡Error! Marcador no definido.**
Ilustración 27 Causas de alarmas Servidores Windows ..... **¡Error! Marcador no definido.**
Ilustración 28 TOP 10 de servidores Windows con mas alarmas ..... **¡Error! Marcador no definido.**
Ilustración 29 Casos suspendidos VS. Solucionados o cerrados Servidores Windows **¡Error! Marcador no definido.**
Ilustración 30 Causas de alarmas Servidores Linux ..... **¡Error! Marcador no definido.**
Ilustración 31 TOP 10 de servidores Linux con más alarmas ..... **¡Error! Marcador no definido.**
Ilustración 32 Casos suspendidos VS. Solucionados o cerrados Servidores Linux **¡Error! Marcador no definido.**
Ilustración 33 Grafica CPU ..... **¡Error! Marcador no definido.**
Ilustración 34 Grafica memoria ..... **¡Error! Marcador no definido.**
Ilustración 35 Seguimiento de Pruebas de Disponibilidad 2026 70
Ilustración 36 Seguimiento Práctica Implementación 71
Ilustración 37 Llamadas Atendidas 72
Ilustración 38 requerimientos solucionados mesa de servicios 74
Ilustración 39 requerimientos solucionados soporte en sitio ..... **¡Error! Marcador no definido.**
Ilustración 40 requerimientos solucionados soporte territoriales 74
Ilustración 41 Requerimientos Cerrados por la Mesa de Servicios 75
Ilustración 42 Casos Cerrados por Soporte en Sitio 76
Ilustración 43 Casos Cerrados por Territoriales 76
Ilustración 44 Medios de Ingreso de Casos 77
Ilustración 45 Gestión Casos - SC 80
Ilustración 46 Gestión SC - Por Grupo 81
Ilustración 47 Comportamiento SWCORE Datacenter Colombia XV 81
Ilustración 48 Sincronización HA de los Switch Core 82
Ilustración 49 Grafica de consumo canal Internet Datacenter 82
Ilustración 50 máquinas virtuales DRP 83
Ilustración 51 Escenario pruebas Apps DRP 84
Ilustración 52 Extremo DC Bogotá 85
Ilustración 53 Extremo DC Cali 85
Ilustración 54 Estado canal de Internet DC Cali 86
Ilustración 55 Estado SWCORE Datacenter alterno 86
Ilustración 56 Estado HA SWCORE Datacenter alterno 87
Ilustración 57 Consumo canal MPLS DC Alterno 87

Ilustración 58 Estado Router MPLS DC Alterno 88
Ilustración 59 Gestión de Casos Windows 89
Ilustración 60 Cumplimiento WSUS 90
Ilustración 61 Block Legacy Authentication 91
Ilustración 62 Fechas de Soporte 93
Ilustración 63 Licencias asignadas 93
Ilustración 64 Gestión Nube Privada 97
Ilustración 65 Nuevo entorno ACEDOC 102
Ilustración 66 Gestión Apps Especializadas 103
Ilustración 67 Arquitectura final Apps ..... **¡Error! Marcador no definido.**
Ilustración 68 Distribución Sitios IIS ..... **¡Error! Marcador no definido.**
Ilustración 69 Gestión Casos IBM 105
Ilustración 70 Licenciamiento adicional componente IBM 108
Ilustración 71 Gestión DDBB 109
Ilustración 72 Estado Bases de Datos 110
Ilustración 73 Firewall de nueva generación. 112
Ilustración 74 Comportamiento ancho de banda 113
Ilustración 75 Tendencia de uso de ancho de banda 114
Ilustración 76 Top de usuarios por números de sesiones 114
Ilustración 77 Top de aplicaciones 115
Ilustración 78 Top de Autenticación 117
Ilustración 79 sesiones fallidas 118
Ilustración 80 Reporte mensual 119
Ilustración 81 Captura de pantalla perfomance 120
Ilustración 82 licencia sandbox 120
Ilustración 83 Detalle servidores 124
Ilustración 84 Top attack types 124
Ilustración 85 Top de ataques 126
Ilustración 86 Políticas y procedimientos 129
Ilustración 87 Consumo canal MPLS DC Principal 132
Ilustración 88 Estado Router MPLS DC Principal 132
Ilustración 89 Topología actualizada 133
Ilustración 90 Interface Fortimanager 134
Ilustración 91 Interface MPLS HUB SDWAN 134
Ilustración 92 Interface Internet HUB SDWAN 135
Ilustración 93 VPN SDWAN establecidas 135
Ilustración 94 Estado HUB SDWAN Datacenter 135
Ilustración 95 Estado HA HUB Sdwan 135
Ilustración 96 Recursos Fortimanager 136
Ilustración 97 Estado de casos Redes y Conectividad 144
Ilustración 98 Asignación de licencias 150
Ilustración 99 Comportamiento de tráfico 151
Ilustración 100 llamada internacional de prueba 152
Ilustración 101 Top Celular 153
Ilustración 102 Top Local 153
Ilustración 103 Requerimientos por garantía 154
Ilustración 104 Disponibilidad y Continuidad TOIP 154
Ilustración 105 Equipos consola antivirus 164
Ilustración 106 Gestión consola antivirus – equipos usuario final 164
Ilustración 107 Top 10 virus detectado 165
Ilustración 108 Descripción de virus 165
Ilustración 109 BOLDATRIANA 167
Ilustración 110 VADMQUINONESP 167
Ilustración 111 BOPCBOGOTA10 168
Ilustración 112 GUDACAICEDO 168
Ilustración 113 Eventos Ransomware ..... **¡Error! Marcador no definido.**
Ilustración 114 captura eventos ransonware ..... **¡Error! Marcador no definido.**
Ilustración 115 Licenciamiento ..... **¡Error! Marcador no definido.**
Ilustración 116 Gestión consola Nessus 169
Ilustración 117 Escaneos programados 169

Ilustración 118 TOP 10 - Activos más explotables 170
Ilustración 119 Vulnerabilidades gestionadas vs en remediación 172
Ilustración 120 revisión configuraciones 173
Ilustración 121 captura envío de correo gestión de vulnerabilidades 174
Ilustración 122 Resultado General 175
Ilustración 123 Resultado de criterios y parámetros - Calidad de llamadas 176
Ilustración 124 Seguimiento Práctica Mejora 177
Ilustración 125 Resultado de Cumplimiento AM 178

Introducción

Objetivo

El presente documento tiene como objetivo dar a conocer a la entidad el informe mensual sobre los servicios y componentes de TI que soportan la infraestructura tecnológica en el Ministerio del Trabajo, de acuerdo con las obligaciones contractuales establecidas en el contrato No. 574 de 2023 suscrito con la ***Unión Temporal Gestión TIC 2023***.

El informe presenta los resultados y el análisis de la gestión de los servicios para el periodo en evaluación que corresponde al mes de julio de 2026

Alcance

A continuación, se mencionan los componentes sobre los cuales se presenta el cumplimiento de las obligaciones:

GERENCIA Y/O ADMINISTRACION
- Gerencia y/o administración

LINEA DE GESTION DE SERVICIOS
- Gestión del Servicio
- Herramienta de gestión ITSM
- Prácticas ITIL 4
- Mesa de Servicio y Soporte en Sitio

LINEA DE SERVICIOS CENTRALES
- DATACENTER
  - Datacenter principal
  - Datacenter Alterno y DRP
  - Procesamiento, almacenamiento y respaldo
  - Aplicaciones especializadas
  - Seguridad informática
  - Licenciamiento
  - Administración, soporte y monitoreo
- CONECTIVIDAD WAN, SD-WAN E INTERNET

LINEA DE SERVICIOS EN SEDE
- Equipos de cómputo de usuario final
- Conectividad WLAN y Red LAN
- Telefonía IP
- Energía regulada UPS
- Outsourcing de Impresión
- Antivirus

MEDICIÓN DE ACUERDOS DE NIVEL DE SERVICIO
BOLSA DE RECURSOS

Definición de Siglas y Expresiones Técnicas

ANS: Acuerdos de Nivel de Servicio.
DRP: Disaster Recovery Plan - Plan de Recuperación ante Desastres
DT: Dirección Territorial.
IM: Incidentes.
ITSM: Information Technology Service Management - Gestión de servicios de TI
OE: Oficina Especial.
RF: Peticiones o Requerimientos de Servicio.
LAN: Local Area Network - Red de Área Local
MDS: Mesa de Servicio
NOC: Network Operations Center - Centro de Operaciones de Red.
SD-WAN: Software Defined Wide Area Network - Red de Área Extensa Definida por - Software.
SOC: Security Operations Center - Centro de Operaciones de Seguridad.
SS: Soporte en Sitio
UPS: Uninterruptable Power Supply - Sistema de Alimentación Ininterrumpida.
UT: Unión Temporal Gestión TIC 2023.
WAF: Web Application Firewall - Firewall de aplicaciones Web.
WLAN: Wireless Local Area Network - Red de Área Local Inalámbrica.

- **Acción de Mejora**: Acción que identifica una actividad, aspecto u oportunidad que pueda mejorarse en un servicio o proceso y al ejecutarse aporta valor a la operación.
- **Procedimientos**: Son los documentos que describen la secuencia ordenada de acciones que concurren en la realización de una función específica, tanto técnica, administrativa, como de gestión.
- **Proceso**: Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados.
- **Acuerdos de Niveles de Servicios (ANS)**: Acuerdo entre un proveedor de Servicios de TI el cliente, describe el Servicio de TI, documenta las Metas de Niveles de Servicio y específica las responsabilidades del Proveedor de Servicios de TI y del Cliente.
- **Contacto**: Interacción entre el usuario y la Mesa de Servicios para solicitar alguno de sus servicios (incidentes, consultas, interacciones de servicio), este puede ser llevado a través de cualquiera de los canales ofrecidos.
- **Interacción**: Término utilizado en la herramienta de gestión que sirve para identificar las peticiones creadas y resueltas durante la atención del primer nivel y que son generados por una petición de servicio de los usuarios.
- **Incidente**: Una interrupción no planificada de un Servicio de TI, una reducción en su calidad o una falla que ha impactado su prestación. En la herramienta de gestión se usa este término para los incidentes que han sido escalados por el primer nivel de atención y son identificados con las letras IM.
- **Incidente Mayor**: Cualquier evento identificado con prioridad crítica.
- **Problema**: Incidentes repetitivos o de gran impacto, del cual no se conoce las causas que lo originan.
- **Peticiones**: Solicitud que realizan los usuarios para los servicios TIC y son representados por la letra (RF).

- **Soporte Primer Nivel**: Corresponde a los grupos de la mesa de servicios que brindan soporte por vía telefónica, correo electrónico, portal web, chat y a las personas que brindan el soporte en sitio en cada una de las sedes del contrato y los grupos de soporte especializados de cada servicio de TI.
- **Nivel Especializado**: Soporte especializado de solución de peticiones de servicios TIC.
- **Usuario**: Es la persona que utiliza o trabaja con algún dispositivo provisto por el Contratista o que utiliza el servicio de TI definido dentro el alcance del contrato.

1 GERENCIA Y/O ADMINISTRACIÓN

Durante el mes objeto del presente informe se firmó el modificatorio 9 con el fin de garantizar la continuidad en la prestación de los servicios tecnológicos que soportan la operación institucional, la Entidad requiere adicionar el Contrato No. 574-2023 por la suma de QUINCE MIL DOSCIENTOS SESENTA Y CUATRO MILLONES CUATROCIENTOS DIECINUEVE MIL NOVECIENTOS CUARENTA Y SIETE PESOS CON NOVENTA Y DOS CENTAVOS ($15.264.419.947,92) M/CTE.

Así mismo, se requiere prorrogar el plazo de ejecución del contrato por el período comprendido entre el 1° de agosto de 2026 y el 31 de diciembre de 2026, con el propósito de garantizar la prestación ininterrumpida de los servicios tecnológicos indispensables para el funcionamiento de la Entidad durante el resto de la vigencia actual.

2 LÍNEA DE GESTIÓN DE SERVICIOS

2.1. Gestión del Servicio

Durante el período del informe, desde la Gestión de Servicios se apoyaron las siguientes actividades:

a. Divulgación de comunicados e información de interés a través de Soporte MT:
Se brindó apoyo a la operación de los servicios con la elaboración y posterior envío de diferentes comunicados y divulgación de información a través de la cuenta de Soporte MT, los comunicados se orientaron a:

- **Incidentes mayores e intermitencias** presentadas en la operación de los servicios de TI y/o aplicaciones.
- **Ventanas de mantenimiento programadas** sobre la infraestructura tecnológica y/o aplicaciones avaladas bajo los lineamientos de la práctica de habilitación de cambios:
  - Mantenimiento en la red (Nivel Central y territoriales por despliegue IPV6).
  - Mantenimiento en el servicio de impresión (actualización PaperCut)
  - Mantenimiento del portal WEB.
  - Mantenimiento BD Gestor Documental
  - Mantenimiento SICIP
  - Mantenimiento de servidor de Base de Datos - se intervienen varias aplicaciones
- **Comunicados de servicios e información de TI:**

Temática	Evidencia correo
Lineamientos de respaldo de información a raíz del concurso de méritos de los funcionarios de la entidad enfocado a: Informar las novedades a la mesa por parte de roles autorizados, manejo de información en OneDrive, verificación y devolución de bienes tecnológicos.	¡INFORMACIÓN IMPORTANTE - LINEA
Promoción del **diligenciamiento de la encuesta de satisfacción de los servicios de tecnologías de la información**, se brindan indicaciones de como diligenciarla.	¡INFORMACIÓN IMPORTANTE ENCUE
Gestión de acceso a la **red WiFi de Visitantes**, como solicitar el acceso, los datos requeridos y las condiciones del servicio.	¡INFORMACIÓN IMPORTANTE ACCES
Divulgación del instructivo de **activación y uso del Agente Virtual Teams Aranda** que permite a los usuarios tener un canal adicional para crear, consultar y verificar información de los casos que solicitan a la Mesa de Servicios del Grupo de Soporte Informático.	¡INFORMACIÓN IMPORTANTE AGENTI
Lineamientos de uso y manejo del **Agente Virtual Aranda en Teams** para la gestión de solicitudes con la Mesa de Servicios.	¡INFORMACIÓN IMPORTANTE AGENTI
Divulgación del instructivo de **uso del Portal de Autogestión de Aranda** que permite a los usuarios tener un canal adicional para crear, consultar y verificar información de los casos que solicitan a la Mesa de Servicios del Grupo de Soporte Informático.	¡INFORMACIÓN IMPORTANTE PORTAI

Tabla 1 Divulgación de información por SoporteMT

b. Traslados, cierres temporales y novedades de sedes:

Sede	Novedad
Segovia / Antioquia	Se hizo traslado el 23/10/2025 y por un tiempo de 6 meses aproximadamente, mientras se efectúan las reparaciones locativas en las instalaciones de la Casa de Justicia (lugar donde está ubicada la inspección). La UT está atenta al retorno para verificar la conexión adecuada de elementos y operación normal de la inspección. Traslado temporal IT SEGOVIA.msg
Sonsón / Antioquia Cañas Gordas / Antioquia	No cuentan con funcionarios asignados, no se tiene información hasta que fecha. Los equipos a cargo de la UT se encuentran en la sede apagados.
El Doncello / Caquetá Tibú / Norte de Santander	Usuarios trabajan en sede una semana al mes, el resto de tiempo trabajan desde las DT.
Ipiales / Nariño	Requiere adecuación del cableado estructurado, el cable está pegado al piso de la oficina con cinta pegante. Ya se presentó en abril de 2026 un accidente, donde un usuario se tropezó y el equipo de cómputo portátil presentó golpes.
Anserma / Caldas	Por remodelación física de la alcaldía del municipio, la sede estuvo en lugar temporal entre el 8/03/2025 y el 29/01/2026, al volver a Casa

Sede	Novedad
	de Justicia a sede fue ubicada en una oficina diferente por disposición de la alcaldía. La sede actual no cuenta con puntos de red ni puntos de energía cercanos a los puestos de trabajo, los puntos de energía se solventaron con extensiones y se dejaron equipos cerca al fortinet.
Tumaco / Nariño	Se trasladó el 16/01/2026 presentándose novedades que fueron reportadas al Coordinador del Grupo de Soporte Informático. La sede no cuenta con puntos de red para la conexión adecuada de los dispositivos, se realizó conexión de equipos con patchcord cerca del equipo Fortinet.
Villeta / Cundinamarca	El funcionario fue trasladado a IT Mosquera, la sede queda temporalmente cerrada sin usuario.
Fusagasugá / Cundinamarca	El funcionario de la sede se retiró, equipos están apagados en la oficina.
Traslados DT Sucre y DT Cauca	Se brinda apoyo a todo lo solicitado por la entidad para la actividad de los traslados. Dentro de las novedades se tiene: - Se disponen en las sedes antenas Starlink para brindar el servicio de conectividad mientras se gestionan las instalaciones de fibras en las nuevas ubicaciones. - En ambas sedes, el 30 de julio se realiza embalaje de equipos a cargo de la UT. - En ambas sedes se realiza el traslado de elementos de TI a cargo de la UT, mientras el ministerio realiza el traslado de mobiliario, archivo y demás elementos de su propiedad. - Durante la primera semana de agosto los usuarios estarán trabajando desde casa mientras en las sedes finalizan las labores de adecuación locativa, ubicación de puestos de trabajo, finalizan labores de cableado estructurado e instalación del rack. - La puesta en marcha a cargo de la UT queda pospuesta hasta que el ministerio finalice trabajos de adecuación de las instalaciones.  RE_ Cronograma de traslado de la sede de  Traslado de la sede del Cauca .msg

Tabla 2 Novedades de sedes

c. **Plan de trabajo documentos SIG para publicación en la SVE:** Durante el período se continua el seguimiento con la Oficina Asesora de Planeación (OAP) para que se continue la publicación en la SVE del formato RFC de la Práctica de Cambios.

d. **Disposición de RAEES y Residuos Electrónicos:** Durante el periodo no se gestiona salida de elementos o residuos tecnológicas en la DT Norte de Santander el día **10 julio de 2026**, los cuales fueron retirados por el Soporte en Sitio Jenny Lizcano, de la misma manera entregados al proveedor SUMA - Desarrollo Ambiental para disposición final:

Elemento	Cantidad
Diademas Lenovo - RAEE	1
Unidad Fusora Impresoras- RAEE	2

Elemento	Cantidad
Unidades de Imagen Impresoras- RAEE	2
Cartuchos y tóner de impresoras de oficina	25

e. **Implementación IPV6 en Dual Stack:** Desde la gestión de servicios se lideró la implementación de IPV6 en Dual Stack en la infraestructura del Ministerio, aquí es importante precisar que en la fase de diagnóstico se identificó que la entidad no tenía ningún avance en la adopción, así como tampoco contaba con un pool asignado a su nombre ante el ente regulador del direccionamiento LACNIC. Por lo anterior, no fue posible que la UT Gestión TIC 2023 diera continuidad a las actividades adelantadas por el anterior proveedor de servicios tecnológicos de la entidad ya que no fue compartida la línea base de la implementación de IPv6

   El proceso inició con la consulta ante LACNIC si el Ministerio contaba con asignación del pool de direcciones IPv6 pero se evidenció que la entidad no tenía asignado ningún direccionamiento. Dado lo anterior y de acuerdo con la obligación del contrato se procedió con la gestión administrativa para que se generara esta compra y asignación, así como elaboración del plan de trabajo y la construcción de los diferentes documentos que solicita la documentación que versa sobre la temática en MinTIC.

Dentro de las actividades administrativas para la gestión de adquisición del pool a nombre de la entidad se incluyeron:

- Creación de usuario del Ministerio ante LACNIC (Entidad proveedora de los prefijos IPv6 para América).
- Revisión documental para la recopilación de la información y adelantar el registro formal ante LACNIC.
- Creación de la lista de distribución asociada al usuario registrado en LACNIC, la cual es el canal de comunicación ante cualquier novedad relacionada con IPV6 para la entidad.
- Diligenciamiento y firmas del Acuerdo de Servicio de Registro entre el Ministerio del Trabajo y LACNIC
- Envío de documentos físicos a LACNIC y aprobación.
- Pago de los servicios ante LACNIC a cargo de la UT y,
- Entrega del pool asignado a la entidad por parte de LACNIC.

A continuación, se presenta una línea del tiempo para detallar las actividades macro ejecutadas durante la gestión administrativa:



Ilustración 1 Línea del tiempo para detallar las actividades macro ejecutadas durante la gestión administrativa

Posterior a ese proceso administrativo, fue posible desarrollar el plan de trabajo propuesto por la UT para la adopción del protocolo IPV6 en dual stack, el cual se desagrego en las siguientes fases y actividades generales, así:



Ilustración 2 Fases y actividades generales adopción del protocolo IPV6

A continuación, se relacionan los logros más significativos del proyecto:

- ✅ Primera implementación institucional de **IPv6 en Dual Stack**.
- ✅ Obtención del **Pool IPv6 oficial ante LACNIC**.
- ✅ Diseño e implementación de la arquitectura IPv6.
- ✅ Despliegue progresivo en la infraestructura tecnológica del Ministerio.
- ✅ Proyecto ejecutado y documentado hasta su cierre.

La ruta donde se consolidó toda la información del proyecto es: **IMPLEMENTACION IPV6**



Ilustración 3 Repositorio de información IPV6

f. Otras actividades

- Como parte de los requisitos del Contrato 574 de 2023 en el documento Anexo técnico base en el numeral 1.6.3 se contempló Fase de cierre donde se indica (…) *Durante la fase de cierre, el CONTRATISTA debe continuar efectuando la prestación del servicio de acuerdo con las especificaciones y ANS establecidos contractualmente. Adicionalmente de manera simultánea debe desarrollar las actividades asociadas a la entrega del servicio y el cierre del proyecto, que consideran el empalme con el operador entrante o la entidad según lo defina la Entidad.* En tal sentido, la Unión Temporal Gestión TIC 2023 elaboró un plan de

cierre y consolidó informes de cierre de cada servicio los cuales fueron cargados en el sitio de Share Point del Grupo de Soporte Informático, se remite al Coordinador del Grupo de Soporte Informático el siguiente correo:



RE_ Plan de cierre
contrato 574 de 2023

- Novedades en seguimiento del Servicio de Equipos de Usuario Final:
  - En junio 2026 se reporta que el equipo con serial **PW0A36XZ**, hostname **BOPJGUARNIZO**, asignado al usuario **Jorge Andrés Guarnizo Molina**, ubicado en la sede **Nivel Central, Piso 5 No reporta en el sistema de gestión de dispositivos**, el funcionario se encuentra en proceso de abandono de cargo y por tal motivo **No realizó la devolución del equipo a su cargo** al personal de soporte en sitio ni al jefe inmediato. Se pide apoyo para adelantar las gestiones correspondientes y lograr la recuperación.



Solicitud apoyo
devolución equipo - P

  - El equipo del Sr. Egberto de Jesus Pedraza ubicado en Nivel Central – Piso 22 (**PW0A3CFL**, hostname **BOPEPEDRAZA**) fue retornado a bodega de Nivel Central, se encontraba pendiente por devolución luego del proceso de retiro de la entidad del usuario.

- **Lineamientos de Oficina TICs para gestión de usuarios e incidentes de seguridad**
  La oficina TICs realizó la publicación en la SVE del documento ***Lineamiento Específico Gestión de Cuentas de Usuario y Cuentas Especiales*** y según informa la jefe de la oficina, desde Secretaria General se remite correo a las áreas para su cumplimiento. Se requiere hacer en la entidad una socialización ya que, al aplicar los nuevos flujos en la MDS, se tendrán que devolver y no atender las solicitudes como se vienen gestionando actualmente, y se requieren notificaciones de novedades de personal por parte de Talento Humano y Gestión Contractual, que en el proceso actual no se da.

  Para el PRO***CEDIMIENTO GESTION DE INCIDENTES DE SEGURIDAD,*** se trabajo desde la práctica de incidentes y catálogo, la inclusión de algunas categorías en Aranda para la clasificación correcta de las solicitudes y vayan en la misma dirección del procedimiento. Se brindará avance de este ítem en el apartado de Prácticas Itil de este mismo documento.

- El 17/07/2026 se coordina ventana de mantenimiento entre el administrador de la herramienta Aranda, administrador de Directorio Activo y la MDS con el propósito de realizar el cambio de la contraseña de la cuenta de Soporte MT bajo el cambio RFC-278107, se desarrolla de forma exitosa.

g. Divulgaciones al equipo de trabajo

- 16/07/2026: Se realiza refuerzo de los lineamientos de la práctica de activos y gestión de inventario al equipo de Soporte de Territorio a cargo de Dayanna Roa.

- 17/07/2026; Se realiza sesión con el equipo del NOC con el propósito de recordar los elementos más importantes del monitoreo de la infraestructura de redes y aplicaciones para fortalecer el conocimiento de los servicios y aplicar mejoras en la atención de los eventos.
- Catalogo: Se realiza socialización al equipo de trabajo desde la Práctica de Catálogo de una nueva categoría que se creó para relacionar y gestionar las solicitudes de falla de SICIP que son atendidas por la especialista Sandra Potes.



¡Socialización
Creación Categoría SI

- 21/07/2026: Se realiza refuerzo de los lineamientos de la Práctica de Habilitación e implementación de Cambios mediante una pieza gráfica a todo el equipo de trabajo.



Lineamientos de la
Práctica de Habilitació

- El 31 de julio se realiza socialización a los equipos de MDS y SS unos ajustes que se implementaran a partir del 1 de agosto 2026 en relación con el Flujo de Inactivación de Usuarios y el Flujo de Traslado de sede o cambio de rol.



Cambios en los
Flujos de Trabajo Inac

2.1.1. Herramienta de Gestión ITSM

Durante julio 2026 se realizaron las siguientes acciones en la herramienta de gestión ITSM Aranda y la herramienta de monitoreo Zabbix:

- Se realizó la creación de nuevos monitores para los equipos de redes.
- Se realizó actualización de parámetros de monitoreo para los hosts de los servicios de redes y administración de servidores, adicionando características SNMP.
- Se realiza la eliminación de la tarea de Backup de OneDrive o correo electrónico ya que desde el equipo de procesos se hicieron ajustes del flujo de desvinculación de usuarios.
- Se adiciono la tarea a los flujos automático Flujo de inactivación de usuario y Flujo de traslado de sede, cambio rol o equipo.
- Se adiciono la tarea Acta de traslado de equipo al flujo automático traslado de sede, cambio rol o equipo.
- Se realiza cambio de especialista de impresión, para ello se reconfiguraron todas las automatizaciones de escalamientos de casos de impresión, alertas de zabbix, y autoasignación de casos.
- Se rediseña el catálogo de servicios de seguridad informática añadiendo nuevas categorías e inactivando las que no están en uso. Esto a raíz del Procedimiento de Incidentes de Seguridad generado por la Oficina TICs.
- Se modifico el reporte de software no autorizado cambiando las aplicaciones permitidas, esto dada la clasificación que se viene adelantando.

2.1.2. Prácticas ITIL 4

Volumetría de Solicitudes Gestionadas:

En el mes de julio 2026 se registraron en la herramienta ITSM 7503 solicitudes asociadas a la prestación de los servicios de TI por parte de la UT.

- Tipificación según la volumetría de casos:
  - Requerimientos de Servicio: 5369
  - Incidentes y Eventos: 762 (en el apartado 2.1.2.8. Práctica de Eventos de este mismo documento se muestra de estos incidentes cuales están asociados a la gestión de eventos resultantes del monitoreo 7x24 que realizan en NOC/SOC de la infraestructura a cargo de la UT).
  - Tareas (asociadas al flujo de desvinculación de usuarios, cambio de rol): 1350
  - Cambios: 21
  - Problemas: 1.
- Casos Anulados: 5 - Se presenta esta información en el Numeral 2.2. Mesa de Servicios y Soporte en Sitio de este documento.
- Estado final de casos a corte de julio 2026:

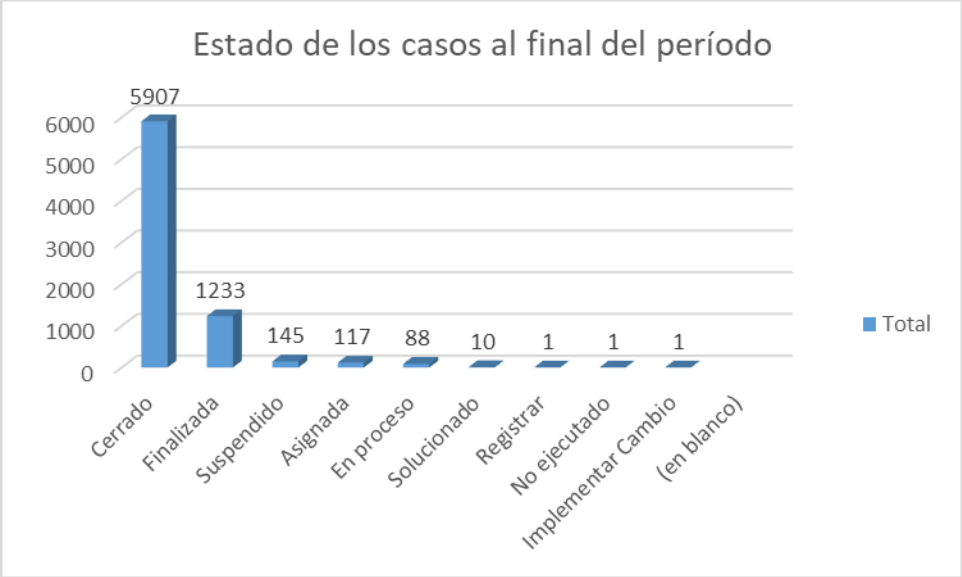


Ilustración 4 Estado final de casos al corte del período

- Gestión por parte de los grupos de especialistas:

Grupo Responsable	Cantidad de casos gestionados	Porcentaje (%)
Responsable_Soporte_Territoriales	2102	28,02
Responsable_Mesa_De_Servicio	1627	21,68
Responsable_Soporte_Bogota	1244	16,58

Grupo Responsable	Cantidad de casos gestionados	Porcentaje (%)
Especialistas_IBM	655	8,73
Responsable_Soporte_Impresoras	520	6,93
NOC	483	6,44
Responsable_De_Servidores_Windows	275	3,67
SOC	189	2,52
Gestor de Inventarios	110	1,47
Especialista_Telefonía_IP	102	1,36
Especialista Nube Privada	51	0,68
Responsable Garantías Equipos	33	0,44
Especialista Base de datos	31	0,41
Especialista Redes	23	0,31
Especialista Herramientas de Gestion	23	0,31
Almacenamiento y Backups	13	0,17
Especialista Nube Publica	9	0,12
Especialista Aplicaciones .Net	5	0,07
Liferay	5	0,07
Líder Seguridad de la Información	3	0,04
Total	7503	100,00

Tabla 3 Atención de solicitudes por Grupo de Especialista

2.1.2.1. Práctica Acuerdos Niveles de Servicio (ANS)

Durante el mes de julio de 2026 se llevó a cabo el proceso de seguimiento, control y medición de los Acuerdos de Niveles de Servicio (ANS) previamente parametrizados en la herramienta de gestión. Esta actividad se realizó en articulación con los líderes responsables de cada servicio, con el propósito de validar el grado de cumplimiento de los compromisos contractuales establecidos.

El ejercicio se desarrolló conforme a lo definido en el **Numeral 7. Medición de Acuerdos de Nivel de Servicio**, garantizando la trazabilidad de la información, la confiabilidad de los datos y la adecuada evaluación del desempeño de los servicios tecnológicos.

- **Medición Indicador Porcentaje de cumplimiento de los ANS**

Nombre	Descripción / Fórmula	Meta	Periodicidad	Resultado
Porcentaje de cumplimiento de los ANS	**CANS = (CSC/TSG)*100** Donde: **CANS:** Cumplimiento ANS **CSC:** Cantidad de servicios cumplidos dentro de los parámetros del ANS **TSG:** Total de servicios gestionados	95%	Mensual	PCE: 39/41*100 PCE: 95,12 %

Tabla 4 Medición Indicador Porcentaje de Cumplimiento de ANS

Como resultado de la medición efectuada durante el mes de julio de 2026, el indicador de cumplimiento de los Acuerdos de Niveles de Servicio alcanzó un valor de 95,12 %, superando la meta contractual establecida del 95 %.

De los 41 servicios gestionados, 39 cumplieron con los parámetros definidos en sus respectivos ANS, lo que evidencia un adecuado desempeño operativo y una gestión efectiva en el seguimiento de los compromisos adquiridos. Este resultado refleja la capacidad de la operación para mantener la continuidad, disponibilidad y calidad de los servicios tecnológicos, respaldada por mecanismos de monitoreo y control que permiten detectar oportunamente posibles desviaciones.

Los resultados obtenidos durante los últimos tres meses son los siguientes

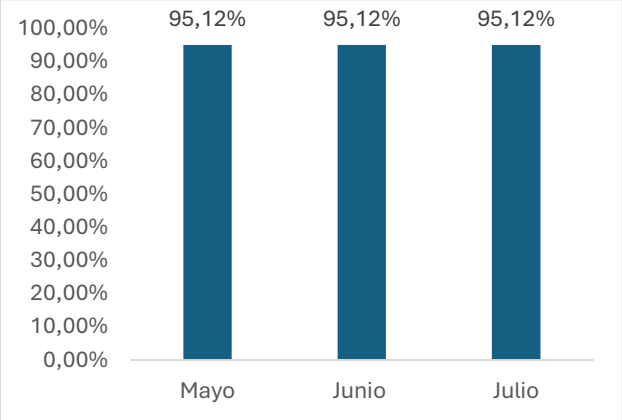


Ilustración 5 Cumplimiento de ANS

Se evidencia un comportamiento **estable** del indicador durante el trimestre evaluado, manteniendo un cumplimiento constante del **95,12%**, superior a la meta contractual definida.

La estabilidad observada demuestra la efectividad de los procesos de gestión, seguimiento y monitoreo implementados sobre los servicios tecnológicos, permitiendo sostener el cumplimiento de los compromisos establecidos sin variaciones significativas durante el periodo analizado.

No obstante, aunque el indicador se mantiene dentro del nivel esperado, la permanencia del mismo resultado durante los tres meses evidencia oportunidades de mejora orientadas a incrementar el porcentaje de cumplimiento. En particular, las desviaciones registradas en los indicadores asociados a la continuidad y disponibilidad del servicio WAN continúan limitando la posibilidad de alcanzar un desempeño superior.

En términos generales, la tendencia refleja una operación estable, controlada y alineada con los niveles de servicio establecidos; sin embargo, resulta conveniente fortalecer las acciones preventivas y correctivas sobre los servicios que presentan incumplimientos recurrentes, con el fin de mejorar la disponibilidad y resiliencia de la infraestructura tecnológica.

- **Indicadores con Desviaciones Identificadas**

Durante el periodo evaluado se identificaron desviaciones en los siguientes indicadores:

- **CWI-2:** Continuidad y disponibilidad del servicio WAN en sedes nacionales con un solo enlace.
- **CWI-3:** Continuidad y disponibilidad del servicio WAN en sedes nacionales con doble enlace.

Las desviaciones registradas corresponden a eventos que afectaron la disponibilidad del servicio WAN en algunas sedes nacionales durante el periodo evaluado. Si bien estas situaciones no representaron una afectación significativa sobre el cumplimiento global del indicador, constituyen oportunidades de mejora para fortalecer la continuidad y resiliencia de la infraestructura de comunicaciones.

El detalle técnico de los eventos, los cálculos efectuados y el comportamiento individual de cada indicador se encuentran documentados en el archivo soporte **"ANS Internet – MPLS"**, el cual constituye la fuente oficial utilizada para la medición y análisis de los resultados.

2.1.2.2. Práctica Habilitación de Cambios

Dar a conocer las actividades de la Práctica Habilitación de Cambios correspondientes a julio de 2026. Este apartado contiene información relevante sobre actividades realizadas y novedades presentadas.

- **Tipificación de los cambios**

Durante el mes de julio de 2026 se gestionaron 21 casos tipificados como Cambios, clasificados en las siguientes categorías:

Servicio	Cantidad	%
Aplicaciones Especializadas	6	28,57%
Administración de Bases de Datos	6	28,57%
Administración de servidores	3	14,29%
Redes y Conectividad	2	9,52%
Energía Eléctrica Regulada - UPS	1	4,76%
Herramientas de Gestión	1	4,76%
Soporte Microinformática	1	4,76%
Telefonía IP	1	4,76%
Total	21	100,00%

Tabla 5 Tipificación de los cambios

- **Relación casos registrados**

A continuación, se presenta la relación de casos registrados en el mes, en total se crearon 21 casos de los cuales se gestionaron como 16 cambios normales y 4 cambios como de emergencia y 1 cambio como estándar.

- **Cambios por estado**

Al corte del mes, 19 casos quedaron estado Cerrado, 1 casos quedaron en Implementar cambio y 1 casos no ejecutado.

- **Medición Indicador Porcentaje de Cambios Exitosos**

Nombre	Descripción / Fórmula	Meta	Periodicidad	Resultado
Porcentaje de cambios exitosos.	**PCE = (NCE/TCI)*100** Donde: **PCE:** Precisión **NCE:** Numero de Cambios Exitosos **TCI:** Total de Cambios implementados	80%	Mensual	PCE: 19/20*100 PCE: 95,00 %

Tabla 6 Medición Indicador Porcentaje de Cambios Exitosos

Durante el período evaluado se implementaron 20 cambios, de los cuales 19 fueron ejecutados exitosamente, alcanzando un 95,00 % de cambios exitosos. Este resultado supera la meta establecida del 80 %, evidenciando una adecuada planificación, evaluación de riesgos, ejecución y validación de los cambios implementados.

En el período evaluado, el cambio **RFC-289445 – Implementar Cambio** permaneció en estado de implementación, debido a que su ejecución estaba programada para una ventana de mantenimiento al finalizar el mes de julio. En consecuencia, no fue posible completar dentro del período evaluado la totalidad de las actividades y validaciones posteriores requeridas para su cierre como un cambio exitoso.

El único cambio no ejecutado correspondía a una actividad a cargo del proveedor Global Hills, el cual no se presentó en la ventana programada, por lo que no fue posible realizar su ejecución con el **RFC-278764**, ya que el proveedor Global Hitss reprogramó su ejecución. El cambio quedó pendiente de una nueva fecha para su implementación.

2.1.2.3. Práctica Gestión de Activos

En la Práctica de Gestión de Activos desarrolló en junio diversas actividades orientadas a garantizar la continuidad operativa, la disponibilidad óptima y el control integral del parque tecnológico de la Entidad. Dichas acciones se ejecutaron en concordancia con los lineamientos y las mejores prácticas de gestión, con un enfoque en la trazabilidad de los activos, el uso eficiente de los recursos tecnológicos, la mitigación de riesgos operativos y el fortalecimiento de la toma de decisiones.

Las principales actividades desarrolladas durante el periodo fueron las siguientes:

- **Seguimiento y actualización del Agente Aranda**

Se realizó el seguimiento al estado del Agente Aranda en los equipos de cómputo, con el objetivo de garantizar su correcto reporte en la consola de ADM. Esta actividad permite asegurar la visibilidad de los activos tecnológicos, facilitando la identificación de su ubicación, estado operativo y disponibilidad desde la consola de administración.

Con el apoyo del equipo de Soporte en Sitio, se llevó a cabo la actualización de la versión del Agente Aranda en los equipos que presentaban versiones desactualizadas o que no estaban reportando correctamente. Como resultado, se actualizaron 181 de los 243 equipos de cómputo identificados, lo que representa un avance del 74,48% en la ejecución de la actividad. Se continuará con el proceso de actualización de los 62 equipos restantes, con el fin de alcanzar el 100 % de cobertura y garantizar que todos los equipos reporten correctamente en la consola de ADM, fortaleciendo el control, la administración y el seguimiento de los activos tecnológicos.

- **Seguimiento a la gestión de activos**

Durante el período reportado, se realizó el monitoreo permanente de la asignación, estado, vigencia y ubicación de los activos tecnológicos, asegurando la actualización del inventario en la herramienta de gestión. Esta actividad permitió contar con información confiable y oportuna para la administración del ciclo de vida de los activos, facilitar la planificación de renovaciones, identificar necesidades de reposición y soportar la toma de decisiones estratégicas relacionadas con la gestión del parque tecnológico.

Adicionalmente se implementó en el aplicativo SGU la opción Cambio de sede y el acta de traslado de manera digital y cambio de ubicación de los usuarios, por lo tanto, se realizó en conjunto con la Practica de Requerimientos el afinamiento de tareas automáticas en flujo de inactivación de usuario y traslado de sede, lo cual, se elimina la tarea de backup de MDS y se adiciona tarea de acta de traslado para actualización de ubicación.

Por último, se realizaron capacitaciones de los procedimientos y lineamientos de la practice de activos y gestión de inventario de los Activos al personal de Soporte en Sitio.

- **Seguimiento a garantías y procesos de siniestro**

Se efectuó el seguimiento y control a los equipos que se encontraban en garantía y en procesos de siniestro, verificando el cumplimiento de los tiempos de atención establecidos por los proveedores y las condiciones contractuales vigentes. Estas acciones estuvieron orientadas a minimizar el impacto en la operación, garantizar la disponibilidad de los recursos tecnológicos y asegurar la continuidad del servicio. De igual manera, se gestionó la entrega de equipos de contingencia, con el fin de mitigar afectaciones a los usuarios finales durante los procesos de reparación o reposición.

- **Revisiones de Software Permitido y No permitido**

Se realizó la revisión y validación del **Listado de aplicaciones identificadas – Módulo Control de Aplicaciones (Trend Micro)** en conjunto con los diferentes servicios, con el propósito de verificar la información registrada, identificar aplicaciones vigentes y actualizar el inventario administrado en la herramienta Aranda. Esta actividad permitió mantener la información alineada con el estado actual de las aplicaciones autorizadas, fortaleciendo el control, la trazabilidad y la administración de la plataforma.

- **Piloto de medición del KPI de Practica de Activos**

De acuerdo con lo definido en la Guía Operacional de la Práctica de activos, se estableció el siguiente Indicador (KPI) trimestral, con el fin de establecer métricas que apoyen a la operación de los servicios TI:

Nombre	Descripción / Fórmula	Meta	Periodicidad	Resultado
Precisión de Información de CI en la CMDB	**P =** (NCAP/TCR) *100 Donde: **P:** Precisión **NCAP:** Numero de CI's con información actualizada y precisa **TCR:** Total CI registrados	85%	Trimestral	**P=**2971/3179 *100 **P=** 93,45%

Tabla 7 KPI Práctica de activos

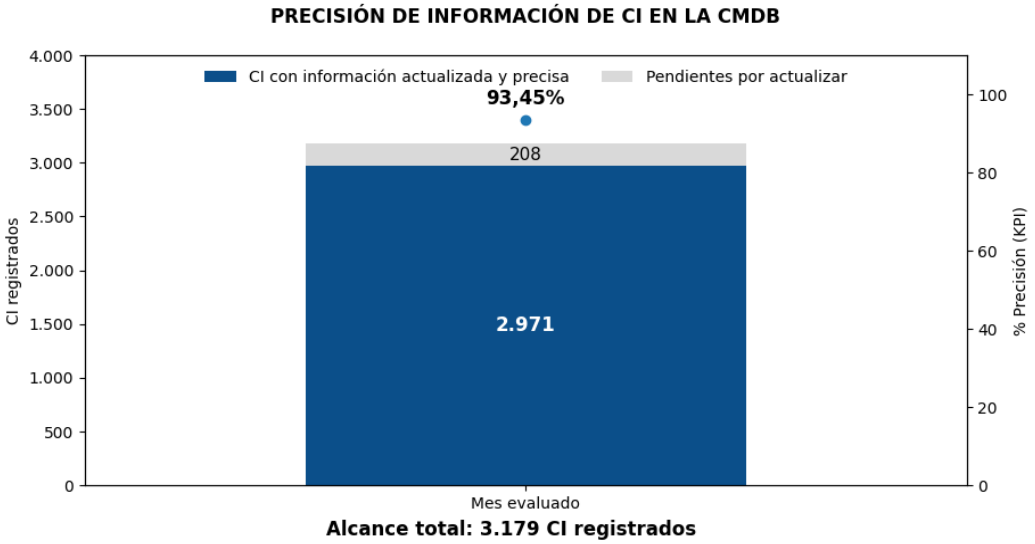


Ilustración 6 Medición de KPI Activos

Este indicador presenta una periodicidad de medición trimestral; por lo tanto, durante el presente periodo no se realizó un nuevo cálculo del KPI hasta el siguiente mes. Se mantienen los resultados obtenidos en la medición realizada en mayo, en la cual se efectuó la validación de la información registrada en la CMDB, SGU y ADM frente a los mapas de soporte físico de cada sede y la herramienta Zabbix, lo cual se verificaron 2.971 equipos, evidenciando consistencia entre la información registrada y la infraestructura física. Las actividades de validación y actualización de la información continuarán ejecutándose de manera permanente, con el fin de completar la revisión de los 3.179 equipos contemplados dentro del alcance del proyecto.

2.1.2.4. Práctica Catálogo de servicios

Durante el mes de julio, en el marco de la práctica de Catálogo de Servicios, se adelantaron actividades orientadas a consolidar y mantener una fuente única, actualizada y confiable de los servicios disponibles para el Ministerio del Trabajo, fortaleciendo la calidad de la información registrada en la herramienta de gestión, mejorando la visibilidad de los servicios

y facilitando su administración, en alineación con las necesidades de la entidad y de la operación de TI.

Como resultado de estas actividades, se actualizó y socializó la matriz de escalamiento, se creó la categoría SICIP y se optimizó el árbol de categorías de Incidentes de Seguridad de la Información, el cual fue revisado y validado con el Especialista de Seguridad Informática, garantizando su alineación con la clasificación definida en la Guía de Gestión de Incidentes de Seguridad de la Información del Ministerio de Trabajo. Adicionalmente, se gestionó el envío del caso al Líder de Herramientas, para la implementación en la herramienta de gestión Aranda de las categorías pendientes, contribuyendo a la estandarización de la clasificación de los servicios e incidentes de seguridad y al fortalecimiento continuo del Catálogo de Servicios.

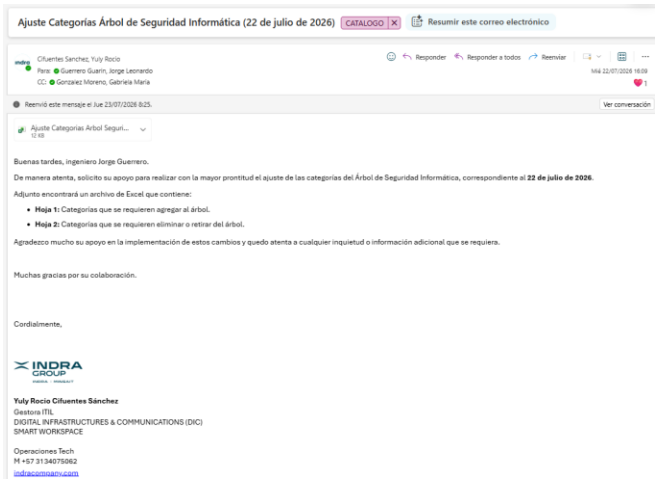


Ilustración 7 Ajuste árbol de categorías seguridad informática

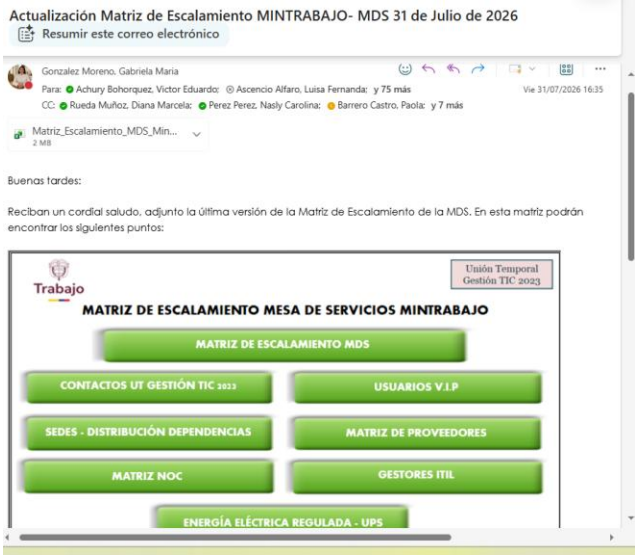
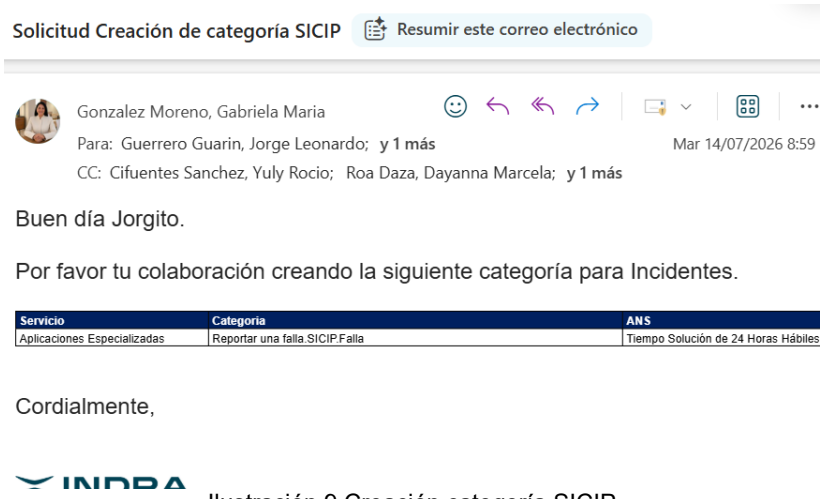


Ilustración 8 Matriz de escalamiento


Solicitud Creación de categoría SICIP Resumir este correo electrónico

Gonzalez Moreno, Gabriela Maria

Para: Guerrero Guarin, Jorge Leonardo; y 1 más Mar 14/07/2026 8:59

CC: Cifuentes Sanchez, Yuly Rocio; Roa Daza, Dayanna Marcela; y 1 más

Buen día Jorgito.

Por favor tu colaboración creando la siguiente categoría para Incidentes.

Servicio	Categoria	ANS
Aplicaciones Especializadas	Reportar una falla.SICIP.Falla	Tiempo Solución de 24 Horas Hábiles

Cordialmente,

INDRA

Ilustración 9 Creación categoría SICIP

- **Seguimiento a la categorización de casos**

Como parte de las actividades de control y aseguramiento de la calidad del Catálogo de Servicios, durante el mes de julio se realizó el seguimiento a la correcta categorización de los casos registrados en la herramienta de gestión, verificando su clasificación de acuerdo con los lineamientos establecidos.

Como resultado de este seguimiento:

- Se identificaron oportunidades de mejora en la categorización de los casos.
- Se brindó retroalimentación a los equipos responsables para corregir las inconsistencias detectadas.
- Se fortaleció la aplicación de los criterios de clasificación definidos en el Catálogo de Servicios.
- Se promovió la estandarización en el registro de la información, contribuyendo a una mayor consistencia y calidad de los datos.

Estas actividades fortalecen la confiabilidad de la información registrada, mejoran la trazabilidad de los casos y favorecen la generación de indicadores más precisos para la gestión y la toma de decisiones.

- **Medición indicador porcentaje de cumplimiento de la actualización del catálogo**

En el proceso de actualización de la Guía Operacional de la Práctica de Catálogo de Servicios, se estableció el siguiente Indicador (KPI), con el fin de establecer métricas que apoyen a la operación de los servicios TI:

Nombre	Descripción / Fórmula	Meta	Periodicidad	Resultado
Porcentaje de cumplimiento de la actualización del Catálogo	CPS=(TCG/TCE) *100 CPS: Cumplimiento en la prestación de los servicios TCE: Total de casos escalados (Recibidos) (Modificación, Agregar o Desactivar el servicio). TCG: Total de casos gestionados (Solucionados) (Modificación, Agregar o Desactivar el servicio).	90%	Mensual	100 % (2/2)

Tabla 8 KPI Práctica Catálogo de Servicios

Con el propósito de medir la oportunidad en la atención de las solicitudes relacionadas con la modificación, creación o desactivación de elementos del Catálogo de Servicios, durante el mes de julio se realizó la medición del indicador:

Durante el período se recibieron y gestionaron oportunamente las siguientes solicitudes:

- **RF-286881:** Ajuste de categorías del Árbol de Seguridad Informática.
- **RF-278086:** Creación de la categoría **SICIP** para incidentes.

Como resultado, se obtuvo la siguiente medición:

- **Total de casos escalados (TCE):** 2
- **Total de casos gestionados (TCG):** 2
- **CPS = (2 / 2) × 100 = 100 %**

El resultado alcanzado fue del **100 %**, superando la meta establecida del **90 %**. Este desempeño evidencia la atención oportuna de las solicitudes de actualización del Catálogo de Servicios y el cumplimiento de las actividades orientadas al fortalecimiento y mejora continua de la información registrada en la herramienta de gestión.

Análisis de tendencias de la Práctica de Catálogo de Servicios

Como parte del fortalecimiento de la Práctica de Catálogo de Servicios, durante el mes de julio se incorporó el análisis de tendencias del catálogo con el propósito de evaluar el comportamiento de las categorías registradas en la herramienta de gestión, identificar oportunidades de mejora y fortalecer la calidad de la información utilizada para la operación y la toma de decisiones.

Comportamiento del catálogo

Durante el período se evidenció la necesidad de actualizar y fortalecer la estructura del Catálogo de Servicios, incorporando nuevos elementos que respondieran a las necesidades operativas y permitieran una clasificación más precisa de los casos registrados. En este contexto, se realizó la creación de la categoría SICIP para la gestión de incidentes y la actualización del árbol de categorías de Incidentes de Seguridad de la Información, alineándolo con la Guía de Gestión de Incidentes de Seguridad de la Información.

Afinamientos realizados sobre las categorías

Con el fin de mejorar la calidad de la información y la confiabilidad de la volumetría e indicadores, se realizaron los siguientes ajustes:

- Actualización y socialización de la matriz de escalamiento.
- Creación de la categoría SICIP para la gestión de incidentes.
- Actualización del árbol de categorías de Incidentes de Seguridad de la Información.
- Solicitud de creación y actualización de las categorías correspondientes en la herramienta de gestión Aranda.

Variaciones identificadas

Como resultado del análisis realizado, se identificó la necesidad de fortalecer la estructura de clasificación del catálogo mediante la incorporación de nuevas categorías y el ajuste de categorías existentes, permitiendo una mayor precisión en el registro y clasificación de los casos relacionados con seguridad de la información.

Impacto en el proceso

Los ajustes implementados permiten mejorar la consistencia de la información registrada, fortalecer la trazabilidad de los casos, optimizar la generación de reportes e indicadores y facilitar el análisis de la operación, contribuyendo a una gestión más eficiente del Catálogo de Servicios.

Acciones de mejora:
Como acciones derivadas del análisis de tendencias se establecieron las siguientes:

- Continuar con la revisión periódica de las categorías del Catálogo de Servicios.
- Realizar seguimiento permanente a la correcta categorización de los casos registrados.
- Fortalecer la socialización de las actualizaciones del catálogo con los equipos de Mesa de Servicios y Soporte en Sitio.
- Verificar la implementación de las categorías aprobadas en la herramienta de gestión Aranda.
- Mantener el análisis de tendencias como un insumo para la mejora continua del Catálogo de Servicios y la optimización de la información utilizada para la gestión e indicadores.

2.1.2.5. Práctica de Problemas

Dar a conocer las actividades de la Práctica de Problemas correspondientes al periodo de julio de 2026. Este apartado contiene información relevante sobre actividades realizadas y novedades presentadas. De acuerdo con el consolidado de casos documentados durante el periodo, se realizó seguimiento a los incidentes recurrentes reportados en la mesa de servicios y a la fecha de corte no se ha identificado la necesidad de crear casos tipo problema.

Cómo parte del análisis estadístico de la práctica de problemas, a continuación, se presenta el estado de los problemas identificados:

CI afectado	# casos creados	Estado de los casos
Controlador de dominio	1	Solución definitiva - cierre
Módulo de radicación - Gestor documental	3 3 1	Error conocido Solución Temporal Solución definitiva - cierre
MINTRABGD01A - Gestor documental	1	Solución definitiva - cierre
Office 365	1	Error conocido
Página web	1	Solución definitiva - cierre
servicio de relay en el ISS	1	Solución Temporal
SISINFO	1	Solución Temporal
Telefonía	1	Solución definitiva - cierre
UPS Manizales	1	Solución Temporal
UPS sedes central	1	Investigación y diagnóstico
SD WAN	1	Solución definitiva - cierre
Total	17	

Tabla 9 Consolidado problemas identificados

Durante el mes de julio se realizó seguimiento al caso 174025 asociado con el Gestor Documental. De acuerdo con la sesión de trabajo realizada el 15 de julio se definieron las acciones que se va a adelantar:

Acciones propuestas y la nueva hoja de ruta:

- Seguimiento al caso TS022469468 registrado ante IBM responsable: Especialista IBM (el fabricante solicitó información adicional la cual será recopilada con el apoyo de Brayan para documentar el caso, dicha recopilación se realizará los días 15 y 16 de julio)
- Consecución de mesa técnica con IBM, continuar con el seguimiento a los mensajes enviados y continuar con la gestión que va adelantar la gerencia del proyecto y el especialista de IBM.

Se realizó nueva sesión de seguimiento el 31 de julio se define las acciones propuestas y la nueva hoja de ruta:

- Seguimiento al caso TS022469468 registrado ante IBM responsable: Especialista IBM (el fabricante solicitó información adicional recopilada 29 de julio) En espera de respuesta.
- Consecución de mesa técnica con IBM, continuar con el seguimiento a los mensajes enviados. Responsable: Especialista IBM

Actividades en curso

- Realización de ventana de mantenimiento de BBDD del 31 de julio al 2 de agosto. Responsable: Administrador base de datos oracle.

Postulación de problema desde la gestión de incidentes- Redes y conectividad

Derivada de la recurrencia de incidentes asociados a la indisponibilidad parcial del servicio de conectividad SD-WAN en varias inspecciones. Durante los días 08 y 09 de julio de 2026,

la herramienta de monitoreo Zabbix generó múltiples alertas sobre pérdida de comunicación en diferentes firewalls SD-WAN. Como parte del análisis técnico realizado, se verificó mediante FortiManager que los dispositivos permanecían operativos; no obstante, se evidenció afectación en la comunicación de los túneles SD-WAN.

En la investigación adelantada se revisó la configuración Dual Stack (IPv4/IPv6) implementada en la solución, identificándose como causa probable un posible defecto (bug) del sistema operativo FortiOS, relacionado con la gestión de las asociaciones de seguridad (Child SA) del protocolo IKE. El comportamiento observado consiste en que el daemon de IKE elimina la Child SA correspondiente a IPv6 del túnel principal (Dialup VPN) al establecer un VPN Shortcut, interpretando erróneamente que existe una asociación equivalente, situación que ocasiona la pérdida de conectividad.

Considerando que este comportamiento no corresponde al funcionamiento esperado del producto, el caso fue escalado al fabricante Fortinet, quedando registrado bajo el Ticket No. 11995017, el cual actualmente continúa en proceso de análisis por parte del fabricante.

Como medida de mitigación, mientras se obtiene una solución definitiva, el equipo técnico ejecuta un procedimiento de recuperación consistente en forzar la caída del VPN Shortcut desde el firewall afectado, manteniendo únicamente la comunicación con el HUB central del Data Center, lo que permite restablecer el servicio.

Dado que este comportamiento se presenta de forma intermitente y ha generado múltiples incidentes asociados a un mismo evento técnico, se considera pertinente la creación de un registro de problema, con el propósito de realizar el seguimiento correspondiente hasta la identificación de la causa raíz y la implementación de una solución definitiva .Los incidentes relacionados son los siguientes:IM-271332 – Chinácota, ,IM-270121 – Girardot,IM-271351 – Guarne,IM-270080 – Guateque,IM-271352 – Palmira,IM-272628 – Popayán,IM-271437 – Roldanillo,IM-270072 – Socorro,IM-271550 – Túquerres,IM-271587 – Túquerres,IM-271343 – Yarumal.

Dando continuidad al estado de Investigación y diagnóstico se realizó mesa de trabajo con los especialistas de redes les comparto las conclusiones de la sesión:

Causa probable: un posible defecto (bug) del sistema operativo FortiOS.
Solución temporal: ejecuta un procedimiento de recuperación consistente en forzar la caída del VPN Shortcut desde el firewall afectado, manteniendo únicamente la comunicación con el HUB central del Data Center, lo que permite restablecer el servicio.

Actividades realizadas:

- Considerando que este comportamiento no corresponde al funcionamiento esperado del producto, el caso fue escalado al fabricante Fortinet, quedando registrado bajo el Ticket No. 11995017, el cual actualmente continúa en proceso de análisis por parte del fabricante.
- Sesión técnica con Fortinet el 16 de julio de 2026, se indicaron algunas recomendaciones a seguir.

Actividades a realizar

- Deshabilitar los shortcut para que pase directamente por el hub, se propone realizar actividad el dia 17 de julio de 2026 a las 6 pm y monitorear. Esta actividad no requiere RFC dado que es un proceso para ajustar un parámetro en la configuración, se va a tomar un backup de los equipos.
- Se coordina nueva mesa técnica con Fortinet para el martes 21 de julio a las 6 pm, pendiente recibir citación.

Dando continuidad al estado de Investigación y diagnóstico se realizó mesa de trabajo con los especialistas de redes les comparto las conclusiones de la sesión:

Actividades realizadas:

- Se realizó la deshabilitación de los shortcut para que pase por el hub y no se ha presentado la creación de nuevos eventos.
- Se realizó la sesión con Fortinet y el especialista brindó orientación para revisión de documentación emitida por fabricante.

Actividades a realizar

- Se va a realizar documentación del caso en fortinet para cierre.

Dando continuidad al estado de solución temporal se realizó mesa de trabajo con los especialistas de redes les comparto las conclusiones de la sesión:

Actividades realizadas:

- No se ha presentado la creación de nuevos eventos relacionados con el problema identificado una vez se realizó la deshabilitación de los shortcut para que el pase directamente por el hub
- Se realizó la documentación del caso de fabricante y se encuentra en seguimiento si se presenta alguna novedad con el servicio

Actividades a realizar

- Se va a realizar seguimiento al caso de fortinet durante el mes de agosto de 2026

Se realiza documentación del problema en la herramienta aranda y se cierra el caso con Solución definitiva.

2.1.2.6. Práctica de Incidentes

Durante el mes, se gestionaron en la Herramienta de Gestión un total de 7.503 solicitudes a nivel general. De este total, el 10,16% %, equivalente a 762 tickets, fueron clasificados y tipificados como incidentes, de acuerdo con la categorización establecida para la operación de servicios TI.

Este volumen incluye:

- Reporte de novedades de los servicios notificados por los usuarios a través de los canales de atención dispuestos para la MDS.
- Gestión registrada por los especialistas y personal de soporte ante solicitudes recibidas en el desempeño de sus funciones.
- Alarmas generadas automáticamente por Zabbix en respuesta a eventos en la infraestructura tecnológica según la parametrización que se tiene del Case Creator en Aranda.

A continuación, se relaciona el detalle del estado de los casos:

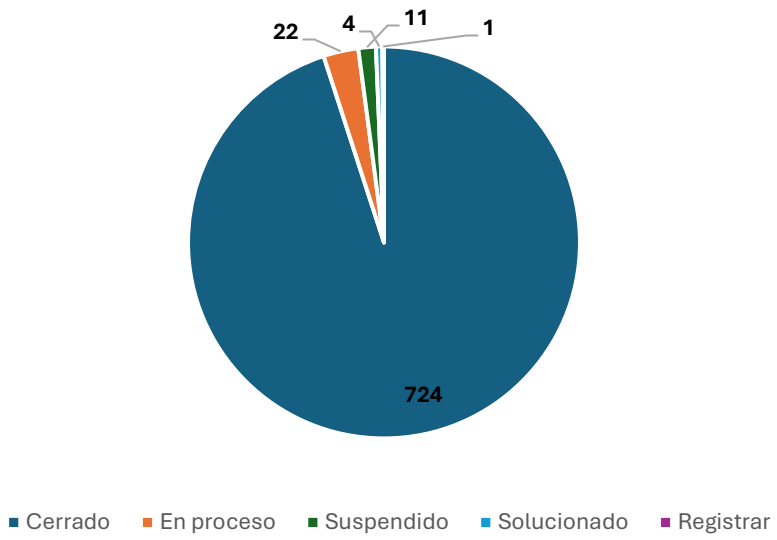


Ilustración 10 Estados Incidentes

- **Categorización de Incidentes por Servicio**

A continuación, se presenta la distribución de los 762 incidentes registrados, clasificados de acuerdo con el servicio afectado, lo que permite identificar los principales focos de impacto en la operación:

Durante el mes se registraron 762 incidentes, evidenciando una mayor concentración en el servicio de Redes y Conectividad, con 532 casos (67,34%), principalmente asociados a alarmas generadas por equipos Router (27,22%), FortiGate (15,95%), Access Point (13,29%) y Starlink (9,87%). Esta tendencia responde al monitoreo proactivo de la plataforma mediante Zabbix, lo que permitió la detección y atención oportuna de eventos de red, minimizando el impacto sobre la operación.

El servicio de Aplicaciones Especializadas representó el 17,72% de los incidentes (140 casos), concentrándose en requerimientos relacionados con el Gestor Documental, especialmente por fallas funcionales, radicación de documentos y procesos de aprobación

y radicación, lo que evidencia la necesidad de continuar fortaleciendo las acciones de mejora sobre este aplicativo.

Por su parte, Soporte Microinformática registró el 13,29% de los incidentes (105 casos), predominando las atenciones relacionadas con impresoras, equipos de cómputo, navegadores y Office 365, mientras que los servicios de Administración de Servidores (0,89%), Telefonía IP (0,38%) y UPS (0,38%) presentaron una baja incidencia, reflejando un comportamiento estable de estos componentes durante el período.

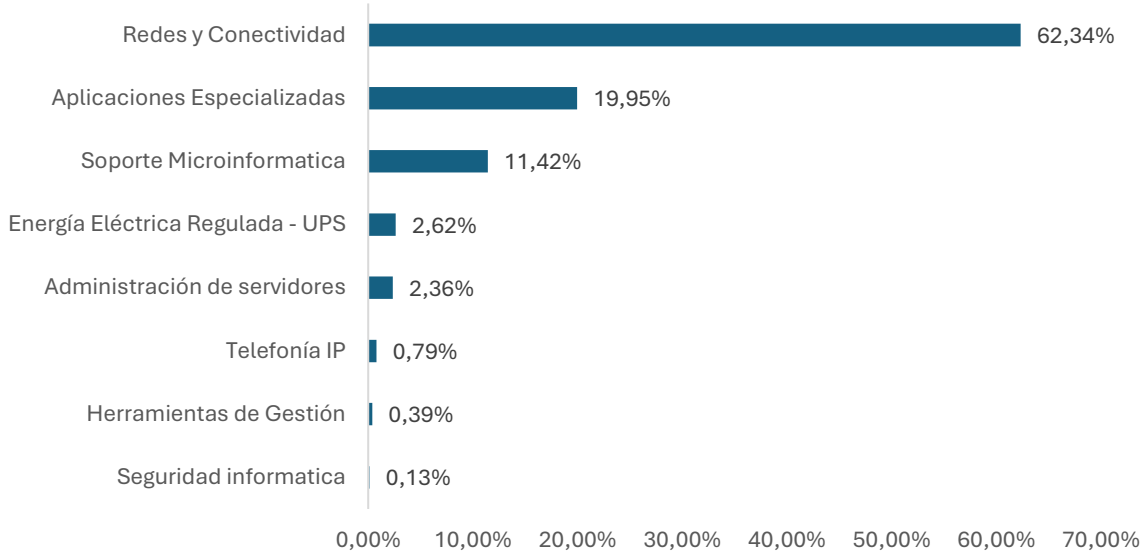


Ilustración 11 Categorización de Incidentes por Servicio

Servicio	Categoría	No	Porcentaje
Redes y Conectividad		**475**	
	Reportar una falla.Alarma Zabbix.Router	203	26,64%
	Reportar una falla.Alarma Zabbix.FortiGate	112	14,70%
	Reportar una falla.Alarma Zabbix.Starlink	111	14,57%
	Reportar una falla.Alarma Zabbix.AP	25	3,28%
	Reportar una falla.Internet.Degradacion	8	1,05%
	Reportar una falla.Alarma Zabbix.Switch	8	1,05%
	Reportar una falla.Internet.Sin servicio	3	0,39%
	Reportar una falla.LAN.Falla punto de red	2	0,26%
	Reportar una falla.Incidente Mayor	2	0,26%
	Reportar una falla.Enlace Sedes (Mlps).Lentitud enlace	1	0,13%
Aplicaciones Especializadas		**152**	
	Reportar una falla.Gestor Documental.Falla Funcional	69	9,06%
	Reportar una falla.Gestor Documental.No permite Aprobar y radicar	37	4,86%
	Reportar una falla.Gestor Documental.Falla radicación	19	2,49%
	Reportar una falla.Gestor Documental.Caida - Degradación	7	0,92%

	Reportar una falla.Gestor Documental.No permite ingresar datos	4	0,52%
	Reportar una falla.Gestor Documental.Falla error - Producir documento	3	0,39%
	Reportar una falla.Gestor Documental.Falla - Error PQRSD	3	0,39%
	Reportar una falla.Gestor Documental.Falla Error - Datacap	2	0,26%
	Reportar una falla.Gestor Documental.Lentitud gestor	2	0,26%
	Reportar una falla.Gestor Documental.Falla - Error TYS	1	0,13%
	Reportar una falla.SIRITI.Falla - Error	1	0,13%
	Reportar una falla.Incidente Mayor	1	0,13%
	Reportar una falla.Gestor Documental.No genera sticker	1	0,13%
	Reportar una falla.Gestor Documental.Falla al cargar archivos	1	0,13%
	Reportar una falla.Gestor Documental.Falla - Error ventanilla	1	0,13%
Soporte Microinformática		**87**	
	Reportar una falla.Falla impresora.Atasco	26	3,41%
	Reportar una falla.Falla impresora.No imprime	19	2,49%
	Reportar una falla.Equipo de cómputo.No enciende	7	0,92%
	Reportar una falla.Equipo de cómputo.Falla - Error conexión a red	6	0,79%
	Reportar una falla.Equipo de cómputo.Lentitud - Bloqueo	5	0,66%
	Reportar una falla.Aplicaciones Office 365.Envio y recepción de correos	4	0,52%
	Reportar una falla.Ofimatica.Falla Aplicaciones Office 365	3	0,39%
	Reportar una falla.Navegadores.Falla Cargue página web	3	0,39%
	Reportar una falla.One Drive.Error de aplicación	2	0,26%
	Reportar una falla.VPN.Falla aplicación	2	0,26%
	Reportar una falla.Navegadores.Falla - Error	2	0,26%
	Reportar una falla.Falla impresora.Impresión deficiente	1	0,13%
	Reportar una falla.Equipo de cómputo.Falla - error	1	0,13%
	Reportar una falla.Ofimatica.Falla ZIP	1	0,13%
	Reportar una falla.Escaner.No escanea	1	0,13%
	Reportar una falla.One Drive.Error sincronización	1	0,13%
	Reportar una falla.Ofimatica.Falla PDF	1	0,13%
	Reportar una falla.Navegadores.Lentitud	1	0,13%
	Reportar una falla.Ofimatica.Falla Word	1	0,13%
Energía Eléctrica Regulada - UPS		**20**	
	Reportar una falla.Alarma Zabbix. UPS	20	2,62%
Administración de servidores		**18**	
	Reportar una falla.Alarma Zabbix.Servidor Windows	17	2,23%
	Reportar una falla.Alarma Zabbix.Servidor Linux	1	0,13%
Telefonía IP		**6**	
	Reportar una falla.Servicios.No ingresan llamadas	5	0,66%
	Reportar una falla.Softphone.Falla - error	1	0,13%
Herramientas de Gestión		**3**	

	Reportar una falla.Monitoreo Zabbix.Alarma desde Zabbix	3	0,39%
Seguridad informática		**1**	
	Reportar una falla.Acceso no autorizado activos de informacion.Acceso a equipos o información no autorizado	1	0,13%
Total general		**762**	**100%**

Tabla 10 Categorización de Incidentes por Servicio

- **Top 10 de Incidentes**

Durante el período evaluado, el Top 10 con mayor número de incidentes permite identificar los componentes tecnológicos y servicios que concentraron la mayor afectación durante el período evaluado, constituyéndose en una herramienta clave para la toma de decisiones y la definición de acciones de mejora.

Los resultados evidencian que la mayor proporción de incidentes se concentra en el servicio de Redes y Conectividad, principalmente en dispositivos monitoreados mediante Zabbix, como Router, FortiGate, Starlink, Access Point (AP) y UPS. Estas jerarquías representan la mayor participación del total de incidentes, lo que refleja la criticidad de la infraestructura de comunicaciones para la operación del Ministerio. Las principales causas identificadas corresponden a fallas en el suministro de energía eléctrica, indisponibilidad o degradación de los servicios de los proveedores de telecomunicaciones, desconexiones físicas de equipos en las sedes e intermitencias de la red, factores que, en su mayoría, son de origen externo o dependen de la infraestructura tecnológica instalada en las diferentes sedes.

En cuanto al servicio de Aplicaciones Especializadas, las incidencias se concentran en el Gestor Documental, principalmente por fallas funcionales, problemas en la radicación y limitaciones para aprobar documentos. Estas situaciones impactan directamente la continuidad de los procesos administrativos y la gestión documental de la entidad, por lo que resulta necesario fortalecer el seguimiento funcional del aplicativo, la identificación de causas raíz y la implementación de mejoras orientadas a incrementar su estabilidad y disponibilidad.

Por su parte, los incidentes asociados a Soporte Microinformática corresponden principalmente a fallas en el servicio de impresión, relacionadas con atascos, desgaste de componentes y problemas operativos de los equipos. Aunque su participación porcentual es menor frente a otros servicios, estos eventos afectan la productividad de los usuarios y requieren mantener estrategias de mantenimiento preventivo y renovación gradual de equipos con mayor nivel de obsolescencia.

De manera transversal, el análisis evidencia que un porcentaje importante de los incidentes tiene su origen en factores externos, como las fallas de energía eléctrica y las afectaciones presentadas por los proveedores de conectividad. En este contexto, el monitoreo continuo mediante Zabbix ha permitido detectar oportunamente las indisponibilidades y facilitar la gestión de los incidentes para reducir los tiempos de atención y restablecimiento del servicio.

Finalmente, la información obtenida del Top 10 constituye un insumo estratégico para orientar las acciones de mejora continua, priorizando iniciativas enfocadas en fortalecer la infraestructura tecnológica, optimizar la gestión con los proveedores de telecomunicaciones, mejorar la resiliencia de la infraestructura eléctrica en las sedes,

incrementar la estabilidad de las aplicaciones críticas y consolidar esquemas de monitoreo preventivo que permitan reducir la recurrencia de incidentes y garantizar la continuidad de los servicios tecnológicos que soportan la operación del Ministerio.

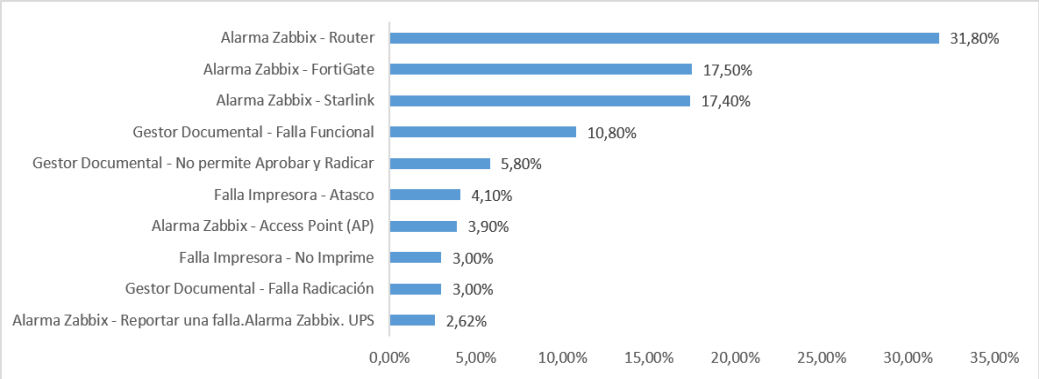


Ilustración 12 Top 10 Incidentes

Servicio	Jerarquía	Incidentes	Porcentaje	Principales causas	Análisis
Redes y Conectividad	**Alarma Zabbix - Router**	**203**	**31,80%**	Desconexión o apagado físico de equipos en sede, falla en red del proveedor y falla de energía eléctrica.	Es la jerarquía con mayor número de incidentes, reflejando la alta dependencia de la infraestructura de comunicaciones y factores externos como el suministro eléctrico y los proveedores de conectividad.
	Alarma Zabbix - FortiGate	**112**	**17,50%**	Falla de energía eléctrica.	La principal afectación corresponde a interrupciones eléctricas que impactan la disponibilidad de los dispositivos de seguridad perimetral.
	Alarma Zabbix - Starlink	**111**	**17,40%**	Desconexión física, falla en la red del proveedor, falla de energía eléctrica e intermitencia/lentitud en la red.	Las incidencias están asociadas tanto a la infraestructura local como a la disponibilidad del proveedor del servicio satelital.
	Alarma Zabbix - Access Point (AP)	**25**	**3,90%**	Bloqueo del dispositivo, desconexiones físicas, fallas eléctricas e intermitencia en la red.	Aunque representa una menor participación, persisten eventos relacionados con disponibilidad y estabilidad de la red inalámbrica.
Aplicaciones Especializadas	**Gestor Documental - Falla Funcional**	**69**	**10,80%**	Falla funcional y errores en la radicación.	Corresponde a la principal jerarquía del servicio, afectando el funcionamiento del Gestor Documental.
	Gestor Documental - No permite Aprobar y Radicar	**37**	**5,80%**	No permite aprobar y radicar, no permite ingresar datos.	Impacta directamente los procesos de gestión documental y la continuidad operativa de los usuarios.
	Gestor Documental - Falla Radicación	**19**	**3,00%**	Falla de radicación y lentitud del gestor.	Se presentan inconvenientes asociados al desempeño y procesamiento de documentos.
Soporte Microinformática	**Falla Impresora - Atasco**	**26**	**4,10%**	Atasco e impresión deficiente.	La mayor cantidad de incidentes del servicio corresponde a problemas mecánicos en impresoras.
	Falla Impresora - No Imprime	**19**	**3,00%**	No imprime y degradación del servicio.	Se evidencian fallas que afectan la disponibilidad del servicio de impresión.
Energía Eléctrica Regulada - UPS	**Reportar una falla.Alarma Zabbix. UPS**	**20**	**2,62%**	Falla de energía eléctrica.	Los incidentes registrados corresponden principalmente a interrupciones del suministro eléctrico que generan alertas sobre las UPS monitoreadas por Zabbix.

Tabla 11 Top 10 Incidentes

- **Casos Suspendidos**

A continuación, se relacionan los casos en estado suspendido y los grupos resolutores responsables

Durante el período evaluado se registraron 11 casos en estado suspendido, los cuales correspondieron a situaciones que requerían actividades externas al proceso normal de atención o dependían de terceros para su continuidad y cierre.

La distribución de los casos suspendidos fue la siguiente:

Grupo	Resultado
NOC	6
Especialistas_IBM	2
Responsable_Mesa_De_Servicio	1
Responsable_Soporte_Bogota	1
Responsable_Soporte_Territoriales	1
Total general	**11**

Tabla 12 Incidentes Suspendidos

Durante el período evaluado se registraron 11 casos en estado suspendido, de los cuales (54,55%) fueron gestionados por el NOC, principalmente debido a incidentes relacionados con la infraestructura de redes cuya resolución dependía de factores externos, como fallas de los proveedores de telecomunicaciones, interrupciones del suministro eléctrico y atención en sitio. Esto confirma que las suspensiones no obedecen a retrasos en la gestión del equipo de soporte, sino a la necesidad de esperar la intervención de terceros para restablecer las condiciones operativas.

Por otra parte, el 36,36% de los casos suspendidos se concentró en Aplicaciones Especializadas (Especialistas IBM, Responsable Mesa de Servicio y Responsable Soporte Bogotá), donde las suspensiones estuvieron asociadas a fallas funcionales del Gestor Documental, requiriendo análisis especializados, validaciones técnicas y la implementación de ajustes por parte de los equipos responsables del aplicativo.

Finalmente, el 9,09% corresponde a Soporte Microinformática, asociado a un incidente de hardware que requirió diagnóstico técnico antes de continuar con la atención.

En términos generales, el comportamiento de los casos suspendidos evidencia que las principales causas corresponden a dependencias externas (proveedores de conectividad, suministro eléctrico y soporte especializado), por lo que se recomienda fortalecer el seguimiento a terceros, establecer acuerdos de escalamiento más ágiles y mantener el monitoreo permanente para reducir los tiempos de suspensión y mejorar la oportunidad en el restablecimiento de los servicios.

- **Incidentes Mayores**

Durante el período se gestionaron tres (3) Incidentes Mayores, de los cuales dos (67%) estuvieron asociados al servicio de Redes y Conectividad y uno (33%) a Aplicaciones Especializadas. Los incidentes de conectividad fueron ocasionados por fallas en la infraestructura de los proveedores de telecomunicaciones, mientras que el incidente del Gestor Documental se originó por una degradación del rendimiento de la plataforma tecnológica. En todos los casos se activó el proceso de atención de Incidentes Mayores, coordinando las acciones entre los equipos técnicos y los proveedores hasta lograr el restablecimiento de los servicios y minimizar el impacto sobre la operación del Ministerio.

Incidente Aranda	Fecha/Hora	Asunto	Acciones realizadas durante la atención del incidente	Causa raíz	Usuarios afectados
IM-278423	15/07/2026 8:00	Incidente Mayor – Falla en la radicación del Gestor Documental	Se reiniciaron los servidores virtuales WASND y los WEBAPP para liberar recursos, se realizó la limpieza de las colas de procesamiento y se verificó el restablecimiento del servicio de radicación.	Degradación del rendimiento de la plataforma tecnológica que soporta el Gestor Documental.	Usuarios a nivel nacional que realizaban procesos de radicación documental.
IM-281722	21/07/2026 9:14	Incidente Mayor – Degradación del servicio de Internet a nivel nacional	Se realizaron pruebas de conectividad, monitoreo de la plataforma SD-WAN, validación de la infraestructura de red, escalamiento al proveedor Cirion y seguimiento hasta la normalización del servicio.	Falla en un componente de la infraestructura del proveedor de telecomunicaciones.	Funcionarios y contratistas de las Direcciones Territoriales a nivel nacional.
IM-286692	24/07/2026 8:26	Incidente Mayor – Caída del servicio de Internet Zona Norte	Se desplegaron cuadrillas para la reparación de la fibra óptica, se realizaron trabajos de empalme y reconstrucción de cableado, nivelación de potencias ópticas y validación de la estabilidad de los enlaces.	Afectación física sobre la infraestructura de fibra óptica del proveedor, ocasionada por múltiples cortes en la red troncal.	Funcionarios y contratistas de las sedes de la Zona Norte del país.

Tabla 13 Incidentes mayores

- **Medición Indicador Porcentaje de efectividad en resolución de Incidentes de servicio y Porcentaje de Incidentes Reabiertos en el Periodo**

De acuerdo con lo definido en el procedimiento de la Práctica de Incidentes, se establecieron los siguientes Indicadores (KPI), con el fin de establecer métricas que apoyen a la operación de los servicios TI:

Nombre	Descripción / Fórmula	Meta	Periodicidad	Resultado
Porcentaje de efectividad en resolución de Incidentes de servicio.	EF=(IFS/IFR) *100 EF: Efectividad en solución de Incidentes. IFS: Incidentes solucionados que cumplen el ANS en el período. IFR: Incidentes registradas en el período.	80%	Mensual	EF=742/762*100 EF= 97,38%
Porcentaje de Incidentes Reabiertos en el Periodo	RRP: Porcentaje de casos Reabiertos en el periodo. IFR: Incidentes Reabiertos en el período. IFS: Incidentes solucionadas en el período.	<2%	Mensual	RRP=1/728*100 RRP= 0,14%

Tabla 14 Medición de KPIs

A continuación, se relaciona el histórico de los resultados de los KPI de la Práctica de Incidentes:

- Efectividad de resolución de Incidentes

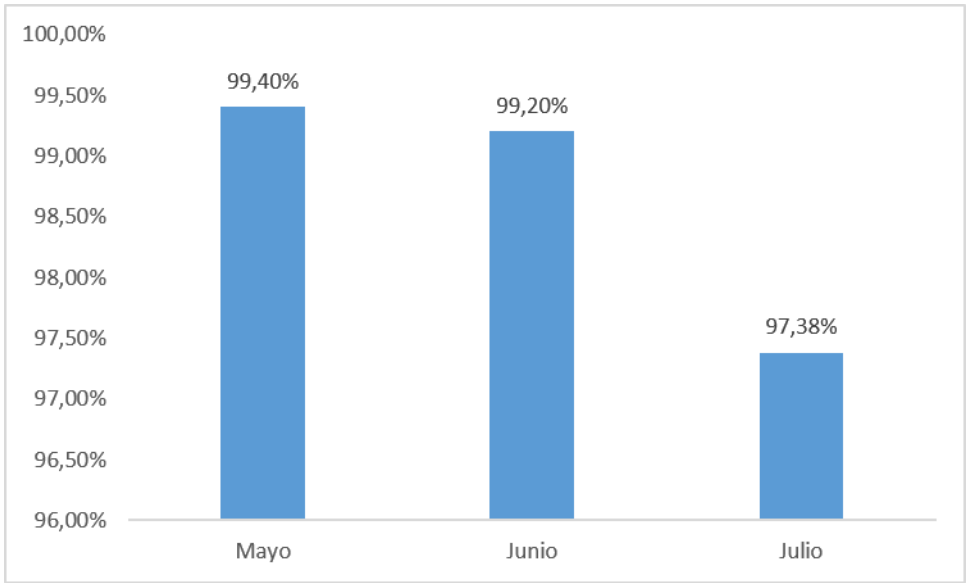


Ilustración 13 Efectividad de resolución de incidentes

El comportamiento histórico del KPI de la Práctica de Gestión de Incidentes evidencia un desempeño estable y consistente durante el trimestre, alcanzando niveles de cumplimiento superiores al 97% en todos los meses evaluados. Los resultados obtenidos fueron 99,40% en mayo, 99,20% en junio y 97,38% en julio, reflejando una gestión eficiente en la atención y resolución de los incidentes reportados.

Si bien en el mes de julio se presenta una variación frente a los meses anteriores, el indicador se mantiene en un nivel de desempeño alto, evidenciando la capacidad operativa de los equipos para gestionar oportunamente los incidentes, incluso en un período en el que se registraron eventos de mayor complejidad e impacto, como los Incidentes Mayores asociados a la infraestructura de conectividad y a las aplicaciones críticas.

Los resultados alcanzados demuestran la efectividad de los procesos de monitoreo, escalamiento y coordinación entre los equipos técnicos y los proveedores de servicio, permitiendo mantener la continuidad operativa y minimizar el impacto sobre los usuarios finales.

En este contexto, se continuará fortaleciendo las actividades de seguimiento preventivo, el análisis de tendencias y la gestión de causas recurrentes, con el propósito de mantener la estabilidad de los servicios, optimizar los tiempos de atención y asegurar el cumplimiento de los niveles de servicio establecidos contractualmente.

El comportamiento del indicador confirma la madurez de la Práctica de Gestión de Incidentes, manteniendo un desempeño superior al 97% durante el período

evaluado y evidenciando una gestión orientada a la continuidad del servicio, la atención oportuna de las incidencias y la mejora continua de los procesos operativos. Este resultado refleja el compromiso del equipo de soporte con la calidad del servicio y el cumplimiento de los acuerdos establecidos con el Ministerio de Trabajo.

- Porcentaje de incidentes reabiertos

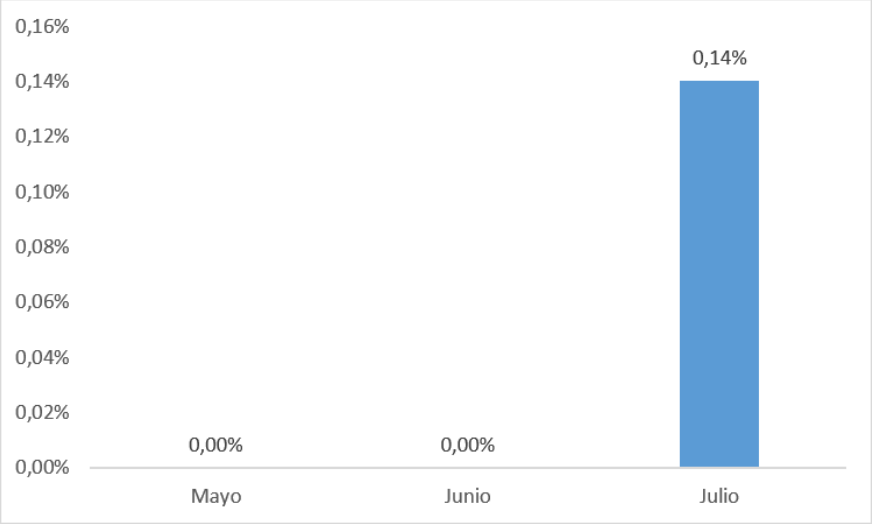


Ilustración 14 Porcentaje de incidentes reabiertos

Durante el período evaluado, el indicador Porcentaje de Incidentes Reabiertos presentó un comportamiento favorable, registrando un 0,00% en los meses de mayo y junio, lo que evidencia que los incidentes fueron resueltos de manera efectiva y cerrados con la validación correspondiente, sin requerir reaperturas.

En julio, el indicador registró un 0,14%, correspondiente a la reapertura de un único incidente (IM-291546). La reapertura se realizó como parte del proceso de validación de la causa de la afectación. Inicialmente, la indisponibilidad se asoció a un evento en el suministro de energía; sin embargo, una vez se obtuvo la confirmación del soporte en sitio, se determinó que la interrupción del servicio obedecía a la desconexión programada de los equipos por actividades de traslado, información que no estaba disponible al momento del cierre inicial.

La reapertura permitió actualizar la causa real del incidente y garantizar la trazabilidad y calidad de la información registrada, asegurando que el cierre definitivo reflejara las condiciones reales de la afectación.
El comportamiento del indicador evidencia un alto nivel de calidad en la gestión de incidentes, manteniendo un porcentaje de reaperturas prácticamente nulo durante el período analizado. La única reapertura registrada respondió a un proceso de validación técnica y actualización de la causa raíz, más que a una solución inefectiva del incidente.

Este resultado demuestra el compromiso de los equipos de soporte con la mejora continua, la precisión en el registro de la información y el cumplimiento de las buenas prácticas de Gestión de Incidentes, garantizando que cada caso sea documentado y cerrado con información técnica validada.

- **Acciones de Fortalecimiento del Proceso de Gestión de Incidentes de Seguridad**

En el marco del fortalecimiento de la Gestión de Incidentes de Seguridad de la Información y en cumplimiento de los lineamientos establecidos por la Oficina TIC del Ministerio de Trabajo, durante el período evaluado el equipo de Procesos adelantó actividades orientadas a la implementación y alineación del proceso con la política, el procedimiento y la guía institucional para la gestión de este tipo de incidentes.

Como parte de las actividades desarrolladas, se ejecutaron las siguientes acciones:

- Se realizó la revisión y validación del árbol de categorías de Incidentes de Seguridad de la Información, verificando su alineación con la clasificación definida en la Guía de Gestión de Incidentes de Seguridad de la Información.
- Se efectuó la validación funcional de la estructura de categorías en conjunto con los responsables técnicos, garantizando su consistencia para la implementación en la herramienta de gestión Aranda.
- Como siguiente actividad, la Dirección de proyectos remitirá la propuesta de categorías y ajustes a la Oficina TIC para su revisión y aprobación. Una vez se cuente con el visto bueno, se dará continuidad al proceso mediante la socialización con las áreas y partes interesadas pertinentes, con el fin de facilitar la apropiación de los lineamientos, asegurar la correcta utilización de las nuevas categorías en la herramienta de gestión y fortalecer el proceso de Gestión de Incidentes de Seguridad de la Información.

2.1.2.7. Práctica de Requerimientos

Dar a conocer las actividades de la Práctica de Requerimientos correspondientes al mes de julio de 2026. Este apartado contiene información relevante sobre los requerimientos generados en el periodo de medición, las actividades realizadas y novedades presentadas.

- En total se registraron 5369 casos tipo requerimiento quedando en los siguientes estados:

Estado	Casos
Cerrado	5163
Solucionado	6
Suspendido	134
En proceso	66

Tabla 15 Estados de Requerimientos

- Durante el mes, se realizaron seguimiento a las tareas de los flujos automatizados de devolución de equipos para traslados en sede y cambio de equipos y Roles.

Por lo anterior, se generaron 1350 tareas, las cuales fueron gestionadas en los siguientes estados:

Estado	Task
Asignada	117
Finalizada	1233

Tabla 16 Estados de Tareas de requerimientos

- Durante el mes, se presentó (1) caso en estado anulado por duplicidad.
- Realizando el seguimiento del Backlog de los casos suspendidos, en la siguiente tabla se observa el avance de atención los casos en este estado desde el periodo anterior al actual.

Grupo Responsable	Junio	Julio
SOC	6	3
Responsable_de_Energia Eléctrica Regulada - UPS	1	0
Gestor de Inventarios	0	1
Especialista Nube Privada	1	2
Especialista Base de datos	1	1
Especialistas IBM	3	8
Responsable Garantías Equipos	7	18
Responsable_de_Servidores_Windows	3	3
Responsable_Mesa_de_Servicio	30	59
Responsable_Soporte_Bogotá	21	15
Responsable_Soporte_Impresoras	1	6
Responsable_Soporte_Territoriales	7	17
Especialista Nube Publica	1	1
Total por Periodo	**83**	**134**

Tabla 17 Seguimiento del Backlog Suspendidos

En el inicio del período, se identificaron 83 casos suspendidos correspondientes al backlog del mes de junio de 2026, lo cual se presenta un aumento de solicitudes este periodo de 51 casos suspendidos respecto al mes anterior. Sin embargo, el 67% de las suspensiones de julio (91 de 134 casos) se concentra en responsable Mesa de Servicio (59 casos) y Responsable Soporte en Sitio (32 casos), los cuales se identifican por espera por usuario por procesos de inactivación de usuarios, devolución de equipos y traslados de sede o cambio de rol de los funcionarios.

De los casos generados como requerimientos, a continuación, se relaciona el top 10 de la jerarquía con mayor solicitud:

Solicitud	Casos
Radicar una solicitud.Directorio activo.Inactivar usuario	1196
Radicar una solicitud.Impresora.Cargue de papel en impresora	507

Radicar una solicitud.Alarma Zabbix.Impresora	380
Radicar una solicitud.Directorio activo.Cambiar contraseña	229
Radicar una solicitud.Directorio activo. Creación de usuario	229
Radicar una solicitud.Impresora.Aumento de cuota	207
Radicar una solicitud.Equipo de computo.Traslado de Sede, Cambio Equipo o Rol	205
Radicar una solicitud.Gestor documental.Asignar Radicado TYS	191
Radicar una solicitud.Gestor documental.Relanzamiento	182
Radicar una solicitud.Impresora.Instalacion - Configuracion	165

Tabla 18 Top 10 de Solicitudes

- En el TOP 10 de solicitudes, se evidencia que las categorías con mayores solicitudes son solicitud Inactivar usuario con 1196 tickets, cargue de papel en impresora con 507 tickets, Alarma Zabbix de Impresora con 380 tickets y Cambiar contraseña con 229 tickets.
- Se realizó seguimiento a requerimientos en backlog, enviando correos a los especialistas para la documentación y cierre de casos pendientes.
- Se realizó en conjunto con la Practica de activos el afinamiento de tareas automáticas en flujo de inactivación de usuario y traslado de sede, lo cual, se elimina la tarea de backup de MDS y se adiciona tarea de acta de traslado para actualización de ubicación, con el fin de la optimización de los procesos y tiempos de respuesta.
- Desde la Práctica de ITIL se realizan auditorias de casos en los que se evidencian oportunidades de mejora, compartidas por correo a los especialistas a quienes se les hace retroalimentación, con base en las novedades encontradas en cada ticket durante este periodo.

Nombre	Descripción / Fórmula	Meta	Periodicidad	Resultado del Periodo
Porcentaje de efectividad en resolución de Requerimientos de servicio.	**EF=(RFS/RFR) *100**	80%	Mensual	**EF=** 5347/5369 *100
	EF: Efectividad en solución de Requerimientos.			
	RFS: Requerimientos solucionados que cumplen el ANS en el período.			**EF= 99,59%**
	RFR: Requerimientos registradas en el período.			
Porcentaje de Requerimientos Reabiertos en el Periodo	**RRP:** Porcentaje de casos Reabiertos en el periodo.	<2%	Mensual	**RRP=** 10/5169*100
	RFR: Requerimientos Reabiertos en el período.			**RRP= 0,08%**
	RFS: Requerimientos solucionadas en el período.			

Tabla 19 Detalle de KIP Practica de Requerimientos

A continuación, se relacionan el histórico de los resultados de los KPI de la Práctica de Requerimientos:

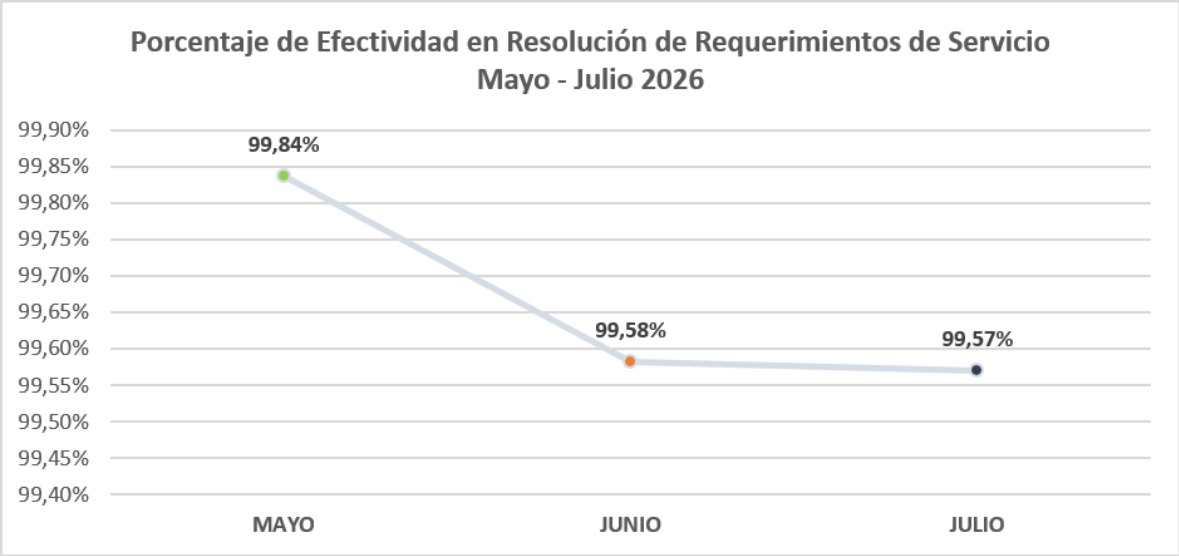


Ilustración 15 KPI Efectividad de Resolución de Requerimientos de Servicio

Durante el periodo comprendido entre mayo y julio de 2026, el indicador de efectividad en la resolución de requerimientos presentó un comportamiento estable y superior al 99,5%, evidenciando un alto nivel de cumplimiento en la atención y cierre de las solicitudes de servicio alcanzando el 99,57%, manteniendo un desempeño prácticamente estable respecto al mes anterior y confirmando la capacidad del proceso para sostener altos niveles de efectividad en la gestión de los requerimientos.

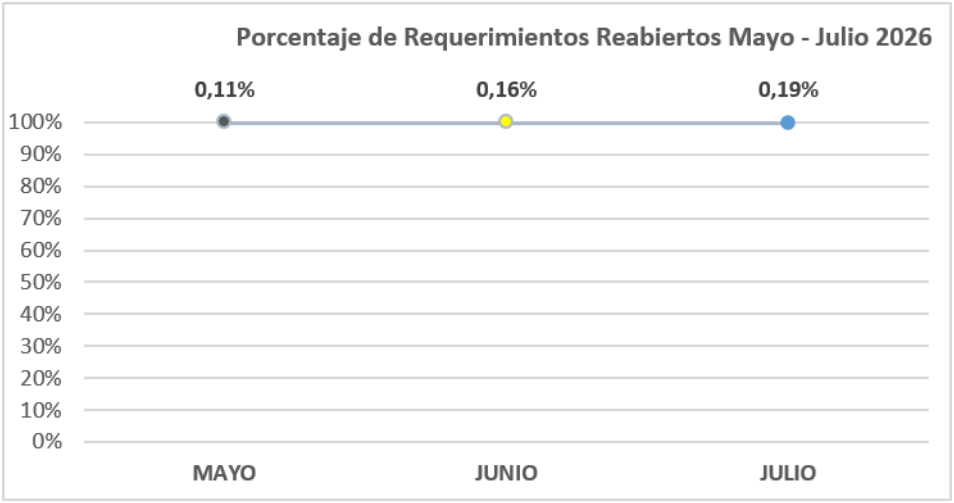


Ilustración 16 Requerimientos de Reabiertos en el periodo

Durante el mes de julio de 2026 se gestionaron 5.169 requerimientos de servicio, de los cuales 5.159 casos (99,81%) fueron resueltos satisfactoriamente sin necesidad de reapertura, mientras que únicamente 10 casos (0,19%) requirieron ser reabiertos pasando de 0,16% a 0,19%, este comportamiento continúa dentro de niveles aceptables del KPI y no representa una afectación significativa en la prestación del servicio, lo cual significa que el 99,5% de los requerimientos fueron resueltos correctamente sin necesidad de ser reabiertos, demuestran la estabilidad de la operación, el compromiso de los equipos de

soporte y la efectividad de los controles implementados para garantizar soluciones oportunas y de calidad.

Se presentaron siete (10) casos reabiertos que se encuentra en estado cerrado, la reapertura del caso se debió a la necesidad de ampliar la información de solución entregada por el especialista. A continuación, se relaciona el estado del caso por requerimiento y grupo responsable:

No. Caso	Descripción de la Solicitud	Grupo Responsable	Causa	Atención al Caso
RF-288005	Radicar una solicitud.Correo Electronico.Configuracion	Responsable Mesa de Servicio	Usuario solicita la ampliación saldo de impresión	Se realizó la revisión del caso, evidenciando que corresponde a un caso informativo, dado que se indica que la solicitud fue solucionada mediante el caso RF-286813. No obstante, el Agente de Mesa de Servicio aplicó de manera incorrecta el estado "Solucionado", motivo por el cual fue necesario completar el proceso y posteriormente reabrir el requerimiento. En consecuencia, se llevará a cabo la respectiva retroalimentación con el agente, con el fin de reforzar el procedimiento adecuado para la gestión y cierre de los casos.
RF-280108	Radicar una solicitud.Equipo de computo.Devolución de equipo (portátil o PC)	Gestor de Inventarios	Se realiza la devolución del equipo asignado al funcionario, correspondiente a un equipo portátil marca Lenovo, modelo ThinkBook 14 G6.	Se realizó la devolución del equipo portatil, lo cual se adjunto el acta de devolución y se procedio solucionar por parte del Soporte en sitio, lo cual al revisar, debia ser validado con el gestor de inventarios, lo cual se procedio a reaperturar el caso para confirmar la devolución, actualización y estado del activo. Por lo anterior, se procederá a reañlizar la retroalimentación al Soporte en Sitio
RF-273873	Radicar una solicitud.Garantía.Equipo Periférico	Responsable Garantías Equipos	Solicita revisión y garantía de diadema	Se recibe requerimiento por parte de la funcionaria debido a que la diadema asignada no reproduce audio, lo que impide su uso para las actividades laborales. Se solicita gestionar la garantía correspondiente en caso de evidenciar falla de hardwar, lo cual se procede al cambio y se soluciona por parte del Soporte en Sitio pero debia ser validado con el gestor de inventarios, lo cual se procedio a reaperturar el caso para confirmar la devolución, actualización y estado del activo. Por lo anterior, se procederá a reañlizar la retroalimentación al Soporte en Sitio
RF-268693	Radicar una solicitud.Gestor documental.Asignacion - Modificacion Roles	Especialistas_IBM	Solicito que en el gestor documental del funcionario, se habilite el módulo de gestión entrada planillas	Se realizó la gestión por parte del especialista, quien informó que el usuario ya podía hacer uso del módulo. Sin embargo, al validar con la Mesa de Servicio, se confirmó que el usuario aún no tenía acceso al módulo de Planillas. Ante esta situación, el especialista efectuó una nueva revisión en el Gestor Documental, realizando los ajustes correspondientes, tras lo cual se confirmó que el usuario ya podía acceder correctamente al portal.

RF-268740	Radicar una solicitud.Gestor documental.Asignar Radicado TYS	Especialistas_IBM	Solicita la usuaria direccionar un radicado a Bogotá a su nombre en el Gestor documental	Se solicita de manera urgente el traslado de un radicado a su nombre, ya que indica es urgente la asignación, por lo cual en varias ocasiones se le ha informado a la usuaria que la solicitud se encuentra asignada al usuario jmancera. Sin embargo, por esta única ocasión procederemos a trasladarla a su cargo, teniendo en cuenta que se requiere su atención con carácter urgente. Es importante recordar que es responsabilidad de la persona que tiene asignada la solicitud realizar el traslado o la reasignación al área o usuario competente cuando corresponda.
RF-268780	Radicar una solicitud.Gestor documental.Asignar Radicado TYS	Especialistas_IBM	Usuario informa presenta falla en el Gestor Documental PQRSDcon el radicado 02EE2026410600000072413	Se solicita con carácter urgente la revisión de la falla presentada en el radicado 02EE2026410600000072413. En atención al requerimiento, el especialista realiza la validación correspondiente e identifica que el error se debe a la alta transaccionalidad de la plataforma del Gestor Documental. Por tal motivo, se solicita al usuario intentar nuevamente el proceso. Sin embargo, el usuario informa a la Mesa de Servicios que la novedad persiste, ya que la primera página del documento continúa descargándose en blanco. Ante esta situación, el especialista realiza nuevamente la descarga del documento, verifica que el archivo se encuentra correcto y adjunta la evidencia correspondiente en Aranda. Posteriormente, indica al usuario que ingrese nuevamente al portal y acceda a su bandeja de trabajo para continuar con el proceso, confirmando con ello la solución de la incidencia y procediendo al cierre del caso.
RF-258765	Radicar una solicitud.Gestor documental.Relanzamiento	Especialistas_IBM	Solicitud de Relanzamiento del radicado 02EE2025410500000108131	Se solicita el relanzamiento del radicado 02EE2025410500000108131. En atención al requerimiento, el especialista realiza la validación correspondiente en el Gestor Documental, evidenciando que dicho radicado no existe en la plataforma, por lo que informa esta novedad al usuario. Posteriormente, el usuario aclara que la solicitud se origina debido a que, al intentar realizar el procedimiento de PQRSD, la bandeja de trabajo asignada aparece vacía, lo que considera un error del sistema. Tras el análisis del caso, se informa al usuario que la novedad no corresponde a un inconveniente del Gestor Documental, sino que debe ser validada internamente por la entidad, ya que no se evidencia ninguna inconsistencia técnica asociada al radicado reportado. Con esta aclaración, se da por solucionado el caso.

RF-259083	Radicar una solicitud.Gestor documental.Relanzamiento	Responsable_Soporte_Bogota	Solicito el relanzamiento del radicado 05EE2026232000000074543 del 18/06/2026 que no se encuentra en la bandeja de trabajo del funcionario.	Se solicita el relanzamiento del radicado 05EE2026232000000074543, lo cual se revisó el caso por el especialista indica esde el soporte de Gestor Documental, no es posible realizar la asignación o el relanzamiento del radicado mencionado. El proceso correcto es que el usuario con el rol de "Jefe de Asignación" realice la debida asignación o reasignación de los casos en mención, al recibir esta respuesta el funcionario envia un correo frente a su inconformidad, se reabre el caso para aclararle al funcionario En atención a su solicitud, informamos que desde el área de Soporte no es posible realizar la asignación de radicados internos, ya que este proceso corresponde al jefe de asignación de cada dependencia, con el fin de garantizar la trazabilidad de la gestión. Por lo anterior, se recomienda revisar el procedimiento descrito en el campo Solución, donde se explica el proceso que deben seguir para realizar la reasignación correspondiente y así podrá ver el registro en su bandeja y se da por solucionado el caso.
RF-278495	Radicar una solicitud.Gestor documental.Relanzamiento	Especialistas_IBM	Solicitud arreglo y relanzamiento del Radicado No.13EE2026712000100002169	Se solicita el relanzamiento del radicado 13EE2026712000100002169. En atención al requerimiento, el especialista realiza la validación correspondiente y habilita nuevamente el radicado para su gestión, informando al usuario que puede revisar nuevamente su bandeja de trabajo. Posteriormente, el usuario confirma que el radicado ya se encuentra disponible; sin embargo, reporta una nueva novedad durante el proceso de remisión al grupo de Archivo Sindical. Indica que, en la comunicación intermedia dirigida a las empresas, el sistema no generó el radicado ni el documento en formato PDF. Asimismo, informa que no se habilitó nuevamente la opción de Aprobar y Radicar y que, al seleccionar el botón Continuar, el proceso permanece en el mismo estado sin permitir avanzar. Ante esta situación, el especialista realiza una nueva revisión del caso, efectúa los ajustes requeridos y adjunta en Aranda la evidencia de la modificación realizada. Finalmente, solicita al usuario intentar nuevamente el procedimiento, confirmando la solución de la incidencia y procediendo con el cierre del caso.

RF-288097	Radicar una solicitud.Software adicional.Asesoria - Consulta	Responsable_Mesa_De_Servicio	Usuario indica presenta un problema con el ingreso de la Pagina COMFAMA	a usuaria reporta inconvenientes para acceder a la página de COMFAMA, indicando que presenta restricciones que le impiden el ingreso. Inicialmente, se le informa que la solicitud se encuentra relacionada con el caso RF-288109, debido a que el sitio web consultado no es administrado por el Ministerio. Posteriormente, la usuaria manifiesta su inconformidad con la respuesta recibida, indicando que esta no corresponde a la solicitud realizada, ya que en ningún momento requirió un restablecimiento de contraseña, sino la habilitación de los permisos necesarios para acceder a la página, debido a las restricciones de navegación existentes. En atención a lo anterior, se informa que la novedad continúa siendo gestionada mediante el caso relacionado, en el cual se realizan las configuraciones y habilitaciones de permisos correspondientes. Adicionalmente, el equipo especialista efectúa varios intentos de contacto con la usuaria para realizar las pruebas de validación; sin embargo, no fue posible establecer comunicación. Finalmente, los especialistas del SOC solicitan a la usuaria realizar las verificaciones correspondientes y, en caso de que la novedad persista, responder a través del mismo medio adjuntando la evidencia del error presentado, con el fin de confirmar si aún existe algún inconveniente asociado a la configuración realizada.

Tabla 20 Casos reabiertos

2.1.2.8. Práctica de Eventos

Durante el mes de julio de 2026, el Centro de Operaciones de Red (NOC), a través del Centro de Diagnóstico y Operaciones (CDO), realizó el monitoreo permanente de la infraestructura tecnológica del Ministerio del Trabajo, ejecutando actividades de supervisión, análisis y gestión proactiva de los eventos generados por la plataforma de monitoreo.

Como resultado de esta gestión se atendieron 509 eventos, manteniendo el seguimiento oportuno sobre la infraestructura tecnológica y contribuyendo a la continuidad de los servicios de TI.

La distribución de los eventos evidencia que los Routers continúan siendo el componente con mayor número de incidencias, con 205 eventos (40%), principalmente asociados a fallas en el suministro de energía eléctrica, desconexiones físicas de los equipos e incidencias en los servicios de telecomunicaciones.

Los dispositivos FortiGate y las Antenas Starlink registraron 113 eventos cada uno (22%), consolidándose como las categorías con mayor volumen de alertas después de los Routers. En ambos casos, la principal causa corresponde a interrupciones del suministro eléctrico, seguidas por desconexiones manuales realizadas en las sedes y eventos de intermitencia en horarios no laborales.

En los Servidores Windows se gestionaron 41 eventos (8%), registrando un incremento frente al mes anterior, principalmente por alertas de consumo elevado de disco y memoria. En contraste, los Servidores Linux presentaron únicamente 2 eventos (0,39%), manteniendo un comportamiento estable durante el periodo.

Por su parte, los Access Point registraron 25 eventos (5%), reflejando una disminución respecto al mes anterior, mientras que los Switches presentaron 10 eventos (2%), manteniendo una baja participación dentro del total de incidencias.

En términos generales, el comportamiento de los eventos confirma que la principal causa de indisponibilidad continúa siendo la inestabilidad del suministro eléctrico en las sedes, especialmente en aquellas ubicadas en zonas apartadas del país, seguida por las desconexiones manuales de los equipos realizadas como medida preventiva por parte del personal en sitio.

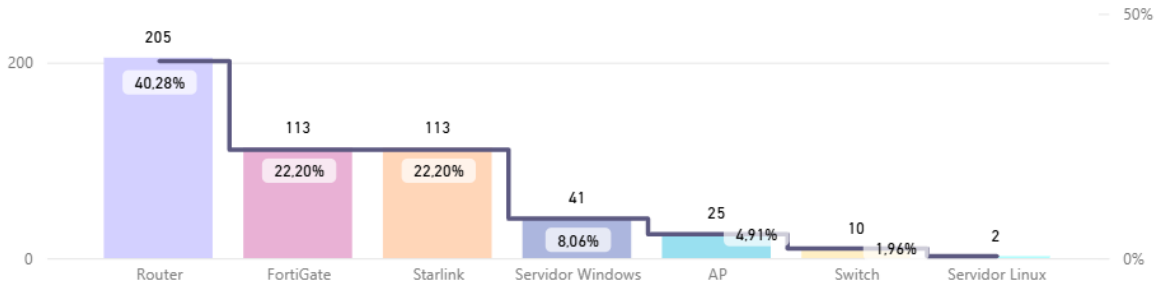


Ilustración Resumen eventos

Incidentes por Categoría de Servicio

A continuación, se presenta un desglose por categoría de las incidencias gestionadas durante el mes de julio por el equipo del NOC, en el marco de las actividades de monitoreo de estado y atención de incidentes sobre la infraestructura tecnológica del Ministerio del Trabajo. La gestión realizada abarca la supervisión proactiva y la resolución de eventos asociados a componentes de red e infraestructura informática, con el objetivo de garantizar la continuidad operativa y mantener los niveles de servicio establecidos.

Redes y conectividad

- **Routers**

Desde el centro de operaciones NOC durante el mes de julio se gestionaron 189 incidentes relacionados con equipos de red Routers en diferentes sedes a nivel nacional, los cuales representaron el 42% de los casos.

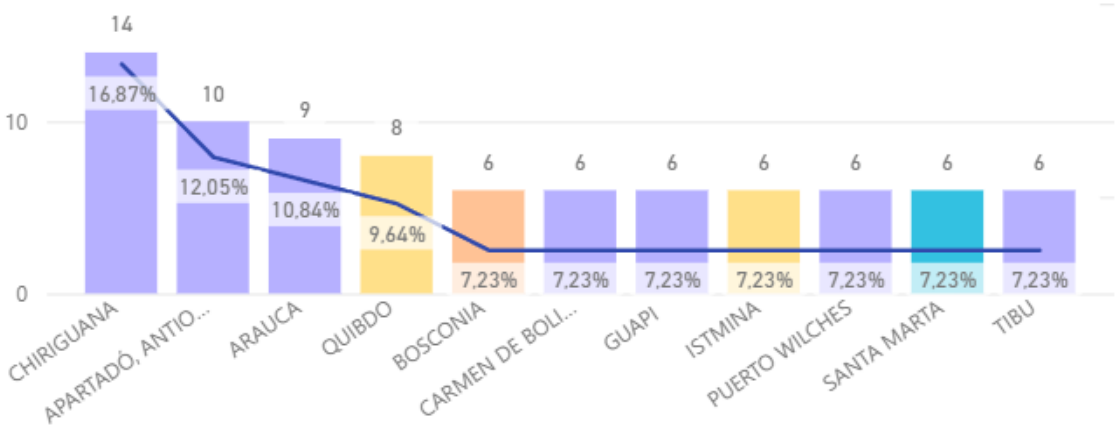


Ilustración Top10 Sedes afectadas por router

- Chiriguana encabeza el top 10, ya que durante el mes de julio los funcionarios han decidido apagar los dispositivos al finalizar su jornada laboral, lo cual ocasiona que más del 80% de los casos estén registrados como desconexiones, seguido de fallas eléctricas.
- En este mes sedes como Apartado, ocupa el segundo lugar, el cual tiene presencia en el TOP desde el mes de mayo, debido a que se presentaron fallas eléctricas durante el mes, sin embargo, para Julio, se evidencia que la sede reporta desconexión física de los dispositivos, siendo esta causa el 80% de los casos reportados.
- Arauca ocupando en julio el tercer lugar, aunque su presencia es intermitente, este es el segundo mes consecutivo dentro del TOP10, esta sede refleja una incidencia relacionada a fallas eléctricas e intermitencias en el servicio, lo cual puede estar relacionada a intermitencias o bajones eléctricos.
- Quibdó a pesar de bajar en el top, ocupando el cuarto lugar, su presencia mes a mes es indiscutible debido a sus múltiples fallas eléctricas lo cual representa más del 70% de los casos reportados.
- Como en el último año, la sede Bosconia sigue apareciendo en el TOP 10, en esta oportunidad ocupando el puesto quinto por desconexiones físicas en sus dispositivos de red.
- En quinto puesto igual que Bosconia, encontramos a Carmen de Bolivar, Guapi, Istmina, Puerto Wilches, Santa Marta y Tibú, identificando con mayor incidencia falla de energía eléctrica presentando un 61% y desconexión de equipos representando un 8%. De las sedes ubicadas en el quinto lugar, Carmen de Bolivar, Puerto Wilches y Tibú son las únicas sedes que presentan reportes a proveedor, con un máximo de 2 casos.

Causas de eventos generados por router

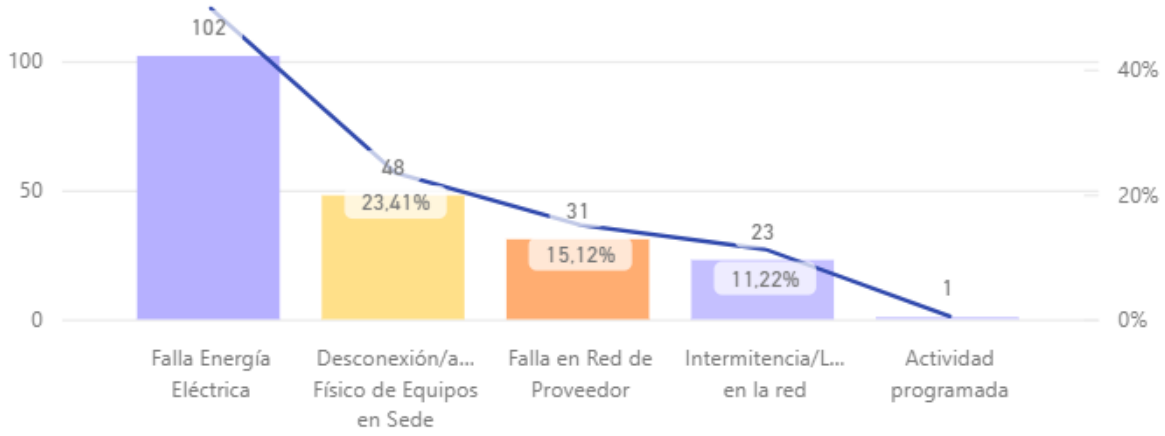


Ilustración Causas de eventos generados por router

- Se evidencia que la causa principal del total de eventos para la categoría de Routers es por Falla Energía Eléctrica ocupando el primer lugar con 102 casos (49,7%), seguido de Desconexión/apagado Físico de Equipos en sede con 48 casos (23%), en tercer lugar, encontramos Fallas en Red de Proveedor con 31 casos (15%), en cuarto lugar, se evidencia Intermitencia/Lentitud en la red con 23 casos (11%) y para finalizar encontramos con 1 caso la causa de Actividad Programada (0.49%).
- Se evidencia un aumento en la cantidad de casos relacionados a proveedores de internet, también se evidencia aumento en casos como intermitencias y desconexión física de equipos en comparación con el mes anterior.
- Las fallas por energía eléctrica representan el 49% de los casos, afecta principalmente a zonas remotas o sin tecnología de respaldo como Chiriguana, Apartado, Quibdó, Bosconia, Guapi, Istmina, Riohacha, entre otras, donde la red eléctrica es inestable o está sujeta a cortes constantes. En muchos casos, las sedes no cuentan con sistemas de respaldo energético (UPS, generadores o paneles solares y banco de baterías), lo que provoca apagones completos de la infraestructura de red. Recomendación crítica: Priorizar la implementación de UPS en sedes con alta recurrencia de fallas eléctricas para garantizar la continuidad del servicio y reducir alarmas innecesarias.
- El 15% de los casos están relacionados a Falla en Red de Proveedor, siendo Carmen de Bolivar y Puerto Wilches las sedes con mayor número de eventos registrados por esta causa. Por esta causa registran 3 casos en estado suspendido y a espera de RFO por parte de ETB.
- El 23% de los casos están relacionados a desconexión apagado físico de equipos en sede, siendo Chiriguana, Apartado y seguida por Bosconia, las sedes que registran mayor cantidad de eventos para esta categoría, los cuales son ocasionados porque los funcionarios apagan los equipos al salir

de turno con el fin de prevenir la afectación de los dispositivos por picos altos en el servicio de energía.

- El 11% de los casos están asociados a Intermitencia/Lentitud en la red, este tipo de incidencias se concentra en regiones con interrupciones del servicio de energía o en la red de datos de proveedor, sin embargo, estas se han registrado en su mayoría en horario no hábil y las cuales no han durado más de 15 a 30 minutos activas. Las sedes con esta incidencia no reportan más de 2 casos asociados a esta causa, a excepción de Arauca, esta sede reporto 4 incidencias relacionadas a intermitencias.

Estado de los casos Router

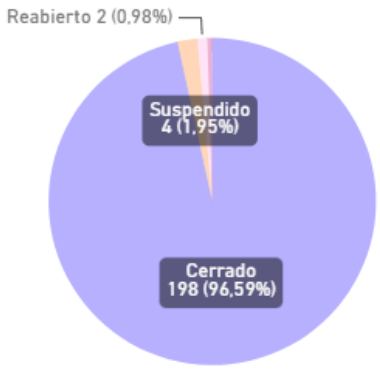


Ilustración Casos suspendidos VS. Casos solucionados/Cerrados de Router

Se evidencia que del total de eventos generados (205) para la categoría de Routers durante el mes de Julio; registran entre cerrados y solucionados representan el 96,59% (198), 4 casos en estado suspendido (1.95%) y 2 casos en estado Reabierto (0.98%).

- Los casos suspendidos corresponden a sedes como
  - Popayan, se encuentra en traslado de sede, razon por la cual los dispositvos estan apagados.
  - Magangue, presenta fallas con la red y esta en revisión por parte del proveedor
  - Fundación, presenta alertas, sin embargo no se conoce la causa, se esperan descartes de primer nivel.
  - Carmen de Bolivar, presenta fallas con la red y esta en revisión por parte del proveedor
  - Sincelejo (2 casos), presenta fallas con la red y esta en revisión por parte del proveedor

- **Switches**

Desde el Centro de Operaciones (NOC), durante el mes de julio se generaron 10 casos referentes a Switches en la herramienta de monitoreo Zabbix en diferentes sedes, los cuales representan el 1.96% del total de los casos, donde se evidencia un aumento de casos en comparación con el mes pasado.

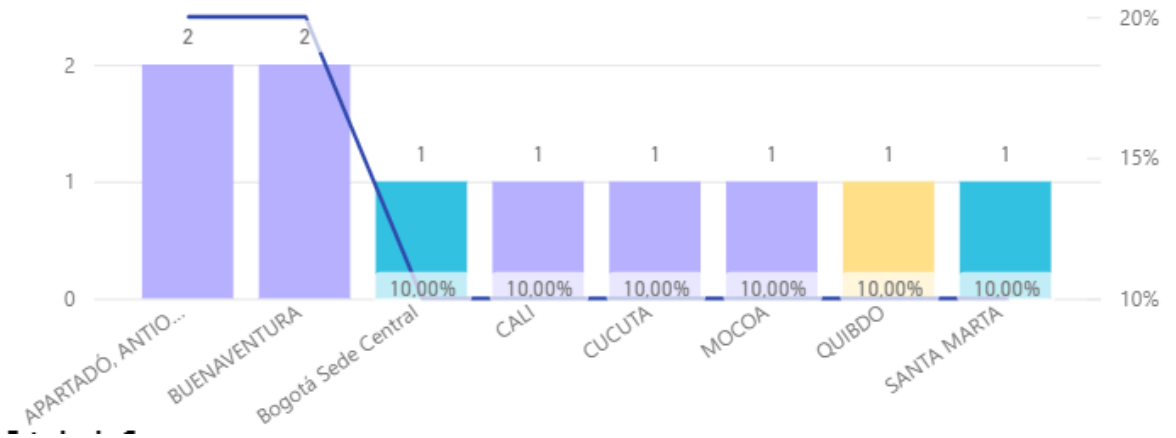


Ilustración Sedes afectadas por Switch

- Los 10 casos registrados en esta categoría, están relacionados a fallas de energía eléctrica con un 60% de las incidencias reportadas, seguido de intermitencias con un 30% de los casos y desconexión física de equipos con un 10%.
- Se evidencia que la mayor cantidad de los casos reportados en esta categoría se registraron en las sedes de Apartado y Buenaventura con 2 casos cada una, 5 de esos 6 casos relacionados a fallas eléctricas y solo 1 caso de Santa Marta relacionado a intermitencias.

Causa de eventos generados por Switch

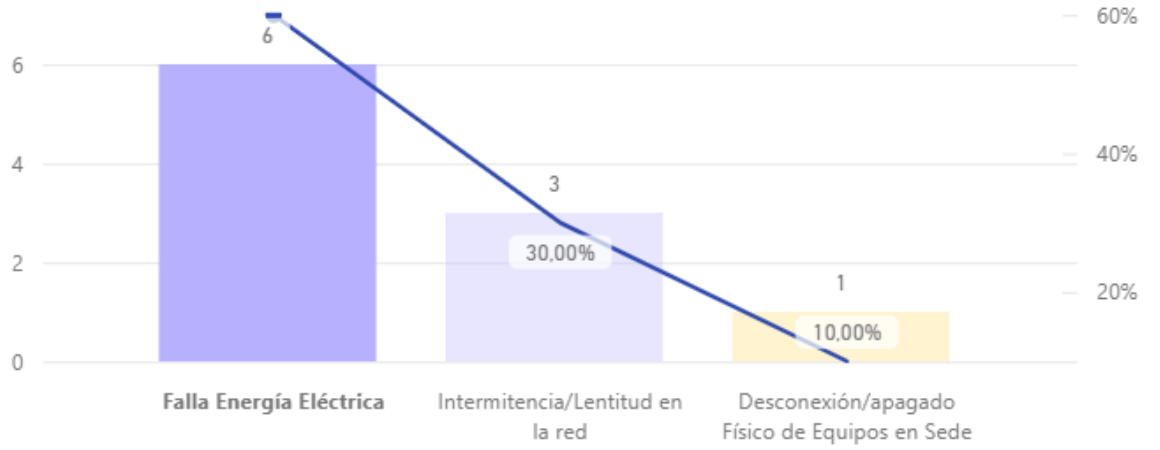


Ilustración Causa de eventos generados por Switch

- Se registra que fallas de energía eléctrica representa el 60% (6 casos), donde cada sede reporta solo 1 caso.
- Buenaventura, es la sede que reporta 2 casos (66%) relacionados a intermitencia.
- Apartado es la única sede que reporta desconexión física de dispositivos a nivel de Switchs con 1 solo caso.
- Esta distribución refuerza nuevamente el patrón observado en otros tipos de dispositivos: la inestabilidad del suministro eléctrico es el factor predominante que impacta la disponibilidad de la infraestructura de red, incluso en equipos pasivos como los Switchs.

Estado de los casos switch

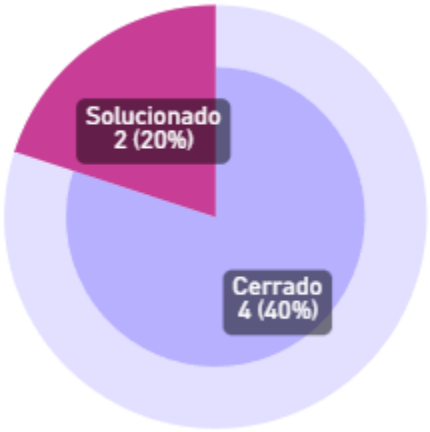


Ilustración Casos suspendidos VS. Casos solucionados de Switch

De los 10 eventos registrados para la categoría de Switches en el mes de julio, los 10 registran en estado cerrado o solucionado, cumpliendo de esta manera el 100% de los casos gestionados por parte del centro de operaciones NOC.

- **Access Point**

Desde el Centro de Operaciones (NOC), durante el mes de julio se gestionaron 25 incidentes asociados a equipos de red WLAN – Access Point en distintas sedes a nivel nacional, los cuales representan el 4.91% del total de casos reportados. Estos eventos fueron abordados dentro de los niveles de servicio establecidos, sin afectación crítica a la operación general de la red.

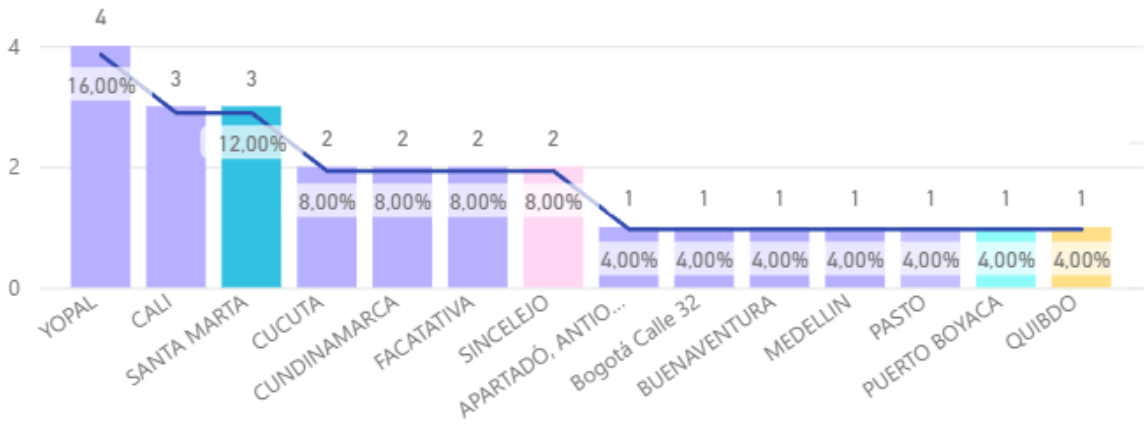


Ilustración Sedes afectadas por Access Point

- Para este mes ser observa una disminución de casos a comparación del mes anterior, sin embargo, se evidencia de igual forma que la causa por falla eléctrica también subió de forma considerable, posicionándose en el TOP 1 en las causas.
- Las sedes más afectadas por AP son Yopal posicionándose en el puesto #1 del TOP, presenta eventos relacionados a desconexión física de equipos con 2 casos, actividades programadas y fallas en energía eléctrica con 1 caso cada una.
- Cali y Santa Marta posicionándose en el puesto #2, reporta 3 eventos cada una, relacionados a fallas de energía eléctrica, intermitencia en la red con el 50% de los eventos y bloqueo de dispositivos.
- Cucuta, Cundinamarca, Facatativá y Sincelejo, se ubican en el puesto #3, estas sedes reportan el 50% de los casos como fallas de energía eléctrica, seguido por intermitencia en la red con un 25% y desconexión física de equipos con otro 25%.
- A pesar de que solo tienen un 1 y una representación del 4% cada una, sedes como Apartado, Bogotá Calle 32, Buenaventura, Medellin, Pasto, Puerto Boyacá y Quibdó, también reportan fallas eléctricas en sus AP.

Causa de eventos generados por AP

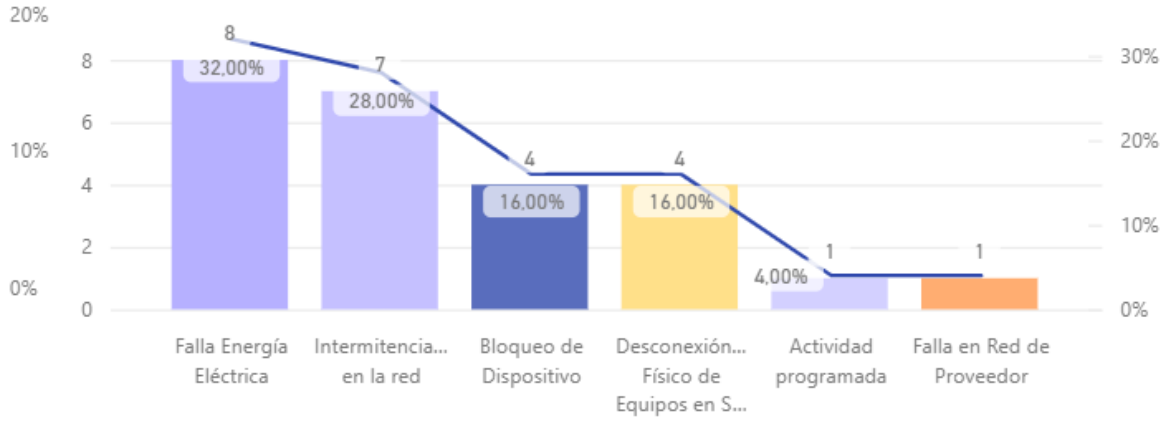


Ilustración Causa de eventos generados por AP

- Para este mes se evidencia una disminución importante en la cantidad de incidencias relacionadas a fallas de energía eléctrica, sin embargo, esta sigue siendo la causa #1 en AP con un 32%.
- Intermitencia en la red duplicado su cantidad de casos para Julio, aumento 4 puntos, representando el 28% de las causas en el mes.
- La causa de bloqueo de dispositivos mantiene su cantidad de eventos registrados, con un 16%, las sedes que se ven afectadas por esta falla so Cali, Bogotá Calle 32, Buenaventura y Puerto Boyacá, con 1 caso cada una.
- La causa desconexión física de equipos tiene una considerable disminución de hasta el 70% de los casos en comparación con el mes anterior, afectando sedes como Yopal y Sincelejo con 2 casos casa una.
- Para finalizar este TOP encontramos actividad controlada y falla en red de proveedor relacionadas a las sedes como Yopal y Santa Marta, siendo la primera la sede con más casos.

Estado de los casos AP

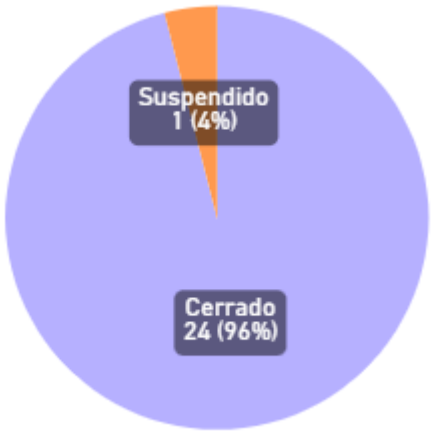


Ilustración Casos suspendidos VS. Casos solucionados de AP

Según lo registrado de los 25 eventos generados por Access Point durante el mes de julio con relación a los casos suspendidos VS. Casos cerrados, se evidencian los 24 casos en estado cerrado, representando el 96% de gestión de casos, por otro lado, contamos con 1 caso aun en gestión para esta categoría, debido a que este AP se desconectó de manera física en la sede y se espera que el funcionario retorne a sitio.

- **Starlink**

Desde el centro de operaciones NOC durante el mes de julio se gestionaron 113 incidentes relacionados con equipos de red Starlink en diferentes sedes a nivel nacional, los cuales representan el 22% del total de los casos.

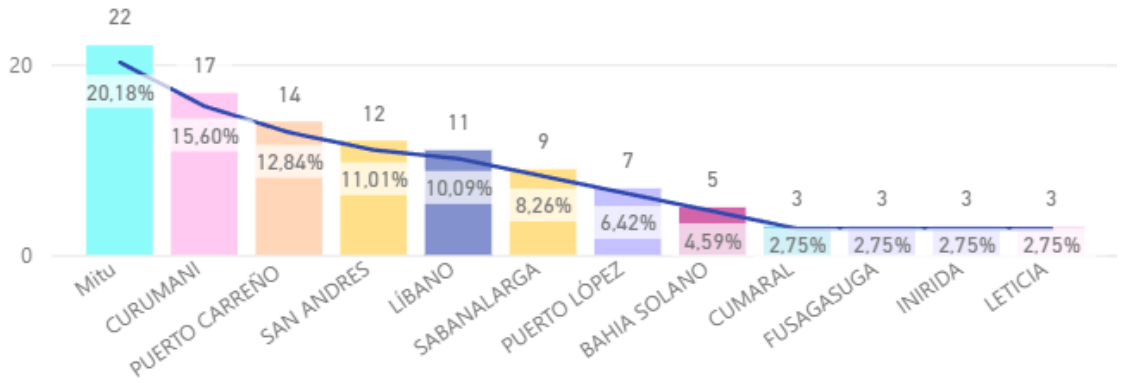


Ilustración Top 10 Sedes afectadas por Starlink

- Para el mes de julio el TOP 10 de las sedes con mayor número de eventos generados para la categoría de Starlink fueron Mitu con 22 eventos, la cual sube en el TOP 1 por segunda vez, siendo la sede en la que mas se evidencian diferentes fallas eléctricas con un 69%, ya sea por tormentas, mantenimientos o incluso por la misma infraestructura de la sede, a pesar de que también se evidencian otro tipo de fallas, estas se dividen en concentraciones más bajas.
- La sede Curumani en el TOP 2, reporta hasta 58% de los casos relacionados a desconexión física de los equipos, seguida de fallas en la energía eléctrica con un 35%.
- La sede en el TOP 3 Puerto Carreño, la cual se evidencia en los primeros lugares mes a mes, por sus múltiples fallas eléctricas o desconexión de dispositivos.
- En el TOP 4 se encuentra San Andrés, siendo la primera vez que esta sede está en los primeros 5 lugares del TOP esta, sede que destaco por las fallas eléctricas presentadas durante el mes, seguida de intermitencias en el servicio.
- Líbano, se queda en el TOP 5 con desconexiones físicas de equipos con un 90%.

- En el TOP 6, 7 y 8 encontramos las sedes como Sabana Larga, Puerto López y Bahia Solano, donde se evidencia que el 66% de los casos corresponden a desconexión física de equipos.
- Finalizando el top con la misma cantidad de eventos 3 casos cada una, encontramos sede como Cumaral Fusagasugá, Inírida y Leticia donde no difieren mucho de las demás sedes reportando fallas eléctricas y desconexiones.

Causa de eventos generados por Starlink

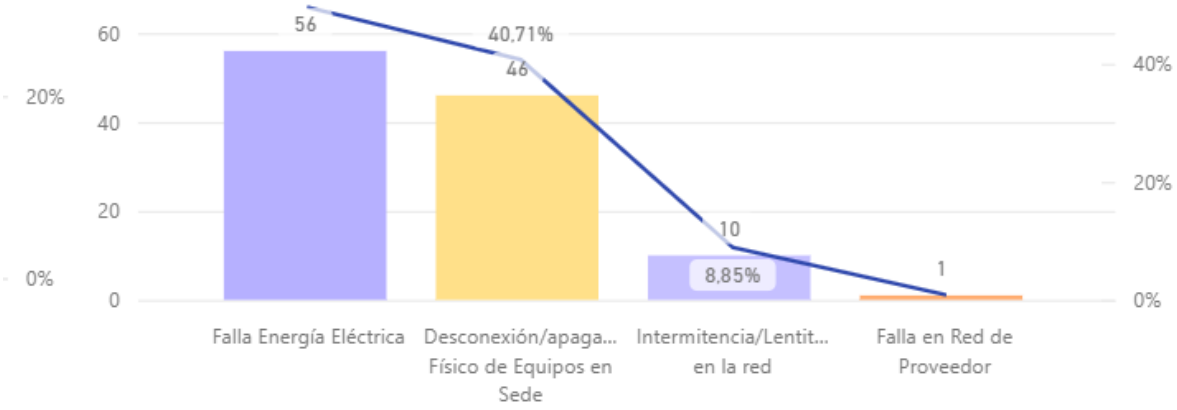


Ilustración Causas de eventos generados por Starlink

- Las fallas relacionadas a energía eléctrica sigue siendo la causa número uno en el TOP, para este mes representa un 49,5% de los casos relacionados al CI Starlink, se ha evidenciado que las zonas más remotas del país son las más afectadas, ya sean por tormentas, lluvias, mantenimientos, daños de terceros, racionamiento o hasta por falta de pago; siendo la sede Puerto Carreño la más afectada en el dia a dia, esta sede en los últimos meses ha ocupado el TOP 1, Mitu, Bahia Solano, Líbano, Puerto Carreño y Puerto López, a pesar de que varían en la posición, han estado presente en el TOP 10 el último año. por esta razón, consideramos importante que se contemple la posibilidad de sistemas de respaldo en estas sedes.
- La desconexión de equipos de manera física para este mes muestra un aumento de casos, sin embargo, sigue ocupando la posición 2 en el TOP, con una representación del 40%, correspondiente a 46 eventos. A pesar de que es una práctica conocida entre los funcionarios la desconexión de los dispositivos no siempre es recomendable, razón por la cual se recomienda la opción de estabilizadores en las sedes, con el objetivo de evitar picos de voltaje y evitar eventos.
- En el TOP 3, la causa de intermitencias o lentitudes con un 8.8%, a pesar de que han disminuido esta causa sigue afectando sedes como Puerto Carreno, Inírida, Mitu, entre otras, con alarmas no superiores a 30 minutos y mínimo de 15 minutos.

- Al final del TOP, en la posición 4, encontramos falla en red del proveedor, con solo 1 evento afectando la sede Mitu.

Estado de los casos Starlink

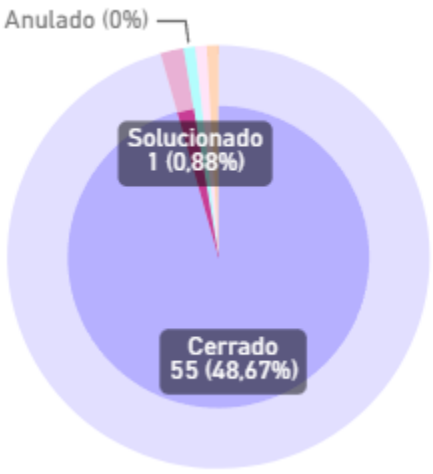


Ilustración Casos suspendidos VS. Casos solucionados de Starlink

Según lo registrado se evidencia que los casos suspendidos VS. Casos solucionados o cerrados del total de los 113 eventos registrados para la categoría Starlink durante el mes de julio, se reportan que el 98% de los casos fueron solucionados y el 3% (2 casos) se encuentra pendiente en estado suspendido, esperando los resultados de las revisiones de soporte en sitio.

- **FortiGate**

Desde el centro de operaciones NOC durante el mes de julio se gestionaron 113 incidentes relacionados con equipos de red FortiGate en diferentes sedes a nivel nacional, los cuales representaron el 22% del total de los casos, ocupando el segundo lugar.

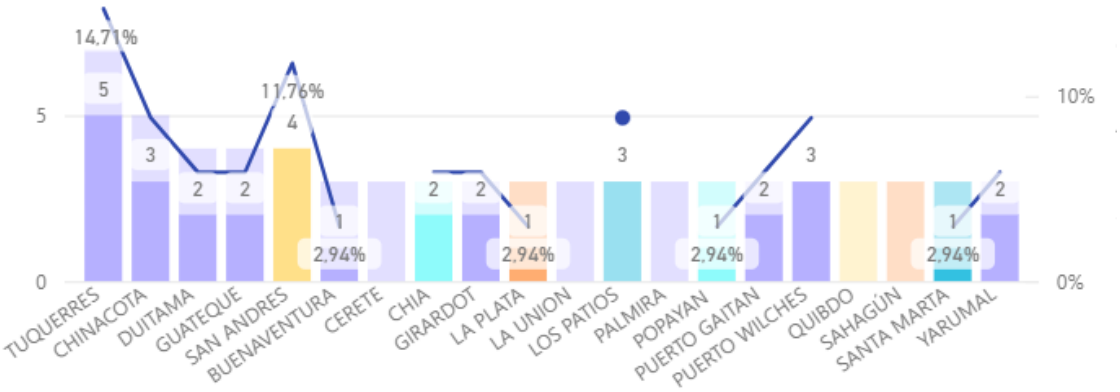


Ilustración Sedes afectadas por FortiGate

- En comparación con el mes anterior, la categoría de FortiGate subió la cantidad de casos en un 15%.
- Tuquerres la sede con los casos reportados 7 eventos, se posicionar en primer lugar, siendo la primera vez en el último semestre que se observa esta sede encabezando el top. Los eventos se relacionan a fallas de energía eléctrica con el 70% y el 30% relacionados a intermitencias.
- En el segundo lugar con 5 eventos, se evidencia la sede Chinácota, esta sede siempre está presente en el TOP 10, con altas incidencias relacionadas a fallas de energía eléctrica.
- En el tercer lugar con 4 casos cada una encontramos sedes como Duitama, Guateque y San Andrés, sedes que también se ven afectadas principalmente por fallas con energía eléctrica.
- En cuarto y último lugar del TOP con 3 casos cada una, encontramos sedes como Buenaventura, Cerete, Chia, Girardot, La plata, La unión, Los Patios, Palmira, Popayán, Puerto Gaitan, Puerto Wilches, Quibdó, Sahagun, Santa Marta y Yumaral, a pesar de que estas sedes no tienen muchos casos, la incidencia también reporta un número considerable de afectaciones por falla eléctrica, lo cual refuerza más el planteamiento de una solución de respaldo para la red eléctrica de las sedes.

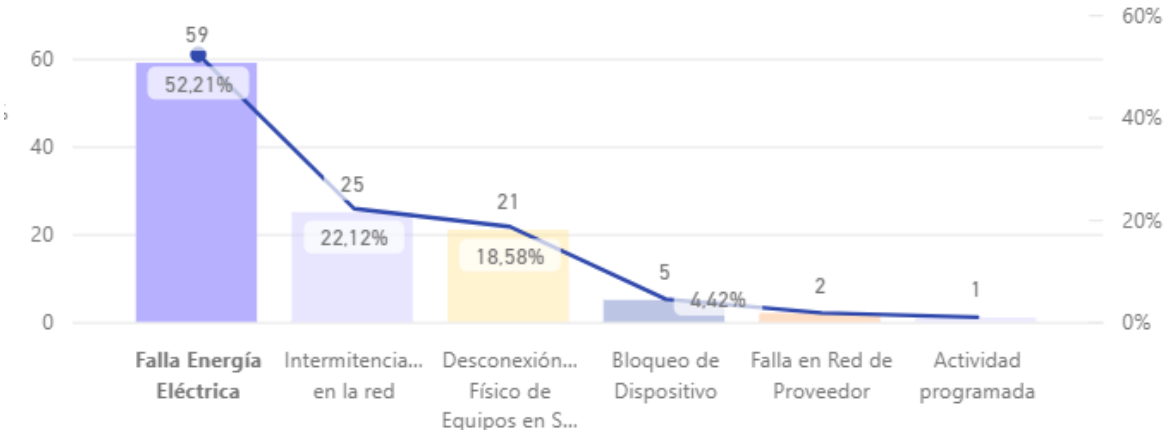


Ilustración Causas de eventos generados por FortiGate

- Durante el mes de julio, los dispositivos SD-WAN presentaron una tasa alta en cuanto a la causa de fallas en energía eléctrica, representando más de la mitad de los casos con un 59%, teniendo una leve disminución este mes, siendo la sede Tuquerres la mas afectada por este tipo de fallas, seguida de San Andrés.
- Intermitencia y/o lentitud continua estable con una baja incidencia con 25 casos, representando un 22%; siendo Quibdó la sede mas afectada por este tipo de fallas.

- Desconexión o apagado de equipos se observa un aumento menor de eventos registrados; con el 18% del total de los casos para esta categoría, los funcionarios en sede, se manera manual realizan la desconexión de los dispositivos, con el fin de evitar, según ellos, fallas en el servicio o daños en los equipos por picos de energía que se puedan presentar durante el horario no hábil. Para este tipo de eventos, Sahagun es la sede con más indecencias seguida de La Plata.
- Bloqueo de dispositivos para este mes aumento 5 casos, representando un 4.4% del total, siendo Duitama y Popayán las sedes mas afectadas.
- Por otro lado, la causa de falla en red de proveedor se mantiene estable y relativamente baja en comparación con meses anteriores, con 2 casos lo cual representa solo el 1.77% de las fallas, es importante resaltar que esta disminución se debe a los ajustes que se han realizado con la reporteria de Zabbix junto con Aranda.
- Para finalizar encontramos la sede de Puerto Gaitan, con 1 evento relacionado a Actividad Programada.

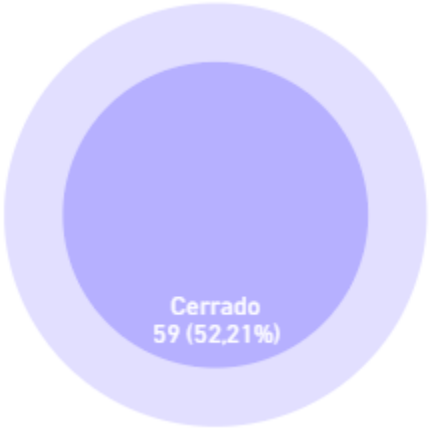


Ilustración Casos suspendidos VS. Casos solucionados de Fortigate

De los 113 eventos reportados en el mes, se evidencia que el 100% de los casos se encuentran en estado cerrado, mostrando así una buena gestión por parte del NOC y el personal en sitio que realiza el apoyo con las revisiones.

- **Casos Escalados a Proveedor de Telecomunicaciones**

Durante el mes de julio se registraron 30 casos que fueron escalados y gestionados con proveedor ETB y TIGO de los cuales quedan 28 (93%) que registran en estado solucionado o cerrado y 2 (7%) en estado suspendido, en proceso o en espera de RFO.

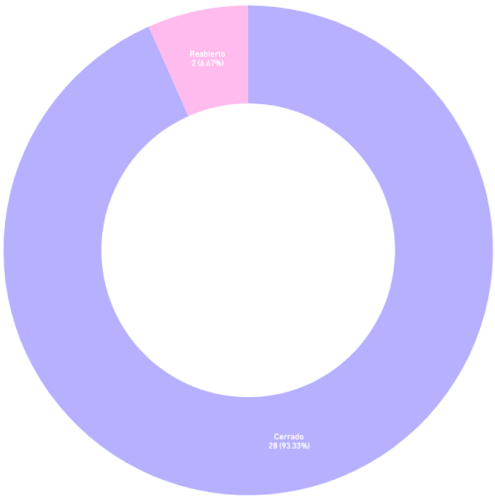


Ilustración Estado de casos escalados a Proveedor

- El caso en Aranda IM-291548 y IM-291546 se relaciona al servicio principal y de respaldo de la sede Sincelejo, ambos proveedores de servicio es ETB, quien asocio estas caídas a una falla de alto impacto, en la cual se encuentran trabajando para corregir errores.

Servicios centrales

- **Servidores Windows**

Durante julio, el Centro de Operaciones de Red (NOC) gestionó 41 eventos asociados a servidores Windows, equivalentes al 8% del total de casos registrados durante el mes.

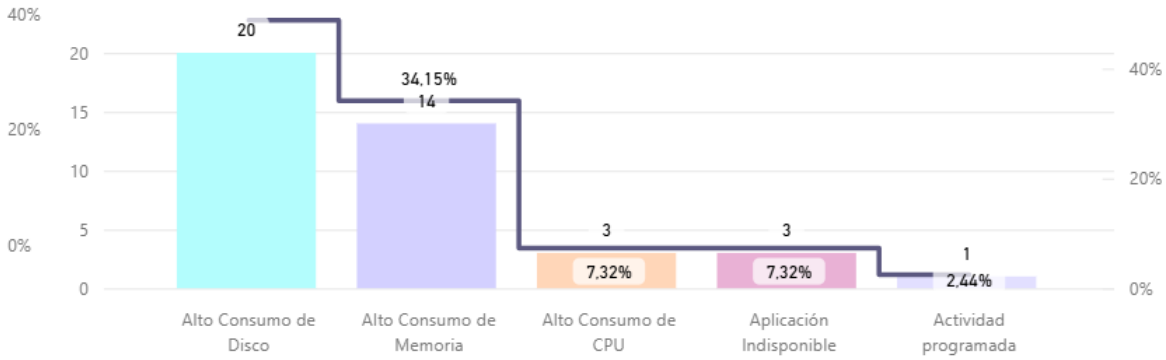


Ilustración Causas de alarmas Servidores Windows

- Se evidencia que para el mes de julio la causa principal y con mayor número de eventos es por alto consumo en disco, siendo el servidor MINTRABCKEXEC el más afectado, acumulando hasta el 70% (14) de los casos relacionados a esta causa, seguido del servidor MINTRABGD08A el cual acumula 3 eventos con un 15% del total, también se observa con 2 casos y un peso del 10% el servidor MINTRABGD07A y con 1 caso representando el 5% el servidor MINTRABAPPNET01.

- El alto consumo de memoria representa el 34% (14) de los casos reportados en el mes, siendo el servidor MINTRAB02 el mas afectado con 9 casos y un peso del 64%, seguido del servidor MTCAPP con 5 casos y un peso del 35,7%.
- La causa alto consumo de CPU con una representación del 7.3% (3), solo afecta a un servidor, el cual es MINTRAB23, con el 100% de los casos relacionados a esta causa.
- Por otro lado, aplicación indisponible, a pesar de tener solo 3 eventos reportados y también un 7.3% de representación afecta a dos servidores, MINTRAB23 con 2 casos y MTCAPP con 1 caso.
- La causa actividad programada tiene una baja incidencia con 1 caso y una representación del 2.44%, la cual afecta únicamente al servidor MINTRAB23.
- Es recomendable la revisión de las aplicaciones que se están viendo afectadas. Por lo tanto, enfocar las acciones correctivas en las causas principales permitirá lograr una reducción significativa en la ocurrencia de incidentes y un mejoramiento clave en la estabilidad operativa del sistema, de igual forma, se recomienda dejar en estado mantenimiento los servidores que tengan actividades programadas con el fin de evitar alertamientos.

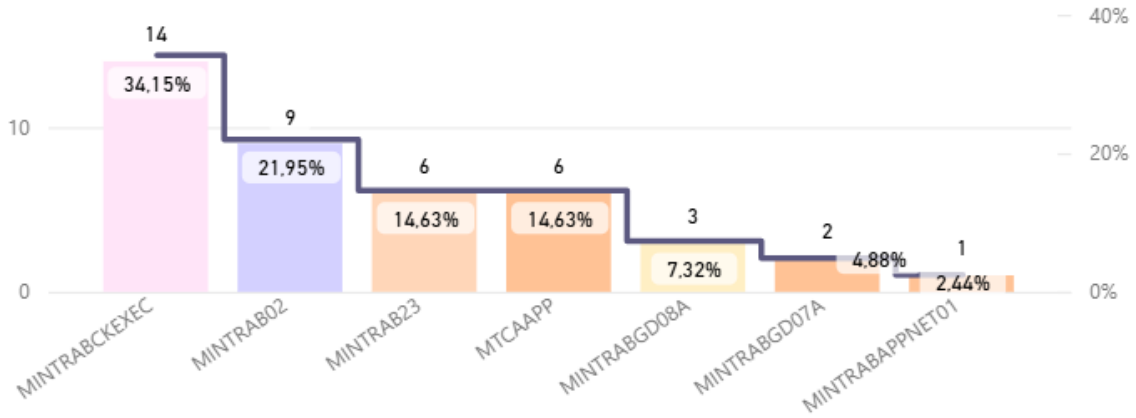


Ilustración TOP 10 de servidores Windows con mas alarmas

- El servidor MINTRABCKEXEC (14 casos) representa el 34% de los eventos reportados, siendo el primer mes que este servidor se encuentra en el top 1, en las causas se evidencian múltiples reportes relacionados a alto consumo en disco duro, siendo la única y reiterada causa que afecto este servidor, igual que MINTRABGD08A el cual reporta 3 casos asociados a esta causa y MINTRABGD07A con 2 casos.
- El servidor MINTRAB02 para este mes se presenta con altos consumos en memoria al 100%, sin reportar otra anomalía.
- Por otro lado el servidor que siempre tiene presencia en el TOP MINTRAB23, presenta múltiples casos relacionados a consumo de CPU (3), aplicación indisponible (2) y actividad programada con 1 caso.

- Para el servidor MTCAPP encontramos casos relacionados a consumo en memoria con 5 eventos y aplicación indisponible con 1 evento.

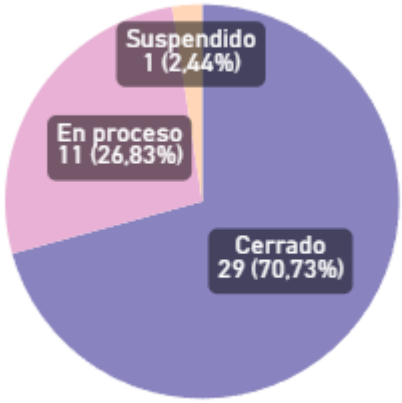


Ilustración Casos suspendidos VS. Solucionados o cerrados Servidores Windows

Se evidencia que, de los 41 eventos registrados durante el mes de julio, 29 (70%) están en estado cerrado y solucionado, 1 caso, se encuentra en estado suspendido relacionado al servidor MINTRABGD07A, categorizado como alto consumo de disco y 11 casos en proceso relacionados al consumo del disco del servidor MINTRABCKEXEC, se ha revisado la documentación de estos casos, sin embargo, no se observa documentación.

- **Servidores Linux**

Durante julio se evidencian 2 casos a servidores Linux, representando el 0,39% del total, lo cual es la segunda cifra más baja del último año relacionado a esta categoría.



Ilustración Causas de alarmas Servidores Linux

En julio se observa que el 100% de los casos pertenecen a consumo de memoria en el servidor MINTRAB60, lo cual es anormal teniendo en cuenta que estos servidores suelen ser estables debido a sus tareas programadas.

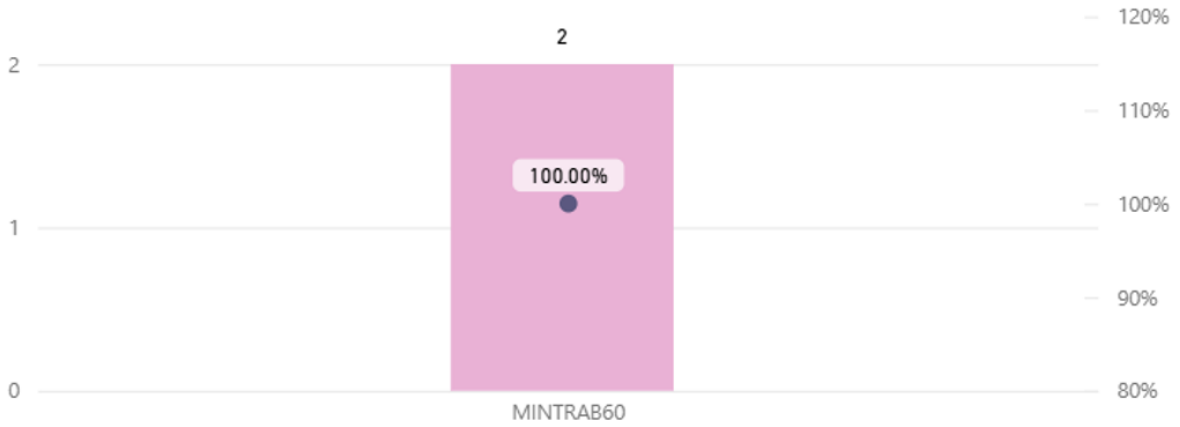


Ilustración TOP 10 de servidores Linux con más alarmas

Para este mes se evidencia que el consumo de memoria estuvo muy presente en el servidor Linux MINTRAB60, representando el 100% de los casos, es el segundo mes consecutivo que este servidor se encuentra uncio en los eventos reportados.

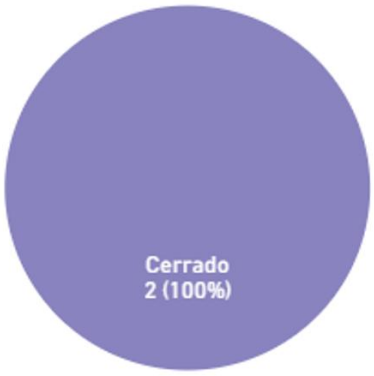


Ilustración Casos suspendidos VS. Solucionados o cerrados Servidores Linux

Se evidencia que los dos casos reportados para julio se encuentran cerrados.

Graficas de CPU zabbix de todo el mes sobre servidores

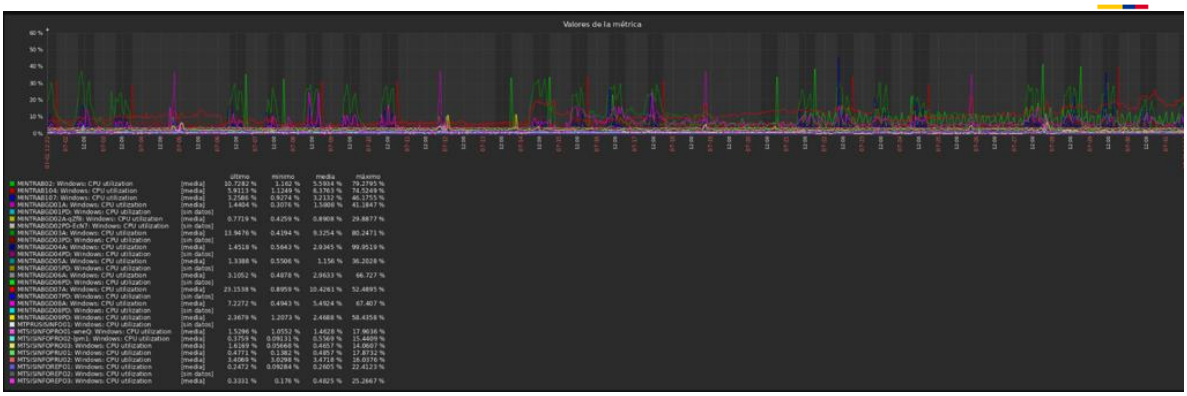


Ilustración Grafica CPU

A continuación, se relaciona el TOP 5 de los servidores que por media tuvieron más utilización de recursos de CPU durante el mes.

CPU

1. MINTRABGD07A 10.4261%
2. MINTRABGD03A 9.3254%
3. MINTRAB104 6.3763%
4. MINTRAB02 5.5934%
5. MINTRABGD08A 5.4924&

Grafica de MEMORIA zabbix de todo el mes sobre servidores

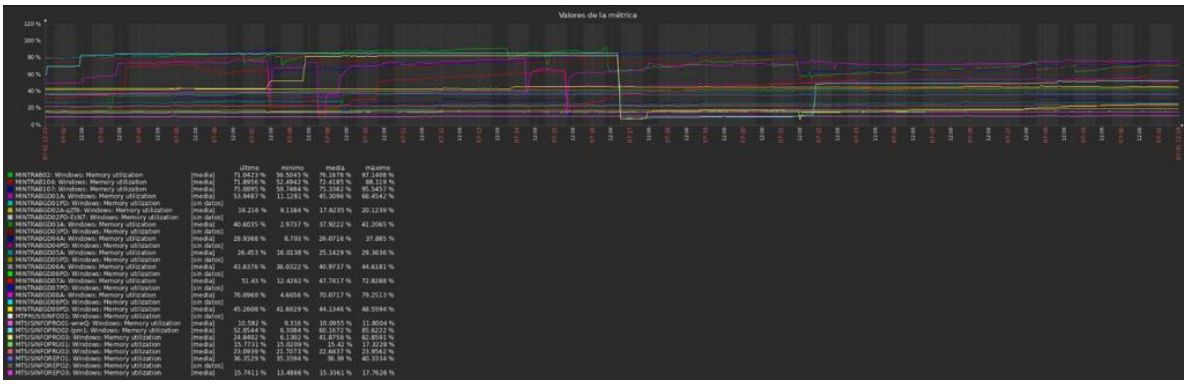


Gráfico 25 Grafica memoria

A continuación, se relaciona el TOP 5 de los servidores que por media tuvieron más utilización de recursos de MEMORIA durante el mes.

MEMORIA

1. MINTRAB02 76.1676%
2. MINTRAB107 75.3363%
3. MINTRAB104 72.4185%
4. MINTRABGD08A 70.0717%
5. MTSISINFOPROO2 60.1672%

2.1.2.9. Práctica de Disponibilidad

Dentro del marco de la práctica de la disponibilidad del servicio se está trabajando en los procesos y las herramientas que permitan cumplir con los objetivos de disponibilidad definidos en la práctica.

A continuación, se muestra la información correspondiente a la disponibilidad de los servicios para el periodo del 1 al 31 de julio de 2026.

Servidores

Cantidad de dispositivos	Disponibilidad consolidada
122	100,00%

Tabla 21 Consolidado disponibilidad de servidores

Directorio Activo

Cantidad de dispositivos	Disponibilidad consolidada
3	100,00%

Tabla 22 Consolidado disponibilidad de Directorio Activo

Los siguientes servidores, se encuentran en el Directorio Activo los cuales estuvieron disponibles durante el periodo.

Servidor	Disponibilidad
MINTRAB02	100,00%
MINTRAB104	100,00%
MINTRAB107	100,00%

Tabla 23 Desagregado de Disponibilidad Directorio Activo

Datacenter Principal

Cantidad de dispositivos	Disponibilidad consolidada
8	100,00%

Tabla 24 Consolidado disponibilidad de equipos Datacenter principal

Los siguientes equipos se encuentran el Datacenter Principal, los cuales estuvieron disponibles durante el periodo.

Equipo	Disponibilidad
Fortimanager_SDWAN	100,00%
CXV-SWCORE1-RAT42-U44-8360	100,00%
CXV-SWCORE2-RAT42-U42-8360	100,00%
CXV-SWDELL1-RAS42-U43-S4148T	100,00%
CXV-SWDELL2-RAS42-U42-S4148T	100,00%
CXV-SWEDGE-RAT42-U40-6300	100,00%
CXV-SWACC-RAAT38-U41-6300	100,00%
CXV-FG-600F-SDWAN-HUB01	100,00%

Tabla 25 Desagregado de Disponibilidad Datacenter Principal

Datacenter Alterno

Cantidad de dispositivos	Disponibilidad consolidada
4	100%

Tabla 26 Consolidado disponibilidad de equipos Datacenter alterno

Los siguientes equipos se encuentran el Datacenter alterno, los cuales estuvieron disponibles durante el periodo.

Equipo	Disponibilidad
STM-FG-600F-SDWAN-HUB02	100%
STM-SWCORE2-R0015-U35-8360	100%
STM-SWDELL1-R0015-U41-S4148T	100%
STM-SWDELL2-R0015-U42-S4148T	100%

Tabla 27 Desagregado Disponibilidad de equipos Datacenter alterno

Redes y conectividad

Cantidad de dispositivos	Disponibilidad consolidada
484	98,47%

Tabla 28 Consolidado disponibilidad de equipos redes y conectividad

Durante el periodo, se realizó constante monitoreo y seguimiento de la disponibilidad de los canales principales y secundarios de internet, con el fin de prever alguna novedad en el servicio y dar una respuesta oportuna desde el NOC y Lideres de Servicio de Conectividad.

Seguridad

Cantidad de dispositivos	Disponibilidad consolidada
8	100,00%

Tabla 29 Consolidado disponibilidad de equipos de seguridad

Los siguientes equipos se encuentran en el Servicio de Seguridad Informática, los cuales estuvieron disponibles durante el periodo:

Equipo	Disponible
MINTRABSUPERVISOR	100,00%
MINTRABVULNE01	100,00%
SOC_Fortianalyzer	100,00%
SOC_FortiDDOS	100,00%
SOC_SandBox	100,00%
SOC_WAF	100,00%
SDWAN-FG600F-SCENTRAL	100,00%
FGT-2200-ColombiaXV	100,00%

Tabla 30 Disponibilidad de equipos Seguridad de la Información

Telefonía

Cantidad de dispositivos	Equipo	Disponibilidad consolidada
1	Telefonía siptrunk.net2phone.com	100%

Tabla 31 Consolidado disponibilidad de equipos de telefonía

Antivirus

Cantidad de dispositivos	Disponibilidad consolidada
1	100%

Tabla 32 Consolidado disponibilidad de plataforma antivirus

Actividades de la Practica de Disponibilidad:

- Seguimiento a los resultados de los cambios presentados en el CAB por partes de especialistas que afecten la disponibilidad del servicio.
- Durante el periodo, se realizó seguimiento a los resultados de las pruebas de disponibilidad DRP en conjunto con la entidad frente a la SVE, el RFC-240499 fue exitoso y sin novedades, las cuales, se completó la documentación de resultados.
- Se realizó seguimiento a los 18 planes de disponibilidad, de los cuales 14 fueron ejecutados y cerrados satisfactoriamente, alcanzando un 77,8% de cumplimiento. Este resultado evidencia un avance significativo en la ejecución de las actividades planificadas, contribuyendo al fortalecimiento de la disponibilidad de los servicios. Por otra parte, 4 planes (22,2%) permanecen pendientes de ejecución, lo cual, se encuentran en proceso de programación y ejecución en los próximos periodos.

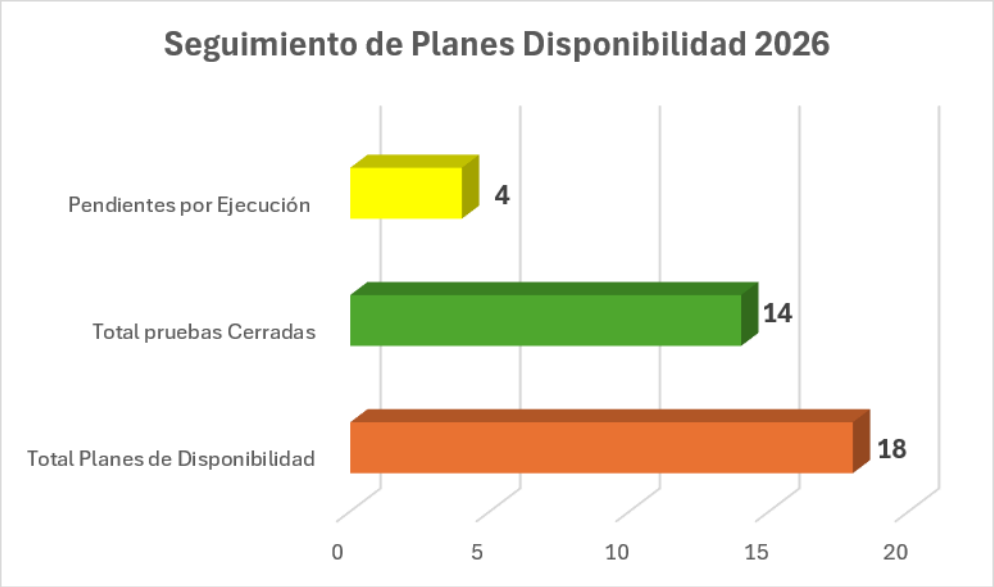


Ilustración 17 Seguimiento de Pruebas de Disponibilidad 2026

2.1.2.10. Práctica de Implementación

Dentro de la aplicación de la práctica, se desarrollaron procesos para apoyar a planificar, programar, ejecutar, controlar, aplicar pruebas e implementar nuevos servicios o incluir modificaciones de las funcionalidades de los aplicativos o sistemas de información en producción.

A continuación, se muestra la información correspondiente a la práctica de implementación para el periodo del 1 al 31 de julio de 2026.

Actividades en curso:

- Revisión de los cambios (RFC) ejecutados durante el periodo, para los cuales (19) cambios fueron aprobados su cierre, ya que cuentan con las evidencias completas de los planes de Pruebas Previas y Posteriores, al corte del 31/07/2026 se encuentra (1) caso abierto (en implementación) y (1) Caso (en ejecución) a la espera de entrega de las evidencias por parte los especialistas.

- Se adjunta al presente informe el Seguimiento de la práctica durante el periodo de cada Cambio presentado al **CAB.**

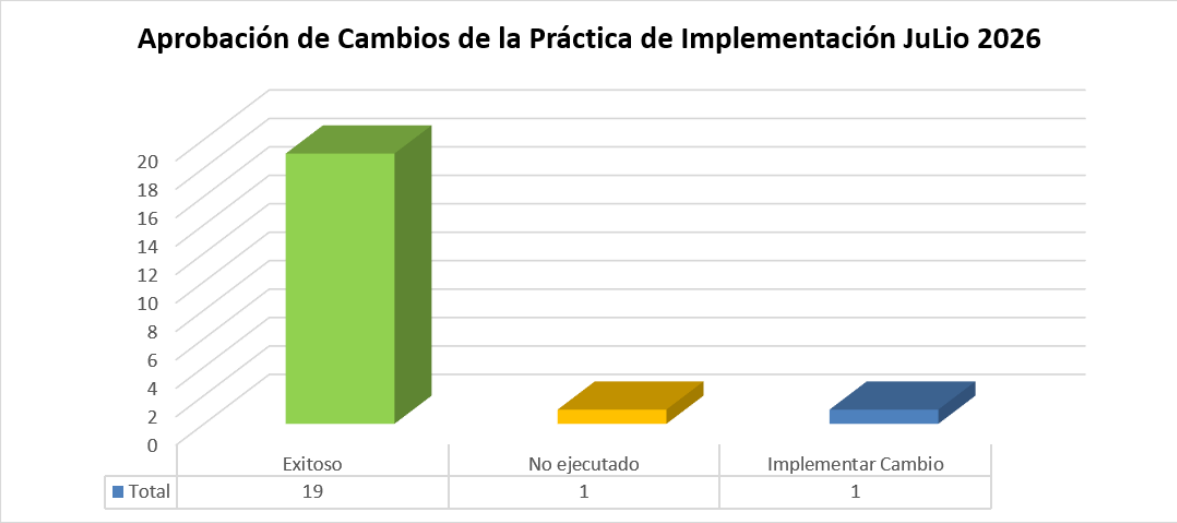


Ilustración 18 Seguimiento Práctica Implementación

Seguimiento de cambios Implementa

2.2 Mesa de Servicios y Soporte en Sitio

A continuación, se presenta la gestión desarrollada durante el mes de julio por la Mesa de Servicios y el personal de Soporte en Sitio, la cual contiene información relevante sobre la operación, hallazgos y actividades realizadas. Esta información permite apoyar la toma de decisiones orientadas a mejorar la calidad del servicio y la percepción de los usuarios.

- **Histórico de Atención de Llamadas**

Para el periodo del mes de julio a la MDS ingresaron 365 llamadas de usuarios finales para solicitar servicios de Soporte Tecnológico, a continuación, se discrimina la clasificación según el servicio solicitado:

Servicio	Entrantes	Atendidas	Atendidas Umbral	No Atendidas umbral	Abandonadas	No Atendidas
COL - Mintrabajo-equipo compu	229	225	221	0	2	2
COL - Mintrabajo-Gestor-documental	73	73	73	0	0	0
COL - Mintrabajo-office365	43	43	43	0	0	0
COL - mintrabajo-Impresora	20	20	20	0	0	0
TOTAL	365	361	357	0	2	2

Tabla 33 Llamadas Atendida por la Mesa de Servicio

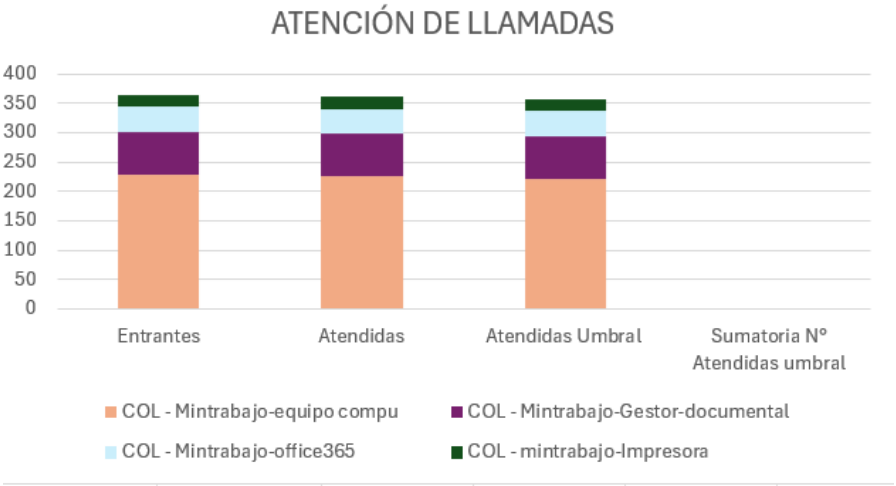


Ilustración 19 Llamadas Atendidas

El servicio más solicitado a través de la atención de llamadas es: Equipo de cómputo con 260 llamadas entrantes, se atendieron 361 solicitudes se observan: 2 llamada abandonada antes de los 20 segundos.

- **Casos Registrados por Categoría de Servicio**

Para este periodo se toma el top 10 de los casos más representativos de los diferentes servicios como: Administración de servidores, Redes y Conectividad, Seguridad Informática, Telefonía IP, Aplicaciones Especializadas, Soporte Microinformática se encuentran en el anexo de nombre DatosMintrabajo_JULIO.xlsx pestaña *categoría.*

- **Análisis de Casos Anulados por Servicio**

Para este periodo se tienen 5 casos anulados para los siguientes servicios:

CASOS ANULADOS	TOTAL
Soporte Microinformatica	2
Herramientas de Gestión	2
Redes y Conectividad	1
Total general	5

Tabla 344 Casos Anulados

Los casos anulados por Soporte Microinformática se deben a 2 solicitudes de: devolución de equipo y Atasco de impresora, Herramientas de Gestión con 2 casos de : Alarma desde Zabbix, y Redes y Conectividad con 1 caso de alarmas de Starlink.

- **Análisis de Casos Suspendidos por Servicio**

Para el periodo del mes de julio, se dio una aumento de casos suspendidos del 33,79% que corresponde a 49 casos para un total de este mes de 145 casos de los siguientes servicios:

CASOS SUSPENDIDOS	TOTAL
Administración de servidores	63
Soporte Microinformatica	49
Seguridad informatica	14
Aplicaciones Especializadas	12
Redes y Conectividad	6
Administración de Bases de Datos	1
Total general	**145**

Tabla 35 Casos Suspendidos

- **Administración de servidores:** 63 casos suspendidos debido a que se ha solicitado información complementaria a los usuarios o están pendientes por disponibilidad del usuario: Inactivar usuario con 47 casos; Backup, con 7 casos; Configuración con 3 casos; Crear/Modificar/Eliminar con 2 casos; Modificar usuarios, Servidor Windows, Asignación de licencia, Configuración MFA con 1 caso para cada categoría.
- **Soporte Microinformática**: 49 casos suspendidos por: Equipo Periférico con 8 casos, Traslado de Sede, Cambio Equipo o Rol con 6 casos, Configuración, Asignación de equipo (portátil o PC) y Equipo Escritorio con 5 casos cada categoría, Instalación – Configuración y Equipo Portátil con 4 casos cada categoría, Backup con 3 casos, Asesoría – Consulta, Solicitud Backup, Cambio de unidad de imagen e Impresora con 2 casos cada categoría, Solicitud de cambio, Préstamo, No enciende, Configuración, Cambio Toner y Mantenimiento preventivo con 1 caso para cada categoría.
- **Seguridad informática:** 14 casos suspendidos: Reporte de eventos con 5 casos, Validación Habilitación Puertos USB con 3 casos, Permitir acceso, Análisis de evento con 2 casos par cada categoría, Agregar a sitios permitidos y Habilitación Puertos USB con 1 caso para cada categoría.
- **Aplicaciones Especializadas:** 12 casos suspendidos debido a: Relanzamiento con 4 casos; Falla Funcional con 3 casos, Asignar Radicado TYS con 2 casos, Instalar – Configurar, Depuración Bandeja y Falla - Error PQRSD con 1 caso para cada categoría.
- **Redes y Conectividad:** 6 casos suspendidos por Router con 4 casos, Starlink y AP, con 1 caso para cada categoría.
- **Administración de Bases de Datos:** 1 casos suspendido por Asesoría – Permisos de base de datos con 1 caso.

- **Análisis General de Casos Solucionados - Incidentes y Requerimientos**

Incidentes solucionados por la Mesa de Servicios: Para este periodo no quedaron incidentes en estado solucionado.

Incidentes solucionados por Soporte en sitio: Para este periodo no quedaron incidentes en estado solucionado.

Incidentes solucionados por Soporte Territoriales: Para este periodo no quedaron incidentes en estado solucionado.

Requerimientos solucionados por la Mesa de Servicios:
En el mes de julio quedo 1 requerimiento en estado solucionado.



Ilustración 20 requerimientos solucionados mesa de servicios

Requerimientos solucionados por Soporte en sitio Bogotá: En el mes de julio no quedaron requerimientos en estado solucionado.

Requerimientos solucionados por Soportes Territoriales: Para el mes de julio quedo 1 requerimiento en estado solucionado.



Ilustración 21 requerimientos solucionados soporte territoriales

- **Casos Cerrados por la Mesa de Servicios, Soporte en Sitio en Nivel Central y Sedes Territoriales.**

Casos Cerrados por la Mesa de Servicios: Se indica el top de 10 de Requerimientos cerrados por la mesa de servicios, para el mes de julio se cerraron 1126 casos, discriminados así: Asesoría – Consulta 230 casos, Cambiar contraseña de cuota 200 casos, Aumento de cuota 199 casos, Creación de usuario 137 casos, Inactivar usuario con 55 casos, Cambio de grupo 45 casos, Configuración 36 casos, Modificar usuarios 35 casos, Backup 33 casos, Instalación y configuración VPN con 20 casos.

En comparación del mes anterior se nota un aumento de casos cerrados por la mesa de un 28,242% que es equivalente a 318 casos.

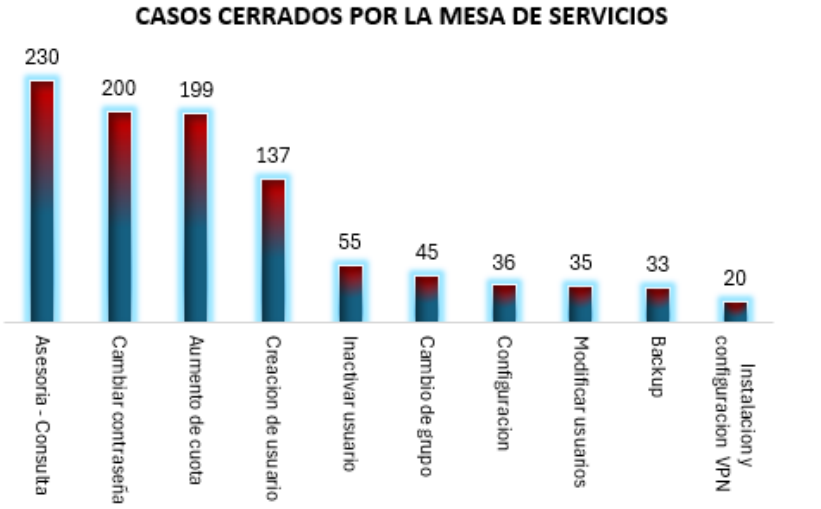


Ilustración 22 Requerimientos Cerrados por la Mesa de Servicios

Casos Cerrados por Soporte en Sitio: Se indica el top 10 de Requerimientos cerrados por soporte en sitio, para el mes de julio se cerraron 1010 casos discriminados así: Cargue de papel en impresora con 238 casos, Asesoría – Consulta con 120 casos, Instalación - Configuración con 108 casos, Configuración con 75 casos, Préstamo con 65 casos, Asignación de equipo (portátil o PC) con 36 casos, Soporte Aplicaciones Office 365 con 35 casos, Análisis de evento y instalación y configuración VPN con 33 casos para cada categoría, Backup con 28 casos.

En comparación con el mes anterior se tiene un aumento del 1,48% que corresponde a 15 casos.



Ilustración 23 Casos Cerrados por Soporte en Sitio

Casos Cerrados por soporte en sitio Territoriales: Se indica el top de 10 de Requerimientos cerrados por soporte en sitio Territoriales, para el mes de julio se cerraron 1731 casos, discriminados así: Asesoría – Consulta con 23 casos, Cargue de papel en impresora con 259 casos, instalación - Configuración con 182 casos, Configuración con 167 casos, Asignación de equipo (portátil o PC) con 77 casos, Instalación-Desinstalación con 68 casos, Mantenimiento preventivo 63 casos, Soporte Aplicaciones Office 365 con 62 casos, Asesoría PDF con 61 casos.

En comparación con el mes anterior se tiene un aumento del 24,72% que corresponde a 428 casos.

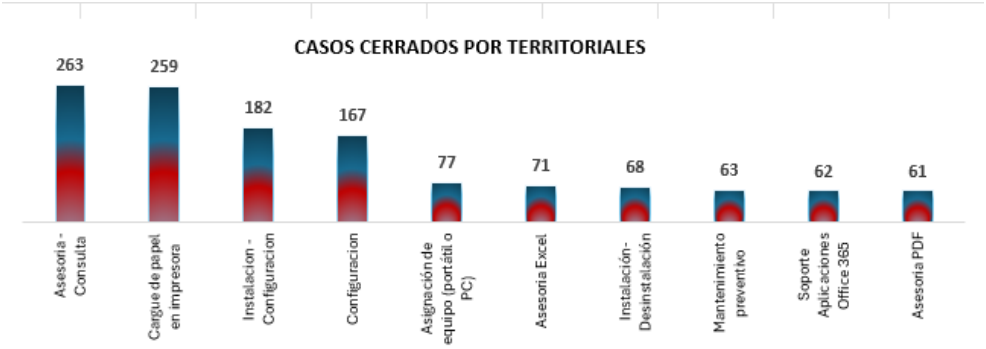


Ilustración 24 Casos Cerrados por Territoriales

- **Casos Atendidos a Usuarios VIPS**

Durante este periodo se crearon 52 solicitudes para ser atendidas por soporte en sitio, para VIPS discriminados a continuación por tipo de caso:

TIPO DE CASO_VIPS	CUMPLIMIENTO	NO_CUMPLE	TOTAL
Incidents	2	0	2
Requerimientos	50	0	50
Total general	**52**	**0**	**52**

Tabla 36 Casos Atendidos usuarios VIPS

Se atendieron 982 solicitudes para el resto de los usuarios discriminados así:

TIPO DE CASO-NO-VIPS	CUMPLIMIENTO	NO_CUMPLE	TOTAL
Incidentes	34	0	34
Requerimientos	948	0	948
Total general	**982**	**0**	**982**

Tabla 37 Casos Atendidos usuarios

- **Medio de Ingreso de Casos**

Durante el período ingresaron a la mesa de servicio 6153 casos a través de los diferentes medios que se tiene habilitados para la atención de solicitudes, como son Correo SoporteMT, Gestión Técnica, alarma de Zabbix, Llamadas Telefónicas, alarma de Fortisiem, Portal Autogestión, casos creados de forma automática por las diferentes herramientas:

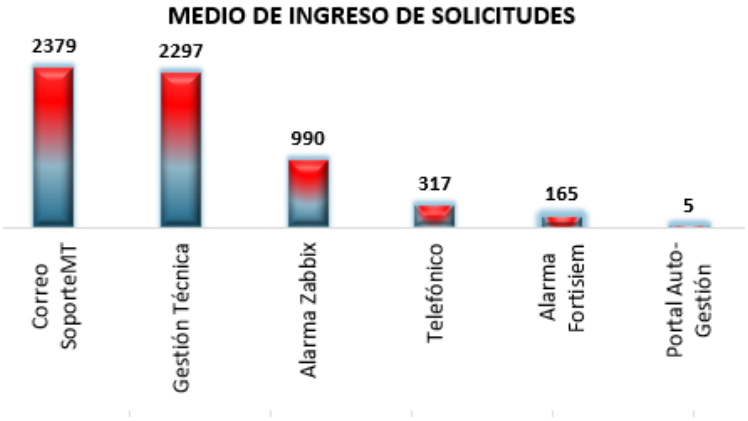


Ilustración 25 Medios de Ingreso de Casos

Gestión técnica es el método más utilizado por los funcionarios del ministerio del trabajo, esta categoría hace referencia a solicitudes que directamente realizan las personas a los soportes, no ingresan a través de la mesa de servicios.

- **Novedades de la operación – Mesa de Servicios y Soporte en sitio Bogotá**

Se continúa con la actualización de BIOS de los equipos de cómputo en operación de la unión temporal.

Se continúa realizando control y autorización por medio de la supervisión para los trámites relacionados a la toma de posesión de cargos por concurso de mérito, para traslados, cambios y trámites relacionados en los cambios de cargo.

Se realiza seguimiento al caso con el objetivo de optimizar los tiempos de atención y fortalecer la percepción del servicio, garantizando una respuesta oportuna y una mejor experiencia para el usuario.

- **Novedades de la operación – Soporte en sitio Territoriales**

Durante el mes de julio de 2026 los profesionales de soporte en sitio territoriales llevaron a cabo las siguientes acciones:

Se realizan 16 visitas a inspecciones donde no se cuenta con personal dedicado para solucionar los casos que requieren atención, entre estos, casos de Internet, Redes, Actualizaciones de BIOS; Software y Agentes instalados, así como la revisión y mantenimiento de impresoras

Se realizó Intervención de 2103 casos, dentro de los que se destacan: Inactivación de usuarios, Cargues de Papel en las impresoras de las diferentes Sedes, Asignación de equipos de cómputo, Instalación y configuración de impresoras y línea base de software,

Configuración de OneDrive, Asesoría en Excel, Instalación de Agente Aranda, Asesoría-Consulta sobre el software instalado, Aplicaciones Office 365 y Asesoría en PDF
Revisión, validación del estado y aseguramiento de los equipos de cómputo de Popayán y Sincelejo para el traslado a la nueva Sede, revisión y ajuste de los cables y los puntos de red en Palmira y en la sede Valle.

Atención de servicios en Sedes Territoriales sin personal de soporte en sitio dedicado
A continuación, se relacionan las visitas en sitio gestionadas durante este período en las sedes donde no se cuenta con personal de Soporte en Sitio dedicado, y que requirieron de esta gestión para dar atención a necesidades de los servicios y atención de incidencias.

Para el período se realizaron las siguientes visitas:

Mes	Territorial	Sede	Servicio	Descripción	Caso
Julio 2026	GUAJIRA	BARRANCAS	Impresora presenta error en pantalla	Se requiere apoyo de soporte en sitio, ya que la impresora no permite imprimir por un error que aparece en pantalla.	IM-273714
Julio 2026	VALLE	SEVILLA	Internet y navegación presentan problemas	Se procede a realizar el cambio de los cables de internet en el switch, reemplazando los que presentaban desgaste. Tras la intervención, se confirma que la conexión queda estable y en funcionamiento normal. El caso queda en seguimiento para validar el comportamiento del servicio durante las jornadas laborales.	RF-270082
Julio 2026	RISARALDA	LA VIRGINIA	Se presenta inconvenientes para usar las herramientas de Office de escritorio	Una vez se removió el número del MFA con ayuda de MDS. se procedió a iniciar sesión nuevamente en la cuenta de Office, activando todos los programas incluidos en la licencia y en OneDrive	IM-269958
Julio 2026	VALLE	CARTAGO	Mantenimiento preventivo de la impresora RICOH-CARTAGO-INSP	se realiza mantenimiento preventivo y correctivo básico a la impresora Ricoh asignada, con el fin de asegurar su adecuado funcionamiento y prevenir fallas en los procesos de impresión.	RF-268240
Julio 2026	VALLE	ROLDANILLO	Mantenimiento preventivo de la impresora RICOH-ROLDANILLO-INSP	Se realiza mantenimiento preventivo semestral a la impresora Ricoh asignada a la Inspección, con el fin de asegurar su adecuado funcionamiento y prevenir fallas en los procesos de impresión	RF-268237
Julio 2026	CAUCA	EL BORDO	Mantenimiento de impresora RICOH - BORDO	Se realiza mantenimiento preventivo y correctivo básico a la impresora Ricoh asignada, con el fin de asegurar su adecuado funcionamiento y prevenir fallas en los procesos de impresión.	RF-271486
Julio 2026	SANTANDER	SABANA DE TORRES	Mantenimiento de impresora RICOH con serial 3353PA50574	Se realizó la verificación funcional del equipo de impresión reportado. Se realizó mantenimiento preventivo de la pantalla, con el objetivo de optimizar la visualización de las opciones y mejorar la experiencia de uso. El proceso fue completado de manera satisfactoria	RF-268009
Julio 2026	VALLE	BUENAVENTURA	Instalación y configuración de un teléfono fijo corporativo IP	Verificar la disponibilidad del dispositivo Audiocodes y los accesorios requeridos (cableado de red y energía). Conectar el teléfono a la red corporativa y a la fuente de energía. Configurar el dispositivo IP mediante las credenciales de usuario de Microsoft Teams. Validar la correcta autenticación con la plataforma de Teams y sincronización de la cuenta.	RF-271547
Julio 2026	SUCRE	SANTIAGO DE TOLÚ	Actualización del sistema operativo de equipo LENOVO	Se ingresa a la configuración del equipo, luego en Windows Update, se procede a descargar e instalar la última versión del sistema operativo Windows 11 PRO; una vez culminado, se reinicia el equipo para	RF-273793

				actualizarlo a la versión 25H2; se adjunta evidencia de la labor en el equipo.	
Julio 2026	MAGDALENA	FUNDACIÓN	Mantenimiento de impresora RICOH con serial 3353PA51228	Se realiza mantenimiento a la impresora de la inspección del municipio de Fundación según las indicaciones dadas	RF-273822
Julio 2026	SANTANDER	SABANA DE TORRES	Mantenimiento preventivo de la impresora con serial 3353PA50574	Se ejecutó mantenimiento preventivo según los lineamientos establecidos, obteniendo resultados satisfactorios. Se llevaron a cabo pruebas operativas en conjunto con el usuario para validar la funcionalidad de la impresora	RF-273642
Julio 2026	SANTANDER	SABANA DE TORRES	Se requiere instalación del agente Aranda en equipo de cómputo asignado.	Se efectuó la verificación del equipo de cómputo del usuario para garantizar condiciones adecuadas de operación. Se procedió con la instalación del aplicativo Agente Aranda, incluyendo configuraciones generales necesarias para su correcto funcionamiento	RF-281890
Julio 2026	CORDOBA	SAHAGÚN	Backup de la información contenida en el computador	Se realiza la copia de respaldo físico de la información contenida en el equipo asignado a la funcionaria María Francisca Bula Vega.Durante la actividad se efectuó el respaldo de la información institucional, verificando la correcta transferencia de los archivos al medio de almacenamiento destinado para tal fin, conforme a los procedimientos establecidos.	RF-271281
Julio 2026	CORDOBA	CERETÉ	Backup de la información contenida en el computador	Se realiza la copia de respaldo físico de la información contenida en el equipo asignado a la funcionaria Martha Cecilia Otero Ruiz.Durante la actividad se efectuó el respaldo de la información institucional, verificando la correcta transferencia de los archivos al medio de almacenamiento destinado para tal fin, conforme a los procedimientos establecidos.	RF-279928
Julio 2026	CESAR	LA JAGUA DE IBIRICO	Asignación de equipo de cómputo, roles en los aplicativos de funcionario David Andrade	Se procede con la creación de usuario y asignación de equipo de cómputo para el nuevo funcionario DAVID STYWHER ANDRADE CALDERON	RF-280265
Julio 2026	VALLE	PALMIRA	Se reporta que el rack de telecomunicaciones sufrió una caída lateral dentro de su estructura	Se estabiliza la estructura y el estado de los equipos. Tras la revisión, se confirma que no se evidencian daños en los dispositivos y que el rack quedó totalmente operativo. Con ello se da solución a la novedad presentada y se procede con el cierre del caso	IM-291265

Tabla 38 Visitas a sedes sin Soporte en Sitio

- Medición ANS Mesa de Servicios

A continuación, el resultado de la medición de los ANS:

Área	Nombre del Indicador	Resultado	Meta
Mesa de Servicio	Tiempo de atención de solicitudes por soporte en sitio	97,20%	95,00%
	Tiempo de solución de incidentes por soporte en sitio	97,14%	90,00%
	Tiempo de solución de requerimientos por soporte en sitio	99,89%	90,00%
	Tiempo de respuesta de la mesa de servicio	98,89%	85,00%
	Abandono de llamadas	0,55%	Máximo 8,00%

Área	Nombre del Indicador	Resultado	Meta
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 39 Medición de ANS Mesa de servicios

3 LINEA DE SERVICIOS CENTRALES

El alcance de esta sección es brindar un estatus de las variables más relevantes del Servicio de Datacenter, aplicaciones especializadas, bases de datos, nube privada y pública prestado por la Unión Temporal Gestión TIC 2023 en instalaciones del Data Center Cirion-Colombia XV y en las instalaciones de sede central del Ministerio del Trabajo, en donde está alojada la infraestructura tecnológica que soporta la operación y servicios del Ministerio del Trabajo.

3.1 Datacenter Principal

Se realizó la gestión efectiva de los requerimientos de servicio, Línea de Servicios centrales realizó atención de un total de 1043 casos distribuidos en requerimientos de servicios, incidentes y cambios. Así como la siguiente distribución de casos por estado, grupo de especialistas y atención de acuerdo con el tipo de usuario.

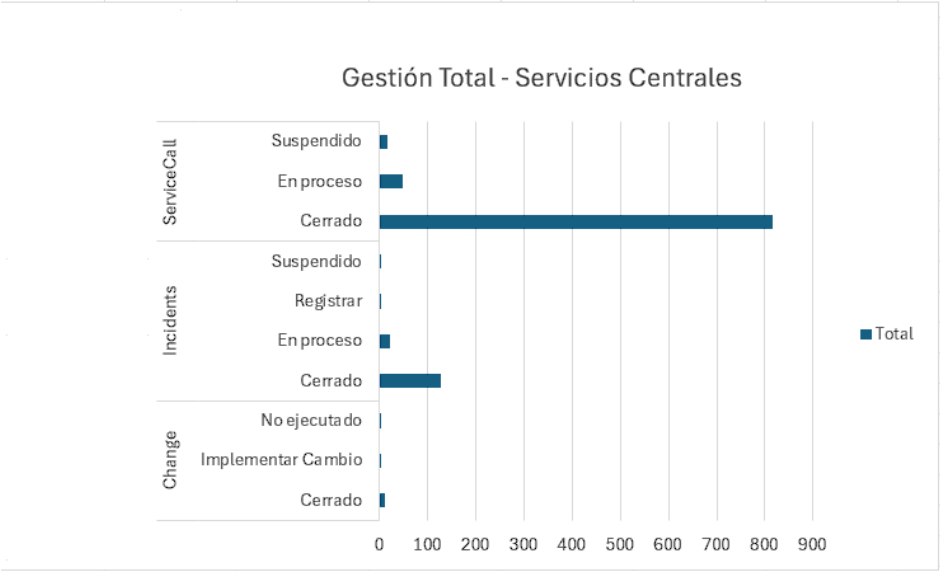


Ilustración 26 Gestión Casos - SC

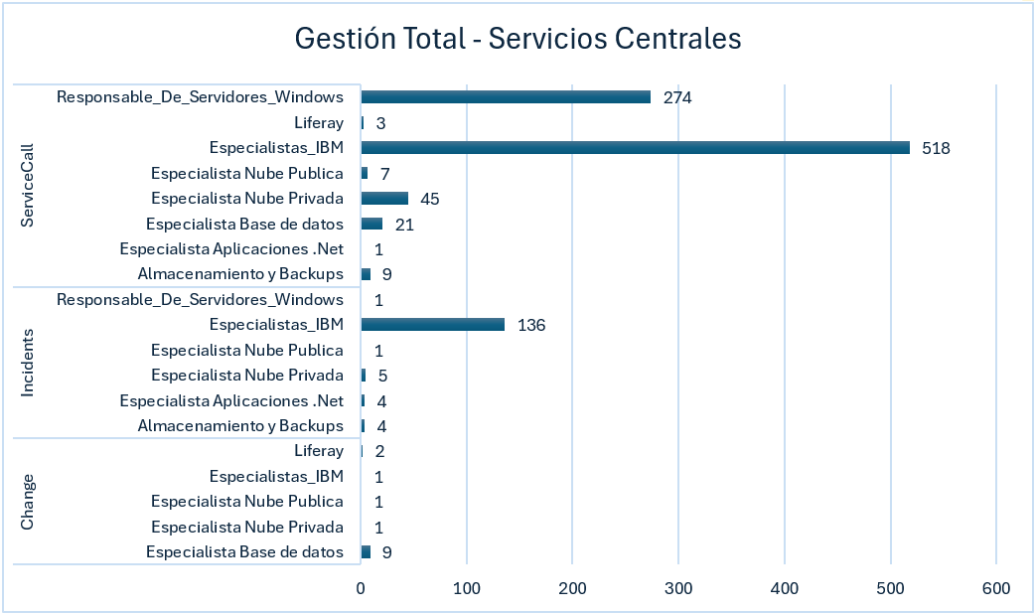


Ilustración 27 Gestión SC - Por Grupo

A nivel de equipos de red en Datacenter, se observa que funcionaron correctamente, no se presentaron caídas ni bloqueos sobre el equipo, se relaciona Ilustración de comportamiento del comportamiento del SWCORE.



Ilustración 28 Comportamiento SWCORE Datacenter Colombia XV

Se verifica la sincronización con el Switch Core2, se observa la configuración HA (Stack), establecida y el SWITCH 1 con el role de principal

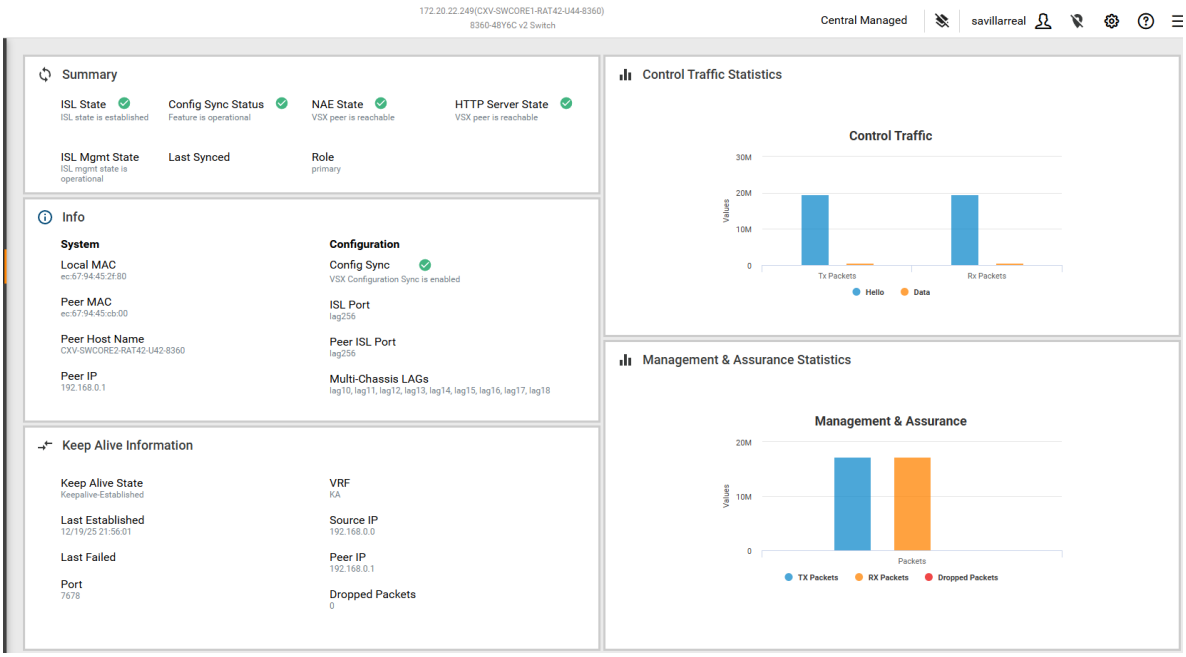


Ilustración 29 Sincronización HA de los Switch Core

-

El canal centralizado de Internet en Datacenter se mantuvo estable, la navegación de todas las sedes se ve reflejado en este canal. Se relaciona gráfica de comportamiento del canal de Internet en Datacenter, donde se observa que no se tuvieron caídas de servicio. Se observa que se tuvo un promedio de tráfico total de 424 Mbps, se han presentado picos de consumo, que no afectan la estabilidad del canal ya que no son constantes.

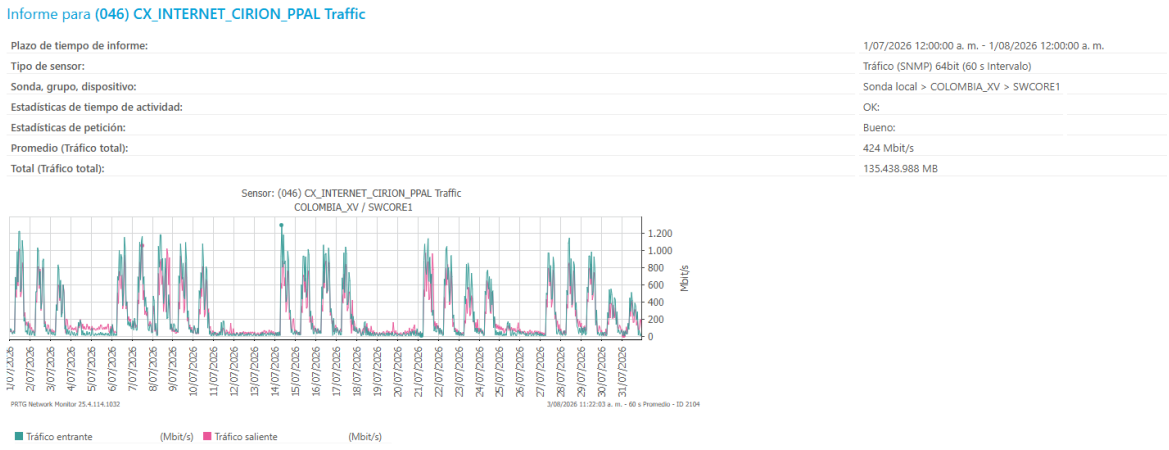


Ilustración 30 Grafica de consumo canal Internet Datacenter

3.1.1 Datacenter Alterno y DRP

Se validaron procesos, actividades relacionadas con la migración y sincronización a través de VMware que permitan una correcta visualización de los recursos a replicar de Datacenter a Datacenter. Se valida procesos y actividades de sincronización a través de VMware que permitan una correcta visualización de los recursos a replicar de Datacenter a Datacenter.

Se finalizaron las actividades de fase 1 para DRP priorizando la replicación de controladores de dominio para así garantizar procesos de autenticación de usuario final y aplicación. Se añaden privilegios de visualización entre VLAN para garantizar comunicación de cada servicio aprovisionado en el entorno aislado de DRP, esto con el fin de evitar problemas de comunicación entre recursos y garantizar un escenario de replicación adecuado.
A nivel de las máquinas virtuales replicadas se visualizan las siguientes VM:

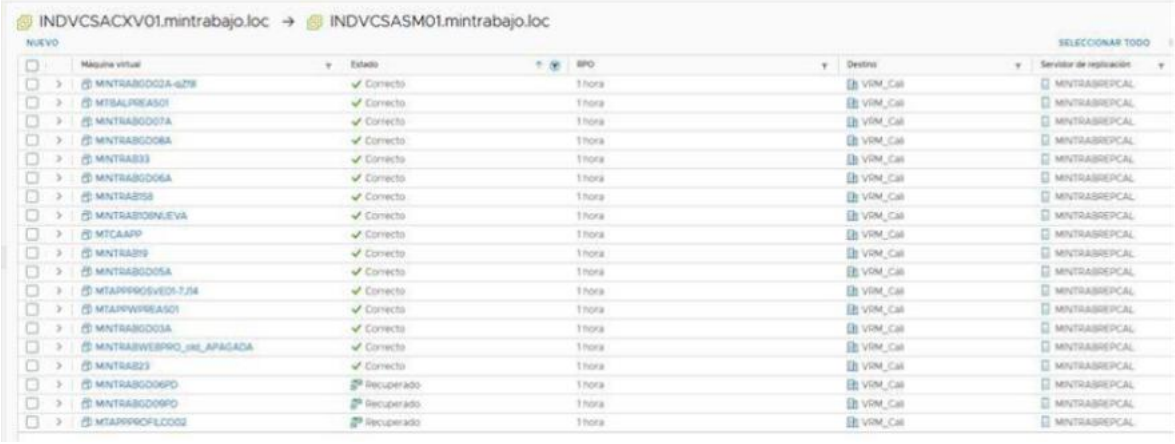


Ilustración 31 máquinas virtuales DRP

De acuerdo con el diagrama de interoperabilidad de Data Center Colombia XV centrado en la infraestructura productiva (no se tiene en cuenta servidores de pruebas ya que el escenario de replicación debe apuntar a un restablecimiento de servicios críticos productivos para dar continuidad a la operación de la entidad).

Podemos definir el siguiente diagrama de replicación con los servicios replicados a través de la solución VMWare Site Recovery. Actualmente se culminó con los ajustes de segmentación de red para preparar el escenario de pruebas para el último trimestre del año de cara a las aplicaciones .NET de acuerdo con lo socializado con la entidad. Las IP fueron asignadas durante el mes de noviembre para realizar las pruebas DRP definidas para el año 2025. De acuerdo con lo anterior, se iniciaron las configuraciones de prueba para replicación de las bases de datos de aplicaciones .NET alojadas en motor MSSQL Server a través de log shipping con una frecuencia de envío de logs cada 15 minutos. Esta prueba y configuración fue realizada en el transcurso del mes de diciembre, documentada a través de la práctica de disponibilidad y revisada por el líder de servicios centrales y la gerente del proyecto.

Se realiza la conmutación manual en la instancia secundaria, conforme al diseño del esquema de Log Shipping, con el objetivo de habilitar las bases de datos y realizar un Full Backup. Dicho backup será posteriormente restaurado en una instancia alternativa de SQL Server, permitiendo restablecer la disponibilidad de las bases de datos y garantizar la continuidad operativa.

La prueba se realizó para las siguientes bases de datos:

No.	Base de Datos	Aplicación
1	MT_EVENTOS	Observatorio Laboral
2	ARCHSINDICAL	Archivo Sindical
3	Bancos	Tesorería
4	CalculadoraLaboral	Calculadora Laboral
5	ESTADOJOVEN	Estado Joven
6	Infraestructura	Cobro Coactivo
7	MTRCobroCoactivo	Cobro Coactivo
8	Siriti2018	Siriti

Tabla 40 Pruebas realizadas

- La prueba de conmutación manual del esquema de Log Shipping se ejecutó de manera controlada y conforme al diseño definido, validando la capacidad de recuperación ante la indisponibilidad de la instancia primaria.
- Se confirmó la recuperación de las bases de datos permitiendo la disponibilidad dentro de los umbrales de RPO y RTO establecidos.
- El ejercicio permitió identificar la necesidad de involucrar a el equipo de aplicaciones para la actualización de cadenas de conexión y la validación funcional posterior.
- Los resultados obtenidos fortalecen el plan de continuidad y recuperación ante desastres, proporcionando insumos para la mejora continua de futuras pruebas.
- En caso de que sea necesario realizar la conmutación del esquema de Log Shipping, se debe contar previamente con los scripts requeridos para dicho proceso, lo que permitirá ejecutar la operación de manera más ágil y eficiente.

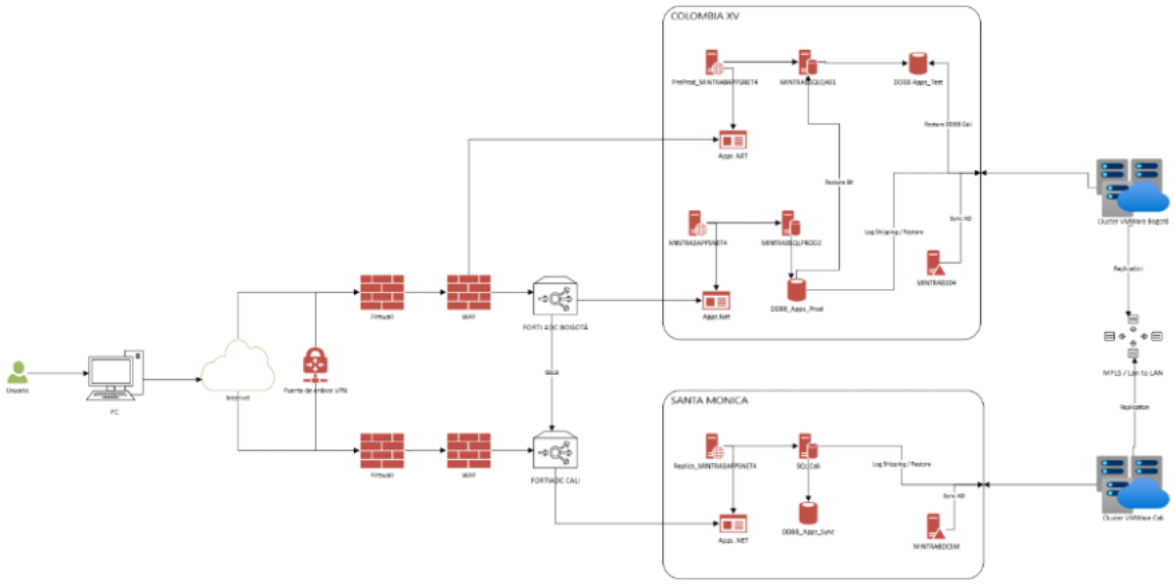


Ilustración 32 Escenario pruebas Apps DRP

A nivel de comunicaciones en DC alterno, se observa que la conexión del LAN to LAN entre los dos Datacenter funcionó correctamento de esta forma se garantizó la conexión entre estos. Se relaciona el comportamiento de tráfico Entre cada extremo de la conexión, donde se observa que se mantuvo activo con tráfico durante el mes. Se observa que se tuvo un promedio total de 8.09 Mbps.

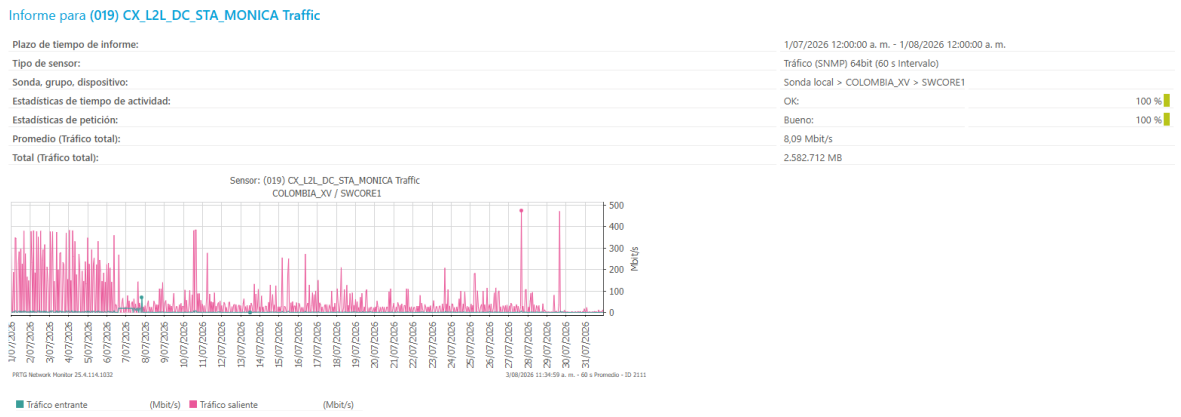


Ilustración 33 Extremo DC Bogotá

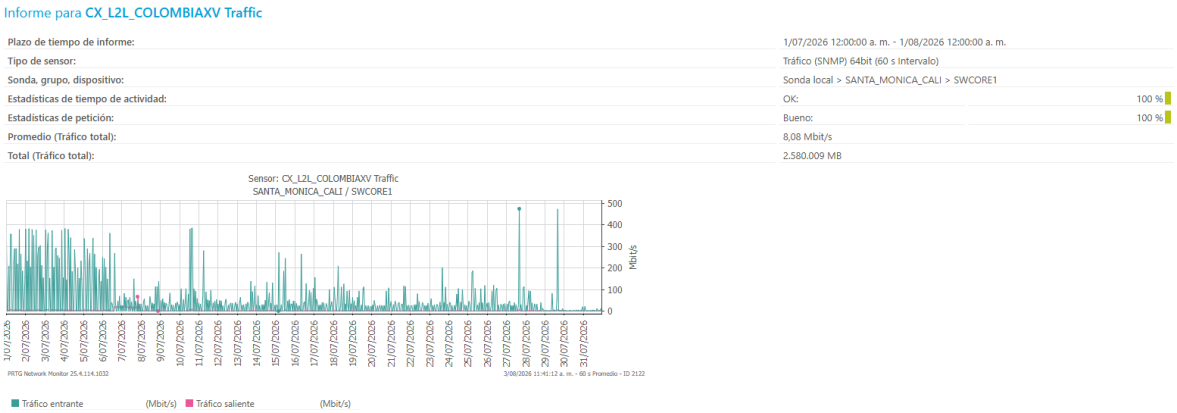


Ilustración 34 Extremo DC Cali

El canal de Internet de datacenter alterno se encuentra operativo, se observa que el canal tiene poco tráfico ya que el tráfico general se usa el canal ubicado en DC Principal. Se observa un promedio de tráfico total de 0.22 Mbps.

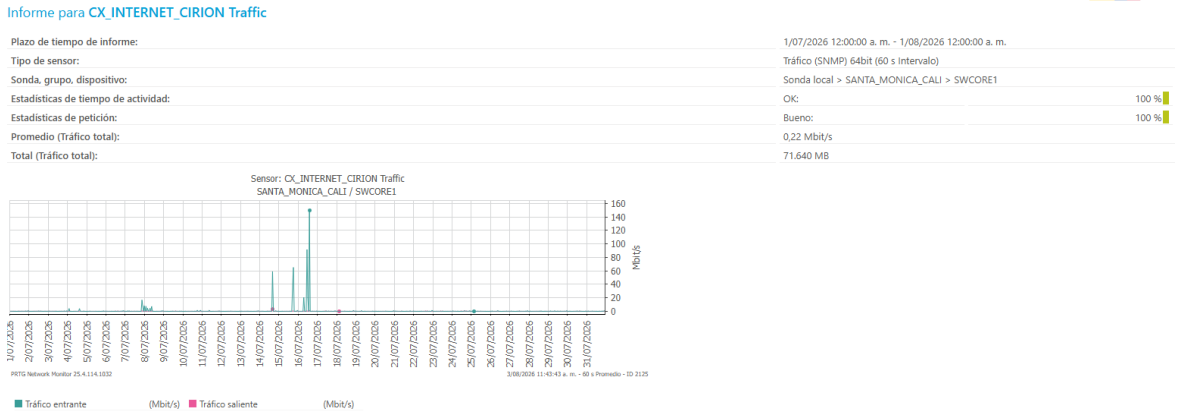


Ilustración 35 Estado canal de Internet DC Cali

Se relaciona el comportamiento del SWCORE de Datacenter alterno, donde se observa que funcionó de forma estable y no presentó caídas ni bloqueos:



Ilustración 36 Estado SWCORE Datacenter alterno

Se verifica el estado del HA (Stack) entre los SWCORE, donde se observa que el SW1 está con el rol de principal y sincronizado.

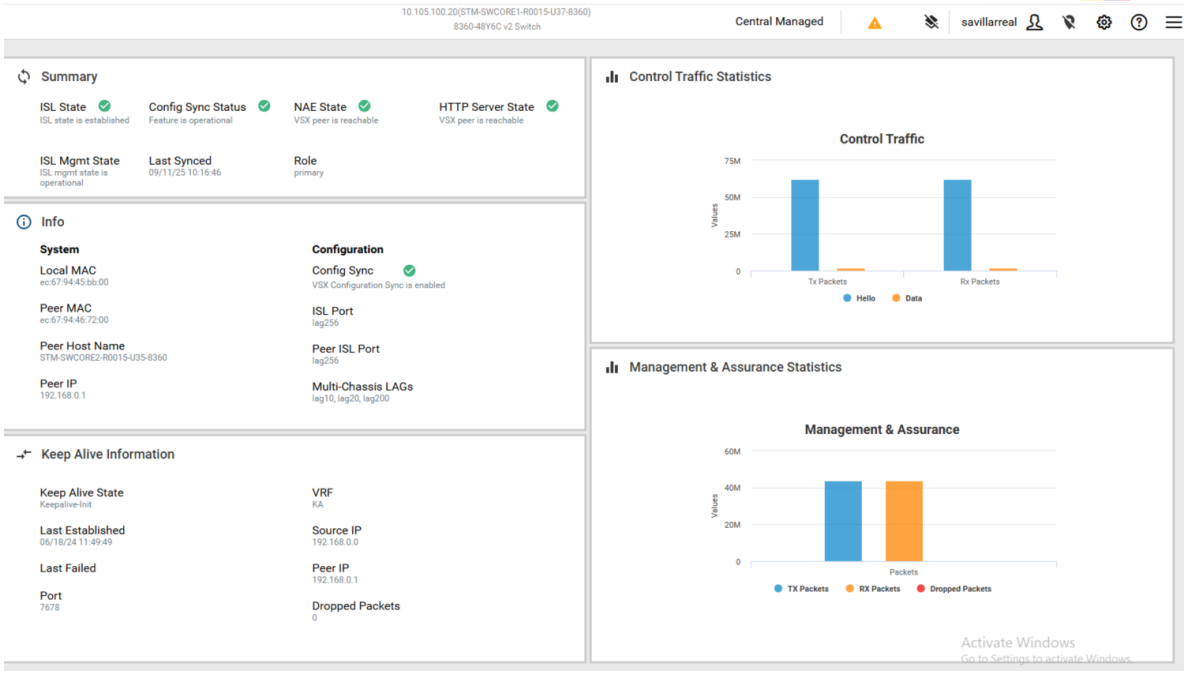


Ilustración 37 Estado HA SWCORE Datacenter alterno

Se verifica el canal MPLS de datacenter alterno, el cual se observa que se ha mantenido activo durante el mes de julio no se presentaron reportes de caídas de servicio. El tráfico en este canal es bajo debido a que es el correspondiente al canal del centro alterno. Se observa que se tiene un promedio de trafico de 0.05 Mbps.

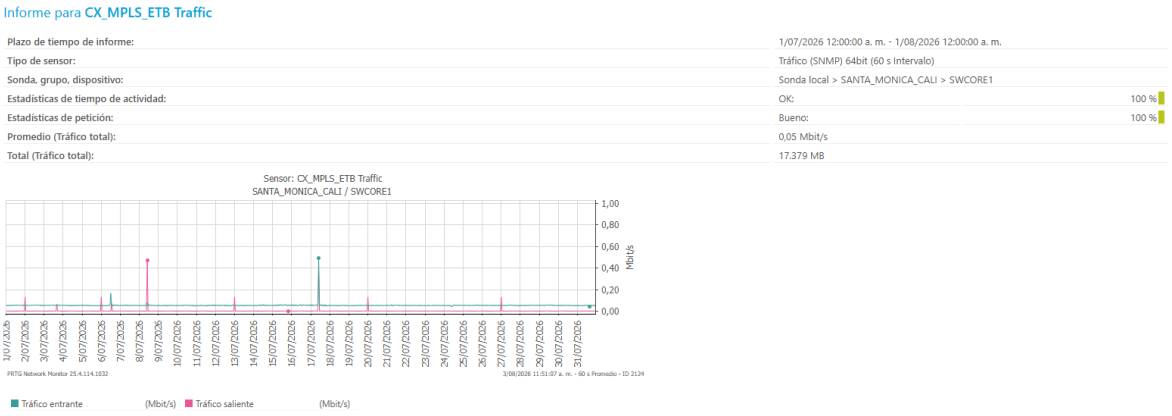


Ilustración 38 Consumo canal MPLS DC Alterno

Se verifica estado del equipo, donde se observa que presenta un uptime de 1 año y 17 semanas, el equipo no ha tenido problemas en procesamiento y memoria. Este equipo recibe la conexión MPLS de respaldo del DC principal, en caso de algún evento en este punto.

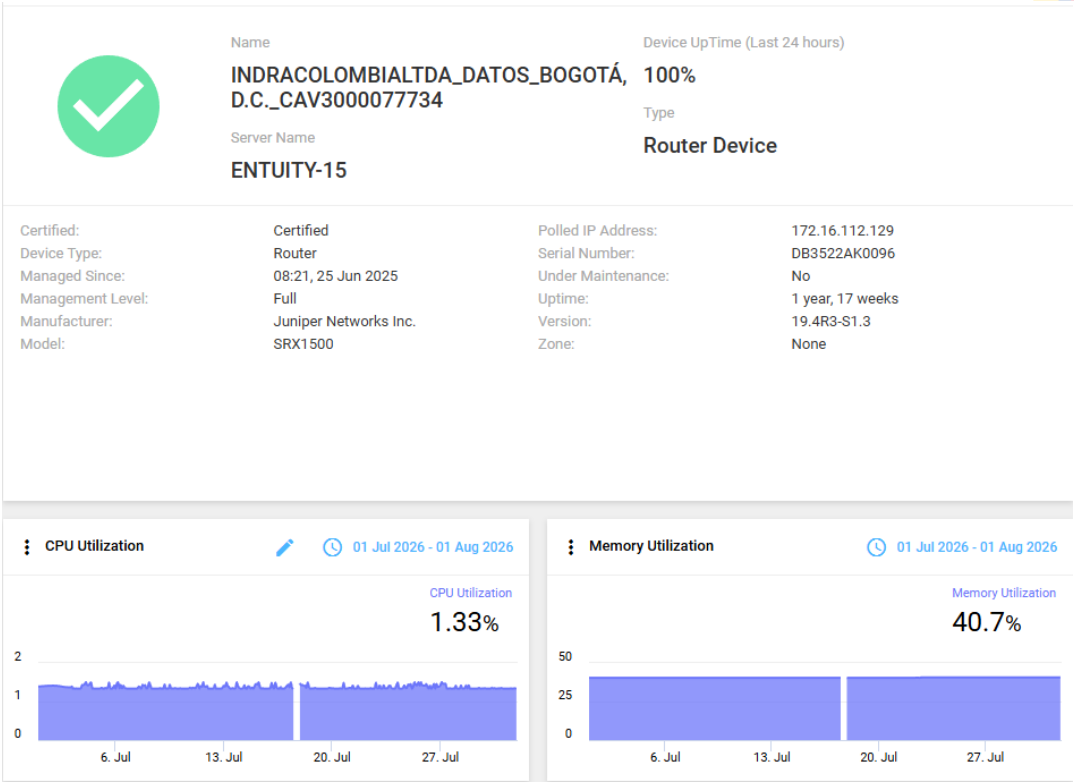


Ilustración 39 Estado Router MPLS DC Alterno

3.1.2 Procesamiento almacenamiento y respaldo Servicio Windows y Office 365.

Se mantuvo la validación periódica de la topología y la arquitectura del Directorio Activo como un componente esencial para asegurar su correcto funcionamiento y su alineación con las necesidades y los objetivos de la entidad.

Durante el período se gestionaron las siguientes solicitudes reportadas a través de Aranda las cuales fueron atendidas por los especialistas de Windows, en total este equipo tuvo la asignación 275 casos:

- 100 requerimientos de servicio relacionados a la asignación de licencias de Office 365 dadas las novedades recientes de personal en la entidad.
- 73 solicitudes de modificación de usuarios
- 23 requerimientos asociados a configuración o modificación de MFA.
- 17 solicitudes asociadas a la creación/modificación/eliminación de buzones compartidos.
- 15 solicitudes asociadas a configuraciones del File Server.
- 14 solicitudes de inactivación de usuarios en AD.

Las categorías restantes asociadas al servicio de Windows se mantienen con un reporte bajo reflejando la estabilidad del servicio de cara a usuario final. Dentro de las labores de administración se encuentran actividades tales como revisar regularmente la base de datos de usuarios para identificar cuantas inactivas, duplicadas o desactualizadas, y proceder con su eliminación o actualización según sea necesario.

La interacción de los requerimientos de servicio asociados al equipo de trabajo de Windows está relacionada en su gran mayoría a asesoría y consultas que generan los funcionarios con respecto al funcionamiento de los servicios de Office 365 a los cuales tienen acceso, seguido por los casos en donde se requiere de algún tipo de configuración sobre sus cuentas, shared mailbox o servicios a los que acceden. Se ha reducido la solicitud de generación de backups significativamente con respecto a meses anteriores y es un comportamiento habitual en el reporte mensual de este tipo de casos.

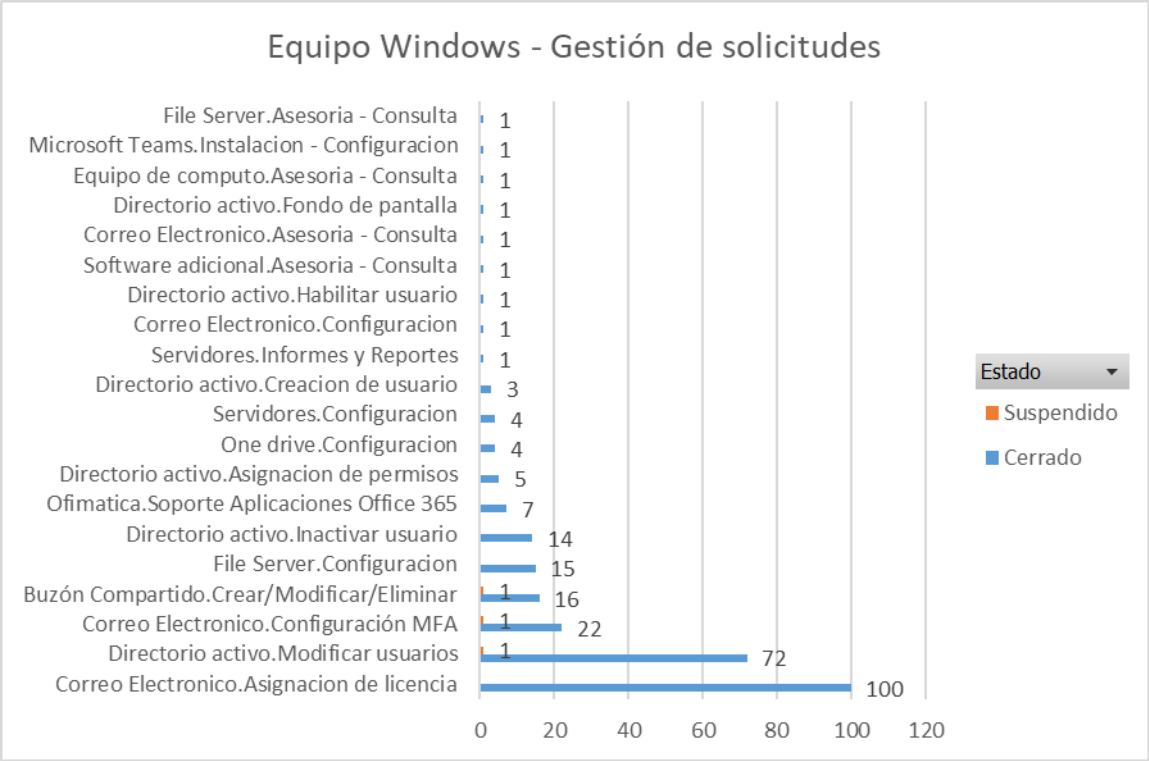


Ilustración 40 Gestión de Casos Windows

Para asegurar la actualización permanente del Directorio Activo y el estado de cada una de las cuentas de usuario final, es importante que la entidad remita de forma periódica (se sugiere bimestral o trimestralmente) informes relacionados con la desvinculación de funcionarios, contratistas, pasantes, entre otros, para realizar las actividades de actualización y liberación de licenciamiento de Office 365. También es importante precisar que es requerido el listado de nombres oficiales de todas las dependencias de la entidad, esto con el fin de estructurar un Plan de Calidad de la información del Directorio Activo y que se alinee con los nombramientos estipulados por la entidad.

Actualmente se está a espera del envío de la información de manera formal por parte de la entidad, pero se ha trabajado de manera articulada con la Oficina de Tecnologías de la Información, para fortalecer este ítem dentro de la entidad. Es un trabajo conjunto, pero se requiere contar con la línea base de información, lo anterior alineado al nuevo lineamiento de gestión y creación de usuarios emitido por la OTIC.

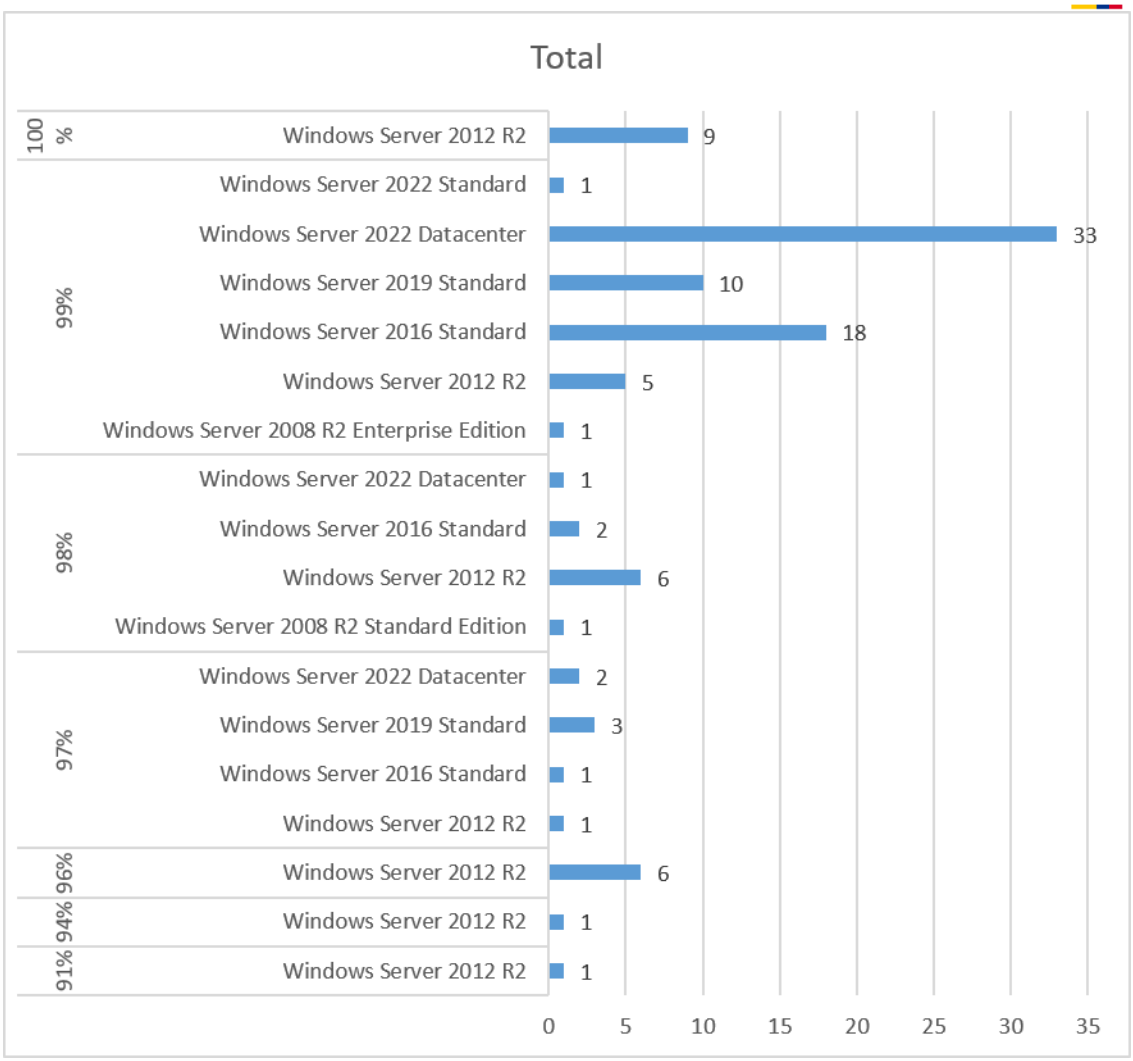


Ilustración 41 Cumplimiento WSUS

En atención a la revisión de las opciones de seguridad de línea base de Microsoft Microsoft 365 admin center por parte del equipo Windows:
Sugiere mejorar la postura de seguridad del tenant Microsoft 365 y conforme a las recomendaciones oficiales de Microsoft, presenta la recomendación de activar la política de seguridad “Block legacy authentication”, actualmente identificada como RECOMMENDED y en estado At risk.

La autenticación heredada (legacy authentication) utiliza protocolos antiguos que no soportan autenticación multifactor (MFA), lo que los convierte en uno de los principales vectores de ataque en entornos Microsoft 365.
De acuerdo con reportes oficiales de Microsoft, más del 97% de los ataques de credential stuffing y el 99% de los ataques de password spray explotan este tipo de autenticación.

La activación de esta política permitirá:

- Bloquear automáticamente protocolos inseguros como POP, IMAP, SMTP AUTH básico, MAPI antiguo y otros mecanismos de autenticación básica. → Puede

impactar algunas aplicaciones o sistemas de información que usen estos protocolos internamente, por lo que es vital que los desarrolladores de las aplicaciones y sistemas de información confirmen o no el uso de estos protocolos.

- Reducir de forma significativa el riesgo de compromisos de cuentas.
- Fortalecer el cumplimiento de buenas prácticas de seguridad alineadas con Zero Trust, Microsoft Secure Score y lineamientos de seguridad.
- Aumentar la efectividad real de MFA y las políticas de acceso condicional.

Por lo anterior, se **recomienda formalmente autorizar la activación de esta política**, como una medida preventiva clave para proteger la información, las identidades y los servicios corporativos en Microsoft 365.

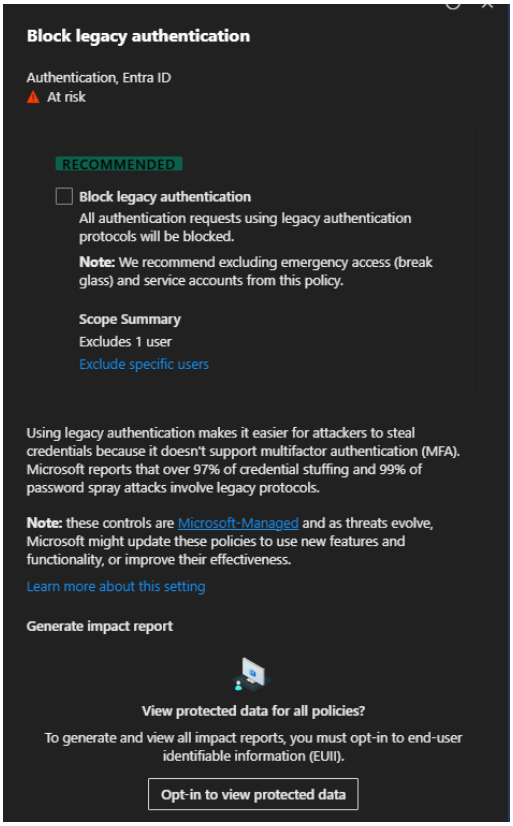


Ilustración 42 Block Legacy Authentication

Tras revisión proactiva del equipo de Windows, Microsoft ha anunciado oficialmente el **retiro definitivo del servicio Microsoft Project Online**, con **fecha efectiva el 30 de septiembre de 2026**.
Este anuncio fue publicado por Microsoft en su canal oficial y forma parte de su estrategia de modernización de las herramientas de gestión del trabajo.

A continuación, se detallan los aspectos más relevantes y el impacto técnico para la organización:

1. ***Alcance del retiro***

   El retiro aplica ***exclusivamente a Microsoft Project Online*** *(servicio SaaS). No se verán afectados los siguientes productos:*

- *Project Desktop (Project Standard / Professional)*
- *Project Server Subscription Edition*
- *Microsoft Planner (básico y premium)*

2. ***Fechas clave***

- ***1 de octubre de 2025:*** *Fin de venta de licencias Project Online-only para nuevos clientes.*
- ***Abril de 2026:*** *Los clientes existentes no podrán crear nuevos tenants de Project Online.*
- ***30 de septiembre de 2026:*** *Retiro definitivo del servicio. A partir de esta fecha no será posible acceder a proyectos, configuraciones ni datos almacenados en Project Online.*

3. ***Impacto técnico***

- *Las instancias actuales de Project Online continuarán operando con normalidad hasta la fecha de retiro.*
- *Tras el 30 de septiembre de 2026,* ***el acceso al servicio y a la información será eliminado****, por lo que existe riesgo de pérdida de datos si no se ejecuta una migración o respaldo previo.*
- *Integraciones actuales con SharePoint Online, flujos de trabajo y reportes dejarán de estar disponibles al finalizar el servicio.*
- *No se requiere ninguna acción administrativa automática por parte de TI para el cierre; sin embargo, la* ***responsabilidad de la migración y respaldo recae en la organización****.*

4. ***Alternativas recomendadas por Microsoft***

Microsoft orienta la transición hacia las siguientes plataformas:

- ***Microsoft Planner (con capacidades premium)****, integrado con Microsoft 365 y Copilot.*
- ***Project Server Subscription Edition****, para escenarios que requieren funcionalidades avanzadas de PPM.*
- ***Dynamics 365 Project Operations****, para organizaciones con necesidades de gestión financiera y de recursos.*
- *Continuidad del uso de* ***Project Desktop*** *como herramienta individual o complementaria.*

5. ***Recomendaciones***

- *Iniciar un* ***análisis de impacto*** *sobre los proyectos activos y dependencias actuales de Project Online.*
- *Definir una* ***estrategia de transición*** *(Planner, Project Server u otra alternativa).*
- *Planificar el* ***respaldo y exportación de la información*** *antes del cierre del servicio.*
- *Comunicar oportunamente a los usuarios finales y actualizar la documentación interna.*

Este cambio representa una oportunidad para modernizar la gestión de proyectos y alinearla con las capacidades actuales de Microsoft 365 y soluciones basadas en IA.
Se recomienda iniciar la planificación con suficiente antelación para evitar impactos operativos.

Link Oficial Microsoft
https://learn.microsoft.com/en-us/lifecycle/products/project-online?utm_source=chatgpt.com

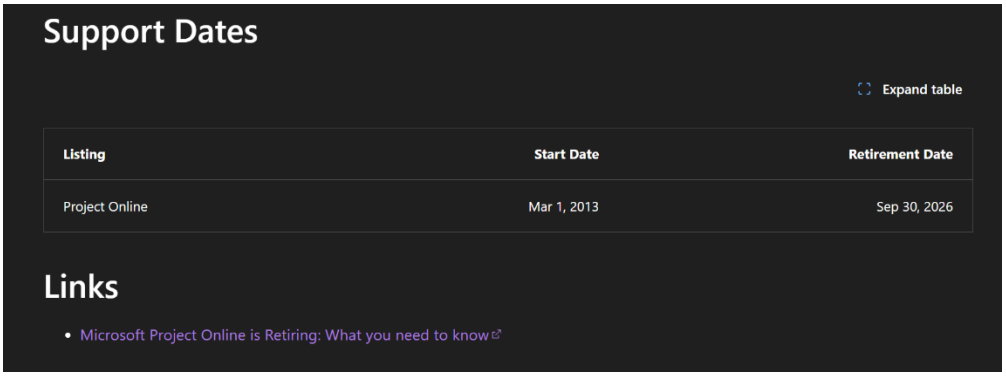


Ilustración 43 Fechas de Soporte

Licencias asignadas

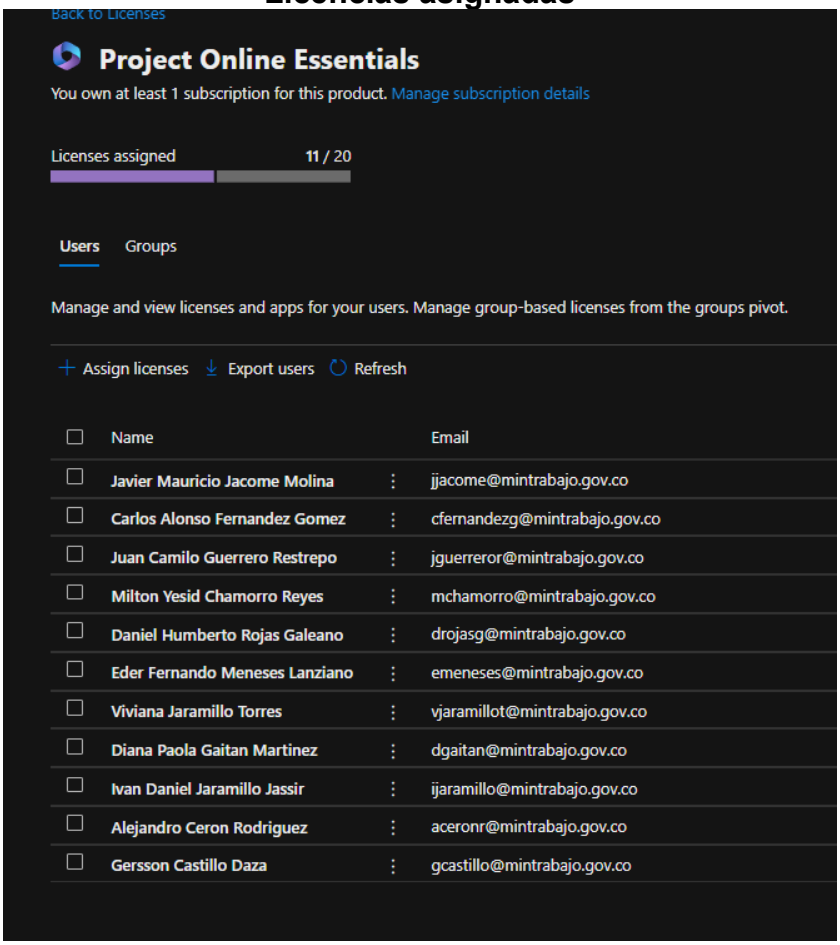


Ilustración 44 Licencias asignadas

3.1.3 Procesamiento, almacenamiento y respaldo - Nube Privada

Se continúa con la ejecución del plan de backups que se ejecuta semanalmente los días viernes y donde se generan respaldos completos de todas las máquinas virtuales críticas alojadas en VMWare, generando un backup full de la semana de

cada máquina y su almacenamiento, y teniendo la opción de un punto de retorno semanal en caso de contingencia o incidencia crítica.

Durante los procesos de afinamiento se ha identificado la criticidad y propuestas de planes de backups totales e incrementales para estas. En donde se identificaron máquinas que, por su criticidad y servicios alojados, ameritan un plan de Backup incremental diario, ya sea de discos, base de datos o máquina virtual completa, dependiendo del escenario y el tipo de máquina virtual. A este plan de Backups se han añadido servidores que han sufrido intervenciones técnicas con finalidad de adecuar la infraestructura virtualizada y depurar máquinas virtuales que no se encuentran en uso por parte de la entidad, pero sí que consumen capacidades que pueden ser aprovechadas por los entornos productivos.

Es importante mencionar que el escenario de arquitectura de la entidad actual nos ha permitido como operador de servicios tecnológicos, identificar diversas acciones de mejora que se han venido ejecutando de manera transversal durante el contrato, pero es importante dar visibilidad de los escenarios observados. Durante los procesos de afinamiento y egreso de equipos no productivos en Datacenter se logra visualizar componentes en estado sensible que podrían poner en riesgo la disponibilidad de servicios críticos como lo es el sistema de información histórica de nómina. Se observa que el servidor físico que aloja la máquina MINTRAB13 es un Dell (PowerEdge 2950) con fecha de salida a mercado 19/10/2015 y cuenta con un OS SUSE Linux Enterprise Server 11 (i586) con fecha de salida al mercado 24/10/2016.

Esta máquina, aunque aloja un sistema de información crítico para la operación, se encuentra en un estado de obsolescencia importante el cual no ha permitido una virtualización adecuada del recurso, por lo cual se debe convivir con esta infraestructura de manera provisional, hasta que se realice un aprovisionamiento en conjunto con el proveedor de este aplicativo a un entorno virtualizado, actualizado y con soporte de OS y de componente de infraestructura. Es importante mencionar que una de las fuentes de este servidor no se encuentra funcional y la batería se encuentra en un estado delicado el cual podría repercutir en la disponibilidad o performance de la aplicación que este servidor aloja.

Se dio visibilidad de esta situación para realizar las maniobras técnicas correspondientes de manera coordinada con el proveedor de este software a la entidad durante el mes de julio de 2024 se realizó esta sesión, en donde se identifican los servidores productivos como parte del escenario de virtualización de la entidad y que su proceso de migración a nuevos servidores de aplicación puede surtirse de la mano del área funcional. Actualmente se está a espera que el área funcional nuevamente permita un espacio de socialización para lograr entender el paradigma de consulta y validar que es posible migrar bajo una modalidad más simple y dejar la dependencia de esta infraestructura en estado de obsolescencia. Para el servidor MINTRAB13, el cual aloja una copia histórica del

anterior aplicativo y base de datos de nómina de la entidad, el proveedor nos confirma que no tiene administración y ningún tipo de gestión sobre el recurso y la información que esta aloja. La entidad confirma tener acceso de consulta a una base de datos y solo es consultada por demanda, pero no está asociada a ningún sistema de información productivo.

Es importante mencionar que el estado sobre la documentación de esta base de datos y el sistema de información que alojaba anteriormente es crítico ya que la entidad no cuenta con documentación, la empresa que desarrollo el aplicativo dejo de existir hace unos años y el desarrollador que tenía contacto con la entidad, desafortunadamente falleció previo al inicio del contrato de la UT.

Para el ítem de servidores de archivos, se refleja la información de diferentes áreas, hemos identificado lo siguiente:

- Se aloja información de diferentes áreas y dependencias sin una estructura organizacional definida.
- Únicamente existen carpetas relacionadas con tópicos en específico o áreas en concreto, pero no una estructura relacional.
- No se observa un estándar de nombramiento para las carpetas, archivos u organización, así como una ausencia de cuotas para controlar la capacidad de almacenamiento por área o carpeta.
- Usuarios con privilegios de asignación de permisos, es decir no existe una centralización en la administración de este servicio.
- Aunque existe un plan de backup incremental de la información, donde se ejecutan backups de la información o discos virtuales donde se aloja la información, estos backups se ejecutan diariamente en horario nocturno, por ende, si un usuario elimina un archivo, carpeta o fichero durante el transcurso del día, no hay garantía de recuperación de la información eliminada o manipulada por los usuarios de la entidad que posean este tipo de permiso.
- Se han encontrado backups de información personal de funcionarios y contratistas dentro del servidor de archivos, así como archivos multimedia, como fotos, videos y música.
- Se han encontrado archivos con extensiones .exe, desconociendo su origen y abriendo una brecha de seguridad importante, teniendo en cuenta que, si surgen incidencias de seguridad de la información, vulneraciones de seguridad, infección de archivos con virus o malware, este sería un canal en donde los usuarios podrían exponer este tipo de archivos que puedan tener esta vulnerabilidad.
- No existe un estándar de nombramiento de carpetas o archivos electrónicos visible en el file server o servidor de archivos, generando inconvenientes en la integridad de la información allí alojada. Es importante tener en cuenta, que Microsoft posee un límite de caracteres para nombramiento de carpetas y archivos, así como unas limitantes en los caracteres introducidos en los nombres, si este estándar no es cumplido, en los procesos de backup o copiado de la información, se podría perder acceso a la misma, debido a que

la ruta se vuelve tan extensa que la propia solución de Microsoft no le permite acceder a la misma.

- La entidad ha aplazado las actividades relacionadas con File Server hasta Julio 2025 y no se volvió a retomar de manera formal por parte de la entidad a pesar de las múltiples comunicaciones y acercamientos del equipo de Servicios centrales con el ánimo de migrar este servicio a una mejor condición. Hasta el momento no se ha obtenido retroalimentación por parte de la entidad.
- Se comparte informe de estado actual a la entidad, tanto a la nueva Jefatura de la Oficina de Tecnologías de la Información como el nuevo Coordinador de Soporte informático.
- Se está a espera de retroalimentación de la documentación de File Server compartida y de la estrategia propuesta para la migración hacia un nuevo entorno.
- La no migración de este tipo de recursos, así como la no actualización, pone en riesgo la implementación de DRP para este servicio en específico.

Es importante mencionar que la entidad no ha fortalecido o establecido una ruta para la retención de los backups de manera clara y concisa, por lo cual el equipo de trabajo creo el plan de backups y se definieron tiempos de retención de estos orientados a Infraestructura de acuerdo con las buenas prácticas y experiencia del equipo de trabajo. No se definen tiempos claros para estos recursos ni para documentos virtuales, file server o backups de usuario final por parte de la entidad.

Se ha solicitado Instrucción a la entidad instrucción con respecto a los siguientes recursos los cuales se encuentran alojados en la Nube Privada de la entidad y por su grado de Obsolescencia crítico y debido a que el sistema Operativo en el que se encuentran aprovisionados estos recursos se encuentra totalmente fuera de soporte, se requiere de una instrucción precisa y clara del cómo proceder con los siguientes recursos:

VM → MINTRAB25: Esta máquina virtual es usada como servidor de bases de datos con Motor MySQL la cual aloja las siguientes bases de datos: ACEDOC, ARL2014, ARLRIESGO, MOODLE_DB, MOODLE_PR, MOODLE_PR y backups históricos de la DDBB de WebABC. Es importante precisar que dentro de la Política de aprovisionamiento de Sistemas de Información emitida por la Oficina de TIC del Ministerio del Trabajo se define que los motores de Base de datos autorizados son MSSQL Server y Oracle. Por lo cual se requiere instrucción formal ya que esta base de datos soporta el Moodle Actual (que se encuentra productivo, pero no se ha dado de baja por la nueva versión que su DDBB fue migrada a SQL Server) y la aplicación ACEDOC la cual también esta alojada en un Apache Tomcat dentro el servidor.

Ambas aplicaciones dependen de la Subdirección de IVC.

- Actualización MINTRAB25: La máquina fue migrada a Windows 2022 y fue separada la base de datos en un servidor independiente, se están realizando pruebas de conectividad de la aplicación. A la fecha la aplicación está estabilizada y solo restaría la validación del área funcional y el visto bueno para apagado y reemplazar el servidor.

Con respecto a los requerimientos del servicio de Nube Privada su categorización nos indica que el comportamiento de reportes asociados a servidores Windows es de mayor demanda en el proyecto, asociado a configuraciones de servicios, revisión de consumo de capacidades a través de alertamientos de la herramienta de Monitoreo Zabbix o solicitud de accesos a carpetas compartidas del servicio de File Server. Se ha venido trabajando articuladamente con la Coordinación de Soporte Informático manteniendo informado del comportamiento de la nube privada y sus capacidades. Así como el apoyo transversal en los proyectos escalados por las áreas funcionales.

Es importante mencionar que se ha venido creando diferentes VM asociados a nuevos servicios que aprovisionará el Ministerio del Trabajo, pero en principio se encuentran en su fase de pruebas por lo cual solo se han creado VM de pruebas. Algunas VM ya fueron intervenidas, pero hasta el momento no son productivas debido a que se está a espera de VB o revisiones de las áreas funcionales.

Para la Nube Privada, se registraron en Aranda 51 solicitudes, 45 de las cuales corresponden a requerimientos de servicio, 5 incidentes y 1 solicitud de cambio. A continuación, se presentan las solicitudes y su estado al final del período.

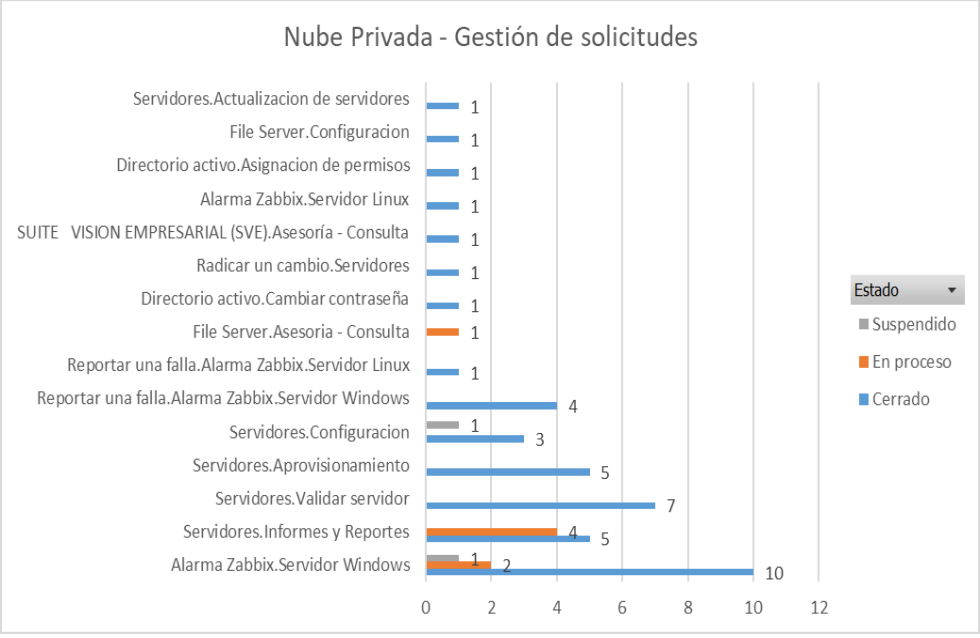


Ilustración 45 Gestión Nube Privada

Es importante precisar que la mayoría de los requerimientos de servicio escalados a la línea de servicio de Nube Privada son escalamientos internos del mismo equipo de trabajo relacionados con optimización de servicios, configuraciones necesarias dentro del servicio, apagado de servidores por desaprovisionamiento, backup de la información, aprovisionamiento de servidores, revisión o validación de recursos asignados. De acuerdo con lo anterior se deja claridad que la línea de Nube Privada está compuesta por los componentes:

- Virtualización VMWare.
- Virtualización Oracle Linux KVM.
- Almacenamiento.
- Backup de la Información.
- Infraestructura Física.
- Datacenter.

Se exponen las capacidades definidas para la nube privada de acuerdo las fichas técnicas, en primera instancia se definen las capacidades definidas contractualmente:

Descripción ítem	Mínimo requerido
Capacidad VCP	657 vCPUs en sitio de producción.
Capacidad Memoria Virtual	2.637 TB de memoria virtual en sitio de producción
Capacidad de Almacenamiento	120 TB usables en sitio de producción
Numero Servidores	106 servidores

Tabla 41 Capacidades iniciales

En segunda instancia se exponen las capacidades definidas tras la ampliación de capacidades de la nube privada:

Descripción / Características	Mínimo requerido
Capacidad VCP	854 vCPUs en sitio de producción.
Capacidad Memoria Virtual	3.38 TB de memoria virtual en sitio de producción
Capacidad de Almacenamiento	156 TB usables en sitio de producción
Numero Servidores	106 servidores (ítem variable, de acuerdo con capacidades consumidas)

Tabla 42 *Capacidades modificatorio*

Se observa una reducción de consumo de capacidades para los ítems de procesamiento y almacenamiento significativos, es una tendencia que se seguirá observando de acuerdo con las migraciones de aplicaciones planteadas.

Total MinT (Con servidores para desaprovisionar + ambientes de pruebas)	
Descripción Características	Total
vCPU	730
RAM	3.06 TB
Almacenamiento	131 ,2TB
Numero de Servidores	109

Tabla 43 *Total capacidades + servers desaprovisionamiento*

Total MinT (Sin servidores para desaprovisionar con ambientes de pruebas)	
Descripción - características	Total
vCPU	730
RAM	3.06 TB
Almacenamiento	131,2 TB
Numero de Servidores	106

Tabla 44 *Total capacidades consumidas*

Total MinT (Sin servidores para desaprovisionar sin ambientes de pruebas)	
Descripción - características	Total
vCPU	556
RAM	2.4 TB
Almacenamiento	113 TB
Numero de Servidores	77

Tabla 45 Total capacidades sin servers de pruebas

Total MinT (Servidores Pruebas y Desarrollo)	
Descripción características	Total
vCPU	160
RAM	602 GB
Almacenamiento	16 TB
Numero de Servidores	29

Tabla 46 Total capacidades ambientes pruebas

- vCPU Ficha: **854** a vCPU consumida: **730 (85.4%)**
- Memoria Ficha: **3.3 TB** a Memoria consumida: **3.06 TB (92.7%)**
- Almacenamiento Ficha: **156 TB** a Almacenamiento consumido: **131,2 TB (84.1%)**
- Número de Servidores Ficha: **106** a Numero de Servidores disponibles: **106**

Se realizó validación de los datos, realizando exclusión de la información asociada a las capacidades consumidas por parte de los servidores de servicios de la operación, es decir máquinas aprovisionadas para operar un servicio y que no hicieron parte de la virtualización de la nube privada de la entidad, aun así realizando esta exclusión, la entidad se encuentra en un escenario de consumos dentro de lo acordado en la ficha en los ítems de vCPU y RAM y almacenamiento aumento ligeramente sus consumos, teniendo en cuenta que se están excluyendo los servidores asociados al servicio de Backup los cuales deben validarse en conjunto con la entidad para considerar o no excluir estos consumos de capacidades de almacenamiento, ya que incluyéndolos dentro de la revisión, nuevamente entraría el ítem de almacenamiento superando la capacidad contratada.

Es importante mencionar que la entidad cuenta con 10 Servidores de pruebas nuevos asociados a nuevas aplicaciones y existe una redundancia de servidores

del servicio SIAS, ya que se aprovisionaron los 3 nuevos servidores de pruebas para este servicio, pero no se encuentran en uso actualmente, por lo cual en cuanto se realice el cambio de los servidores antiguos a los nuevos, se reducirán las capacidades consumidas, así como el servidor creado de manera temporal para el Asessment realizado para aplicaciones a migrar hacía Azure ya fue desaprovisionado tras autorización de la OTIC. De igual forma no se restan las capacidades de estos servidores al no estar en escenario productivo o pruebas pero dan la visual a la entidad de que no están superando su holgura de crecimiento.

vCPUs		RAM - TB	Capacidad Disco
Consumos	**730**	**3.06 TB**	**131.2 TB**

Tabla 47 *Consumos totales*

Es importante mencionar que, en el proceso de redimensionamiento de la nube privada de la entidad, los ambientes de pruebas son los que están creciendo de manera continua (nuevos aprovisionamientos), por lo cual se debe entrar a revisar procesos de reducción de capacidades de estos entornos. De igual forma se han reducido capacidades y desaprovisionado servidores para reducir los consumos sin afectar la disponibilidad de servicios productivos. En el escenario actual, la entidad tiene capacidad de crecimiento o ampliación de capacidades de los servicios ya aprovisionados. Se está en proceso de revisión para reducción de capacidades de servidores de aplicación como SISINFO por asignación de capacidades en RAM elevadas en contra parte con sus consumos.

También se expone que el servidor MINTRAB60 que cumple su rol como File Server principal, ha sufrido diferentes intervenciones de ampliación de capacidades de disco virtual, teniendo en cuenta que este servicio a crecido exponencialmente, se está trabajando en una política de retención de backups de usuario final, ya que estos backups están consumiendo una cantidad importante de almacenamiento en el file server y a largo plazo se puede convertir en una actividad y/o tarea demandante de almacenamiento y de tareas operativas que puede convertirse en una solución no sostenible dadas las capacidades de almacenamiento contratadas. Se está realizando depuración de los backups de PST ya entregados a usuario final con el fin de optimizar cargas de almacenamiento en el File Server. Se está a espera de un plan de trabajo en conjunto con la entidad, tanto para depurar la información, como para poder migrar a una infraestructura mucho más estable.

En el ejercicio de arquitectura para Azure, se ha enfatizado en la estructura actual, como se encuentra el Tenant a nivel de componente de infraestructura como servicio en nube y la interacción contra otros componentes de aplicación, ya sea en la misma nube pública, como conexiones hacia On Premises. Se definen los escenarios en donde se plantean cambios o mejoras sobre las propias implementaciones del Ministerio en el marco de la implementación de buenas prácticas para la gestión y

administración de estos componentes. Así como el seguimiento proactivo de las sesiones y documentación técnica entregados por Go To Cloud en el marco de Assesment sobre el Tenant de la entidad.

3.1.4 Aplicaciones Especializadas

Se observaron escenarios en donde se identifican aplicaciones que por su arquitectura y uso de componentes deprecados como versiones anteriores de Framework, sistema operativo entre otros componentes, no permiten una migración transparente a un OS con soporte vigente, por lo cual hay que explorar cada escenario para las aplicaciones con un énfasis .Net para realizar los procesos de separación y adecuación de cada aplicativo, se dará visibilidad de las aplicaciones impactadas y alojadas en el server MINTRAB23 para concretar sesiones con áreas funcionales y estructura un plan de trabajo de afinamiento y transición a sistemas operativos y componentes .Net más actualizados. Estos procesos de afinamiento permitirán un mejor rendimiento sobre las aplicaciones de la entidad, una mejora en su performance y la alineación con buenas prácticas y modelos de arquitectura que permiten una mejor administración, soporte y monitoreo de estas. Estas aplicaciones han sido migradas a nuevos entornos 2022 y algunas han sido desaprovisionadas por solicitud de las áreas funcionales y la OTIC.

En el marco de esta validación, se realizó un escaneo de vulnerabilidades a nivel de aplicaciones en donde el equipo de seguridad (SOC) identifica diversas vulnerabilidades asociadas a aplicaciones alojadas en entorno virtualizado (On premises) en servidores de aplicación que poseen obsolescencia tanto a nivel de sistema operativo como a nivel de arquitectura de software. En estos informes se mencionan problemas a nivel de parámetros de seguridad, la falta de credenciales robustas puede exponer la infraestructura a riesgos significativos, tales como accesos no autorizados, ataques de fuerza bruta, y otras amenazas de seguridad. Para mitigar estos riesgos y proteger la información sensible, es crucial que todos los usuarios adopten contraseñas fuertes y seguras.

Es importante que la entidad tenga visibilidad de que los procesos de actualización de sistema operativo van de la mano con mitigación de vulnerabilidades y que estos procesos podrían afectar la disponibilidad de las aplicaciones por su estructura y arquitectura y por ende se debe obtener la información de las aplicaciones mencionadas en los correos electrónicos enviados a la Coordinación del Grupo de Soporte Informático para así minimizar los impactos que pueden surtir las aplicaciones al migrarse. Haciendo énfasis en que aplicaciones realmente están productivas y que sitios en el IIS deben conservarse o no, ya que, con esto, se pueden tomar decisiones enfocadas en el dimensionamiento de los nuevos servidores con sistema operativo actualizado y bajo soporte y de las capacidades asignadas a estos y aprovechar de una forma más optima los recursos contratados.

Se propuso la independización del aplicativo SIRITI del servidor MINTRAB23 el cual aloja más de 40 aplicativos, lo cual podría indicar un inconveniente a la hora de gestionar controles de cambios ya que el despliegue de paquetes podría afectar el funcionamiento de otra aplicación que coexista en este entorno, esto debido a que cada aplicación fue desarrollada con diferentes prácticas y arquitecturas que a la hora de aprovisionarse en un solo entorno, podría provocar inconvenientes de cara al despliegue de controles de cambios para cada aplicación.

Tras este ejercicio la aplicación ya se encuentra migrada y lista para salir a producción en un servidor totalmente independiente y sin coexistencia de otras aplicaciones en su mismo entorno, lo cual permite un mejor funcionamiento del componente GeoServer.

La aplicación ACEDOC fue migrada de manera exitosa a un nuevo entorno de DDBB y de aplicación. Por ahora las pruebas que hemos realizado han sido satisfactorias a nivel técnico, pero para una salida a producción exitosa, es requerido que el área funcional, pueda realizar pruebas sobre este nuevo entorno, garantizando accesibilidad y funcionalidad de la aplicación, esto con el fin de dar viabilidad operativa a una salida a producción y posteriormente dar de baja los servidores actuales que se encuentran en estado de obsolescencia crítico y es un riesgo para la entidad a nivel de seguridad informática y de la información.
Actualmente el acceso a este nuevo entorno de ACEDOC es el siguiente: http://acedoc.mintrabajo.gov.co/acedoc_mintrabajo/index_ingreso.php

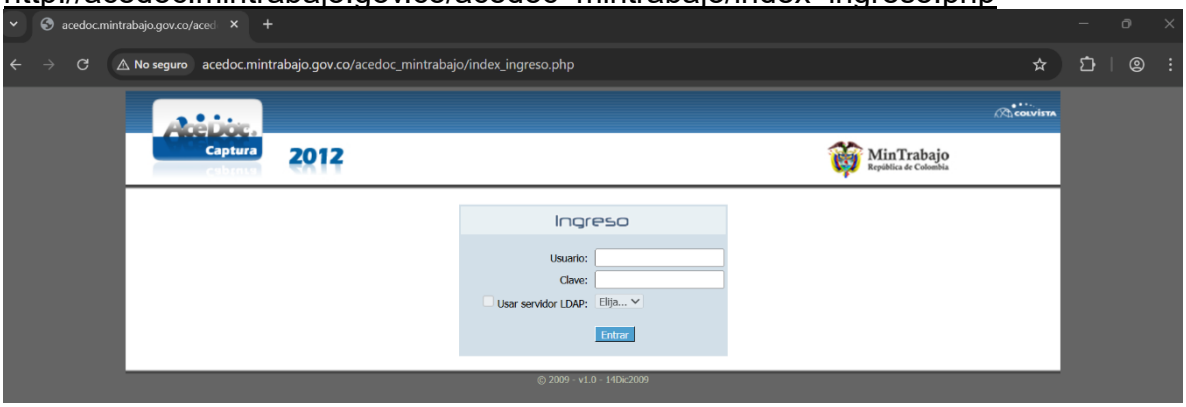


Ilustración 46 Nuevo entorno ACEDOC

Se comparte la información de gestión de casos por categoría del servicio de aplicaciones especializadas. En la herramienta Aranda se registraron un total de 844 solicitudes para el servicio, así:

- 688 requerimientos
- 152 incidentes
- 6 cambios

A continuación, se presenta la distribución de las solicitudes por categoría y su estado al final del período:

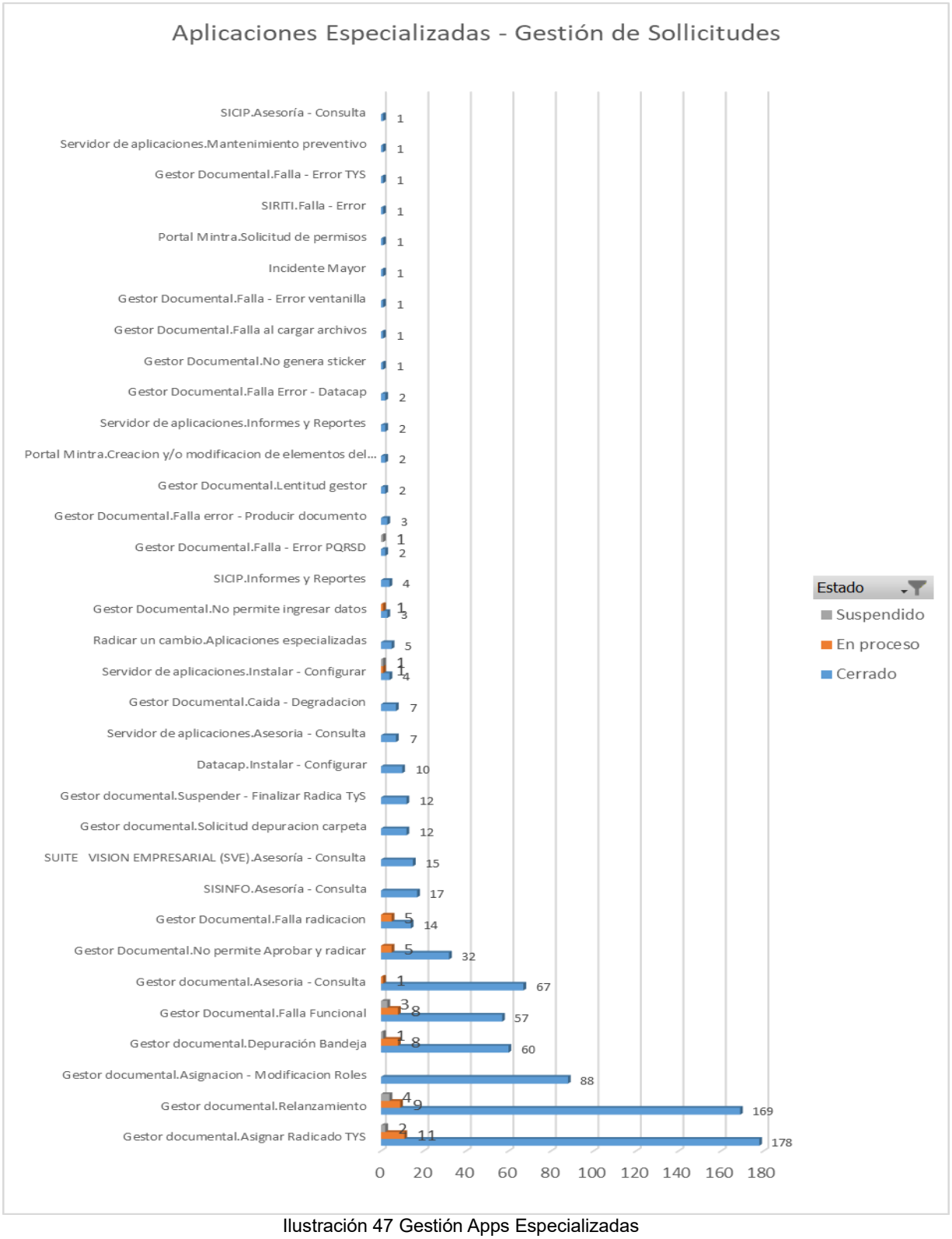


Ilustración 47 Gestión Apps Especializadas

Migración Aplicaciones .NET

En el marco de la migración de aplicaciones .NET, se observan que algunas aplicaciones están marcadas como productivas, pero actualmente no están operativas, se debe contemplar si realmente se encuentran en uso por parte de la entidad para realizar la migración del componente NET, DDBB SQL y Sistema Operativo o si de lo contrario debe generarse un backup, pero no continuar con la migración de estas aplicaciones.

De acuerdo con el contexto anterior se informa que las aplicaciones especializadas migradas a satisfacción a nivel de base de datos a entorno SQL Server 2022 son las siguientes:

- Tmigrante
- FTrutec
- Biblioteca Virtual de trabajo
- Calculadora Laboral
- Censo Sindical
- Centro de entrenamiento
- Conjovenes
- Contratos
- Estado Joven
- FTrue
- Saber hacer vale
- Subsistema de formación para el trabajo
- Ftalentos empleo

Actualmente solo restan las aplicaciones Observatorio, nómina y cobro coactivo para migración a nuevo entorno.

Portal Web

Se realizó el paso a producción del micrositio de prevención de ofertas laborales fraudulentas y trata de personas., esto con el visto bueno de la oficina TIC y la Web Máster de la entidad.

IBM-Gestor Documental

Se realizó mantenimiento en la base de datos del gestor documental para desfragmentar campos de unas tablas y así, mejorar el rendimiento de la aplicación.

Se comparte la información de gestión de casos por parte del Equipo de IBM, en la herramienta Aranda se registraron un total de 654 solicitudes para el servicio, así:

- 518 requerimientos
- 136 incidentes
- 1 cambio

A continuación, se presenta la distribución de las solicitudes por categoría y su estado al final del período:

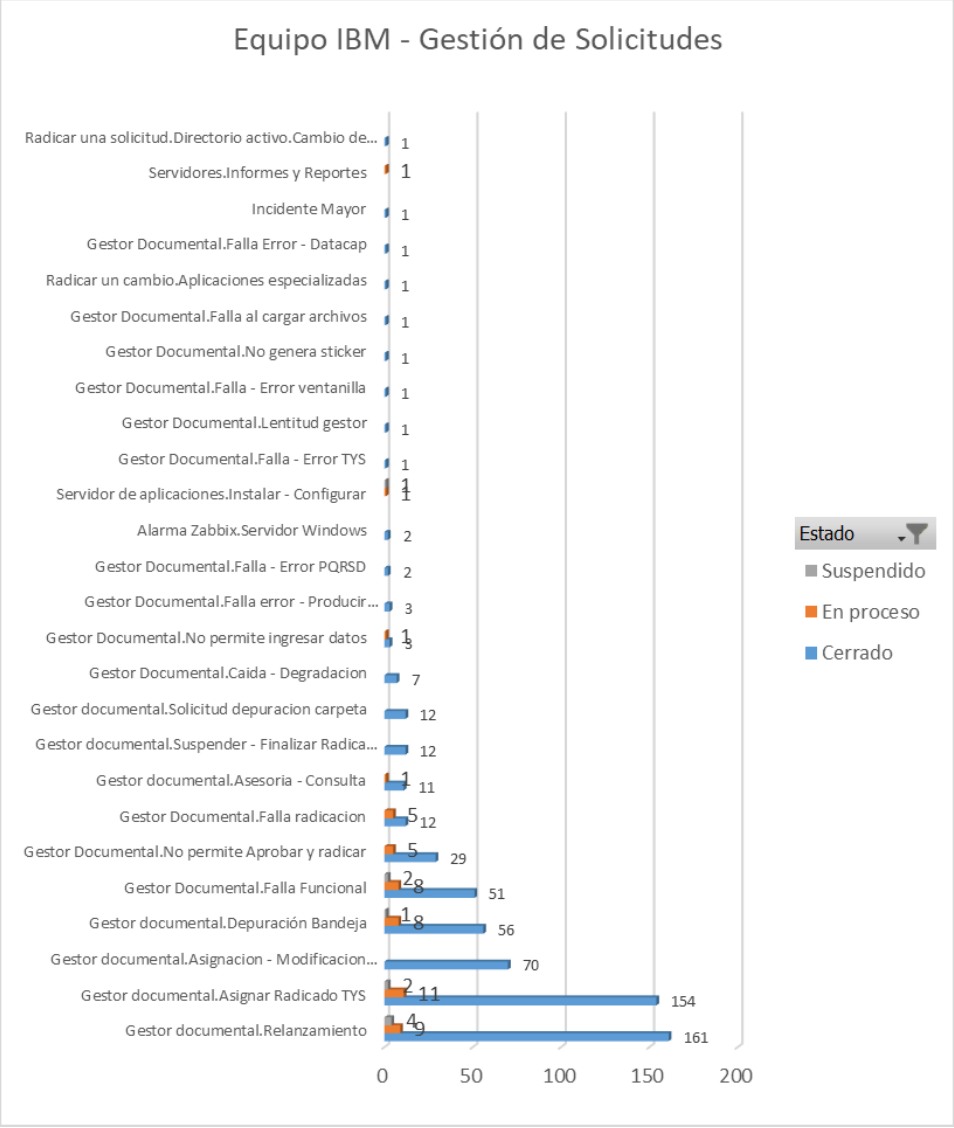


Ilustración 48 Gestión Casos IBM

A continuación, se detalla el Top 5 de las categorías que generan mayor gestión de casos en la plataforma de gestor documental:

- Relanzamiento de tareas (174 casos) Asociado a diferentes razones dentro de la operación, como redistribución de tareas, errores funcionales, depuración de instancias entre otros.
- Radicar una solicitud - Asignar Radicado TYS (167 casos) Las causas principales están asociadas a la reasignación y asignación de actividades que fueron cerradas por tiempo, así como a solicitudes inactivas debido a mantenimiento del sistema.
- Asignación - modificación de roles (70 casos).
- Radicar una solicitud - Depuración de Bandeja (65 casos) Eliminación de casos activos una vez el proceso de documentos ha sido transferido al módulo de Instrumentos Archivísticos, conforme al ciclo de vida documental.
- Falla funcional (61 casos) Consultas relacionadas con procesos del Gestor Documental en las que los usuarios reportan errores durante los procesos o flujos durante radicación o al intentar subir documentos, lo cual impide completar correctamente la solicitud, así como desconocimiento del usuario de la operación realizada o del flujo como está estructurado.

Es importante mencionar que, así como se requieren licenciamiento para el aprovisionamiento de la capa de aplicación, también deben validarse la disponibilidad de licenciamiento de base de datos, ya que actualmente la totalidad de licencias de DDBB Oracle, se encuentran asignadas a las bases de datos del portal web, gestor documental, nómina y SISINFO. Y que al cambiar su modelo de base de datos a Cluster Activo el licenciamiento del otor puede cambiar y deban contemplar un crecimiento, adquisición o cambio del tipo del licenciamiento de acuerdo a las nuevas arquitecturas implementadas dentro de la Infraestructura de la entidad.

Mes	Suma de Total Instancias
Diciembre 2025	109540
Enero 2026	83242
Febrero 2026	148858
Marzo 2026	151041
Abril 2026	139558
Mayo 2026	138164
Junio 2026	22945
Julio 2026	157896
Total acumulado	947.398

Tabla 48 *Suma Instancias*

Mes	Suma de Total Documentos
Diciembre 2025	174277
Enero 2026	136435
Febrero 2026	177295

Marzo 2026	202780
Abril 2026	175530
Mayo 2026	165033
Junio 2026	182745
Julio 2026	211511
Total acumulado	1.251.329

Tabla 49 Total Docs

Mes	Suma de Total radicados
Diciembre 2025	**59671**
Enero 2026	53821
Febrero 2026	68311
Marzo 2026	74463
Abril 2026	68784
Mayo 2026	66376
Junio 2026	66314
Julio 2026	83195
Total, acumulado	481.264

Tabla 50 Total Radicados

De acuerdo con el funcionamiento actual del sistema de gestión documental, se exponen las capacidades actuales contrastadas con las capacidades requeridas a nivel de Cores asignados a las máquinas virtuales aprovisionadas para la puesta en marcha del Gestor documental. Es importante mencionar que estas capacidades solamente enmarcan ampliación para funcionamiento del escenario actual, es decir una optimización del sistema actual sin incluir nuevos desarrollos o funcionalidades ya que estas deben ser dimensionadas y expuestas de manera específica para plasmar el crecimiento de las capacidades de los contenedores del componente IBM.

En atención al requerimiento de renovación del licenciamiento de Oracle, en revisión con el equipo de trabajo sugerimos el siguiente escenario de asignación de cores virtuales para las bases de datos de Oracle de la entidad:

Es importante mencionar que únicamente se dimensionaron dos entornos de pruebas que contemplamos como críticos y que la entidad debería tener; base de datos de gestor documental y base de datos de la página web.

De acuerdo con este esquema de licenciamiento (únicamente para base de datos) el licenciamiento de WebLogic, Diagnostic Pack y Tuning Pack no cambiaría y no incluiría el Oracle Premier Support for Systems que es el que soporta la infraestructura física del ODA X5, pero es importante que la entidad contemple el licenciamiento de la herramienta Oracle Cloud Control, que permite la visualización en tiempo real de las bases de datos, máquinas virtuales y capas medias de Oracle.

Para ello, sugerimos la importancia de validar con el proveedor de estas licencias, para que realice la aclaración de acuerdo con este dimensionamiento y que el Ministerio del trabajo, tenga claridad del costo de las licencias que requiere renovar para la vigencia 2025-2026.

Numero de PVU por Core	70			
Server Cores actual	Consumo Total PVU actual	Cores Adicionales	Cores Totales (Redimensionado)	PVU Totales (Redimensionado)
6	420	4	10	700
4	280	4	8	560
2	140	0	2	0
8	560	0	8	0
4	280	0	4	0
8	560	2	10	700
8	560	0	8	0
8	560	0	8	0

Tabla 51 Dimensionamiento Servers IBM - Virtualización Optima

De acuerdo con lo definido contractualmente la distribución de licenciamiento sobre la capa de aplicación es la siguiente:

- Servidor WANSD: 7 cores asignados actualmente a transición a 8 cores.
- Servidor BAW: 5 Cores asignados actualmente a transición a 6 cores.
- Servidor BUS Conectó: 3 Cores asignados actualmente à transición a 4 Cores.

Esto se traduce en licenciamiento de componente IBM de la siguiente forma:

P/N	DESCRIPCION	QTY
D03S0LL	IBM App Connect Standard Processor Value Unit (PVU) License + SW Subscription & Support 12 Months	70
D20RULL	IBM Cloud Pak for Business Automation Virtual Processor Core License + SW Subscription & Support 12 Months	10
D55WJLL	IBM WebSphere Application Server Network Deployment Processor Value Unit (PVU) License + SW Subscription & Support 12 Months	70

Ilustración 49 Licenciamiento adicional componente IBM

Bases de Datos

A nivel del servicio que soporta las bases de datos de la entidad, los especialistas MSSQL y Oracle han realizado diferentes actividades para dar diagnóstico y estado actual de las aplicaciones a nivel transaccional, de capacidad y de almacenamiento, identificando diferentes acciones de mejora para el gestor documental, que posee una criticidad elevada para la misionalidad y la funcionalidad del ministerio.

Se han presentado diferentes controles de cambios para las bases de datos alojadas y soportadas por MSSQL, cambios relacionados con ventanas de mantenimiento, estabilización, Backup, migraciones de versión y de base de datos, reinicios asociados a ventanas de mantenimiento, ejecución de scripts entre otras actividades descritas dentro de cada RFC. Según las acciones de mejora identificadas en cada ventana de mantenimiento, se han construido documentos, topologías e informes asociados a las indisponibilidades (asociadas a ventanas de

mantenimiento, procesos de estabilización de proceso de bases de datos y afinamiento de servicio) de los servicios soportados desde bases de datos.
Se comparte la información de gestión de casos por parte de los Especialistas de Base de Datos, en la herramienta Aranda se registraron un total de 31 solicitudes, así:

- 21 requerimientos
- 10 cambios

A continuación, se presenta la distribución de las solicitudes por categoría y su estado al final del período:

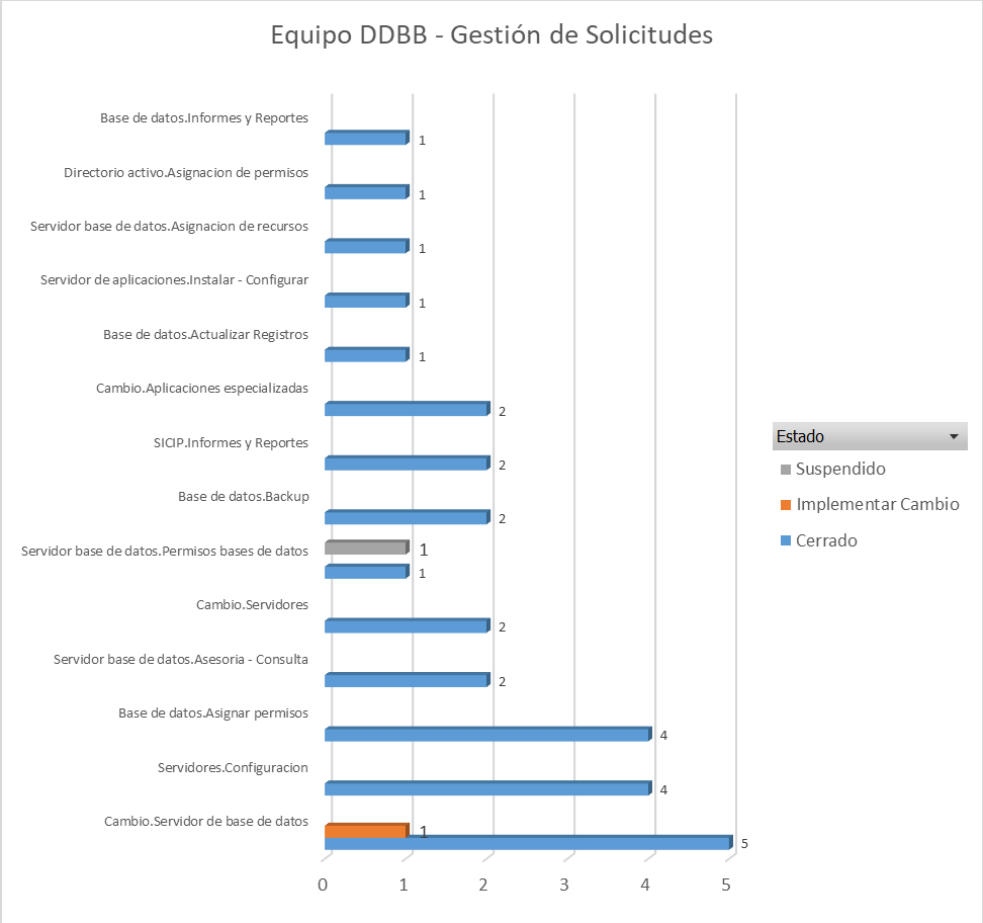


Ilustración 50 Gestión DDBB

A nivel de los procesos de migración y actualización de versión de MSSQL Server, ya se encuentran aprovisionados los servidores y ya se realizaron las pruebas de restauración en nuevos entornos, se garantiza interoperabilidad con las DDBB de MSSQL que consumen servicios de Oracle y ya se encuentran varias bases de datos en el nuevo entorno y se encuentran productivas. Durante el mes de Julio se migró casi el 85% de las DDBB de producción y pruebas y se encuentran operando en los nuevos servidores de MSSQL Server. Debido al cambio de versión, se

realizaron cambios dentro de las configuraciones para obtener una compatibilidad completa en versión 2022. Todo de manera satisfactoria y sin indisponibilidades no controladas.

- Estado de las Bases de Datos – Oracle Gestor Documental

A nivel del versionamiento de las bases de datos en Oracle se mapea la siguiente matriz expuesta por Oracle en donde se observa las fechas de soporte, soporte extendido y compatibilidad de estos:

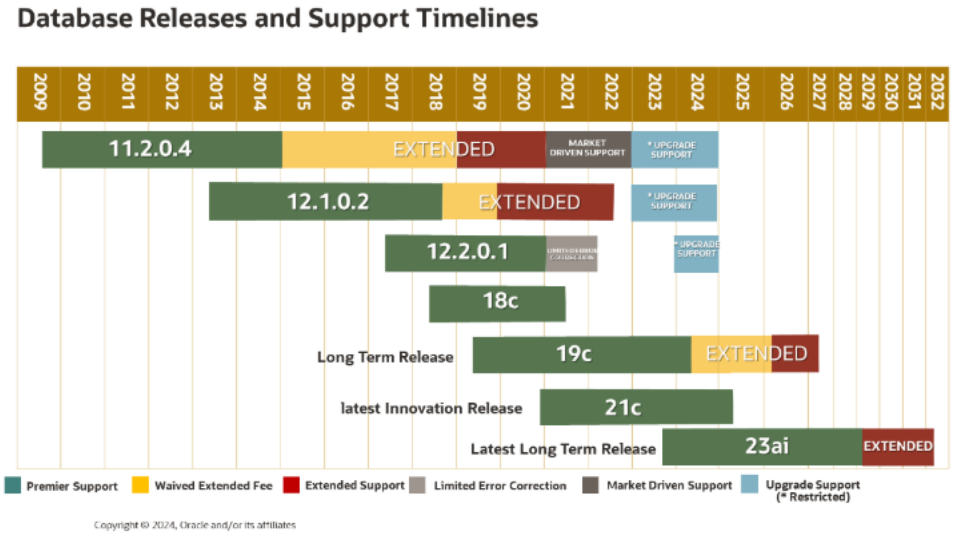


Ilustración 51 Estado Bases de Datos

Se observa que la compatibilidad del versionamiento a donde debería llegar el ministerio (19c) tiene soporte extendido hasta 2027 y es la versión de base de datos que posee más estabilidad frente a 21c y 23ai. Es importante aclarar que la infraestructura que aloja las bases de datos actuales (x5) no posee soporte a nivel de bases de datos para surtir procesos de actualización a 19c actualmente.

Para una actualización de la infraestructura que posea soporte para el versionamiento de base de datos 19c se podría explorar la posibilidad de infraestructura (x10) bajo un modelo de clúster y no bajo un modelo alta disponibilidad (HA), esto garantizaría una actualización de infraestructura y soporte para los versionamiento de base de datos a donde debería orientarse el escenario del Ministerio.

Actualmente, el ministerio de trabajo tiene desplegadas sobre el ODA X5-2 un total de 7 bases de datos en versión 12c, estas bases de datos son productivas y desarrollo en el siguiente apartado se mostrarán las aplicaciones que han sido mapeadas y que consumen conexiones sobre las bases de datos del ODA X5-2. En el siguiente apartado se listan las aplicaciones que hacen uso de las bases de datos de la entidad y que consumen su conexión mediante esquemas específicos:

APLICACION	BD	ESQUEMA	ENTORNO
Gestor documental, BI pensiones	*mintrasg*	*bpmdba, sgd, fnt_fpos, fnt_gcd, fnt_icn, fnt_os, analitica_ pensiones, corr_adm*	*Producción*
SIGEP	*sigep*	*Sigep, presigep, dessigep*	*Producción - desarrollo*
RUI	*dbmintra*	*rui, rui_consulta, ruipru, filcodev,simpc,simpcdes*	*Producción - desarrollo*
sid4, simpc, catalogo rman	*dbpsimpc*	*sid4, simpcprod,rman*	*producción*
LIFERAY - FILCO	*pliferay*	*Liferaypro, liferaypru, filcodev, filcopru*	*Producción - desarrollo*

Tabla 52 Apps & DDBB Oracle

3.1.5 No aplica

3.1.6 Seguridad Informática

A continuación, se describen y enumeran los diferentes servicios de seguridad que se prestan para el Ministerio del Trabajo. En cada apartado se pueden evidenciar los detalles de cada servicio.

3.1.6.1 Firewalls de nueva generación

Durante el mes de julio de 2026, los firewalls de Fortinet operaron en condiciones óptimas, garantizando la protección de la seguridad perimetral de la infraestructura tecnológica. Se efectuó un monitoreo continuo de la red con el propósito de asegurar que únicamente el tráfico autorizado accediera a los recursos internos de la entidad.

De igual manera, se mantuvieron e implementaron políticas de seguridad orientadas a la prevención de amenazas externas, realizando los ajustes requeridos conforme a las necesidades específicas del Ministerio de Trabajo.

En cuanto a la disponibilidad del servicio, se evidenció un cumplimiento del **100 %** durante el periodo reportado, lo que indica que no se presentaron interrupciones ni afectaciones en la operación del firewall.

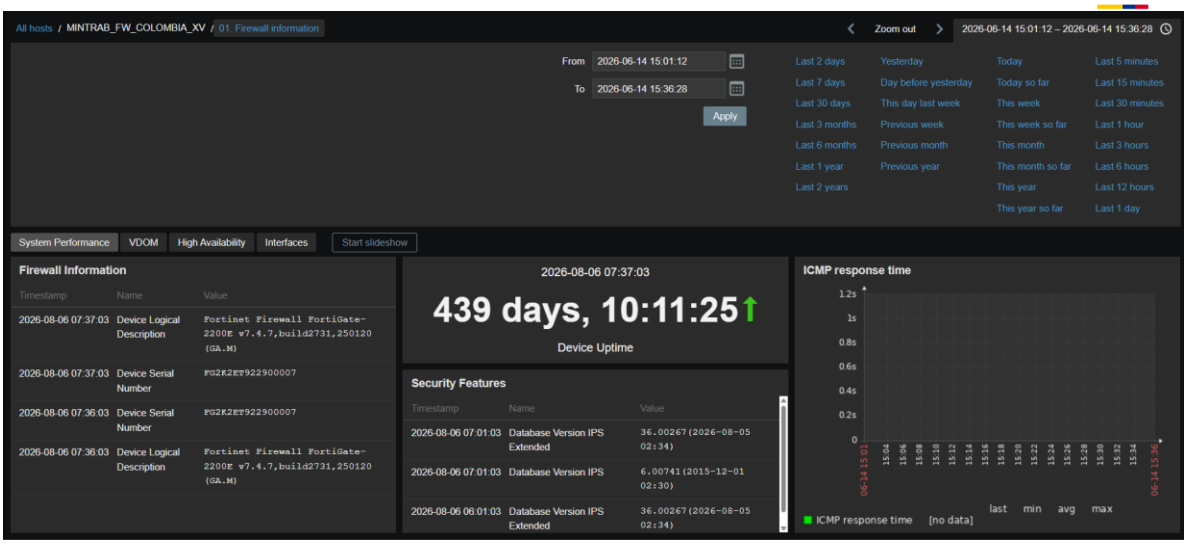


Ilustración 52 Firewall de nueva generación.

El Informe de aplicaciones y ancho de banda de Fortinet proporciona una visión detallada para identificar las aplicaciones y usuarios en la red que están utilizando la mayor cantidad de ancho de banda y presentando los mayores riesgos. Este informe, resume los hallazgos y ofrece una evaluación global del riesgo, junto con acciones recomendadas para abordarlos de manera efectiva.

Ancho de Banda

Se presenta un resumen del uso de ancho de banda y el número de sesiones durante el período del mes de julio. Este análisis del resumen de ancho de banda proporciona una visión clara de los patrones de uso durante el periodo, permitiendo una mejor gestión y planificación de los recursos de red.

Elemento	Observación actualizada de acuerdo con el gráfico
Tendencia general	El comportamiento del tráfico mantiene un patrón estable, periódico y predecible durante todo el mes de julio. Se observan ciclos recurrentes de incremento y disminución del tráfico, sin variaciones abruptas que evidencien anomalías operativas o transferencias masivas inusuales.
Volumen promedio	El tráfico recibido continúa predominando sobre el tráfico enviado. Los valores de recepción oscilan aproximadamente entre **2 TB y 12 TB diarios**, mientras que el tráfico enviado permanece relativamente estable entre **1 TB y 3 TB**, comportamiento esperado para una entidad con alto consumo de servicios internos y externos.
Tráfico recibido (azul)	Presenta un comportamiento cíclico con picos cercanos a **12 TB** alrededor de los días **8–9, 20–21 y 27–28 de julio**. Entre estos periodos se observan reducciones hasta aproximadamente **2–4 TB**, lo que evidencia variaciones normales asociadas a la operación institucional.
Tráfico enviado (amarillo)	El tráfico saliente se mantiene estable durante todo el periodo, con valores aproximados entre **1 y 3 TB diarios**. Se observan ligeros incrementos alrededor de los días **6–10, 15–18, 22–25 y 27–30 de julio**, sin evidenciar comportamientos atípicos o sostenidos que sugieran posibles fugas de información.
Días de mayor actividad	Los mayores volúmenes de tráfico combinado se presentan aproximadamente entre los días **7–10, 15–18, 20–22 y 27–29 de julio**, predominando el tráfico recibido. Este comportamiento es consistente con procesos de sincronización, consumo de aplicaciones institucionales, servicios en la nube y actividades propias de la operación diaria.
Días de menor tráfico	Se identifican reducciones del tráfico alrededor de los días **4–5, 11–13, 18–19, 25–26 y al cierre del mes (30–31 de julio)**. Estos comportamientos son consistentes con periodos

	de menor actividad operativa y ciclos normales de utilización de la infraestructura tecnológica.
Relación enviada/recibido	Continúa observándose una marcada predominancia del tráfico recibido sobre el enviado, comportamiento coherente con un entorno institucional donde prevalece el consumo de aplicaciones corporativas, portales web, servicios en la nube y procesos de actualización. El tráfico saliente permanece dentro de rangos esperados y no evidencia incrementos significativos.
Comportamiento esperado / Riesgo	El comportamiento observado corresponde a un patrón estable y consistente con la operación normal del Ministerio del Trabajo. No se identifican en la gráfica indicios de congestión, saturación o transferencias salientes extraordinarias. Desde la perspectiva del monitoreo de red.

Tabla 53 Tendencia de uso de ancho de banda

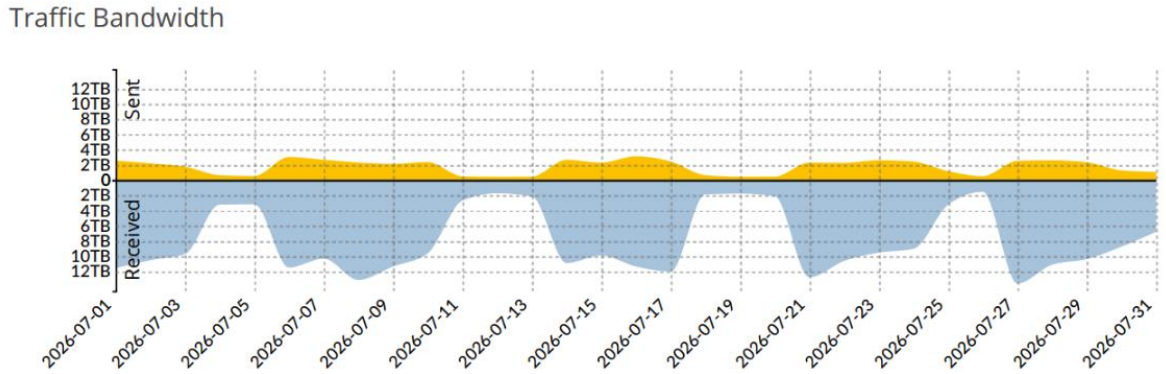


Ilustración 53 Comportamiento ancho de banda

Usuarios con mayor consumo de ancho banda

Esta imagen presenta un análisis del uso del ancho de banda por usuarios e IP's, centrándose en los 10 principales usuarios que generan tráfico en la red durante el período del mes de julio. La identificación de los 10 principales usuarios de ancho de banda proporciona información valiosa sobre los patrones de uso de la red y los puntos críticos de congestión.
A continuación, se detallan los hallazgos más relevantes:

N.°	Usuario/IP	Total de datos (aprox.)	Observaciones
1	**172.20.22.167**	**43 TB**	Corresponde al mayor consumo de ancho de banda del período, con predominio del **tráfico recibido**. El comportamiento es consistente con un servidor de aplicaciones o una plataforma de alto consumo de información.
2	**172.20.22.251**	**19 TB**	Registra el segundo mayor consumo del período, principalmente asociado a **tráfico recibido**. Se recomienda validar su relación con servicios documentales, sincronización de información o aplicaciones institucionales críticas.
3	**172.20.22.27**	**13 TB**	Presenta un volumen significativo de tráfico recibido. El comportamiento puede estar relacionado con aplicaciones institucionales o servicios internos con alta demanda de información.
4	**mduarteo**	**6.85 TB**	Usuario con consumo significativo de ancho de banda, con predominio del tráfico recibido. Se recomienda validar que el consumo corresponda a funciones operativas, transferencia de archivos o actividades propias del cargo.

5	**172.28.28.38**	**6.21 TB**	El consumo se concentra prácticamente en su totalidad en **tráfico saliente**. Debido a este comportamiento, se recomienda validar los destinos, aplicaciones y procesos asociados para confirmar que correspondan a actividades autorizadas.
6	**172.20.44.102**	**6 TB**	Registra un comportamiento mixto, aunque con predominio del tráfico saliente. Se recomienda validar los procesos internos o aplicaciones institucionales asociados al consumo.
7	**172.20.22.179**	**5.86 TB**	Consumo concentrado principalmente en tráfico recibido, consistente con un servidor corporativo o aplicación institucional con interacción recurrente de usuarios.
8	**JPADUA**	**3.22 TB**	Usuario con consumo principalmente recibido. El volumen se encuentra por debajo de los principales consumidores, pero debe mantenerse dentro del monitoreo regular para validar su correspondencia con actividades autorizadas.

Tabla 54 usuarios con mayor consumo de ancho de banda

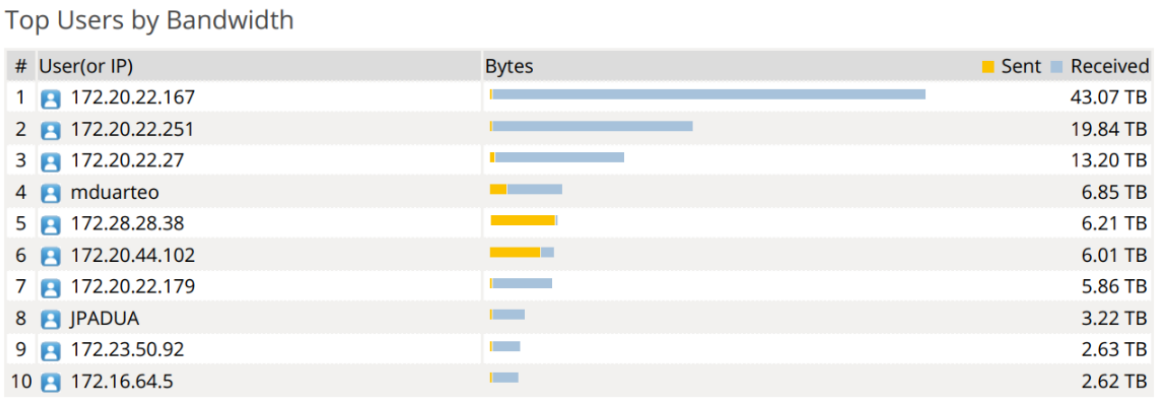


Ilustración 54 Tendencia de uso de ancho de banda

Top de usuarios por número de sesiones

La imagen corresponde al apartado “Top Users by Sessions” del informe perimetral de julio 2026 del Ministerio de Trabajo, donde se listan los usuarios o direcciones IP que generaron el mayor número de sesiones de red durante el periodo.

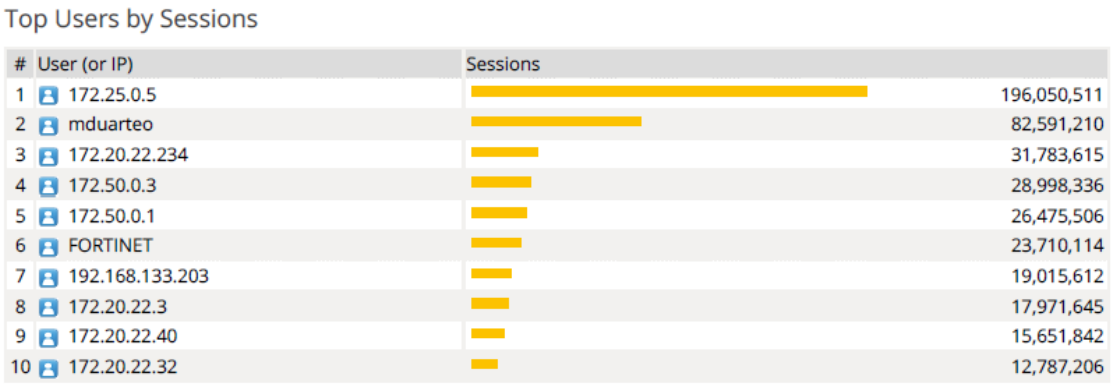


Ilustración 55 Top de usuarios por números de sesiones

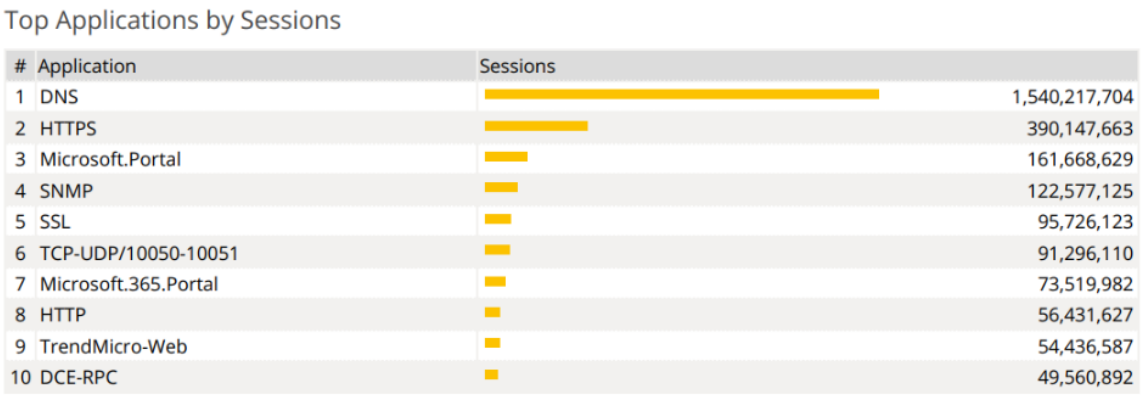
Análisis Top Users by Sessions

N°	Usuario/IP	Sesiones	Observaciones
1	**172.25.0.5**	**196.050.511**	IP con la mayor cantidad de conexiones. Muy probablemente corresponde a un **servidor interno o sistema de autenticación/proxy**, encargado de canalizar solicitudes de múltiples usuarios.
2	**mduarteo**	82.591.210	Usuario con actividad muy elevada. Puede estar vinculado a gestion de alguna plataforma (Mireya Duarte Osma)
3	**172.20.22.234**	31.783.615	Servidor interno asociado a un controlador de dominio.
4	**FORTINET**	23.710.114	Tráfico legítimo del sistema de seguridad (firewall, antivirus o gestión de eventos).
5	**Resto de IPs internas (rango 172.16–172.22)**	Entre **12 y 18 millones de sesiones**	Volumen esperado para servicios de autenticación, proxy, o endpoints activos de red.

Tabla 55 Top de usuarios por sesiones

Top Applications by Bandwidth

La imagen corresponde al apartado “Top Applications by Bandwidth” del informe perimetral de julio 2026 del Ministerio de Trabajo. Este bloque muestra las aplicaciones o protocolos que más ancho de banda consumieron durante el mes, expresado en terabytes (TB), y diferenciando tráfico enviado (amarillo) y recibido (azul).


Top Applications by Sessions

#	Application	Sessions
1	DNS	1,540,217,704
2	HTTPS	390,147,663
3	Microsoft.Portal	161,668,629
4	SNMP	122,577,125
5	SSL	95,726,123
6	TCP-UDP/10050-10051	91,296,110
7	Microsoft.365.Portal	73,519,982
8	HTTP	56,431,627
9	TrendMicro-Web	54,436,587
10	DCE-RPC	49,560,892

Ilustración 56 Top de aplicaciones

Aplicación	Número de sesiones	Descripción
DNS	**1,540,217,704**	Corresponde a la aplicación con mayor número de sesiones del período. Este comportamiento es consistente con la resolución continua de nombres requerida por usuarios, servidores, aplicaciones y servicios institucionales. Debido a su alto volumen, se recomienda mantener el monitoreo para identificar consultas anómalas, dominios maliciosos o posibles patrones de DNS tunneling.
HTTPS	**390,147,663**	Segundo servicio con mayor número de sesiones. Corresponde principalmente al acceso cifrado a aplicaciones web, servicios en la nube, plataformas SaaS, portales institucionales y navegación segura por Internet.

Microsoft.Portal	**161,668,629**	Actividad relacionada con el acceso a portales y servicios de Microsoft. El volumen refleja un uso intensivo de plataformas corporativas, servicios de autenticación y recursos en la nube.
SSL	**95,726,123**	Sesiones asociadas a comunicaciones cifradas mediante SSL/TLS. El comportamiento es consistente con aplicaciones corporativas, servicios web y conexiones seguras hacia plataformas internas y externas.
SNMP	**122,577,125**	Protocolo utilizado para la supervisión y administración de dispositivos de red e infraestructura tecnológica. El elevado número de sesiones puede estar asociado a consultas periódicas de plataformas de monitoreo; se recomienda validar que los orígenes correspondan exclusivamente a herramientas autorizadas.
TCP-UDP/10050-10051	**91,296,110**	Puertos comúnmente asociados a comunicaciones entre agentes y servidores de plataformas de monitoreo. El volumen observado es consistente con la recolección continua de métricas, disponibilidad y estado de los activos tecnológicos.
TrendMicro.Web	**54,436,587**	Actividad asociada a la solución de seguridad Trend Micro, incluyendo consultas a servicios web, validaciones de reputación, actualizaciones, telemetría y comunicaciones con la infraestructura del fabricante.
Microsoft.365.Portal	**73,519,982**	Sesiones relacionadas con el acceso a servicios de Microsoft 365, incluyendo autenticación, correo, colaboración y aplicaciones empresariales en la nube. El comportamiento es consistente con el uso institucional de la plataforma.
HTTP	**56,431,627**	Tráfico web sin cifrado. Aunque puede corresponder a aplicaciones internas, redirecciones o servicios heredados, se recomienda revisar su uso y promover la migración a HTTPS cuando sea técnicamente posible.
DCE-RPC	**49,560,892**	Protocolo utilizado ampliamente en entornos Microsoft Windows para comunicación entre servicios, administración remota y operaciones de dominio. El volumen observado puede ser consistente con la operación de la infraestructura, pero debe mantenerse bajo monitoreo debido a su relevancia en actividades de movimiento lateral.

Tabla 56 Top de aplicaciones

Top 15 Authenticated Logins by VPN Connections

La imagen corresponde al apartado “Authenticated Logins” del informe perimetral de julio 2026 del Ministerio de Trabajo (MinTrabajo), y presenta el comportamiento de los usuarios que se conectaron por VPN (SSL-Tunnel) durante el periodo analizado.

Authenticated Logins

#	User	Type	First Used	Total Number of Connections	Total Duration Connected(HH:MM:SS)
1	contaccenter	ssl-tunnel	2026-06-01 07:15:26	143	217:08:28
2	cjimenez	ssl-tunnel	2026-06-01 08:36:58	99	130:31:37
3	jepinzon@noc_indra	ssl-tunnel	2026-06-02 06:09:30	91	375:50:53
4	aorozcoca	ssl-tunnel	2026-06-01 10:34:40	89	124:23:46
5	lanzola	ssl-tunnel	2026-06-01 03:28:17	78	172:33:31
6	ovalderrama	ssl-tunnel	2026-06-01 10:35:21	77	99:48:41
7	gtorres	ssl-tunnel	2026-06-01 21:17:56	77	155:17:25
8	dfdiazd@noc_indra	ssl-tunnel	2026-06-01 00:06:14	71	299:26:29
9	RMURCIA	ssl-tunnel	2026-06-01 07:06:27	68	82:38:24
10	ltriana	ssl-tunnel	2026-06-02 06:16:18	68	86:08:54
11	cbueno	ssl-tunnel	2026-06-05 11:26:28	63	141:41:01
12	dramos	ssl-tunnel	2026-06-02 09:39:32	57	56:30:41
13	dosma	ssl-tunnel	2026-06-02 11:10:10	56	45:29:35
14	bcamargo	ssl-tunnel	2026-06-01 06:45:02	56	86:24:08
15	agente7	ssl-tunnel	2026-06-01 15:32:03	54	128:59:17

Ilustración 57 Top de Autenticación

Indicador	Descripción actualizada
Tipo de conexión	El **100 %** de las sesiones identificadas se realizaron mediante **SSL-Tunnel**, evidenciando el uso de la **VPN FortiGate** como mecanismo principal de acceso remoto seguro a la red institucional.
Usuarios más activos (por duración)	Los usuarios con mayor tiempo acumulado de conexión son: **jepinzon@noc_indra** (~313:04 h), **tecnicoamirl** (~257:24 h), **contaccenter** (~233:23 h), **lazambranor@noc_indra** (~193:37 h) y **dfdiazd@noc_indra** (~192:00 h). Este comportamiento es consistente con funciones de operación del NOC, monitoreo continuo, soporte técnico y administración remota de la infraestructura.
Mayor duración total	El mayor tiempo acumulado corresponde al usuario **jepinzon@noc_indra**, con aproximadamente **313 horas**, seguido por **tecnicoamirl** (~257 horas) y **contaccenter** (~233 horas). Estas sesiones prolongadas se encuentran alineadas con actividades permanentes de monitoreo y soporte operativo.
Mayor cantidad de conexiones	Los usuarios con mayor número de conexiones registradas son: **contaccenter (153 conexiones)**, **cjimenez (116)**, **dacero (108)**, **jepinzon@noc_indra (97)** y **aorozcoca (92)**. Este comportamiento es característico de usuarios con múltiples reconexiones, turnos operativos o actividades recurrentes de soporte.
Duraciones elevadas (>200 h)	Se identifican tres usuarios con actividad superior a **200 horas**: **jepinzon@noc_indra** (~313 h), **tecnicoamirl** (~257 h) y **contaccenter** (~233 h). Estas conexiones deben corresponder a funciones autorizadas de monitoreo, operación y administración continua.
Duraciones medias-altas (100 h – 200 h)	Los usuarios **lazambranor@noc_indra** (~193 h), **dfdiazd@noc_indra** (~192 h), **cjimenez** (~173 h), **agendarl** (~145 h), **lanzola** (~142 h), **aorozcoca** (~137 h), **RMURCIA** (~120 h) y **rovalle** (~113 h) presentan un uso intensivo de la VPN, asociado a actividades de soporte técnico, monitoreo y operación remota.
Duraciones medias (50 h – 100 h)	Los usuarios **dosma** (~72 h), **dnitolac** (~52 h) y **dacero** (~48 h, cercano al rango medio) presentan un uso recurrente de la VPN, consistente con actividades operativas y de soporte periódico.
Duraciones bajas (<50 h)	El usuario **idjimenez** (~32 h) registra el menor tiempo acumulado de conexión dentro de los usuarios mostrados, lo que sugiere un acceso puntual asociado a actividades específicas o requerimientos operativos ocasionales.

Tabla 57 Consolidado de indicadores

Failed Login Attempts by User

Esta imagen corresponde al apartado “Failed Login Attempts” del informe perimetral de julio 2026 del Ministerio de Trabajo (MinTrabajo).

Refleja los intentos de autenticación fallidos en la VPN (tipo ssl-web) es decir, accesos no exitosos al portal web seguro de Fortinet y constituye un indicador directo de posibles intentos de fuerza bruta o errores de acceso administrativo.

Failed Login Attempts

#	User	Type	Total Number of Failed Attempts
1	admin	ssl-web	3,250
2	record	ssl-web	392
3	guest	ssl-web	281
4	test	ssl-web	255
5	training	ssl-web	227
6	backup	ssl-web	224
7	temp	ssl-web	207
8	demo	ssl-web	199
9	support	ssl-web	188
10	reception	ssl-web	180

Ilustración 58 sesiones fallidas

Análisis
Durante julio 2026 se registraron múltiples intentos fallidos de acceso VPN, orientados a cuentas administrativas genéricas, lo que confirma la presencia de actividad automatizada externa (fuerza bruta).

El sistema respondió correctamente, sin accesos exitosos detectados, pero se recomienda reforzar la autenticación multifactor (MFA), aplicar bloqueo por IP, y eliminar cuentas por defecto para reducir la exposición perimetral.

3.1.6.2 Sandbox – Amenazas día 0

El servicio de Sandbox para el Ministerio del Trabajo se utiliza para crear entornos aislados y seguros donde se pueden ejecutar archivos o programas sospechosos para analizar su comportamiento. La función principal del Sandbox es detectar y analizar posibles amenazas de seguridad, como malware o software malicioso, sin comprometer la seguridad del sistema principal. Para el mes de julio de 2026, se generaron 66 eventos analizados, los cuales fueron limpiados de algún tipo de amenazas

Scan Statistics - Last 4 Weeks

Inputs	*Pending*	*Processing*	Malicious	High Risk	Medium Risk	Low Risk	Clean	Other	Total
Device	*0*	*0*	0	10	35	28	3,401	0	*3,474*
Adapter	*0*	*0*	0	0	0	0	0	0	*0*
On Demand	*0*	*0*	0	0	0	0	0	0	*0*
Network Share	*0*	*0*	0	0	0	0	0	0	*0*
Sniffer	*0*	*0*	0	0	0	0	0	0	*0*
URL	*0*	*0*	0	0	0	0	0	0	*0*
All Sources	*0*	*0*	0	10	35	28	3,401	0	*3,474*

File Scan - Last 4 Weeks

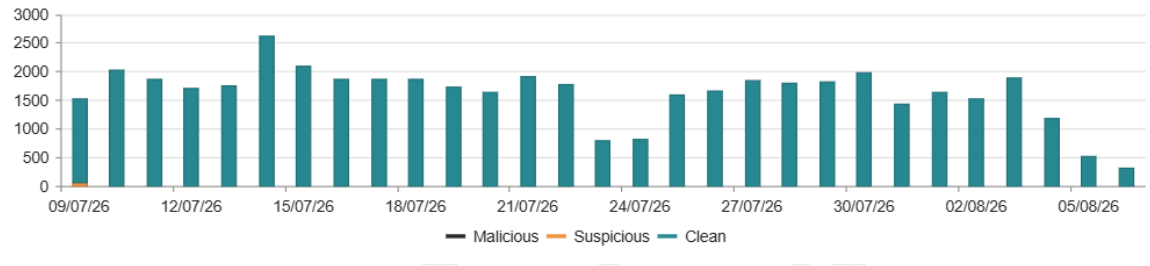


Ilustración 59 Reporte mensual

Este informe de rendimiento proporciona un análisis detallado del comportamiento y la eficiencia de FortiSandbox durante el mes de julio. Incluye estadísticas sobre la cantidad de archivos analizados, el rendimiento del sistema, la eficiencia en la detección de amenazas y recomendaciones para mejorar el rendimiento y la seguridad.

Perfomance

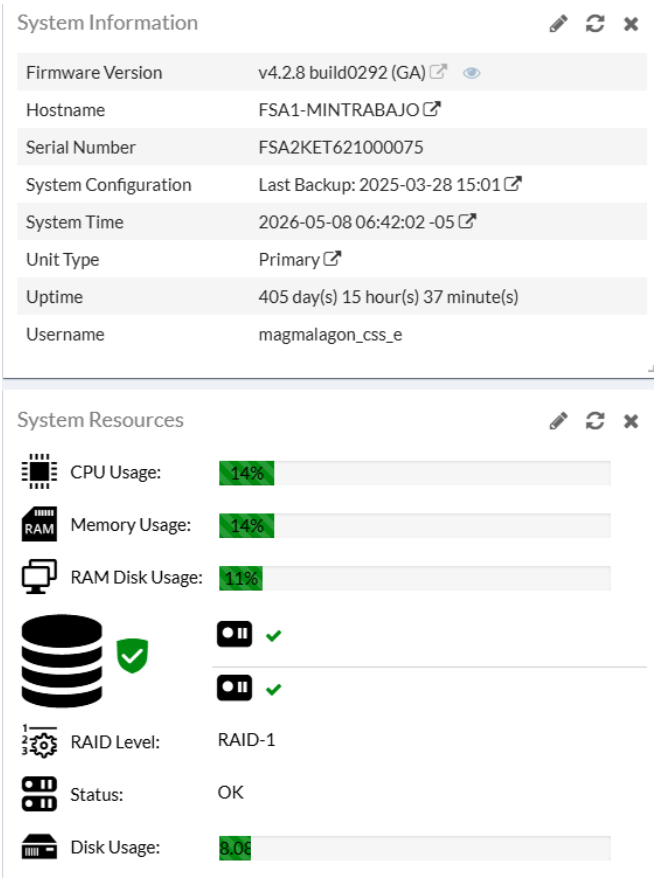


Ilustración 60 Captura de pantalla perfomance

Licencia Sandbox

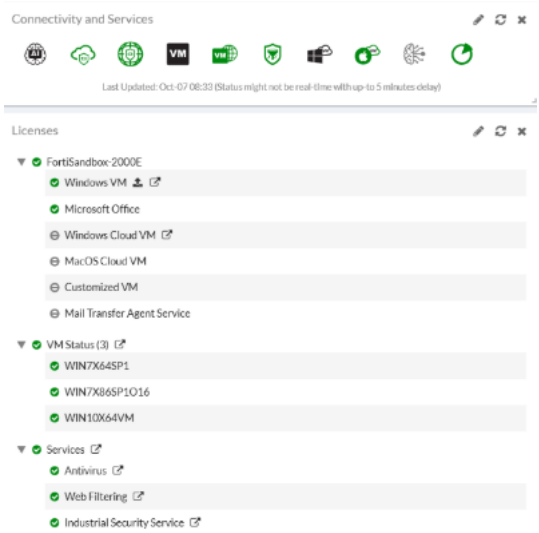


Ilustración 61 licencia sandbox

3.1.6.3 SIEM - Solución de correlación de eventos de seguridad, disponibilidad y recursos

El presente informe constituye el último informe mensual de operaciones del SOC del Ministerio de Trabajo, correspondiente al mes de julio de 2026, con el que se cierra formalmente el Contrato 574 de 2023. Se incluye análisis comparativo cuatrimestral (abril–mayo–junio–julio) para evidenciar las tendencias del período contractual y los hallazgos pendientes de resolución al momento del cierre.

El período comprende 30 días de monitoreo continuo sobre la infraestructura TI ministerial.

2.987	490	8.064+	391 TB
EPS Pico máximo (julio 2026)	EPS Promedio sostenido	eventos totales detectados	ISAKMP – VPN tráfico total
↓ vs 3.494 jun / 4.584 abr-may	*≈ Estable (vs 422 julio)*	*↑ Mayor volumen del período*	*↓ vs 408 TB julio*

EPS pico continúa su tendencia descendente: 4.584 (abr/may) → 3.494 (jun) → 2.987 (jul). La correlación con el shutdown de logging de Windows detectado en junio sigue sin resolución confirmada.

Website Access Policy Violation: 5.036 casos — segundo mes consecutivo de incremento (3.027 en mayo, 3.551 en junio, 5.036 en julio), superando niveles de abril.

Large Outbound Transfer: 957 casos — cuarto mes consecutivo activo con los mismos usuarios implicados (casanabriap y emoralesr).

MediaFire con 9.27 TB desde un equipo específico en horario nocturno es el hallazgo de red más relevante del período.

Google.Gemini aparece por primera vez con 449 conexiones — uso de IA generativa externa sin política formal documentada.

Los servidores mantienen alta disponibilidad (uptime sostenido, RTT 1 ms) — la infraestructura cierra el contrato en condiciones operativas óptimas.

Dispositivos Fuente de Eventos (Reporting Devices)

Dispositivo	MAX EPS	AVG EPS	Observación
MINTRABCOLLECTOR – Windows Server 2012 R2	1.677	1.1	Microsoft – servidor de infraestructura principal
MINTRABCOLLECTOR – Windows Server 2019	1.610	0.86	Microsoft – servidor de infraestructura
MINTRABCOLLECTOR – FortiOS	1.308	132.36	Fortinet – firewall perimetral (AVG más alto: fuente más consistente)
MINTRABCOLLECTOR – Windows Server 2016	908	0.92	Microsoft – servidor de infraestructura
MINTRABCOLLECTOR – TrendMicro Vision One	479	19.66	Antivirus cloud – volumen consistente con telemetría EDR

MINTRABCOLLECTOR – Office365	408	6.4	Microsoft O365 – fuente de eventos de correo y colaboración
mintrabsupervisor.mintrabajo.loc	80	0.07	Servidor de supervisión – bajo volumen, normal
mintrabworker.mintrabajo.loc	76	0.09	Servidor worker – bajo volumen, normal

Tabla 58 Fuentes de eventos

3.1.6.3.1 Incidentes por Tipo

El mes de julio de 2026 presenta el mayor volumen de incidentes del período contractual analizado. La siguiente sección detalla cada tipo de incidente con análisis de tendencia y evaluación del impacto:

Tipo de Incidente	Abr	May	Jun	Jul
Website Access Policy Violation	5.022	3.027	3.551	5.036
Office365 SendAs/SendOnBehalf	1.075	N/R	640	1.113
Large Outbound Transfer	767	927	936	957
Group Policy Object Modified	N/A	2.395	2.485	934
LOT To Outside My Country	N/A	N/A	816	827
Website Policy Violation – High (NUEVO)	N/A	N/A	555	555

Tabla 59 Tipos de incidentes

3.1.6.3.3. Hosts e IPs Implicados

Los siguientes activos concentran la mayor parte de los incidentes detectados durante el período:

Host / IP	ABR	MAY	JUN	JUL	Estado al Cierre
Mintrab104.mintrabajo.loc	**NO**	**SÍ**	**SÍ**	**SÍ**	ACTIVO 3 MESES – Correlacionado con Event ID 4625 (NTLM)..
Mintrab02.mintrabajo.loc	**SÍ**	**SÍ**	**SÍ**	**SÍ**	ACTIVO 4 MESES – El host más persistente del período
Mintrab107.mintrabajo.loc	**NO**	**SÍ**	**SÍ**	**SÍ**	ACTIVO 3 MESES – Segundo host más persistente.
172.16.68.28 (BOPBVANEGASM) – NUEVO	**N/A**	**N/A**	**N/A**	**NUEVO**	Equipo que generó 9.27 TB hacia MediaFire en horario nocturno (25-26 julio).

Tabla 60 Hosts e IPs Implicados

3.1.6.3.4. Usuarios con Mayor Actividad de Riesgo

Usuario	ABR	MAY	JUN	JUL
casanabriap	SÍ	SÍ	SÍ	SÍ
emoralesr	N/A	SÍ	SÍ	SÍ
kserrano / kserrano@mintrabajo.gov.co	N/A	N/A	SÍ	SÍ
dtboyaca@mintrabajo.gov.co	N/A	N/A	SÍ	SÍ
BOPBVANEGASM (usuario MediaFire)	N/A	N/A	N/A	NUEVO

Tabla 61 Usuarios con Mayor Actividad de Riesgo

3.1.6.3.5. Aplicaciones por Ancho de Banda

El análisis comparativo indica una expansión de la actividad que debe ser validada contra los proyectos y actividades del período:

Aplicación	Total	Enviado	Recibido	Evaluación de Seguridad
ISAKMP – VPN IPsec	391.22 TB	178.77 TB	212.45 TB	Normal. VPN bidireccional para acceso remoto y site-to-site.
SSL/TLS v1.3	166.75 TB	7.66 TB	159.08 TB	Normal. Predominio de descarga coherente con consumo de servicios web y SaaS.
TrendMicro Services (Cloud.IT)	91.40 TB	87.89 TB	3.51 TB	Trafico Normal de herramienta de Antivirus
DTLS – UDP cifrado	55.24 TB	8.16 TB	47.08 TB	Consistente con videoconferencia y colaboración. Sin anomalías identificadas.
SSL/TLS v1.2	16.89 TB	13.47 TB	3.41 TB	Tráfico TLS
MediaFire (Storage.Backup)	9.27 TB	155.34 GB	9.12 TB	Descarga masiva nocturna desde 172.16.68.28
NTP	6.08 TB	3.92 TB	2.15 TB	Disminuye (era 8.81 TB en may, 6.28 en jun).
STUN – P2P/WebRTC	3.95 TB	93.42 GB	3.86 TB	NUEVO. Protocolo P2P para establecimiento de sesiones.
Google.Services	1.62 TB	355.99 GB	1.28 TB	Servicios Google corporativos. Normal para entorno con G Suite o acceso a servicios Google.

Tabla 62 Aplicaciones por Ancho de Banda

3.1.6.4.6 Top Disponibilidad de servidores

La imagen proporciona un análisis de los servidores monitoreados por FortiSIEM, destacando los 10 servidores que generaron eventos de disponibilidad en términos de seguridad durante el mes de julio 2026. Ofrece información valiosa sobre los patrones de disponibilidad de servidores en lo relacionado con la última fecha de reinicio. A continuación, se presentan los hallazgos más relevantes:
Los servidores con mayor tiempo de disponibilidad continua en los últimos 30 días sin presentar eventos son:

Hallazgos relevantes:

- Servidores como MINTRAB03 y MINTRAB94 presentan más de 230 días de operación sin interrupciones.
- La latencia promedio es de 1 ms, indicando estabilidad total.
- Muestra un entorno estable y confiable, apto para soportar las operaciones institucionales.

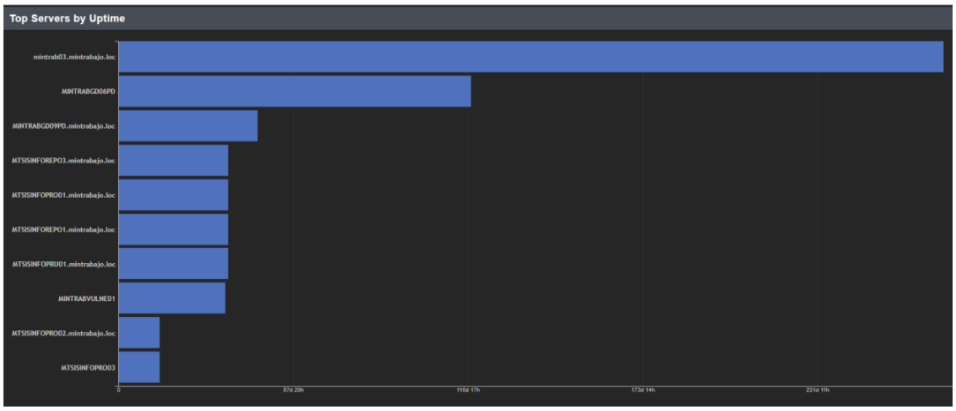


Ilustración 62 Detalle servidores

3.1.6.4 WAF - Servicio de tipo “Firewall de Aplicaciones Web”

Durante el mes de julio 2026, el WAF del Ministerio del Trabajo registró un volumen elevado de intentos de ataque, con patrones consistentes de explotación, divulgación de información y consultas sospechosas dirigidas a aplicaciones públicas institucionales.

El reporte confirma que el WAF está bloqueando correctamente los principales vectores identificados, sin evidencias de compromiso exitoso durante el periodo evaluado.

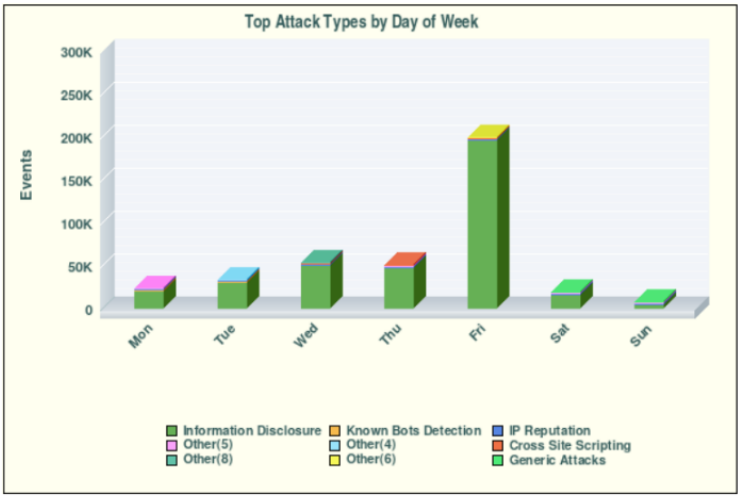


Ilustración 63 Top attack types

Análisis

Análisis	Descripción actualizada
Distribución de ataques por día	La mayor concentración de eventos de seguridad se presenta durante el **viernes**, alcanzando aproximadamente **200.000 eventos**, muy por encima del resto de la semana. Entre **miércoles y jueves** se observa una actividad intermedia (50.000–60.000 eventos), mientras que lunes, martes, sábado y domingo mantienen volúmenes considerablemente menores.
Inicio de semana	El **lunes** registra aproximadamente **25.000 eventos**, reflejando un nivel moderado de actividad. El **martes** presenta un ligero incremento, alcanzando alrededor de **35.000–40.000 eventos**, consistente con el aumento de la actividad operativa de la entidad.
Mitad de semana	Entre **miércoles y jueves** se evidencia un incremento progresivo, con volúmenes cercanos a **50.000–60.000 eventos**, manteniéndose una actividad constante de reconocimiento y exploración automatizada sobre los servicios expuestos a Internet.
Viernes	El **viernes** representa el mayor pico de actividad del período, alcanzando aproximadamente **200.000 eventos**, lo que evidencia un incremento significativo del tráfico malicioso detectado. Este comportamiento puede estar asociado a campañas automatizadas de escaneo masivo, intentos de explotación de vulnerabilidades conocidas o incremento del tráfico proveniente de bots hacia los servicios publicados.
Fin de semana	Durante **sábado y domingo** el volumen disminuye considerablemente, registrando aproximadamente **20.000 eventos** el sábado y menos de **10.000 eventos** el domingo. Esta reducción es consistente con una menor actividad institucional y un descenso en la interacción con los servicios publicados.
Tipo de ataques predominantes	Predominan ampliamente los eventos clasificados como **Information Disclosure**, seguidos por **Cross Site Scripting (XSS)**, **Known Bots Detection**, **IP Reputation**, **Generic Attacks** y otras categorías de menor incidencia. Este comportamiento refleja principalmente actividades de reconocimiento, escaneo automatizado e intentos de explotación sobre aplicaciones y servicios expuestos.
Detección de bots conocidos	Se identifican eventos asociados a **Known Bots Detection**, especialmente durante el viernes, lo que evidencia actividad automatizada proveniente de herramientas de reconocimiento y botnets que interactúan con los servicios institucionales publicados.
Ataques Cross Site Scripting (XSS)	Se observan eventos relacionados con **Cross Site Scripting (XSS)**, principalmente durante los días de mayor actividad. Estos intentos buscan inyectar código malicioso en aplicaciones web y son mitigados por las políticas implementadas en el **Web Application Firewall (FortiWeb)**.
Eventos asociados a reputación IP	Se mantienen eventos relacionados con **IP Reputation**, provenientes de direcciones IP catalogadas como maliciosas o sospechosas. Este comportamiento confirma la exposición permanente de los servicios institucionales a tráfico potencialmente hostil desde Internet.

Tabla 63 Tipo de ataque

3.1.6.5 Solución de Anti-DDoS

Durante el período del mes de julio, se registraron eventos 6 de ataques de denegación de servicio distribuido (DDoS) a las aplicaciones publicadas en internet por el Ministerio de Trabajo.

Top Attacked Subnets

Subnet	SPP	Direction	Drops	Events
PAGINA_MINTRABAJO	PAGINA_MINTRABAJO	Outbound	71	5
GESTOR_DOC_MINT	GESTOR_DOC_MINT	Outbound	20	1

Ilustración 64 Top de ataques

Análisis Detallado:

PAGINA_MINTRABAJO también muestra un número bajo de intentos salientes bloqueados (71), lo que sugiere riesgo bajo en aplicaciones web institucionales.

3.1.6.5.1 Login Fallidos

Durante el mes de julio 2026, no se registraron eventos de inicio de sesión fallidos, los cuales no fueron detectados por la herramienta de seguridad implementada por la UT contra ataques de denegación de servicio (DDoS). Es de aclarar que estos intentos de inicios de sesión corresponden a los ingresos que realizaron los especialistas que atienden el servicio. A continuación, se presentan los hallazgos más destacados:

3.1.6.6 Casos atendidos de los servicios de seguridad

A continuación, se detalla el listado de casos que han sido tratados durante el mes, y que corresponde a casos del servicio de seguridad informática:

3.1.6.6.1 Incidentes

Durante el mes de julio no se registró incidentes atendidos dentro del servicios de seguridad informática:

3.1.6.6.2 Requerimientos

A continuación, se detalla el listado de requerimientos atendidos dentro del servicios de seguridad informática, los cuales fueron 189 gestionados por el equipo de analistas, especialistas, líder SOC y demás especialistas que apoyan la gestión:

No. Caso	Fecha Registro	Asunto	Grupo Responsable	Categoria
RF-288165	27/07/2026 12:01	Equipo aislado BOPLANGEL	SOC	Asesoria - Consulta
RF-261375	2/07/2026 11:11	licencia para eliminar antivirus	SOC	Desinstalacion
RF-268842	7/07/2026 15:06	licencia para eliminar antivirus	SOC	Desinstalacion
RF-271301	9/07/2026 7:41	Eliminar licencia de antivirus	SOC	Desinstalacion
RF-258772	1/07/2026 8:01	PRIORIDAD ALTA: HABILITAR PUERTOS USB	SOC	Habilitación Puertos USB
RF-261426	2/07/2026 13:20	Solicitud apertura de puertos de forma temporal	SOC	Habilitación Puertos USB

RF-268165	6/07/2026 10:15	Solicitud habilitación puerto USB	SOC	Habilitación Puertos USB
RF-268407	6/07/2026 16:48	Habilitación Puertos USB	SOC	Habilitación Puertos USB
RF-268524	7/07/2026 8:34	RE: Habilitacion puertos usb	SOC	Habilitación Puertos USB
RF-268781	7/07/2026 12:50	RE: Solicitud apertura USB	SOC	Habilitación Puertos USB
RF-271375	9/07/2026 9:39	Habilitación Puerto USB	SOC	Habilitación Puertos USB
RF-271399	9/07/2026 10:09	HABILITAR PUERTO USB AUXILIAR DEL DESPACHO DE DIRECCIÓN	SOC	Habilitación Puertos USB
RF-271502	9/07/2026 12:18	Autorización puerto USB	SOC	Habilitación Puertos USB
RF-271622	9/07/2026 17:36	SOLICITUD HABILITACIÓN PUERTOS USB - SERVIDORES GRUPO DE PREVENCIÓN, INSPECCIÓN, VIGILANCIA Y CONTROL DIRECCIÓN TERRITORIAL NORTE DE SANTANDER.	SOC	Habilitación Puertos USB
RF-273811	10/07/2026 12:01	HABILITAR PUERTOS USB A LA FUNCIONARIA NIDIA XIOMARA JIMENEZ CAICEDO	SOC	Habilitación Puertos USB
RF-273883	10/07/2026 15:16	Solicitud de habilitación de Puertos Usuario PTPJALEGRIA	SOC	Habilitación Puertos USB
RF-278613	15/07/2026 10:18	HABILITACION PUERTO USB	SOC	Habilitación Puertos USB
RF-278687	15/07/2026 12:47	Solicitud copia de seguridad	SOC	Habilitación Puertos USB
RF-279901	16/07/2026 9:47	RV: solicitud de puertos usb	SOC	Habilitación Puertos USB
RF-281766	21/07/2026 9:44	RE: HABILITACION DE PUERTOS USB EN EQUIPOS	SOC	Habilitación Puertos USB
RF-281846	21/07/2026 11:04	Solicitud copia de seguridad-habilitacion de puertos USB	SOC	Habilitación Puertos USB
RF-281922	21/07/2026 14:48	ACTIVACIÓN PUERTO USB	SOC	Habilitación Puertos USB
RF-288228	27/07/2026 14:48	RE: HABILITACION DE PUERTOS USB EN EQUIPOS	SOC	Habilitación Puertos USB
RF-284386	23/07/2026 4:29	FortiSIEM Alert: TLP:RED - Mintrabajo - Command interpreter in Windows cmd or powershell	SOC	Generar reporte
TK-258789	1/07/2026 8:15	Habilitación de Puertos con Líder de Seguridad Informática	SOC	Inactivar usuario
RF-271589	9/07/2026 15:43	FortiSIEM Alert: TLP:RED - Mintrabajo - Brute Force Host Windows Login Success	SOC	Seguridad Informática
RF-276954	12/07/2026 21:00	FortiSIEM Alert: TLP:RED - Mintrabajo - Multiple Logon Failures: VPN	SOC	Seguridad Informática
RF-278786	15/07/2026 16:00	FortiSIEM Alert: TLP:RED - Mintrabajo - Brute Force Host Windows Login Success	SOC	Seguridad Informática
RF-289835	29/07/2026 12:19	Bloqueo en pagina Simo	SOC	Agregar a sitios permitidos
RF-280306	17/07/2026 11:36	Habilitación de tráfico	SOC	Agregar puertos
RF-268068	6/07/2026 8:53	MINTRABAJO | Comunicación Segmento 43 - Gestor Documental	SOC	Permitir acceso
RF-269989	8/07/2026 10:36	RE: IPv6 Infraestructura Centralizada	SOC	Permitir acceso
RF-279894	16/07/2026 9:26	Reporte bloqueo redes sociales	SOC	Permitir acceso
RF-283193	22/07/2026 10:25	Solicitud validación de página	SOC	Reportes Seguridad Informática
RF-258898	1/07/2026 10:44	configuraciones reglas adicionales VPN AZURE	SOC	Autorización conexión equipos visitantes
RF-269864	8/07/2026 7:03	RV: 4433484252; CASO 4400144021832018294970 8, TRASLADO DE EXCEPCIONES – SEDE: JDO. 12° CIVIL MPAL. - RIOHACHA	SOC	Revisar correo malicioso
RF-270166	8/07/2026 16:12	Correo sospechoso	SOC	Revisar correo malicioso
RF-285637	23/07/2026 16:10	RV: Solicitud de ejecución de pruebas de seguridad – Calculadora Laboral	SOC	Análisis vulnerabilidades
RF-289368	28/07/2026 8:22	RV: RESULTADO PRUEBA DE ESCANEO - CALCULADORA LABORAL	SOC	Análisis vulnerabilidades
RF-271361	9/07/2026 9:19	CORREO MALICIOSO	SOC	Análisis de Correos

RF-278685	15/07/2026 12:37	Re: Revisión Urgente REFERENCIA: Extensión de jurisprudencia ASUNTO: SOLICITUD DE INTERVENCION PARA EL CUMPLIMIENTO DE LA LEY	SOC	Análisis de Correos
RF-283254	22/07/2026 12:59	Verificar Informacion Importante: VALIDAR-CUENTA / validación correo sospechoso	SOC	Análisis de Correos
RF-260146	1/07/2026 23:36	FortiSIEM Alert: TLP:RED - Mintrabajo - Multiple Logon Failures: VPN	SOC	Análisis de evento
RF-270044	8/07/2026 12:27	FortiSIEM Alert: TLP:RED - Mintrabajo - Office365: Suspicious File Type Uploaded	SOC	Análisis de evento
RF-270102	8/07/2026 14:21	FortiSIEM Alert: TLP:RED - Mintrabajo - Possible Brute Force Alert Windows	SOC	Análisis de evento
RF-280433	19/07/2026 7:56	FortiSIEM Alert: TLP:RED - Mintrabajo - Brute Force Host Windows Login Success	SOC	Reporte de eventos
RF-285624	23/07/2026 15:59	FortiSIEM Alert: TLP:RED - Mintrabajo - Office365 Phishing Attempt Detected	SOC	Reporte de eventos
RF-286767	24/07/2026 10:01	FortiSIEM Alert: TLP:RED - Mintrabajo - Possible Brute Force Alert Windows	SOC	Reporte de eventos
RF-286973	24/07/2026 17:57	FortiSIEM Alert: TLP:RED - Mintrabajo - Possible Brute Force Alert Windows	SOC	Reporte de eventos
RF-288191	27/07/2026 14:09	FortiSIEM Alert: TLP:RED - Mintrabajo - Possible Brute Force Alert Windows	SOC	Reporte de eventos
RF-288322	27/07/2026 17:50	FortiSIEM Alert: TLP:RED - Mintrabajo - Possible Brute Force Alert Windows	SOC	Reporte de eventos
RF-291077	30/07/2026 7:59	Splunk Alert: UCC - Office365 Password Spray - Threat	SOC	Reporte de eventos

Tabla 64 Reporte de requerimientos julio

3.1.6.7 Análisis de riesgo

Se han identificado tres riesgos principales en la infraestructura del Ministerio de Trabajo durante el mes de julio:

- **Ejecución de archivos maliciosos**

Riesgo	Impacto	Probabilidad
Archivos ejecutables comunes pueden ser utilizados para distribuir malware, ransomware o puertas traseras.	Compromiso de la integridad, confidencialidad y disponibilidad de los sistemas	Alta, debido al uso frecuente de estos archivos y la falta de controles estrictos.

Tabla 65 Vulnerabilidades en la infraestructura

- **Vulnerabilidades en la infraestructura**

Riesgo	Impacto	Probabilidad
La infraestructura de TI presenta vulnerabilidades que pueden ser explotadas por atacantes	Acceso no autorizado, escalamiento de privilegios y explotación de fallos en la red	Media-Alta, dependiendo de la criticidad de las vulnerabilidades detectadas.

Tabla 66 Vulnerabilidades en la infraestructura

- **Ataques de Phishing dirigidos**

Riesgo	Impacto	Probabilidad
intentos de phishing dirigidos a altos funcionarios, como el ministro de Trabajo, con el objetivo de robo de credenciales o entrega de malware.	intentos de phishing dirigidos a altos funcionarios, como el ministro de Trabajo, con el objetivo de robo de credenciales o entrega de malware.	alta, debido al uso constante de correos electrónicos en la comunicación oficial.

Tabla 67 ataques de phishing

3. Medidas de Mitigación Recomendadas

Control y restricción de archivos ejecutables:

- Se realizó plan de trabajo para Implementar restricciones de ejecución de ejecutables en servidores y estaciones de trabajo.
- Se realizó unas listas blancas de software permitido.
- Monitoreo y análisis continuo de archivos sospechosos.

Gestión de vulnerabilidades:

- Se están aplicando parches y actualizaciones de seguridad en la infraestructura de TI.
- Se realizó revisión periódica (semanal) de la matriz de vulnerabilidades y su priorización.

Prevención y respuesta ante phishing:

- Se tiene Implementado de filtros avanzados de correo electrónico y autenticación multifactor (MFA).
- Se realizó análisis a los correos sospechosos y reporte inmediato de intentos de phishing.

3.1.6.8 Políticas y procedimiento de seguridad

Dentro las actividades realizadas en el mes de julio 2026, se realizó la revisión, ajuste, observaciones de algunos procedimientos y políticas que describimos a continuación

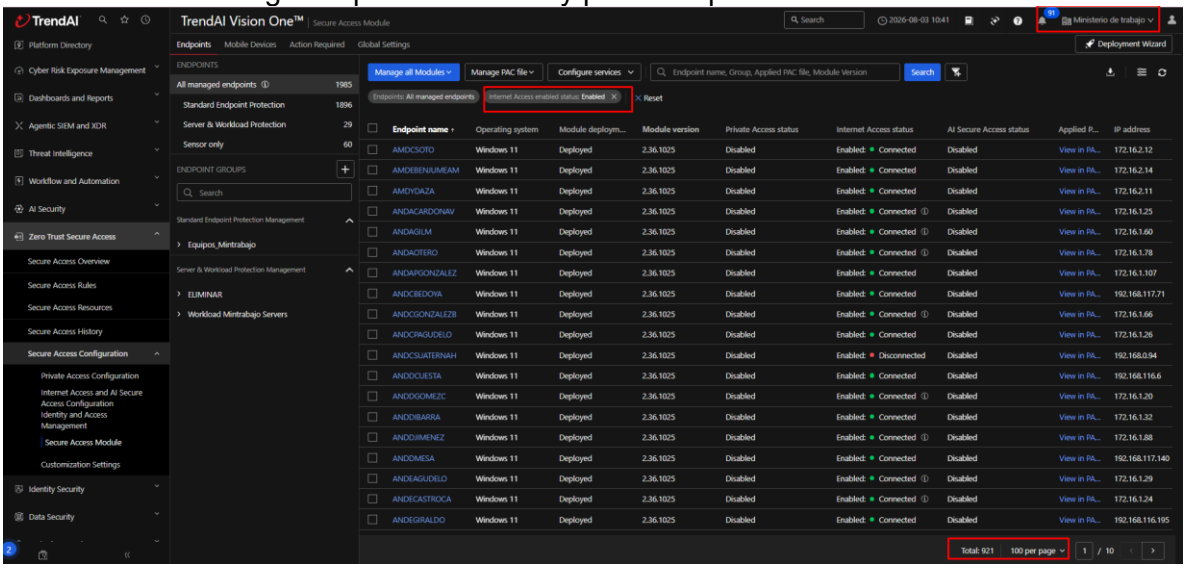


Ilustración 65 Políticas y procedimientos

Actualmente, el servicio de Zero Trust Network Access (ZTNA) se encuentra en proceso de ajuste y optimización de las reglas de acceso a Internet. A la fecha, se han desplegado 921 agentes funcionales en las distintas Direcciones Territoriales (DTs), lo cual ha permitido establecer una capa adicional de protección frente a amenazas cibernéticas y prevenir posibles fugas de información. Esta implementación fortalece significativamente los mecanismos de control de acceso y seguridad en los equipos de la entidad

3.1.7 Licenciamiento

A continuación, se presenta la información del licenciamiento:

Licencia	Referencia	Fecha de Vigencia	Estado
IBM	Del 01/06/2023 hasta el 31/07/2026	Vigente	**IBM (10896)**
LIFERAY	Del 01/08/2025 hasta el 31/07/2026	Vigente	**LIFERAY**

Tabla 68 Licenciamiento

3.1.8 Administración, soporte y monitoreo

- Servidores
- Se trabajó con el equipo de Monitoreo a nivel de herramienta Zabbix realizando actualización de máquinas virtuales que salen de operación por obsolescencia o desuso y por ende deben retirarse del monitoreo de la herramienta y del NOC, esto ha permitido disminuir el nuero de servidores dentro de la plataforma y el monitoreo y tener únicamente la información exacta de los servidores que están productivos o en entorno de pruebas y en uso. Se envía línea base tanto al NOC como a SOC.

Nube pública

- Se validó la infraestructura aprovisionada en Azure, que se encontraba en proceso de monitorear adecuadamente y se configuró un monitoreo sobre las IP públicas de los recursos expuestos y funcionales actualmente, se sostienen sesiones con áreas funcionales y se entrega informe sobre uno de los componentes para que los propietarios de cada suscripción en nube realicen monitoreo sobre la nube a través de Azure Monitor. Dentro del modelo de arquitectura a implementar, se tienen contemplado los componentes de Azure Monitor críticos que deben tenerse en cuenta para tener trazabilidad.
- Dentro de la documentación relacionada con Nube publica se agrega un ítem de Monitoreo y se abarcan las recomendaciones y acciones a realizar por parte de la UT y de la entidad a nivel de monitoreo de componentes de nube pública y la información que la herramienta Azure Monitor arroja desde los accesos que posee la UT al Tenant.

DDBB

- Se realiza actualización de la base de datos indicando el nombre del especialista a quien deben reportarse las indisponibilidades y a quien deben llegar los alertamientos automáticos de la herramienta Zabbix, se da visibilidad al NOC de la misma para el escalamiento para ser asertivos en las asignaciones a los profesionales de servicios centrales para su atención.
- Se ajustaron nuevos umbrales para diferentes aplicaciones y servicios a nivel de bases de datos MSSQL Server.

Almacenamiento

- Se agregan monitoreos sobre almacenamientos y datastore para establecer seguimiento de las holguras de crecimiento.
- Se crean alertamientos nuevos desde VMWare para validar estado de los almacenamientos.

- Se ajustaron los umbrales de los alertamientos de las diferentes LUN para evitar notificaciones innecesarias.
- Se mitigan los alertamientos sobre las LUN de VMWare.

Medición ANS Datacenter y Nube Pública

A continuación, el resultado de la medición de los ANS:

ID	Indicadores	Resultado	Meta
DC-1	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
DC-2	Continuidad y disponibilidad del datacenter principal	100,00%	99.95%
DC-3	Continuidad y disponibilidad del datacenter alterno	100,00%	99,60%
DC-4	Continuidad y disponibilidad de la plataforma de procesamiento, almacenamiento y respaldo	100,00%	99,70%
DC-5	Tiempo de solución de incidentes asociado a los servicios de aplicaciones especializadas	97,60%	90,00%
DC-6	Tiempo de solución de requerimientos asociado a los servicios de aplicaciones especializadas	100,00%	90,00%
DC-7	Continuidad y disponibilidad de los servicios de directorio activo	100,00%	99,60%
DC-8	Continuidad y disponibilidad de los servicios de seguridad informática	100,00%	99,90%
DC-9	Tiempo de solución de incidentes asociado a los servicios de administración, soporte y monitoreo	97,46%	90,00%
DC-10	Tiempo de solución de requerimientos asociado a los servicios de administración, soporte y monitoreo	99,82%	90,00%
DC-11	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 69 Medición ANS Datacenter

ID	Indicadores	Resultado	Meta
NP-1	Continuidad y disponibilidad de la nube pública	100,00%	99,90%
NP-2	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100%

Tabla 70 Medición ANS Nube Pública

3.2 No aplica

3.3 Conectividad WAN, SDWAN e Internet

3.3.1 Canales WAN

A nivel de canales WAN, se prestó el servicio en cada sede territorial de forma estable, no obstante, en las sedes donde se presentó algún tipo de falla se generó el respectivo caso con el proveedor de conectividad, los incidentes presentados se ven reflejados en el ítem 3.3.1.1.

Se observa en la gráfica de consumo, que el tráfico fue estable durante el mes de julio, no se observan caídas del canal, no se presenta saturación sobre este canal. Es de aclarar que los túneles SDWAN sobre MPLS se conectan por medio de este canal.

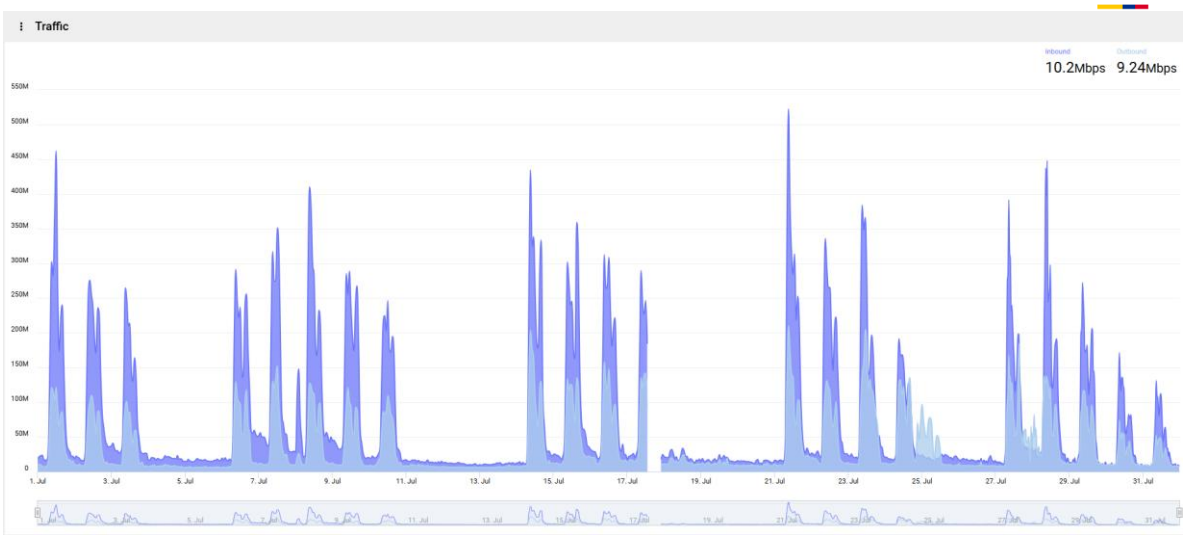


Ilustración 66 Consumo canal MPLS DC Principal

De igual forma se observa que el equipo del proveedor de servicios se encuentra operando de forma estable y no presentó reinicios, se observa un uptime de un año y 12 semanas y tiene consumo promedio de CPU no superior de 1% y de memoria de 40.7%, no se presenta problemas de procesamiento de equipo.

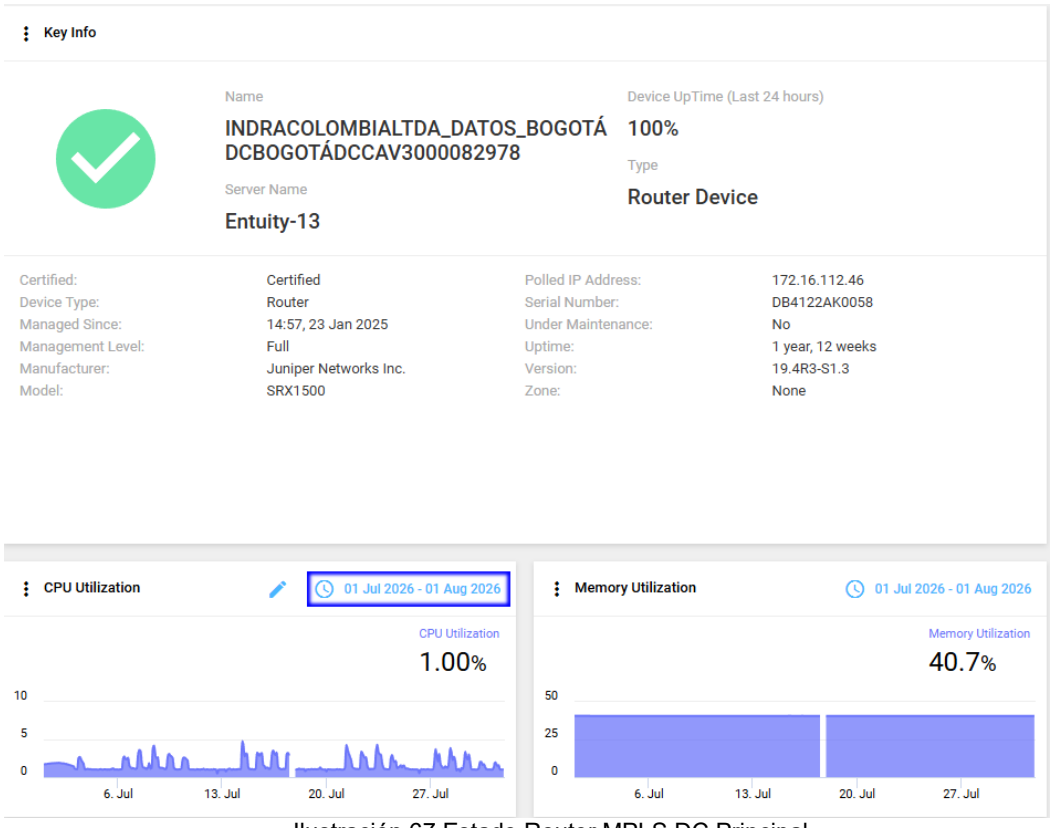


Ilustración 67 Estado Router MPLS DC Principal

3.3.1.1 Incidentes de Conectividad

Durante el julio, se presentaron novedades en el servicio de internet en las siguientes sedes, las cuales fueron escaladas con el proveedor de conectividad:

Dirección Territorial	Caso Asociado	% de Disponibilidad
Bogota Calle 32	IM-285534	98,25%
Carmen de Bolivar	IM- 283263	95,28%
Magangue	IM-283264	94,33%
Chiriguana	IM- 288779	97,70%
Tocancipa	IM-271346	96,79%
Granada	IM-278279	99,23%

Tabla 71 Incidentes de conectividad

3.3.1.2 Topología Actual

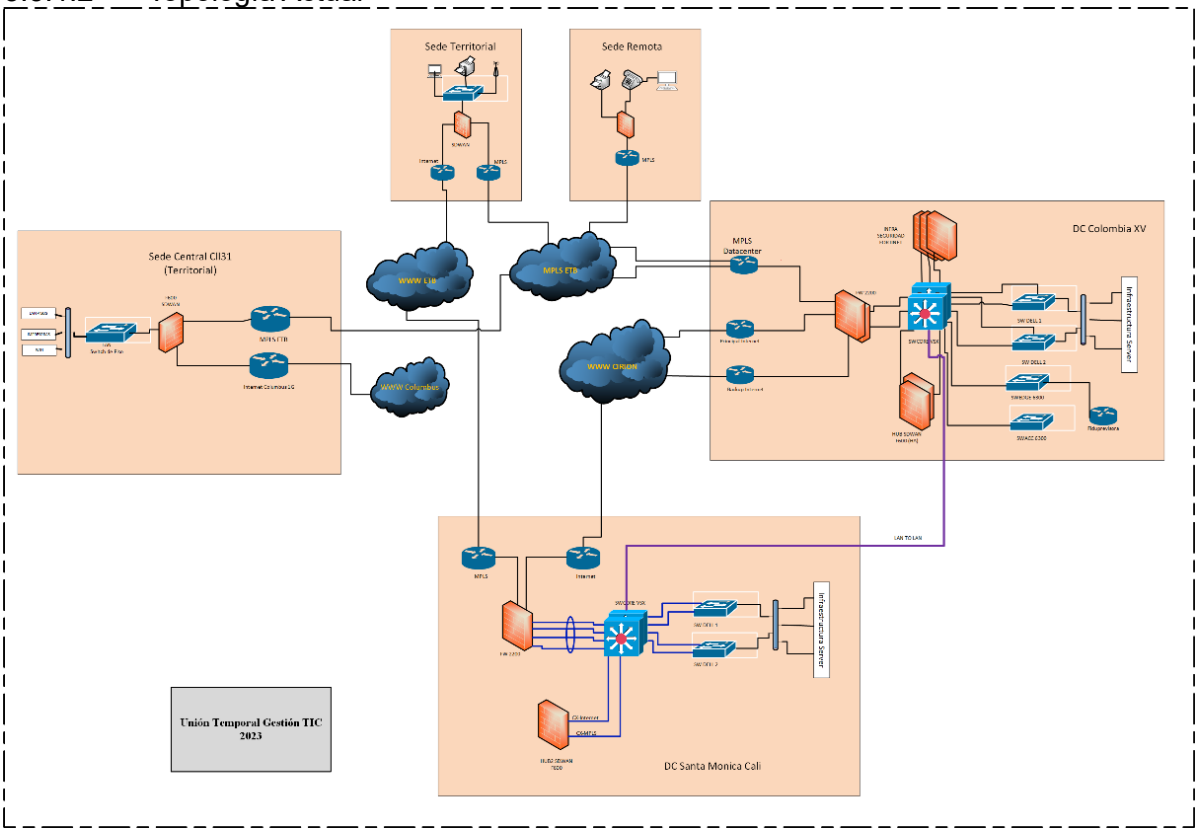


Ilustración 68 Topología actualizada

3.3.2 Canales SDWAN e Internet Dedicado

A nivel de canales de Internet Dedicado, se prestó el servicio en cada sede territorial de forma estable, no obstante, en las sedes donde se presentó algún tipo de falla se generó el respectivo caso con el proveedor, los incidentes presentados se ven reflejados en el ítem 3.3.1.1.

A nivel SDWAN se tienen los equipos registrados en la plataforma Fortimanager, desde donde se observa el estado de los equipos de las sedes territoriales e inspecciones, al igual que el estado de los túneles SDWAN establecidos contra el HUB SDWAN en Datacenter, se tienen 153 equipos registrados en esta plataforma.

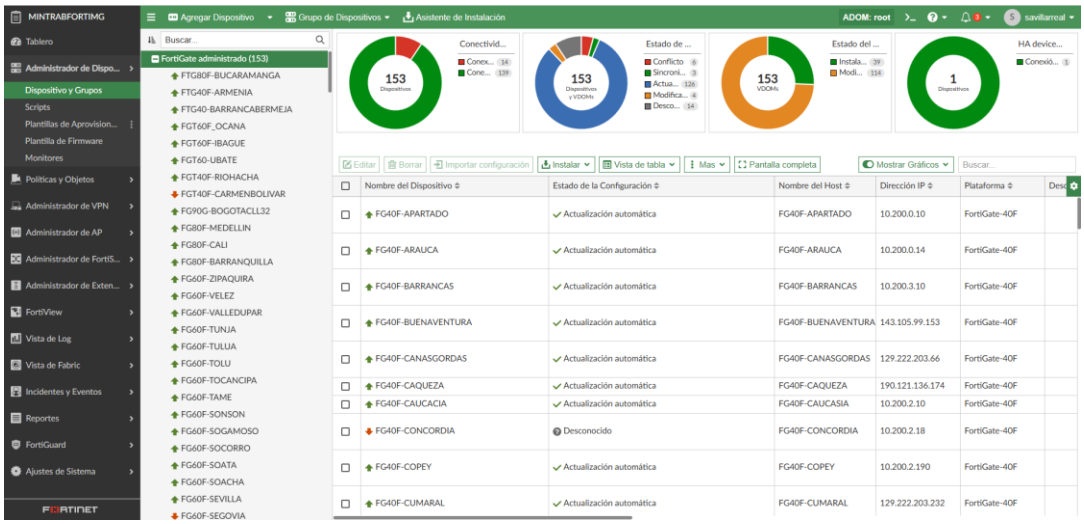


Ilustración 69 Interface Fortimanager

Desde el HUB SDWAN F600, en DataCenter se observa el consumo promedio del canal MPLS, donde no se presenta saturación. Se observa que se tuvo un promedio de 208.23 Mbps de consumo con un máximo de 1.32 Gbps, este canal es de 2GB, con el tráfico generado se observa que no presentó saturación durante el mes.

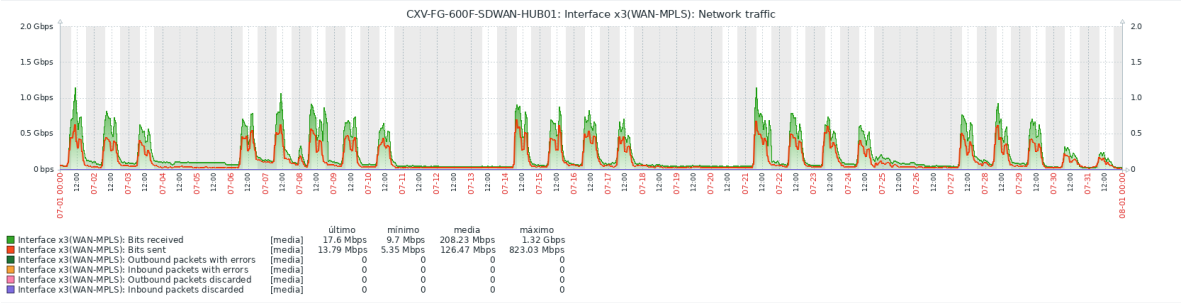


Ilustración 70 Interface MPLS HUB SDWAN

De igual forma, la interface de Internet del HUB no presenta saturación, por esta interface se establece el túnel de respaldo de las sedes territoriales. Se observa que se tuvo un promedio de 41.52 Mbps de consumo en el mes donde se tuvo un máximo de 363.24 Mbps. Este canal es de 1GB, con el tráfico generado en el mes, no se presentó saturación.

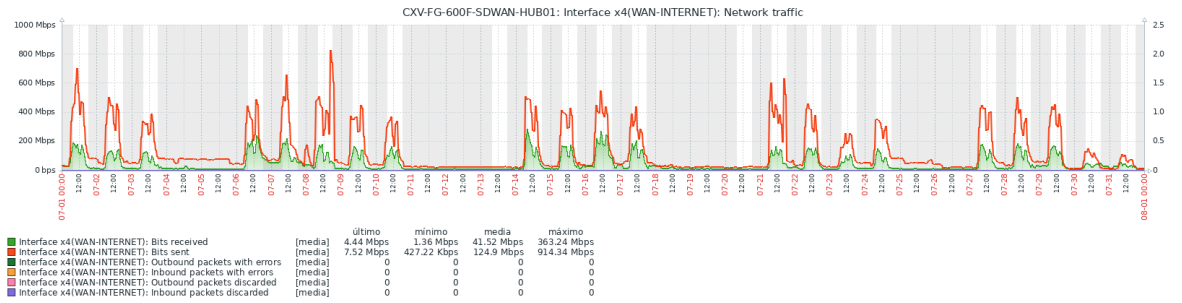


Ilustración 71 Interface Internet HUB SDWAN

Se relaciona las VPNs SDWAN establecidas contra el HUB SDWAN de datacenter, tanto por el canal MPLS y el canal de Internet.

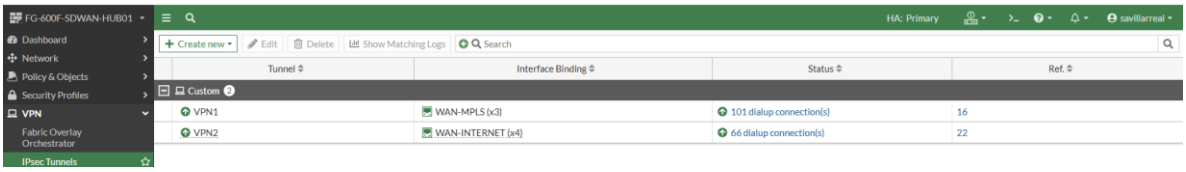


Ilustración 72 VPN SDWAN establecidas

El comportamiento del HUB SDWAN en cuanto a memoria, se observa que no ha tenido alto procesamiento, se observa un pico máximo de 24% de utilización de memoria, el equipo ha trabajado de forma estable sin presentar picos que causen algún bloqueo o algún reinicio de este.

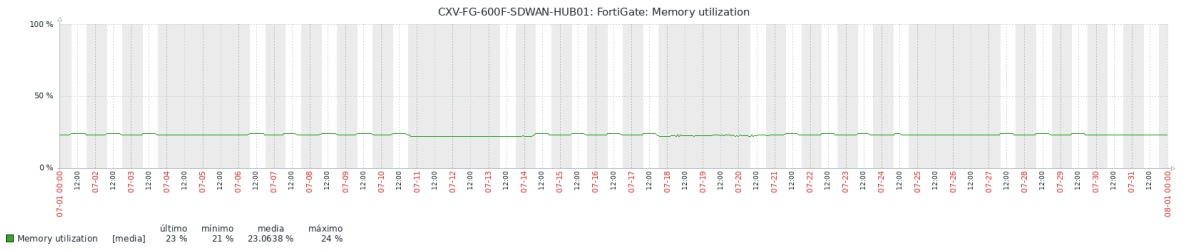


Ilustración 73 Estado HUB SDWAN Datacenter

Se verifica el estado del HA del equipo, donde se observa que se encuentra establecido y sincronizado, no se observan cambios en los roles entre los dos equipos, es decir no se ha presentado afectación sobre el equipo principal.

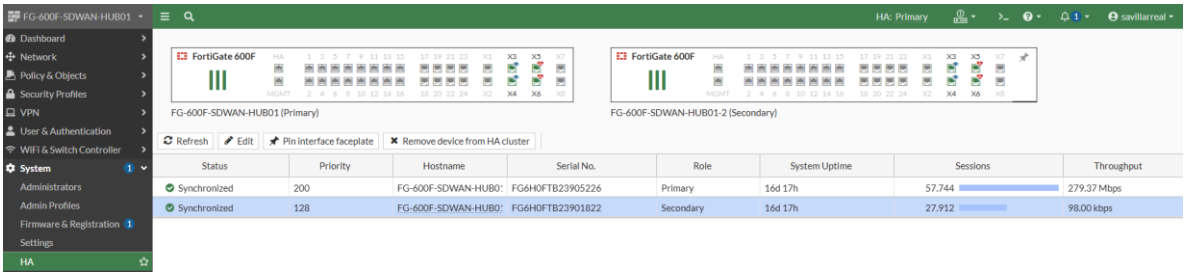


Ilustración 74 Estado HA HUB Sdwan

En cuanto al Fortimanager, se observa los recursos usados para su operación, donde no se tienen picos de procesamiento a nivel de memoria y CPU



Ilustración 75 Recursos Fortimanager

Medición de ANS Conectividad WAN e Internet:

A continuación, el resultado de la medición de los ANS:

ID	Indicadores	Resultado	Meta
CWI-1	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
CWI-2	Continuidad y disponibilidad del servicio de WAN en sedes nacionales con un solo enlace	(*)	99,60%
CWI-3	Continuidad y disponibilidad del servicio de WAN en sedes nacionales con doble enlace (principal MPLS + secundario Internet dedicado)	(*)	99,90%
CWI-4	Continuidad y disponibilidad del servicio de internet en Datacenter principal	100,00%	99,95%
CWI-5	Continuidad y disponibilidad del servicio de internet en Datacenter alterno	100,00%	99,70%
CWI-6	Continuidad y disponibilidad del servicio de WAN en Datacenter principal	100,00%	99,95%
CWI-7	Continuidad y disponibilidad del servicio de WAN en Datacenter alterno	100,00%	99,95%
CWI-8	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 72 Medición de ANS Conectividad WAN e Internet

(*) De acuerdo con la solicitud de la Coordinador del Grupo de Soporte Informático los valores de la continuidad y disponibilidad se encuentran desagregados en el archivo ANS Internet – MPLS y a continuación, se indica el detalle del mes de julio:

CWI-2 Continuidad y disponibilidad del servicio de WAN en sedes nacionales con un solo enlace:

Dirección Territorial	Caso Asociado	% de Disponibilidad	% Penalidad	Valor Penalidad un enlace
Carmen de Bolivar	IM- 283263	95,28%	3%	$ 9.518
Magangue	IM-283264	94,33%	10%	$ 31.725
Chiriguana	IM- 288779	97,70%	3%	$ 9.518
Tocancipa	IM-271346	96,79%	3%	$ 9.518
Granada	IM-278279	99,23%	3%	$ 9.518
Total				**$ 69.796**

Tabla 73 Desagregado sedes con novedad un solo enlace

CWI-3 Continuidad y disponibilidad del servicio de WAN en sedes nacionales con doble enlace:

Dirección Territorial	Caso Asociado	% de Disponibilidad	% Penalidad	Valor Penalidad doble enlace	
Bogota Calle 32	IM-285534	98,25%	3%	$	95.176
Total				**$**	**95.176**

Tabla 74 Desagregado sedes con novedad con doble enlace

4 LINEA DE SERVICIOS EN SEDE

4.1.1.1 Equipos de Cómputo de usuario final

Durante el período, se atendieron las solicitudes relacionadas con la revisión, diagnóstico, pruebas, retiro y asignación de equipos de cómputo. Asimismo, se brindó soporte y seguimiento a las novedades presentadas en el parque computacional de equipos Lenovo, con el fin de garantizar su correcto funcionamiento y disponibilidad.

- **Instalaciones de Equipos y Entrega a Usuarios Finales:**

A continuación, se presentan los equipos dispuestos para la operación conforme al Anexo de Distribución de Equipos y también los equipos efectivamente instalados:

Ítem	Cantidad Equipos Contractual	Cantidad Equipos Instalados	Cantidad Equipos Almacén
Equipos de escritorio	**1172**	1134	38
Equipos portátiles	**1000**	982	138
Equipos portátiles adicionales	**120**		
Total	**2292**	**2116**	**176**

Tabla 75 Cantidades de equipos Contractual – Instalados - Almacén

Nota: Es importante aclarar que el número de funcionarios es inferior al total de equipos de cómputo disponibles para la operación. La cantidad de asignación reflejado corresponde a la totalidad de los equipos, incluyendo tanto los de línea base como los adicionales.

Durante el período, se suspendió la asignación de equipos a contratistas, pasantes, funcionarios con doble asignación, salas de conciliación y otros casos, una vez se recibió el aval del Coordinador del Grupo de Soporte Informático. Esta medida se adoptó debido al ingreso del personal vinculado a través del concurso, con el fin de priorizar la disponibilidad de los equipos para dichas incorporaciones

- **Gestión de Inventario**:

Durante el período, se atendieron las solicitudes de retiro, traslado y asignación de equipos de cómputo, de acuerdo con los requerimientos de los usuarios y las necesidades operativas de la entidad.

ASIGNACION DE EQUIPOS JULIO		
SEDE	ESCRITORIO	PORTATIL
DT Antioquia	2	3
DT Atlántico	1	
DT Bogotá		7
DT Bolívar	2	2
DT Boyacá	2	1
DT Caldas	1	
DT Caquetá	2	
DT Casanare	1	
DT Cesar	2	
DT Choco		1
DT Córdoba	3	5
DT Meta		1
DT Nariño	2	2
DT Norte de Santander	1	4
DT Quindío	4	1
DT Santander	4	1
DT Sucre		1
DT Tolima		2
DT Valle del Cauca		1
Inspección Ocaña	1	
Inspección Sabana de torres	1	
Nivel Central	1	22
OE Apartado		1
OE Barrancabermeja	1	
TOTAL	**31**	**55**

Tabla 76 Cantidades de equipos asignados nivel nacional

DEVOLUCION DE EQUIPOS JULIO		
SEDE	ESCRITORIO	PORTATIL
DT Antioquia	5	1
DT Atlántico	1	
DT Bogotá	2	2
DT Bolívar	1	1
DT Boyacá	1	1
DT Caldas	2	
DT Caquetá	2	
DT Casanare	1	
DT Cesar	1	
DT Córdoba	3	2
DT Guajira		1
DT Nariño		1
DT Norte de Santander		3
DT Quindío	3	
DT Santander	4	1
DT Sucre		1

DT Tolima	1	
DT Valle del Cauca		4
Inspección Acacias	1	
Inspección Cerete	1	
Inspección Fusagasugá	1	
Inspección Sabana de torres	1	
Inspección Sahagún	1	
Inspección Tolú	1	
Nivel central	4	15
OE Apartado		1
TOTAL	**37**	**34**

Tabla 77 Cantidades de equipos por devolución nivel nacional

Se llevó a cabo la consolidación de las actas de asignación y devolución. Las actas fueron digitalizadas y almacenadas en el repositorio del Nivel Central y Territorial, quedando debidamente organizadas y disponibles para su consulta.

- **Gestión de Garantías:**

Durante el mes de julio se reportó un total de 32 casos de garantía. A continuación, se detallan los estados asociados a estos casos:

Estado de caso	Cantidad
Cerrado	16
Suspendido	16
Total	**32**

Tabla 78 Estado de casos de garantía.

Se detalla el cumplimiento del ANS de los casos en garantía:

ANS	Cerrado	Suspendido	Total
CUMPLE	16	16	32
NO CUMPLE			
Total	**16**	**16**	**32**

Tabla 79 ANS casos de garantía.

Fecha de Reporte	Serial	Parte	Falla	Sede	No. Caso	Estado
1/07/2026	VNAA64WZ	Monitor	Distorsión grafica	DT Antioquia	RF-259038	Cerrado
2/07/2026	HC3BBLQK	Diadema	Intermitencia en audio	Nivel Central	RF-261442	Cerrado
6/07/2026	VNAA64KW	Monitor	líneas blancas horizontales	DT Atlántico	RF-268037	Cerrado
6/07/2026	PW09Z328	Portátil	No enciende	Nivel Central	RF-268056	Cerrado
6/07/2026	MJ0LS5VK	Escritorio	Presenta, bloqueo	DT Cauca	RF-268303	Cerrado

8/07/2026	PW0A3BG5	Portátil	Daño en puerto	DT Nariño	RF-270161	Cerrado
9/07/2026	HC3BBNET	Diadema	Daño auricular izquierdo	Nivel Central	RF-271604	Cerrado
10/07/2026	HC3BBNAZ	Diadema	No produce sonido	DT Valle del Cauca	RF-273873	Cerrado
14/07/2026	VNAA5YYC	Monitor	Esta de color verde,	Insp, Cisneros	RF-278088	Cerrado
14/07/2026	VNAA62AC	Monitor	Esta de color verde,	DT Antioquia	RF-278125	Cerrado
15/07/2026	VNAA64GD	Monitor	Presenta rayas	OE Barrancabermeja	RF-278441	Cerrado
15/07/2026	HC3BBN58	Diadema	Audio defectuoso	DT Bogotá	RF-278615	Cerrado
16/07/2026	HC3BBN56	Diadema	Solo suena un auricular	Nivel Central	RF-280042	Cerrado
21/07/2026	HC3BBN7X	Diadema	No se escucha	DT Bogotá	RF-281888	Cerrado
22/07/2026	AVLC39SA4MM	Mouse	No enciende	DT Antioquia	RF-283255	Cerrado
28/07/2026	HC3BBM66	Diadema	Distorsión de sonido	DT Tolima	RF-289375	Cerrado
2/07/2026	MJ0LS5DQ	Escritorio	Equipo no enciende	DT San Andrés	RF-261298	Suspendido
6/07/2026	VNAA6269	Monitor	presentando líneas verticales permanentes	Insp.Mosquera	RF-268194	Suspendido
7/07/2026	VNAA635B	Monitor	líneas rosadas	DT Putumayo	RF-268854	Suspendido
14/07/2026	VNAA64BY	Escritorio	líneas horizontales en la parte inferior	DT Antioquia	RF-278031	Suspendido
21/07/2026	PW0A3CEP	Portátil	Equipo no enciende	DT Córdoba	RF-281989	Suspendido
23/07/2026	VNAA624G	Monitor	dos líneas horizontales	Insp,Aguachica	RF-285483	Suspendido
23/07/2026	VNAA621Y	Monitor	Fallas de imagen	DT Santander	RF-285518	Suspendido
24/07/2026	PW0A3CE2	Portátil	No funciona Touchpad	Nivel Central	RF-286751	Suspendido
24/07/2026	PW0A3BG8	Portátil	Abultamiento	DT Cesar	RF-286830	Suspendido
27/07/2026	VNAA61T7	Monitor	Fuga de colores	DT Caquetá	RF-288202	Suspendido
27/07/2026	VNAA622H	Monitor	fallas de imagen	DT Santander	RF-288204	Suspendido
28/07/2026	VNAA627G	Monitor	Por línea horizontales	DT Córdoba	RF-289420	Suspendido
29/07/2026	HC3BBMAD	Diadema	Daño en micrófono	Nivel Central	RF-289804	Suspendido
29/07/2026	PW0A3CHK	Portátil	No enciende	OE Barrancabermeja	RF-289925	Suspendido
30/07/2026	VLC39SA4KE	Mouse	Clic izquierdo no funciona	DT Cesar	RF-291119	Suspendido
31/07/2026	VNAA64G9	Monitor	Líneas rosadas	Insp. Orito	RF-291327	Suspendido

Tabla 80 ANS Relación casos de garantía

- **Siniestros por daño y hurto:**

Durante la ejecución del contrato, se han presentado siniestros de equipos de cómputo Lenovo atribuibles a accidentes, mal uso por parte de los usuarios finales, robo o pérdida. A continuación, se presenta el consolidado y se detalla el estado actual de cada caso:

Funcionario responsable	Serial	DT	Parte afectada	Estado	Caso Aseguradora/ Lenovo
Muñoz Suescun Yiseth Andrea	PW0A3BE0	DT Cauca	Derrame de líquidos	Aseguradora 08/04/2025// Aseguradora realizó entrega de portátil en Bogotá con serial PW0A3BMM	PRG_2025_1221329

Pavel Santodomingo	PW0A3CDZ	Nivel Central	Derrame de líquidos	Aseguradora realizó la reposición del equipo con serial PW0A3BP1 se hace devolución de equipo dañado	PRG_2025046910//2023159675
Bernardo Ardila Fernández	PW09Z34H	Valledupar	Golpes en esquinas	Aseguradora hace entrega de equipo	PRG_2025_4160592
Galia Lena Álvarez Hernández	PW0A3CHL	Nivel Central	Golpes en esquinas	Aseguradora realizó la reposición del equipo con serial PW09ZT67 /se realiza entrega de equipos dañado	
Henrry Samir Gómez Ortiz	PW0A36X6	Nivel central	Robo	En proceso con aseguradora	PRG_2026_2206888
Ana Mireya Escobar Tierradentro	MJ0LS5TW	Popayán/	No enciende	Se deja una cpu de reposición/Aseguradora/ 09/05/2025 Se realiza reposición de equipos MZ01E5KG	PRG_2025_1766918
Lacides Manuel Morales Ortega	MJ0LS5XL	Sincelejo/ San Marcos	Se apaga y no enciende	Se realiza reposición de equipo MZ01E5KA	PRG_2025_1921454
Jesús Manuel Martínez Franco	PW0A3BEY	Montería	Golpes en esquinas	Aseguradora hace entrega de equipo PW0A370B.	PRG_2025_4160302
Adriana Patricia Martínez Arévalo	PW09Z369	Nivel central	Equipo no da imagen	Se adjunta acta de asignación de equipo de reposición por aseguradora PW09ZT6N 05/08/2025	PRG_2025_2251570
Miguel Ángel Izquierdo Hospital	PW0A3BFT	Nivel Central	Falla en puerto de carga	Aseguradora realizó la reposición del equipo con serial PW09ZT78, se realiza devolución de equipo dañado	PRG_2025_4159804
William Ricardo Álvarez Gómez	PW0A3CK3	Nivel Central	Robo	Se deja equipo de reposición en bodega dado que ya se le había asignado PW0A3AVL al funcionario.	PRG_2025_3861658
Amber Duran Lozano	PW0A3BJM	Nivel central	Reporta varias grietas en el equipo portátil	Aseguradora realizó la reposición del equipo con serial PW0A3BPJ	PRG_2025-4611910
Maria Isabel Cuenca Mendoza	PW0A3BPB	Cali Valle	no responde correctamente a comandos del teclado integrado	Aseguradora realiza reposición de equipo PF68AZS3	PRG_2026_2853
Laura Estefanía Mendoza Quintero	PW0A3CKM	DT Quindío	Robo	Se realiza envió de portátil PW0A3BHA de contingencia/ Se realiza reposición de equipo PF68B03K	
Valeria Márquez Pereira	PW0A3AZW	Nivel central	Robo	Se realiza asignación de equipo de contingencia PW0A36XS/Se realiza reposición de equipo PF68AZRT	PRG_2024_1504426
Silvia Patricia Rojas Ardila	MJ0LS5CD	B/manga	Robo	Pendiente reposición por parte de aseguradora	PRG_2025_4989622
Cindy Julieth Feria Molina	PW0A0FN2	Nivel Central	Robo	Se realiza asignación de equipo PW09ZT6H/Se realiza reposición de equipo PF68B03E	PRG_2026_62277
Jhonny Santander Cerinza	PW0A3AWT	DT Santander	Golpe en cover	Pendiente reposición de equipo	PRG_2026_858978
Viviana Stephanys Plaza Amador	MJ0LS534	La Jagua	No enciende	Pendiente reposición de equipo	PRG_2026_1097575
Brenny Liliana Martínez Gómez	PW0A3CF5	DT Santander	Existe un objeto extraño alojado en su interior	Se envía documentación para proceso con aseguradora	PRG_2026_2209296

Marino Alexander Pantoja Reyes	PW0A3BE5	Ipiales	Daño en teclado	Pendiente reposición	PRG_2026_2208716
Johana Faride Guevara Espinel	PW0A36XX	Bucaramanga	Puerto de entrada de carga no recibe voltaje	Se envía correo para iniciar proceso con aseguradora 25/05/2026	PRG_2026_2207852
Yurley Katherine Castro Sánchez	PW0A3CEG	Nte de Santander	Hurto	Se envía documentación para inicio por aseguradora 24/06/2026	Pte radicado

Tabla 81 Equipos en siniestro

- **Gestión de solicitudes para el servicio**

A continuación, se presenta la gestión de solicitudes de soporte atendidas para este servicio:

- Se registraron en Aranda un total de 32 solicitudes tipificadas así:
  - Incidentes: 0 casos
  - Requerimientos: 32 casos

- Al corte de mes de julio quedaron en estado:
  - Cerrado: 16 casos.
  - Suspendido: 16 casos.

- 29 casos corresponden a solicitudes de usuarios estándar y 3 a usuarios VIP.

- La tabla que se muestra a continuación muestra los Grupos de Especialistas que dieron atención a las solicitudes del servicio:
-

Grupo responsable	Cantidad de solicitudes
Gestor de garantías	30
Gestor de inventarios	2
Total, general	

Tabla 82 Solicitudes de Equipos Usuario Final – Según Grupo Responsable

- La tabla que se muestra a continuación indica las categorías en las que fueron clasificados estos casos en Aranda:

Tipificación / Categoría	Cantidad de Solicitudes
Incidentes	**0**
Requerimientos	**32**
Equipo Periférico	**19**
Equipo Escritorio	**7**
Equipo Portátil	**6**
Total	**32**

Tabla 83 Solicitudes de Equipos Usuario Final – Según Grupo Responsable

4.1.2 Equipos de Escritorio

Durante el mes de julio, se continuó la gestión y atención de los equipos de cómputo de escritorio asignados a los usuarios de la entidad con problemas de salud y autorizados por la coordinación, en el nivel central y en las sedes territoriales.

4.1.3 Equipos Portátiles

Durante el mes de julio se realizó la gestión y atención de todos los equipos de cómputo portátiles asignados a los usuarios de la entidad tanto en el nivel central como en las sedes territoriales.

ID	Indicadores	Resultado	Meta
EUF-1	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
EUF-2	Cumplimiento en la entrega del informe	100,00%	100,00%

Tabla 84 Medición ANS Equipos de Usuario Final

4.2 Conectividad LAN y WLAN

A continuación, se relacionan las novedades y actividades relevantes gestionadas durante el mes por el equipo de redes y conectividad:

- Se realizó gestión en la revisión y solución de alertas sobre dispositivos como Access Point con la colaboración de los soportes en sitio. No se presentan novedades sobre equipos de acceso.
- Se realizó gestión y seguimiento a alertas de caídas y degradación de servicio sobre canales de comunicación (MPLS e Internet) para lograr el restablecimiento del servicio por parte del proveedor de conectividad.
- Se gestionó reemplazo de adaptador antena Starlink en Riosucio Choco para el restablecimiento del servicio.
- Se ejecutó sincronización de firewalls en oficinas Territoriales e Inspecciones con configuración del Fortimanager.
- Se gestionó reemplazo de adaptador antena Starlink en Curumaní / Cesar para el restablecimiento del servicio. El 1/07/2026 se gestiona la doble garantía de la antena en esta inspección que presento doble falla por fluctuaciones eléctricas. La UT realizó la compra de un supresor de picos ya que no se adelantó ninguna verificación pon parte de la sede al tema de conexiones o revisión con el dueño del predio.
- Se activó el protocolo IPv6 en los túneles SD-WAN de oficina Sede Central.
- El 10/07/2026 se hace la ejecución del cambio RFC-268678 relacionado con las Pruebas HA del equipo SD-WAN F600 en el Datacenter Colombia XV, resulta exitosa la actividad.
- Se realizó revisión del problema PM-278729 acerca de la creación shortcut advpn y perdida de conectividad SD-WAN con algunas oficinas (intermitencia en los túneles SD-WAN)y se dio la respectiva solución durante el mes, se realizó escalamiento al proveedor quien identificó posible bug en FortiOS, el fabricante asignó el caso No. 11995017.

- Se realiza acompañamiento al aliado Apicom para la actividad de reconfiguración de la tarjeta de red y el monitoreo de red por SNMP para la UPS del piso 25.

A continuación, se relaciona la gestión de solicitudes en Aranda por parte de los responsables del servicio:

- Los especialistas gestionaron un total de 23 solicitudes escaladas a través de la herramienta Aranda. Al corte del mes los 23 casos quedaron en estado Cerrado. Los casos obedecen a la revisión de alertas sobre caída de servicios de conectividad, degradación y lentitud sobre los canales, bloqueo e intermitencia en red de Access Points, ejecución de RFCs para habilitar protocolo IPv6 en túneles SD-WAN de Sede Central, ejecutar pruebas de HA en HUB Colombia XV y reconfiguración de tarjeta de red UPS piso 25, atención de alertas por el problema PM-278729 postulado y configuración puertos de red. Los demás casos relacionados con el servicio se gestionaron por parte del NOC, los detalles se relacionan en el apartado 2.1.2.8. Práctica de Eventos de este mismo documento.

A continuación, se relaciona el TOP 5 de las solicitudes más frecuentes asociadas al servicio:

Categoría	Cantidad de solicitudes
Asesoría - Consulta	4
Degradación	4
Starlink	3
AP	2
FortiGate	2

Tabla 85 Top 5 de categorías en el Servicio de conectividad LAN-WLAN

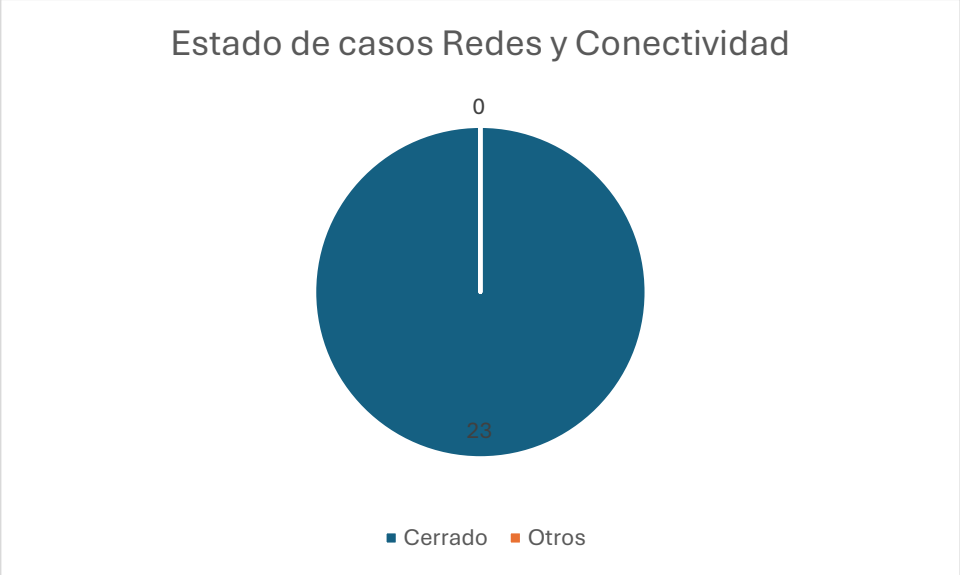


Ilustración 76 Estado de casos Redes y Conectividad

Este servicio comprende la administración y gestión de los siguientes dispositivos:

4.2.1 Switch CORE Sede Principal

Se encuentra operativo en Datacenter a través del cual se concentran las conexiones de infraestructura de servicios y aplicaciones e infraestructura de seguridad.

4.2.2 Switch para conexiones perimetrales (EDGE) en sede principal

Se encuentra operativo en Datacenter recibiendo las conexiones del canal de internet y conexiones perimetrales.

4.2.3 Switch de acceso 24 puertos

Se encuentran operativos y en monitoreo los siguientes equipos:

Dirección Territorial	Población y/o ciudad de ubicación	Cantidad switches 24 puertos
Territorial Atlántico	BARRANQUILLA	1
Territorial Bolívar	Cartagena	1
Territorial Boyacá	TUNJA	1
Territorial Caldas	MANIZALEZ	1
Territorial Caquetá	FLORENCIA	1
Territorial Casanare	YOPAL	1
Territorial Cesar	VALLEDUPAR	1
Territorial Córdoba	MONTERIA	1
Territorial Cundinamarca	FACATATIVÁ	1
Territorial Magdalena	SANTA MARTA	1
Territorial Norte de Santander	CÚCUTA	1
Territorial Putumayo	MOCOA	1
Territorial Risaralda	PEREIRA	1
Territorial Santander	BUCARAMANGA	1
Territorial Tolima	IBAGUÉ	1
Territorial Valle	CALI	2*
Sede Nivel Central	BOGOTA	7
	Total	**24**

Tabla 86 Distribución y Cantidades de switch 24 puertos

(*) Se instaló 1 equipo adicional en la Territorial Valle del Cauca en la ciudad de Cali.

4.2.4 Switch de acceso 48 puertos

Se encuentran operativos y en monitoreo los siguientes equipos:

Dirección Territorial	Población y/o ciudad de ubicación	Cantidad switches 48 puertos
Territorial Antioquia	MEDELLIN	4*
Territorial Arauca	ARAUCA	1
Territorial Atlántico	BARRANQUILLA	2
OE Barrancabermeja	BARRANCABERMEJA	1
Calle 32	BOGOTA	5

Dirección Territorial	Población y/o ciudad de ubicación	Cantidad switches 48 puertos
Territorial Bolívar	Cartagena	1
Territorial Boyacá	TUNJA	1
Territorial Caldas	MANIZALEZ	1
Territorial Cauca	POPAYAN	1
Territorial Cesar	VALLEDUPAR	1
Territorial Chocó	QUIBDÓ	1
Territorial Córdoba	MONTERIA	1
Territorial Cundinamarca	FACATATIVÁ	1
Territorial Guajira	RIOHACHA	1
Territorial Huila	NEIVA	1
Territorial Magdalena	SANTA MARTA	1
Territorial Meta	VILLAVICENCIO	1
Territorial Nariño	PASTO	1
Territorial Norte de Santander	CÚCUTA	1
Territorial Quindío	ARMENIA	1
Territorial Risaralda	PEREIRA	1
Territorial Santander	BUCARAMANGA	2
Territorial Sucre	SINCELEJO	1
Territorial Tolima	IBAGUÉ	1
OE Urabá Apartadó	APARTADÓ	1
Territorial Valle	CALI	2
OE Buenaventura	BUENAVENTURA	1
Sede Nivel Central	BOGOTA	34*
	Total	**71**

Tabla 87 Distribución y Cantidades de Switch 48 puertos

(*) Se instalaron 8 equipos adicionales en las siguientes sedes:

Sede Nivel Central P19: 3 de 48 puertos
P24: 2 de 48 puertos
P25: 2 de 48 puertos
Medellín 1 de 48 puertos

4.2.5 Puntos de Acceso

Se encuentran operativos y en monitoreo los siguientes equipos:

Dirección Territorial	Población y/o ciudad de ubicación	Cantidad Access Points
Territorial Antioquia	MEDELLIN	4
Territorial Arauca	ARAUCA	1
Territorial Atlántico	BARRANQUILLA	3
OE Barrancabermeja	BARRANCABERMEJA	2
Calle 32	BOGOTA	5
Territorial Bolívar	Cartagena	2
Territorial Boyacá	TUNJA	2
Territorial Caldas	MANIZALEZ	2

Dirección Territorial	Población y/o ciudad de ubicación	Cantidad Access Points
Territorial Caquetá	FLORENCIA	1
Territorial Casanare	YOPAL	2
Territorial Cauca	POPAYAN	2
Territorial Cesar	VALLEDUPAR	2
Territorial Chocó	QUIBDÓ	2
Territorial Córdoba	MONTERIA	2
Territorial Cundinamarca	FACATATIVÁ	2
Territorial Guajira	RIOHACHA	2
Territorial Huila	NEIVA	0
Territorial Magdalena	SANTA MARTA	2
Territorial Meta	VILLAVICENCIO	3
Territorial Nariño	PASTO	2
Territorial Norte de Santander	CÚCUTA	3
Territorial Putumayo	MOCOA	1
Territorial Quindío	ARMENIA	3
Territorial Risaralda	PEREIRA	2
Territorial Santander	BUCARAMANGA	1
Territorial Sucre	SINCELEJO	2
Territorial Tolima	IBAGUÉ	3*
OE Urabá Apartadó	APARTADÓ	2
Territorial Valle	CALI	4
OE Buenaventura	BUENAVENTURA	1
Sede Nivel Central	BOGOTA	46
	Total	**111**

Tabla 88 Distribución de puntos de acceso

Territorial Norte de Santander - Cúcuta: El AP fue enviado e instalado en la DT Santander / Bucaramanga
Calle 32: Se instaló 1 Access Point en la sala de reuniones quedando 5 en total operativos.
Territorial Tolima -Ibagué: En la sede permitieron la instalación de 3 AP y 1 equipo restante se encontraba en Stock. El 11/06/2025 se gestionó la recolección del AP disponible y se envió a sede Central.

- **Medición de ANS LAN y WLAN**

A continuación, el resultado de la medición de los ANS:

ID	Indicadores	Resultado	Meta
LW-1	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
LW-2	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 89 Medición ANS LAN y WLAN

4.3 Telefonía IP

Este servicio comprende Terminales HardPhone compatibles Teams Phone.

4.3.1 Teléfono Gama Media

Se cuenta con los siguientes equipos:

Dirección territorial	Población y/o ciudad de ubicación	Cantidad teléfonos Gama Media
Territorial Antioquia	MEDELLIN	1
Territorial Atlántico	BARRANQUILLA	1
Territorial Bogotá	BOGOTA	1
Territorial Santander	BUCARAMANGA	1
Territorial Valle	CALI	1
Sede Nivel Central	BOGOTA	45*
	Total	**50**

Tabla 90 Equipos gama media

(*)
Nivel Central disponibilidad de 13 teléfonos, a espera de asignación por demanda por parte de la entidad

4.3.2 Teléfono Gama Baja

La totalidad de los equipos de telefonía tanto de gama media como de gama baja fueron puestos a disposición para el servicio y se encuentran en cada sede de acuerdo con el anexo de distribución de equipos.

Se indica a continuación las novedades presentadas en la operación de los 350 teléfonos de gama baja:

Dirección territorial	Población y/o ciudad de ubicación	Cantidad teléfonos Gama Baja	Novedad
ANTIOQUIA	AMAGA	1	Cerrada se envió teléfono a Medellín
CASANARE	MONTERREY	1	Cerrada
CAUCA	BOLIVAR	1	Cerrada
CORDOBA	TIERRA ALTA	1	Cerrada
QUINDIO	QUIMBAYA	1	Cerrada
QUINDIO	CALARCA	1	Cerrada
SUCRE	MAJAGUAL	1	Cerrada
TOLIMA	CASA DE JUSTICIA (IBAGUÉ)	1	Cerrada
	Total	**8(*)**	

Tabla 91 Sedes cerradas

Estado	Cantidad
Operativos	327
Inspecciones cerradas	8**(*)**
Disponibles para asignación por MinTrabajo	15
Total	**350**

Tabla 92 Consolidado de teléfonos gama baja

Adicionalmente el servicio de Telefonía IP incluye:

4.3.3 Troncales SIP

La troncal SIP estuvo operativa y funcionando adecuadamente. Se dispuso de la troncal SIP con el proveedor de atención al ciudadano BPM, en el cual el redireccionamiento de llamadas de las opciones 0 y 2, se encuentra operando de manera satisfactoria. Adicional se crea el menú de operadora para el grupo “1070” soporte IVC el cual continúa operando de manera correcta.

4.3.4 No Aplica

4.3.5 No Aplica

4.3.6 Módems 4G – Con plan de 50 Gbps

A continuación, se mencionan los equipos en operación en Nivel Central y DT para el servicio de MIFI y los equipos disponibles para asignación según novedades o solicitudes del ministerio.

Sede	Cantidad
Asignados Nivel Central y DT	25
Disponibles para asignación	5
Total	30

Tabla 93 Consolidado equipos MIFI

De acuerdo con la directriz recibida, los cinco equipos restantes se tienen en almacén como stock y se destinarán a una asignación emergente por solicitud expresa del cliente.

- **Gestión del servicio**

En el mes de julio de 2026, se presentaron las siguientes novedades sobre el servicio:

- Operatividad sobre la grabación de llamadas en la mesa de servicios.
- Configuración de permisos de llamadas a celular, larga distancia nacional, local a coordinadores e implementación de licenciamiento correspondiente al Addon Phone System a nivel nacional.
- Se tienen teléfonos hardphone disponibles para aprovisionamiento al usuario final a nivel nacional, se relacionan en este informe las cantidades según cada referencia.
- Se continúa el monitoreo sobre las troncales para las opciones 2 y 0 configuradas en el IVR para atención al ciudadano con el nuevo aliado BPM.
- En seguimiento al caso RF-188953, se informa que se mantiene monitoreo diario sobre la línea 1080 correspondiente a la mesa de servicios, con el objetivo de verificar continuamente el comportamiento del servicio; adicionalmente, se están recopilando y almacenando de forma permanente las trazas y evidencias técnicas derivadas de las pruebas realizadas, permitiendo un control detallado de la operación y garantizando la estabilidad y disponibilidad del servicio, sin evidenciarse a la fecha anomalías en la infraestructura.



Validación caso
RF-188953 - Falla de

- Durante el mes en curso se realizó el proceso de configuración y aprovisionamiento de extensión y asignación de licencia de Teams Phone Standard en el tenant de Microsoft

Teams para un usuario solicitado. Los cambios fueron aplicados exitosamente. Se adjuntaron manuales de soporte y configuración para referencia. Estado actual: Todos los usuarios se encuentran activos - RF-228798 – RF - 278436 - RF-276958 - RF-261339.



Asignación ext_
virtual_Teams_Caso_

- Durante el período se remite correo al Ing. Guillermo Guerra indicando que teniendo en cuenta la próxima renovación del licenciamiento, se debe considerar que es necesario, durante la vigencia de las licencias adquiridas del complemento Teléfono Microsoft Teams Estándar (Add-on Phone System), se active y configure correctamente la licencia adicional denominada Cuenta de recursos de Teléfono Microsoft Teams (Teams Resource Account) la cual tiene costo cero. Lo anterior debido a que la Cuenta de recursos de Teléfono Microsoft Teams es fundamental para el funcionamiento de recursos automatizados dentro del entorno de **Teams Phone System**, como los Operadores Automáticos (Auto Attendants) y Colas de llamadas (Call Queues). Estas cuentas permiten enrutar llamadas a menús interactivos o grupos de agentes sin estar asociadas a un usuario específico.



Recordatorio técnico
– Cuentas de recurso

- Se realizó la actualización de la infraestructura de telefonía a la última versión de firmware y software liberada por el fabricante de la plataforma. La cual se autoriza bajo el cambio RFC-270098, con el propósito de incorporar mejoras en rendimiento, funcionalidades y seguridad.



El Cambio No_
RFC-270098 se le ha

- **Asignación de Licencias – Extensiones**

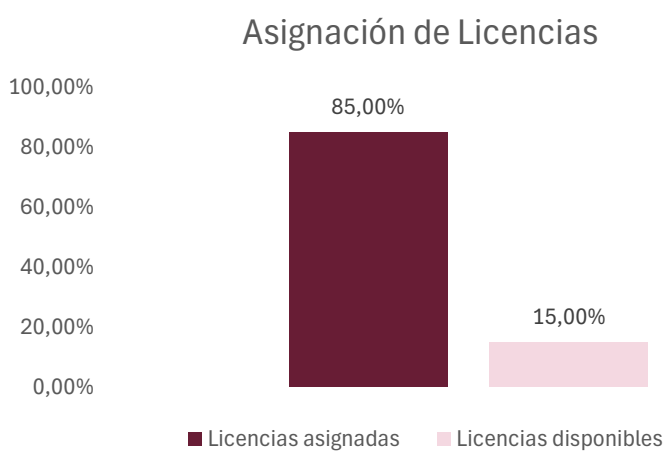


Ilustración 77 Asignación de licencias

Durante el mes en gestión, se han asignado un total de 510 extensiones a nivel nacional. Actualmente, permanecen disponibles 90 extensiones.

- **Estadísticas de Tráfico**

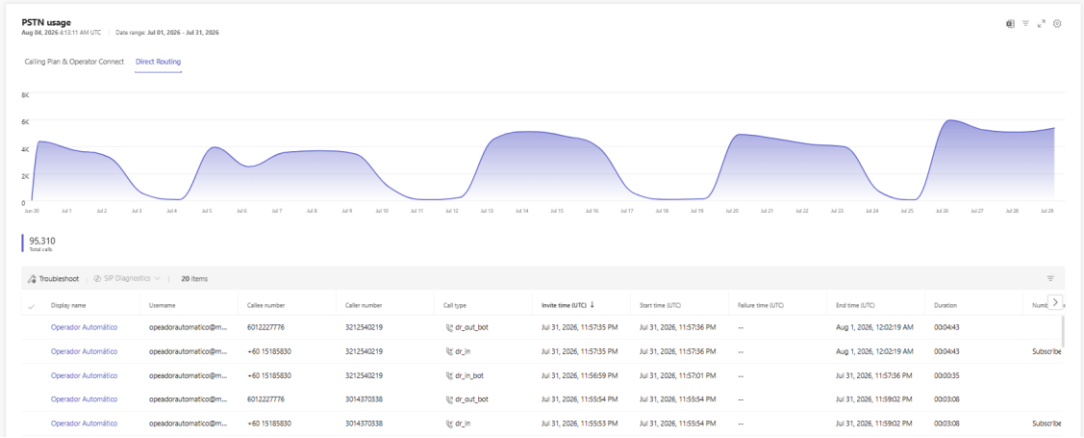


Ilustración 78 Comportamiento de tráfico

En la gráfica anterior se visualizan las tendencias de uso del servicio, en el periodo correspondiente al mes de julio de 2026, donde se atendieron un total de 95,310 llamadas.

Servicio	Minutos Disponibles	Minutos Utilizados
Locales	Ilimitados	1844.19
Celular	1000	931.1
Nacional	Ilimitados	852.27
Internacional	700	6.20
Total		3233,76

Tabla 94 Minutos, consumos

- **Consumo de llamadas LDN (Larga Distancia Nacional)**

Con respecto a las llamadas realizadas a destinos larga distancia nacional en el mes de julio de 2026, se identifica que se realizaron llamadas con una duración total de 425.27 minutos.

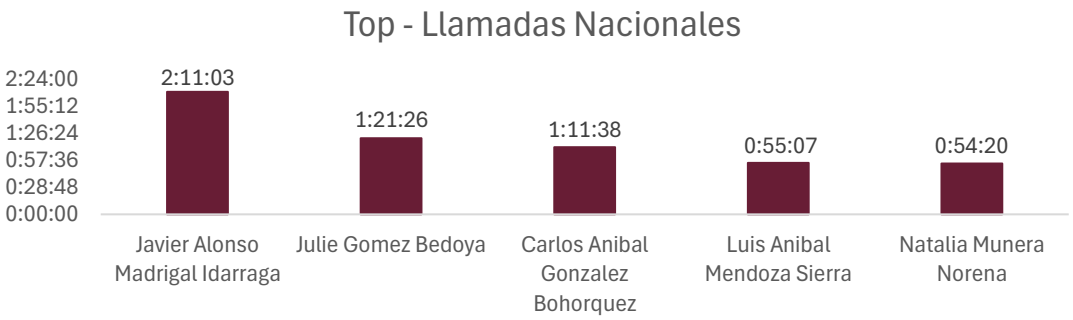


Tabla 95 Top llamadas nacionales

N°	Usuario	Área	Tiempo llamadas
1	Javier Alonso Madrigal Idarraga	Grupo de Resolución de Conflictos y Conciliaciones - DT Antioquia	2:11:03
2	Julie Gomez Bedoya	Grupos de Riesgos – DT Valle del Cauca	1:21:26
3	Carlos Anibal Gonzalez Bohorquez	Administrativa – DT Antioquia	1:11:38
4	Luis Anibal Mendoza Sierra	Inspector Municipal – DT Antioquia	0:55:07
5	Natalia Munera Norena	Grupo de Riesgos Laborales - DT Antioquia	0:54:20

Tabla 96 Top 5 consumo de llamadas

- **Consumo de llamadas LDI (Larga Distancia Internacional)**

Con respecto a las llamadas internacionales en el mes de julio de 2026, se muestra que se registra una llamada a destinos de larga distancia internacional realizada a modo de prueba con la finalidad de garantizar el funcionamiento. A continuación, se muestra el Ilustración correspondiente.

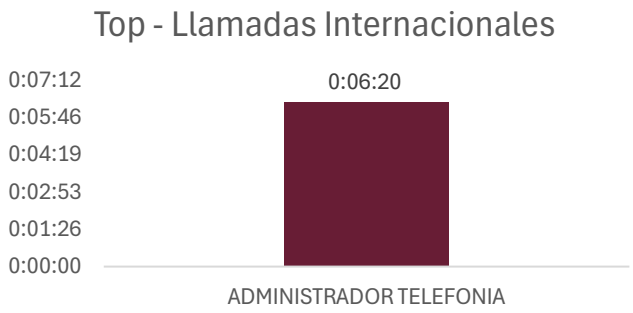


Ilustración 79 llamada internacional de prueba

Como se puede observar en el grafico anterior, se evidencia que, en el mes de julio de 2026 se ha generado un consumo de llamada a destino internacional (España) por el administrador de telefonía, este a modo de prueba con el fin de validar la operatividad del servicio en las llamadas realizadas a larga distancia internacional.

N°	Usuario	Área	Tiempo llamadas
1	Administrador Telefonía	UT	0:06:20

Tabla 97 Top 5 llamadas LDI

- **Consumo de llamadas destinos celulares**

Con respecto a las llamadas realizadas a celular en el mes de julio de 2026, se identifica que se realizaron llamadas con una duración total de 931.1 minutos (15,51 horas).

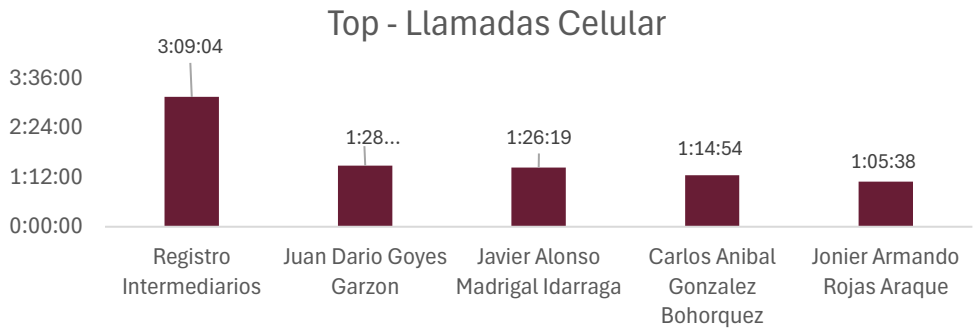


Ilustración 80 Top Celular

N°	Usuario	Área	Tiempo llamadas
1	Registro Intermediarios	Grupo de Registro Único de Intermediarios	3:09:04
2	Juan Dario Goyes Garzon	Dialogo Social – DT Antioquia	1:28:51
3	Javier Alonso Madrigal Idarraga	Grupo de Resolución de Conflictos y Conciliaciones - DT Antioquia	1:26:19
4	Carlos Anibal Gonzalez Bohorquez	Administrativa – DT Antioquia	1:14:54
5	Jonier Armando Rojas Araque	Inspector Municipal – DT Caquetá	1:05:38

Tabla 98 Top 5 llamadas Celular

- **Consumo de llamadas locales**

Con respecto a las llamadas realizadas a destinos locales en el mes de julio de 2026, se identifica que se realizaron llamadas con una duración total de 1844.19 minutos (30,73 horas).

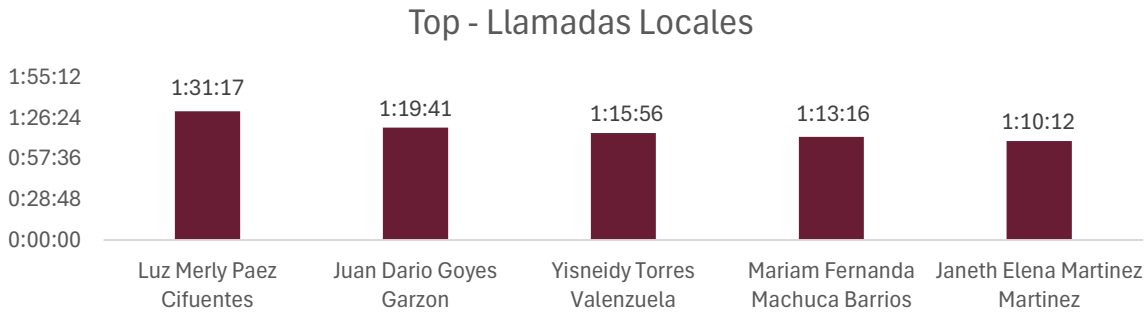


Ilustración 81 Top Local

N°	Usuario	Área	Tiempo llamadas
1	Luz Merly Paez Cifuentes	Comunicaciones DT – Bogotá	1:31:17
2	Juan Dario Goyes Garzon	Dialogo Social – DT Antioquia	1:19:41
3	Yisneidy Torres Valenzuela	Inspector Municipal – DT Caquetá	1:15:56
4	Mariam Fernanda Machuca Barrios	Grupo de Resolución de Conflictos y Conciliaciones - DT Bolivar	1:13:16
5	Janeth Elena Martinez Martinez	Subdirección Administrativa y Financiera – DT Bogotá	1:10:12

Tabla 99 Top 5 llamadas locales

- **Capacitaciones y divulgaciones**

En el mes de julio no se realizó proceso de capacitación y/o divulgaciones.

- **Mejores Prácticas**

Se avanza en la liberación de licencias a nivel nacional por demanda y se continuará con la validación de los respaldos de grabaciones de las llamadas que ingresan a la mesa de servicios.

- **Medición de ANS – Telefonía IP**

A continuación, el resultado de la medición de los ANS correspondientes:

TIP-1 Tiempo de solución de requerimientos de garantía

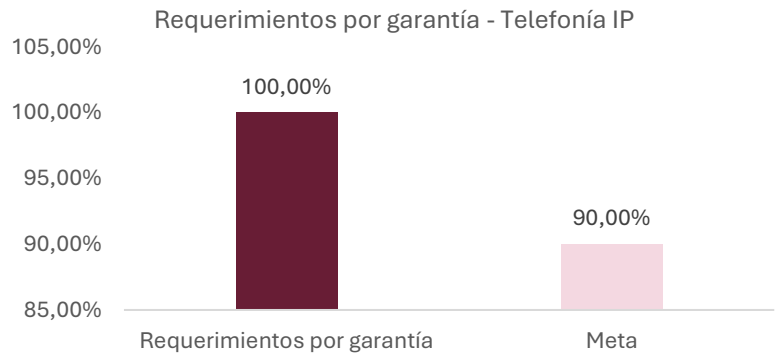


Ilustración 82 Requerimientos por garantía

En el periodo correspondiente a este informe no se generaron requerimientos nuevos de garantía, por tal motivo el valor reportado de cumplimiento se mantiene en el 100%.

TIP-2: Continuidad y disponibilidad de los servicios de Telefonía IP

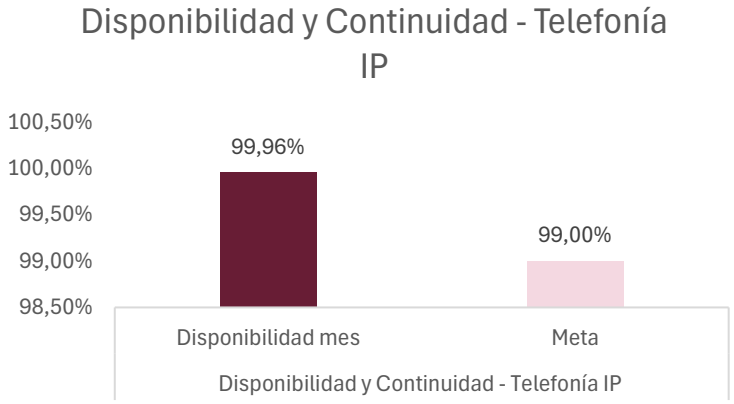


Ilustración 83 Disponibilidad y Continuidad TOIP

En el periodo correspondiente al mes de julio, se evidenció un comportamiento estable de los servicios de telefonía, cumpliendo lo establecido en los ANS pactados para el servicio.

A continuación, el resultado de la medición de los ANS correspondientes:

ID	Indicadores	Resultado	Meta
TIP-1	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
TIP-2	Continuidad y disponibilidad de los servicios de telefonía IP	99,96%	99,00%
TIP-3	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 100 Medición ANS Telefonía IP

4.4 Energía Regulada UPS

El servicio de Energía Regulada UPS comprende las sedes indicadas por la Entidad dentro de los anexos técnicos del contrato, con una distribución de equipos por locación así:

- SEDE NIVEL CENTRAL (14 equipos)
- TERRITORIAL TOLIMA (1 equipo)
- TERRITORIAL BOYACÁ (1 equipo)
- TERRITORIAL BOLÍVAR (1 equipo)
- TERRITORIAL CALDAS (1 equipo)
- TERRITORIAL RISARALDA (1 equipo)
- OE BARRANCABERMEJA (1 equipo)
- TERRITORIAL SANTANDER (1 equipo)
- TERRITORIAL ANTIOQUIA (1 equipo)

TOTAL EQUIPOS: 22

4.4.1 UPS 10 kVA

SEDE	POBLACIÓN Y/O CIUDAD	UBICACIÓN EN LA SEDE	CANTIDAD DE TOMACORRIENTES ASOCIADAS	MARCA	REFERENCIA UPS	NUMERO DE SERIE UPS
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 25	63	ABLEREX	KRONOS UL10D	TD8062B8B001
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 24	53	ABLEREX	KRONOS UL10D	TD7049D7F0002
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 3	53	ABLEREX	KRONOS UL10D	TD7049D7F0001
TERRITORIAL TOLIMA	IBAGUÉ	Centro de Cableado piso 5	39	ABLEREX	AB-MSIII10000	MA6133C9M0007
TERRITORIAL BOYACÁ	TUNJA	Centro de cableado sótano	27	ABLEREX	AB-MSIII10000	MA8007CAB0015
TERRITORIAL BOLÍVAR	CARTAGENA	Cuarto Técnico en el primer piso, debajo de las escaleras	54	ABLEREX	AB-MSIII10000	MA6133C9M0060
TERRITORIAL CALDAS	MANIZALES	Centro de cableado principal piso 3	44	ABLEREX	AB-MSIII10000	MA8007CAB0037

TERRITORIAL RISARALDA	PEREIRA	Centro de cableado piso 4 contiguo al auditorio	32	ABLEREX	AB-MSIII10000	MA6133C9M0043

Tabla 101 Inventario de UPS – 10kVA

4.4.2 UPS 15 kVA

Durante la implementación de la solución del servicio para el cliente Ministerio del Trabajo no se realiza instalación de UPS de 15kVA, el detalle de esto se entregó a la Supervisora del Contrato del momento, en el INFORME UT GESTION TIC 2023 - ENTREGA LINEA DE SERVICIO EER UPS

Ruta Repositorio MinTrabajo: 3. INFORME UT GESTION TIC 2023 - ENTREGA LINEA DE SERVICIO EER UPS.pdf

4.4.3 UPS 20 kVA

SEDE	POBLACIÓN Y/O CIUDAD	UBICACIÓN EN LA SEDE	MARCA	REFERENCIA UPS	NUMERO DE SERIE UPS
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 23	ABLEREX	KRONOS UL20D	TD8004CC80020
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 22	ABLEREX	KRONOS UL20D	TD2110B2M0006
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 21	ABLEREX	KRONOS UL20D	TD8004CC80001
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 20	ABLEREX	KRONOS UL20D	TD8004CC80025
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 19	ABLEREX	KRONOS UL20D	TD8004CC80023
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 18	ABLEREX	KRONOS UL20D	TD8004CC80012
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 17	ABLEREX	KRONOS UL20D	TD2110B2M0004
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 10	ABLEREX	KRONOS UL20D	TD9121BAS0008
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 9	ABLEREX	KRONOS UL20D	TD8004CC80015
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 8	ABLEREX	KRONOS UL20D	TD8004CC80003
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 5	ABLEREX	KRONOS UL20D	TD8004CC80002
TERRITORIAL SANTANDER	BUCARAMANGA	Cuarto técnico piso 2	ABLEREX	KRONOS-UL20D	TD8004CC80018
TERRITORIAL ANTIOQUIA	MEDELLÍN	cuarto técnico primer piso	ABLEREX	KRONOS-UL20D	TD4007C740004
OE BARRANCABERMEJA	BARRANCABERMEJA	Cuarto técnico primer piso	ABLEREX	KRONOS-UL20D	TD8004CC80004

Tabla 102 Inventario de UPS – 20Kva

- **Gestión del servicio**

Las UPS se encuentran instaladas y operativas según distribución dada por el cliente a nivel contractual, durante el período no se presentan fallas en el servicio que requieran cambios de equipos en ninguna sede ni gestión de garantías que requiera reemplazo de partes/repuestos por parte de la UT.

A continuación, se relacionan los casos gestionados:

No. Caso	Tipo de Caso	Estado	Descripción	Solución
RFC-285643	Change	Cerrado	Se solicita la creación del siguiente RFC de Emergencia con el fin de que el proveedor realice la reconfiguración la tarjeta de red en la UPS del piso 25 y recuperar el monitoreo por SNMP. Fecha ejecución: lunes 27 de julio a partir de las 9am, sin afectación.	Se ejecuta RFC y se logró recuperar red y monitoreo SNMP de la tarjeta de red de la UPS del piso 25 con resultado exitoso, se adjunta formato de Entrega de Pruebas Previas y Posteriores

Tabla 103 Casos gestionados – Energía Eléctrica Regulada UPS

Se generaron unos incidentes adicionales relacionados en el apartado 2.1.2.6. Práctica de Incidentes que están relacionados a un Incidente Mayor de Conectividad en la zona que generó alertas de todos los dispositivos monitoreados en Zabbix para las DT Antioquia, DT Risaralda y DT Boyacá, pero se aclara que el servicio estuvo completamente disponible.

- **Novedades UPS**
  - En febrero 2026 se realizó escalamiento a la entidad referente a la novedad con la UPS en la territorial de Santander (Bucaramanga) propiedad de la UT, ya que se encontró que hay picos de voltaje de entrada con valores de 135V, se requiere hacer validación con la empresa proveedora de energía ya que de lo contrario sería necesario adquirir un regulador de voltaje para corregir las alertas que está presentando la UPS. Sin novedades de esto durante el período del informe.
  - Se realizó escalamiento de la UPS de la OE Apartadó propiedad del ministerio, ya que el personal de soporte en sitio reitera que se presentan eventos sobre el equipo, el apoyo que brinda actualmente nuestro técnico es generar el reinicio correspondiente, pero en ocasiones algunos usuarios de la sede no comprenden que se encuentra fuera de nuestro alcance su reparación y atención. En julio de 2025 el Coordinador del Grupo de Soporte Informático tuvo cruce de correos con el Grupo de Recursos Físicos solicitando apoyo solventar la novedad o en su defecto, para que la dependencia responsable de este equipo pueda emitir una respuesta formal a la directora de la OE con el propósito de oficializar las acciones que se desarrollarían para esta UPS.
  - Tarjeta de red UPS OE Barrancabermeja: Luego de novedad eléctrica prolongada en la sede de la OE Barrancabermeja, se recupera el servicio y la UPS enciende de nuevo sin novedades. Sin embargo, se pierde comunicación entre la tarjeta de red de la UPS y la herramienta de monitoreo Zabbix, se reporta de inmediato al aliado para que se gestione el diagnóstico correspondiente. Se realiza sesión remota con el especialista y se adiciona esta novedad al reporte con el fabricante para ser gestionado en la misma revisión de laboratorio.

En Mayo 2026 se ejecutan las mismas acciones en la tarjeta de la UPS que se adelantaron en las UPS de Bogotá, pero no fue posible normalizar el monitoreo. Durante junio 2026, se continua el diagnóstico por parte del fabricante Ablerex y se traslada la tarjeta hasta sus

laboratorios para revisión. Para el mes de Julio 2026 nos informan que la tarjeta no superó las pruebas y requiere ser remplazada, se solicita el cambio de la parte a Ablerex.

- El 27/07/2026 se realiza configuración de la tarjeta de red de la UPS del Piso 25 Nivel Central para monitoreo por SNMP, la cual se tenía pendiente de intervenir porque estábamos a espera de disponibilidad en el despacho para acceso al centro de cableado. Se realiza actividad con éxito bajo el cambio RFC-285643 de forma exitosa, no se presenta afectación del servicio.

- **Medición de ANS Energía regulada**

A continuación, el resultado de la medición de los ANS:

ID	Indicadores	Resultado	Meta
ER-1	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
ER-2	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 104 Medición ANS Energía Eléctrica UPS

4.5 No aplica

4.6 Outsourcing de Impresión

El servicio de Outsourcing de impresión contempla los siguientes equipos distribuidos a nivel nacional para la prestación del servicio, así:

Referencia	Tipo	Cantidad
Ricoh IM430	Blanco y Negro	265
Ricoh IMC400F	Color	1

Tabla 105 Inventario de impresoras para el servicio

A continuación, se relacionan las actividades e información relevante para este servicio:

- Para el mes de julio, el responsable del servicio gestionó un total de 520 solicitudes escaladas a través de Aranda. Al corte del mes, 514 casos quedaron en estado Cerrado/Solucionado, 6 en estado Suspendido (los casos suspendidos se deben a envío de consumibles y revisión de garantía por parte del proveedor).
- Se realiza el monitoreo constante de la capacidad de almacenamiento del buzón srvscanner@mintrabajo.gov.co para asegurar que se cuente con espacio disponible o generar la depuración correspondiente para evitar novedades en la prestación del servicio; actualmente se encuentra al 32% de la capacidad total del almacenamiento (capacidad total 100gb).
- El administrador del servicio de outsourcing de impresión remitió semanalmente vía correo electrónico al Coordinador del Grupo de Soporte Informático e interesados el consolidado de consumo de clics acumulado durante el período, lo anterior con

el propósito de notificar el momento en que se supera el umbral definido de consumo establecido para el servicio.

- Se realizó la asignación de cuotas de clics de impresión de usuarios finales bajo el caso Aranda RF-258841; allí se relaciona el listado total de usuarios con el aprovisionamiento. Así mismo, se realiza monitoreo periódico de saldo de clics de usuarios para hacer asignación manual para aquellos que estén próximos a consumirlos y atención de clics por demanda en la mesa de servicios.
- El 2/07/2026 se realiza el despliegue del servicio de impresión en IPV6 donde la red de impresión de cada sede alcanza el servidor de Impresiones en protocolo IPv6, la actividad estuvo a cargo del equipo de redes y seguridad. Se realiza sin novedades para el servicio.
- El 18/07/2026 se realiza ventana de actualización de aplicativo PaperCut MF, se realiza el paso de la versión 24, a la versión 26 bajo el cambio RFC-280103, la cual resulta exitosa, se realizan pruebas de funcionalidades de impresoras con apoyo del personal de soporte sin novedades.

En la siguiente tabla se muestra el TOP 10 de usuarios que más generaron clics de impresión y fotocopiado en Blanco / Negro a nivel nacional durante el período:

Nombre de la impresora	Ubicación	Nombre de Usuario	Nombre Completo	Blanco y negro
ricohpiso23b	Bogotá sede central	lpanche	Luis Fernando Panche Chiquiza	5.488
ricohpiso23b	Bogotá sede central	rrico	Ramiro Rico Paredes	4.341
ricoh-ibague-radicacion	Tolima	jgonzalezcu	Jose Eugenio Gonzalez Cuella	2.993
ricoh-bmanga-ofc305	Bucaramanga	amateus	Andrea Johana Mateus Parra	2.906
ricohpiso19a	Bogotá sede central	pnustes	Patricia Celestial Nustes Barrera	2.765
ricoh-cali-piso3	Cali	nquinteroca	Nancy Quintero Cardozo	2.569
ricoh-guadalajara-buga-infp	Cali	vfierro	Viviana Fierro Herrera	2.515
ricoh-medellin-piso3	Medellin	gmeneses	Gloria Yanet Meneses Agudelo	2.403
ricoh-bmanga-ofc205	Bucaramanga	wmantilla	Wendy Nathalia Mantilla Torres	2.371
ricoh-apartado-2piso-c	Antioquia	mibarguen	Maria Dolores Ibarguen Torres	2.363

Tabla 106 Consumo de impresiones y copias por usuario - Impresoras B/N

TopUsuJul.xlsx

En la siguiente tabla se muestra el TOP 10 de impresoras con mayor uso:

Nombre de la impresora	Ubicación	Blanco y negro
ricohpiso23b	Bogotá Sede Central	15.627
ricohcl32-rcc	Bogotá Territorial	15.566
ricoh-cali-piso3	Cali	13.086

Nombre de la impresora	Ubicación	Blanco y negro
ricoh-cali-piso4	Cali	12.320
ricohpiso10b	Bogotá Sede Central	12.097
ricohpiso21a	Bogotá Sede Central	11.778
ricoh-bmanga-ofc303	Bucaramanga	10.839
ricohpiso12a	Bogotá Sede Central	10.298
ricoh-bmanga-ofc205	Bucaramanga	10.087
ricohpiso5a	Bogotá Sede Central	9.599

Tabla 107 Top 10 de impresoras con mayor uso



TopImpJul.xlsx

En la siguiente tabla se muestra el top de usuarios que más generaron impresiones a color durante el período:

Nombre de la impresora	Ubicación	Nombre de Usuario	Nombre Completo	Color
ricohpiso25c	Bogotá Sede Central	ymedinag	Yeisson Medina Gonzalez	2512
ricohpiso25c	Bogotá Sede Central	bhernandez	Bibiana Hernandez Hernandez	103
ricohpiso25c	Bogotá Sede Central	jrey	Julian Andres Rey Reina	21

Tabla 108 Top usuarios impresión a color



TopPiso25C.xlsx

En la siguiente tabla se muestra el Top de oficinas con mayor volumen de impresión:

Oficina	Color	Blanco y negro	Doble Cara	Páginas simples	Total, Páginas	Trabajos realizados	Promedio de Páginas por trabajo
Nivel Central	2636	150.547	112.162	41.021	153.183	41.257	248,9
D.T. Valle del Cauca	0	51.371	38.332	13.039	51.371	14.144	87,9
D.T. Santander	0	39.847	29.070	10.777	39.847	10.828	111,2
D.T. Antioquia	0	30.574	21.902	8.672	30.574	8.723	92,3
D.T. Bogotá	0	26.090	17.042	9.048	26.090	7.682	26,4
D.T. Atlantico	0	23.439	15.642	7.797	23.439	6.264	68,8
D.T. Tolima	0	18.766	12.480	6.286	18.766	4.747	77,1
D.T. Norte de Santander	0	17.837	12.666	5.171	17.837	5.129	78,8
D.T. Cundinamarca	0	17.832	11.928	5.904	17.832	4.535	103,9
OE	0	16.648	9.852	6.796	16.648	4.848	103,2

Tabla 109 Top oficinas



TopOfiJul.xlsx

En la siguiente tabla se muestra el TOP 10 de impresoras que más usan el servicio de fotocopiado:

Impresora	Ubicación	Tipo de trabajo	Copias
RICOH-GAU-B	D.T. Bogotá	COPY	2.530
RICOH-CAQUETA-PISO1-PPAL	D.T. Caqueta	COPY	1.889
RICOH-CUCUTA-P2	D.T. Norte de Santander	COPY	1.568
RICOH-MEDELLIN-PISO1	D.T. Antioquia	COPY	1.542
RICOH-BMANGA-OFC305	D.T. Santander	COPY	1.214
RICOH-LETICIA	D.T. Amazonas	COPY	1012
RICOH-QUINDIO-PISO1-ATC	D.T. Quindio	COPY	962
RICOH-MEDELLIN-PISO2-RCC	D.T. Antioquia	COPY	957
RICOH-MONTERIA-PISO2	D.T. Cordoba	COPY	811
RICOH-CALI-PISO4	D.T. Valle del Cauca	COPY	809

Tabla 110Top 10 impresoras más usadas del servicio de fotocopiado

Top_Cop_Jul.xlsx

Se indica a continuación el top de usuarios a los que más veces se les realizó ampliación de cuota de impresión en el periodo.

Nombre de Usuario	Nombre Completo	Transacción	Total, Cuota asignada	Veces que se aumento
wmantilla	Wendy Nathalia Mantilla Torres	ADJUST	3.285	7
ruribe	Rafael Uribe Agredo	ADJUST	3.201	7
asanchez	Alfonso Sanchez Carrillo	ADJUST	2.358	6
csalazara	Claudia Patricia Salazar Agudelo	ADJUST	1.680	6
evelasco	Edinson Ovidio Velasco Aguilar	ADJUST	2.500	6
hparra	Hector Julio Parra Orozco	ADJUST	2.300	6
mquinones	Maria Marleny Quinones Puerta	ADJUST	2.484	6
bdeavila	Berta Stella De Avila Fajardo	ADJUST	2.200	5
cnavas	Cesar Augusto Navas Vega	ADJUST	2.140	5
dmartinezh	Dario Jose Martinez Hoyos	ADJUST	1.600	5

Tabla 111 Ampliación de cuota de impresión

TopCuotaJul.xlsx

- Despacho de papel, tóner y unidades a nivel nacional

A continuación, se relaciona el despacho de papel que se ha gestionado por parte de la UT durante el último trimestre:

	may-26		jun-26		jul-26	
	Resmas Carta	Resmas Oficio	Resmas Carta	Resmas Oficio	Resmas Carta	Resmas Oficio
Total, Resmas	470	335	240	199	178	57
Total, Cajas por Tamaño	47,00	33,50	24,00	19,90	17,80	5,70
Total, Cajas Enviadas	**80,50**		**43,90**		**22,50**	

Tabla 112 Despacho de papel a sedes del Ministerio del Trabajo

Durante el período, se despacharon a sedes del ministerio un total de 7 toners para impresora B/N IM430 y 5 unidades de imagen.

4.6.1 No aplica

4.6.2 Multifuncional B/N rango medio – Cargo fijo mensual

Descripción	Unidad	Cantidad
Multifuncional blanco y negro rango medio - Cargo fijo mensual	Unidad-mes	265

Tabla 113Cargo mensual multifuncional rango medio

4.6.3 Impresora Color rango medio – Cargo fijo mensual

Descripción	Unidad	Cantidad
Impresora color rango medio - Cargo fijo mensual	Unidad-mes	1

Tabla 114 Cargo mensual impresora color

4.6.4 No aplica

4.6.5 Multifuncional B/N rango medio – Clic de impresión

A continuación, se detallan las cantidades de clics de impresión correspondientes al mes de julio de 2026:

MES	DETALLE	CANTIDAD
Julio	Multifuncional blanco y negro rango medio - Clic de impresión tóner y papel carta	**554.528**
	TOTAL	**554.528**

Tabla 115 Clics de impresión de julio 2026 – Multifuncional B/N

A continuación, se indica la tendencia de consumo para los últimos 3 meses:

Mes 2026	Mayo	Junio	Julio
Cantidad de clics consumidos	590.377	544.116	554.528

Tabla 116 Tendencia de consumo de clics B/N

El consumo mensual establecido para el servicio es de **450.000** clics de impresión en B/N a nivel nacional; para el período del informe se presentó un consumo de **518.376** clics de impresión (esto incluye **4.789** de la impresora de contratos piso 8) y **36.152** de fotocopias para un total de **554.528** para este servicio.

Impresora Color rango medio – Clic de impresión
A continuación, se detallan las cantidades de clics de impresión de color correspondientes al mes de julio de 2026:

MES	DETALLE	CANTIDAD
Julio	Impresora color rango medio - Cargo fijo mensual - Clic de impresión tóner y papel carta	**2.688**
	Total	**2.688**

Tabla 117 Clics de Impresión – Impresora Color

A continuación, se indica la tendencia de consumo para la vigencia 2026:

Mes	Mayo	Junio	Julio
Cantidad de clics consumidos	921	226	2688

Tabla 118Tendencia de consumo de clics color

El consumo mensual establecido para el servicio por la entidad es de **1.500** clics de impresión en color para el único equipo de este tipo ubicado en Nivel Central; para el período del informe se presentó un consumo de **2636** clics de impresión y **52** de fotocopias para un total de **2688** clics para este servicio, por lo cual no se superó dicho consumo.

- Medición de ANS Outsourcing de impresión

A continuación, el resultado de la medición de los ANS:

ID	Indicadores	Resultado	Meta
OI-1	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
OI-2	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 119 Medición ANS Outsourcing de Impresión

4.7 Antivirus

A continuación, se presenta la información relacionada con la gestión del servicio de antivirus en el Ministerio de Trabajo, donde se pueden apreciar los siguientes detalles:

4.7.1 Instalaciones de antivirus en servidores

El antivirus TrendMicro ha mostrado un rendimiento sólido en la protección de los sistemas contra amenazas informáticas, manteniendo una alta tasa de detección y neutralizando diversas formas de software malicioso y otras vulnerabilidades de seguridad.

En julio de 2026, se aseguró la cobertura de la infraestructura de servidores con antivirus activos. Estos agentes están monitoreando continuamente los eventos de seguridad que puedan presentarse.

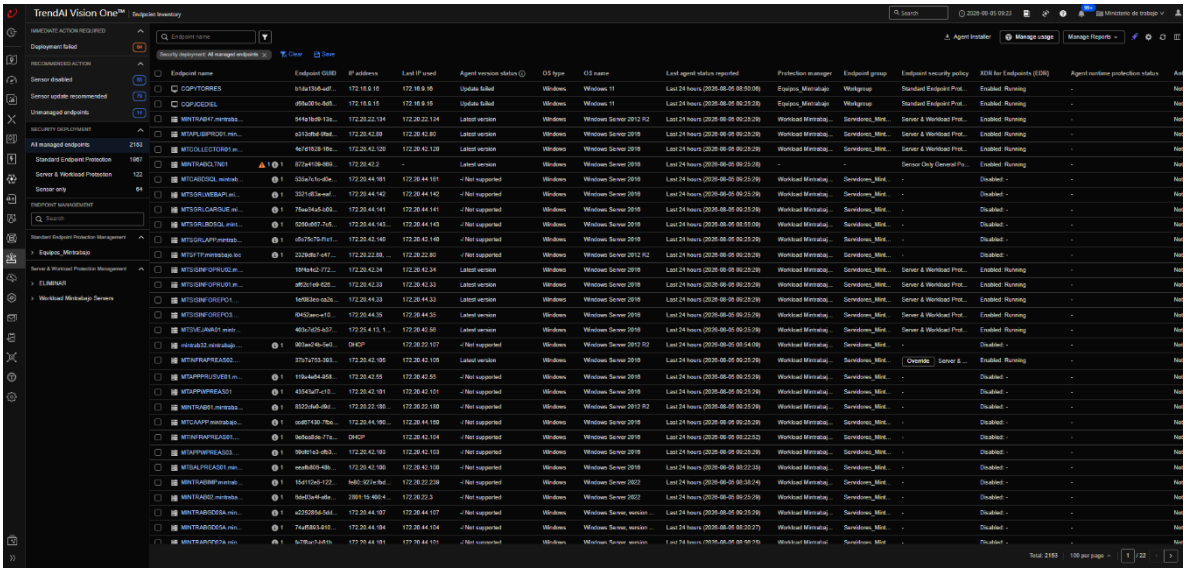


Ilustración 84 Equipos consola antivirus

4.7.2 Instalación de antivirus PCs usuarios final

Como parte de la actualización del parque computacional, se instaló el agente antivirus en los equipos de cómputo, que gestiona eficazmente los recursos, permite un monitoreo para la detección y neutralizando software malicioso y otras vulnerabilidades de seguridad.

A continuación, se evidencia la cantidad de endpoint que se encuentran instaladas en las estaciones de trabajo de los usuarios (2018) de Mintrabajo, se cuenta con 2255 licencias, se tienen disponibles 155.

Ilustración 85 Gestión consola antivirus – equipos usuario final

4.7.3 Top 10 Virus Detectados

Durante el mes analizado, los eventos detectados por la plataforma Trend Micro se detectaron un total de 63 eventos, lo que permite evaluar el grado de riesgo asociado a cada actividad observada en los Endpoint, estos fueron controlados por la herramienta haciendo con algunos de ellos el bloqueo, de otros la eliminación, y también enviando a cuarentena:

Análisis de los Datos:

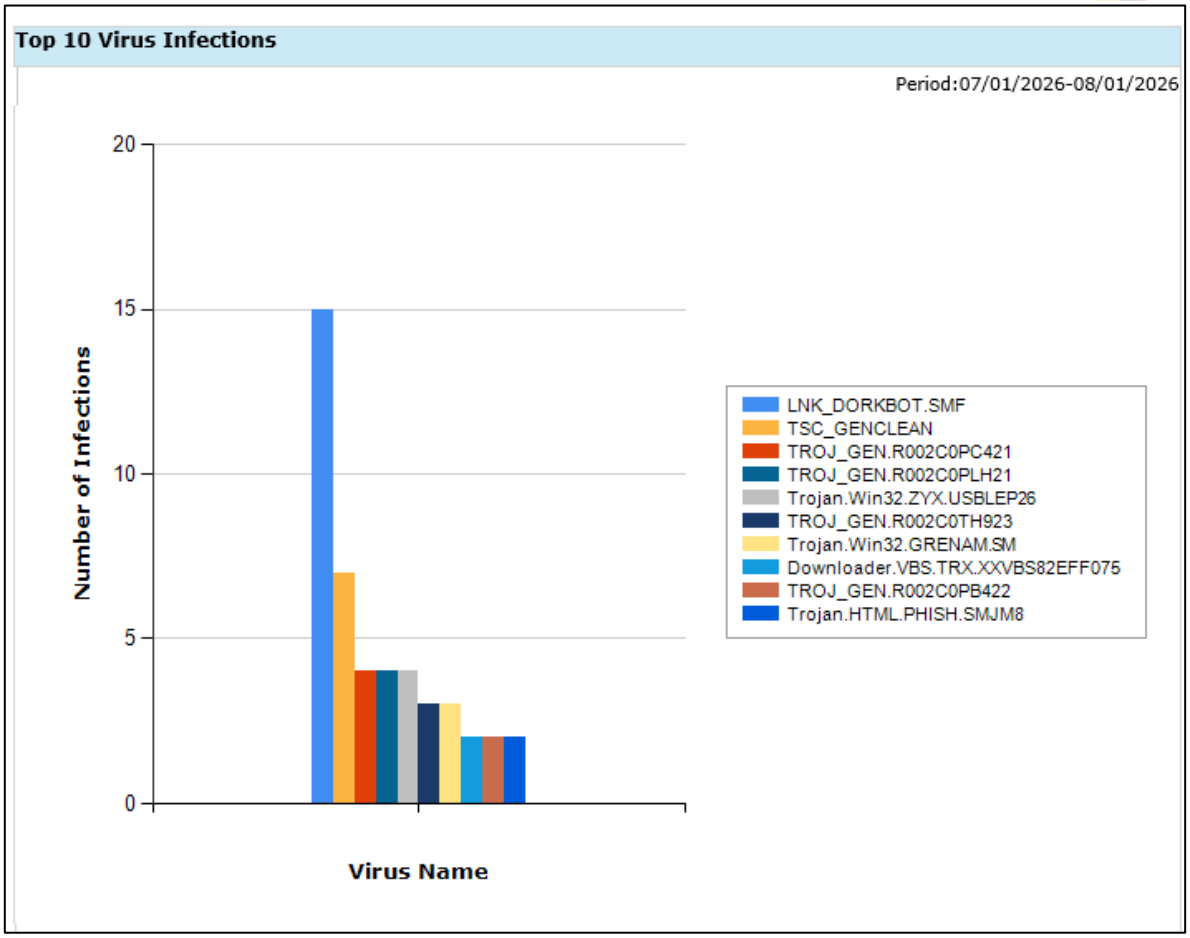


Ilustración 86 Top 10 virus detectado

Top 10 Virus Infections

Virus Name	# of Infections	Detected By
LNK_DORKBOT.SMF	15	Desktop (15)
TSC_GENCLEAN	7	Desktop (7)
TROJ_GEN.R002C0PC421	4	Desktop (4)
TROJ_GEN.R002C0PLH21	4	Desktop (4)
Trojan.Win32.ZYX.USBLEP26	4	Desktop (4)
TROJ_GEN.R002C0TH923	3	Desktop (3)
Trojan.Win32.GRENAM.SM	3	Desktop (3)
Downloader.VBS.TRX.XXVBS82EFF075	2	Desktop (2)
TROJ_GEN.R002C0PB422	2	Desktop (2)
Trojan.HTML.PHISH.SMJM8	2	Desktop (2)

Ilustración 87 Descripción de virus

Durante el período analizado, la solución de seguridad Trend Micro detectó y neutralizó múltiples eventos de malware en estaciones de trabajo institucionales. Todas las amenazas fueron contenidas de manera oportuna, sin evidencia de propagación lateral, persistencia ni impacto operativo sobre los servicios críticos.

LNK_DORKBOT.SMF: es una detección de archivos de acceso directo creados por una familia de gusanos que se propagan a través de la mensajería instantánea y las unidades extraíbles. Los archivos LNK detectados e encuentran comúnmente en unidades extraíbles y se utilizan para ejecutar un archivo ejecutable que también se encuentra en la unidad. Si el usuario intenta abrir el acceso directo, este ejecuta el gusano y abre una ventana del Explorador de archivos.

TSC_GENCLEAN: corresponde a un identificador genérico utilizado por las soluciones de Trend Micro para registrar la ejecución de su mecanismo de limpieza (Generic Clean) sobre un archivo o elemento potencialmente malicioso. Este identificador no representa una familia de malware específica, sino que indica que el motor de protección realizó acciones de remediación, tales como la limpieza, cuarentena o eliminación del objeto detectado.

TROJ_GEN.R002C0PC421: es una denominación de detección genérica de Trend Micro para archivos que presentan comportamientos sospechosos característicos de un troyano (Trojan). En las detecciones con prefijo TROJ_GEN, Trend Micro no identifica necesariamente una familia específica de malware, sino que utiliza mecanismos heurísticos y de reputación para marcar archivos potencialmente maliciosos.

TROJ_GEN.R002C0PLH21: es una detección genérica de Trend Micro para un archivo identificado como troyano (Trojan) o con comportamiento potencialmente malicioso. El prefijo TROJ_GEN indica que la detección se basa en análisis heurísticos, reputación o comportamientos sospechosos, y no necesariamente en una familia específica de malware. Trojan.Win32.ZYX.USBLEP26: es una detección genérica de Trend Micro para archivos de Windows que presentan características compatibles con un troyano. El prefijo ZYX corresponde a la nomenclatura interna de Trend Micro para clasificar variantes genéricas, mientras que USBLEP26 identifica una firma específica dentro de esa categoría. A diferencia de una familia de malware conocida (como Emotet o QakBot), esta detección no identifica un malware concreto, sino un archivo cuyo comportamiento o estructura coincide con patrones maliciosos.

TOP 5 EQUIPOS

A continuación, se genera un top 5 de las amenazas durante el mes de julio 2026:

HOST	Cantidad	Virus/malware
CNDLPENA	18	LNK_DORKBOT.SMF, Trojan.LNK.RETADUP.SMF, TSPY_PASSTEAL.UGR
BODHARIAST	13	TROJ_FRS.VSNTIM25, TROJ_GEN.R002C0PB422, TROJ_GEN.R002C0PLH21, TROJ_GEN.R002C0RFN23, TROJ_GEN.R002C0RKM24,Trojan.Win32.ZYX.USBLEU26, Trojan.Win32.ZYX.USBLF526, Trojan.Win32.ZYX.USBLFC26
URPMMUSKUS	7	Downloader.VBS.TRX.XXVBS82EFF075, TSC_GENCLEAN

CQDXBETANCOURTH	6	TROJ_GEN.R002C0DGQ21, TROJ_GEN.R002C0TH923, Trojan.HTML.PHISH.SMJM8
BOPCBOGOTA3	4	TROJ_GEN.R002C0PC421

Tabla 120 Top 5 Equipos

CNDLPENA

En el equipo se registran 18 principalmente asociadas a la amenaza reconocida como LNK_DORKBOT.SMF que corresponde a detecciones de archivos con extensión LNK detectados e encuentran comúnmente en unidades extraíbles y se utilizan para ejecutar un archivo ejecutable que también se encuentra en la unidad. Si el usuario intenta abrir el acceso directo, este ejecuta el gusano y abre una ventana del Explorador de archivos.

Generated	Received	Product Entity/E...	Product	Product/Endpoin...	Product/Endpoin...	Managing Serve...	Domain	Rule ID	Virus/Malware
07/23/2026 12:44:...	07/23/2026 12:46:...	CNDLPENA	Apex One	172.16.15.11	88-AE-DD-91-C3-6B	Windows	Workgroup	LNK_DORKBOT.SMF	LNK_DORKBOT.SMF
07/24/2026 10:14:...	07/24/2026 10:15:...	CNDLPENA	Apex One	172.16.15.11	88-AE-DD-91-C3-6B	Windows	Workgroup	LNK_DORKBOT.SMF	LNK_DORKBOT.SMF
07/24/2026 16:29:...	07/24/2026 16:31:...	CNDLPENA	Apex One	172.16.15.11	88-AE-DD-91-C3-6B	Windows	Workgroup	LNK_DORKBOT.SMF	LNK_DORKBOT.SMF
07/24/2026 16:29:...	07/24/2026 16:31:...	CNDLPENA	Apex One	172.16.15.11	88-AE-DD-91-C3-6B	Windows	Workgroup	LNK_DORKBOT.SMF	LNK_DORKBOT.SMF
07/24/2026 16:29:...	07/24/2026 16:31:...	CNDLPENA	Apex One	172.16.15.11	88-AE-DD-91-C3-6B	Windows	Workgroup	LNK_DORKBOT.SMF	LNK_DORKBOT.SMF
07/24/2026 16:29:...	07/24/2026 16:31:...	CNDLPENA	Apex One	172.16.15.11	88-AE-DD-91-C3-6B	Windows	Workgroup	LNK_DORKBOT.SMF	LNK_DORKBOT.SMF
07/24/2026 16:29:...	07/24/2026 16:31:...	CNDLPENA	Apex One	172.16.15.11	88-AE-DD-91-C3-6B	Windows	Workgroup	LNK_DORKBOT.SMF	LNK_DORKBOT.SMF
07/24/2026 16:29:...	07/24/2026 16:31:...	CNDLPENA	Apex One	172.16.15.11	88-AE-DD-91-C3-6B	Windows	Workgroup	LNK_DORKBOT.SMF	LNK_DORKBOT.SMF
07/24/2026 16:29:...	07/24/2026 16:31:...	CNDLPENA	Apex One	172.16.15.11	88-AE-DD-91-C3-6B	Windows	Workgroup	LNK_DORKBOT.SMF	LNK_DORKBOT.SMF

Ilustración 88 CNDLPENA

BODHARIAST

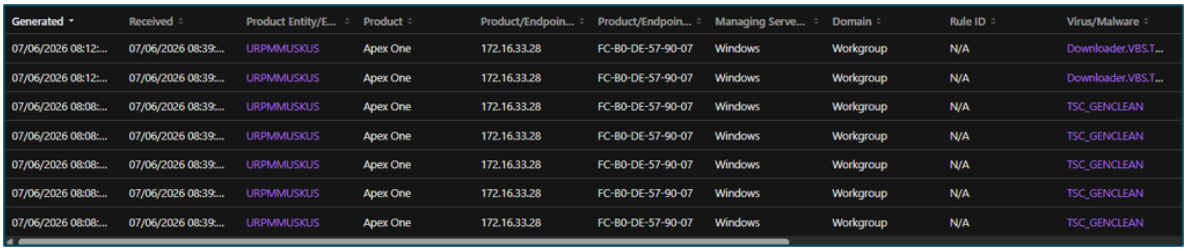
En el equipo se registran 13 detecciones asociadas a las amenazas reconocidas como Troyanos de tipo Generico los archivos fueron eliminados de manera correcta por parte del antivirus. Adicional el equipo y no fue necesario ejecutar acciones adicionales en el equipo.

Generated	Received	Product Entity/E...	Product	Product/Endpoin...	Product/Endpoin...	Managing Serve...	Domain	Rule ID	Virus/Malware	Endpoint Infecti...	Policy Name
07/17/2026 17:06:...	07/17/2026 17:07:...	BODHARIAST	Apex One	172.16.50.24	88-AE-DD-96-29-17	Windows	Workgroup	TROJ_FRS.VSNTIM...	TROJ_FRS.VSNTIM...	Local or network d...	USB Permitido
07/17/2026 17:02:...	07/17/2026 17:02:...	BODHARIAST	Apex One	172.16.50.24	88-AE-DD-96-29-17	Windows	Workgroup	TROJ_GEN.R002C0...	TROJ_GEN.R002C0...	Local or network d...	USB Permitido
07/17/2026 17:04:...	07/17/2026 17:04:...	BODHARIAST	Apex One	172.16.50.24	88-AE-DD-96-29-17	Windows	Workgroup	TROJ_GEN.R002C0...	TROJ_GEN.R002C0...	Local or network d...	USB Permitido
07/17/2026 17:04:...	07/17/2026 17:04:...	BODHARIAST	Apex One	172.16.50.24	88-AE-DD-96-29-17	Windows	Workgroup	TROJ_GEN.R002C0...	TROJ_GEN.R002C0...	Local or network d...	USB Permitido
07/17/2026 17:02:...	07/17/2026 17:02:...	BODHARIAST	Apex One	172.16.50.24	88-AE-DD-96-29-17	Windows	Workgroup	TROJ_GEN.R002C0...	TROJ_GEN.R002C0...	Local or network d...	USB Permitido
07/17/2026 17:04:...	07/17/2026 17:04:...	BODHARIAST	Apex One	172.16.50.24	88-AE-DD-96-29-17	Windows	Workgroup	TROJ_GEN.R002C0...	TROJ_GEN.R002C0...	Local or network d...	USB Permitido
07/17/2026 17:02:...	07/17/2026 17:02:...	BODHARIAST	Apex One	172.16.50.24	88-AE-DD-96-29-17	Windows	Workgroup	TROJ_GEN.R002C0...	TROJ_GEN.R002C0...	Local or network d...	USB Permitido
07/17/2026 17:01:...	07/17/2026 17:02:...	BODHARIAST	Apex One	172.16.50.24	88-AE-DD-96-29-17	Windows	Workgroup	TROJ_GEN.R002C0...	TROJ_GEN.R002C0...	Local or network d...	USB Permitido
07/17/2026 17:08:...	07/17/2026 17:08:...	BODHARIAST	Apex One	172.16.50.24	88-AE-DD-96-29-17	Windows	Workgroup	TROJ_GEN.R002C0...	TROJ_GEN.R002C0...	Local or network d...	USB Permitido
07/17/2026 17:01:...	07/17/2026 17:02:...	BODHARIAST	Apex One	172.16.50.24	88-AE-DD-96-29-17	Windows	Workgroup	Trojan.Win32.ZYX....	Trojan.Win32.ZYX....	Local or network d...	USB Permitido
07/17/2026 16:58:...	07/17/2026 16:58:...	BODHARIAST	Apex One	172.16.50.24	88-AE-DD-96-29-17	Windows	Workgroup	Trojan.Win32.ZYX....	Trojan.Win32.ZYX....	Local or network d...	USB Permitido
07/17/2026 16:58:...	07/17/2026 16:59:...	BODHARIAST	Apex One	172.16.50.24	88-AE-DD-96-29-17	Windows	Workgroup	Trojan.Win32.ZYX....	Trojan.Win32.ZYX....	Local or network d...	USB Permitido
07/17/2026 17:05:...	07/17/2026 17:05:...	BODHARIAST	Apex One	172.16.50.24	88-AE-DD-96-29-17	Windows	Workgroup	Trojan.Win32.ZYX....	Trojan.Win32.ZYX....	Local or network d...	USB Permitido

Ilustración 89 BODHARIAST

URPMMUSKUS

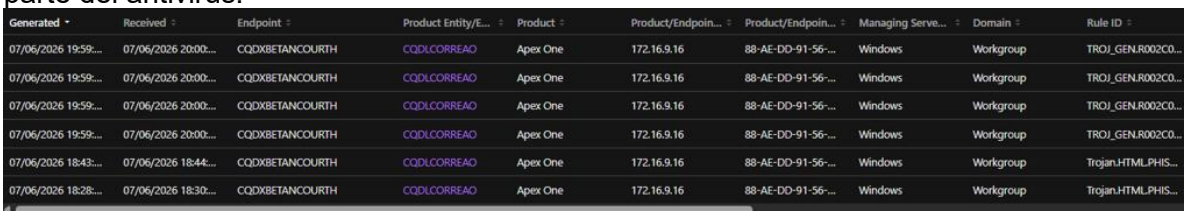
En el equipo se reportan 7 detecciones de la amenaza de una amenaza denominada TSC_GENCLEAN y Downloader.VBS.TRX.XXVBS82EFF075 los archivos fueron eliminados y controlados de manera correcta por parte del antivirus.



Generated	Received	Product Entity/E...	Product	Product/Endpoin...	Product/Endpoin...	Managing Serve...	Domain	Rule ID	Virus/Malware
07/06/2026 08:12:...	07/06/2026 08:39:...	URPMMUSKUS	Apex One	172.16.33.28	FC-B0-DE-57-90-07	Windows	Workgroup	N/A	Downloader.VBS.T...
07/06/2026 08:12:...	07/06/2026 08:39:...	URPMMUSKUS	Apex One	172.16.33.28	FC-B0-DE-57-90-07	Windows	Workgroup	N/A	Downloader.VBS.T...
07/06/2026 08:08:...	07/06/2026 08:39:...	URPMMUSKUS	Apex One	172.16.33.28	FC-B0-DE-57-90-07	Windows	Workgroup	N/A	TSC_GENCLEAN
07/06/2026 08:08:...	07/06/2026 08:39:...	URPMMUSKUS	Apex One	172.16.33.28	FC-B0-DE-57-90-07	Windows	Workgroup	N/A	TSC_GENCLEAN
07/06/2026 08:08:...	07/06/2026 08:39:...	URPMMUSKUS	Apex One	172.16.33.28	FC-B0-DE-57-90-07	Windows	Workgroup	N/A	TSC_GENCLEAN
07/06/2026 08:08:...	07/06/2026 08:39:...	URPMMUSKUS	Apex One	172.16.33.28	FC-B0-DE-57-90-07	Windows	Workgroup	N/A	TSC_GENCLEAN
07/06/2026 08:08:...	07/06/2026 08:39:...	URPMMUSKUS	Apex One	172.16.33.28	FC-B0-DE-57-90-07	Windows	Workgroup	N/A	TSC_GENCLEAN

Ilustración 90 URPMMUSKUS

CQDXBETANCOURTH
En el equipo se reportan 3 detecciones de la amenaza de una amenaza denominada Mal_Nemucod-JS33 los archivos fueron eliminados y controlados de manera correcta por parte del antivirus.



Generated	Received	Endpoint	Product Entity/E...	Product	Product/Endpoin...	Product/Endpoin...	Managing Serve...	Domain	Rule ID
07/06/2026 19:59:...	07/06/2026 20:00:...	CQDXBETANCOURTH	CQDLCORREAO	Apex One	172.16.9.16	88-AE-DD-91-56-...	Windows	Workgroup	TROJ_GEN.R002C0...
07/06/2026 19:59:...	07/06/2026 20:00:...	CQDXBETANCOURTH	CQDLCORREAO	Apex One	172.16.9.16	88-AE-DD-91-56-...	Windows	Workgroup	TROJ_GEN.R002C0...
07/06/2026 19:59:...	07/06/2026 20:00:...	CQDXBETANCOURTH	CQDLCORREAO	Apex One	172.16.9.16	88-AE-DD-91-56-...	Windows	Workgroup	TROJ_GEN.R002C0...
07/06/2026 19:59:...	07/06/2026 20:00:...	CQDXBETANCOURTH	CQDLCORREAO	Apex One	172.16.9.16	88-AE-DD-91-56-...	Windows	Workgroup	TROJ_GEN.R002C0...
07/06/2026 18:43:...	07/06/2026 18:44:...	CQDXBETANCOURTH	CQDLCORREAO	Apex One	172.16.9.16	88-AE-DD-91-56-...	Windows	Workgroup	Trojan.HTML.PHIS...
07/06/2026 18:28:...	07/06/2026 18:30:...	CQDXBETANCOURTH	CQDLCORREAO	Apex One	172.16.9.16	88-AE-DD-91-56-...	Windows	Workgroup	Trojan.HTML.PHIS...

Ilustración 91 CQDXBETANCOURTH

4.7.4 Servicio de Vulnerabilidades

A continuación, se muestra un resumen de los resultados, actividades y procesos relacionados al servicio de gestión de vulnerabilidades, que han sido llevadas a cabo durante el mes de julio 2026 sobre la infraestructura tecnológica registrada del Ministerio de Trabajo, con el objetivo de identificar los hallazgos a nivel de vulnerabilidades que pueden alterar el nivel de exposición cibernética del negocio.

Se informó que el equipo de infraestructura comenzará de inmediato a elaborar un plan de trabajo para remediar estas vulnerabilidades. Asimismo, se acordó enviar un informe detallado de las vulnerabilidades encontradas al Ingeniero Luis Guerra.

Se informó al Ministerio de trabajo y equipo infraestructura que se procede con la primera fase de la **Prueba de Vulnerabilidades** del **primer semestre de 2026** para el proyecto Ministerio del Trabajo, de acuerdo con el cronograma de ejecución propuesto.

Plan de acción y remediación de vulnerabilidades
Priorización: Priorizar las vulnerabilidades críticas y de alta severidad para su remediación inmediata. Automatización: Considerar el uso de herramientas de gestión de parches automatizadas para agilizar el proceso en cual se está implementado un WSUS.
Validación: Realizar pruebas exhaustivas antes de implementar parches en entornos de producción.

4.7.4.1 Inventario y licenciamiento

El inventario de activos registrado en la herramienta Tenable Nessus Professional, se basa en la priorización y selección de aquellos activos que son críticos o core

del negocio para el Ministerio del Trabajo y los resultados del escaneo “TCP Discovery” inicial, con el fin de validar el alcance desde el servidor Nessus. Al cierre de julio del 2026 se tienen registrados 345 activos TI, de los cuales, se registró un alcance sobre 319 (92%) activos.

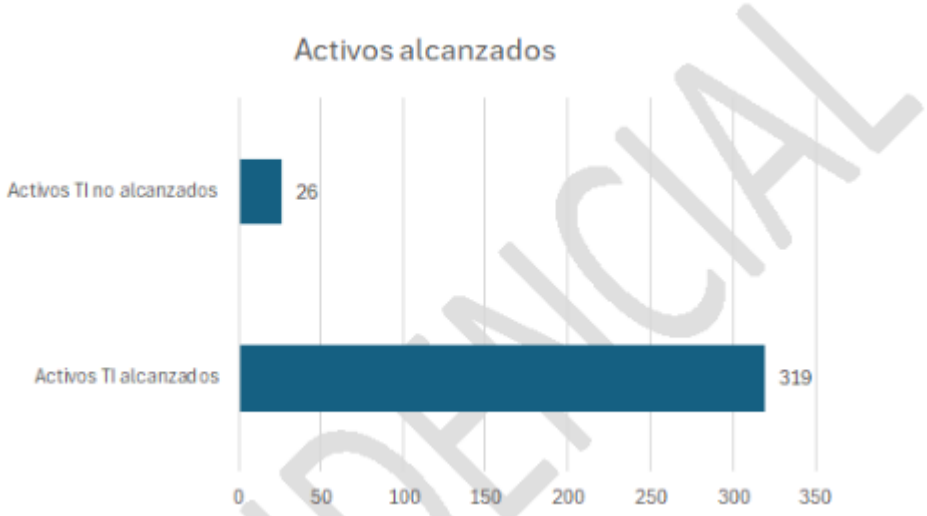


Ilustración 92 *Gestión consola Nessus*

4.7.4.2 Escaneos programados

La programación de los escaneos de vulnerabilidades se viene realizando mensualmente el último fin de semana de cada mes, acorde a las obligaciones contractuales definidas entre las dos partes; generando los reportes a través de la plataforma de Tenable Nessus Professional. La segmentación que se tiene para la infraestructura del Ministerio de Trabajo corresponde a:

MINTRABAJO MENSUAL – WINDOWS SERVER.
MINTRABAJO MENSUAL – FORTINET.
MINTRABAJO MENSUAL – WINDOWS DESKTOP.
MINTRABAJO MENSUAL – VMWARE.
MINTRABAJO MENSUAL – NETWORKING.
MINTRABAJO MENSUAL – FORTISIEM.
MINTRABAJO MENSUAL – LINUX. Rtinet.

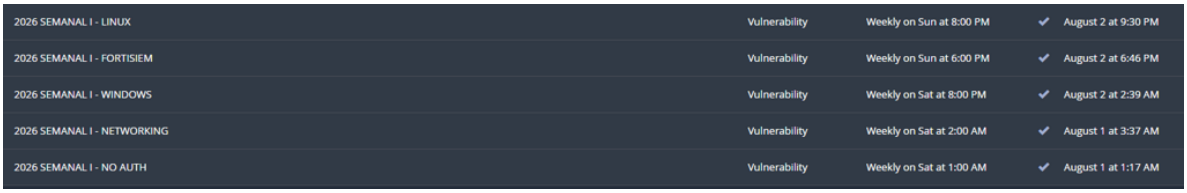


Ilustración 93 *Escaneos programados*

Clasificación de Prioridad de Vulnerabilidad por Instancias Totales (VPR)
La plataforma Tenable io calcula un VPR (Vulnerability Priority Rating) dinámico para la mayoría de las vulnerabilidades. El VPR es un complemento dinámico de los datos

proporcionados por la puntuación CVSS de la vulnerabilidad, ya que Tenable actualiza el VPR para reflejar el panorama de amenazas actual a nivel mundial. Los valores de VPR oscilan entre 0,1 y 10; un valor más alto representa una mayor probabilidad de explotación.

- Rating 9.0-10 (Critico).
- Rating 7.0-8.9 (Alto).
- Rating 4.0-6.9 (Medio).
- Rating 0-3.9 (Bajo).

4.7.4.3 TOP 10 – Vulnerabilidades más explotables

Al cierre de julio del 2026, el activo TI con la mayor cantidad de vulnerabilidades identificadas corresponde al host (172.20.22.188), con un total de 2.428 hallazgos, corresponde a un servidor Red Hat Enterprise Linux Server release 7.9 (Maipo) y la mayoría de las vulnerabilidades están asociadas a Unpatched, es decir, son actualizaciones de paquetes pendientes que no se pueden desplegar debido a que el proveedor no las ha autorizado en los repositorios originales de Red Hat.

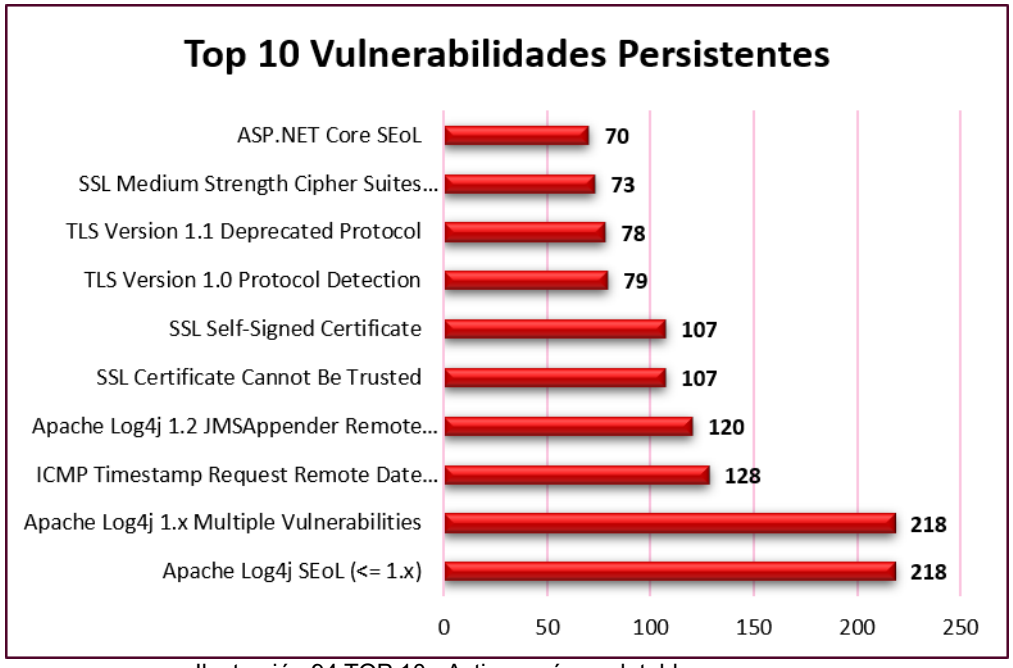


Ilustración 94 TOP 10 - Activos más explotables

Al cierre de julio del 2026, la vulnerabilidad identificada con la mayor cantidad de persistencias corresponde a (Apache Log4j SEoL (<= 1.x)), con un total de 218 hallazgos, consiste en un tipo de paquete ICMP, específicamente tipo 13 y 14, los cuales le permiten a un ciberdelincuente conocer la fecha y hora del dispositivo que responde a la solicitud.

4.7.4.4 Estrategia de remediación y/o mitigación

La estrategia de remediación de vulnerabilidades implementada en MINTRABAJO consiste en priorizar las vulnerabilidades según la criticidad; y definir fechas contempladas para cerrarlas. Por lo que las fechas corresponden a:

- Vulnerabilidades Criticas: sobre estas vulnerabilidades se enfocará la mayoría de los esfuerzos para una rápida mitigación.
- Vulnerabilidades Altas – Se trabajarán en conjunto con la vulnerabilidad críticas, pero estas tendrán una menor criticidad en la mitigación.
- Vulnerabilidades Medias y bajas – Estas vulnerabilidades se trabajar a un periodo más amplio debido a que no tienen un impacto critico o alto en la operación.

Para cumplir con la estrategia de remediación, se programan sesiones semanales con el equipo resolutor (Windows, Linux y Oracle) con el objetivo de validar los avances en la remediación. Sin embargo, dado que estas fechas son planificadas, es posible que algunas vulnerabilidades se extiendan más allá de lo previsto. En estos casos, se documentarán las vulnerabilidades extendidas junto con una justificación detallada del retraso.

4.7.4.5 Resumen de mitigación efectuada

A continuación, se contrasta un resumen de las actividades relacionas con la gestión de vulnerabilidades correspondientes al Snapshot del semestre I 2026, el cual reportó un total de 4.343 vulnerabilidades TI en las severidades:

- 974 vulnerabilidades críticas.
- 1.691 vulnerabilidades altas.
- 1.965 vulnerabilidades medias.
- 370 vulnerabilidades bajas.

Durante el periodo de julio del 2026, se remediaron un total de **38 vulnerabilidades**, de las cuales, 3 fueron de severidad crítica, 23 de severidad alta, 9 de severidad media y 3 de severidad baja. Por otro lado, con relación a **indicadores semestrales**, se gestionaron un total de **38 vulnerabilidades**, de las cuales, 3 fueron de severidad crítica, 23 de severidad alta, 9 de severidad media y 3 de severidad baja

.

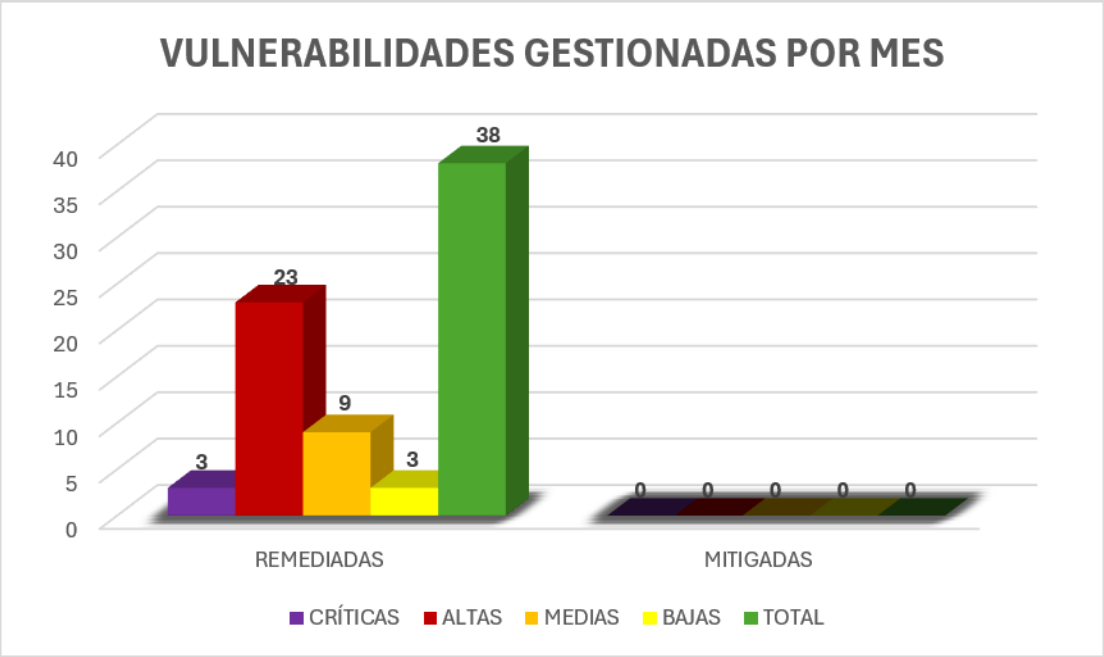


Ilustración 95 Vulnerabilidades gestionadas vs en remediación

Ethical Hacking del **primer semestre 2026**

Se informa la finalización satisfactoria de todas las fases del Ethical Hacking correspondiente al primer semestre de 2026 para el proyecto del Ministerio del Trabajo, alcanzando un 100 % de ejecución de las actividades definidas en el cronograma.

Durante el desarrollo del ejercicio se completaron satisfactoriamente las siguientes fases:

- Levantamiento de información: 100 %.
- Planeación de la prueba: 100 %.
- Ejecución de las pruebas de Ethical Hacking: 100 %.
- Documentación y elaboración del informe de resultados: 100 %.
- Presentación y socialización de resultados: 100 %.

Como resultado, el ejercicio de Ethical Hacking se encuentra completamente finalizado, incluyendo la validación del alcance, la ejecución de las pruebas de seguridad sobre los activos definidos, el análisis y documentación de los hallazgos identificados y la presentación de los resultados obtenidos.

De esta manera, se da por cumplido el cronograma de ejecución y cerrado el ciclocompleto de la actividad de Ethical Hacking del primer semestre de 2026, quedando como etapa posterior el seguimiento a los planes de acción y a la remediación de los hallazgos identificados.

FASE	RIESGO	RESPONSABLE	PROGRESO	FECHA INICIO	FECHA FIN	DÍAS
Levantamiento de Información	Bajo	Delgado Triana, Hector Alexander	100%	Marzo 30, 2026	Abril 1, 2026	3
Planeación de la Prueba	Bajo	Delgado Triana, Hector Alexander	100%	Abril 6, 2026	Abril 24, 2026	15
Ejecución de la Prueba	Alto	Delgado Triana, Hector Alexander	100%	Junio 2, 2026	Junio 17, 2026	9
Documentación	Medio	Delgado Triana, Hector Alexander	100%	Junio 18, 2026	Julio 01, 2026	9
Presentación de Resultados	Bajo	Delgado Triana, Hector Alexander	100%	Julio 02, 2026	Julio 10, 2026	5

Ilustración 96 revisión configuraciones

Anexo Vulnerabilidades

Se anexa informe detallado de la gestión de vulnerabilidades, y Export de las vulnerabilidades encontradas sobre la infraestructura.

Dando cumplimiento al reporte mensual de vulnerabilidades, se realizó envió a la Coordinador del Grupo de Soporte Informático, el informe de vulnerabilidades correspondiente al mes de julio 2027, se adjunta informe socializado.

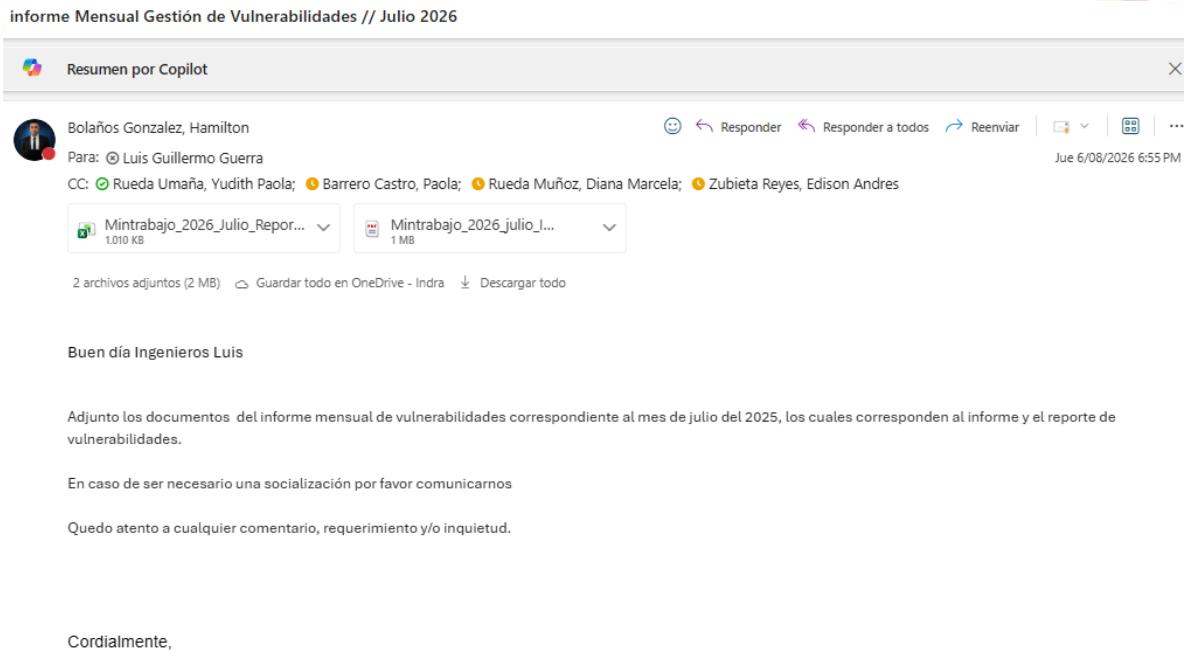


Ilustración 97 captura envío de correo gestión de vulnerabilidades

- Medición de ANS Antivirus

A continuación, el resultado de la medición de los ANS:

ID	Indicadores	Resultado	Meta
AV-1	Cobertura de antivirus	98,27%	95,00%
AV-2	Continuidad y disponibilidad de la plataforma	100,00%	98,00%
AV-3	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 121 Medición de ANS Antivirus

5 GESTIÓN DE CALIDAD DE INFORMACIÓN

Este apartado tiene el propósito de brindar la información de las evaluaciones de la calidad documental de los casos y la calidad de las llamadas realizadas al personal de Mesa de Servicios, Soporte en Sitio y Especialistas, con el propósito de identificar acciones de mejora en la prestación de los servicios:

- Calidad documental de Casos: Realizando la revisión y cumplimiento de los criterios definidos en la calidad documental de los casos registrados en la herramienta de gestión.
- Calidad de Llamadas: Realizando la revisión y cumplimiento de los criterios definidos en los casos atendidos por el centro de servicio por medio de llamadas telefónicas.

A continuación, se detalla la metodología utilizada para la realización de las evaluaciones:

5.1 Evaluación calidad documental de casos

En el mes se realizó la evaluación cuantitativa de la muestra de 275 casos documentados en la Herramienta de Gestión.

Para el cálculo Calidad Documental de Casos, se tienen en cuenta el número de criterios cumplidos Vs el número total de criterios, aplicando el peso porcentual para cada criterio.

Para esto, se evalúan por cada caso, los 13 criterios definidos, obteniendo el siguiente resultado:

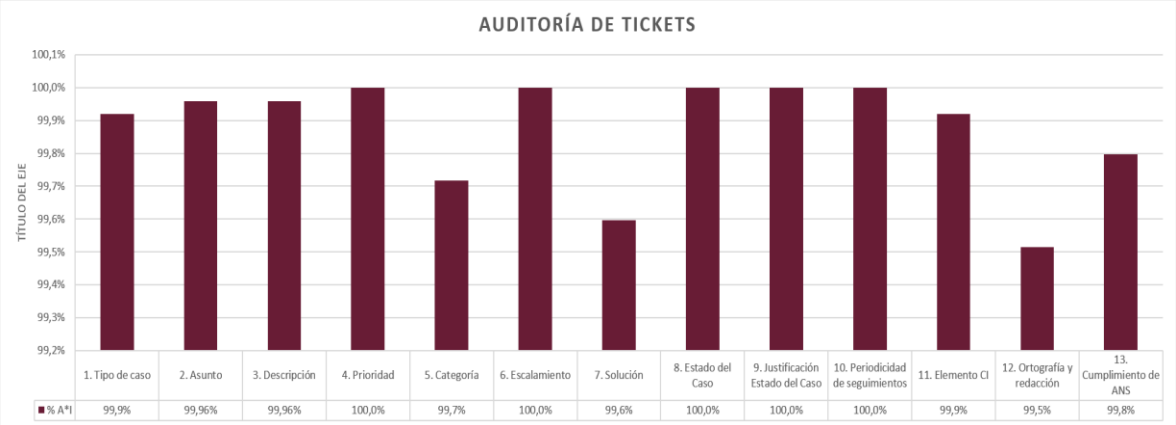


Ilustración 98 Resultado General

Durante el período evaluado, la calidad documental de los casos registró un desempeño superior al 98,39% en todos los criterios auditados, evidenciando un alto nivel de cumplimiento en el diligenciamiento de la información por parte de los equipos de soporte.

Los criterios Prioridad, Estado del Caso, Justificación del Estado y escalamiento alcanzaron un cumplimiento del 100%, lo que demuestra consistencia en la clasificación de los casos, el adecuado registro de su estado y la calidad en la documentación.

Las principales oportunidades de mejora se identificaron en el criterio Ortografía y redacción, el cual presentó 12 hallazgos, alcanzando un cumplimiento del 99,5%. Esto evidencia la necesidad de fortalecer la correcta redacción y revisión de la ortografía al solucionar los tickets.

De igual forma, se identificaron observaciones en los criterios Categoría y Solución, con 7 y 10 hallazgos, respectivamente, reflejando oportunidades para reforzar la adecuada clasificación de los casos y el nivel de detalle de las actividades ejecutadas para su resolución. También se presentaron hallazgos menores en Tipo de caso (2), Descripción (1), Asunto (1), Cumplimiento de ANS (5) y Elemento CI (2), los cuales representan desviaciones puntuales frente al total de registros evaluados.

En términos generales, los resultados evidencian un adecuado nivel de calidad documental, manteniendo indicadores superiores al 98,38% en la mayoría de los criterios evaluados. No obstante, se continuará con las actividades de retroalimentación y seguimiento orientadas a fortalecer los criterios mayor afectación, la correcta categorización de los casos y la documentación de las soluciones implementadas, con el propósito de mantener la confiabilidad y consistencia de la información registrada en la herramienta de gestión.

5.2 Evaluación de calidad de llamadas

Durante el mes se realizó la evaluación cuantitativa de una muestra de llamadas con una duración superior a 1 minuto y 30 segundos. Para esta medición se evaluaron 21 llamadas, considerando los criterios definidos para el proceso de aseguramiento de la calidad.

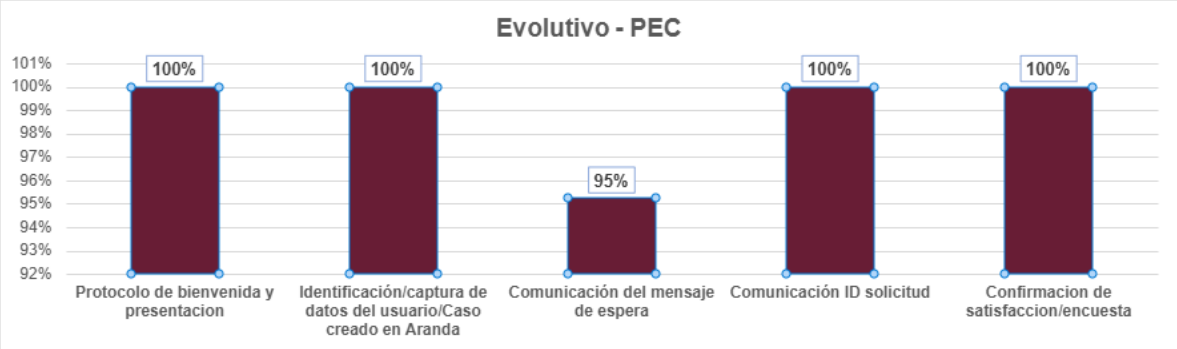


Ilustración 99 Resultado de criterios y parámetros - Calidad de llamadas

Adicionalmente, durante el período se efectuaron 21 monitoreos de calidad sobre las llamadas gestionadas en la operación. Como resultado, se obtuvo un cumplimiento del 99%

- Protocolo de bienvenida y presentación.
- Identificación y captura de datos del usuario.
- Comunicación del mensaje de espera.
- Comunicación del ID de la solicitud.
- Confirmación de satisfacción y aplicación de encuesta.

Estos resultados evidencian un cumplimiento integral de los lineamientos establecidos para la atención de los usuarios, reflejando una adecuada aplicación de los protocolos de servicio, una comunicación clara y efectiva durante las interacciones y un correcto cierre de las llamadas. En términos generales, la operación mantuvo un desempeño sobresaliente en la calidad de la atención telefónica, consolidando el compromiso del equipo con la prestación de un servicio oportuno, estandarizado y orientado a la satisfacción del usuario.

5.3 Práctica de Mejora

En este apartado se presentan las actividades desarrolladas en el marco de la Práctica de Mejora Continua durante el mes de julio de 2026. Asimismo, se consolidan las acciones de mejora identificadas por los Servicios TIC y las Prácticas ITIL, orientadas al fortalecimiento y optimización continua de la gestión de los servicios.

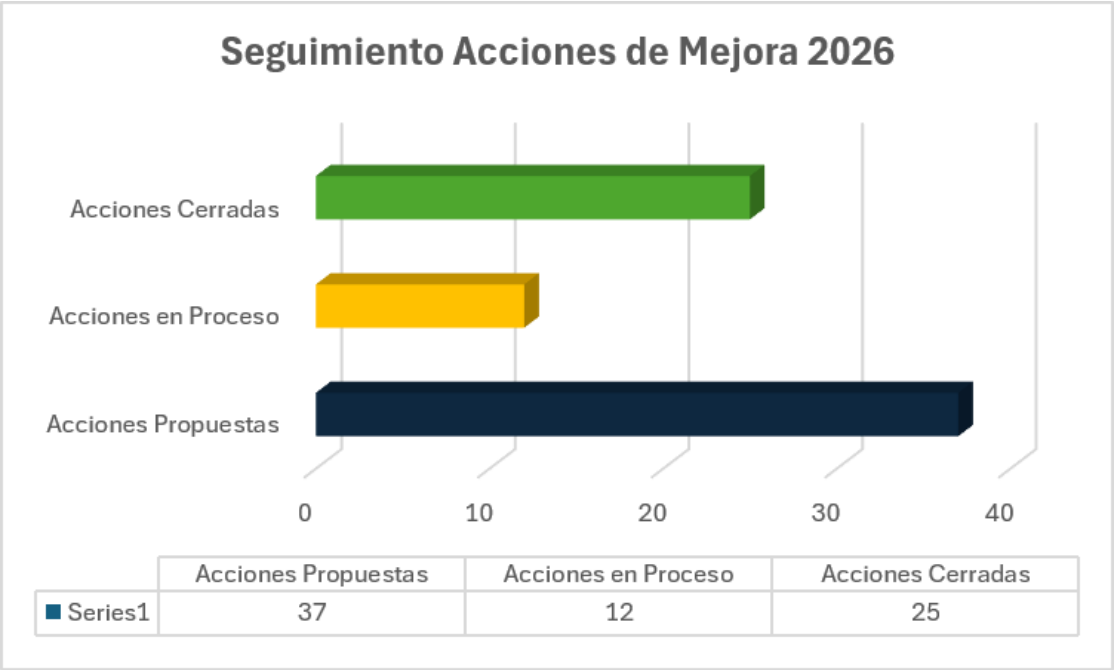


Ilustración 100 Seguimiento Práctica Mejora

En la gráfica anterior se observa el seguimiento a las acciones de mejora identificadas durante 2026. Al corte del 31 de julio de 2026, de un total de 37 acciones de mejora, 25 se encuentran cerradas, lo que representa un avance del 67,57 %, respaldadas con las evidencias entregadas por los responsables de cada acción. Las 12 acciones restantes continúan en proceso de implementación, conforme al plan de trabajo establecido.

Durante el inicio de la Práctica de Mejora se realizaron diferentes actividades de socialización y capacitación con el propósito de establecer mecanismos para la identificación, registro y participación de los diferentes Servicios TIC en la gestión de las acciones de mejora. Como resultado, se definió el siguiente indicador para medir el cumplimiento de las acciones propuestas, con una periodicidad **trimestral**.

Nombre	Fórmula	Meta	Periodicidad
Cumplimiento de las fechas previstas de las acciones de mejora registradas	**IMP**: Implementación de Mejoras de ITIL de servicios/gestiones	>= 70%	Trimestral
	AMI: Cantidad de Acciones ejecutadas en el periodo.		
	TAM: Total de Acciones planificadas para el período.		

Tabla 122 KPI Practica de Mejora

La última medición del indicador corresponde al trimestre comprendido entre abril y junio de 2026, cuyos resultados se presentan a continuación.

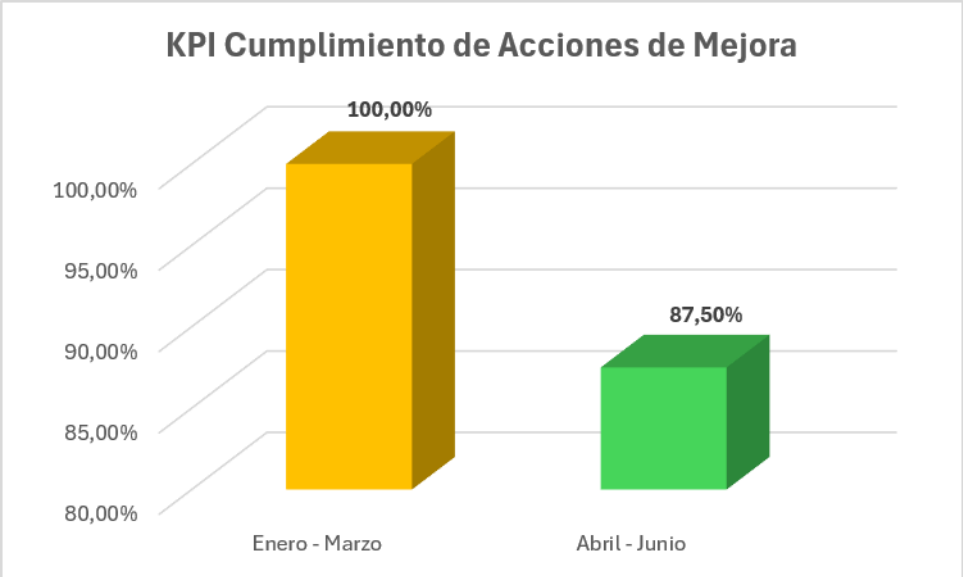
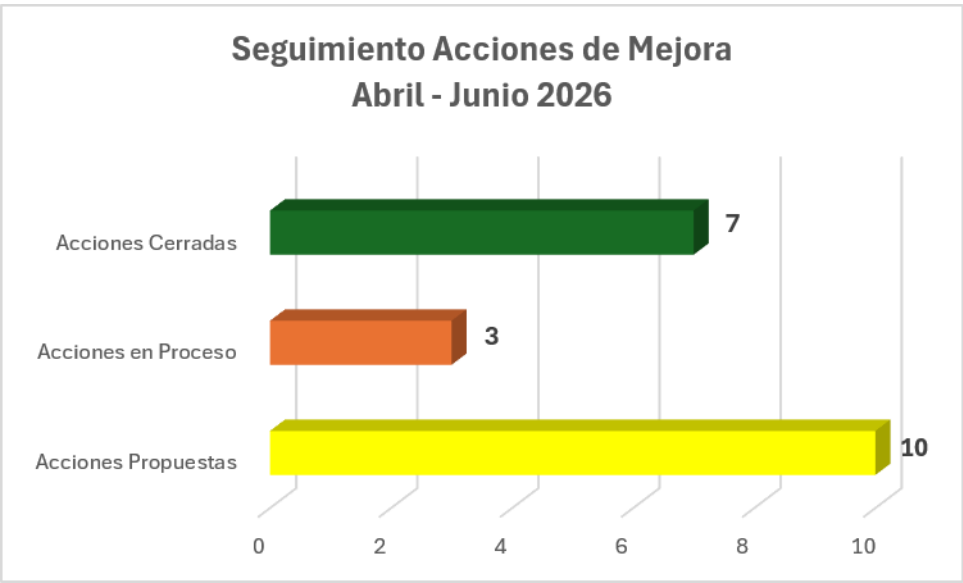


Ilustración 101 Resultado de Cumplimiento AM

Durante este período se realizó el seguimiento a 10 acciones de mejora, de las cuales 7 fueron ejecutadas y 3 quedaron pendientes, alcanzando un cumplimiento del 87,5 %. Este resultado evidencia una adecuada gestión y seguimiento de las actividades de mejora, reflejando el compromiso de los equipos responsables en la ejecución de las acciones definidas para fortalecer la prestación del servicio y promover la mejora continua del proyecto.



Al cierre del período evaluado, permanecen 3 acciones pendientes de finalización, sobre las cuales se continuará realizando seguimiento con los responsables para garantizar su ejecución y el cumplimiento de los compromisos establecidos.

Para el mes de julio de 2026 no aplica la medición de este indicador, debido a que su periodicidad es trimestral. En consecuencia, la siguiente evaluación se realizará al finalizar el trimestre julio–septiembre de 2026, una vez se cuente con la información consolidada correspondiente a los meses de julio, agosto y septiembre.

6 GESTION DE RIESGOS

A continuación, se indica el seguimiento a los riesgos identificados para los servicios prestados:

SERVICIO/ PRÁCTICA	NOMBRE	DESCRIPCIÓN	¿MATERIALIZADO?	ACCIONES PARA REALIZAR
Todos	Posibilidad de incumplimiento de obligaciones contractuales	Posibilidad de incumplimiento de obligaciones contractuales relacionadas con cumplimiento, responsabilidad de empleados, proveedores o terceros	NO	Las pólizas se encuentran vigentes
Todos	Incumplimiento en los ANS establecidos en el contrato	Incumplimiento en los ANS establecidos en el contrato	SI	En el periodo se presentaron incumplimiento de 2 ANS relacionados con el servicio de conectividad y se aplicaron las penalizaciones correspondientes
Todos	Ausencia del personal asignado	Ausencia del personal, encargado de gestionar, administrar y operar los servicios.	NO	El personal asignado estuvo disponible durante el periodo.
Todos	Imposibilidad de acceso a la Herramienta de Gestión Aranda	Falla de acceso a la herramienta de gestión.	NO	La herramienta de gestión ha estado disponible
Eventos/ servicio de monitoreo	Imposibilidad acceso a Herramienta monitoreo (Zabbix)	Falla de acceso a la herramienta de monitoreo	NO	La herramienta de gestión ha estado disponible
Mesa de servicios	Problemas de funcionalidad en la cuenta de soportemt@mintrabajo.gov.co.	Falla en el acceso y/o sincronización del correo soportemt@mintrabajo.gov.co	NO	El correo electrónico institucional ha estado disponible
Mesa de servicios	Imposibilidad de contacto por la línea telefónica de la mesa de servicios	Falla en el ingreso de las llamadas a la mesa de servicios	NO	La línea telefónica ha estado disponible
Mesa de servicios	Desborde de solicitudes (vía correo electrónico y/o llamadas) en la Mesa de Servicios	Aumento eventual de la cantidad de solicitudes que supera la capacidad de atención de los Agentes de la Mesa de servicios	NO	No se ha presentado desborde de solicitudes
Mesa de servicios	Riesgo de seguridad de la información que comprometan la confidencialidad, integridad o disponibilidad de la información.	Posibilidad de uso indebido de la cuenta genérica del cliente, asignada para la Mesa de servicios	NO	No se ha presentado dicha situación.

SERVICIO/ PRÁCTICA	NOMBRE	DESCRIPCIÓN	¿MATERIALIZADO ?	ACCIONES PARA REALIZAR
Soporte en Sitio	Incumplimiento de los compromisos pactados por atención de actividades urgentes - no planeadas	Solicitud de realización de actividades urgentes no planeadas que afectan la prestación del servicio de acuerdo con lo planeado	NO	No se ha presentado dicha situación.
Todas las prácticas	Deficiencias en la adopción de las prácticas de ITIL	Resistencia a la adopción de las prácticas de ITIL por las partes interesadas	NO	Se proporcionó capacitación a los involucrados
Práctica de Activos	Posibilidad de pérdida de inventario	La pérdida de inventario se produce cuando las cantidades reales del inventario son inferiores a las registradas en el módulo de gestión	NO	Se realizó seguimiento con el equipo de trabajo para revisar los compromisos de la práctica, adicional revisión del inventario físico, SGU y ADM con apoyo de Soporte en Sitio.
Todos	Ausencia del personal asignado	Ausencia del personal, encargado de gestionar, administrar y operar los servicios.	NO	El personal asignado estuvo disponible durante el periodo.
Todos	Indisponibilidad de la nube privada que afecte la prestación de servicios de TI	Falla en la prestación de los servicios de TI por falla en la infraestructura de TI provista por la UT	NO	Se dispuso de la infraestructura y recursos que soportan las estrategias de contingencia y recuperación. El suministro del servicio de energía eléctrica fue normal en los sitios alternos. Se realización copias de respaldo de las bases de datos, información y sistemas de información se realiza de acuerdo con la política institucional de copias de respaldo.
Todos	Pérdida de información	Falla en la generación de las copias de respaldo de la información centralizada	NO	Se realizan pruebas de restauración de backups generados por la herramienta definida para el proyecto
Todos	Pérdida de disponibilidad	Perdida de disponibilidad de la infraestructura que soporta los servicios y activos de información de TI	NO	No se ha presentado dicha situación.
Todos	Pérdida de integridad	La ausencia de actualizaciones de seguridad en las aplicaciones podría poner en riesgo la integridad y disponibilidad de los sistemas, permitiendo la ejecución de código malicioso.	NO	Se realizó la planeación del primer ejercicio de Ethical Hacking. Se ejecutaron de manera oportuna y permanente las actualizaciones y controles necesarios para remediar las vulnerabilidades detectadas durante las pruebas de seguridad.
DRP	Indisponibilidad de servicios de TI	Indisponibilidad de la Infraestructura principal alojada en Datacenter Cirion Colombia XV	NO	Se dispuso de la infraestructura y recursos que soportan las estrategias de contingencia y recuperación. El suministro del servicio de energía eléctrica fue normal en los sitios alternos. Se realización de copias de respaldo de las bases de datos, información y sistemas de información se realiza de acuerdo

SERVICIO/ PRÁCTICA	NOMBRE	DESCRIPCIÓN	¿MATERIALIZADO ?	ACCIONES PARA REALIZAR
				con la política institucional de copias de respaldo.
Servicios centrales Servicios en sede	Fallas en los servicios de TI que afecten las actividades de la entidad producto realizar cambios no programados	Presentación de incidentes en la infraestructura tecnológica	NO	Se cuenta con los procedimientos y documentación de la práctica para que los cambios se registren y ejecuten adecuadamente
SD -WAN	Falla en la infraestructura del servicio instalada en DC	Falla de uno o varios equipos que se encuentran provistos en el DC	NO	No se ha presentado dicha situación Se está trabajando en el cronograma de pruebas de disponibilidad de los diferentes servicios
LAN /WLAN	Falla en Switch Core / switch de borde	Indisponibilidad del servicio de conectividad por falla del switch core	NO	El servicio de conectividad ha estado disponible
Todos	Ausencia del personal asignado	Ausencia del personal, encargado de gestionar, administrar y operar los servicios.	NO	El personal asignado estuvo disponible durante el periodo.
Telefonía IP	Falla o pérdida de conectividad en troncal SIP	Indisponibilidad del servicio de telefonía por falla en la troncal SIP	NO	La troncal SIP ha estado disponible
Telefonía IP	Falla en el servicio de conectividad	Indisponibilidad del servicio de telefonía por falla en el servicio de conectividad	NO	El servicio SD WAN ha estado disponible
Telefonía IP	Falla del Admin Center de Microsoft Teams	Indisponibilidad del servicio de telefonía por falla Microsoft Teams	NO	El Admin Center de Microsoft Teams ha estado disponible
Outsourcing de impresión	Falla en el servidor de impresión.	Indisponibilidad del servicio de impresión por falla del servidor	NO	El servicio de impresión ha estado disponible.

Tabla 123 Gestión de Riesgos

7 BOLSA DE RECURSOS

Para el período del informe el Ministerio del Trabajo autorizó el uso de la bolsa de recursos para la inclusión de los rubros que se detalla a continuación:

Descripción	Cantidad	Precio total antes de IVA
Switch de acceso 48 puertos	8	$4.068.408
Clics adicionales B/N	49075	$7.066.800
Clics adicionales color	1188	$703.296
	Subtotal	$11.838.504

Tabla 124 Bolsa de Recursos

8 MEDICIÓN DE ACUERDOS DE NIVEL DE SERVICIO

En cumplimiento de lo dispuesto en el Anexo Técnico Base 10102023 – definitivo, Fase de Operación que indica entre otras obligaciones del contratista las siguientes:

Iniciar la medición de ANS y seguimiento de los servicios, entendiéndose que los ANS deben ser configurados desde la fase de transición.

Efectuar la medición de los ANS mensualmente.

Se procedió a realizar la medición de los ANS a partir de la data exportada de Aranda, la cual permite reflejar el comportamiento del servicio y realizar su medición con la parametrización de los ANS establecidos en el documento Anexo acuerdos de niveles de servicio (ajustada adenda) 10102023, como se refleja a continuación:
Se incluye información actualizada del reporte de ANS.

Área	Nombre Indicador	Resultado	Meta
Mesa de Servicio	Tiempo de atención de solicitudes por soporte en sitio	97,20%	95,00%
	Tiempo de solución de incidentes por soporte en sitio	97,14%	90,00%
	Tiempo de solución de requerimientos por soporte en sitio	99,89%	90,00%
	Tiempo de respuesta de la mesa de servicio	98,89%	85,00%
	Abandono de llamadas	0,55%	Máximo 8,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Equipos de usuario final	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
ANTIVIRUS	Cobertura de antivirus	98,27%	95,00%
	Continuidad y disponibilidad de la plataforma	100,00%	98,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
LAN y WLAN	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Energía Regulada	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Datacenter	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Continuidad y disponibilidad del datacenter principal	100,00%	99.95%
	Continuidad y disponibilidad del datacenter alterno	100,00%	99,60%
	Continuidad y disponibilidad de la plataforma de procesamiento, almacenamiento y respaldo	100,00%	99,70%
	Tiempo de solución de incidentes asociado a los servicios de aplicaciones especializadas	97,60%	90,00%
	Tiempo de solución de requerimientos asociado a los servicios de aplicaciones especializadas	100,00%	90,00%
	Continuidad y disponibilidad de los servicios de directorio activo	100,00%	99,60%
	Continuidad y disponibilidad de los servicios de seguridad informática	100,00%	99,90%
	Tiempo de solución de incidentes asociado a los servicios de administración, soporte y monitoreo	97,46%	90,00%
	Tiempo de solución de requerimientos asociado a los servicios de administración, soporte y monitoreo	99,82%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Nube pública	Continuidad y disponibilidad de la nube pública	100,00%	99,90%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Outsourcing de impresión	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Telefonía IP	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Continuidad y disponibilidad de los servicios de telefonía IP	99,96%	99,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Conectividad WAN e Internet	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Continuidad y disponibilidad del servicio de WAN en sedes nacionales con un solo enlace	(*)	99,60%
	Continuidad y disponibilidad del servicio de WAN en sedes nacionales con doble enlace (principal MPLS + secundario Internet dedicado)	(*)	99,90%
	Continuidad y disponibilidad del servicio de internet en Datacenter principal	100,00%	99,95%
	Continuidad y disponibilidad del servicio de internet en Datacenter alterno	100,00%	99,70%
	Continuidad y disponibilidad del servicio de WAN en Datacenter principal	100,00%	99,95%
	Continuidad y disponibilidad del servicio de WAN en Datacenter alterno	100,00%	99,95%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 125 Medición de Acuerdos de Niveles de Servicio

(*) De acuerdo con la solicitud del Coordinador del Grupo de Soporte Informático los valores de la continuidad y disponibilidad se encuentran desagregados en el archivo ANS Internet - MPLS.

Cumplimiento en la entrega del informe de gestión mensual para todos los servicios. Meta de cumplimiento del indicador del 100%, se entrega el informe a la Supervisión del Contrato y Coordinador del Grupo de Soporte Informático dentro del tiempo comprometido.

9 ANEXOS

- Certificación_backup_servidores
- Consumo de cuotas julio
- Detalle_llamadas_recibidas_(01.07.2026-31.07.2026)
- Datos_Mintrabajo_julio
- Informe Sistema Nacional de Registro de Trabajadores - SNRT

FIN DEL DOCUMENTO