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

Agosto de 2026

DOCUMENTO/ ARCHIVO	
Código:	**Informe Gestión - Unión Temporal Gestión TIC 2023**
Nombre Archivo:	**Informe Gestión - Unión Temporal Gestión TIC 2023 – Agosto 2026**
Fecha:	08/09/2026
Versión:	1

REGISTRO DE CAMBIOS			
Versión	**Páginas**	**Fecha Modificación**	**Motivo del cambio**
1	168	08/09/2026	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**

Trabajo

Índice

Introducción 9
Objetivo 9
Alcance 9
Definición de Siglas y Expresiones Técnicas 10
1 GERENCIA Y/O ADMINISTRACIÓN 11
2 LÍNEA DE GESTIÓN DE SERVICIOS 11
2.1. Gestión del Servicio 11
2.1.2. Prácticas ITIL 4 18
2.1.2.1. Práctica Acuerdos Niveles de Servicio (ANS) 19
2.1.2.2. Práctica Habilitación de Cambios 21
2.1.2.3. Práctica Gestión de Activos 23
2.1.2.4. Práctica Catálogo de servicios 24
2.1.2.5. Práctica de Problemas 29
2.1.2.6. Práctica de Incidentes 30
2.1.2.7. Práctica de Requerimientos 38
2.1.2.8. Práctica de Eventos 42
2.1.2.9. Práctica de Disponibilidad 53
2.1.2.10. Práctica de Implementación 56
2.2 Mesa de Servicios y Soporte en Sitio 57
3 LINEA DE SERVICIOS CENTRALES 67
3.1 Datacenter Principal 67
3.1.1 Datacenter Alterno y DRP 69
3.1.2 Procesamiento almacenamiento y respaldo Servicio Windows y Office 365. 75
3.1.3 Procesamiento, almacenamiento y respaldo - Nube Privada 80
3.1.4 Aplicaciones Especializadas 86
3.1.5 No aplica 96
3.1.6 Seguridad Informática 96
3.1.6.1 Firewalls de nueva generación 96
3.1.6.2 Sandbox – Amenazas día 0 103
3.1.6.3 SIEM - Solución de correlación de eventos de seguridad, disponibilidad y recursos 105
3.1.6.4 WAF - Servicio de tipo “Firewall de Aplicaciones Web” 109
3.1.6.5 Solución de Anti-DDoS 110
3.1.6.6 Casos atendidos de los servicios de seguridad 111
3.1.6.7 Análisis de riesgo 112
3.1.6.8 Políticas y procedimiento de seguridad 113
3.1.7 Licenciamiento 113
3.1.8 Administración, soporte y monitoreo 114
3.2 No aplica 115
3.3 Conectividad WAN, SDWAN e Internet 115
3.3.1 Canales WAN 115
3.3.1.1 Incidentes de Conectividad 117
3.3.1.2 Topología Actual 117
3.3.2 Canales SDWAN e Internet Dedicado 118
4 LINEA DE SERVICIOS EN SEDE 121
4.1.1.1 Equipos de Cómputo de usuario final 121
4.1.2 Equipos de Escritorio 127
4.1.3 Equipos Portátiles 127
4.2 Conectividad LAN y WLAN 127
4.2.1 Switch CORE Sede Principal 129
4.2.2 Switch para conexiones perimetrales (EDGE) en sede principal 129
4.2.3 Switch de acceso 24 puertos 129
4.2.4 Switch de acceso 48 puertos 129
4.2.5 Puntos de Acceso 130
4.3 Telefonía IP 131
4.3.1 Teléfono Gama Media 131

4.3.2 Teléfono Gama Baja 132
4.3.3 Troncales SIP 132
4.3.4 No Aplica 133
4.3.5 No Aplica 133
4.3.6 Módems 4G – Con plan de 50 Gbps 133
4.4 Energía Regulada UPS 139
4.4.1 UPS 10 kVA 139
4.4.2 UPS 15 kVA 140
4.4.3 UPS 20 kVA 140
4.5 No aplica 142
4.6 Outsourcing de Impresión 142
4.6.1 No aplica 146
4.6.2 Multifuncional B/N rango medio – Cargo fijo mensual 146
4.6.3 Impresora Color rango medio – Cargo fijo mensual 146
4.6.4 No aplica 146
4.6.5 Multifuncional B/N rango medio – Clic de impresión 146
4.6.6. Impresora Color rango medio – Clic de impresión 146
4.7 Antivirus 147
4.7.1 Instalaciones de antivirus en servidores 147
4.7.2 Instalación de antivirus PCs usuarios final 148
4.7.3 Top 10 Virus Detectados 149
4.7.4 Servicio de Vulnerabilidades 153
4.7.4.1 Inventario y licenciamiento 154
4.7.4.2 Escaneos programados 154
4.7.4.4 Estrategia de remediación y/o mitigación 157
4.7.4.5 Resumen de mitigación efectuada 157
5 GESTIÓN DE CALIDAD DE INFORMACIÓN 160
5.1 Evaluación calidad documental de casos 160
5.2 Evaluación de calidad de llamadas 161
5.3 Práctica de Mejora 162
6 GESTION DE RIESGOS 164
7 BOLSA DE RECURSOS 166
8 MEDICIÓN DE ACUERDOS DE NIVEL DE SERVICIO 166
9 ANEXOS 168

Tabla 1 Divulgación de información por SoporteMT 12
Tabla 2 Novedades de sedes 14
Tabla 3 Atención de solicitudes por Grupo de Especialista 19
Tabla 4 Medición Indicador Porcentaje de Cumplimiento de ANS 19
Tabla 5 Tipificación de los cambios 21
Tabla 6 Medición Indicador Porcentaje de Cambios Exitosos 22
Tabla 7 KPI Práctica de activos 24
Tabla 8 KPI Práctica Catálogo de Servicios 27
Tabla 9 Consolidado problemas identificados 30
Tabla 10 Categorización de Incidentes por Servicio 33
Tabla 11 Top 10 Incidentes 35
Tabla 12 Incidentes Suspendidos 35
Tabla 13 Incidentes mayores 36
Tabla 14 Medición de KPIs 36
Tabla 15 Estados de Requerimientos 39
Tabla 16 Estados de Tareas de requerimientos 39
Tabla 17 Seguimiento del Backlog Suspendidos 39
Tabla 18 Top 10 de Solicitudes 40
Tabla 19 Detalle de KIP Practica de Requerimientos 40
Tabla 20 Casos reabiertos 42
Tabla 21 Consolidado disponibilidad de servidores 54

Tabla 22 Consolidado disponibilidad de Directorio Activo 54
Tabla 23 Desagregado de Disponibilidad Directorio Activo 54
Tabla 24 Consolidado disponibilidad de equipos Datacenter principal 54
Tabla 25 Desagregado de Disponibilidad Datacenter Principal 54
Tabla 26 Consolidado disponibilidad de equipos Datacenter alterno....54
Tabla 27 Desagregado Disponibilidad de equipos Datacenter alterno 55
Tabla 28 Consolidado disponibilidad de equipos redes y conectividad 55
Tabla 29 Consolidado disponibilidad de equipos de seguridad 55
Tabla 30 Disponibilidad de equipos Seguridad de la Información 55
Tabla 31 Consolidado disponibilidad de equipos de telefonía 55
Tabla 32 Consolidado disponibilidad de plataforma antivirus 55
Tabla 33 Llamadas Atendida por la Mesa de Servicio 57
Tabla 34 Llamadas exceptuadas por la Mesa de Servicio....58
Tabla 35 Casos Anulados....59
Tabla 36 Casos Suspendidos 59
Tabla 37 Casos Atendidos usuarios VIPS 64
Tabla 38 Casos Atendidos usuarios 64
Tabla 39 Visitas a sedes sin Soporte en Sitio....66
Tabla 40 Medición de ANS Mesa de servicios....66
Tabla 41 Bases de Datos con LogShipping 71
Tabla 42 Capacidades iniciales 84
Tabla 43 Capacidades modificatorio....85
Tabla 47 Total capacidades ambientes pruebas....85
Tabla 48 Consumos totales 85
Tabla 49 *Suma Instancias* 91
Tabla 50 Total Docs....92
Tabla 51 Total Radicados 92
Tabla 52 Dimensionamiento Servers IBM - Virtualización Optima....93
Tabla 53 Apps & DDBB Oracle....95
Tabla 54 Tendencia de uso de ancho de banda....97
Tabla 55 usuarios con mayor consumo de ancho de banda....99
Tabla 56 Top de usuarios por sesiones....100
Tabla 57 Top de aplicaciones 101
Tabla 58 Consolidado de indicadores....103
Tabla 59 Fuentes de eventos 106
Tabla 60 Tipos de incidentes 106
Tabla 59 Hosts e IPs Implicados....107
Tabla 62 Aplicaciones por Ancho de Banda 108
Tabla 63 Tipo de ataque....110
Tabla 64 Reporte de requerimientos agosto....112
Tabla 65 Vulnerabilidades en la infraestructura....112
Tabla 66 Vulnerabilidades en la infraestructura....112
Tabla 67 ataques de phishing....112
Tabla 68 Licenciamiento....113
Tabla 69 Medición ANS Datacenter....115
Tabla 70 Medición ANS Nube Pública....115
Tabla 71 Incidentes de conectividad....117
Tabla 72 Medición de ANS Conectividad WAN e Internet 120
Tabla 73 Desagregado sedes con novedad un solo enlace 121
Tabla 74 Desagregado sedes con novedad con doble enlace 121
Tabla 75 Cantidades de equipos Contractual – Instalados - Almacén....121
Tabla 76 Cantidades de equipos asignados nivel nacional 122
Tabla 77 Cantidades de equipos por devolución nivel nacional 123
Tabla 78 Estado de casos de garantía. 123
Tabla 79 ANS casos de garantía. 123
Tabla 80 ANS Relación casos de garantía 124

Tabla 81 Equipos en siniestro....126
Tabla 82 Solicitudes de Equipos Usuario Final – Según Grupo Responsable....126
Tabla 83 Solicitudes de Equipos Usuario Final – Según Grupo Responsable....126
Tabla 84 Medición ANS Equipos de Usuario Final....127
Tabla 85 Top 5 de categorías en el Servicio de conectividad LAN-WLAN....128
Tabla 86 Distribución y Cantidades de switch 24 puertos....129
Tabla 87 Distribución y Cantidades de Switch 48 puertos....130
Tabla 88 Distribución de puntos de acceso....131
Tabla 89 Medición ANS LAN y WLAN....131
Tabla 90 Equipos gama media....132
Tabla 91 Sedes cerradas....132
Tabla 92 Consolidado de teléfonos gama baja....132
Tabla 93 Consolidado equipos MIFI....133
Tabla 94 Minutos, consumos....135
Ilustración 94 Top llamadas nacionales....135
Tabla 96 Top 5 consumo de llamadas....136
Tabla 97 Top 5 llamadas LDI....136
Tabla 98 Top 5 llamadas Celular....137
Tabla 99 Top 5 llamadas locales....137
Tabla 100 Medición ANS Telefonía IP....139
Tabla 101 Inventario de UPS – 10kVA....139
Tabla 102 Inventario de UPS – 20Kva....140
Tabla 103 Casos gestionados – Energía Eléctrica Regulada UPS....141
Tabla 104 Medición ANS Energía Eléctrica UPS....142
Tabla 105 Inventario de impresoras para el servicio....142
Tabla 106 Consumo de impresiones y copias por usuario - Impresoras B/N....143
Tabla 107 Top 10 de impresoras con mayor uso....144
Tabla 108 Top usuarios impresión a color....144
Tabla 109 Top oficinas....144
Tabla 110 Top 10 impresoras más usadas del servicio de fotocopiado....145
Tabla 111 Ampliación de cuota de impresión....145
Tabla 112 Despacho de papel a sedes del Ministerio del Trabajo....145
Tabla 113Cargo mensual multifuncional rango medio....146
Tabla 114 Cargo mensual impresora color....146
Tabla 115 Clics de impresión de agosto 2026 – Multifuncional B/N....146
Tabla 116 Tendencia de consumo de clics B/N....146
Tabla 117 Clics de Impresión – Impresora Color....147
Tabla 118Tendencia de consumo de clics color....147
Tabla 119 Medición ANS Outsourcing de Impresión....147
Tabla 120 Top 5 Equipos....152
Tabla 121 Medición de ANS Antivirus....160
Tabla 122 KPI Practica de Mejora....163
Tabla 123 Gestión de Riesgos....166
Tabla 124 Medición de Acuerdos de Niveles de Servicio....167

Índice de Ilustraciones

Ilustración 1 Estado final de casos al corte del período....18
Ilustración 2 Cumplimiento de ANS....20
Ilustración 3 Ajuste tareas árbol de categorías seguridad informática....25
Ilustración 4 Matriz de escalamiento....26
Ilustración 5 Actualización grupo NOC....27
Ilustración 6 Estados Incidentes....31
Ilustración 7 Categorización de Incidentes por Servicio....32
Ilustración 8 Top 10 Incidentes....34
Ilustración 9 Efectividad de resolución de incidentes....37
Ilustración 10 KPI Efectividad de Resolución de Requerimientos de Servicio....41

Ilustración 11 Requerimientos de Reabiertos en el periodo....41
Ilustración 12 Resumen de incidentes....43
Ilustración 13 Top 10 Sedes afectadas por Router....44
Ilustración 14 Causas de eventos generados por Router....46
Ilustración 15 Sedes afectadas por Switch....46
Ilustración 16 Causa de eventos generados por Switch....47
Ilustración 17 Top 9 Sedes afectadas por Access Point....47
Ilustración 18 Causa de eventos generados por AP....48
Ilustración 19 Top 10 Sedes afectadas por Starlink....48
Ilustración 20 Causas de eventos generados por Starlink....49
Ilustración 21 Top Sedes afectadas por FortiGate....50
Ilustración 22 Causas de eventos generados por FortiGate....50
Ilustración 23 Causas de alarmas Servidores Windows....51
Ilustración 24 Causas de alarmas Servidores Linux....52
Ilustración 25 Grafica CPU....52
Ilustración 26 Grafica memoria....53
Ilustración *27 Seguimiento de Pruebas de Disponibilidad 2026*....56
Ilustración 28 Seguimiento Práctica Implementación....57
Ilustración 29 Llamadas Atendidas....58
Ilustración 30 Incidentes soporte en sitio....60
Ilustración 31 incidentes solucionados por territoriales....60
Ilustración 32 requerimientos solucionados mesa de servicios....61
Ilustración 33 requerimientos solucionados soportes....61
Ilustración 31 requerimientos solucionados soporte territoriales....62
Ilustración 32 Requerimientos Cerrados por la Mesa de Servicios....62
Ilustración 33 Casos Cerrados por Soporte en Sitio....63
Ilustración 34 Casos Cerrados por Territoriales....63
Ilustración 35 Medios de Ingreso de Casos....64
Ilustración 36 Gestión Casos – SC....67
Ilustración *37* Gestión SC - Por Grupo....68
Ilustración 38 Comportamiento SWCORE Datacenter Colombia XV....68
Ilustración 39 Sincronización HA de los Switch Core....69
Ilustración 40 Grafica de consumo canal Internet Datacenter....69
Ilustración 41 máquinas virtuales DRP....70
Ilustración 42 Escenario Apps DRP....71
Ilustración 43 Extremo DC Bogotá....72
Ilustración 44 Extremo DC Cali....72
Ilustración 45 Estado canal de Internet DC Cali....72
Ilustración 46 Estado SWCORE Datacenter alterno....73
Ilustración 47 Estado HA SWCORE Datacenter alterno....74
Ilustración 48 Consumo canal MPLS DC Alterno....74
Ilustración 49 Estado Router MPLS DC Alterno....75
Ilustración 50 Gestión de Casos Windows....76
Ilustración 51 Cumplimiento WSUS....77
Ilustración 52 Block Legacy Authentication....78
Ilustración 53 Fechas de Soporte....80
Ilustración 54 Licencias asignadas....80
Ilustración 55 Gestión Nube Privada....84
Ilustración 56 Nuevo entorno ACEDOC....88
Ilustración 57 Gestión Apps Especializadas....89
Ilustración 58 Gestión Casos IBM....90
Ilustración 59 Licenciamiento adicional componente IBM....93
Ilustración 60 Gestión DDBB....94
Ilustración 61 Estado Bases de Datos....95
Ilustración 62 Firewall de nueva generación.....96
Ilustración 63 Comportamiento ancho de banda....98

Ilustración 64 Tendencia de uso de ancho de banda....99
Ilustración 65 Top de usuarios por números de sesiones....99
Ilustración 66 Top de aplicaciones....100
Ilustración 67 Top de Autenticación....102
Ilustración 68 sesiones fallidas....103
Ilustración 69 Reporte mensual....104
Ilustración 70 Captura de pantalla perfomance....104
Ilustración 71 licencia sandbox....105
Ilustración 72 Comportamiento de EPS....106
Ilustración 73 Detalle servidores....108
Ilustración 74 Top attack types....109
Ilustración 75 Top de ataques....110
Ilustración 76 Políticas y procedimientos....113
Ilustración 77 Consumo canal MPLS DC Principal....116
Ilustración 78 Estado Router MPLS DC Principal....116
Ilustración 79 Topología actualizada....117
Ilustración 80 Interface Fortimanager....118
Ilustración 81 Interface MPLS HUB SDWAN....118
Ilustración 82 Interface Internet HUB SDWAN....119
Ilustración 83 VPN SDWAN establecidas....119
Ilustración 84 Estado HUB SDWAN Datacenter....119
Ilustración 85 Estado HA HUB Sdwan....120
Ilustración 86 Recursos Fortimanager....120
Ilustración 87 Estado de casos Redes y Conectividad....128
Ilustración 88 Asignación de licencias....134
Ilustración 89 Comportamiento de tráfico....135
Ilustración 90 llamada internacional de prueba....136
Ilustración 91 Top Celular....136
Ilustración 92 Top Local....137
Ilustración 93 Requerimientos por garantía....138
Ilustración 94 Disponibilidad y Continuidad TOIP....138
Ilustración 95 Equipos consola antivirus....148
Ilustración 96 Gestión consola antivirus – equipos usuario final....149
Ilustración 97 Top 10 virus detectado....150
Ilustración 98 Descripción de virus....150
Ilustración 99 BOPMFTRIANA....152
Ilustración 100 ANPJCHERNANDEZM....153
Ilustración 101 ARDMGIRALDO....153
Ilustración 102 CTDJORTEGAJ....153
Ilustración 103 *Gestión consola Nessus*....154
Ilustración 104 *Escaneos programados*....155
Ilustración 105 TOP 10 - Vulnerabilidades por severidad....156
Ilustración 106 Tendencia de vulnerabilidades trimestral....156
Ilustración 107 Vulnerabilidades gestionadas vs en remediación....158
Ilustración 108 revisión configuraciones....159
Ilustración 109 captura envío de correo gestión de vulnerabilidades....159
Ilustración 110 Resultado General....160
Ilustración 111 Resultado de criterios y parámetros - Calidad de llamadas....161
Ilustración 112 Seguimiento Práctica Mejora....162
Ilustración 113 Resultado de Cumplimiento AM....163

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 agosto 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 no se generaron modificatorios.

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 divulgación de información a través de comunicados desde la cuenta de Soporte MT, estos fueron:

- **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 del Portal WEB, aplicativo SIRITI, Actualización del SO de los equipos Fortigate en el Data Center, Servidores de Aplicaciones RUI y SISINFO, base de datos RUAF, Base de Datos Pila, Actualización de la Suite Visión Empresarial (SVE).
- **Afectación en la conectividad de las sedes** DT Valle del Cauca, Choco, Risaralda, Caldas, Quindío con sus inspecciones anexas, **luego del terremoto** ocurrido el 10 de agosto 2026.
- **Comunicados de servicios e información de TI:**

Temática	Evidencia correo
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
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

Temática	Evidencia correo
Lineamientos de uso y manejo del **One Drive** y la responsabilidad del manejo de la información institucional.	¡INFORMACIÓN IMPORTANTE LINEAM
Políticas Institucionales en Seguridad de la Información (Sistema de Gestión de Seguridad de la Información) – **Este comunicado fue solicitado por la Oficina TICs.**	POLÍTICAS DE LA SEGURIDAD DE LA IN
Comunicado de **uso del Fortitoken,** cuando se usa, como solicitar apoyo en caso de requerirlo, como generar la descarga de la aplicación, activación del código QR y uso en la sesión.	uso del doble factor de autenticación de VI
Comunicado de posibles alertas de Trend Micro durante el acceso a servicios de Google en el marco de las actividades de monitoreo y fortalecimiento de la seguridad de la información, y según boletín **emitido por Colcer**t.	¡INFORMACIÓN IMPORTANTE - Alerta
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 *Villeta / Cundinamarca *Fusagasugá / Cundinamarca * El Doncello / Caquetá	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.
Tibú / Norte de Santander	Usuario trabaja en sede una semana al mes, el resto de tiempo trabaja desde la 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	Requiere adecuación del cableado de red y eléctríco, desde el 29/01/2026 luego de remodelación de la alcaldía.Se ubican los puestos de trabajo cercanos a los puntos de energía (que se solventaron con extensiones) y al fortinet.

Sede	Novedad
Tumaco / Nariño	Se trasladó el 16/01/2026 pero 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.
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 estuvieron trabajando desde casa mientras en las sedes finalizaron las labores de adecuación locativa, ubicación de puestos de trabajo, finalizan labores de cableado estructurado e instalación del rack. - Se informo diariamente los avances al Coordinador de Grupo de Soporte Informático y se remite correo final indicando normalidad en los servicios de TI desde el 10 de agosto con la llegada de usuarios a las sedes.  RE_ Traslado de la sede de la Dirección T  RE_ Traslado de la sede del Cauca .msg
Bosconia / Cesar	El 12 de agosto informan traslado de la IT Bosconia, se coordina apoyo el técnico del soporte de la territorial para desplazarse a la zona y apoyar a la inspectora, se deja MiFi como contingencia mientras se gestiona el traslado del canal de fibra.
Hatonuevo / Guajira	El 19 de agosto la IT Fonseca en la Guajira realiza traslado al municipio Hatonuevo en el mismo departamento. El personal de soporte de la DT asiste a la sede para apoyar labores de desconexión y embalaje, se habilita conectividad temporal mediante MiFi mientras se gestiona lo correspondiente al traslado del enlace de fibra.  Novedad Traslado IT Fonseca _ Guajira a ot
Cumaral / Meta	El 24/08/2026 reportan novedad de traslado de la inspección Cumaral el día de la mudanza, se coordina personal técnico para el desmonte, traslado e instalación de la antena Starlink en la nueva sede. Se remite correo a la entidad indicando que los equipos quedan operativos y con servicio de internet, se incluye registro fotográfico de cómo se dejó ubicado el soporte.  RE_ Traslado inspección Cumaral _

Sede	Novedad
DT Tolima	El director territorial habilito trabajo en casa desde el 13 al 25 de agosto para el personal de la sede.
La Plata / Huila	Desde el 12 al 28 de agosto la IT La Plata se estuvo apagada por trabajos de adecuaciones en la sede, los equipos fueron almacenados temporalmente y la usuaria brinda atención desde un espacio acondicionado.

Tabla 2 Novedades de sedes

- **Novedades en sedes por terremoto del 10 de agosto:**
  Se remite diariamente al Coordinador del Grupo de Soporte informático las actualizaciones de sedes correspondientes luego del terremoto del 10 de agosto, asociadas al estado de las sedes, retiro de equipos por funcionarios, estado del servicio de conectividad, entre otras. Esta actividad se realiza diariamente y está a cargo del supervisor de soporte de territorio.


Novedad en sedes afectadas por terremc


Novedades en sedes_ agosto 26.msg


Novedades en sedes territoriales_ agosto 2

Dentro de las novedades más relevantes se tienen:

Sede	Estado		Novedades
	Abierta	Cerrada	
Armenia	X		Estuvo cerrada desde el 10 de agosto y se dio apertura el 1 septiembre 2026.
Pereira		X	- No se ha tenido acceso a la oficina para evaluar daños dada la criticidad en la zona, en revisión estructural del edificio. - Se embalan, trasladan e instalan 9 equipos de escritorio en ubicación alterna, la sede cuenta con red LAN y acceso a internet. - El 1 de septiembre se acondiciona zona alterna para operación de personal esencial, los demás están en casa.
Dosquebradas		X	Sin acceso a la sede para validación de equipos y servicios.
La Virginia - Santa Rosa de Cabal	X		Sedes operando con normalidad
Manizales		X	- No se ha tenido acceso a la oficina para evaluar estado de todos los equipos de TI, se están adelantando trabajos locativos de arreglos de la sede, se apoya en reubicación de rack y UPS en el centro de cableado. - Se embalan, trasladan e instalan 3 portátiles y 1 impresora a una ubicación alterna. - El personal se encuentra con trabajo en casa.
Anserma. Manzanares, La Dorada, Salamina, Riosucio	X		Sedes operando con normalidad
Cali		X	- No se ha retornado trabajo en la sede, primero se adelantaron labores de revisión estructural. - Por indicación del director, se retiraron varios equipos para trabajo en casa de los usuarios.

Sede	Estado		Novedades
	Abierta	Cerrada	
			- Se envían desde Bogotá nueve (9) equipos portátiles, para asignación para trabajo en casa.
Buga, Roldanillo, Cartago, Tuluá, Palmira		X	Sedes cerradas, sin acceso.
Sevilla		X	Sin acceso a la sede, edificio presentó fallas considerables e irreparables, informan que se debe demoler.
Buenaventura	X		Estuvo cerrada desde el 10 de agosto y se dio apertura el 1 septiembre 2026.
Quibdó	X		Sede operativa una semana después sin novedades.
Riosucio, Bahia Solano	X		Sedes operando con normalidad
Istmina		X	Sin acceso, sin poder validar

En lo que ha sido posible verificar en las sedes que tienen restricción de acceso se tienen los siguientes siniestros por daño:

- Pereira: 1 monitor.
- Armenia: 2 monitores y 1 CPU, la CPU al parecer tiene la MEM RAM suelta pero si enciende, se registró el caso de garantía con Lenovo.
- Sevilla: Al parecer todo el inventario de TI se encuentra siniestrado (equipo de escritorio, impresora, teléfono, Fortinet, equipos de conectividad).

c. Disposición de RAEES y Residuos Electrónicos: Para esta obligación se adelantaron las siguientes actividades:

- 12/08/2026: Se remite a la entidad la información de Gestión Ambiental – Segundo cuatrimestre 2026 (de abril a julio 2026) relacionada con:
  - Informe de seguimiento de consumo de papel
  - Bitácora de generación de residuos tecnológicos (relacionando cantidades)
  - Certificados de disposición final



- Se gestiona la salida de DT Antioquia (Ciudad Medellin) de los siguientes elementos el 21 de agosto de 2026 , los cuales fueron retirados por el técnico de soporte Andres Castañeda y entregados al proveedor (SUMA Desarrollo Ambiental) para disposición final.

Elemento	Cantidad
Cartuchos de tóner vacíos	24
Unidades de Tambor de Impresora- RAEE	3
Unidad Fusora Impresoras- RAEE	1



RE_ Solicitud de
Salida de elementos D

- Se da respuesta a la entidad sobre la cantidad de colaboradores de la UT Gestión TIC 2023 que laboran en instalaciones de Nivel Central como insumo del reporte de Riesgos de Gestión Ambiental, para los meses de abril a julio de 2026.

VIGENCIA 2026	
Meses	**No. Colaboradores UT - Nivel Central**
ABRIL	53
MAYO	53
JUNIO	52
JULIO	53

d. Otras actividades

- **Publicación de documentos en la SVE:**
  Se tiene pendiente por parte de la Oficina Asesora de Planeación (OAP) que se haga la publicación en la SVE del **formato RFC de la Práctica de Habilitación de Cambios**. Debido a las actualizaciones recientes realizadas a los procedimientos de Itil basadas en las auditorías internas que se han realizado, se entregará un nuevo paquete de documentos al Coordinador del Grupo de Soporte Informático.

- **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

- **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 Secretaría 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 trabajó desde la práctica de incidentes y catálogo, la divulgación con el equipo de trabajo de las nuevas 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.

e. Divulgaciones al equipo de trabajo

- El 3 y 4 de agosto se realiza divulgación al equipo de Soporte de Territorio las novedades que se dan en el Flujo de Desvinculación y el Flujo de Cambio de Sede o Rol para actualización de ubicación de los usuarios cuando se presentan traslados.
- 10/08/2026: Se comparte comunicado con el equipo de soporte en Sitio para reforzar la documentación de los casos de devolución, asignación y traslado de equipos y las plantillas que se tienen disponibles para tal fin.



Documentación de
casos en Aranda.msg

- 24/08/2026: Se realiza divulgación al equipo del SOC sobre las nuevas categorías del Árbol de Seguridad Informática para la gestión de los incidentes de seguridad informática y la creación de tareas relacionadas para la gestión de los demás especialistas de la operación.

2.1.1. Herramienta de Gestión ITSM

Durante agosto 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 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.
- Se realizo la creación de un Script que permite realiza la configuración de los agentes de inventarios de los equipos de manera automática.
- Se realiza automatización de la ejecución del script de verificación de configuración y desconexión de agentes de inventarios, esta automatización consiste en consultar automáticamente la base de datos de equipos, identificar cuales no están logrando conectarse, intentar una conexión desatendida y actualizar la configuración, esto con el fin de reducir los equipos con inventarios de más de 8 días.
- Se realizo la creación de un tablero de control que permite ver en tiempo real como se está comportando la actualización de agentes de inventarios, su nivel alcanzado y los errores más comunes presentados al momento de ejecutarse, este tablero se

puede consultar en: http://172.20.22.194:8080/Dashboard.html

- El 13 de agosto se realizó la actualización de Aranda AQM a la versión 9.43.0 bajo el RFC-293738.
- El 5 de agosto se realizó la actualización de Aranda ADM a la versión 9.5.0 bajo el RFC-294152.

2.1.2. Prácticas ITIL 4

Volumetría de Solicitudes Gestionadas:

En el mes de agosto 2026 se registraron en la herramienta ITSM 7145 solicitudes asociadas a la prestación de los servicios de TI por parte de la UT.

- Tipificación según la volumetría de casos:
  - Requerimientos de Servicio: 5024
  - Incidentes y Eventos: 592 (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): 1507
  - Cambios: 22
  - Problemas: 0.
- Casos Anulados: 3 - 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 agosto 2026:

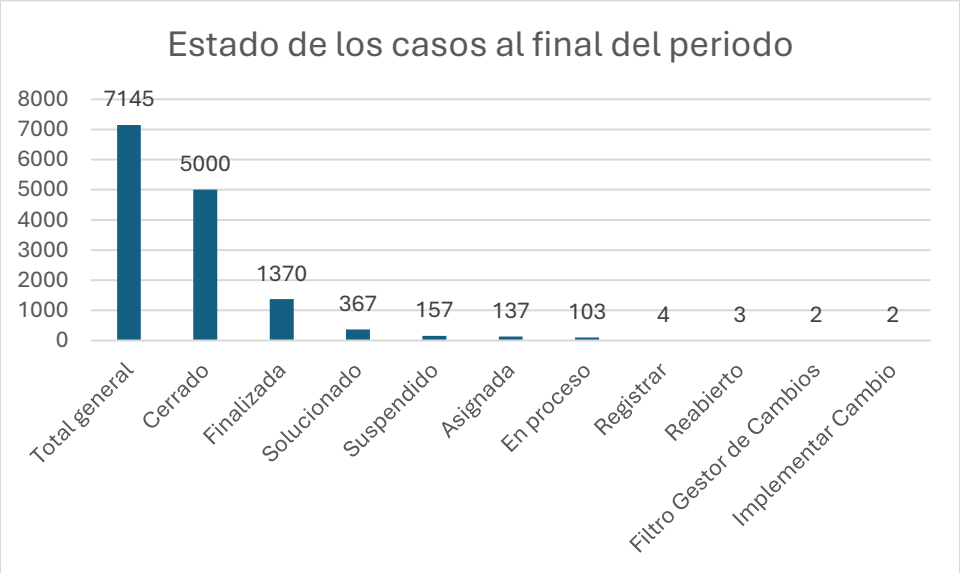


Ilustración 1 Estado final de casos al corte del período

- Gestión por parte de los grupos de especialistas:

Grupo Responsable	Cantidad de casos reportados	Porcentaje%
Responsable_Soporte_Territoriales	1733	24,25
Responsable_Mesa_De_Servicio	1561	21,85
Responsable_Soporte_Bogota	1540	21,55
Especialistas_IBM	530	7,42
Responsable_Soporte_Impresoras	438	6,13
NOC	411	5,75
SOC	318	4,45
Responsable_De_Servidores_Windows	257	3,60
Gestor de Inventarios	112	1,57
Especialista_Telefonía_IP	72	1,01
Especialista Nube Privada	55	0,77
Especialista Herramientas de Gestion	37	0,52
Responsable Garantías Equipos	27	0,38
Especialista Base de datos	17	0,24
Especialista Nube Publica	11	0,15
Especialista Redes	9	0,13
Liferay	7	0,10
Almacenamiento y Backups	3	0,04
Especialista Aplicaciones .Net	3	0,04
Gestión del Servicio	2	0,03
Líder Seguridad de la Información	2	0,03
Total general	7145	100,00

Tabla 3 Atención de solicitudes por Grupo de Especialista

2.1.2.1. Práctica Acuerdos Niveles de Servicio (ANS)

Durante el mes, 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 agosto 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

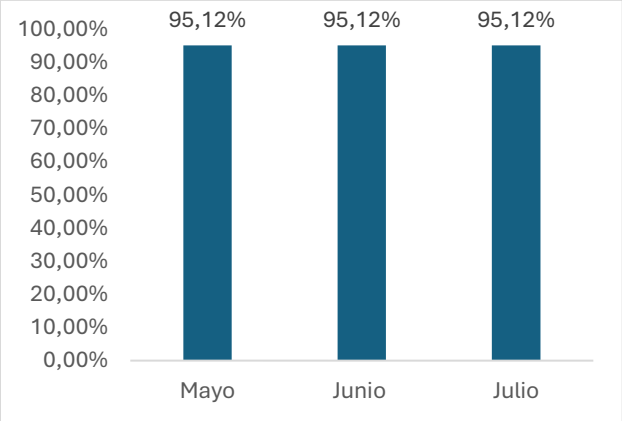


Ilustración 2 Cumplimiento de ANS

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 Identificada**

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 al mes de agosto de 2026. Este apartado contiene información relevante sobre actividades realizadas y novedades presentadas.

Novedades Cambios Estándar: Se gestionó la **identificación, análisis, formalización y aprobación** de dos nuevos procedimientos correspondientes al reinicio controlado de los servicios del Portal Web y a la creación y/o modificación de elementos del Portal. Posteriormente, estos fueron identificados como **Cambios Estándar y establecidos bajo condiciones de aplicación controlada**, fortaleciendo el modelo de gestión mediante la estandarización, optimización y control de actividades recurrentes.

- **Tipificación de los cambios**

Durante el mes de agosto de 2026 se gestionaron 22 casos tipificados como Cambios, clasificados en las siguientes categorías:

Servicio	Cantidad	%
Administración de Bases de Datos	2	9,09%
Administración de servidores	9	40,91%
Aplicaciones Especializadas	5	22,73%
Herramientas de Gestión	2	9,09%
Seguridad informatica	2	9,09%
Soporte Microinformatica	1	4,55%
Telefonía IP	1	4,55%
Total general	**22**	100,00%

Tabla 5 Tipificación de los cambios

- **Relación casos registrados**

A continuación, se presenta la relación de casos registrados en el mes de agosto, en total se crearon 22 casos de los cuales se gestionaron como 12 cambios normales y 3 cambios como cambios de emergencia y 7 cambios como estándar.

- **Cambios por estado**

Al corte del mes, 18 casos quedaron estado Cerrado, 2 casos quedaron en Implementar cambio y 2 casos en Filtro Gestor de Cambios.

- **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: 17/18*100 PCE: 95,00 %

Tabla 6 Medición Indicador Porcentaje de Cambios Exitosos

Durante el período evaluado se implementaron 18 cambios, de los cuales 17 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.

Es importante precisar que, de los 22 cambios gestionados durante el periodo, se implementaron 18 cambios, mientras que los 4 restantes quedaron programados o pendientes de aprobación para su implementación en los primeros días del mes de septiembre.

De los 18 cambios implementados durante el periodo, 17 fueron ejecutados exitosamente y 1 presentó resultado fallido, correspondiente al RFC-294159, debido a una falla de hardware presentada en el equipo Fortinet durante su ejecución. Como parte de la gestión de la novedad, fue necesario activar el procedimiento de garantía (RMA) con el fabricante para el reemplazo del equipo. Una vez recibido el equipo de reemplazo, se gestionó el RFC-320489 para realizar el cambio físico del dispositivo en el Data Center y efectuar las actividades de configuración y validación correspondientes. El cambio fue implementado exitosamente, permitiendo restablecer la operación y atender de manera definitiva la falla identificada en el equipo inicialmente intervenido.

En cuanto a los 4 cambios que no fueron implementados durante el periodo, los RFC-325383 y RFC-325412 quedaron en estado “Implementar Cambio”, con fecha de implementación programada para el 1 de septiembre. Por su parte, los RFC-328699 y RFC-328710 permanecieron en estado “Filtro Gestor de Cambios”, pendientes de la correspondiente revisión y aprobación en las instancias de PRECAB y CAB, de acuerdo con el flujo establecido para la gestión y autorización de cambios.

2.1.2.3. Práctica Gestión de Activos

En la Práctica de Gestión de Activos desarrolló en agosto 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.

- **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.

Posterior al terremoto se realizó el envío de nueve (9) portátiles al DT Valle con el propósito de entregar equipos de contingencia a las funcionarios que se encuentran en trabajo en casa. Se recibió reporte daño de dos (2) monitores y una (1) torre de Armenia los cuales se están gestionando con proveedor. Se realizó movimiento de los activos de Manizales y Pereira a ubicaciones temporales.

Frente a los traslados de Sincelejo y Popayan se realizó la instalación de los equipos en las nuevas instalaciones, de igual manera se prestó apoyo en traslado e instalación de equipos por cambio de sede en Bosconia, Cumaral y de Fonseca a Hatonuevo.
Así mismo, a través de la gestión de cambios se realizó cambio del equipo Firewall en el DataCenter Colombia XV.
El seguimiento de siniestros se describe en el apartado 4.1.1.1 equipos de usuario final.

- **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.

- **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=**3994/4020*100 **P=** 99.35%

Tabla 7 KPI Práctica de activos

Durante agosto, el KPI de Precisión de Información de CI en la CMDB presentó un resultado de 99,35%, superando en 14,35 puntos porcentuales la meta establecida del 85%. Frente al resultado de julio (93,45%), se evidencia una mejora de 5,90 puntos porcentuales, lo que refleja un comportamiento favorable en la calidad, actualización y confiabilidad de la información registrada en la CMDB. Se recomienda mantener las actividades de validación, actualización y control de calidad implementadas, con el propósito de sostener este nivel de desempeño en los próximos periodos.

2.1.2.4. Práctica Catálogo de servicios

Durante el mes de agosto, en el marco de la práctica de Catálogo de Servicios, se dio continuidad a las actividades asociadas a la implementación y fortalecimiento de las nuevas categorías de Incidentes de Seguridad de la Información creadas en la herramienta de gestión Aranda durante el mes de julio. Como parte de esta gestión, se realizó la socialización de las nuevas categorías y lineamientos de atención con los grupos del SOC, Mesa de Servicios, Soporte en Sitio de la Sede Central y Soporte en Sitio de las Territoriales, fortaleciendo su correcta aplicación en la clasificación y gestión de los incidentes.

Adicionalmente, se realizó la actualización y socialización de la Matriz de Escalamiento en tres oportunidades durante el mes (6, 19 y 28 de agosto), debido a las novedades presentadas en los usuarios VIP asociadas a la coyuntura del cambio de Gobierno, actualizaciones de personal y la incorporación de las nuevas categorías de Seguridad de la Información a raíz del procedimiento generado y publicado por la Oficina TICs.

Asimismo, se gestionó la configuración de los grupos responsables de apoyo y escalamiento que deben estar disponibles en Aranda para la creación de tareas por parte del SOC, permitiendo realizar, cuando sea necesario, el escalamiento a los equipos especializados durante la atención de los incidentes clasificados en las 15 nuevas categorías de Seguridad de la Información.

Estas actividades permitieron fortalecer la actualización, consistencia y trazabilidad de la información del Catálogo, así como mejorar los mecanismos de clasificación, asignación y escalamiento de los incidentes de seguridad, en alineación con las necesidades de la operación.



Solicitud para agregar grupos de Nube privada y Redes en las tareas de Incidentes de seguridad de la información CATALOGO

Resumir este correo electrónico

Cifuentes Sanchez, Yuly Rocio
Para: Guerrero Guarin, Jorge Leonardo
CC: Barrero Castro, Paola; Perez Perez, Nasly Carolina; Gonzalez Moreno, Gabriela Maria

Responder · Responder a todos · Reenviar
Vie 21/08/2026 17:01

Estimado Ingeniero Jorge, espero que se encuentre muy bien.

Le escribo para solicitar amablemente su valioso apoyo con un requerimiento prioritario. De acuerdo con lo conversado en la reunión sobre las nuevas categorías para incidentes del árbol de seguridad de la información, sobre la creación de tareas en estos incidentes, el próximo lunes al mediodía realizaremos la socialización con el equipo del SOC.

Con el fin de mostrarles un ejemplo claro de creación y asignación de tareas en los incidentes de seguridad, necesitamos que se incluyan y tambien sea posible asignar tareas por parte del SOC, al **grupo de redes** y a los **especialistas de nube privada**. Esto garantizará que el SOC tenga la visibilidad y disponibilidad para asignarles tareas cuando se necesite.

Adicionalmente, aprovechando su conocimiento y experiencia como especialista en la herramienta de Aranda, queríamos extenderle dos consultas puntuales para esta sesión:

1. **Configuración de solución de tareas:** Notamos una configuración sobre el tiempo para solucionar la tarea. Nos gustaría saber si es posible retirar dicha configuración o, en su defecto, cuál sería su recomendación técnica para darle el mejor manejo conceptual con el equipo.
2. **Notificaciones:** ¿El sistema Aranda envía una notificación automática a los especialistas en el momento exacto en que se les asigna una tarea?

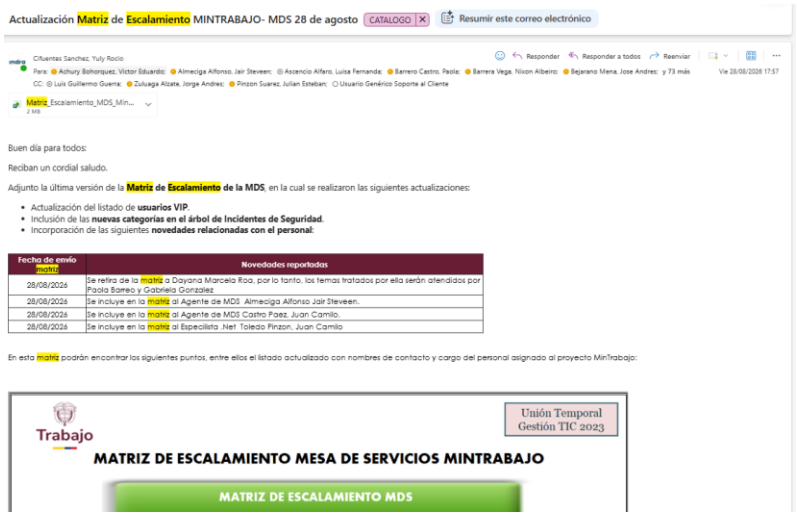
Le agradezco muchísimo su valiosa ayuda con este ajuste y sus orientaciones técnicas.

Quedo atenta a sus comentarios,

INDRA GROUP

Yuly Rocio Cifuentes Sánchez
Gestora ITIL
DIGITAL INFRASTRUCTURES & COMMUNICATIONS (DIC)
SMART WORKSPACE

Ilustración 3 Ajuste tareas árbol de categorías seguridad informática



Actualización Matriz de Escalamiento MINTRABAJO- MDS 28 de agosto CATALOGO

Resumir este correo electrónico

Cifuentes Sanchez, Yuly Rocio
Para: Achury Bohorquez, Victor Eduardo; Almeciga Alfonso, Jair Steveen; Ascencio Alfaro, Luisa Fernanda; Barrero Castro, Paola; Barrera Vega, Nixon Albeiro; Bejarano Mena, Jose Andres; y 73 más
CC: Luis Guillermo Guerra; Zuluaga Alzate, Jorge Andres; Pinzon Suarez, Julian Esteban; Usuario Genérico Soporte al Cliente

Responder · Responder a todos · Reenviar
Vie 28/08/2026 17:57

Matriz_Escalamiento_MDS_Min...
2 MB

Buen día para todos:

Reciban un cordial saludo.

Adjunto la última versión de la **Matriz de Escalamiento de la MDS**, en la cual se realizaron las siguientes actualizaciones:

- Actualización del listado de **usuarios VIP**.
- Inclusión de las **nuevas categorías en el árbol de Incidentes de Seguridad**.
- Incorporación de las siguientes **novedades relacionadas con el personal**:

Fecha de envío matriz	Novedades reportadas
28/08/2026	Se retira de la matriz a Dayana Marcela Roa, por lo tanto, los temas tratados por ella serán atendidos por Paola Barrea y Gabriela Gonzalez.
28/08/2026	Se incluye en la matriz al Agente de MDS Almeciga Alfonso Jair Steveen.
28/08/2026	Se incluye en la matriz al Agente de MDS Castro Paez, Juan Camilo.
28/08/2026	Se incluye en la matriz al Especilista .Net Toledo Pinzon, Juan Camilo

En esta matriz podrán encontrar los siguientes puntos, entre ellos el listado actualizado con nombres de contacto y cargo del personal asignado al proyecto MinTrabajo:

Trabajo

Unión Temporal Gestión TIC 2023

MATRIZ DE ESCALAMIENTO MESA DE SERVICIOS MINTRABAJO

MATRIZ DE ESCALAMIENTO MDS

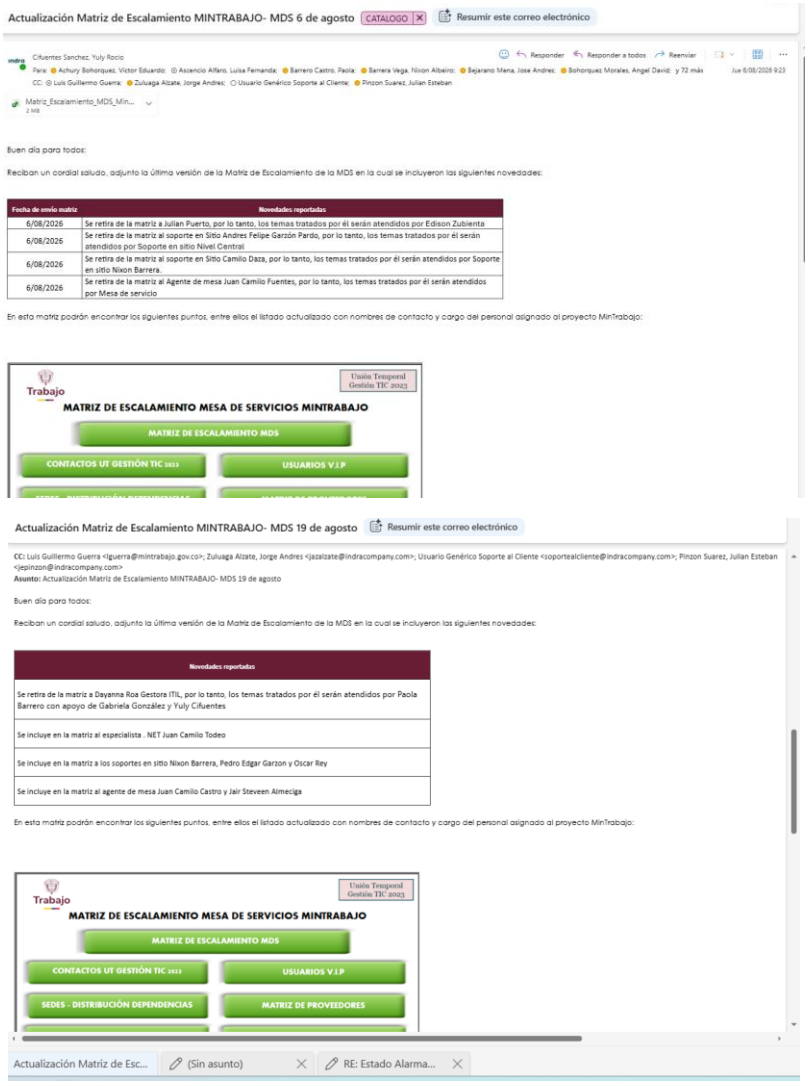
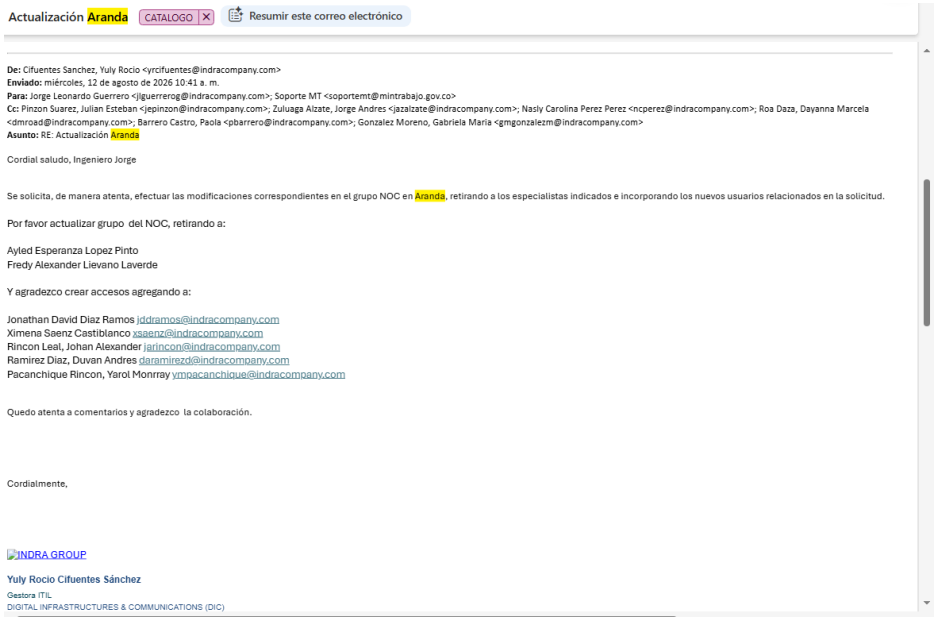


Ilustración 4 Matriz de escalamiento


Actualización Aranda CATALOGO Resumir este correo electrónico

De: Cifuentes Sanchez, Yuly Rocio <yrcifuentes@indracompany.com>
Enviado: miércoles, 12 de agosto de 2026 10:41 a. m.
Para: Jorge Leonardo Guerrero <jlguerrerog@indracompany.com>; Soporte MT <soportemt@mintrabajo.gov.co>
Cc: Pinzon Suarez, Julian Esteban <jepinzon@indracompany.com>; Zuluaga Alzate, Jorge Andres <jazalzate@indracompany.com>; Nasly Carolina Perez Perez <ncperez@indracompany.com>; Roa Daza, Dayanna Marcela <dmroad@indracompany.com>; Barrero Castro, Paola <pbarrero@indracompany.com>; Gonzalez Moreno, Gabriela Maria <gmgonzalezm@indracompany.com>
Asunto: RE: Actualización Aranda

Cordial saludo, Ingeniero Jorge

Se solicita, de manera atenta, efectuar las modificaciones correspondientes en el grupo NOC en Aranda, retirando a los especialistas indicados e incorporando los nuevos usuarios relacionados en la solicitud.

Por favor actualizar grupo del NOC, retirando a:

Ayled Esperanza Lopez Pinto
Fredy Alexander Lievano Laverde

Y agradezco crear accesos agregando a:

Jonathan David Diaz Ramos jddramos@indracompany.com
Ximena Saenz Castiblanco xsaenz@indracompany.com
Rincon Leal, Johan Alexander jarincon@indracompany.com
Ramirez Diaz, Duvan Andres daramirezd@indracompany.com
Pacanchique Rincon, Yarol Monrray ympacanchique@indracompany.com

Quedo atenta a comentarios y agradezco la colaboración.

Cordialmente,

INDRA GROUP
Yuly Rocio Cifuentes Sánchez
Gestora ITIL
DIGITAL INFRASTRUCTURES & COMMUNICATIONS (DIC)

Ilustración 5 Actualización grupo NOC

- **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 agosto se continuó con el seguimiento a la correcta categorización de los casos registrados en la herramienta de gestión, verificando la aplicación de las categorías y criterios definidos.

Este seguimiento permitió fortalecer la correcta utilización del árbol de categorías, promover la estandarización en el registro de los casos y contribuir a la calidad y confiabilidad de la información utilizada para la gestión y generación de indicadores.

- **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	N/A

Tabla 8 KPI Práctica Catálogo de Servicios

- Con el propósito de medir la oportunidad en la atención de las solicitudes relacionadas con la actualización y mantenimiento de los elementos gestionados en la herramienta

Aranda, durante el mes de agosto se realizó la medición del indicador Porcentaje de Cumplimiento de la Actualización del Catálogo (CPS).

- Durante el periodo no se presentaron solicitudes de modificación del árbol de categorías del Catálogo de Servicios. No obstante, se recibió y gestionó una solicitud relacionada con la actualización del grupo NOC en Aranda, que contempló el retiro de especialistas y la incorporación de nuevos usuarios, de acuerdo con las novedades reportadas.

Resultado: No aplica (0/0). Durante el mes de agosto no se recibieron solicitudes relacionadas con la creación, modificación o desactivación de servicios o elementos del Catálogo de Servicios. Las gestiones realizadas durante el periodo correspondieron a la actualización de usuarios y grupos de atención en Aranda, actividad que no se encuentra contemplada dentro del alcance definido para la medición del presente indicador.

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 **agosto** se dio continuidad al análisis de tendencias del catálogo, orientado a realizar seguimiento a la implementación de las mejoras efectuadas en el mes de julio, evaluar su adopción por parte de los equipos responsables y fortalecer la calidad, consistencia y trazabilidad de la información registrada en la herramienta de gestión.

Comportamiento del catálogo

Durante el periodo se evidenció una tendencia hacia la consolidación de las nuevas categorías de Incidentes de Seguridad de la Información implementadas en Aranda durante el mes de julio. En este contexto, se realizó la socialización de las categorías y lineamientos de atención con los grupos del SOC, Mesa de Servicios, Soporte en Sitio de la Sede Central y Soporte en Sitio de las Territoriales, fortaleciendo su aplicación en la clasificación y gestión de los casos.

Afinamientos realizados sobre las categorías

Con el fin de fortalecer la calidad de la información, la correcta asignación y el escalamiento de los casos, durante el periodo se realizaron las siguientes acciones:

- Seguimiento a la correcta utilización de las 15 nuevas categorías de Incidentes de Seguridad de la Información.
- Actualización y socialización de la Matriz de Escalamiento en tres oportunidades durante el mes.
- Configuración de los grupos responsables de apoyo y escalamiento en Aranda para la gestión de tareas por parte del SOC.
- Actualización del grupo NOC en Aranda, mediante el retiro e incorporación de especialistas de acuerdo con las novedades reportadas.

Variaciones identificadas

El análisis permitió identificar que durante agosto las principales variaciones estuvieron relacionadas con la actualización de responsables y mecanismos de escalamiento,

derivadas de novedades de personal, cambios en los usuarios VIP y la incorporación de las nuevas categorías de Seguridad de la Información. No se presentaron nuevas modificaciones estructurales al árbol de categorías durante el periodo.

Impacto en el proceso

Las acciones realizadas permitieron consolidar las mejoras implementadas en el mes anterior, fortalecer la correcta clasificación y trazabilidad de los incidentes de seguridad y mejorar los mecanismos de asignación y escalamiento hacia los grupos especializados. Asimismo, la actualización periódica de la Matriz de Escalamiento contribuyó a mantener información vigente y acorde con las necesidades de la operación.

Acciones de mejora

Como resultado del análisis de tendencias, se establecieron las siguientes acciones:

- Continuar con el seguimiento a la correcta categorización de los incidentes de Seguridad de la Información.
- Mantener actualizada la Matriz de Escalamiento frente a las novedades de personal, usuarios VIP y cambios en los grupos responsables.
- Verificar periódicamente la correcta configuración de los grupos de apoyo y escalamiento en Aranda.
- Continuar fortaleciendo la socialización de las categorías y lineamientos de atención con los equipos involucrados.
- Mantener el análisis de tendencias como mecanismo de seguimiento y mejora continua del Catálogo de Servicios.

2.1.2.5. Práctica de Problemas

Dar a conocer las actividades de la Práctica de Problemas correspondientes al periodo de agosto 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 durante la vigencia del contrato:

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 agosto se realizó seguimiento al caso 174025 asociado con el Gestor Documental. De acuerdo con la sesión de trabajo realizada el 24 de agosto se definieron las acciones que se va a adelantar:

Acciones propuestas y la nueva hoja de ruta:

1. Seguimiento al caso TS022469468 registrado ante IBM Responsable: Jimmer
2. 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 y de aplicación en la primera semana de septiembre . Responsable: Especialista DBA Oracle y Especialista IBM
- Revisión de las notas técnicas de IBM Responsables: Especialistas Nube Privada

3. Sesión de seguimiento 17 de septiembre.

2.1.2.6. Práctica de Incidentes

Durante el mes, se gestionaron en la Herramienta de Gestión un total de 7.145 solicitudes a nivel general; de este total, el 12.06%, equivalente a 592 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 todos los niveles de escalamiento ante solicitudes recibidas en el desempeño y operación de los servicios.
- 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:

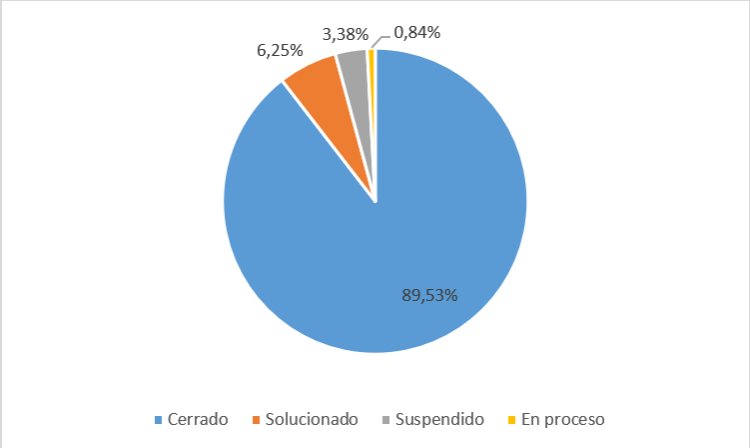


Ilustración 6 Estados Incidentes

- **Categorización de Incidentes por Servicio**

Durante agosto de 2026 se registraron 592 incidentes, evidenciando una mayor concentración en los servicios de Redes y Conectividad, Aplicaciones Especializadas y Soporte Microinformática, que en conjunto representan aproximadamente el 93,4 % de los casos reportados.

En Redes y Conectividad, los eventos asociados a Router, Starlink, FortiGate, AP y Switch corresponden principalmente a alertas generadas por el monitoreo Zabbix ante pérdida de comunicación o disponibilidad de los dispositivos en las sedes. De los 386 incidentes registrados en el servicio, 382 (98,96 %) tienen como causal registrada falla de energía eléctrica, 3 (0,78 %) desconexión o apagado físico de equipos y 1 (0,26 %) bloqueo de dispositivo

En Aplicaciones Especializadas, se presentaron 85 incidentes (14,4 %), con mayor participación de casos relacionados con aspectos funcionales y procesos de radicación del Gestor Documental. Este comportamiento evidencia la importancia de continuar con el seguimiento de las causas recurrentes y las oportunidades de estabilización del servicio, así como de reforzar el uso adecuado de los flujos y funcionalidades por parte de los usuarios, con el fin de prevenir errores operativos que puedan generar reportes e incidentes.

Por su parte, Soporte Microinformática registró 82 incidentes (13,9 %), destacándose casos relacionados con impresoras, equipos de cómputo, Office 365 y navegadores. Estos incidentes pueden responder a diferentes causales, incluyendo condiciones físicas o mecánicas de los equipos, configuración, disponibilidad, aspectos asociados al uso y otras condiciones operativas. En este sentido, se identifican oportunidades para fortalecer las acciones preventivas, el análisis de recurrencia y la documentación de soluciones conocidas, diferenciando las situaciones atribuibles directamente al servicio de aquellas que requieren gestión con otras áreas, usuarios o terceros.

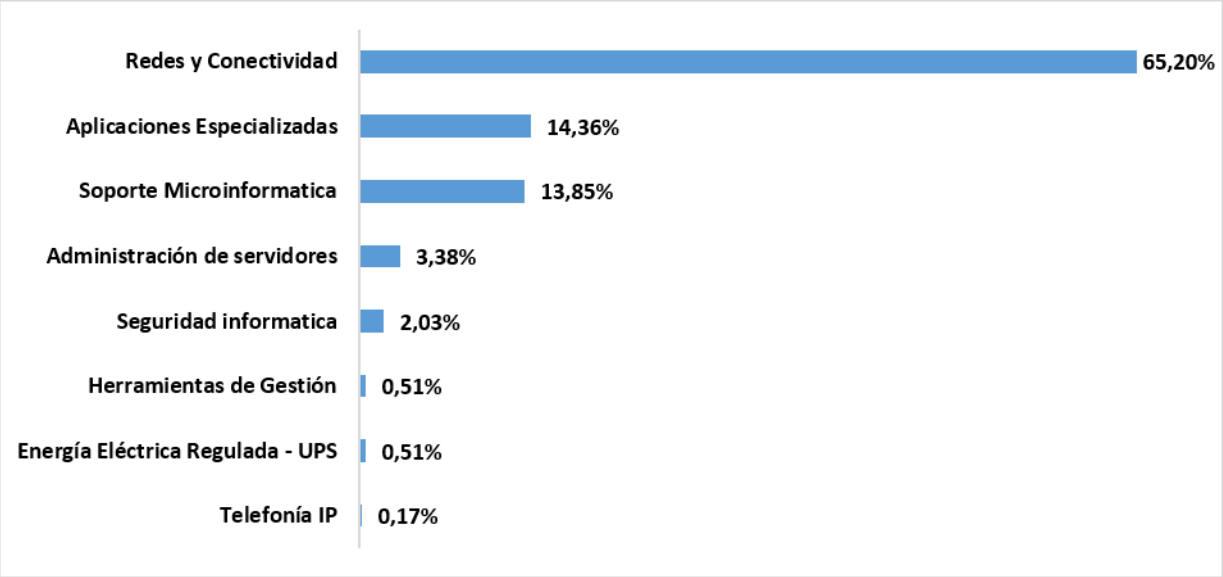


Ilustración 7 Categorización de Incidentes por Servicio

Servicio	Categoría	No	Porcentaje
Redes y Conectividad		**386**	
	Reportar una falla.Alarma Zabbix.Router	204	34,46%
	Reportar una falla.Alarma Zabbix.Starlink	85	14,36%
	Reportar una falla.Alarma Zabbix.FortiGate	61	10,30%
	Reportar una falla.Alarma Zabbix.AP	18	3,04%
	Reportar una falla.Alarma Zabbix.Switch	14	2,36%
	Reportar una falla.Internet.Sin servicio	2	0,34%
	Reportar una falla.LAN.Falla punto de red	2	0,34%
Aplicaciones Especializadas		**85**	
	Reportar una falla.Gestor Documental.Falla Funcional	49	8,28%
	Reportar una falla.Gestor Documental.Falla radicación	28	4,73%
	Reportar una falla.Gestor Documental.Falla - Error PQRSD	3	0,51%
	Reportar una falla.Gestor Documental.No permite Aprobar y radicar	2	0,34%
	Reportar una falla.Gestor Documental.Falla Error – Datacap	1	0,17%
	Reportar una falla.Gestor Documental.No genera sticker	1	0,17%
	Reportar una falla.Incidente Mayor	1	0,17%
Soporte Microinformatica		**82**	
	Reportar una falla.Falla impresora.No imprime	23	3,89%
	Reportar una falla.Falla impresora.Atasco	12	2,03%
	Reportar una falla.Equipo de computo.Falla - Error conexión a red	7	1,18%
	Reportar una falla.Ofimatica.Falla Aplicaciones Office 365	7	1,18%
	Reportar una falla.Equipo de computo.Lentitud – Bloqueo	6	1,01%
	Reportar una falla.Aplicaciones Office 365.Envio y recepción de correos	6	1,01%

Servicio	Categoría	No	Porcentaje
	Reportar una falla.Equipo de computo.No enciende	5	0,84%
	Reportar una falla.Navegadores.Falla – Error	5	0,84%
	Reportar una falla.Navegadores.Bloqueo Navegador	2	0,34%
	Reportar una falla.Equipo de computo.Falla de sistema operativo	1	0,17%
	Reportar una falla.Falla impresora.Daño físico	1	0,17%
	Reportar una falla.Falla impresora.No Escanea	1	0,17%
	Reportar una falla.Monitor Pc.Falla- Error	1	0,17%
	Reportar una falla.Monitor Pc.No enciende	1	0,17%
	Reportar una falla.Mouse - Teclado - Base - Diadema.Falla General	1	0,17%
	Reportar una falla.Navegadores.Falla Cargue pagina web	1	0,17%
	Reportar una falla.Ofimatica.Falla Excel	1	0,17%
	Reportar una falla.VPN.Falla aplicación	1	0,17%
Administración de servidores		**20**	
	Reportar una falla.Alarma Zabbix.Servidor Windows	17	2,87%
	Reportar una falla.Alarma Zabbix.Servidor Linux	2	0,34%
	Reportar una falla.Directorio Activo.Falla autentificcion de usuario	1	0,17%
Energía Eléctrica Regulada - UPS		**3**	
	Reportar una falla.Alarma Zabbix.UPS	3	0,51%
Herramientas de Gestión		**3**	
	Reportar una falla.Monitoreo Zabbix.Alarma desde Zabbix	3	0,51%
Seguridad informática		**12**	
	Reportar una falla.Soporte Antivirus.Falla – error	6	1,01%
	Reportar una falla.Alarma Zabbix.Seguridad Informática	3	0,51%
	Reportar una falla.Escaneo de redes.Exploración de puertos o servicios autorizada	2	0,34%
	Reportar una falla.Soporte Antivirus.Incidente por Malware	1	0,17%
Telefonía IP		**1**	
	Reportar una falla.Incidente Mayor	1	0,17%
Total general		**592**	

Tabla 10 Categorización de Incidentes por Servicio

- **Top 10 de Incidentes**

El análisis del Top 10 de incidentes evidencia una concentración de casos en las jerarquías asociadas al monitoreo de Router, Starlink y FortiGate, que representan conjuntamente el 68,49 % de los incidentes incluidos en el Top 10. Estos resultados permiten identificar los componentes con mayor recurrencia para orientar el seguimiento de las causas y las acciones de mejora.

Redes y Conectividad concentra la mayor afectación, especialmente en las jerarquías Router (39,92%), Starlink (16,63%) y FortiGate (11,94%). En conjunto, estas tres jerarquías representan 68,49% de los incidentes reportados, constituyéndose como los principales

componentes involucrados y, por tanto, como referentes para el seguimiento y análisis de recurrencia.

En Aplicaciones Especializadas, los incidentes se concentran en el Gestor Documental, principalmente en aspectos funcionales y procesos de radicación. Además del seguimiento a las causas recurrentes y oportunidades de estabilización, resulta importante reforzar el uso adecuado de los flujos y funcionalidades por parte de los usuarios, como medida preventiva frente a errores operativos que puedan generar reportes.

En Soporte Microinformática, los incidentes se concentran en la operación y disponibilidad de los equipos de impresión, particularmente en casos de no impresión y atascos. Las causas pueden estar relacionadas con condiciones físicas o mecánicas, configuración, disponibilidad de los equipos o aspectos asociados al uso, por lo que se recomienda diferenciar aquellas situaciones atribuibles directamente al servicio de las que requieren gestión sobre los equipos, usuarios u otras condiciones operativas.

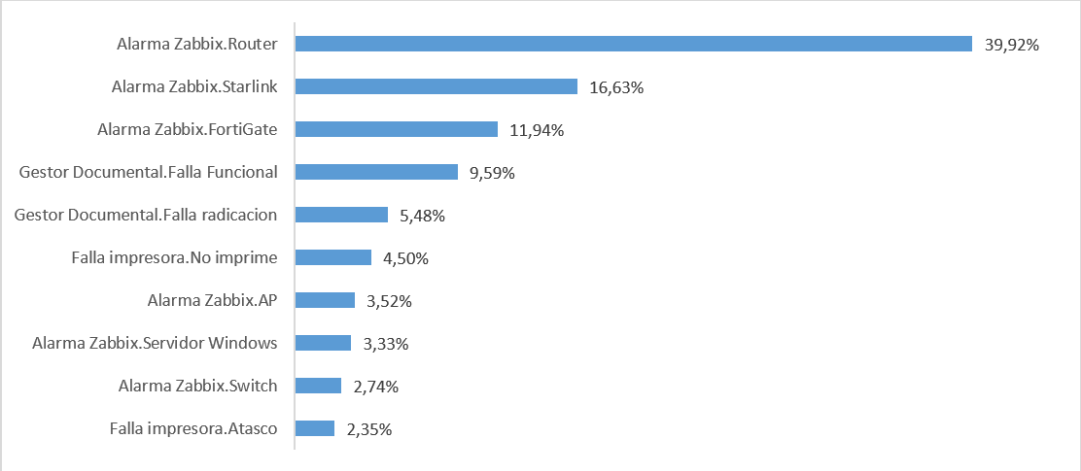


Ilustración 8 Top 10 Incidentes

Servicio	Jerarquía	Incidentes	Porcentaje	Principales causas	Análisis
Redes y Conectividad	Alarma Zabbix – Router	**204**	**39,92%**	Desconexión o apagado físico de equipos en sede, fallas en la red del proveedor y fallas de energía eléctrica.	Es la jerarquía con mayor número de incidentes, evidenciando una alta dependencia de la infraestructura de comunicaciones y de factores externos como energía y proveedores.
Redes y Conectividad	Alarma Zabbix – Starlink	**85**	**16,63%**	Desconexión física, fallas en la red del proveedor, fallas de energía eléctrica e intermitencia o lentitud en la red.	Segunda jerarquía con mayor afectación. Los incidentes están asociados principalmente a la disponibilidad del servicio satelital, conectividad y energía.
Redes y Conectividad	Alarma Zabbix – FortiGate	**61**	**11,94%**	Principalmente fallas de energía eléctrica y pérdida de comunicación con el dispositivo.	Las afectaciones impactan la disponibilidad de los dispositivos de seguridad perimetral y la continuidad de la conectividad.

Servicio	Jerarquía	Incidentes	Porcentaje	Principales causas	Análisis
Redes y Conectividad	Alarma Zabbix - AP	**18**	**3,52%**	Bloqueo del dispositivo, desconexiones físicas, fallas eléctricas e intermitencia en la red.	Aunque presenta una menor participación, evidencia oportunidades de mejora en la estabilidad y disponibilidad de la red inalámbrica.
Redes y Conectividad	Alarma Zabbix - Switch	**14**	**2,74%**	Fallas de energía eléctrica, desconexión física y pérdida de comunicación.	Los eventos afectan la conectividad interna de las sedes y están relacionados con disponibilidad de equipos e infraestructura.
Aplicaciones Especializadas	Gestor Documental - Falla Funcional	**49**	**9,59%**	Fallas funcionales y errores durante la operación del Gestor Documental.	Es la principal jerarquía del servicio, afectando directamente la operación de los usuarios y el procesamiento de documentos.
Aplicaciones Especializadas	Gestor Documental - Falla Radicación	**28**	**5,48%**	Errores durante el proceso de radicación y dificultades en el procesamiento de documentos.	Las incidencias impactan los procesos de gestión documental y pueden generar retrasos en la continuidad operativa.
Soporte Microinformática	Falla Impresora - No Imprime	**23**	**4,50%**	Fallas de impresión, indisponibilidad del equipo y degradación del servicio.	Principal afectación del servicio de microinformática, generando indisponibilidad del servicio de impresión para los usuarios.
Soporte Microinformática	Falla Impresora - Atasco	**12**	**2,35%**	Atasco de papel, problemas mecánicos e impresión deficiente.	Los incidentes corresponden principalmente a problemas físicos y mecánicos de las impresoras.
Administración de servidores	Alarma Zabbix - Servidor Windows	**17**	**3,33%**	Alertas asociadas a disponibilidad, rendimiento o comportamiento anómalo de servidores Windows.	Los eventos evidencian la importancia del monitoreo preventivo mediante Zabbix para identificar oportunamente condiciones que puedan afectar la disponibilidad de los servidores.

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 19 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	14
Especialista Aplicaciones .Net	2
Responsable_Soporte_Impresoras	2
Especialista Nube Privada	1
Total general	**19**

Tabla 12 Incidentes Suspendidos

La distribución de los 19 incidentes suspendidos evidencia una alta concentración en el NOC, con 14 casos (73,68%). Los demás grupos presentan una participación significativamente menor: Especialista Aplicaciones .Net y Responsable_Soporte_Impresoras, con 2 casos cada uno (10,53%), y Especialista Nube Privada, con 1 caso (5,26%).

- **Incidentes Mayores**

Durante el período se gestionaron tres (3) Incidentes Mayores, asociados a los servicios de Telefonía IP, Redes y Conectividad y Navegadores. Las afectaciones estuvieron relacionadas con una incidencia en la troncal SIP, un evento sísmico que afectó infraestructura de fibra óptica y una falla intermitente de navegación asociada a Mozilla Firefox. Dos (2) incidentes fueron restablecidos y uno (1) permanecía en investigación al cierre del período

Incidente Aranda	Fecha/Hora	Asunto	Acciones realizadas durante la atención del incidente	Causa raíz	Usuarios afectados	Fecha/ Hora fin	Estado
IM-297886	06/08/2026 07:28	Indisponibilidad en la recepción de llamadas del Ministerio de Trabajo	Se realizaron pruebas y se escaló el caso al especialista y proveedor para atención prioritaria.	Incidencia en la **troncal SIP**, afectando el ingreso y salida de llamadas.	Toda la entidad, afectando el servicio de telefonía.	10/08/2026 14:52	Cerrado
IM-303437	10/08/2026 08:30	Afectación masiva de comunicaciones luego de terremoto en Colombia	Se coordinó con ETB la atención y reparación de la infraestructura afectada, validando posteriormente la conectividad.	Sismo que ocasionó fractura de pigtails de fibra óptica en la Central Santa Mónica.	Sedes de Valle, Roldanillo, Pereira, Istmina, Armenia y Quibdó.	13/08/2026 2:12	Cerrado
IM-328407	31/08/2026 08:35	Falla/Bloqueo navegador Mozilla Firefox por ZTNA	Se realizaron pruebas en diferentes equipos, navegadores y redes, validando DNS, filtrado web y listas blancas.	En investigación. Se identificaron eventos HTTP 429 y posibles bloqueos por exceso de solicitudes.	Usuarios con acceso a plataformas web mediante Mozilla Firefox, con afectación intermitente.	En investigación	En investigación

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=591/593*100 EF= 99.66%
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=0/593*100 RRP= 0,00%

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

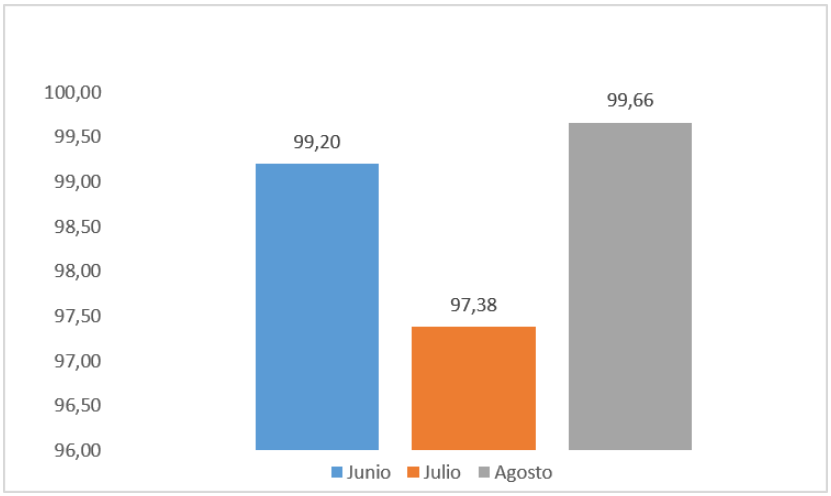


Ilustración 9 Efectividad de resolución de incidentes

Se evidencia un desempeño favorable durante el trimestre, manteniendo resultados superiores al 97%. Los resultados fueron 99,20% en junio, 97,38% en julio y 99,66% en agosto.
En agosto se observa una recuperación significativa del indicador, con un incremento de 2,28 puntos porcentuales frente a julio, alcanzando el resultado más alto del trimestre. Este comportamiento refleja la efectividad de las actividades de atención, seguimiento y resolución de incidentes.

El resultado obtenido evidencia una adecuada capacidad operativa de los equipos para gestionar los incidentes y mantener la continuidad de los servicios, incluso ante eventos de mayor complejidad registrados durante el período.
Se continuará fortaleciendo el monitoreo, seguimiento preventivo, análisis de tendencias y gestión de causas recurrentes, con el propósito de mantener el desempeño del indicador y contribuir a la estabilidad y calidad de los servicios.

Durante el período evaluado, el indicador Porcentaje de Incidentes Reabiertos presentó un comportamiento favorable, manteniéndose en 0,00 % durante junio y agosto, mientras que en julio registró un 0,14 %, correspondiente a la reapertura de un único incidente (IM-291546).

La reapertura registrada en agosto se realizó como parte del proceso de validación y actualización de la causa de la afectación. Inicialmente, la indisponibilidad fue asociada a un evento relacionado con el suministro de energía; sin embargo, posterior a la confirmación obtenida con el soporte en sitio, se determinó que la interrupción obedecía a la desconexión programada de los equipos por actividades de traslado, información que no se encontraba disponible al momento del cierre inicial.

La reapertura permitió actualizar la causa real del incidente y garantizar la trazabilidad, consistencia 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 efectividad en la Gestión de Incidentes, con un porcentaje de reaperturas prácticamente nulo durante el período analizado. La única reapertura registrada respondió a una actividad de validación técnica y actualización de la causa raíz, y no a una solución inefectiva del incidente.

En conclusión, el resultado de 0,00 % en junio, 0,14 % en julio y 0,00 % en agosto demuestra estabilidad en la gestión y cierre de los incidentes, así como el compromiso de los equipos de soporte con la calidad de la información, la trazabilidad de los casos y la mejora continua.

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

Durante el mes de agosto, como parte de las actividades de fortalecimiento del proceso de Gestión de Incidentes de Seguridad de la Información, se realizaron las socializaciones correspondientes con las áreas que interactúan en la gestión de este tipo de incidentes.
En estas jornadas se presentaron los lineamientos establecidos para la Gestión de Incidentes de Seguridad de la Información, así como los criterios relacionados con la identificación, reporte, clasificación, atención y seguimiento de los incidentes.

Asimismo, se socializó la estructura de categorías definida para la gestión de los incidentes en la herramienta Aranda, con el propósito de que las áreas involucradas conozcan su aplicación y puedan realizar una correcta clasificación de los casos de acuerdo con los lineamientos establecidos.

Las socializaciones permitieron fortalecer el conocimiento y apropiación del proceso por parte de las áreas involucradas, aclarar responsabilidades y resolver inquietudes relacionadas con la interacción entre los diferentes equipos durante la gestión de los 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 agosto 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 5024 casos tipo requerimiento quedando en los siguientes estados:

Estado	Casos
Cerrado	4452
En proceso	98
Reabierto	2
Registrar	4
Solucionado	330

Suspendido	138

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 1507 tareas, las cuales fueron gestionadas en los siguientes estados:

Estado	Task
Asignada	137
Finalizada	1370

Tabla 16 Estados de Tareas de requerimientos

- Durante el mes, no se presentaron casos anulados.
- 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	Julio	Agosto
SOC	3	4
Especialista Aplicaciones .Net	0	2
Gestor de Inventarios	1	0
Responsable_De_Servidores_Windows	3	5
Especialistas IBM	8	0
Liferay	0	1
Especialista Nube Privada	2	7
Especialista Nube Publica	1	1
Responsable Garantías Equipos	18	15
Responsable_Soporte_Territoriales	17	26
Responsable_Soporte_Impresoras	6	11
Responsable_Soporte_Bogotá	15	27
Responsable_Mesa_de_Servicio	59	44
Especialista Base de datos	1	0
NOC	0	14
Total por Periodo	**134**	**157**

Tabla 17 Seguimiento del Backlog Suspendidos

En el inicio del período, se identificaron 134 casos suspendidos correspondientes al backlog del mes de julio de 2026, lo cual se presenta un aumento de solicitudes este periodo de 23 casos suspendidos respecto al mes de agosto. Sin embargo, el 28% de las suspensiones de agosto (44 de 157 casos) se concentra en responsable Mesa de Servicio (44 casos) y Responsable Soporte en Sitio (27casos), 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.Impresora.Cargue de papel en impresora	429
Radicar una solicitud.Equipo de computo.Traslado de Sede, Cambio Equipo o Rol	324
Radicar una solicitud.Alarma Zabbix.Impresora	278

Radicar una solicitud.Directorio activo.Cambiar contraseña	214
Radicar una solicitud.Impresora.Aumento de cuota	195
Radicar una solicitud.Impresora.Instalacion - Configuracion	174
Radicar una solicitud.Gestor documental.Relanzamiento	160
Radicar una solicitud.Directorio activo.Creacion de usuario	158
Radicar una solicitud.Evento Fortisiem.Seguridad Informática	148
Radicar una solicitud.Impresora.Cargue de papel en impresora	429

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 1286 tickets, cargue de papel en impresora con 429 tickets, Traslado de Sede, Cambio Equipo o Rol 324 ticketsAlarma Zabbix de Impresora con 278 tickets y Cambiar contraseña con 214 tickets.
- Se realizó seguimiento a requerimientos en backlog, enviando correos a los especialistas para la documentación y cierre de casos pendientes.
- 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=** 4974/5024 *100
	EF: Efectividad en solución de Requerimientos.			
	RFS: Requerimientos solucionados que cumplen el ANS en el período.			**EF= 99,00%**
	RFR: Requerimientos registradas en el período.			
Porcentaje de Requerimientos Reabiertos en el Periodo	**RRP:** Porcentaje de casos Reabiertos en el periodo.	<2%	Mensual	**RRP=** 2/4782*100
	RFR: Requerimientos Reabiertos en el período.			**RRP= 0,04%**
	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:

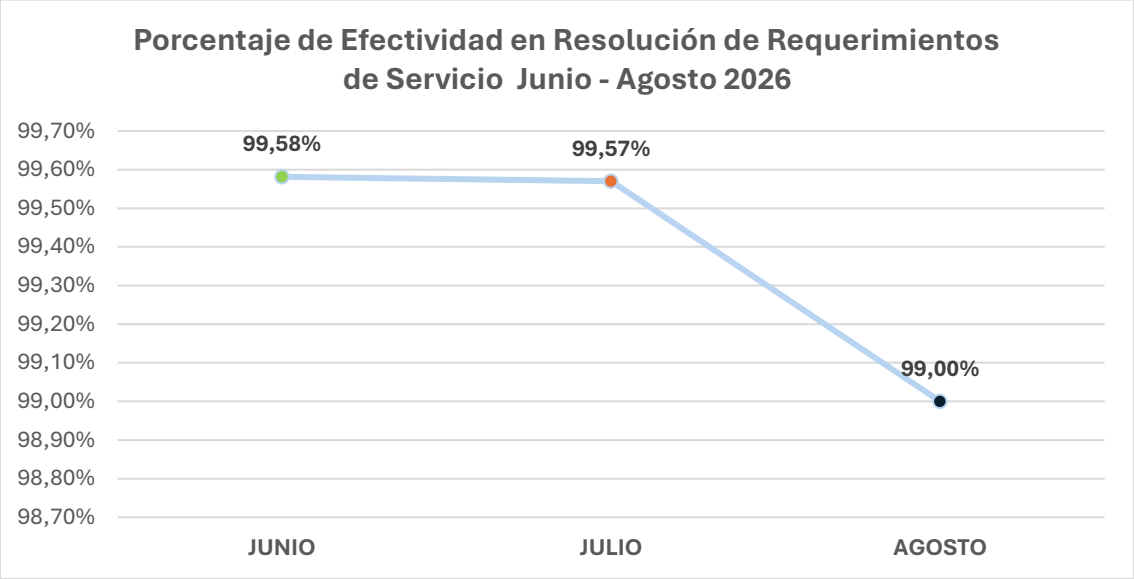


Ilustración 10 KPI Efectividad de Resolución de Requerimientos de Servicio

Durante el periodo comprendido entre junio y agosto de 2026, el indicador de efectividad en la resolución de requerimientos presentó un comportamiento estable y superior al 99,00%, evidenciando un alto nivel de cumplimiento en la atención y cierre de las solicitudes de servicio, 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.

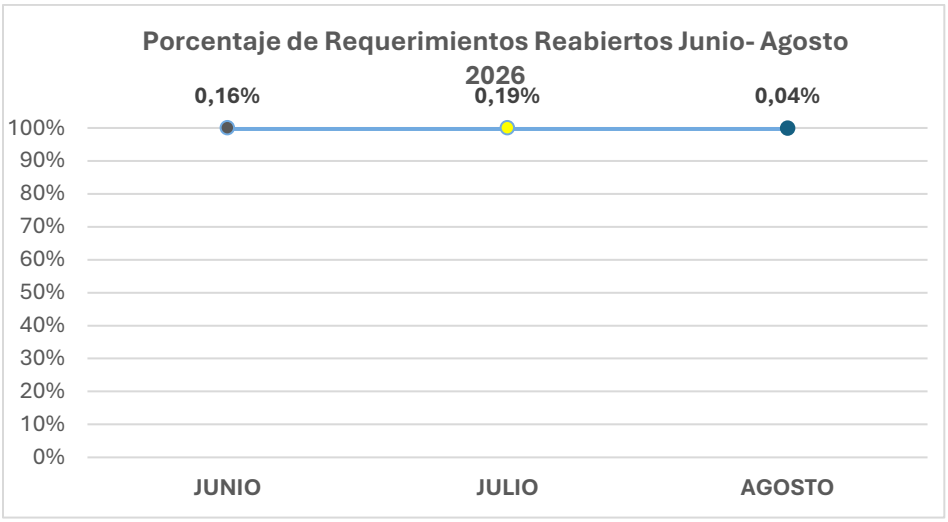


Ilustración 11 Requerimientos de Reabiertos en el periodo

Durante el mes de agosto de 2026 se gestionaron 5.024 requerimientos de servicio, de los cuales 4782 casos (95.18%) fueron resueltos satisfactoriamente sin necesidad de reapertura, mientras que únicamente 2 casos (0.039%) requirieron ser reabiertos pasando de 0,19% a 0,04%, 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 99,6% 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 dos (2) 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-326572	Usuario: jpalomino@mintrabajo.gov.co Nombre: Jose Luis Palomino Rivillas Territorial o piso: DT Valle Trabajando desde: Casa Observaciones: Usuario indico que requiere acompañamiento para la instalacion y configuracion del aplicativo fortclient, el cual indico que se pueden contactar en el aplicativo de teams.	Responsable_Soporte_Territoriales	El caso fue escalado con información incompleta y el técnico de soporte en sitio lo documentó con esa información	La mesa de servicios ajusta el caso y completa la información, el técnico de soporte en sitio atiende el caso con la siguiente documentación*: Se recibe requerimiento por parte del funcionario Jose Luis Palomino Rivillas, quien solicita acompañamiento para la instalación y configuración del aplicativo FortiClient, debido a que se encuentra trabajando desde casa.* *Se brinda el acompañamiento requerido y se realiza la instalación y configuración correspondiente del aplicativo.* *El funcionario confirma que el servicio queda funcionando correctamente.* *El caso queda solucionado, atendido y cerrado.*
RF-328706	Ing muy buenas tardes ¿Podría informarme el día de mañana a qué hora nos reunimos? Para el proceso pendiente.	Responsable_Mesa_De_Servicio	El caso fue creado con la funcionalidad de correo electrónico de aranda donde el técnico de soporte en sitio le solicita al usuario disponibilidad para finalizar el alistamiento de la máquina	Se procede con el cierre del caso, el cual corresponde a una solicitud de tipo informativo. La gestión se realiza en el marco del caso RF-308854, brindando retroalimentación basada en la información previamente enviada por el usuario. Con esto, se da por finalizada la atención de la solicitud.

Tabla 20 Casos reabiertos

2.1.2.8. Práctica de Eventos

El presente informe resume las actividades de monitoreo proactivo ejecutadas por el Centro de Operaciones de Red (NOC) sobre la infraestructura tecnológica del Ministerio del Trabajo durante el mes de agosto. La labor desarrollada por el Centro de Diagnóstico y Operaciones (CDO) permitió identificar y gestionar oportunamente un total de 434 eventos, evidenciando la capacidad de monitoreo y respuesta frente a condiciones que pueden afectar la continuidad operativa de los servicios de TI.

Los Routers constituyeron la categoría con mayor número de eventos, con 210 casos (48% del total), principalmente asociados a fallas de energía eléctrica, desconexiones o apagados físicos de equipos, fallas en la red del proveedor e intermitencias. Este comportamiento se

concentra especialmente en sedes remotas o con condiciones de suministro eléctrico inestables.

Starlink ocupó el segundo lugar, con 86 eventos (19,8%). Aunque se evidencia una disminución frente a periodos anteriores, las fallas eléctricas y la desconexión física de los equipos continúan siendo los principales factores asociados.
FortiGate registró 61 eventos (14,6%), presentando una disminución frente al mes anterior.

Los principales factores estuvieron relacionados con fallas de energía comercial, desconexiones físicas e intermitencias. Los servidores Windows registraron 41 eventos (9,45%), con predominio del alto consumo de memoria; los servidores Linux registraron 4 eventos (0,92%). Access Point presentó 18 eventos (4,15%) y Switch 14 eventos (3,23%).

De manera general, los resultados muestran que las condiciones de energía eléctrica continúan siendo uno de los principales factores externos que generan alertamientos sobre la infraestructura de red. Se recomienda priorizar medidas de respaldo energético en las sedes con mayor recurrencia y fortalecer el seguimiento de los casos que requieren intervención de terceros o del soporte en sitio.

El presente informe evidencia el compromiso del equipo NOC con la continuidad operativa de los servicios de TI mediante una gestión proactiva, orientada a la detección temprana, atención y seguimiento de eventos, así como a la identificación de oportunidades de mejora.

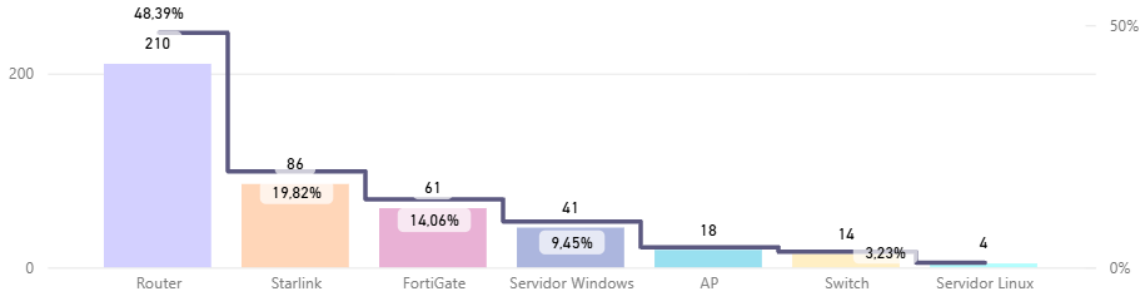


Ilustración 12 Resumen de incidentes

Incidentes por Categoría de Servicio

A continuación, se presenta el desglose de las incidencias gestionadas durante agosto por el equipo NOC, en el marco de las actividades de monitoreo de estado y atención de eventos sobre la infraestructura tecnológica del Ministerio del Trabajo. La gestión comprende la supervisión proactiva y la resolución de eventos asociados a componentes de red e infraestructura informática, con el propósito de contribuir a la continuidad operativa y al cumplimiento de los niveles de servicio establecidos.

Redes y conectividad

Routers

Durante agosto, el NOC gestionó 210 eventos relacionados con equipos de red Routers en diferentes sedes a nivel nacional, equivalentes al 48% del total de casos registrados

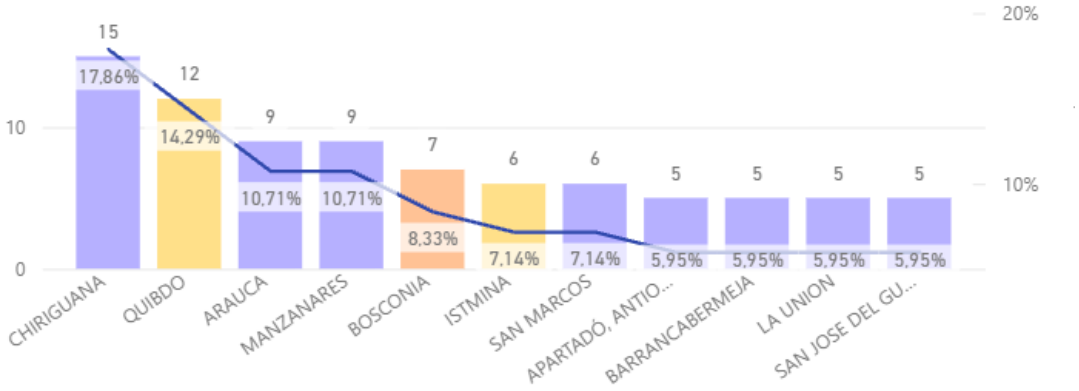


Ilustración 13 Top 10 Sedes afectadas por Router

La sede Chiriguaná presenta una alta recurrencia asociada al apagado de los dispositivos al finalizar la jornada laboral, generando más del 80% de los casos por desconexión, seguido de fallas eléctricas. Quibdó ocupa nuevamente una posición destacada, con más del 75% de sus casos relacionados con fallas eléctricas.

Arauca se mantiene dentro del TOP 10 por tercer mes consecutivo, con eventos relacionados con fallas eléctricas e intermitencias del servicio. Manzanares también registra recurrencia asociada a energía y desconexiones físicas. Bosconia continúa apareciendo en el TOP, principalmente por desconexiones físicas de sus dispositivos de red.

Istmina y San Marcos presentan eventos relacionados principalmente con fallas de energía y desconexiones de equipos. Otras sedes como Apartadó, Barrancabermeja, San José y Unión muestran combinaciones de fallas eléctricas, desconexiones, intermitencias y eventos asociados al proveedor.

La principal causa de los eventos de Routers fue la falla de energía eléctrica, con 130 casos (61,90%). Le siguieron la desconexión o apagado físico de equipos, con 39 casos (18,57%); las fallas en la red del proveedor, con 27 casos (12,86%); y la intermitencia o lentitud de la red, con 14 casos (6,67%).

Las fallas de energía eléctrica representan el principal factor de afectación y se concentran principalmente en sedes remotas o sin mecanismos suficientes de

respaldo energético. Se recomienda priorizar la implementación de UPS y otras alternativas de respaldo en las sedes con mayor recurrencia.

Las fallas asociadas a proveedores representan el 12,86% de los eventos. Arauca concentra la mayor cantidad de casos por esta causa y se observa una disminución frente a periodos anteriores.

Las desconexiones o apagados físicos representan el 18,57%. En varias sedes los funcionarios realizan esta práctica para prevenir daños derivados de posibles picos de energía. Se recomienda reforzar las directrices operativas sobre el manejo de los equipos y evaluar alternativas de protección eléctrica.

Las intermitencias o lentitudes representan el 6,67% y se concentran principalmente en eventos registrados en horario no hábil, con duraciones observadas de entre 15 y 30 minutos.

De los 210 eventos de Routers, 203 (96%) se encuentran cerrados o solucionados y 7 (3,3%) permanecen suspendidos. Los casos suspendidos corresponden a situaciones como cierre o demolición de sedes, escalamiento a proveedor, revisión por soporte en sitio y afectaciones de infraestructura.
Entre los casos suspendidos se encuentran Sevilla, por cierre del edificio debido a demolición; Quibdó, escalado al proveedor de telecomunicaciones y pendiente de respuesta; Manizales, Fonseca y Bosconia, escalados a soporte en sitio; Istmina, sede cerrada sin causa conocida; y Dos Quebradas, afectada por un terremoto y actualmente cerrada.

Adicionalmente, durante el periodo se presentó una afectación extraordinaria asociada al sismo del 10 de agosto de 2026, gestionada bajo el Incidente Mayor IM-303437 – Afectación masiva de comunicaciones. El sismo ocasionó la fractura de pigtails de fibra óptica en la Central Santa Mónica, afectando la conectividad de las sedes de Valle, Roldanillo, Pereira, Istmina, Armenia y Quibdó. Se coordinó con ETB la atención y reparación de la infraestructura afectada, realizando posteriormente la validación de la conectividad.

Este evento corresponde a una afectación de carácter extraordinario asociada a infraestructura y fuerza mayor, por lo que se diferencia de las recurrencias operativas identificadas en las sedes. Su gestión mediante un Incidente Mayor

permitió coordinar de manera centralizada la atención, escalamiento y recuperación del servicio.
En términos generales, los resultados evidencian que la energía eléctrica continúa siendo la principal causa estructural de afectación, seguida de las desconexiones físicas.

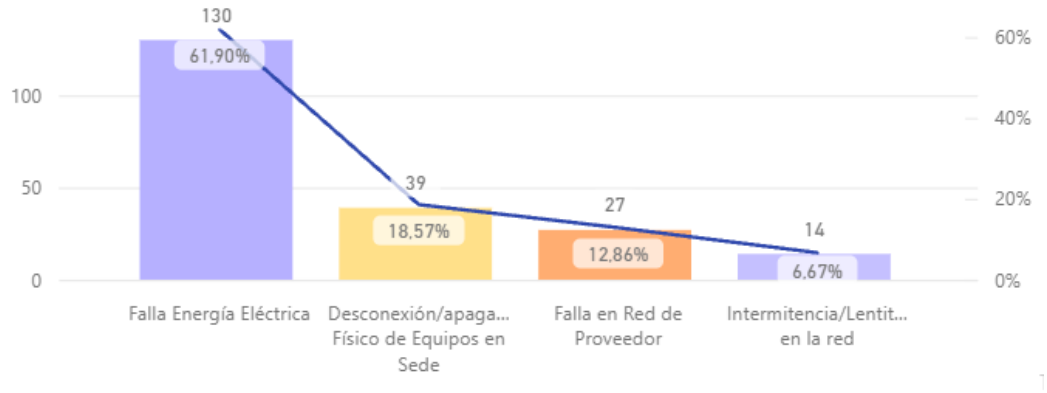


Ilustración 14 Causas de eventos generados por Router

Switch

Durante agosto se registraron 14 eventos relacionados con Switches, equivalentes al 3,23% del total, evidenciándose un incremento frente al mes anterior.

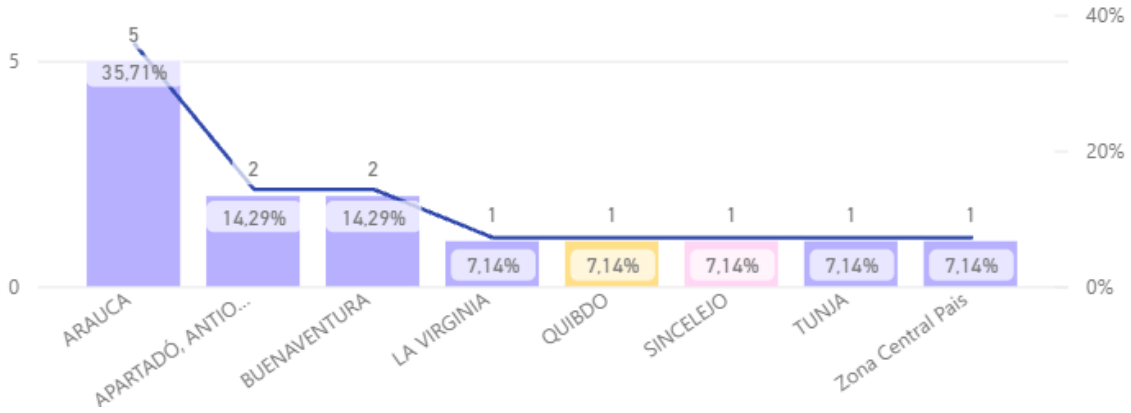


Ilustración 15 Sedes afectadas por Switch

Arauca ocupó el primer lugar con 5 casos, principalmente asociados a fallas eléctricas e intermitencias. Apartadó y Buenaventura registraron 2 casos cada una, con predominio de fallas eléctricas. La Virginia, Quibdó, Sincelejo, Tunja y la zona central del país registraron un caso cada una, principalmente asociado a energía eléctrica.

Las fallas de energía eléctrica representaron el 78% (11 casos). Arauca registró 2 casos (14%) asociados a intermitencia y Apartadó presentó un caso por desconexión física.

La distribución confirma que la inestabilidad del suministro eléctrico continúa siendo un factor predominante para la disponibilidad de la infraestructura de red.

Los 14 eventos registrados se encuentran en estado cerrado o solucionado, correspondiente al 100% de los casos gestionados por el NOC.

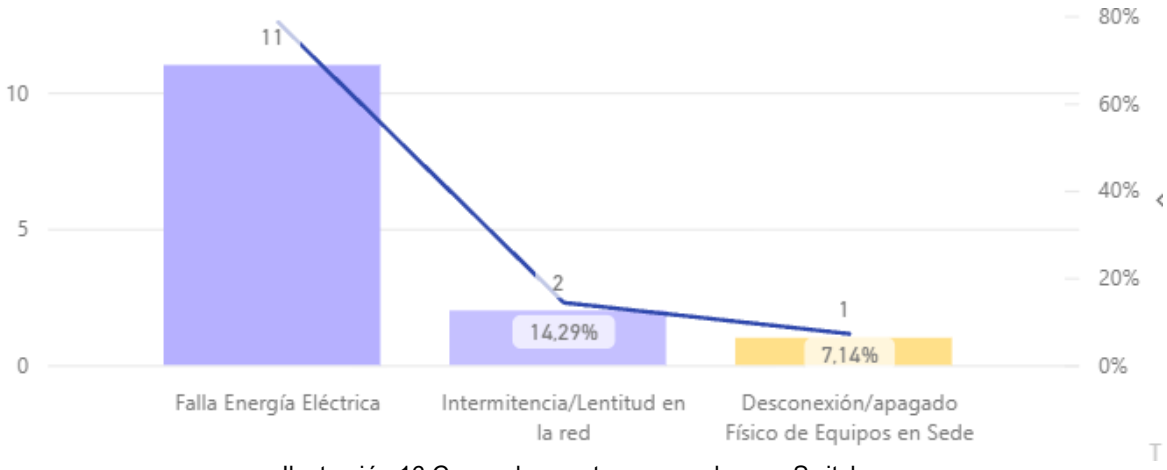


Ilustración 16 Causa de eventos generados por Switch

Access Point

Durante agosto se gestionaron 18 eventos asociados a equipos WLAN – Access Point, equivalentes al 4,15% del total de casos. Se evidenció una disminución frente a los meses anteriores.

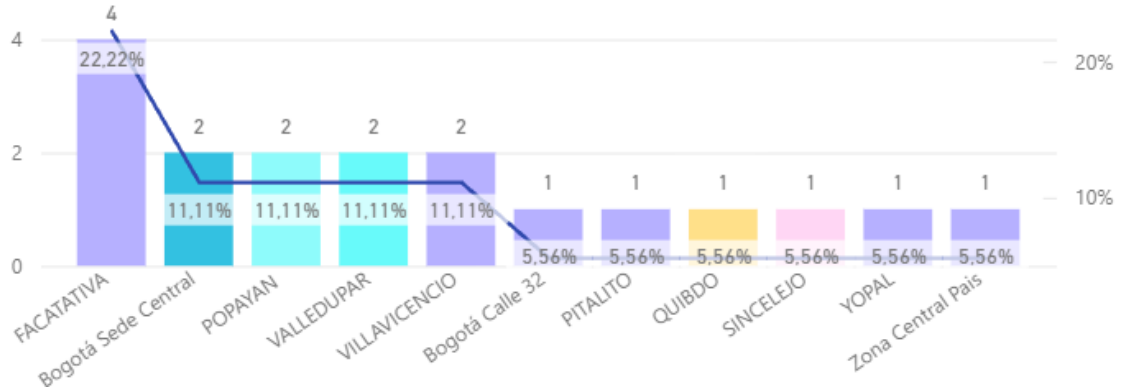


Ilustración 17 Top 9 Sedes afectadas por Access Point

Facatativá ocupó el primer lugar con 4 casos, todos relacionados con fallas de energía eléctrica. Bogotá, Popayán, Valledupar y Villavicencio registraron 2 eventos cada una,

principalmente por fallas eléctricas y, en menor proporción, bloqueo de dispositivos. Bogotá Calle 32, Pitalito, Quibdó, Sincelejo, Yopal y la zona central registraron un caso cada una.

La falla de energía eléctrica fue la principal causa, con una participación del 66%. El bloqueo de dispositivos representó el 16%. También se registraron eventos por desconexión física e intermitencia.

De los 18 eventos, 17 (94%) se encuentran cerrados o solucionados. Un caso permanece en gestión debido a la desconexión física del AP y se encuentra pendiente del retorno del funcionario a la sede para realizar la revisión correspondiente.

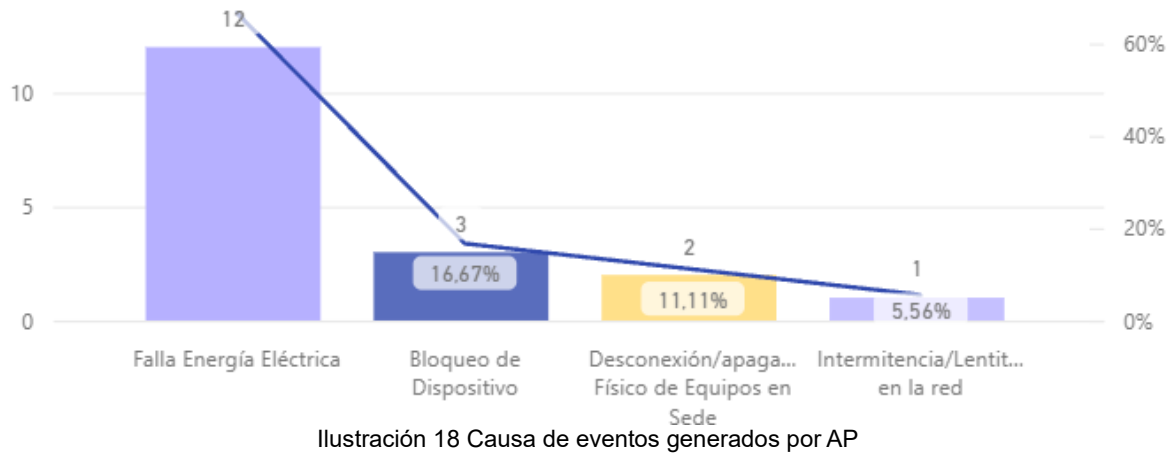


Ilustración 18 Causa de eventos generados por AP

Starlink

Durante agosto se gestionaron 86 eventos relacionados con equipos Starlink, equivalentes al 19,8% del total de casos.

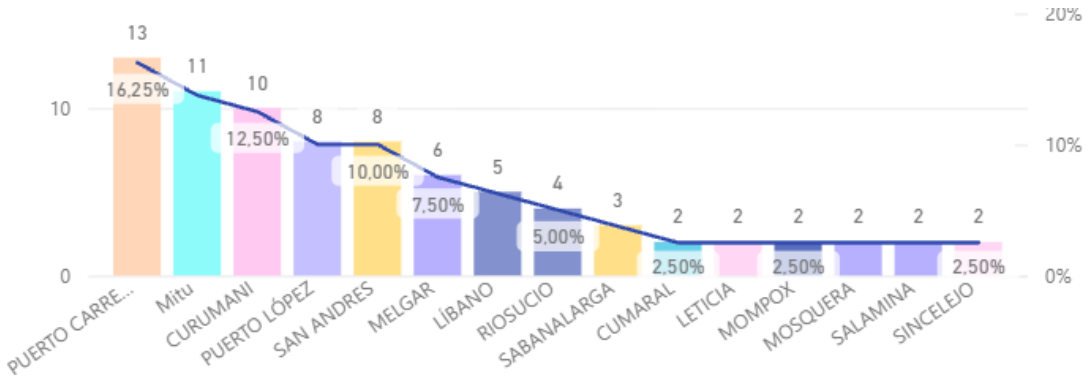


Ilustración 19 Top 10 Sedes afectadas por Starlink

Puerto Carreño registró 13 eventos y ocupó el primer lugar del TOP 10. El 61% de sus eventos estuvo asociado a fallas eléctricas relacionadas con tormentas, mantenimientos o

condiciones de infraestructura. Mitú registró 90% de casos por energía eléctrica y un caso por intermitencia. Curumaní presentó 10 eventos, con 60% asociados a fallas de energía. Puerto López y San Andrés registraron 8 casos cada una, con predominio de fallas eléctricas (68%) y desconexión física (31%). Melgar registró 6 casos, todos relacionados con energía eléctrica. Líbano registró 5 casos, de los cuales el 80% correspondió a desconexiones físicas.

Las fallas de energía eléctrica representaron el 68% de los eventos Starlink y constituyeron la principal causa. La desconexión física ocupó el segundo lugar con 24% (21 eventos). Las fallas en la red del proveedor y las intermitencias o lentitudes representaron 3,49% cada una.

En las sedes remotas, los eventos eléctricos pueden estar asociados a tormentas, lluvias, mantenimientos, daños de terceros, racionamientos o condiciones de suministro. Se recomienda evaluar la instalación de estabilizadores y mecanismos de respaldo energético para reducir la recurrencia.

De los 86 eventos registrados para Starlink, el 100% fue solucionado o cerrado.

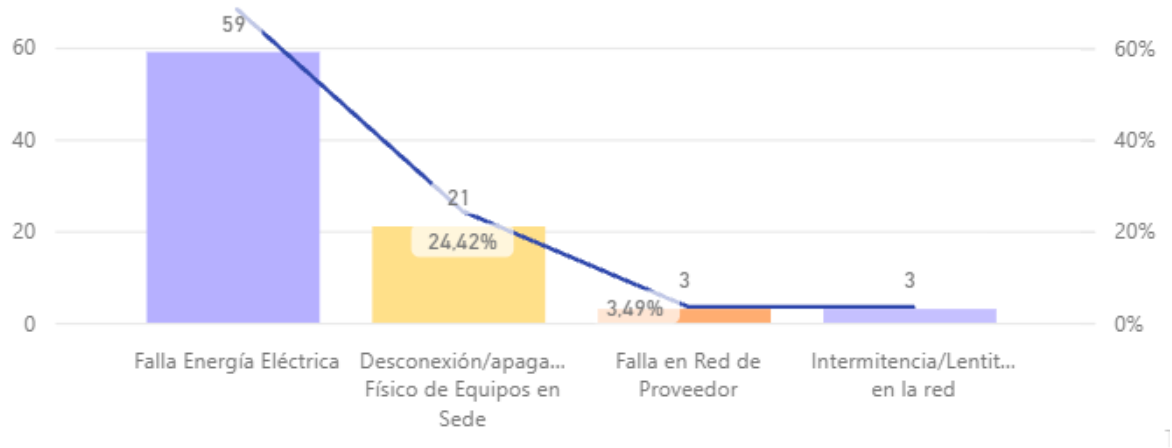


Ilustración 20 Causas de eventos generados por Starlink

FortiGate

Durante agosto se gestionaron 61 eventos relacionados con equipos FortiGate, equivalentes al 14,6% del total de casos. La categoría presentó una disminución frente al mes anterior.

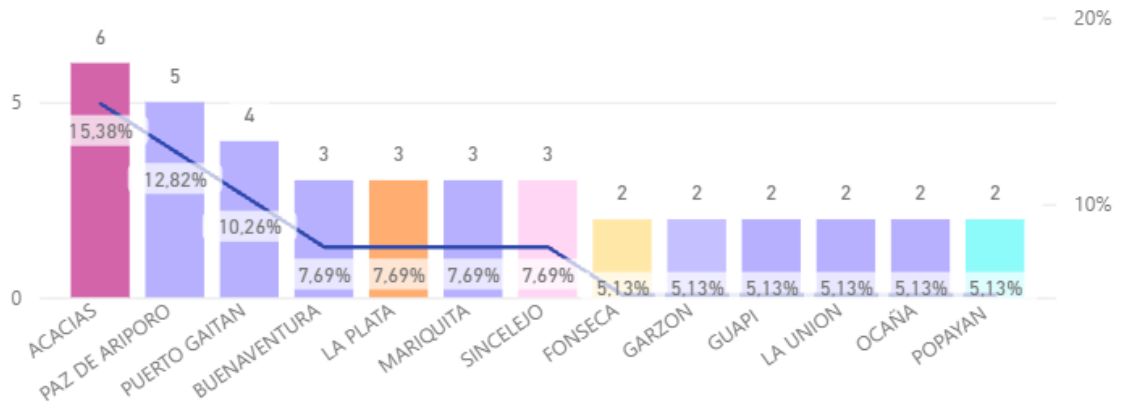


Ilustración 21 Top Sedes afectadas por FortiGate

Acacías registró 6 casos, con predominio de fallas eléctricas (83%). Paz de Ariporo presentó 5 casos, de los cuales el 80% estuvo relacionado con fallas eléctricas. Puerto Gaitán registró 4 casos, principalmente por energía eléctrica (75%) y un caso por intermitencia.

Buenaventura, La Plata, Mariquita y Sincelejo registraron 3 casos cada una, principalmente asociados a energía eléctrica y desconexiones físicas. Fonseca, Garzón, Guapi, La Unión, Ocaña y Popayán registraron 2 casos cada una, con predominio de fallas eléctricas.

Las fallas de energía eléctrica representaron el 77% de los eventos FortiGate. La intermitencia o lentitud registró 7 casos (11%). La desconexión o apagado de equipos representó el 9% y las fallas en red del proveedor registraron 1 caso (1,6%).

Se destaca que la disminución de eventos asociados a la red del proveedor está relacionada con los ajustes realizados sobre la reportería de Zabbix y su integración con Aranda.

De los 61 eventos reportados, el 98% se encuentra cerrado y un caso permanece suspendido, equivalente al 2%. El caso corresponde a la sede Buga, actualmente en adecuaciones.

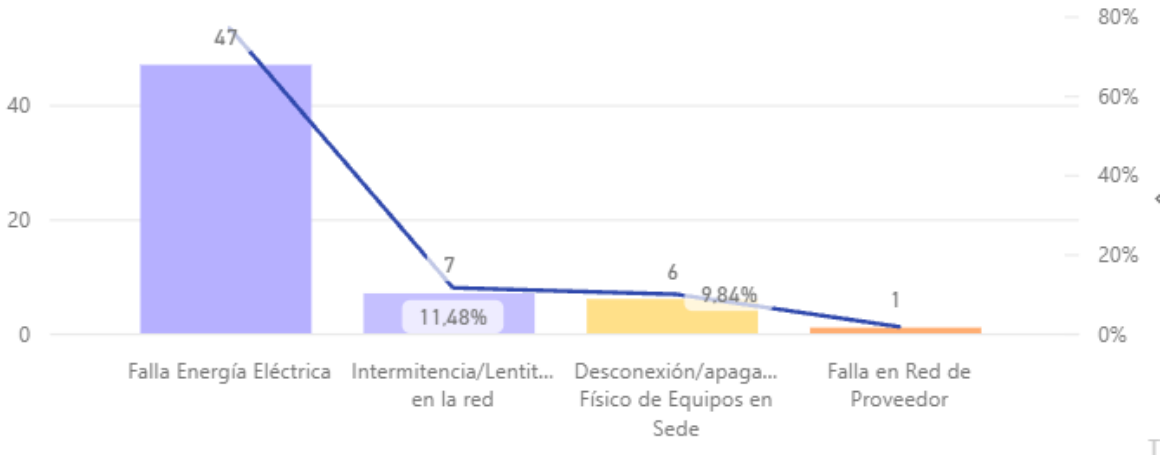


Ilustración 22 Causas de eventos generados por FortiGate

Casos Escalados a Proveedor de Telecomunicaciones

Durante el mes de agosto se registraron 13 casos que fueron escalados y gestionados con proveedor de los cuales el 100% fueron solucionados.

Servicios centrales

Servidores Windows

Durante agosto, el NOC gestionó 41 eventos asociados a servidores Windows, equivalentes al 9,45% del total de casos.

El alto consumo de memoria fue la principal causa de eventos durante el mes. MTCAAPP registró 11 casos (44%) y MINTRAB107 registró 10 casos (40%), concentrando entre ambos servidores el 84% de los eventos asociados a esta causa.
El alto consumo de disco ocupó el segundo lugar, con 7 casos (17%). MINTRABSQLPROD1 presentó el mayor número de reportes, seguido de MINTRABCKEXEC.

También se registraron eventos por aplicación indisponible, servidor apagado, actividad programada y reinicio de servidor. Para las actividades programadas se recomienda mantener los servidores en estado de mantenimiento, con el fin de evitar alertamientos durante ventanas previamente planificadas.

En el TOP de servidores, MTCAAPP ocupa el primer lugar con 11 casos, todos asociados a consumo de memoria RAM. MINTRAB107 registra 10 casos, igualmente asociados a alto consumo de memoria. MINTRAB23 presenta eventos relacionados con aplicación indisponible y reinicio de servidor. MINTRABCKEXEC y MINTRABSQLPROD1 registran 4 casos cada uno.

De los 41 eventos registrados, 30 (73%) se encuentran cerrados o solucionados, 5 se encuentran suspendidos y 6 permanecen en proceso. Los casos en proceso están relacionados principalmente con consumo de memoria y disco. Se identificó ausencia de documentación o comentarios del especialista en los casos revisados, por lo cual se recomienda fortalecer el registro de las actividades ejecutadas y las acciones de seguimiento.

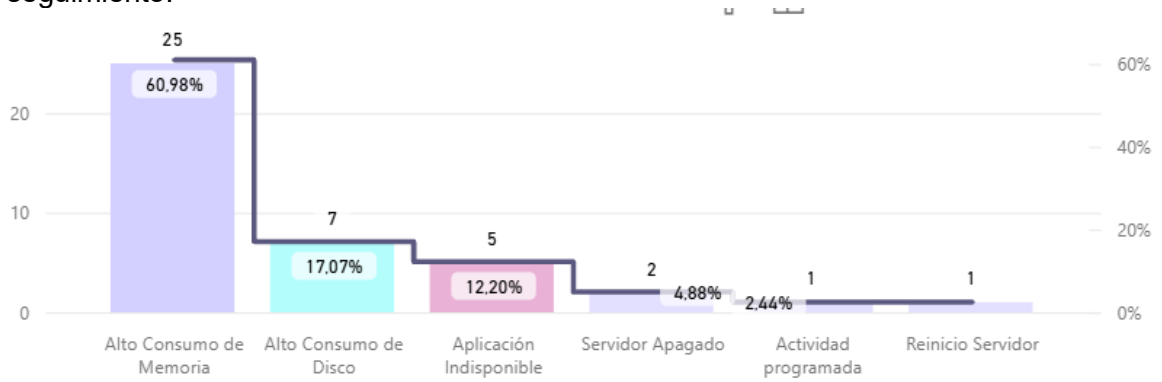


Ilustración 23 Causas de alarmas Servidores Windows

Servidores Linux

Durante agosto se registraron 4 eventos asociados a servidores Linux, equivalentes al 0,92% del total. Aunque se observa un leve aumento, la incidencia continúa siendo baja frente a los servidores Windows.

El 75% de los eventos estuvo asociado a consumo de disco en el servidor MINTRAB60, el cual presenta recurrencia durante los últimos tres meses. El 25% restante correspondió a un evento de consumo de memoria en MINTRAB162.

MINTRAB60 ocupa el primer lugar por recurrencia, asociado a consumo de disco, mientras que MINTRAB162 registra eventos relacionados con consumo de memoria.

El documento fuente registra 4 casos para agosto y señala 1 caso cerrado y 3 en proceso; adicionalmente, indica que no se observan comentarios por parte del especialista en la plataforma. Se recomienda validar y actualizar el estado y la documentación de estos casos para asegurar la trazabilidad de la gestión.

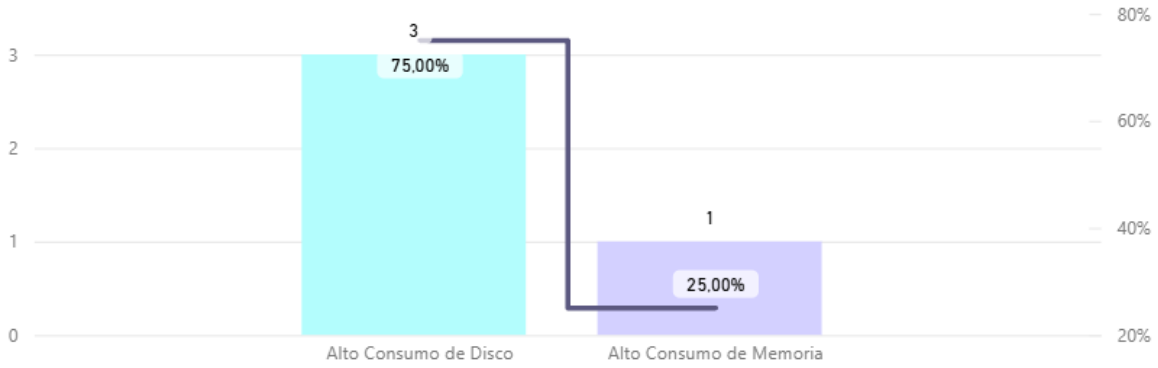


Ilustración 24 Causas de alarmas Servidores Linux

Graficas de CPU zabbix

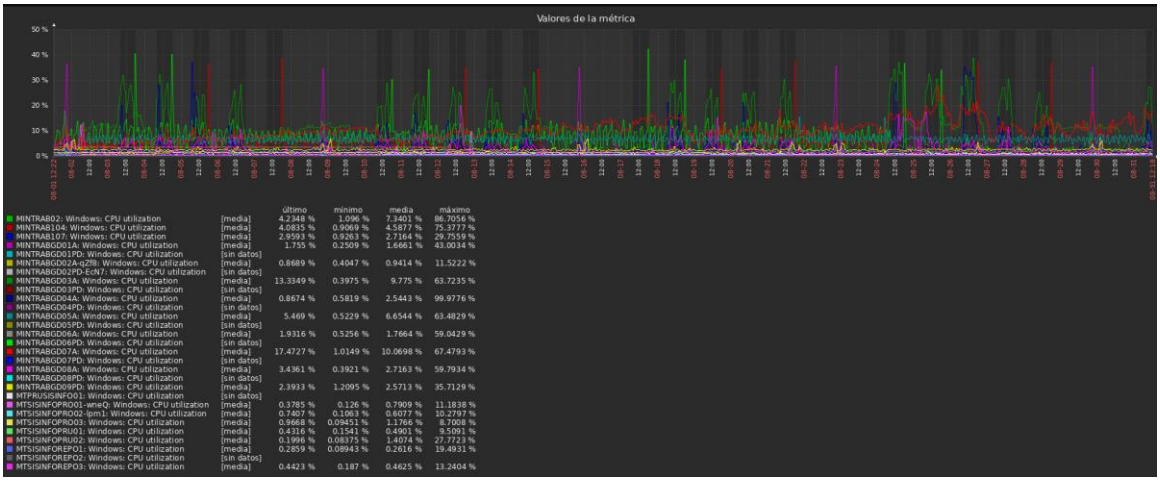


Ilustración 25 Grafica CPU

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 10.0698%
2. MINTRAB02 7.3401%
3. MINTRABGD05A 6.6544%
4. MINTRAB104 4.5877%
5. MINTRAB107 2.7164%
6. MINTRABGD08A 2.7163%

Grafica de MEMORIA zabbix

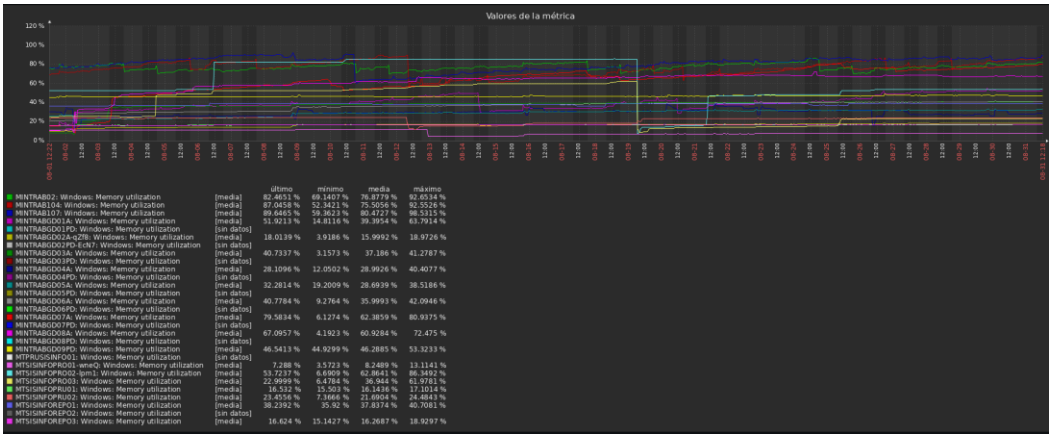


Ilustración 26 Grafica memoria

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. MINTRAB107 80.4727% (controlador de dominio)
2. MINTRAB02 76.8779% (controlador de dominio)
3. MINTRAB104 75.5056% (controlador de dominio)
4. MTSISINFOPRO02 62.8641% (SISINFO)
5. MINTRABGD07A 62.3859% (Gestor Documental)

Datacenter (Cali - Bogota)

Durante el mes no se evidencian eventos relacionados a los DataCenter de Ministerio de Trabajo.

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 agosto de 2026.

Servidores

Cantidad de dispositivos	Disponibilidad consolidada
118	99.99%

Tabla 21 Consolidado disponibilidad de servidores

Directorio Activo

Cantidad de dispositivos	Disponibilidad consolidada
3	99.99%

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	99.99%
MINTRAB104	99.99%
MINTRAB107	99.99%

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	99.99%
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	93,85%

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	99.97%
MINTRABVULNE01	99.97%
SOC_Fortianalyzer	99.08%
SOC_FortiDDOS	99.08%
SOC_SandBox	100,00%
SOC_WAF	99.08%
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.
- Se realizó seguimiento a los 18 planes de disponibilidad, de los cuales 4 planes (22,2%) permanecen pendientes de ejecución, lo cual, se encuentran en proceso de programación y ejecución en los próximos periodos.

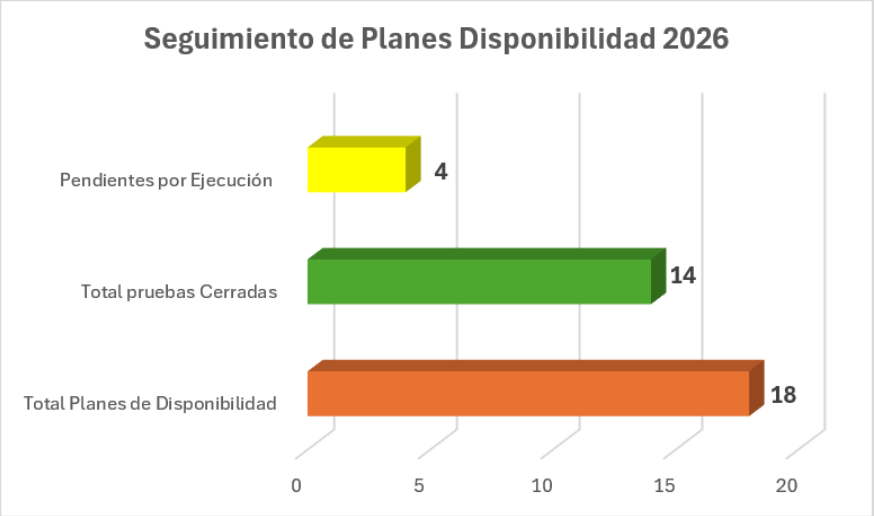


Ilustración *27 Seguimiento de Pruebas de Disponibilidad 2026*

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 agosto de 2026.

Actividades en curso:

- Revisión de los cambios (RFC) ejecutados durante el periodo, para los cuales (18) cambios fueron aprobados su cierre, ya que cuentan con las evidencias completas de los planes de Pruebas Previas y Posteriores, al corte del 31/08/2026 se encuentra (1) caso abierto (en implementación) 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.**

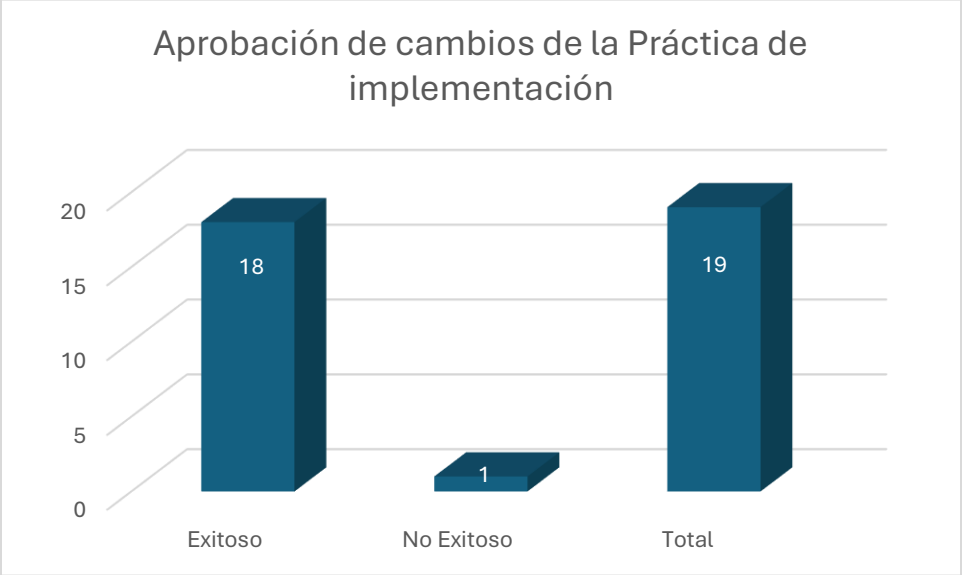


Ilustración 28 Seguimiento Práctica Implementación

Seguimiento%20de%20cambios%20Imp

2.2 Mesa de Servicios y Soporte en Sitio

A continuación, se presenta la gestión desarrollada durante el mes de agosto 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 agosto a la MDS ingresaron 368 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	Sumatoria N° Atendidas umbral	Abandonadas	No Atendidas
COL - Mintrabajo-equipo compu	228	219	214	5	2	7
COL - Mintrabajo-Gestor-documental	68	67	66	0	1	0
COL - Mintrabajo-office365	49	49	48	0	0	0
COL - mintrabajo-Impresora	23	22	22	1	0	1
TOTAL	368	357	350	6	3	8

Tabla 33 Llamadas Atendida por la Mesa de Servicio

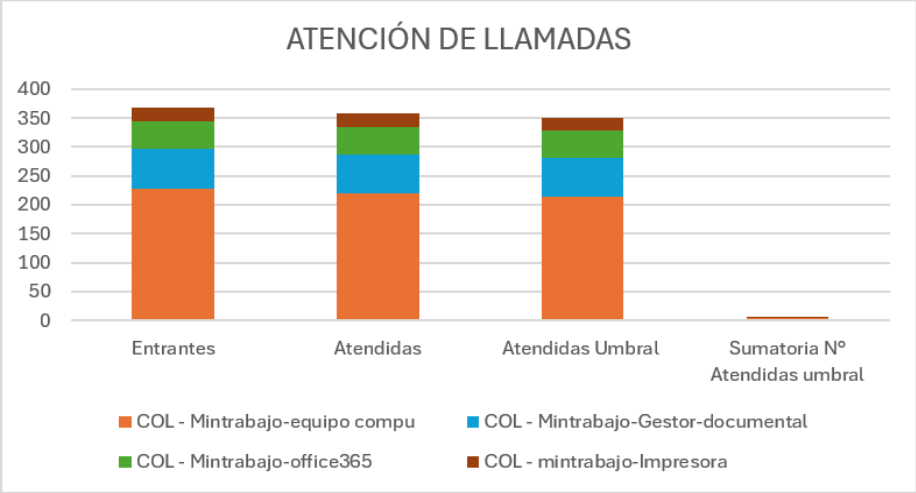


Ilustración 29 Llamadas Atendidas

El servicio con mayor demanda a través del canal de atención telefónica fue “Equipo de Cómputo”, con un total de 228 llamadas entrantes. Como resultado de esta gestión, se atendieron 357 solicitudes.

Durante el período analizado se registraron 6 llamadas abandonadas antes de los 20 segundos. No obstante, estas corresponden al evento ocurrido el 10 de agosto, fecha en la cual se presentó el sismo de alcance nacional. En cumplimiento de los protocolos de seguridad y por instrucción de la administración del edificio, se realizó el proceso de evacuación, lo que impactó temporalmente la atención telefónica.

Teniendo en cuenta esta situación extraordinaria, las 6 llamadas abandonadas se consideran justificadas y se excluyen del análisis operativo, al encontrarse dentro de los tiempos establecidos para la evacuación y atención de la emergencia.

Servicio	Entrantes	Atendidas	Atendidas Umbral	Sumatoria N° Atendidas umbral	Abandonadas	No Atendidas
COL - Mintrabajo-equipo compu	228	219	214	0	2	2
COL - Mintrabajo-Gestor-documental	68	67	66	0	1	1
COL - Mintrabajo-office365	49	49	48	0	0	0
COL - mintrabajo-Impresora	23	22	22	0	0	0
TOTAL	368	357	350	0	3	3

Tabla 34 Llamadas exceptuadas por la Mesa de Servicio

- **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_AGOSTO.xlsx pestaña *categoría.*

- **Análisis de Casos Anulados por Servicio**

Para este periodo se tienen 3

CASOS ANULADOS	TOTAL
Herramientas de Gestión	3
Total general	**3**

Tabla 35 Casos Anulados

Los casos anulados por Herramientas de Gestion se deben a 2 incidentes por Alarma desde Zabbix, y un cambio para ejecutar en Aranda por error de registro.

- **Análisis de Casos Suspendidos por Servicio**

Para el periodo del mes de agosto, se dio un aumento de casos suspendidos del 7,64% que corresponde a 12 casos para un total de este mes de 157 casos de los siguientes servicios:

CASOS SUSPENDIDOS	TOTAL
Soporte Microinformatica	74
Administración de servidores	45
Seguridad informatica	15
Redes y Conectividad	13
Aplicaciones Especializadas	9
Energía Eléctrica Regulada - UPS	1
Total general	**157**

Tabla 36 Casos Suspendidos

- **Soporte Microinformática:** 74 casos suspendidos debido a que se ha solicitado información complementaria a los usuarios o están pendientes por disponibilidad del usuario: Asesoría - Consulta con 18 casos; Backup, con 10 casos; Equipo Periférico con 7 casos; Equipo Escritorio y Cambio Toner con 6 casos cada categoría; Asignación de equipo (portátil o PC) y Traslado de Sede, Cambio Equipo o Rol con 5 casos cada categoría, Préstamo y Equipo Portátil con 3 casos cada categoría, Devolución de equipo (portátil o PC) con 2 casos, Solicitud Backup, No Escanea, Cambio de unidad Fusora, Equipo Impresora, Daño físico, Asesoría-Consulta, Cambio de Unidad de Imagen, Configuración e Instalacion-Configuracion con 1 caso para cada categoría.

- **Administración de Servidores:** 45 casos suspendidos, Inactivar Usuario con 19 casos, Backup con 6 casos, Servidor Windows con 5 casos, Asignación de Licencias, Modificar Usuarios y Configuración con 3 casos cada categoría, crear/Modificar/Eliminar con 2 casos, Cambiar contraseña, Asesoría-Consulta, Habilitar usuario y Configuración MFA con 1 caso para cada categoría.

- **Soporte Microinformática**: 15 casos suspendidos por: Validación Habilitación Puertos USB con 6 casos, Reporte de eventos y Habilitación de Puertos USB con 3 casos cada categoría, Agregar Listas Blancas, Configuración Consola y Análisis vulnerabilidades con 1 caso parta cada categoría.
- **Redes y Conectividad:** 13 casos suspendidos por Router con 9 casos, Starlink con 2 casos FortiGate, y AP con 1 caso para cada categoría.
- **Aplicaciones Especializadas:** 9 casos suspendidos debido a:
  Asignación- modificación Roles y Depuracion Bandeja con 2 casos; relanzamiento, Asesoría-Consulta, Solicitud de permisos, Instalar - -Configurar con 1 caso para cada categoría.

- **Energía Eléctrica Regulada:** 1 caso suspendido por Energía Eléctrica Regulada 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 quedaron 2 incidentes en estado solucionado.



Ilustración 30 Incidentes soporte en sitio

Incidentes solucionados por Soporte Territoriales: Para este periodo quedaron 5 incidentes en estado solucionado.

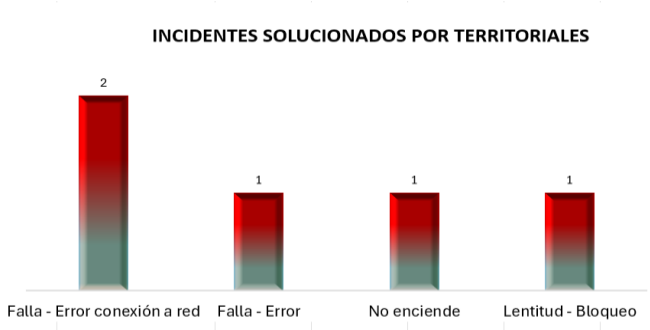


Ilustración 31 incidentes solucionados por territoriales

Requerimientos solucionados por la Mesa de Servicios:
En el mes de agosto quedaron 51 requerimiento en estado solucionado.

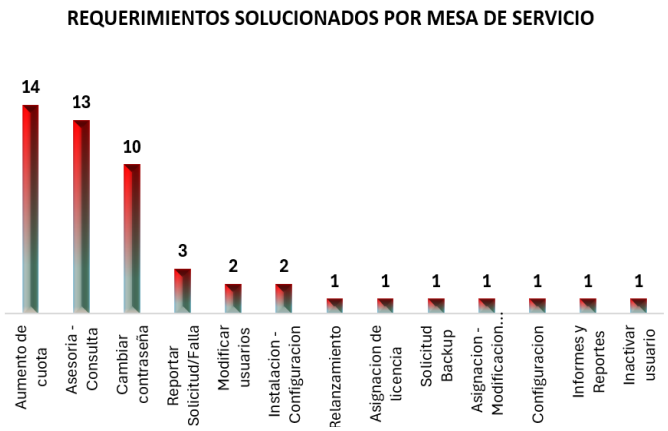


Ilustración 32 requerimientos solucionados mesa de servicios

Requerimientos solucionados por Soporte en sitio Bogotá: En el mes de agosto quedaron 43 requerimientos en estado solucionado.



Ilustración 33 requerimientos solucionados soportes

Requerimientos solucionados por Soportes Territoriales: Para el mes de agosto quedo 174 requerimiento en estado solucionado.

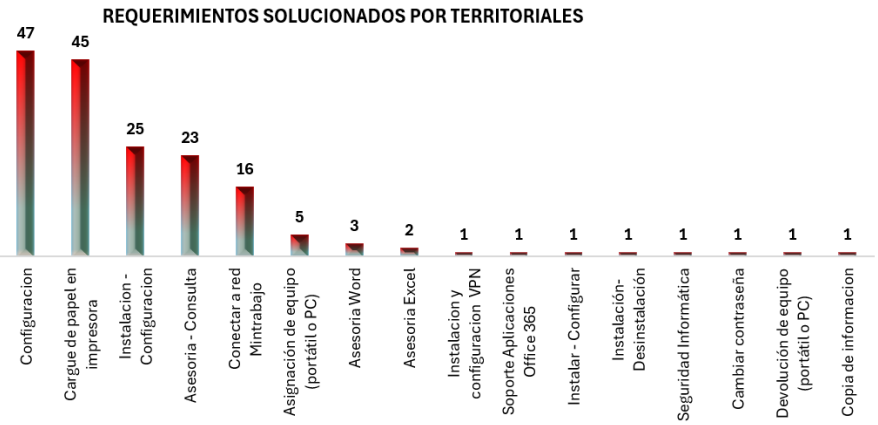


Ilustración 34 requerimientos solucionados soporte territoriales

- **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 agosto se cerraron 1098 casos, discriminados así: Asesoría – Consulta 274 casos, Cambiar contraseña 182 casos, Aumento de cuota 172 casos, Inactivar usuario 97 casos, Creación de usuario con 86 casos, Cambio de grupo 43 casos, Backup con 32 casos, Configuración 31 casos, Habilitar usuario 27 casos y traslado de Sede, Cambio Equipo o Rol con 22 casos.

En comparación del mes anterior se nota una disminución de casos cerrados por la mesa de un 2,48% que es equivalente a 28 casos.

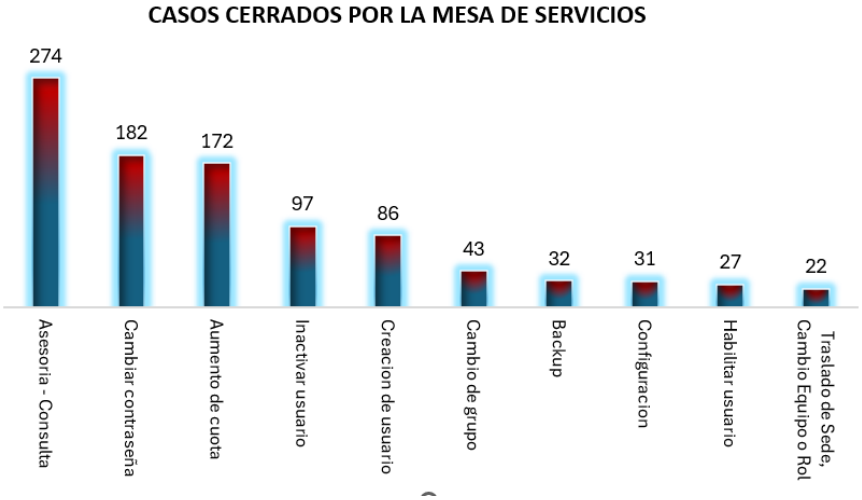


Ilustración 35 Requerimientos Cerrados por la Mesa de Servicios

Casos Cerrados por Soporte en Sitio: Se indica el top 10 de Requerimientos cerrados por soporte en sitio, para el mes de agosto se cerraron 908 casos discriminados así: Cargue de papel en impresora con 224 casos, Asesoría – Consulta con 148 casos, Configuración

con 55 casos, Préstamo con 47 casos, Asignación de equipo (portátil o PC) con 43 casos, Seguridad Informática con 30 casos, Soporte Aplicaciones Office 365 con 28 casos, Reporte de evento con 23 casos y Backup con 22 casos.

En comparación con el mes anterior se tiene una disminución del 10,09% que corresponde a 102 casos.

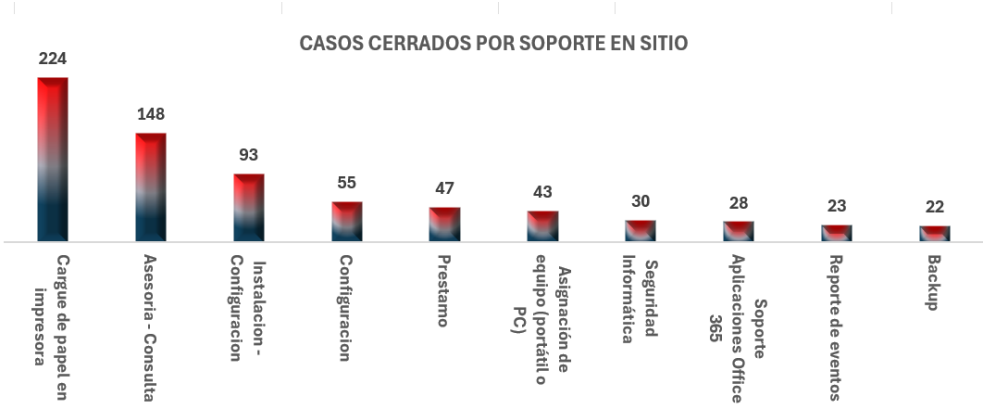


Ilustración 36 Casos Cerrados por Soporte en Sitio

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 agosto se cerraron 1298 casos, discriminados así: Asesoría – Consulta con 238 casos, Cargue de papel en impresora con 141 casos, Configuración con 134 casos, Instalación Configuración con VPN y Asesoría Excel con 65 casos cada categoría, Asesoría PDF con 53 casos, Mantenimiento preventivo 46 casos, Asesoría Word con 41 casos, Asignación de equipo(portátil o PC) con 361 casos.

En comparación con el mes anterior se tiene una disminución del 25,01% que corresponde a 433 casos.

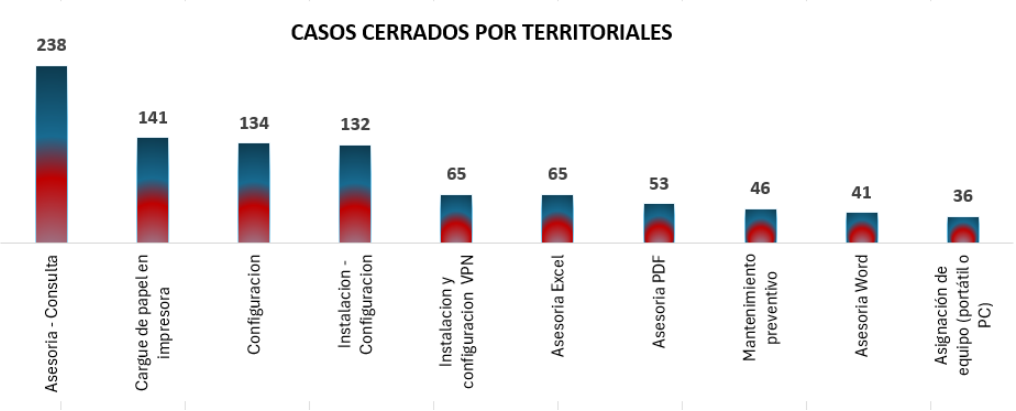


Ilustración 37 Casos Cerrados por Territoriales

- **Casos Atendidos a Usuarios VIPS**

Durante este periodo se crearon 65 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	3	0	3
Requerimientos	61	1	62
Total general	**64**	**1**	**65**

Tabla 37 Casos Atendidos usuarios VIPS

Se atendieron 926 solicitudes para el resto de los usuarios discriminados así:

TIPO DE CASO-NO-VIPS	CUMPLIMIENTO	NO_CUMPLE	TOTAL
Incidentes	24		24
Requerimientos	901	1	902
Total general	**925**	**0**	**926**

Tabla 38 Casos Atendidos usuarios

- **Medio de Ingreso de Casos**

Durante el período ingresaron a la mesa de servicio 5631 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:

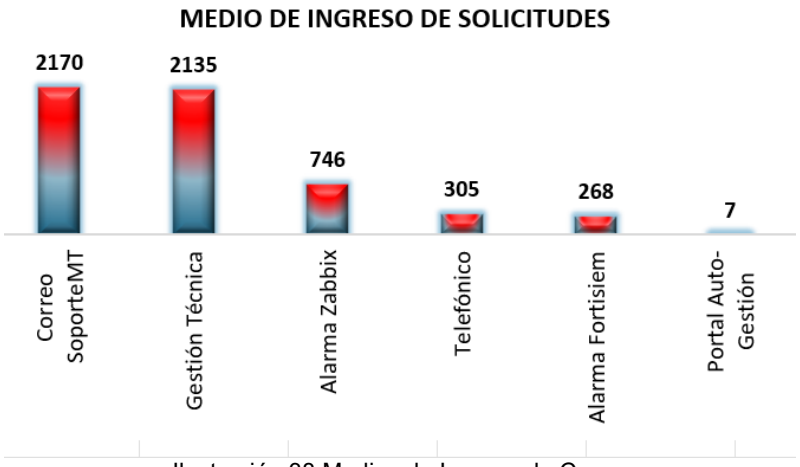


Ilustración 38 Medios de Ingreso de Casos

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 está ejecutando la actualización del agente Aranda en los equipos del ministerio.

Se continúa realizando 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 agosto de 2026 los profesionales de soporte en sitio territoriales llevaron a cabo las siguientes acciones:

Se realizan 7 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 1733 casos, dentro de los que se destacan: Cargues de Papel en las impresoras de las diferentes Sedes, Inactivación de usuarios, Configuración de OneDrive, Instalación y configuración de impresoras, Instalación y configuración de VPN, Ofimática. Asesoría en Excel, Ofimática. Asesoría en PDF, Asesoría-Consulta OneDrive, Asignación de equipos de cómputo y Equipo de cómputo.Conectar a red Mintrabajo.

Revisión, validación del estado y aseguramiento de los equipos de cómputo de Valle, Armenia, Pereira y Manizales para el traslado a nueva Sede o atención de manera remota de los mismos en vista de la emergencia generada por el terremoto

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
Agosto 2026	ANTIOQUIA	RIONEGRO	Ejecutar borrado seguro desde BIOS	Se procedió con el proceso de borrado seguro del equipo ANDJALVAREZ según el manual, se realizó proceso y se adjuntó evidencias, al culminar proceso se instaló el sistema operativo y se configuro usuario de Apicom para luego realizar proceso de asignación, la tarea se resolvió correctamente.	TK-289559
Agosto 2026	VALLE	PALMIRA	Instalación de cable RJ45 Cat 6 – Adecuación para navegación	Se valida la novedad del cable de red en mal estado y se determina la necesidad de instalar un nuevo cable para garantizar estabilidad y mejor rendimiento en la conexión. Se procede a realizar la instalación de un cable RJ45 categoría 6, reemplazando el anterior en mal estado	RF-316645

Mes	Territorial	Sede	Servicio	Descripción	Caso
Agosto 2026	ATLANTICO	CAMPO DE LA CRUZ	Ejecutar borrado seguro desde BIOS	Se ingresa la contraseña de la BIOS, se accede a la opción de borrado seguro, se inicia el proceso del borrado seguro con la herramienta “Lenovo Secure Wipe”, se adjunta las imágenes del proceso del borrado seguro, paso a paso.Finalizando de forma satisfactoria, se adjuntan evidencias	RF-307137 TK-308190
Agosto 2026	CAUCA	SANTANDER DE QUILICHAO	Devolución de equipo y entrega. Borrado seguro	Se gestiona la devolución del equipo de cómputo y demás elementos tecnológicos asignados, incluyendo teléfono, diadema, monitor, teclado, mouse y torre, los cuales se entregan en óptimas condiciones.	RF-325390
Agosto 2026	VALLE	PALMIRA	Instalación de cable RJ45 Cat 6 – Adecuación para navegación	Solución aplicada: Se procede a realizar la instalación de un cable RJ45 categoría 6, reemplazando el anterior en mal estado. Tras la intervención, se ejecutan pruebas de conectividad confirmando que la velocidad de navegación mejoró significativamente.	RF-328363 RF-328364 RF-328365 RF-28366 RF-328367
Agosto 2026	NORTE DE SANTANDER	CHINACOTA	REVISÓN DE EQUIPO DE COMPUTO	Se realizar mantenimiento básico y optimización del equipo con el fin de mejorar su funcionamiento y mantener actualizado el sistema operativo.	RF-328417 TK-323131 TK-323135 TK-323136 TK-323139
Agosto 2026	GUAJIRA	FONSECA	Desconexión de equipo	Se requiere de parte de soporte en sitio la visita a la inspección de Fonseca para la desconexión de los equipos tecnológicos que serán trasladados junto con la inspección a otro municipio.	RF-319066 RF-319068

Tabla 39 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
MDS-1	Tiempo de atención de solicitudes por soporte en sitio	99,25%	95,00%
MDS-2	Tiempo de solución de incidentes por soporte en sitio	98,89%	90,00%
MDS-3	Tiempo de solución de requerimientos por soporte en sitio	98,64%	90,00%
MDS-4	Tiempo de respuesta de la mesa de servicio	98,04%	85,00%
MDS-5	Abandono de llamadas	2,17%	Máximo 8,00%
MDS-6	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla *40* Medición de ANS Mesa de servicios

Nota: El resultado del indicador MDS-5 (2,17%) se encuentra dentro de la meta establecida (≤8,00%). Las 6 llamadas abandonadas antes de los 20 segundos estuvieron asociadas al evento extraordinario del 10 de agosto de 2026, ocasionado por el sismo de alcance nacional. La evacuación preventiva de las instalaciones, realizada en cumplimiento de los protocolos de seguridad y por

instrucción de la administración del edificio, generó una afectación temporal en la atención telefónica. Por lo anterior, estos casos se consideran justificados y atribuibles a una situación extraordinaria, sin impacto sobre el comportamiento operativo habitual del servicio.

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 883 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.

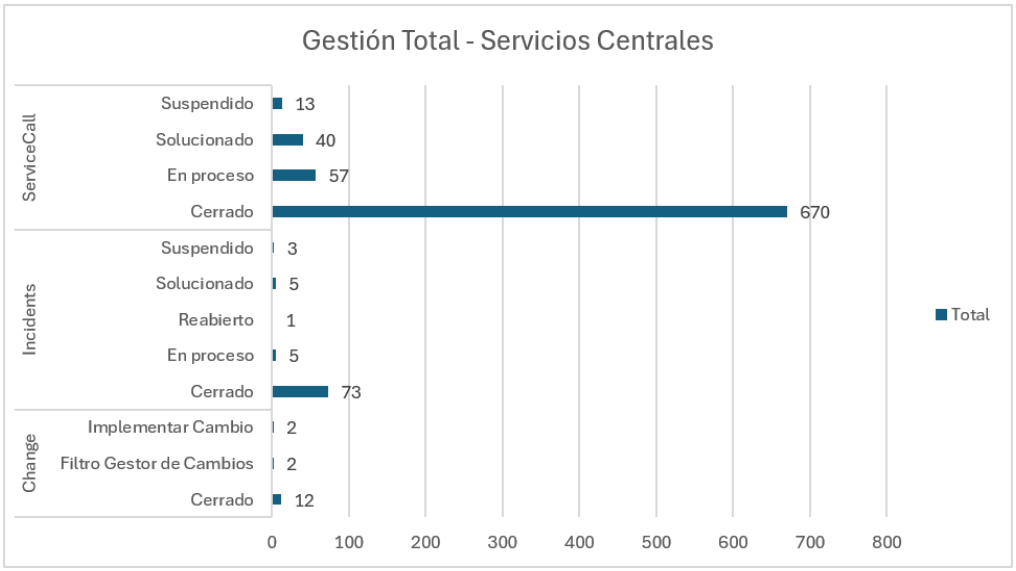


Ilustración 39 Gestión Casos – SC

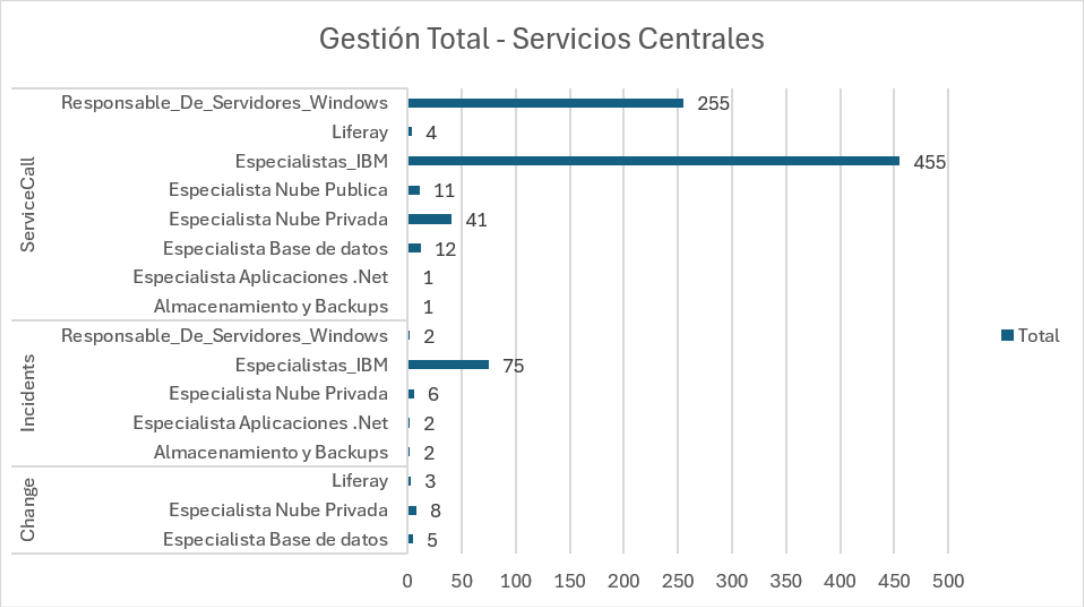


Ilustración 40 Gestión SC - Por Grupo

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 41 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

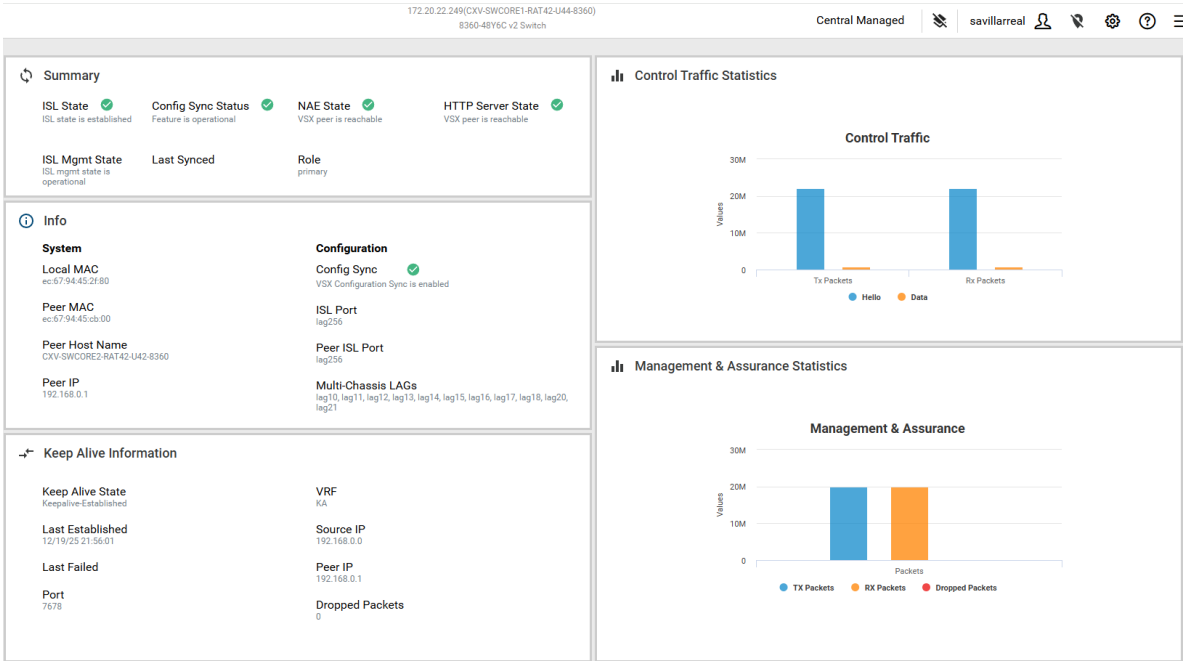


Ilustración 42 Sincronización HA de los Switch Core

-

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 383 Mbps, se han presentado picos de consumo, que no afectan la estabilidad del canal ya que no son constantes.

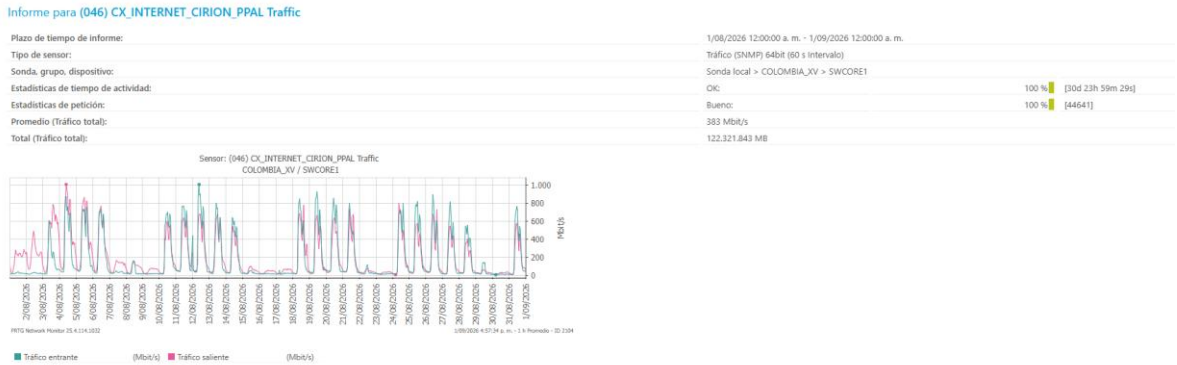


Ilustración 43 Grafica de consumo canal Internet Datacenter

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:

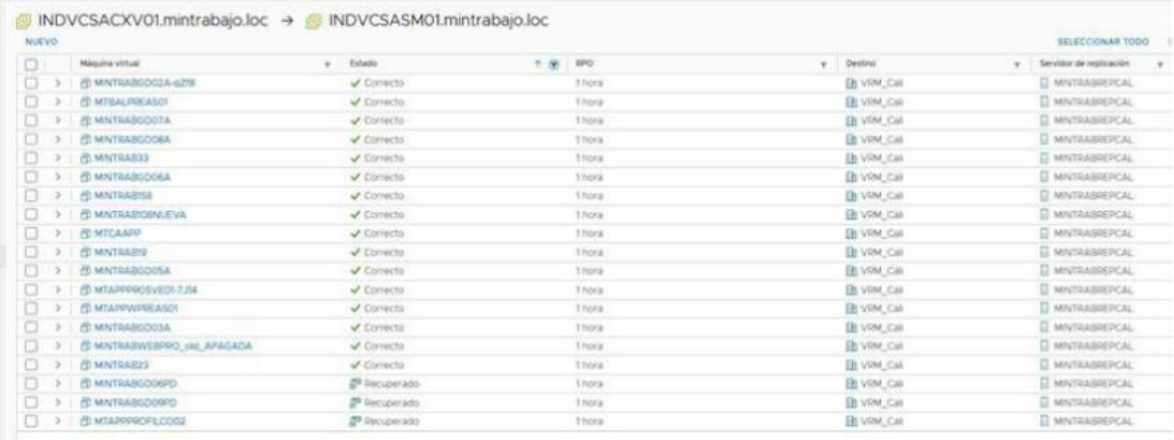


Ilustración 44 máquinas virtuales DRP

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. Se cuenta con segmentación de red independientes y defirentyes a las del Datacenter principal para preparar el escenario y restaurar servicios en Cali en caso de ser necesario. 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 tiene 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 de 2025 y actualmente se mantiene operativa, 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.

No.	Base de Datos	Aplicación
1	AS*DB*RUE	RUE
2	RUE	RUE
3	ESTADOJOVEN	Estado Joven
4	Bancos	Tesorería

No.	Base de Datos	Aplicación
5	CalculadoraLaboral	Calculadora Laboral
6	ESTADOJOVEN	Estado Joven
7	Infraestructura	Cobro Coactivo
8	MTRCobroCoactivo	Cobro Coactivo
9	Siriti2018	Siriti
10	CentrosEntrenamiento	Centros de Entrenamiento
11	Rutec	Rutec
12	ARCHSINDICAL	Archivo Sindical
13	yfsveapp	SVE
14	SABERHACERVALE	Saber Hacer Vale
15	sveapp	SVE

Tabla 41 Bases de Datos con LogShipping

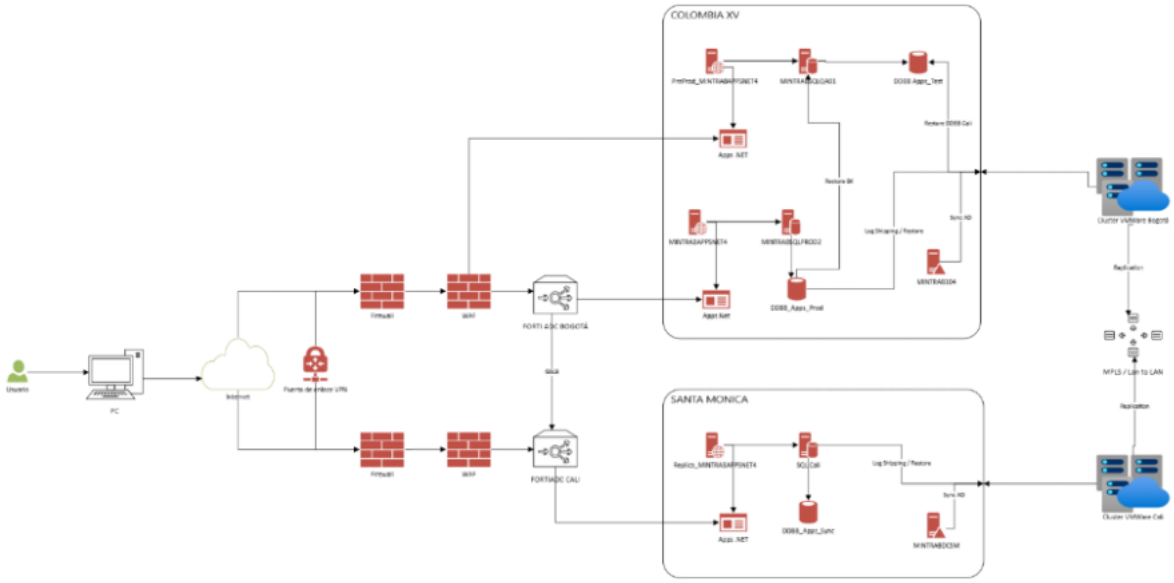


Ilustración 45 Escenario Apps DRP

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 0.81 Mbps.

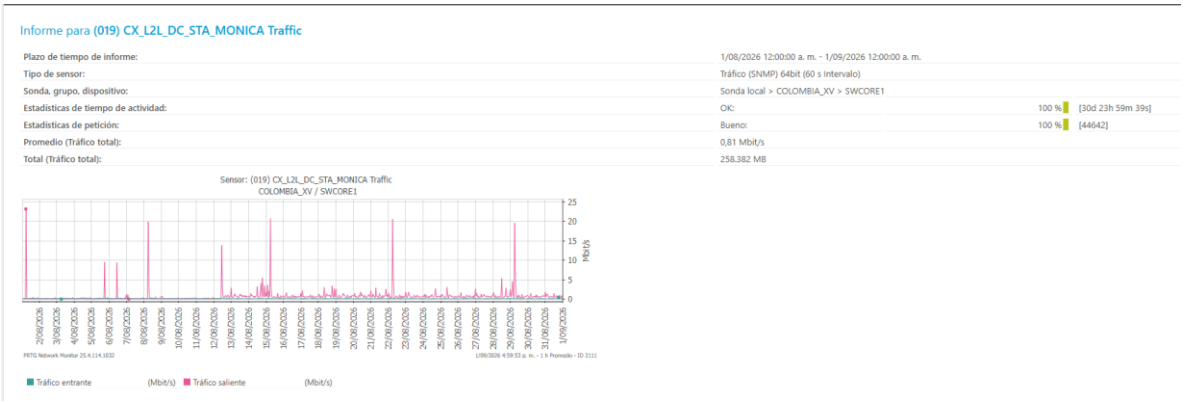


Ilustración 46 Extremo DC Bogotá

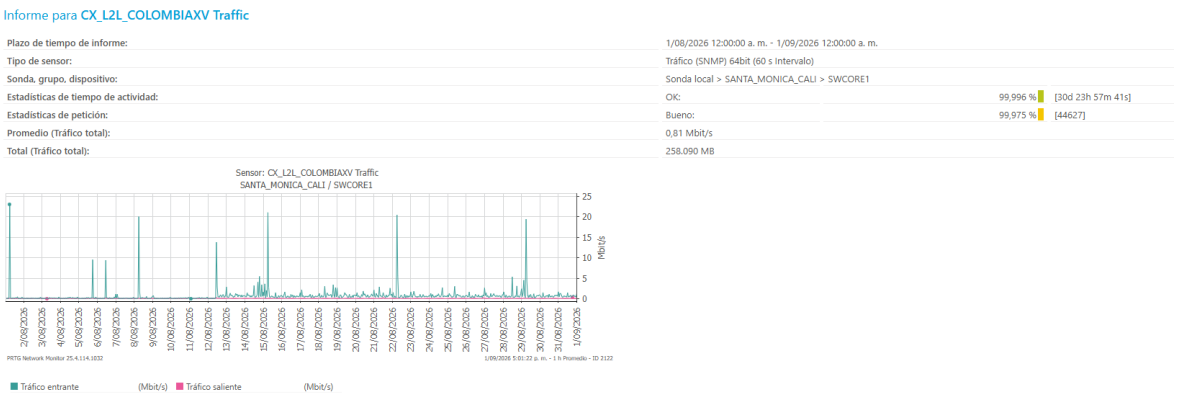


Ilustración 47 Extremo DC Cali

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 0.12 Mbps.

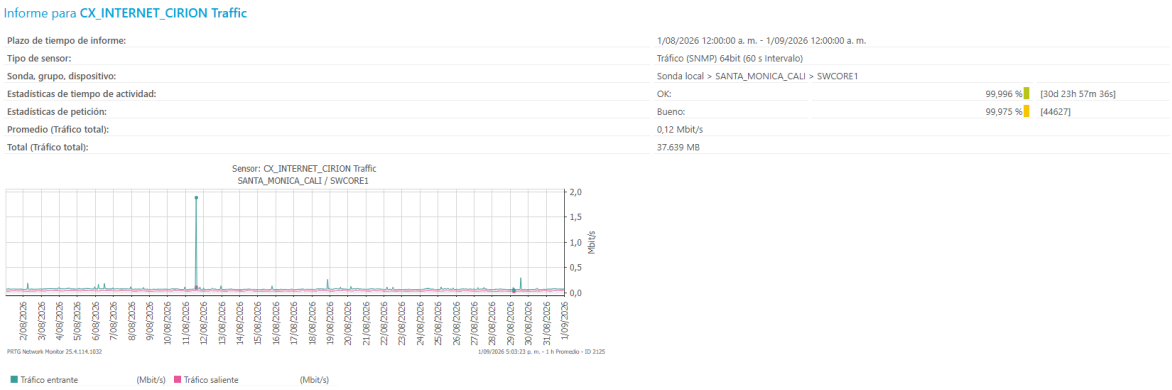


Ilustración 48 Estado canal de Internet DC Cali

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



Ilustración 49 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.

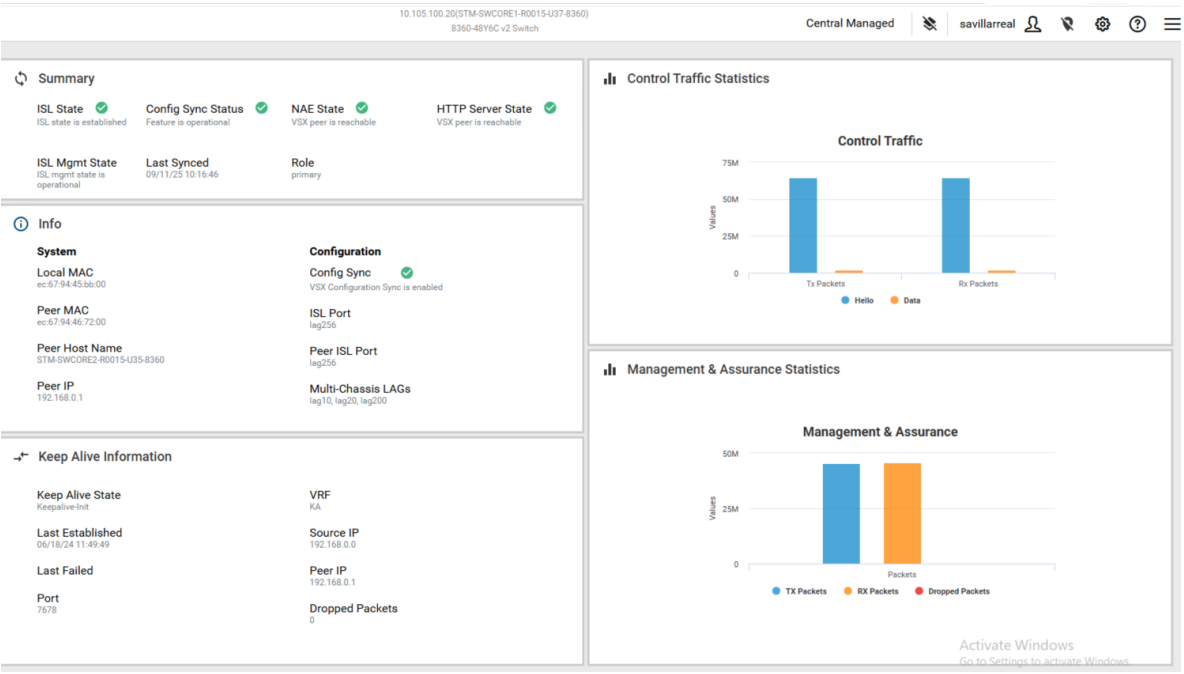


Ilustración 50 Estado HA SWCORE Datacenter alterno

Se verifica el canal MPLS de datacenter alterno, el cual se observa que se ha mantenido activo durante el mes de agosto 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.

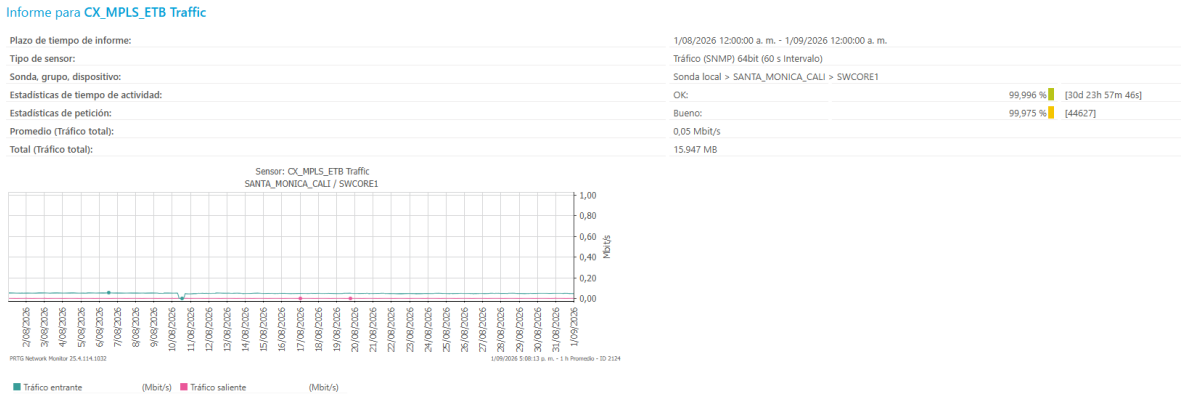


Ilustración 51 Consumo canal MPLS DC Alterno

Se verifica estado del equipo, donde se observa que presenta un uptime de 1 año y 21 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.

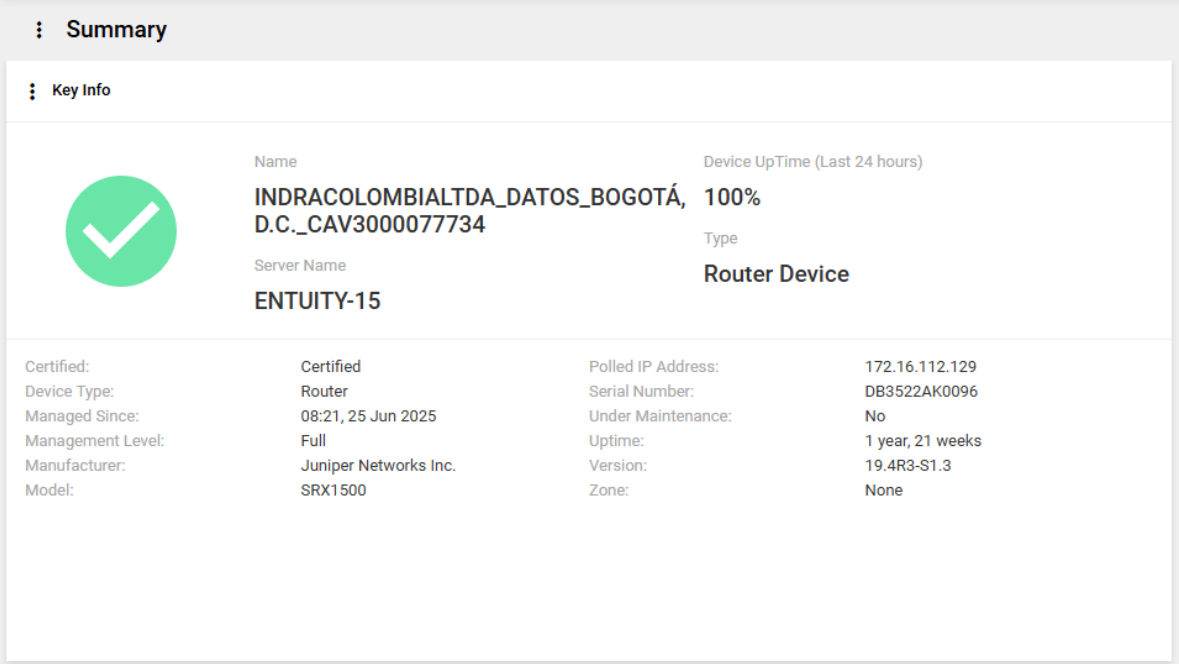


Ilustración 52 Estado Router MPLS DC Alterno

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 257 casos:

- 70 requerimientos de servicio relacionados a la asignación de licencias de Office
- 67 solicitudes de modificación de usuarios
- 27 requerimientos asociados a configuración o modificación de MFA.
- 12 solicitudes asociadas a la creación/modificación/eliminación de buzones compartidos.
- 23 solicitudes de inactivación de usuarios en AD.
- 25 solicitudes de configuración general.

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.

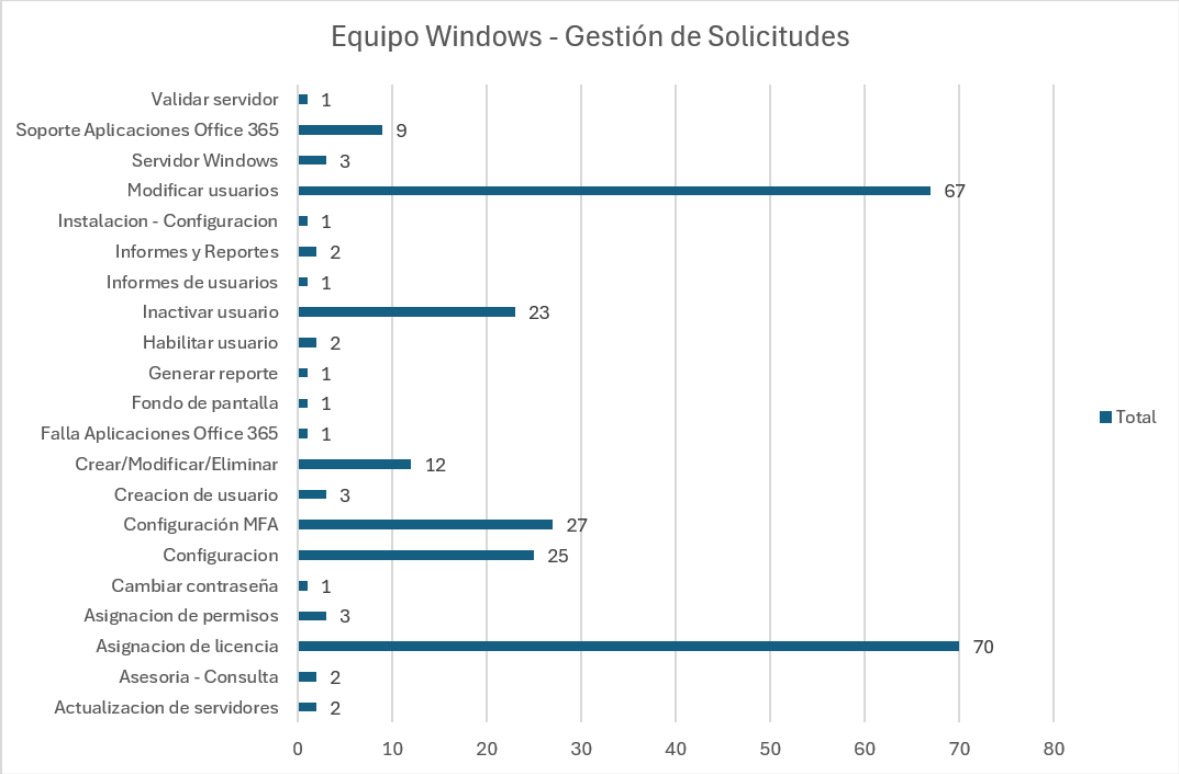


Ilustración 53 Gestión de Casos Windows

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, se realizó la solicitud a 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.

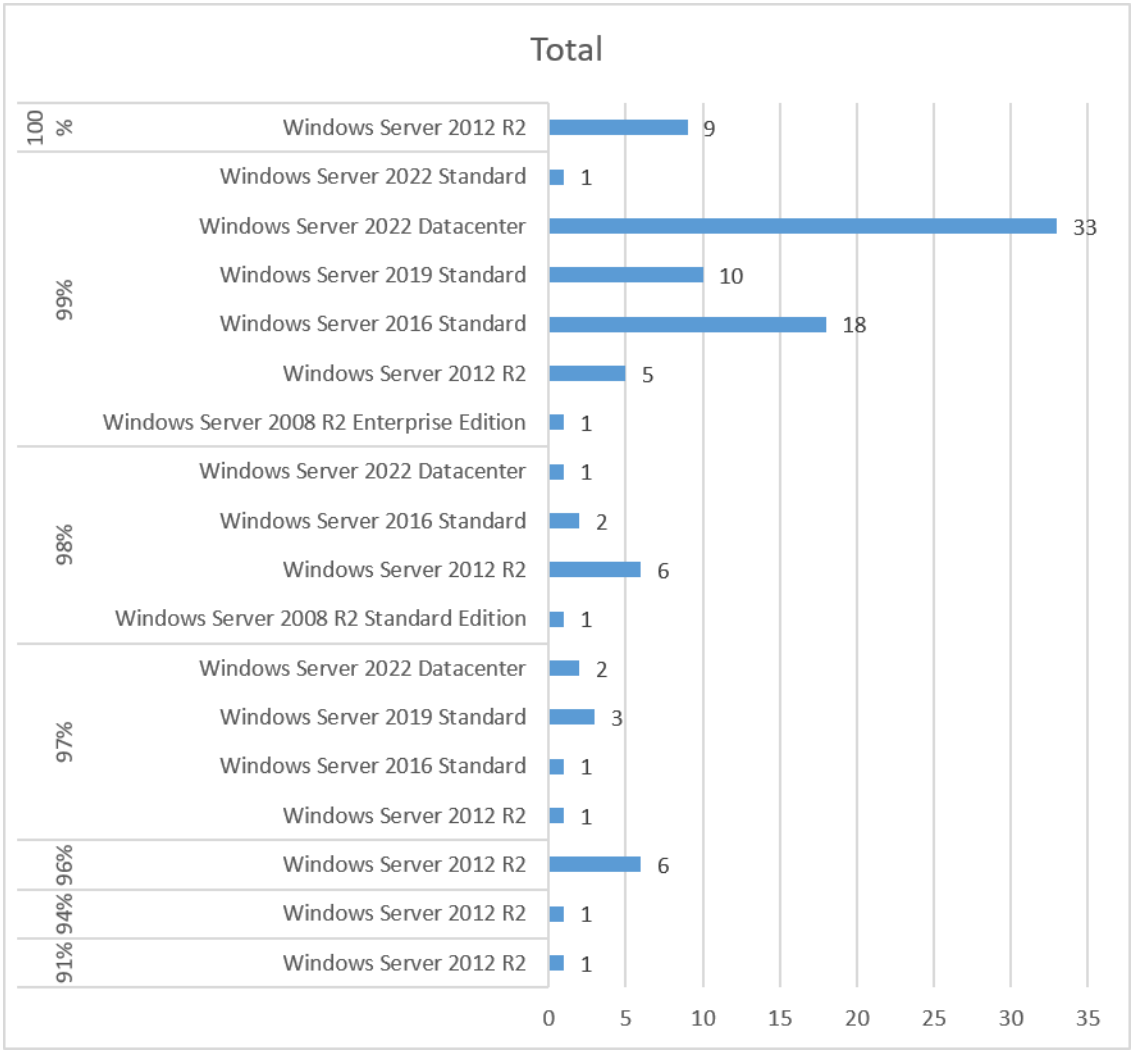


Ilustración 54 Cumplimiento WSUS

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.

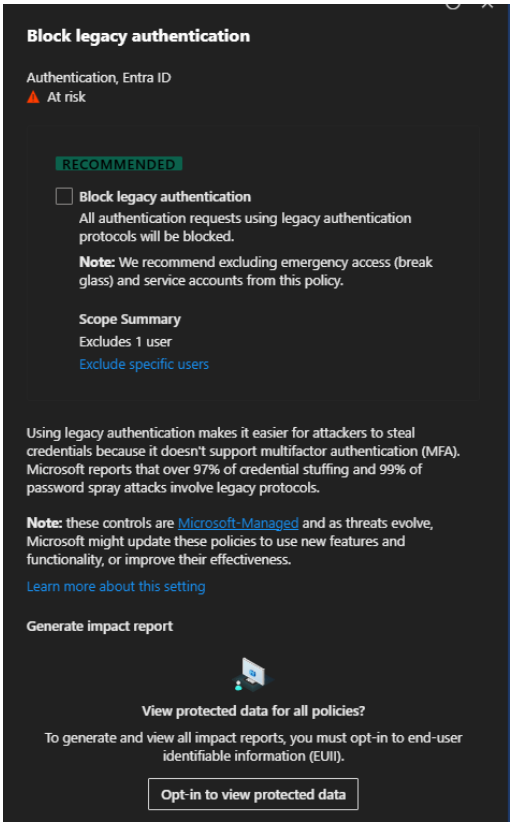


Ilustración 55 Block Legacy Authentication

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

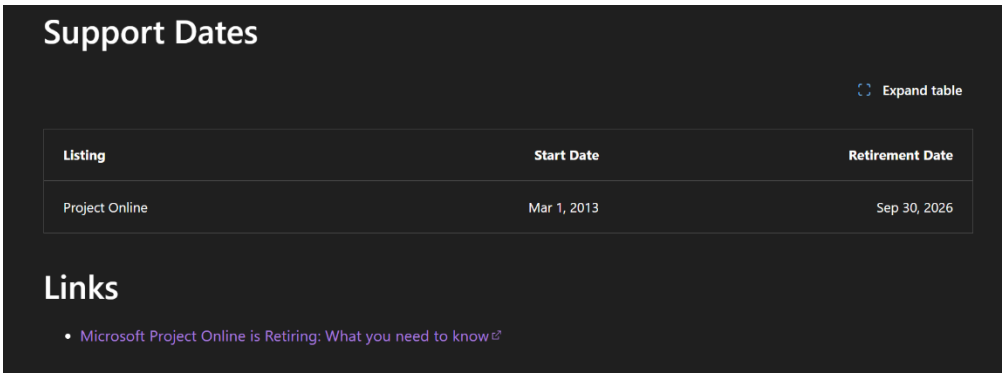


Ilustración 56 Fechas de Soporte

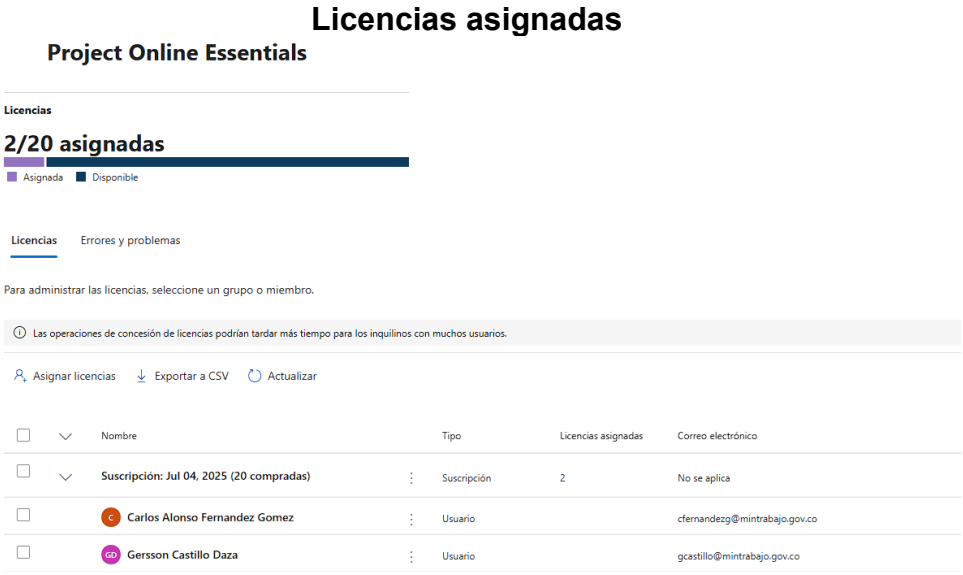


Ilustración 57 Licencias asignadas

3.1.3 Procesamiento, almacenamiento y respaldo - Nube Privada

Se continúa con la ejecución del plan de backups de la infraestructura 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 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 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. 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 58 solicitudes, 42 de las cuales corresponden a requerimientos de servicio, 8 incidentes y 8 solicitud de cambio. A continuación, se presentan las solicitudes y su estado al final del período.

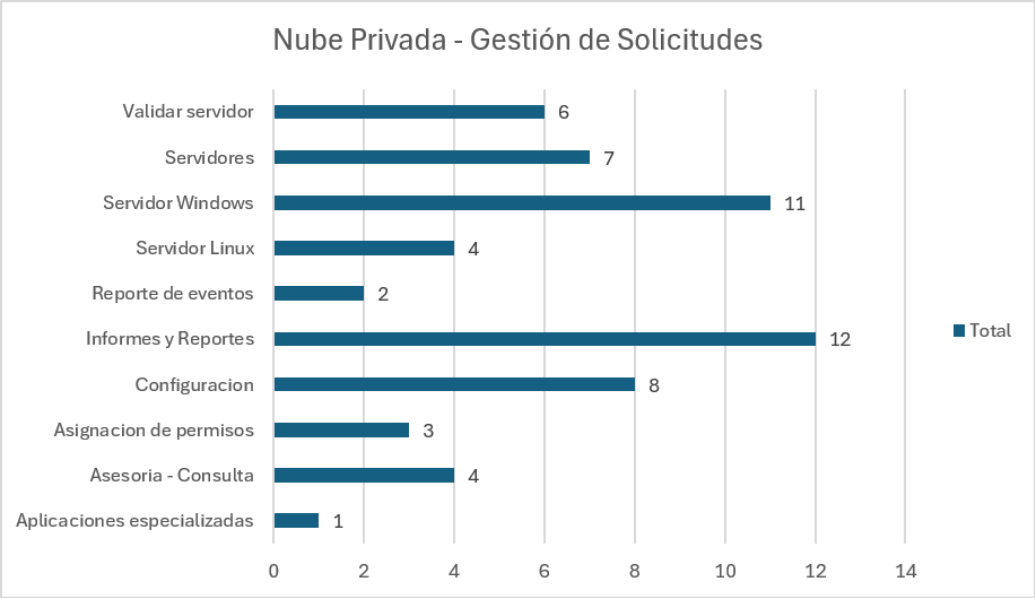


Ilustración 58 Gestión Nube Privada

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 42 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 43 *Capacidades modificatorio*

Durante agosto se evidenció un aumento en la utilización de recursos de infraestructura respecto a julio. El consumo de vCPU creció 6.5%, el de almacenamiento 6.7% y el de memoria RAM 0.3%.

Total MinT (Servidores Pruebas y Desarrollo)	
Descripción características	Total
vCPU	160
RAM	972 GB
Almacenamiento	28.2 TB
Numero de Servidores	40

Tabla 44 Total capacidades ambientes pruebas

- vCPU Ficha: **854** a vCPU consumida: **777 (91%)**
- Memoria Ficha: **3.3 TB** a Memoria consumida: **3.07 TB (93.03%)**
- Almacenamiento Ficha: **156 TB** a Almacenamiento consumido: **140 TB (89.74%)**
- 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 6 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 Asesment 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	**777**	**3.07 TB**	**140 TB**

Tabla 45 *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 parte del grupo IVC se reportó algunos inconvenientes en la aplicación migrada tales como, error en links de acceso y la funcionalidad de desbloqueo de usuarios. Tras validación de los especialistas, se evidenció que estas funcionalidades estaban apuntando al servidor anterior. Se realizó la corrección y el apuntamiento a la nueva infraestructura y se solucionó el inconveniente. 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

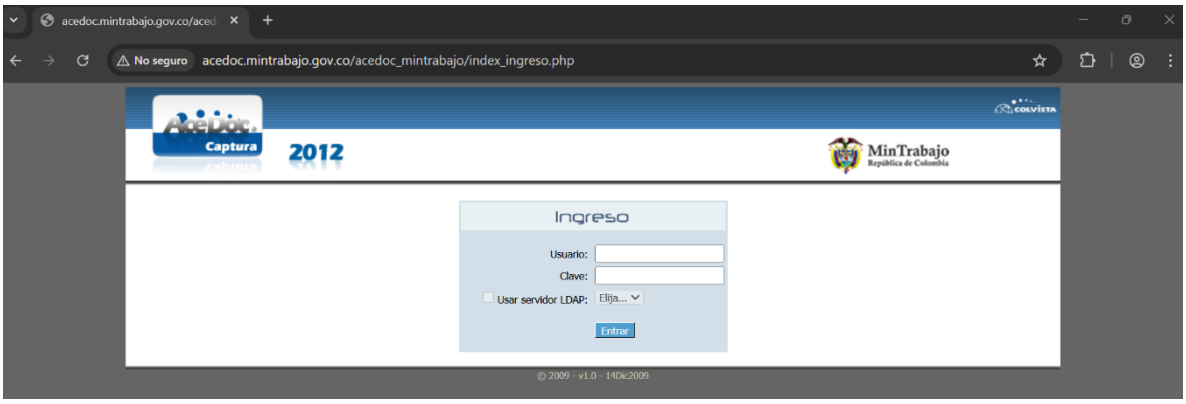


Ilustración 59 Nuevo entorno ACEDOC

Se comparte la información de gestión de casos por categoría del servicio de aplicaciones especializadas. En la herramienta Aranda se registraron un total de 543 solicitudes para el servicio, así:

- 463 requerimientos
- 75 incidentes
- 5 cambios

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

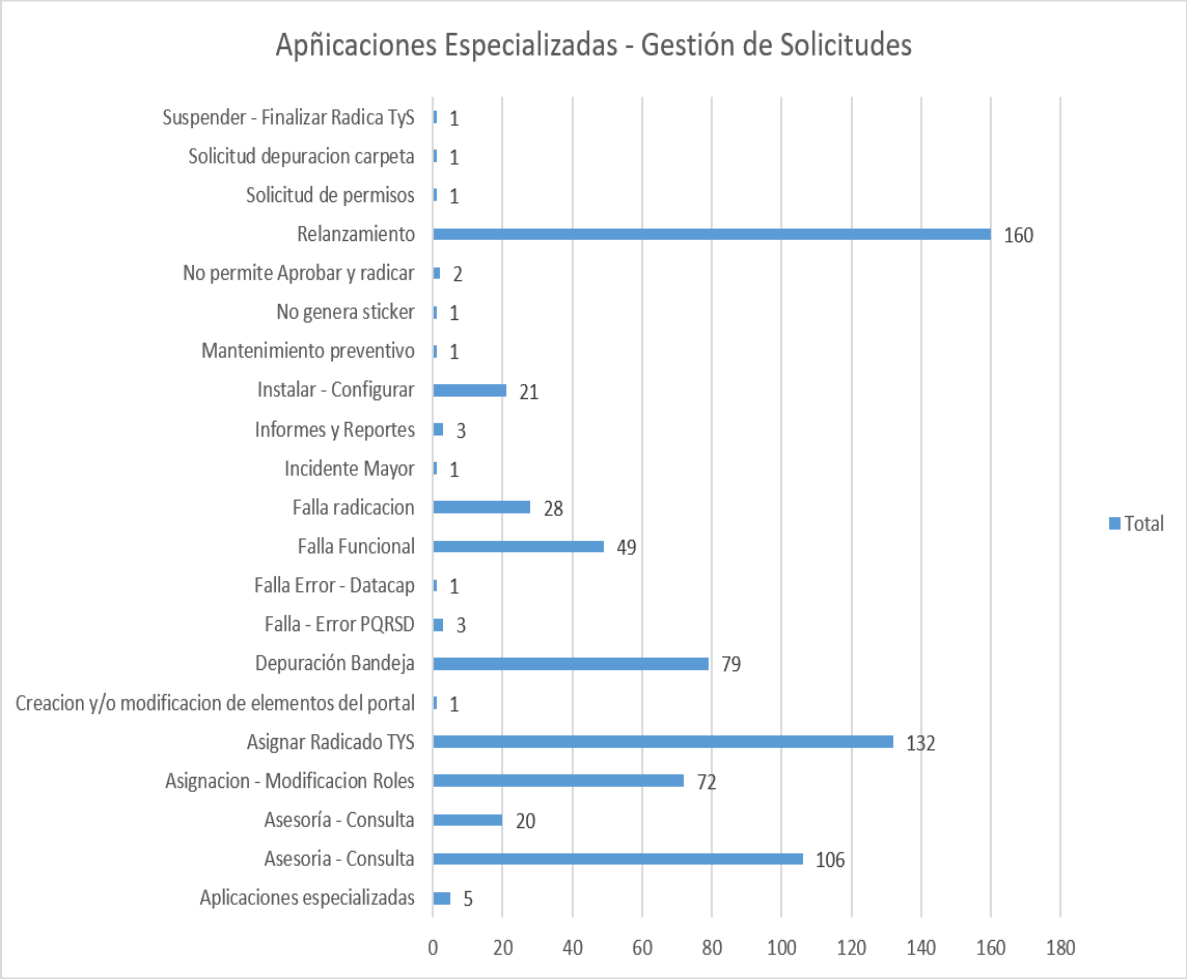


Ilustración 60 Gestión Apps Especializadas

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

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 comparte la información de gestión de casos por parte del Equipo de IBM, en la herramienta Aranda se registraron un total de 530 solicitudes para el servicio, así:

- 455 requerimientos
- 75 incidentes

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

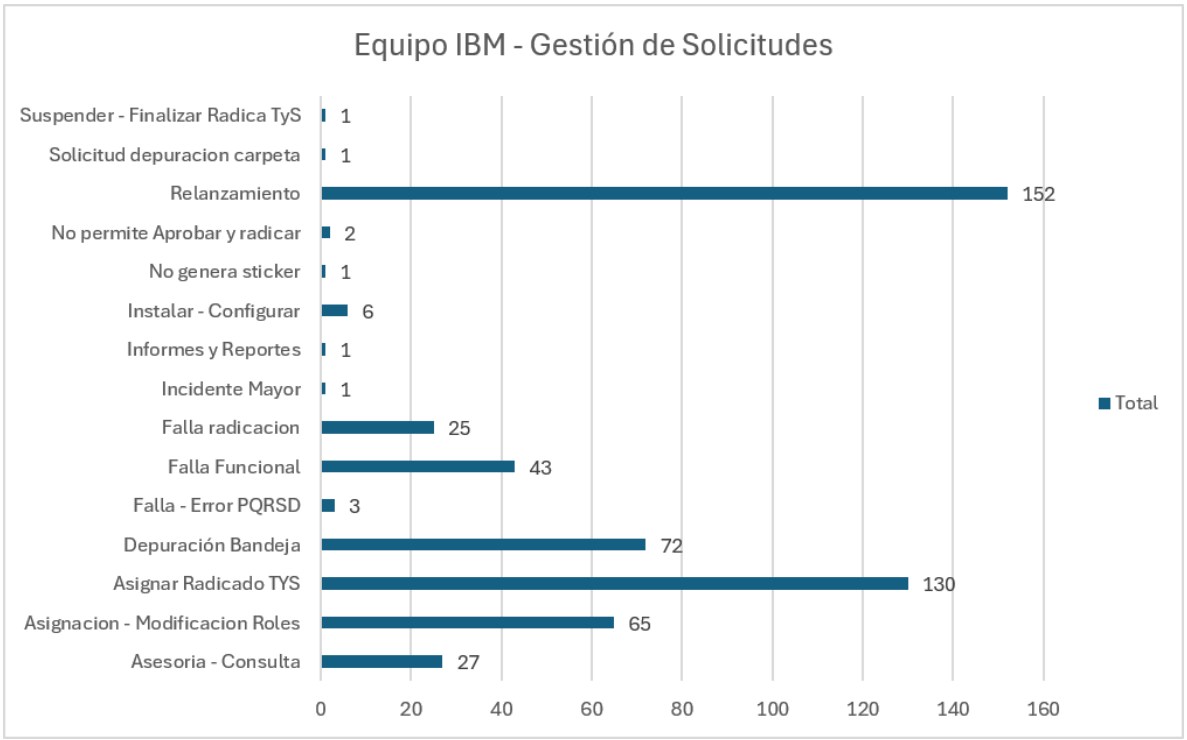


Ilustración 61 Gestión Casos IBM

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 (152 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 (130 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 (65 casos).
- Radicar una solicitud - Depuración de Bandeja (72 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 (43 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 motor 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
Agosto 2026	125848
Total acumulado	**1182786**

Tabla 46 *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
Agosto 2026	174720
Total acumulado	**1.600.326**

Tabla 47 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
Agosto 2026	68861
Total, acumulado	**609796**

Tabla 48 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 49 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 62 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 17 solicitudes, así:

- 12 requerimientos
- 5 cambios

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

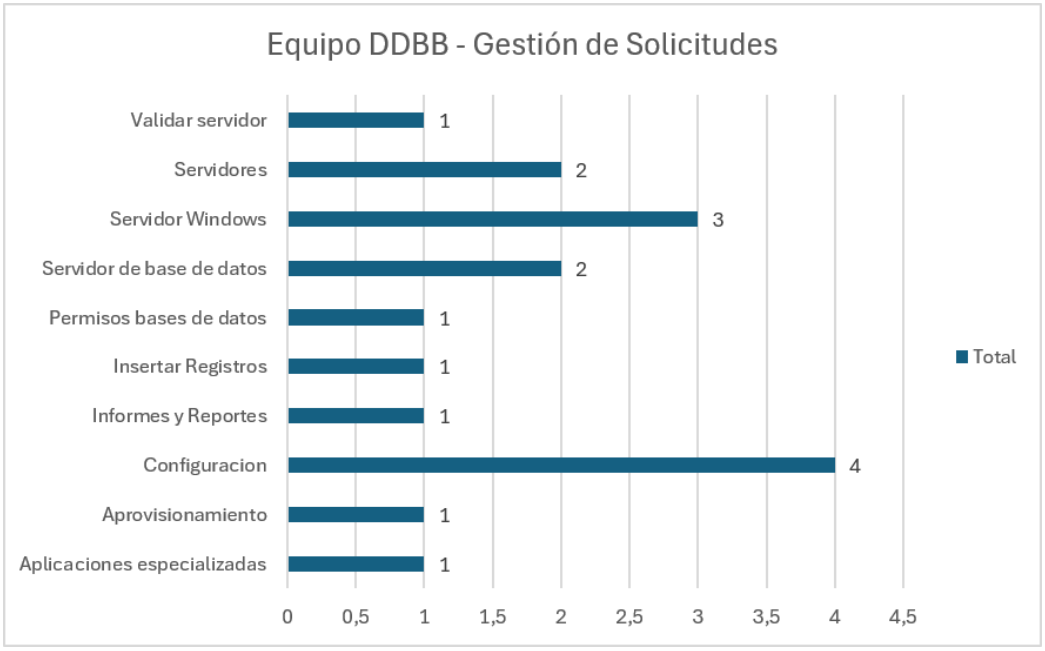


Ilustración 63 Gestión DDBB

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 Agosto se migró 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:

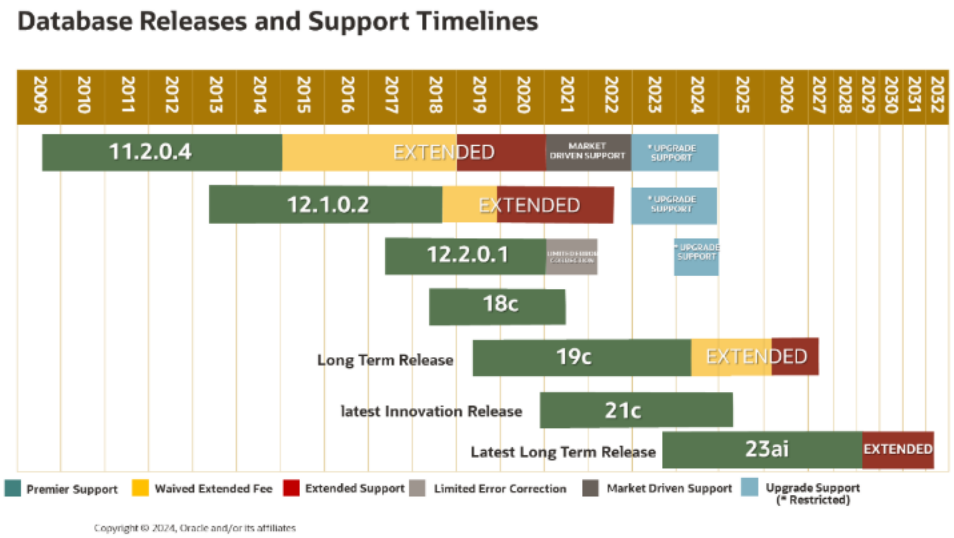


Ilustración 64 Estado Bases de Datos

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 50 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 agosto 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.

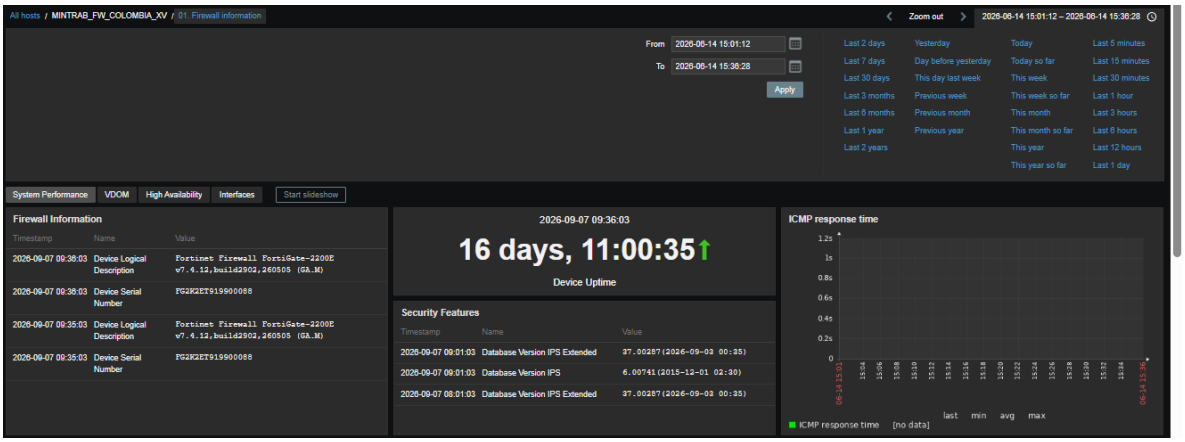


Ilustración 65 Firewall de nueva generación.

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 agosto. 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 – Agosto 2026
Tendencia general	Durante agosto de 2026 el tráfico presenta un comportamiento predominantemente cíclico. Se observa una mayor variación del tráfico recibido durante los primeros días del mes y posteriormente ciclos recurrentes de incremento y disminución. El tráfico enviado mantiene un comportamiento considerablemente más estable durante todo el periodo.
Volumen promedio	El tráfico recibido continúa predominando ampliamente sobre el tráfico enviado. De acuerdo con la escala de la gráfica, la recepción fluctúa aproximadamente entre 2 TB y 20 TB, dependiendo del día, mientras que el tráfico enviado se mantiene generalmente entre 0,5 TB y 3 TB.
Tráfico recibido (azul)	Presenta las mayores variaciones del periodo. El pico principal se observa aproximadamente entre el 4 y 6 de agosto, alcanzando valores cercanos a 20 TB. Posteriormente se identifica otro incremento relevante entre el 11 y 14 de agosto, cercano a 11–12 TB. Durante la segunda mitad del mes los volúmenes son menores, aunque se observan incrementos aproximados de 7–9 TB alrededor del 18–21 y 24–28 de agosto.
Tráfico enviado (amarillo)	El tráfico saliente presenta un comportamiento estable y considerablemente inferior al recibido, generalmente entre 0,5 y 3 TB. Se observan incrementos moderados alrededor del 3–6, 10–14, 18–21, 24–28 y 31 de agosto, sin evidenciarse en la gráfica incrementos extraordinarios o sostenidos del volumen saliente.
Días de mayor actividad	La mayor actividad se concentra principalmente entre el 3 y 6 de agosto, impulsada por el tráfico recibido, que alcanza el máximo mensual cercano a 20 TB. También se observan periodos relevantes aproximadamente entre el 10–14, 18–21 y 24–28 de agosto.
Días de menor tráfico	Se observan disminuciones importantes aproximadamente alrededor del 1–2, 8–9, 15–17, 22–23 y 29–30 de agosto. En algunos de estos periodos el tráfico recibido desciende aproximadamente hasta 2–4 TB.
Relación enviado/recibido	Se mantiene una marcada predominancia del tráfico recibido frente al enviado. Incluso durante el periodo de mayor actividad, el incremento está concentrado principalmente en recepción, mientras que el tráfico saliente conserva niveles relativamente estables. Este comportamiento es consistente con un entorno donde predomina el consumo de aplicaciones, navegación, servicios institucionales y servicios en la nube.

Tabla 51 Tendencia de uso de ancho de banda

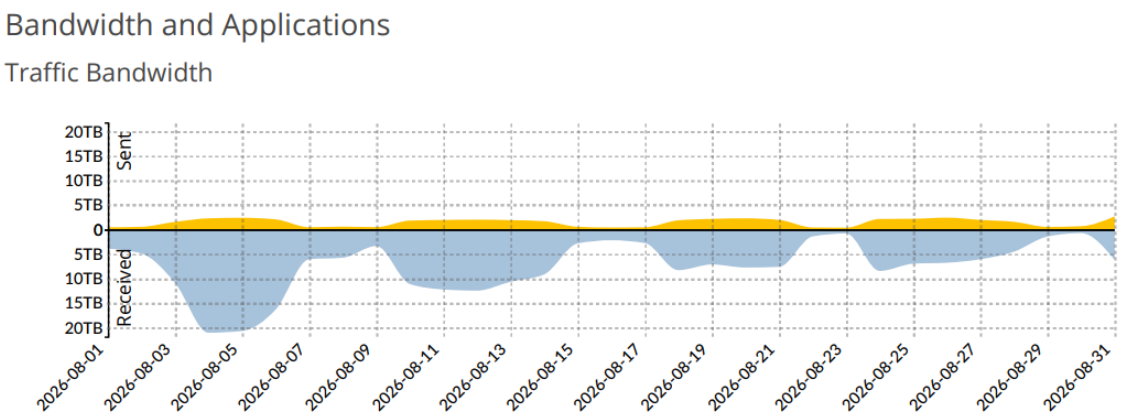


Ilustración 66 Comportamiento ancho de banda

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 agosto. 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	Nombre del activo	Función	Total aprox.	Observación / recomendación según función
1	172.20.22.167	MINTRABRUIPD.mintrabajo.loc	Servidor institucional	65.17 TB	Es el activo con mayor consumo del período, principalmente de tráfico recibido. .
2	172.20.22.27	MINTRAB19.mintrabajo.loc	File Server	10.49 TB	El volumen observado es coherente con la función de servidor de archivos, debido a las operaciones de consulta, descarga, almacenamiento y transferencia de información realizadas por los usuarios. Se recomienda mantener el monitoreo del consumo y verificar variaciones significativas frente a su línea base histórica.
3	172.20.44.102	MINTRABGD03A.mintrabajo.loc	Gestor Documental	6.35 TB	El tráfico registrado es consistente con un Gestor Documental, debido al intercambio permanente de documentos entre usuarios, aplicaciones y repositorios institucionales. S
4	172.28.28.38	MINTRAB60.mintrabajo.loc	File Server	5.81 TB	El predominio de tráfico saliente puede ser consistente con la función de File Server, dado que el servidor entrega archivos e información a usuarios y sistemas que los solicitan.
5	172.20.22.179	Por identificar	Por identificar	2.55 TB	El activo presenta un consumo moderado.
6	172.20.22.251	Por identificar	Por identificar	2.39 TB	El consumo se encuentra por debajo de los principales activos del período.
7	mduarteo	Usuario identificado	Estación/usuario	**2.13 TB**	El consumo corresponde a un usuario identificado. Se recomienda mantener el monitoreo habitual y revisar únicamente incrementos relevantes respecto de su comportamiento histórico o consumos que no correspondan con las funciones asignadas.
8	172.25.0.7	Por identificar	Por identificar	**1.99 TB**	Presenta un volumen relativamente bajo frente a los principales consumidores. Se recomienda

N.°	Usuario / IP	Nombre del activo	Función	Total aprox.	Observación / recomendación según función
					identificar el activo y su función para incorporar el comportamiento observado dentro de su línea base de tráfico.
9	172.16.60.10	Por identificar	Por identificar	**1.90 TB**	El volumen observado no destaca frente a los principales consumidores. Se recomienda completar la caracterización del activo y mantenerlo dentro del monitoreo regular de tráfico.
10	dparra	Usuario identificado	Estación/usuario	**1.66 TB**	Presenta el menor consumo dentro del Top 10. El comportamiento puede mantenerse dentro del monitoreo habitual, verificando desviaciones relevantes frente al patrón histórico del usuario.

Tabla 52 usuarios con mayor consumo de ancho de banda

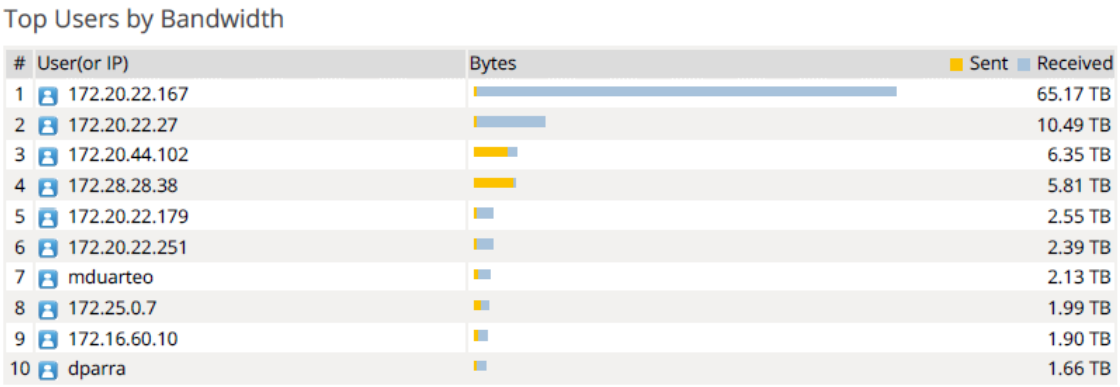


Ilustración 67 Tendencia de uso de ancho de banda

Top de usuarios por número de sesiones

La imagen corresponde al apartado “Top Users by Sessions” del informe perimetral de agosto 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.

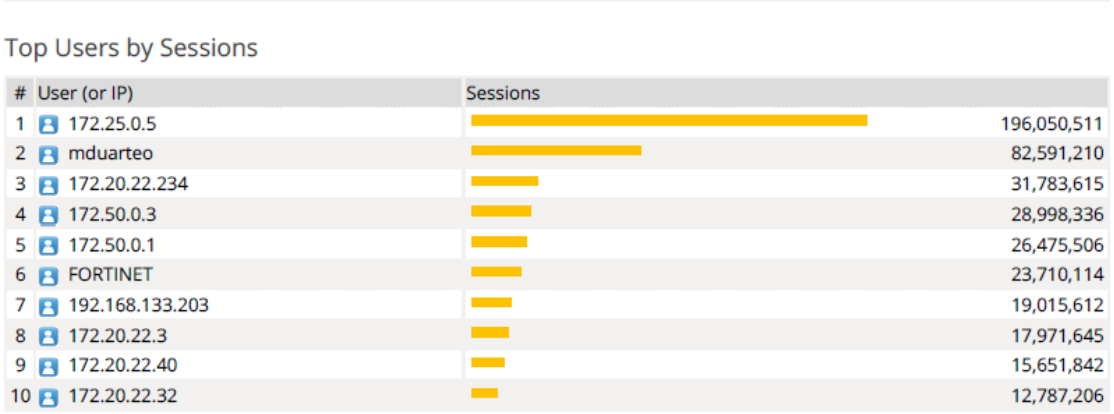


Ilustración 68 Top de usuarios por números de sesiones

Análisis Top Users by Sessions

N.°	Usuario/IP	Sesiones	Observaciones actualizadas
1	**172.25.0.5**	**203.125.021**	Registra la mayor cantidad de sesiones del período, concentrando un volumen significativamente superior al

			resto. Por su comportamiento, puede corresponder a un servidor, servicio centralizado o componente que canaliza múltiples conexiones. .
2	**172.20.22.40**	**47.178.523**	Presenta el segundo mayor número de sesiones, aunque considerablemente por debajo del primer activo.
3	**mduarteo**	**31.129.985**	Usuario con un volumen significativo de sesiones. Puede estar asociado a actividades recurrentes sobre plataformas o servicios institucionales.
4	**172.20.22.234**	**28.418.106**	Corresponde a un servidor interno asociado a un controlador de dominio. El elevado número de sesiones puede ser consistente con funciones de autenticación, consultas de directorio y comunicación permanente con equipos y servicios de la infraestructura institucional.
5	**FORTINET**	**20.539.356**	Corresponde a componentes de la infraestructura de seguridad Fortinet. El número de sesiones puede estar relacionado con actividades de inspección, administración y procesamiento de comunicaciones de seguridad. Se recomienda evaluar su comportamiento frente a la línea base propia de estos componentes.

Tabla 53 Top de usuarios por sesiones

Top Applications by Bandwidth

La imagen corresponde al apartado “Top Applications by Bandwidth” del informe perimetral de agosto 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).

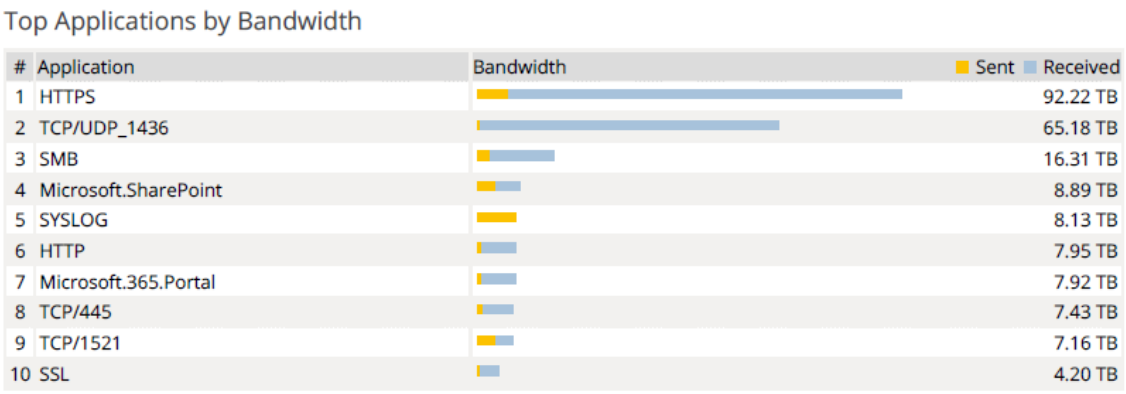


Ilustración 69 Top de aplicaciones

N.°	Aplicación / Protocolo	Ancho de banda	Descripción / análisis
1	HTTPS	92.22 TB	Es la aplicación/protocolo con mayor consumo de ancho de banda del período, con predominio significativo del tráfico recibido. El comportamiento es consistente con navegación web cifrada, aplicaciones institucionales, servicios cloud, plataformas SaaS y transferencia de información mediante HTTPS.
2	TCP/UDP_1436	65.18 TB	Registra el segundo mayor volumen del período, predominantemente de tráfico recibido..
3	SMB	16.31 TB	Corresponde al protocolo utilizado principalmente para compartición de archivos y recursos en red. El volumen observado

			es coherente con la presencia de File Servers institucionales y operaciones de consulta, descarga y transferencia de archivos. Se recomienda mantener monitoreo sobre accesos y volúmenes asociados a los servidores de archivos.
4	Microsoft.SharePoint	8.89 TB	Tráfico asociado al uso de Microsoft SharePoint, incluyendo consulta, carga, descarga, sincronización y colaboración sobre documentos institucionales. El comportamiento es consistente con el uso corporativo de Microsoft 365 y servicios documentales en la nube.
5	SYSLOG	8.13 TB	Corresponde a comunicaciones utilizadas para la centralización y envío de registros de eventos desde dispositivos, servidores y soluciones de seguridad hacia plataformas de monitoreo. El volumen puede estar relacionado con la generación continua de logs de la infraestructura. Se recomienda mantener control sobre las fuentes autorizadas y la capacidad de almacenamiento/procesamiento.
6	HTTP	7.95 TB	Corresponde a tráfico web mediante HTTP. Puede estar relacionado con aplicaciones internas, servicios heredados, actualizaciones o redirecciones. Debido a que HTTP no proporciona cifrado de manera nativa, se recomienda mantener identificados los servicios que aún lo utilizan y migrar a HTTPS cuando técnica y funcionalmente sea posible.
7	Microsoft.365.Portal	7.92 TB	Tráfico relacionado con el acceso a servicios corporativos de Microsoft 365, incluyendo autenticación, colaboración, correo y aplicaciones empresariales. El volumen observado es consistente con el uso institucional de servicios Microsoft en la nube.
8	TCP/445	7.43 TB	El puerto TCP/445 está principalmente relacionado con SMB/CIFS y servicios de compartición de archivos en entornos Windows. Su presencia es consistente con la operación de los File Servers identificados. Por su relevancia de seguridad, se recomienda mantener restringido su uso a segmentos, sistemas y usuarios autorizados y monitorear comunicaciones no habituales.
9	TCP/1521	7.16 TB	Puerto comúnmente asociado a comunicaciones con bases de datos Oracle. El volumen puede corresponder al intercambio de información entre aplicaciones y servidores de base de datos.
10	SSL	4.20 TB	Corresponde a comunicaciones cifradas identificadas como SSL/TLS. El comportamiento puede estar asociado a aplicaciones corporativas, servicios web y conexiones seguras con plataformas internas o externas. Presenta el menor volumen dentro del Top 10 analizado.

Tabla 54 Top de aplicaciones

Top 15 Authenticated Logins by VPN Connections

La imagen corresponde al apartado “Authenticated Logins” del informe perimetral de agosto 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	2026-08-03 07:02:35	155	217:19:54
2	jepinzon@noc_indra	ssl-tunnel	2026-08-01 05:48:17	147	425:10:09
3	cjimenez	ssl-tunnel	2026-08-02 16:36:17	115	106:05:13
4	mdrodriguez	ssl-tunnel	2026-08-11 08:37:59	78	113:57:32
5	Alopezv	ssl-tunnel	2026-08-25 09:35:42	77	04:35:52
6	lpiza	ssl-tunnel	2026-08-03 08:27:14	76	55:28:29
7	jgonzalezcu	ssl-tunnel	2026-08-02 20:23:47	74	39:41:01
8	ZGOMEZ	ssl-tunnel	2026-08-03 06:59:42	74	83:08:15
9	eyreyes	ssl-tunnel	2026-08-03 08:06:43	72	97:46:04
10	nquinteroca	ssl-tunnel	2026-08-06 07:01:16	72	83:13:28
11	rovalle	ssl-tunnel	2026-08-03 08:34:46	67	84:09:02
12	oidarraga	ssl-tunnel	2026-08-05 14:59:58	67	79:34:11
13	lanzola	ssl-tunnel	2026-08-01 00:05:39	66	138:45:46
14	aorozcoca	ssl-tunnel	2026-08-03 15:30:17	66	89:46:27
15	jbgiraldo	ssl-tunnel	2026-08-12 09:42:39	65	27:43:28

Ilustración 70 Top de Autenticación

Indicador	Descripción actualizada – Agosto 2026
Tipo de conexión	El 100 % de las conexiones mostradas corresponden al tipo SSL-Tunnel, manteniéndose la VPN SSL como mecanismo utilizado para el acceso remoto de los usuarios incluidos en el Top 15.
Usuarios más activos (por duración)	Los mayores tiempos acumulados corresponden a jepinzon@noc_indra (~425:10 h), contaccenter (~217:19 h), lanzola (~138:45 h), mdrodriguez (~113:57 h) y cjimenez (~106:05 h). Destaca especialmente jepinzon@noc_indra, cuyo tiempo acumulado es considerablemente superior al resto de usuarios mostrados.
Mayor duración total	El mayor tiempo acumulado corresponde a jepinzon@noc_indra, con aproximadamente 425 horas y 10 minutos, seguido por contaccenter, con aproximadamente 217 horas y 19 minutos. Son los únicos usuarios de la gráfica que superan las 200 horas acumuladas durante el período.
Mayor cantidad de conexiones	Los usuarios con mayor número de conexiones son contaccenter (155), jepinzon@noc_indra (147), cjimenez (115), mdrodriguez (78) y Alopezy (77). Estos valores reflejan una mayor recurrencia de conexión durante el período y deben analizarse considerando las funciones y necesidades de acceso remoto de cada usuario.
Duraciones elevadas (>200 h)	Se identifican dos usuarios con tiempos acumulados superiores a 200 horas: jepinzon@noc_indra (~425:10 h) y contaccenter (~217:19 h). En particular, el usuario asociado al NOC puede presentar tiempos elevados por actividades de soporte, monitoreo y administración remota. Se recomienda mantener seguimiento de estas cuentas conforme a los perfiles y horarios autorizados.
Duraciones medias-altas (100 h – 200 h)	Se identifican tres usuarios dentro de este rango: lanzola (~138:45 h), mdrodriguez (~113:57 h) y cjimenez (~106:05 h). Presentan un uso intensivo de la VPN, aunque considerablemente inferior al registrado por los dos usuarios con mayor duración.
Duraciones medias (50 h – 100 h)	Dentro de este rango se encuentran eyreyes (~97:46 h), aorozcoca (~89:46 h), rovalle (~84:09 h), ZGOMEZ (~83:08 h), nquinteroca (~83:13 h), oidarraga (~79:34 h) y lpiza (~55:28 h). Estos registros evidencian un uso recurrente de la VPN durante el período.

Duraciones bajas (<50 h)	Los menores tiempos acumulados corresponden a jgonzalezcu (~39:41 h), jbgiraldo (~27:43 h) y Alopezy (~04:35 h). En particular, Alopezy presenta 77 conexiones pero solo aproximadamente 4 horas y 35 minutos acumulados, lo que evidencia conexiones de corta duración y mayor recurrencia frente a su tiempo total conectado.
Comportamiento de reconexiones	Se destaca contaccenter con 155 conexiones y jepinzon@noc_indra con 147, seguidos por cjimenez (115). También resulta relevante Alopezy, que registra 77 conexiones con solo ~4:35 h acumuladas, comportamiento que puede estar asociado a sesiones breves o reconexiones frecuentes y que conviene contrastar con su patrón habitual de acceso.

Tabla 55 Consolidado de indicadores

Failed Login Attempts by User

Esta imagen corresponde al apartado “Failed Login Attempts” del informe perimetral de agosto 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	10,087
2	test	ssl-web	908
3	guest	ssl-web	297
4	thomas	ssl-web	264
5	charles	ssl-web	263
6	vpn	ssl-web	242
7	scanner	ssl-web	229
8	support	ssl-web	229
9	scan	ssl-web	210
10	david	ssl-web	205

Ilustración 71 sesiones fallidas

Análisis

Durante agosto 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 agosto de 2026, se generaron 4809 eventos analizados, los cuales fueron limpiados de algún tipo de amenazas



Ilustración 72 Reporte mensual

Este informe de rendimiento proporciona un análisis detallado del comportamiento y la eficiencia de FortiSandbox durante el mes de agosto. 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

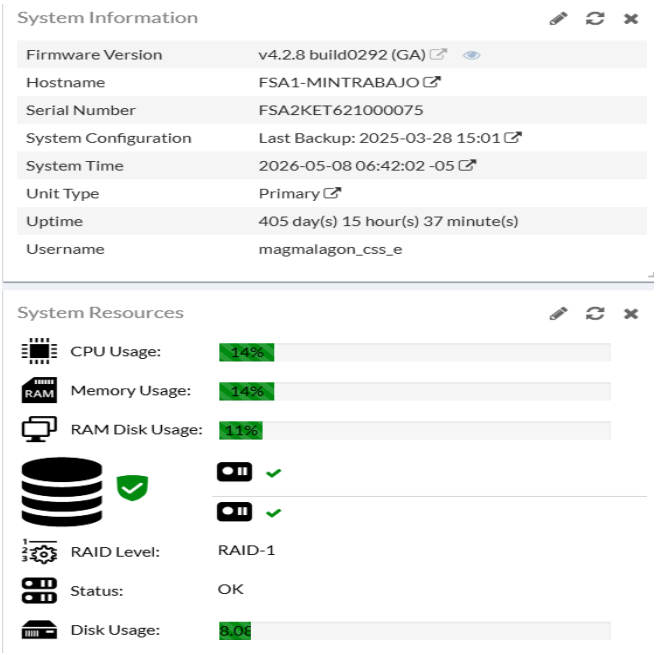


Ilustración 73 Captura de pantalla perfomance

Licencia Sandbox

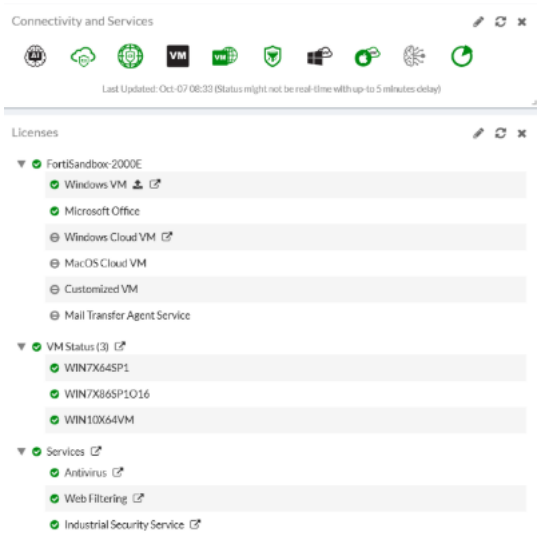


Ilustración 74 licencia sandbox

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

Durante agosto de 2026 la plataforma FortiSIEM procesó un promedio de 547 EPS (pico de 3,284 EPS) sobre la infraestructura del Ministerio del Trabajo, cubriendo sede central, 33 direcciones territoriales y 125 puntos de atención municipal. El análisis de correlación de eventos identificó 3 hallazgos altos y 2 hallazgos operativos gestionables a nivel técnico.

Criticidad	Hallazgo	Descripción
Alta	Large Outbound Transfer to Outside My Country (912 eventos)	Posible fuga de información institucional hacia un destino externo no corporativo; se recomienda implementar una solución DLP para fortalecer la prevención y control de exfiltración de datos.
Alta	Usuario casanabriap	Cuenta administradora del Directorio Activo con privilegios elevados.
Media	2,555 violaciones de política de navegación web	Actividad asociada a navegación de usuarios hacia páginas no permitidas por la política corporativa.
Baja	Tráfico anómalo hacia MediaFire — 9.27 TB, predominante descarga	Uso de almacenamiento no corporativo (shadow IT) y riesgo de fuga de datos

Infraestructura y capacidad de procesamiento (EPS)

El indicador de EPS (Events Per Second) permite evaluar si la plataforma SIEM opera dentro de su capacidad contratada y si el volumen de eventos generados por la infraestructura del Ministerio es consistente con meses anteriores.

Indicador	Valor Agosto 2026	Lectura de negocio
Pico máximo de eventos indexados	3,284 EPS	Dentro de capacidad contratada; sin degradación de servicio

Promedio de eventos indexados	547 EPS	Consistente con carga operativa habitual

Tabla 56 Fuentes de eventos

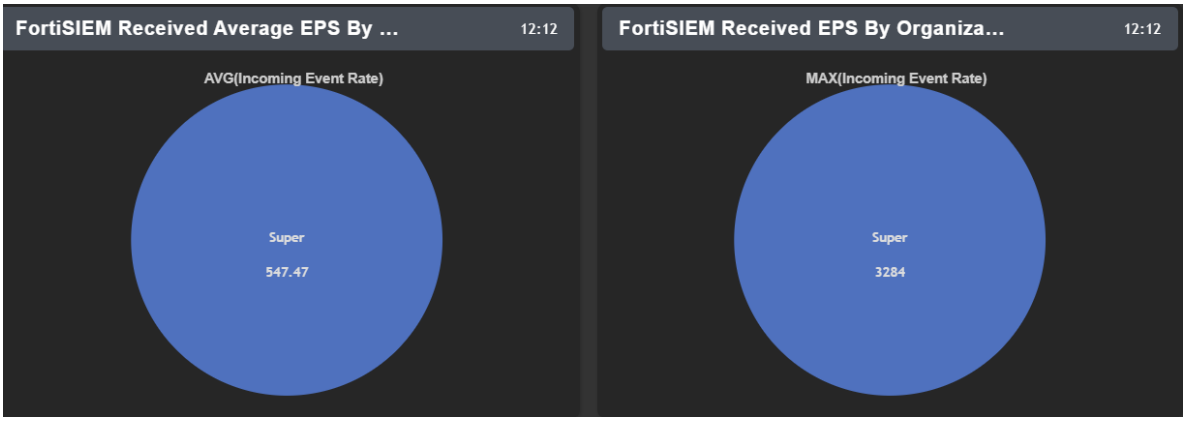


Ilustración 75 Comportamiento de EPS

3.1.6.3.1 Incidentes por Tipo

El mes de agosto 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:

#	Incidente	Casos	Probabilidad	Impacto	Criticidad	Activo / Usuario
1	Website access policy violation	2,555	Alta (recurrente)	Bajo-Medio	Media	Múltiples hosts
2	Large Outbound Transfer	956	Media	Medio	Media-Alta	Mintrab02, Mintrab107
3	Large Outbound Transfer to Outside My Country	912	Media	Alto	Alta	Mintrab104 / 201.234.143.90

Tabla 57 Tipos de incidentes

3.1.6.3.3. Top Applications by Bandwidth

- ISAKMP: 391.22 TB totales (178.77 TB enviados / 212.45 TB recibidos) uso intensivo de túneles VPN IPsec para interconexión entre sedes y acceso remoto seguro.
- SSL_TLSv1.3: 166.75 TB, predominio de tráfico recibido (159.08 TB) navegación HTTPS hacia aplicaciones web y plataformas SaaS.
- Trend.Micro.Services: 91.40 TB, predominantemente saliente (87.89 TB) telemetría, sincronización de políticas y actualización de firmas de seguridad; comportamiento esperado del endpoint gestionado.
- DTLS: 55.24 TB videoconferencia y comunicaciones en tiempo real sobre UDP cifrado.
- MediaFire (Storage.Backup): 9.27 TB, con 9.12 TB recibidos patrón de descarga masiva desde

FortiGate: Top Applications by Bandwidth

Application	Category	Total Bandwi...	Sent Bandwi...	SUM(Receiv
ISAKMP	Network.Service	391.22 TB	178.77 TB	212.45 TB
SSL_TLSv1.3	Network.Service	166.75 TB	7.66 TB	159.08 TB
Trend.Micro.Services	Cloud.IT	91.4 TB	87.89 TB	3.51 TB
DTLS	Network.Service	55.24 TB	8.16 TB	47.08 TB
SSL_TLSv1.2	Network.Service	16.89 TB	13.47 TB	3.41 TB
SSL_TLSv1.3.PQC	Network.Service	9.58 TB	387.79 GB	9.2 TB
MediaFire	Storage.Backup	9.27 TB	155.34 GB	9.12 TB
NTP	Network.Service	6.08 TB	3.92 TB	2.15 TB
STUN	Network.Service	3.95 TB	93.42 GB	3.86 TB
Google.Services	General.Interest	1.62 TB	355.99 GB	1.28 TB

Tabla 58 Hosts e IPs Implicados

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	Categoría	Conexiones	Evaluación de Seguridad
NTP	Network.Servce	**1.181.450**	Es la aplicación con mayor número de conexiones del período. NTP es utilizado para la **sincronización horaria de servidores, estaciones y dispositivos de infraestructura**. El alto número de conexiones puede ser consistente con consultas periódicas de múltiples activos; se recomienda mantener restringidos y controlados los servidores NTP autorizados.
Microsoft.Outlook	Email	**12.108**	Actividad asociada al servicio de **correo electrónico corporativo de Microsoft**. El volumen de conexiones es consistente con procesos de sincronización, consulta y envío/recepción de correo. Se considera tráfico esperado dentro de la operación institucional.
Amazon.Services	General.Interest	**1.092**	Corresponde a conexiones hacia servicios asociados a infraestructura de **Amazon/AWS**. El volumen es reducido frente a las aplicaciones principales.
WhatsApp_File.Transfer	Collaboration	**347**	Corresponde a actividades de **transferencia de archivos mediante WhatsApp**. Aunque el número de conexiones es bajo, por tratarse de transferencia de información mediante una plataforma externa, se recomienda mantener su monitoreo y verificar su correspondencia con las políticas institucionales de uso y manejo de información.
Duolingo	General.Interest	**93**	Aplicación asociada a servicios de aprendizaje de idiomas. Presenta un volumen bajo de conexiones. Se recomienda gestionar su acceso conforme a las **políticas institucionales de navegación y uso aceptable de Internet**.
QQ_Music	Video/Audio	**87**	Servicio de reproducción de contenido multimedia. El número de conexiones es bajo; se recomienda mantener su clasificación y control conforme a las políticas de navegación institucionales, especialmente respecto al consumo de recursos para fines no relacionados con la operación.
Waze	General.Interest	**35**	Servicio de navegación y geolocalización. Registra un número reducido de conexiones y no representa un volumen significativo dentro del período. Su acceso debe mantenerse sujeto a las políticas institucionales de navegación.
Computrace	General.Interest	**30**	Se identifican **30 conexiones** clasificadas por FortiGate como Computrace. Debido a que puede estar relacionado con funcionalidades de administración o seguimiento de dispositivos, se recomienda validar si corresponde a software

Aplicación	Categoría	Conexiones	Evaluación de Seguridad
			autorizado dentro del inventario institucional antes de establecer su legitimidad.
Google.Translate_Websites	General.Interest	**26**	Corresponde al acceso a servicios web de **Google Translate**. El número de conexiones es bajo y debe mantenerse dentro del monitoreo habitual y de las políticas institucionales de navegación.
Sumo.Logic	Cloud.IT	**3**	Servicio cloud relacionado con **gestión, análisis y monitoreo de logs**. Únicamente registra 3 conexiones. Si la plataforma forma parte de servicios autorizados, el comportamiento puede considerarse esperado; de lo contrario, se recomienda validar el origen de las conexiones.

Tabla 59 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 agosto 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 MINTRABGD06PD presentan más de 260 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.

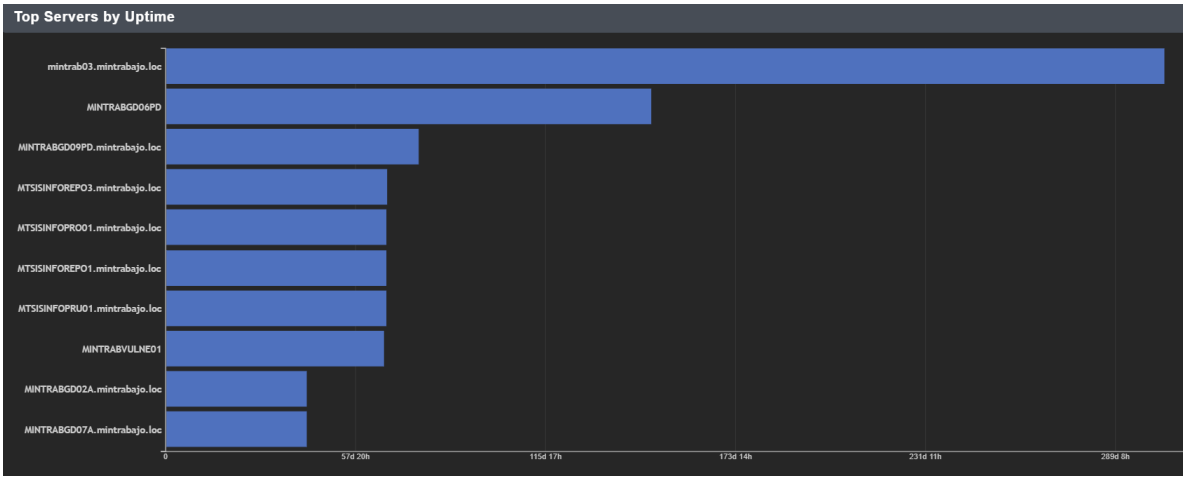


Ilustración 76 Detalle servidores

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

Durante el mes de agosto 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.

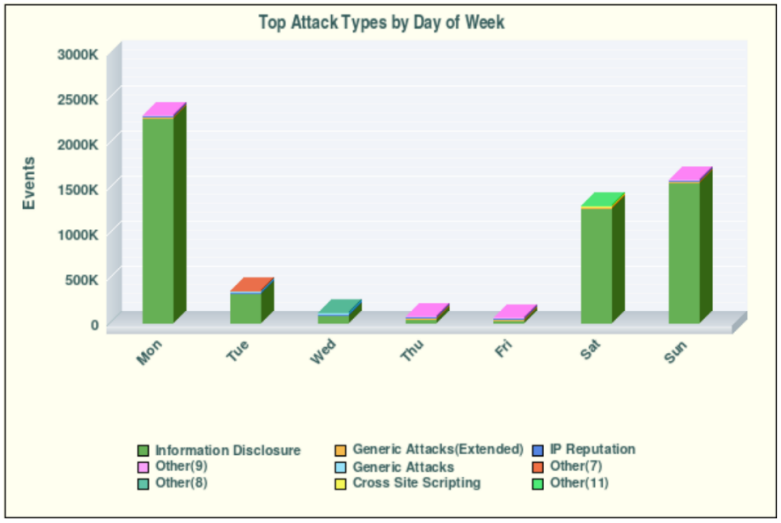


Ilustración 77 Top attack types

Análisis

Análisis	Descripción actualizada
Distribución de ataques por día	La mayor concentración de eventos se presenta el **lunes**, con aproximadamente **230.000–240.000 eventos**. Le siguen el **domingo**, con cerca de **170.000**, y el **sábado**, con aproximadamente **140.000–150.000 eventos**. De martes a viernes se observa una disminución significativa de la actividad, con volúmenes considerablemente inferiores.
Inicio de semana	El **lunes constituye el principal pico de actividad del período**, alcanzando aproximadamente **230.000–240.000 eventos**. El **martes** presenta una reducción significativa, ubicándose alrededor de **40.000–50.000 eventos**. La diferencia entre ambos días evidencia una alta concentración de eventos al inicio de la semana.
Mitad de semana	Durante **miércoles y jueves** la actividad disminuye considerablemente frente al lunes y martes. El miércoles registra aproximadamente **20.000–30.000 eventos**, mientras que el jueves se mantiene alrededor de **15.000–20.000 eventos**. Estos días representan niveles relativamente bajos dentro del comportamiento semanal observado.
Viernes	A diferencia del período anterior, el **viernes ya no representa el principal pico de actividad**. En la gráfica actual registra aproximadamente **15.000–20.000 eventos**, ubicándose entre los días de menor volumen. Se observa participación de categorías adicionales a Information Disclosure, aunque con una incidencia reducida frente a los principales días del período.
Fin de semana	Se evidencia un **incremento significativo durante el fin de semana**. El sábado registra aproximadamente **140.000–150.000 eventos**, mientras que el domingo alcanza cerca de **170.000**, convirtiéndose en el segundo día con mayor actividad. Este comportamiento demuestra que los eventos sobre los servicios expuestos continúan independientemente

Análisis	Descripción actualizada
	de la reducción de la actividad laboral institucional y es compatible con tráfico automatizado desde Internet.
Tipo de ataques predominantes	La categoría **Information Disclosure** presenta una predominancia clara durante el período, especialmente el **lunes, sábado y domingo**. También se identifican eventos de **Generic Attacks (Extended), Generic Attacks, Cross Site Scripting, IP Reputation** y las categorías agrupadas **Other (7), Other (8), Other (9) y Other (11)**, aunque con una participación considerablemente menor.
Information Disclosure	Constituye la **categoría dominante de la gráfica** y explica gran parte de los elevados volúmenes registrados el lunes, sábado y domingo. Estos eventos pueden estar asociados a solicitudes orientadas a obtener o identificar información expuesta por aplicaciones y servicios. Se recomienda mantener el seguimiento sobre los activos y URLs que concentran estas detecciones.
Ataques Cross Site Scripting (XSS)	La gráfica identifica eventos clasificados como **Cross Site Scripting**, aunque su participación es reducida frente a Information Disclosure. Estos eventos corresponden a intentos dirigidos contra aplicaciones web y deben mantenerse bajo seguimiento mediante las políticas y controles de protección implementados en el WAF.
Eventos asociados a reputación IP	Se identifican eventos clasificados como **IP Reputation**, aunque representan una proporción menor del total. Estos registros están asociados a comunicaciones provenientes de direcciones cuya reputación ha generado una clasificación de seguridad y deben continuar siendo gestionados conforme a las políticas de protección perimetral.

Tabla 60 Tipo de ataque

3.1.6.5 Solución de Anti-DDoS

Durante el período del mes de agosto, se registraron eventos 8 de ataques de denegación de servicio distribuido (DDoS) a las aplicaciones publicadas en internet por el Ministerio de Trabajo.

Top Attacks

Attack	SPP	Direction	Drops	Events
State Anomalies: Foreign packet (Out of State)	PAGINA_MINTRABAJO	Outbound	98	8

Ilustración 78 Top de ataques

Análisis Detallado:

PAGINA_MINTRABAJO también muestra un número bajo de intentos salientes bloqueados (98), lo que sugiere riesgo bajo en aplicaciones web institucionales.

3.1.6.5.1 Login Fallidos

Durante el mes de agosto 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 agosto 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 318 gestionados por el equipo de analistas, especialistas, líder SOC y demás especialistas que apoyan la gestión:

No. Caso	Fecha Registro	Asunto	Grupo Responsable	Categoria
RFC-294159	4/08/2026 10:55	Firewall	SOC	Firewall
RF-328400	31/08/2026 8:25	Asesoria - Consulta	SOC	Asesoria - Consulta
RF-309020	13/08/2026 14:41	Validación Habilitación Puertos USB	SOC	Validación Habilitación Puertos USB
RF-328540	31/08/2026 11:28	Validación Habilitación Puertos USB	SOC	Validación Habilitación Puertos USB
RF-317948	18/08/2026 16:19	Solicitud Backup	SOC	Solicitud Backup
RF-308375	12/08/2026 11:52	Agregar puertos	SOC	Agregar puertos
RF-323189	24/08/2026 15:36	Crear politica	SOC	Crear politica
RF-306007	11/08/2026 15:11	Permitir acceso	SOC	Permitir acceso
RF-319239	19/08/2026 16:04	Permitir acceso	SOC	Permitir acceso
RF-328428	31/08/2026 9:08	Permitir acceso	SOC	Permitir acceso
RF-327168	28/08/2026 9:49	Asesoria - Consulta	SOC	Asesoria - Consulta
RF-328660	31/08/2026 15:41	Asesoria - Consulta	SOC	Asesoria - Consulta
RF-319082	19/08/2026 10:32	Instalacion - Configuracion	SOC	Instalacion - Configuracion
RF-328637	31/08/2026 14:46	Instalacion - Configuracion	SOC	Instalacion - Configuracion
RF-319028	19/08/2026 8:24	Reporte de Vulnerabilidades	SOC	Reporte de Vulnerabilidades
RF-293703	3/08/2026 10:08	Reportes Seguridad Informática	SOC	Reportes Seguridad Informática
RF-303589	10/08/2026 12:58	Reportes Seguridad Informática	SOC	Reportes Seguridad Informática
RF-303603	10/08/2026 14:07	Reportes Seguridad Informática	SOC	Reportes Seguridad Informática
RF-303644	10/08/2026 14:49	Reportes Seguridad Informática	SOC	Reportes Seguridad Informática
RF-321626	21/08/2026 7:46	Reportes Seguridad Informática	SOC	Reportes Seguridad Informática
RF-294132	4/08/2026 10:23	Revisar correo malicioso	SOC	Revisar correo malicioso
RF-294136	4/08/2026 10:27	Revisar correo malicioso	SOC	Revisar correo malicioso
RF-303467	10/08/2026 9:30	Revisar correo malicioso	SOC	Revisar correo malicioso
RF-303468	10/08/2026 9:31	Revisar correo malicioso	SOC	Revisar correo malicioso
RF-320566	20/08/2026 15:03	Revisar correo malicioso	SOC	Revisar correo malicioso
RF-320575	20/08/2026 15:12	Revisar correo malicioso	SOC	Revisar correo malicioso
RF-323077	24/08/2026 12:22	Revisar correo malicioso	SOC	Revisar correo malicioso
RF-326744	26/08/2026 16:17	Revisar correo malicioso	SOC	Revisar correo malicioso
RF-326882	27/08/2026 10:45	Revisar correo malicioso	SOC	Revisar correo malicioso
RF-327018	27/08/2026 15:55	Revisar correo malicioso	SOC	Revisar correo malicioso
RF-328646	31/08/2026 14:56	Análisis vulnerabilidades	SOC	Análisis vulnerabilidades
RF-298120	6/08/2026 12:51	Análisis de Correos	SOC	Análisis de Correos
RF-319064	19/08/2026 9:52	Análisis de Correos	SOC	Análisis de Correos
RF-311383	14/08/2026 13:57	Análisis de Malware	SOC	Análisis de Malware
RF-293805	3/08/2026 13:47	Asesoria - Consulta	SOC	Asesoria - Consulta
RF-294139	4/08/2026 10:28	Asesoria - Consulta	SOC	Asesoria - Consulta
RF-294141	4/08/2026 10:29	Asesoria - Consulta	SOC	Asesoria - Consulta
RF-327161	28/08/2026 9:40	Agregar Listas blancas	SOC	Agregar Listas blancas
RF-320465	20/08/2026 11:43	Analisis de archivo	SOC	Analisis de archivo
RF-326865	27/08/2026 10:04	Analisis de archivo	SOC	Analisis de archivo
RF-328398	31/08/2026 8:20	Análisis Equipo de Computo	SOC	Análisis Equipo de Computo
RF-294330	4/08/2026 15:47	Configuracion consola	SOC	Configuracion consola
RF-308214	12/08/2026 8:01	Configuracion consola	SOC	Configuracion consola
RF-311417	14/08/2026 14:38	Configuracion consola	SOC	Configuracion consola
RF-326868	27/08/2026 10:20	Configuracion consola	SOC	Configuracion consola
RF-293712	3/08/2026 10:29	Generación de reportes	SOC	Generación de reportes
IM-321817	21/08/2026 15:42	Exploración de puertos o servicios no autorizada	SOC	Exploración de puertos o servicios no autorizada

No. Caso	Fecha Registro	Asunto	Grupo Responsable	Categoria
IM-323099	24/08/2026 14:04	Exploración de puertos o servicios no autorizada	SOC	Exploración de puertos o servicios no autorizada
IM-328453	31/08/2026 9:25	Bloqueo Navegador	SOC	Bloqueo Navegador
IM-328381	31/08/2026 7:43	Falla - error	SOC	Falla - error
IM-328402	31/08/2026 8:25	Falla - error	SOC	Falla - error
IM-328403	31/08/2026 8:26	Falla - error	SOC	Falla - error

Tabla 61 Reporte de requerimientos agosto

3.1.6.7 Análisis de riesgo

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

- **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 62 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 63 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 64 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 agosto 2026, se realizó la revisión, ajuste, observaciones de algunos procedimientos y políticas que describimos a continuación:

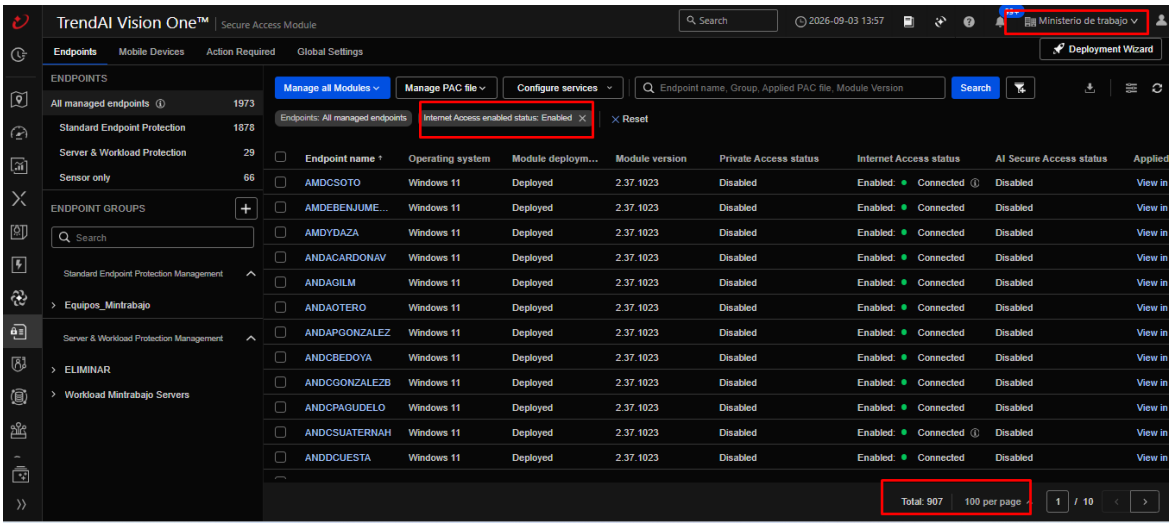


Ilustración 79 Políticas y procedimientos

Actualmente, el servicio de Zero Trust Network Access (ZTNA) se encuentra implementado con optimización de las reglas de acceso a Internet. A la fecha, se han desplegado 907 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 31/12/2026	Vigente	**IBM (10896)**
LIFERAY	Del 01/08/2025 hasta el 31/12/2026	Vigente	**LIFERAY**

Tabla 65 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 numero 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.

Almacenamiento

- 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%	100,00%
DC-2	Continuidad y disponibilidad del datacenter principal	100,00%	100,00%
DC-3	Continuidad y disponibilidad del datacenter alterno	100,00%	100,00%

ID	Indicadores	Resultado	Meta
DC-4	Continuidad y disponibilidad de la plataforma de procesamiento, almacenamiento y respaldo	100,00%	100,00%
DC-5	Tiempo de solución de incidentes asociado a los servicios de aplicaciones especializadas	97,25%	97,25%
DC-6	Tiempo de solución de requerimientos asociado a los servicios de aplicaciones especializadas	100,00%	100,00%
DC-7	Continuidad y disponibilidad de los servicios de directorio activo	100,00%	100,00%
DC-8	Continuidad y disponibilidad de los servicios de seguridad informática	100,00%	100,00%
DC-9	Tiempo de solución de incidentes asociado a los servicios de administración, soporte y monitoreo	98,85%	98,85%
DC-10	Tiempo de solución de requerimientos asociado a los servicios de administración, soporte y monitoreo	99,15%	99,15%
DC-11	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 66 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 67 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 agosto, 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.

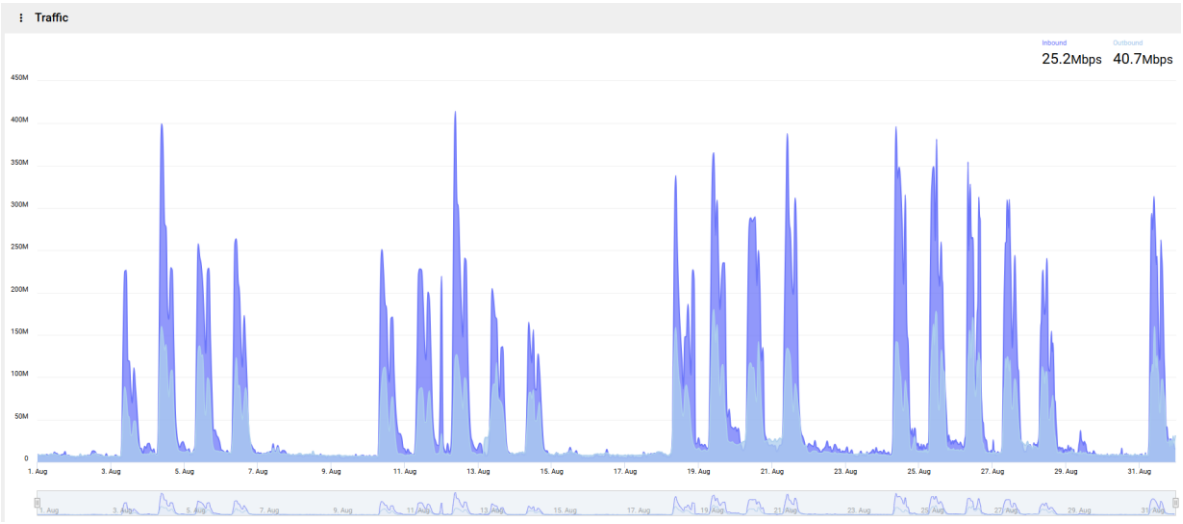


Ilustración 80 Consumo canal MPLS DC Principal

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 16 semanas y tiene consumo promedio de CPU no superior de 1.33% y de memoria de 40.7%, no se presenta problemas de procesamiento de equipo.

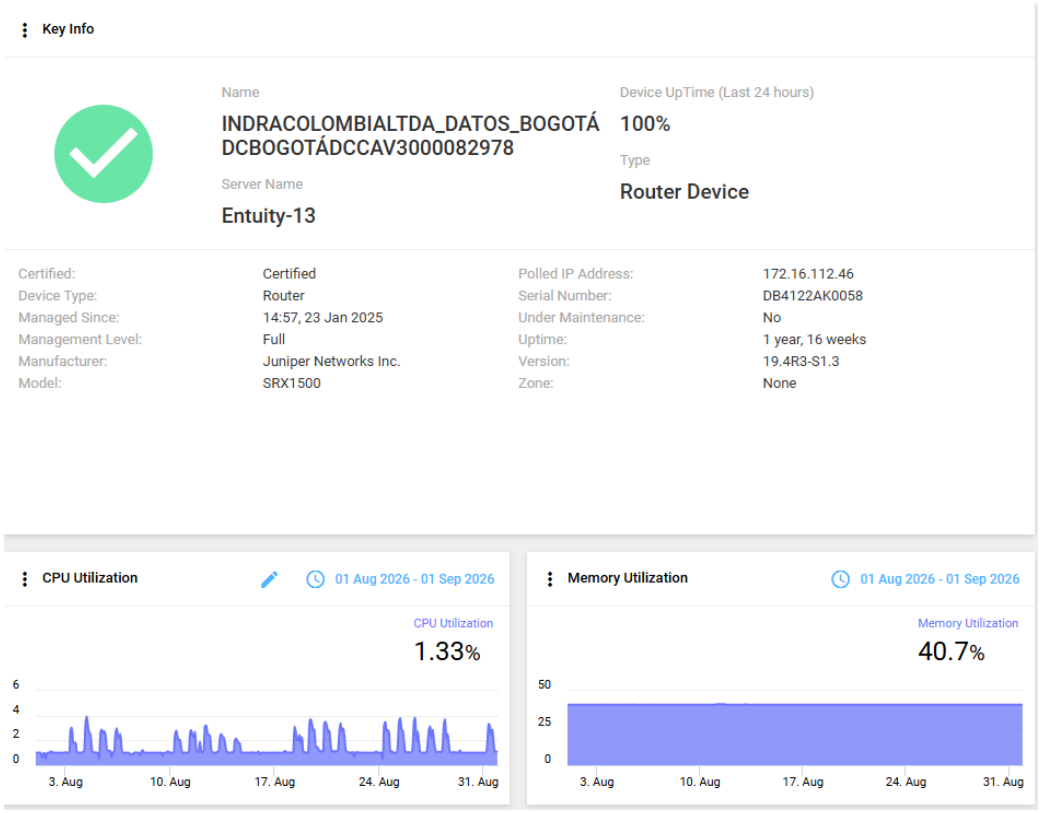


Ilustración 81 Estado Router MPLS DC Principal

3.3.1.1 Incidentes de Conectividad

Durante el mes de agosto, 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
Barrancabermeja	IM-308982	97,99%
Quibdó	IM-320611	81,32%
Tunja	IM-308518 / IM-308866 / IM-309126 / IM-325308	98,66%
Cúcuta	IM-308783 / IM-325311	98,27%
Pasto	IM-320445	99,42%
Guarne	IM-325324	92,14%
Santa Bárbara	IM-294247	77,50%
Campo de la Cruz	IM-303429	85,62%
Carmen de Bolívar	IM-293645 / IM-330798	97,89%
Magangué	IM-291345	98,90%
Puerto Boyacá	IM-303425	85,63%
Soatá	IM-293957 / IM-322962	79,74%
Riosucio Caldas	IM-303419	85,63%
Funza Mosquera	IM-308226	80,37%
La Unión	IM-327099	97,98%
Barbosa	IM-303427	74,07%

Tabla 68 Incidentes de conectividad

3.3.1.2 Topología Actual

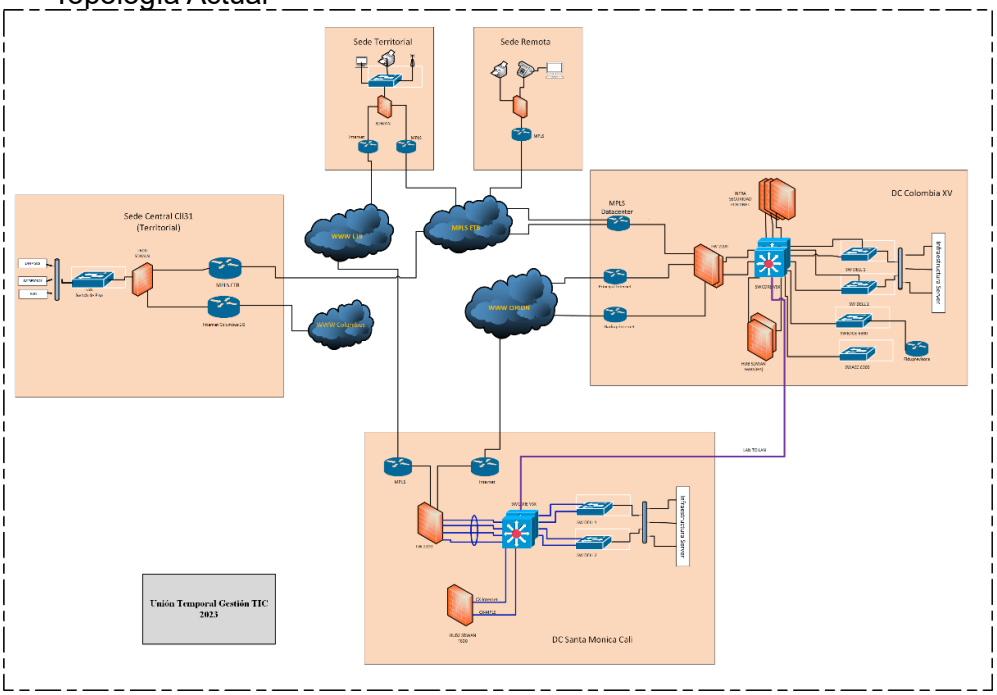


Ilustración 82 Topología actualizada

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. SDWAN

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.

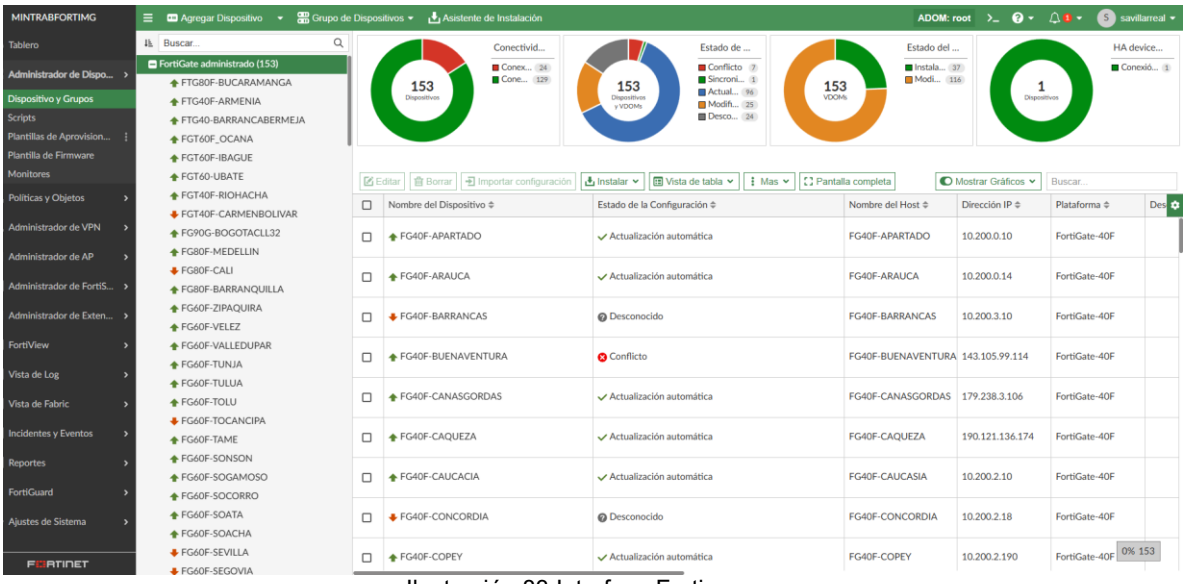


Ilustración 83 Interface Fortimanager

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 159.17 Mbps de consumo con un máximo de 1.19 Gbps, este canal es de 2GB, con el tráfico generado se observa que no presentó saturación durante el mes.

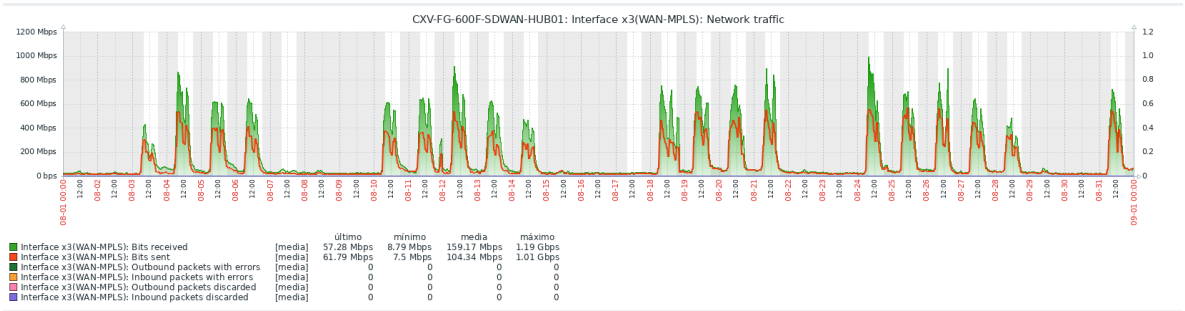


Ilustración 84 Interface MPLS HUB SDWAN

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 30.76 Mbps de consumo en el mes donde se tuvo un máximo de 726 Mbps. Este canal es de 1GB, con el tráfico generado en el mes, no se presentó saturación.

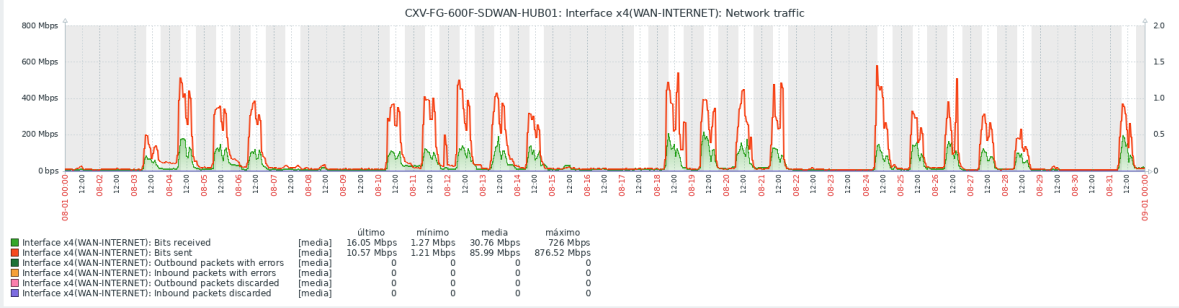


Ilustración 85 Interface Internet HUB SDWAN

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

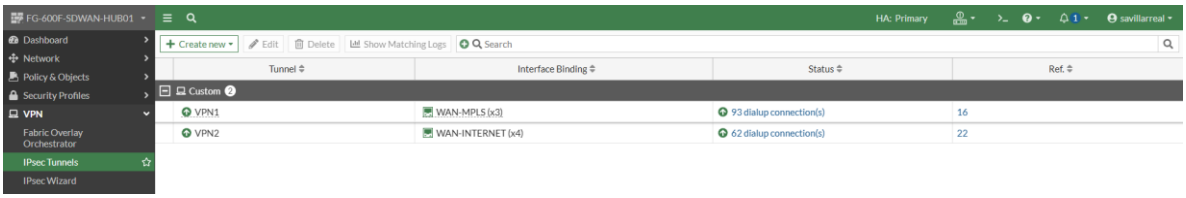


Ilustración 86 VPN SDWAN establecidas

El comportamiento del HUB SDWAN en cuanto a memoria, se observa que no ha tenido alto procesamiento, se observa un pico máximo de 25% de utilización de memoria, el equipo ha trabajado de forma estable sin presentar picos que causen algún bloqueo o algún reinicio de este.

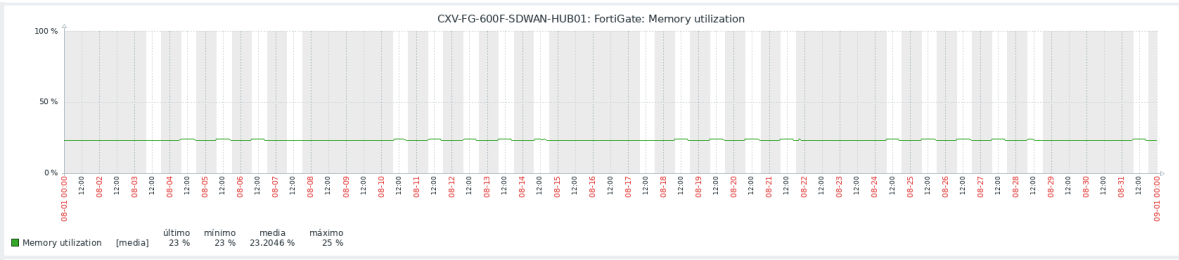


Ilustración 87 Estado HUB SDWAN Datacenter

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.

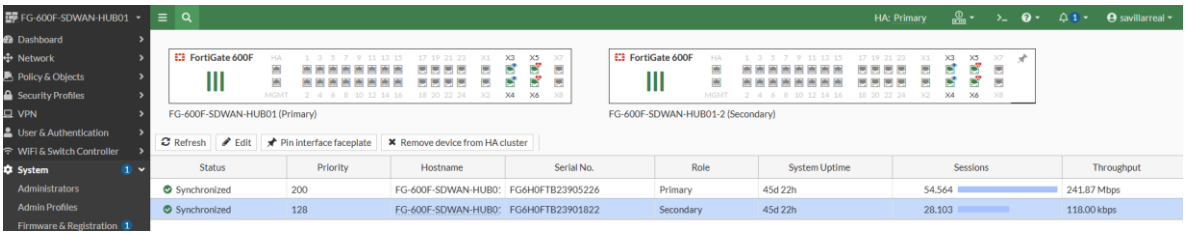


Ilustración 88 Estado HA HUB Sdwan

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

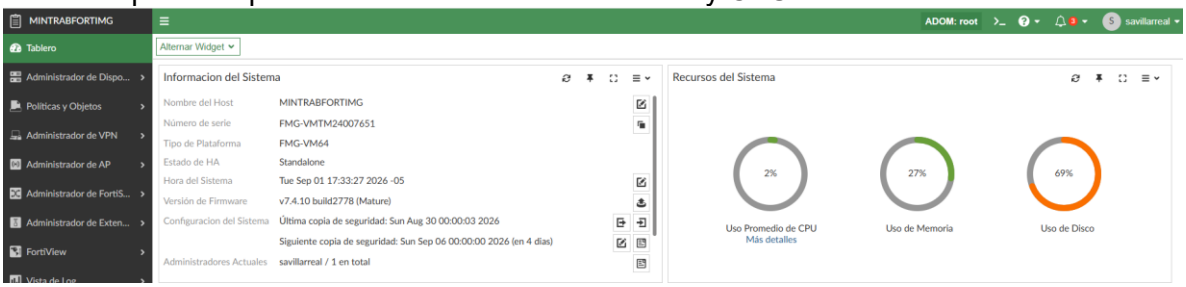


Ilustración 89 Recursos Fortimanager

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 69 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 agosto:

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

Inspección	Caso Asociado	% de Disponibilidad	% Penalidad	Valor Penalidad un enlace
Guarne	IM-325324	92,14%	10%	$ 32.699
Santa Bárbara	IM-294247	77,50%	20%	$ 65.398

Campo de la Cruz	IM-303429	85,62%	10%	$	32.699
Carmen de Bolívar	IM-293645 / IM-330798	97,89%	3%	$	9.810
Magangué	IM-291345	98,90%	3%	$	9.810
Puerto Boyacá	IM-303425	85,63%	10%	$	32.699
Soatá	IM-293957 / IM-322962	79,74%	20%	$	65.398
Riosucio Caldas	IM-303419	85,63%	10%	$	19.629
Funza Mosquera	IM-308226	80,37%	20%	$	65.398
La Unión	IM-327099	97,98%	3%	$	9.810
Barbosa	IM-303427	74,07%	50%	$	163.496
Total				**$**	**506.846**

Tabla 70 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
Barrancabermeja	IM-308982	97,99%	3%	$ 25.694
Quibdó	IM-320611	81,32%	20%	$ 256.939
Tunja	IM-308518 / IM-308866 / IM-309126 / IM-325308	98,66%	3%	$ 38.541
Cúcuta	IM-308783 / IM-325311	98,27%	3%	$ 51.388
Pasto	IM-320445	99,42%	3%	$ 38.541
Total				**$ 411.103**

Tabla 71 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**	1123	49
Equipos portátiles	**1000**	963	157
Equipos portátiles adicionales	**120**		
Total	**2292**	**2086**	**206**

Tabla 72 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 de recibe el lineamiento de no asignación de equipos a contratistas.

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 continúa aplicando 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 AGOSTO		
SEDE	**ESCRITORIO**	**PORTATIL**
DT Arauca	1	0
DT Atlántico	7	1
DT Bogotá	5	3
DT Bolivar	1	1
DT Boyacá	0	1
DT Caldas	1	0
DT Casanare	1	0
DT Guajira	1	0
DT Magdalena	0	1
DT Meta	0	1
DT Norte de Santander	0	1
DT Putumayo	0	1
DT Santander	2	1
DT Sucre	1	1
DT Tolima	2	1
DT Valle del Cauca	0	1
Inspección Acacias	1	0
Nivel Central	4	34
TOTAL	**27**	**48**

Tabla 73 Cantidades de equipos asignados nivel nacional

DEVOLUCION DE EQUIPOS AGOSTO		
SEDE	**ESCRITORIO**	**PORTATIL**
DT Antioquia	1	
DT Arauca	1	
DT Atlántico	7	3
DT Bogotá	7	2
DT Bolivar	1	
DT Boyacá	1	1

DT Caldas	1	
DT Caquetá		1
DT Casanare	1	
DT Cauca	2	
DT Guajira		1
DT Magdalena		1
DT Santander	1	1
DT Sucre	1	1
DT Tolima		2
Inspección Chinácota	1	
Inspección Girardot	1	
Nivel central	11	55
TOTAL	**37**	**68**

Tabla 74 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.

Adicionalmente, durante la primera semana de agosto, se realiza la recolección de los tres (3) equipos portátiles HP ProBook 440 propiedad de la UT que se encontraban en el Piso 25 – Nivel Central en la modalidad de alquiler desde febrero 2026. Se realiza remplazo de equipos cuando fue necesario.

- **Gestión de Garantías:**

Durante el mes de agosto, se registró un total de **26 casos de garantía**. A continuación, se detallan los estados correspondientes a cada uno de estos casos

Estado de caso	Cantidad
Cerrado	10
Proceso	1
Suspendido	15
Total	**26**

Tabla 75 Estado de casos de garantía.

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

ANS	Cerrado	Proceso	Suspendido	Total
CUMPLE	10	1	15	26
NO CUMPLE				
Total	**10**	**1**	**15**	**26**

Tabla 76 ANS casos de garantía.

Fecha de Reporte	Serial	Parte	Falla	Sede	No. Caso	Estado
20/08/2026	HC3BBMX7	Diadema	Audio distorsionado	Nivel Central	RF-320507	Cerrado

Fecha de Reporte	Serial	Parte	Falla	Sede	No. Caso	Estado
20/08/2026	HC3BBLHL	Diadema	El sonido no funciona	Santander	RF-320456	Cerrado
19/08/2026	AVLC39SA5BJ	Mouse	No da clic ni se mueve	Barrancabermeja	RF-319192	Cerrado
18/08/2026	VNAA62G4	Monitor	Líneas	Puerto Asis	RF-317724	Cerrado
12/08/2026	3B809PY	Cargador	Carga lenta	Nivel Central	RF-308306	Cerrado
11/08/2026	AVLC39SA4KB	Mouse	Clic derecho no funciona	Cesar	RF-305879	Cerrado
14/08/2026	VNAA62MT	Monitor	líneas horizontales.	Yopal	RF-311443	Cerrado
13/08/2026	VNAA64AX	Monitor	líneas horizontales	Bolivar	RF-309130	Cerrado
11/08/2026	VNAA62D2	Monitor	Líneas horizontales	Sucre	RF-306031	Cerrado
4/08/2026	VNAA63GM	Monitor	líneas verticales, distorsión	Magdalena	RF-294320	Cerrado
31/08/2026	MJ0LS489	Cpu	Se reinicia y/o apaga	Sucre	RF-328709	En proceso
25/08/2026	PW0A3BL6	Portatil	Equipo no enciende	Sahagun	RF-325290	Suspendido
20/08/2026	PW0A3BQ0	Portatil	No recibe Carga	Barrancabermeja	RF-320541	Suspendido
3/08/2026	PW0A3BD9	Portatil	No carga	Yopal	RF-293723	Suspendido
28/08/2026	HC3BBLSE	Diadema	Interferencia	Cesar	RF-327330	Suspendido
27/08/2026	VNAA61ZK	Monitor	Líneas horizontales	Bolivar	RF-326986	Suspendido
26/08/2026	VNAA63ML	Escritorio	Líneas horizontales	La Dorada	RF-326690	Suspendido
24/08/2026	HC3BBL1J	Diadema	Dejo de funcionar	Atlántico	RF-323150	Suspendido
19/08/2026	HC3BAHN4	Diadema	Audio no funciona	Malaga	RF-319069	Suspendido
13/08/2026	VNAA64BX	Monitor	líneas rosas	Amazonas	RF-308921	Suspendido
4/08/2026	PW0A3CFZ	Portatil	No carga	Nivel Central	RF-294116	Suspendido
30/08/2026	MJ0LS5WY	Cpu	No enciende	Buenaventura	RF-328362	Suspendido
24/08/2026	VNAA64HC	Monitor	Distorsión gráfica	Apartado	RF-323140	Suspendido
19/08/2026	VNAA64KD	Monitor	presenta colores distorsionados	Cauca	RF-319211	Suspendido
19/08/2026	VNAA61TC	Monitor	presenta colores distorsionados	Cauca	RF-319204	Suspendido
18/08/2026	MJ0LS5CK	Monitor	Bloqueos operativos	Cauca	RF-317782	Suspendido

Tabla 77 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

Funcionario responsable	Serial	DT	Parte afectada	Estado	Caso Aseguradora/ Lenovo
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	Pendiente Reposición	PRG_2026_2206888
Ana Mireya Escobar Tierradentro	MJ0LS5TW	Popayán/	No enciende	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 reposición de equipo PW0A370B.	PRG_2025_4160302
Adriana Patricia Martínez Arévalo	PW09Z369	Nivel central	Equipo no da imagen	Aseguradora realiza reposición 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 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	Aseguradora 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 encuentre en proceso con aseguradora	PRG_2026_2209296
Marino Alexander Pantoja Reyes	PW0A3BE5	Ipiales	Daño en teclado	Se realiza reparación del equipo por parte de la aseguradora	PRG_2026_2208716

Funcionario responsable	Serial	DT	Parte afectada	Estado	Caso Aseguradora/ Lenovo
Johana Faride Guevara Espinel	PW0A36XX	Bucaramanga	Puerto de entrada de carga no recibe voltaje	Pendiente reparación por parte de aseguradora	PRG_2026_2207852
Yurley Katherine Castro Sánchez	PW0A3CEG	Nte de Santander	Hurto	Pendiente reposición por parte de aseguradora	PRG_2026_2797172

Tabla 78 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 26 solicitudes tipificadas así:
  - Incidentes: 0 casos
  - Requerimientos: 26 casos

- Al corte de mes de agosto quedaron en estado:
  - Cerrado: 10 casos.
  - Proceso: 1
  - Suspendido: 15 casos.

- 26 casos corresponden a solicitudes de usuarios estándar y 0 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	25
Gestor de inventarios	1
Total, general	

Tabla 79 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	**26**
Equipo Periférico	**13**
Equipo Escritorio	**10**
Equipo Portátil	**3**
Total	**26**

Tabla 80 Solicitudes de Equipos Usuario Final – Según Grupo Responsable

4.1.2 Equipos de Escritorio

Durante el mes de agosto, 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 agosto 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 81 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 actualizaron los esquemas de red de todas las oficinas territoriales y esquemas de piso de sede central.
- Se corrigió vulnerabilidad SSH Server CBC Mode Ciphers Enabled reportada en Switch Aruba Mocoa y vulnerabilidad SSH Weak MAC Algorithms Enabled, SSH Weak Exchange Algorithms Enable reportada en switch SW2960-MINTRABAJO-WTC-P25-SW1.
- Se amplió el canal MPLS de sede central y se configuró en la regla de SD-WAN para balancear el tráfico.
- Desde el equipo de redes se creó una nueva red WiFi exclusiva para el despacho de la ministra y su equipo de trabajo cercano, se configuró nuevo segmento de red, nuevo SSID y se configuraron permisos de navegación con la ayuda del SOC. Esto se hizo bajo el caso Aranda RF-308889.
- Se trabajó en el aseguramiento de los puertos de acceso de los dispositivos de SD-WAN en cada una de las oficinas para el escaneo de vulnerabilidades.
- Se adelanta revisión e identificación de los puntos de red de la DT Bogotá para un total de 89 puntos incluidos los Access Point. En proceso de generación del informe con los hallazgos para presentarlo al ministerio.
- Se reporta falla del punto de datos P19-PPA D-02 en el Piso 19 – Nivel Central debido a que no está dando red. El Coordinador del Grupo de Soporte Informático

solicita al área responsable en la entidad gestionar la revisión del punto por el personal técnico del edificio.



RE_ Solicitud
Certificación Punto de

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

- Los especialistas gestionaron un total de 9 solicitudes escaladas a través de la herramienta Aranda. Al corte del mes 7 quedaron en estado Cerrado, 1 en estado en Proceso y 1 Solucionado.
  Los casos obedecen a la revisión de alertas sobre caída de servicios de conectividad, pruebas de saturación canales, conexión a red WiFi, creación de segmento de red para ministra.

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

Categoría	Cantidad de solicitudes
FortiGate	2
Reservar IP	2
Configuración de Nueva red	1
Asesoría - Consulta	1
Aprovisionamiento de segmento de red	1

Tabla 82 Top 5 de categorías en el Servicio de conectividad LAN-WLAN

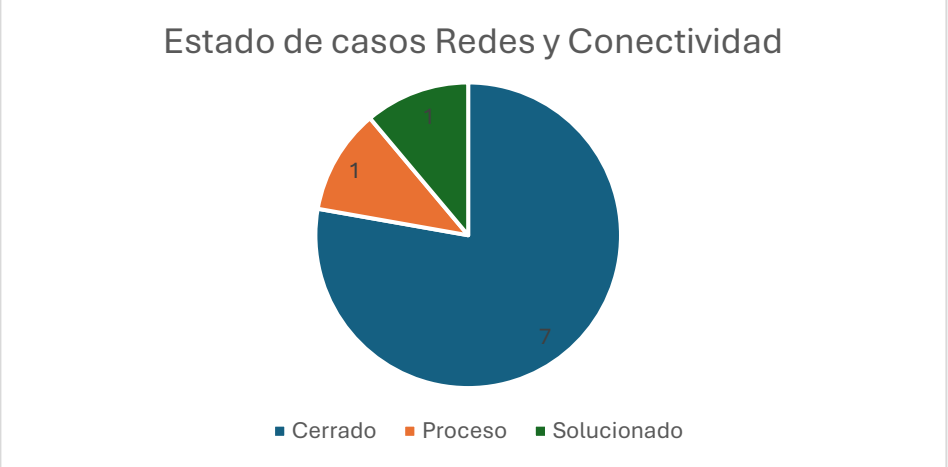


Ilustración 90 Estado de casos Redes y Conectividad

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 83 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
Territorial Bolívar	Cartagena	1
Territorial Boyacá	TUNJA	1
Territorial Caldas	MANIZALEZ	1
Territorial Cauca	POPAYAN	1

Dirección Territorial	Población y/o ciudad de ubicación	Cantidad switches 48 puertos
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 84 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
Territorial Caquetá	FLORENCIA	1
Territorial Casanare	YOPAL	2
Territorial Cauca	POPAYAN	2
Territorial Cesar	VALLEDUPAR	2
Territorial Chocó	QUIBDÓ	2

Dirección Territorial	Población y/o ciudad de ubicación	Cantidad Access Points
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 85 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 86 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 87 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 88 Sedes cerradas

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

Tabla 89 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 90 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 agosto 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

- 6/08/2026: Se presenta falla del IVR de la línea del ministerio, se genera el incidente mayor IM-297886, se hace revisión y se identifica que la causa raíz es falla troncal SIP y se solventa con apoyo del proveedor. La falla se da desde inicio de operación 6:30am hasta las 10:03am.
- 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-297957– RF – 303370 - RF-308168.



Asignación ext.
virtual_Teams_Caso_

- 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-308264, con el propósito de incorporar mejoras en rendimiento, funcionalidades y seguridad.



RE VENTANA DE
MANTENIMIENTO DE

- **Asignación de Licencias – Extensiones**

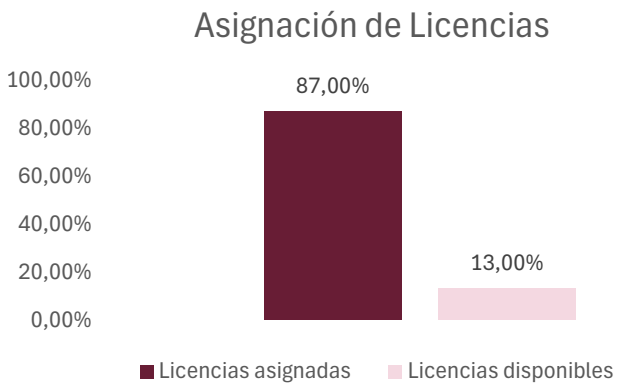


Ilustración 91 Asignación de licencias

Durante el mes en gestión, se han asignado un total de 520 extensiones a nivel nacional. Actualmente, permanecen disponibles 80 extensiones.

- **Estadísticas de Tráfico**

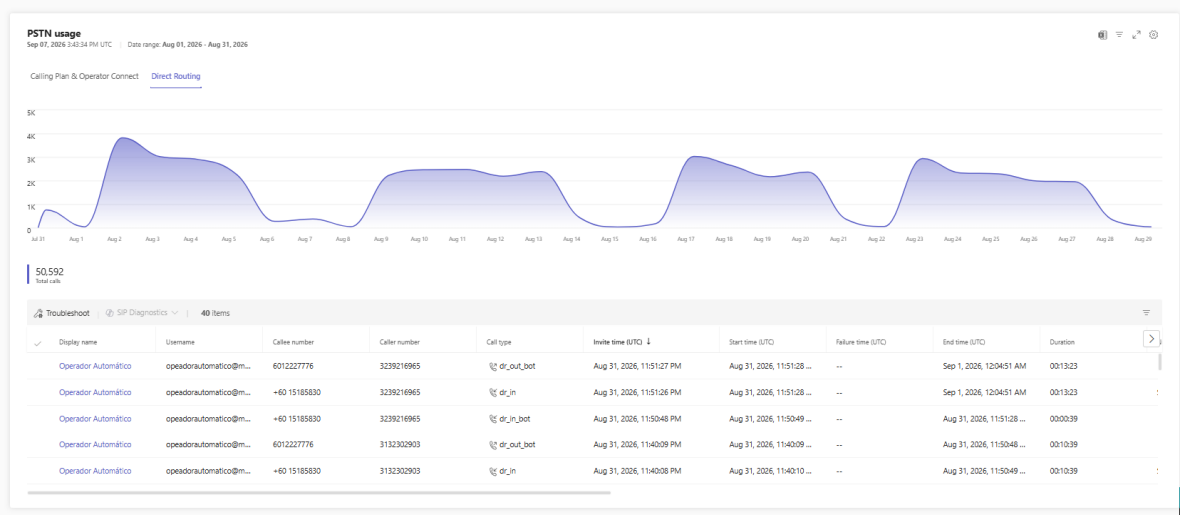


Ilustración 92 Comportamiento de tráfico

En la gráfica anterior se visualizan las tendencias de uso del servicio, en el periodo correspondiente al mes de agosto de 2026, donde se atendieron un total de 50,592 llamadas.

Servicio	Minutos Disponibles	Minutos Utilizados
Locales	Ilimitados	1421.29
Celular	1000	849.22
Nacional	Ilimitados	521.12
Internacional	700	4.18
Total		2795,81

Tabla 91 Minutos, consumos

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

Con respecto a las llamadas realizadas a destinos larga distancia nacional en el mes de agosto de 2026, se identifica que se realizaron llamadas con una duración total de 521.12 minutos.

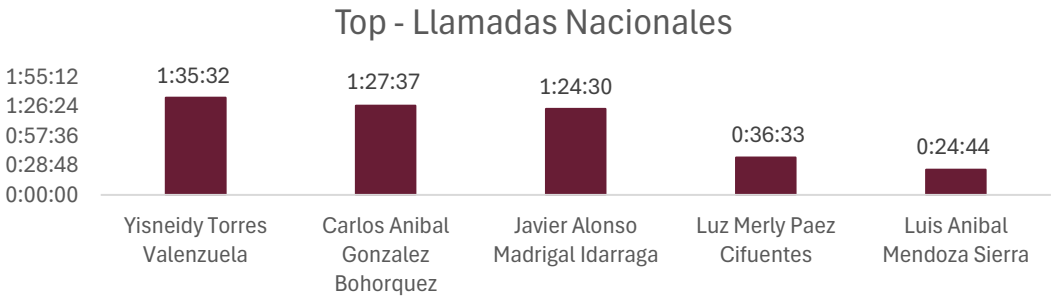


Ilustración 92 Top llamadas nacionales

N°	Usuario	Área	Tiempo llamadas
1	Yisneidy Torres Valenzuela	Grupo de inspección D.T Caquetá	1:35:32
2	Carlos Anibal Gonzalez Bohorquez	Inspector municipal D.T Antioquia	1:27:37

3	Javier Alonso Madrigal Idarraga	Grupo de Resolución de Conflictos y Conciliaciones D.T Antioquia	1:24:30
4	Luz Merly Paez Cifuentes	Comunicaciones D.T Bogotá	0:36:33
5	Luis Anibal Mendoza Sierra	Inspector municipal D.T Antioquia	0:24:44

Tabla 93 Top 5 consumo de llamadas

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

Con respecto a las llamadas internacionales en el mes de agosto 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.

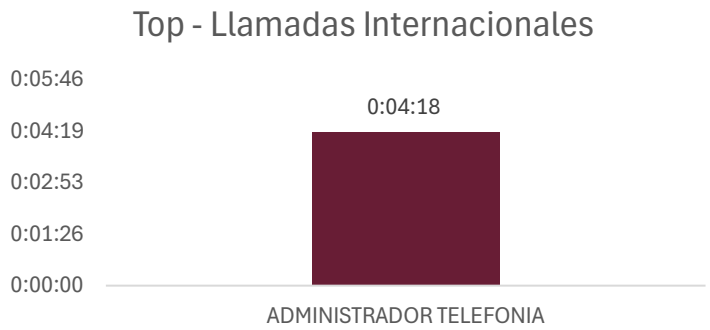


Ilustración 93 llamada internacional de prueba

Como se puede observar en el grafico anterior, se evidencia que, en el mes de agosto 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	0:04:18

Tabla 94 Top 5 llamadas LDI

- **Consumo de llamadas destinos celulares**

Con respecto a las llamadas realizadas a celular en el mes de agosto de 2026, se identifica que se realizaron llamadas con una duración total de 849.22 minutos (14,15 horas).

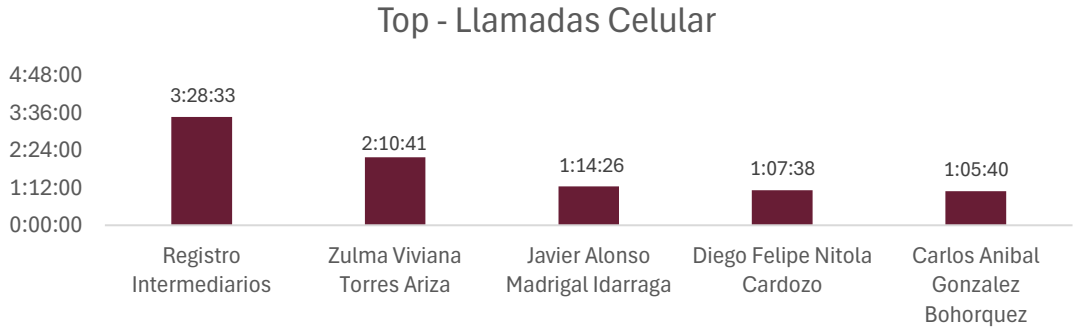


Ilustración 94 Top Celular

N°	Usuario	Área	Tiempo llamadas
1	Registro Intermediarios	Grupo de Registro Único de Intermediarios Bogotá	3:28:33
2	Zulma Viviana Torres Ariza	Comunicaciones D.T Bogotá	2:10:41
3	Javier Alonso Madrigal Idarraga	Grupo de Resolución de Conflictos y Conciliaciones D.T Antioquia	1:14:26
4	Diego Felipe Nitola Cardozo	Grupo de Atención al Ciudadano D.T Boyacá	1:07:38
5	Carlos Anibal Gonzalez Bohorquez	Inspector municipal D.T Antioquia	1:05:40

Tabla 95 Top 5 llamadas Celular

- **Consumo de llamadas locales**

Con respecto a las llamadas realizadas a destinos locales en el mes de agosto de 2026, se identifica que se realizaron llamadas con una duración total de 1421.29 minutos (23,68 horas).

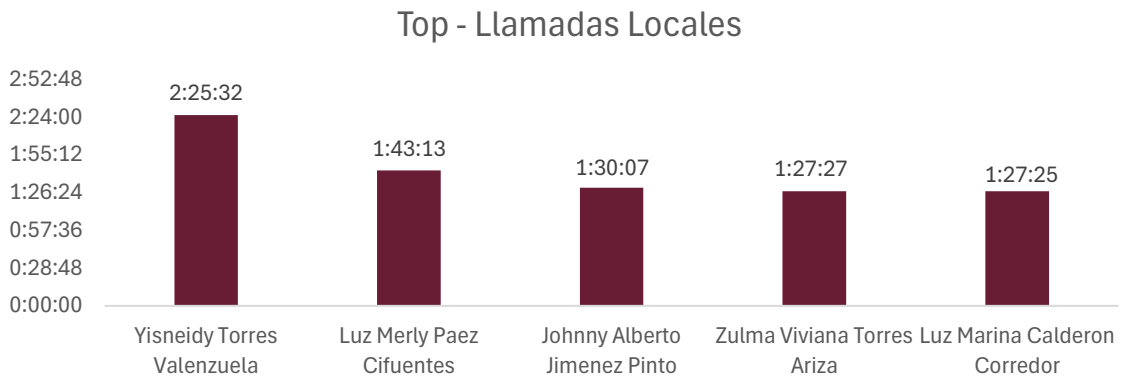


Ilustración 95 Top Local

N°	Usuario	Área	Tiempo llamadas
1	Yisneidy Torres Valenzuela	Grupo de inspección D.T Caquetá	2:25:32
2	Luz Merly Paez Cifuentes	Comunicaciones D.T Bogotá	1:43:13
3	Johnny Alberto Jimenez Pinto	Grupo de Defensa Judicial D.T Bogotá	1:30:07
4	Zulma Viviana Torres Ariza	Comunicaciones D.T Bogotá	1:27:27
5	Luz Marina Calderon Corredor	Grupo Interno de Trabajo de Nomina e Incapacidades Bogotá	1:27:25

Tabla 96 Top 5 llamadas locales

- **Capacitaciones y divulgaciones**

En el mes de agosto 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. Adicionalmente, se continúa con el proceso de actualización y modernización de la plataforma de telefonía en conjunto con Microsoft, orientado a mantener la plataforma actualizada y optimizar su operación.

- **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

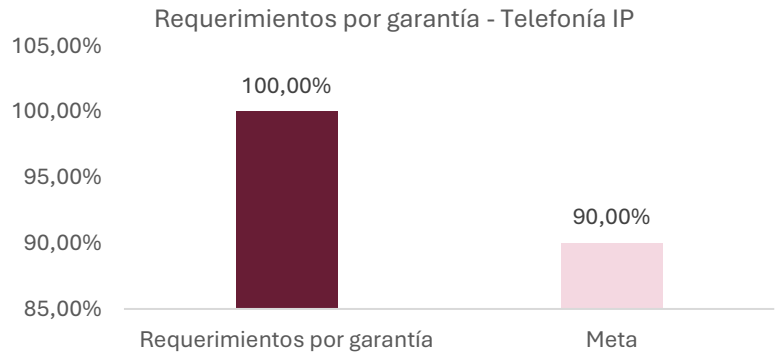


Ilustración 96 Requerimientos por garantía

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

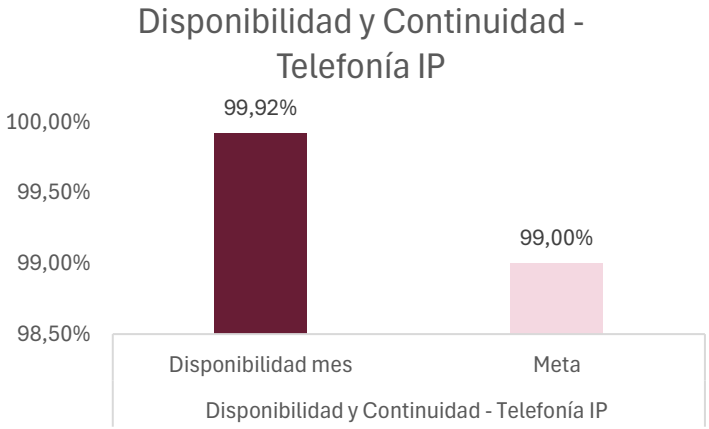


Ilustración 97 Disponibilidad y Continuidad TOIP

En el periodo correspondiente al mes de agosto, 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	99,92%	99,00%
TIP-3	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 97 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 98 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 99 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
IM-303411	Incidents	Suspendido	Se ha detectado un evento en el sistema de monitoreo Zabbix. A continuación, se detallan los datos del evento: Nombre del Host: UPS_Pereira IP del Host: 172.16.25.9 Tipo de Equipo: UPS Evento: UPS en estado Baterias Severidad: Disaster Fecha y Hora del Evento: 2026.08.10 07:39:05 Valor Actual del Ítem: Baterias (5) CI: {RelatedCI=UPS_Pereira} Por favor, toma las medidas necesarias para solucionar este problema lo antes posible.	Se realizará nueva validación en horario hábil
IM-308950	Incidents	Cerrado	Se ha detectado un evento en el sistema de monitoreo Zabbix. A continuación, se detallan los datos del evento: Nombre del Host: UPS_Tunja IP del Host: 172.16.7.10 Tipo de Equipo: UPS Evento: UPS en estado Baterias Severidad: Disaster Fecha y Hora del Evento: 2026.08.13 11:37:45 Valor Actual del Ítem: Baterias (5) CI: {RelatedCI=UPS_Tunja} Por favor, toma las medidas necesarias para solucionar este problema lo antes posible.	Se procede a cerrar el caso ya que el alertamiento presente en la herramienta zabbix esta en estado solventado, Proveedor ETB indica que el servicio fue afectado por una falla de alto impacto y nos indica que el personal especializado indicando que el servicio esta restablecido.
IM-309042	Incidents	Cerrado	Se ha detectado un evento en el sistema de monitoreo Zabbix. A continuación, se detallan los datos del evento: Nombre del Host: UPS_Tunja IP del Host: 172.16.7.10 Tipo de Equipo: UPS Evento: UPS en estado Baterias Severidad: Disaster Fecha y Hora del Evento: 2026.08.13 14:52:46 Valor Actual del Ítem: Baterias (5) CI: {RelatedCI=UPS_Tunja} Por favor, toma las medidas necesarias para solucionar este problema lo antes posible.	Se realiza validación con soporte en sitio y la alerta fue debido a una falla de energía eléctrica prolongada en la zona.

Tabla 100 Casos gestionados – Energía Eléctrica Regulada UPS

- **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. Para agosto 2026, la tarjeta se encuentra en proceso de importación.

- **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 101 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 102 Inventario de impresoras para el servicio

A continuación, se relacionan las actividades realizadas por el administrador del servicio de impresión, e información relevante para este servicio:

- Para el mes de agosto, el responsable del servicio gestionó un total de 438 solicitudes escaladas a través de Aranda. Al corte del mes, 427 casos quedaron en estado Cerrado/Solucionado, 11 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 31% de la capacidad total del almacenamiento (capacidad total 100gb).
- Se 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-293820; 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 19/08/2026 se realiza instalación de impresora con serial 3353PA50669 en la sede de Montelíbano como contingencia; proveedor realizo visita técnica el día 28/08/2026 en la cual se cambia disco duro de la impresora con serial 3353P955743 quedando totalmente funcional.
- El 29/08/2026 se realiza ventana de parchado de seguridad de aplicativo PaperCut MF, instalando la versión (26.0.4-PO-4560) de manera exitosa en el cambio RFC-327252, se realizan pruebas de impresión, copia y escaneo con apoyo del personal de soporte en sitio sin novedades. No se presenta afectación del servicio y la ventana resulta exitosa.

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
ricoh-bmanga-ofc305	Bucaramanga	amateus	Andrea Johana Mateus Parra	3.711
ricohpiso10b	Bogotá sede central	ocardenas	Omaira Alexandra Cardenas Saavedra	3.282
ricoh-ibague-radicacion	Ibague	jgonzalezcu	Jose Eugenio Gonzalez Cuella	2.842
ricoh-soacha-piso1	Soacha	mrodriguezo	Maria Yudy Rodriguez Ocampo	2.826
ricoh-bmanga-ofc303	Bucaramanga	evelasco	Edinson Ovidio Velasco Aguilar	2.619
ricoh-bmanga-ofc205	Bucaramanga	lberbeo	Laura Daniela Berbeo Ardila	2.437
ricoh-bmanga-ofc101	Bucaramanga	kpimiento	Karym Yuliana Pimiento Osorio	2.360
ricoh-apartado-2piso-c	Aguachica	mibarguen	Maria Dolores Ibarguen Torres	2.326
ricohpiso19b	Bogotá sede central	pnustes	Patricia Celestial Nustes Barrera	2.100
ricoh-apartado-2pisoa	Aguachica	tllanes	Tatiana Llanes Ibarguen	2.026

Tabla 103 Consumo de impresiones y copias por usuario - Impresoras B/N

topusuarioagosto.xlsx

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

Nombre de la impresora	Ubicación	Blanco y negro
ricohpiso5a	Bogotá sede central	15.189
ricohcl32-rcc	Bogota calle32	13.956
ricohpiso10b	Bogotá sede central	11.681
ricohpiso12a	Bogotá sede central	11.281

Nombre de la impresora	Ubicación	Blanco y negro
ricoh-bmanga-ofc303	Bucaramanga	10.927
ricoh-bmanga-ofc205	Bucaramanga	10.722
ricoh-baq-dir	Barranquilla	10.608
ricohpiso21a	Bogotá sede central	10.217
ricohpiso9a	Bogotá sede central	9.560
ricoh-caqueta-piso1-ppal	Caqueta	8.794

Tabla 104 Top 10 de impresoras con mayor uso

Top_Imp_Ago.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	2.831
ricohpiso25c	Bogotá Sede Central	mruizb	Maria Jose Ruiz Bechara	41
ricohpiso25c	Bogotá Sede Central	jrey	Julian Andres Rey Reina	36
ricohpiso25c	Bogotá Sede Central	cmorar	Claudia Nelly Mora Rios	3

Tabla 105 Top usuarios impresión a color

Top_Piso_25C_Ago.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	2.911	148.122	110.574	40.459	151.033	40.419	5,5
D.T. Santander	-	38.332	27.690	10.642	38.332	10.565	6,9
D.T. Antioquia	-	26.525	19.886	6.639	26.525	7.867	5,3
D.T. Atlantico	-	25.955	17.370	8.585	25.955	7.355	7,5
D.T. Bogotá	-	22.797	14.066	8.731	22.797	7.535	5,6
D.T. Cundinamarca	-	18.392	12.840	5.552	18.392	4.429	8,6
D.T. Norte de Santander	-	17.487	12.086	5.401	17.487	4.819	8,1
OE	-	15.405	9.902	5.503	15.405	4.682	6,5
D.T. Tolima	-	14.402	10.402	4.000	14.402	3.237	7,9
D.T. Cesar	-	11.379	8.356	3.023	11.379	3.391	6,1

Tabla 106 Top oficinas

Top_Ofi_Ago.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	2.104
RICOH-CAQUETA-PISO1-PPAL	D.T. Caqueta	COPY	1.653
RICOH-MEDELLIN-PISO1	D.T. Antioquia	COPY	1.139
RICOH-NEIVA-IVC	D.T. Huila	COPY	1.011
RICOH-BMANGA-OFC205	D.T. Santander	COPY	961
RICOH-BAQ-DIR	D.T. Atlantico	COPY	939
RICOH-BMANGA-OFC305	D.T. Santander	COPY	920
RICOH-NEIVA-ATC	D.T. Huila	COPY	897
RICOHGAU-A	D.T. Bogotá	COPY	871
RICOHPISO9A	Nivel Central	COPY	791

Tabla 107 Top 10 impresoras más usadas del servicio de fotocopiado

Top_Cop_Ago.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
cnuneza	Cindy Tatiana Nunez Aguillon	ADJUST	2.280	8
evelasco	Edinson Ovidio Velasco Aguilar	ADJUST	2.984	8
ndiaz	Nelson Augusto Diaz Diaz	ADJUST	2.760	8
ipantojar	Imelda Pantoja Rosero	ADJUST	2.325	7
pzuluaga	Paula Andrea Zuluaga Ramirez	ADJUST	2.573	7
aenriquez	Amanda Patricia Enriquez Guerrero	ADJUST	2.100	6
dromeroq	Diana Lisset Romero Quiroga	ADJUST	1.997	6
amendoza	Alcides Mendoza Bermudez	ADJUST	1.952	5
aparada	Andres Isachar Parada Figueroa	ADJUST	1.380	5
aquevedo	Ana Yaneth Quevedo Quintero	ADJUST	1.500	5

Tabla 108 Ampliación de cuota de impresión

- 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:

	Jun-26		Jul-26		Ago-26	
	Resmas Carta	Resmas Oficio	Resmas Carta	Resmas Oficio	Resmas Carta	Resmas Oficio
Total, Resmas	240	199	178	57	269	71
Total, Cajas por Tamaño	24,00	19,90	17,80	5,70	26,90	7,10
Total, Cajas Enviadas	**43,90**		**22,50**		**34,00**	

Tabla 109 Despacho de papel a sedes del Ministerio del Trabajo

Durante el período, se despacharon a sedes del ministerio un total de 11 toners para impresora B/N IM430, 3 unidades de imagen y 1 unidad fusora.

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 110Cargo 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 111 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 agosto de 2026:

MES	DETALLE	CANTIDAD
Agosto	Multifuncional blanco y negro rango medio - Clic de impresión tóner y papel carta	**526.180**
	TOTAL	**526.180**

Tabla 112 Clics de impresión de agosto 2026 – Multifuncional B/N

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

Mes 2026	Junio	Julio	Agosto
Cantidad de clics consumidos	544.116	554.528	526.180

Tabla 113 Tendencia de consumo de clics B/N

El consumo mensual establecido para el servicio es de **620.000** clics de impresión en B/N a nivel nacional; para el período del informe se presentó un consumo de **491.432** clics de impresión (esto incluye **4.133** de la impresora de contratos piso 8) y **34.748** de fotocopias para un total de **526.180** para este servicio.

4.6.6. Impresora Color rango medio – Clic de impresión

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

MES	DETALLE	CANTIDAD
Agosto	Impresora color rango medio - Cargo fijo mensual - Clic de impresión tóner y papel carta	**3.342**
	Total	**3.342**

Tabla 114 Clics de Impresión – Impresora Color

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

Mes	Junio	Julio	Agosto
Cantidad de clics consumidos	226	2.688	3.342

Tabla 115Tendencia 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 **2.911** clics de impresión y **431** de fotocopias para un total de **3.342** clics para este servicio, por lo cual se superó dicho consumo.

Teniendo en cuenta que durante el periodo se presentó un consumo superior al volumen mensual contratado, con un excedente de 1.842 clics a color, y que la factura no contempla un rubro específico para la facturación de clics adicionales, se aplicará la equivalencia establecida de 1 clic a color por cada 4 clics en blanco y negro. En consecuencia, los 1.842 clics a color equivalen a 7.368 clics en blanco y negro, los cuales serán incorporados a la línea de consumo mensual de clics de blanco y negro.

- **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 116 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 agosto 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.

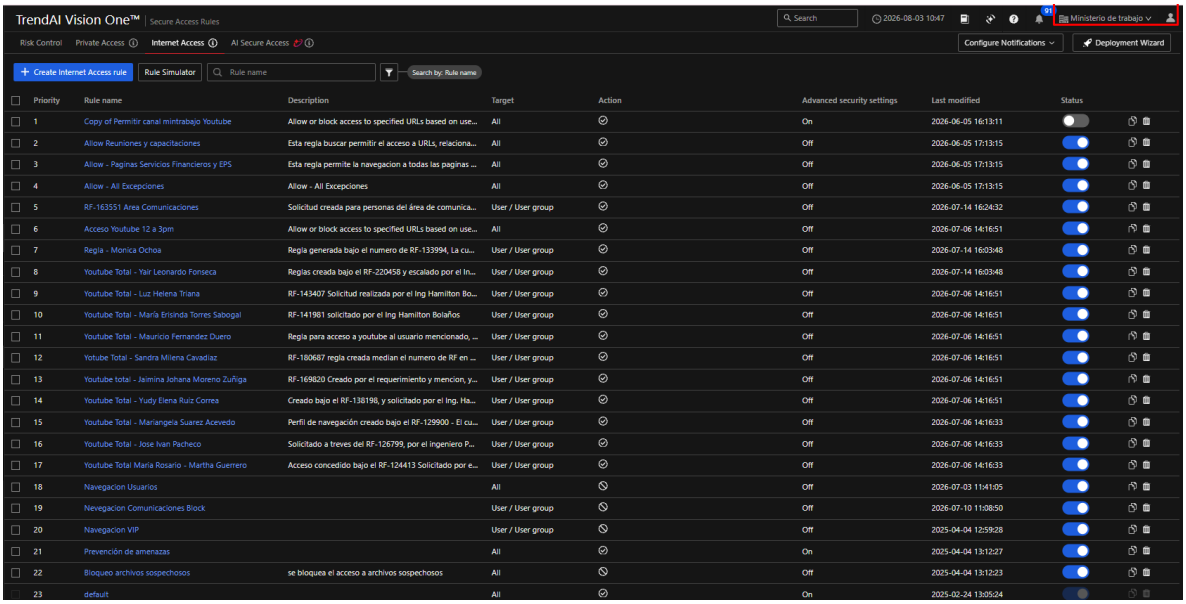


Ilustración 98 Equipos consola antivirus

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 (2129) de Mintrabajo, se cuenta con 2255 licencias, se tienen disponibles 96.

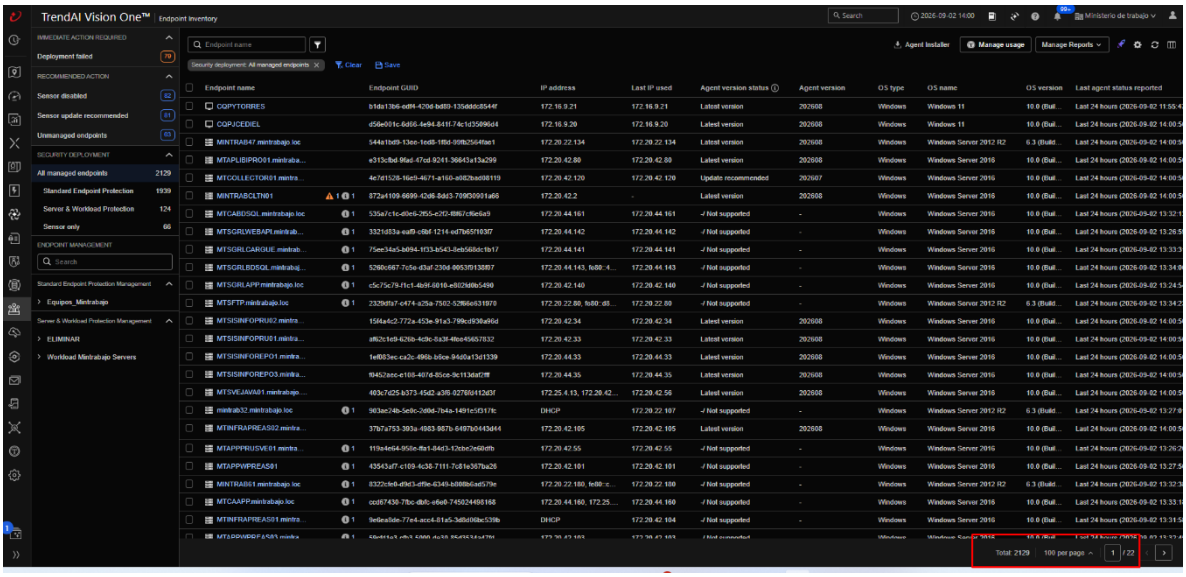


Ilustración 99 Gestión consola antivirus – equipos usuario final

4.7.3 Top 10 Virus Detectados

Durante el mes analizado, los eventos detectados por la plataforma Trend Micro se detectaron un total de 36 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:

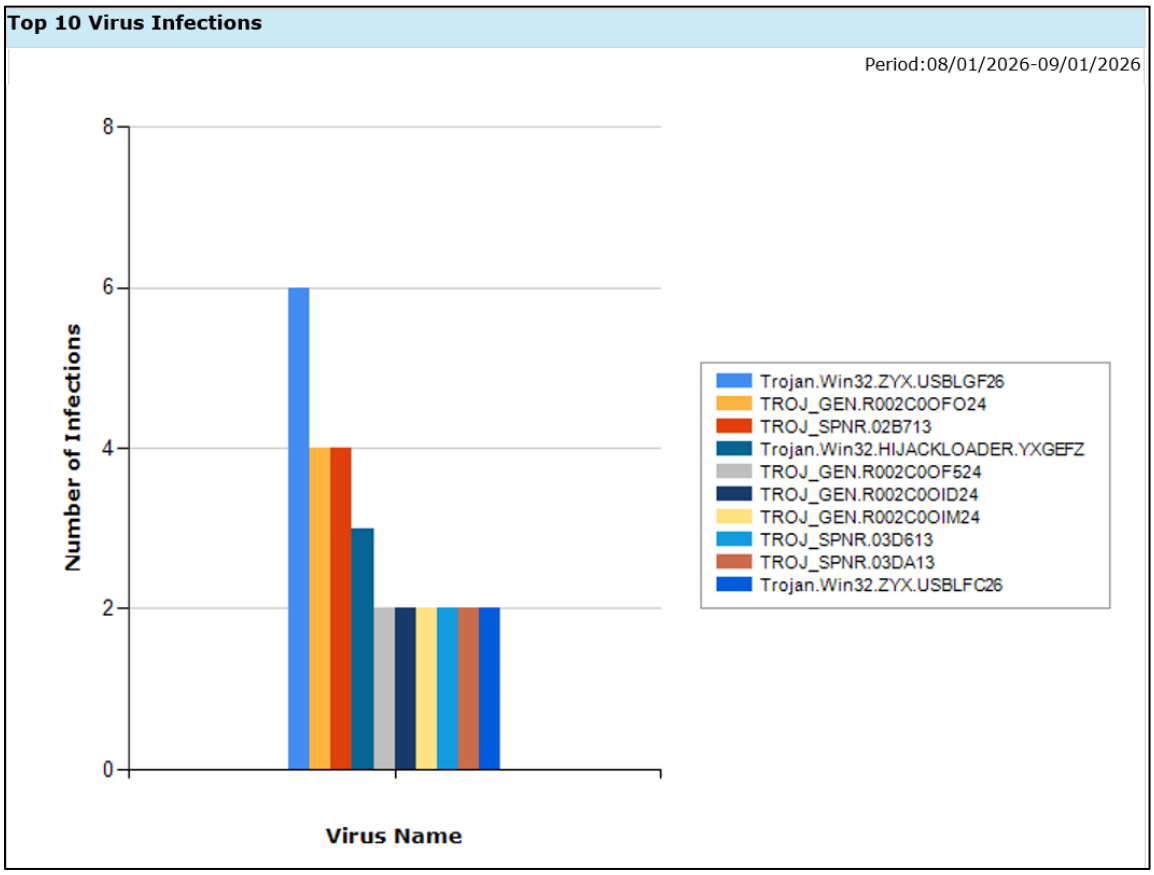


Ilustración 100 Top 10 virus detectado

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 101 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.

Trojan.Win32.ZYX.USBLGF26: 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.

TROJ_GEN.R002C0OFO24: Esta correspondiente a una clasificación genérica asociada a la categoría de troyanos (TROJ). Este tipo de detección se genera cuando el motor de seguridad identifica características o patrones compatibles con comportamiento malicioso, sin que necesariamente corresponda a una familia específica de malware. Para determinar el nivel de riesgo del evento, se recomienda validar el archivo involucrado, su ubicación, hash, proceso de origen y la acción ejecutada por la solución de seguridad, así como verificar si se presentaron eventos relacionados en el mismo equipo.

TROJ_SPNR.02B713: Corresponde a una detección de Trend Micro asociada a la categoría de troyanos (TROJ). La identificación SPNR hace referencia a una detección genérica empleada por el motor de seguridad para identificar archivos que presentan características, patrones o comportamientos compatibles con una amenaza de tipo troyano.

Trojan.Win32. HIJACKLOADER.YXGEFZ; Corresponde a una detección de Trend Micro asociada a un troyano de tipo HijackLoader, una familia de malware utilizada como cargador para facilitar la ejecución o distribución de otras amenazas en sistemas Windows. Este tipo de malware puede emplear técnicas de manipulación o secuestro de procesos legítimos para evadir mecanismos de seguridad y ejecutar código malicioso.

TROJ_GEN.R002C0OF524, TROJ_GEN.R002C0OID24 y TROJ_GEN.R002C0OIM24: Corresponde a detecciones asociadas a la categoría de troyanos (TROJ). La denominación GEN indica que se trata de una detección genérica, mediante la cual el motor de seguridad identifica características, patrones o comportamientos compatibles con código malicioso, sin necesariamente asociarlo a una familia específica de malware.

TROJ_SPNR.03D613, TROJ_SPNR.03DA13: Corresponde detecciones asociadas a la categoría de troyanos (TROJ). La identificación SPNR corresponde a una clasificación utilizada por el motor de detección para identificar archivos que presentan características o patrones compatibles con comportamiento potencialmente malicioso.

Trojan.Win32.ZYX.USBLFC26: Corresponde a detecciones asociadas a la categoría de troyanos para sistemas Windows. La identificación ZYX.USBLFC26 corresponde a una clasificación utilizada por el motor de detección para identificar archivos que presentan características compatibles con código o comportamiento potencialmente malicioso. Este tipo de amenaza puede estar asociado a archivos distribuidos mediante dispositivos de almacenamiento extraíbles, dependiendo del origen y contexto de la detección.

TOP 5 EQUIPOS

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

Host	Cant	Virus/Malware
BOPMFTRIANA	26	TROJ_FAKEAV.SMVP, Trojan.Win32.ZYX.USBLGF26, TROJ_GEN.R002C0OFO24
ANPJCHERNANDEZM	3	TSC_GENCLEAN, Backdoor.JS.XWORM.YXGHKZ
ARDMGIRALDO	3	Trojan.Win32.HIJACKLOADER.YXGEFZ
CTDJORTEGAJ	2	Trojan.Win32.ZYX.USBLFC26
BOPPW0A3B02	1	Backdoor.Win64.DACIC.TL0101H526ZZ

Tabla 117 Top 5 Equipos

BOPMFTRIANA

En el equipo se registran 26 detecciones, principalmente asociadas a la amenaza reconocida como Trojan.Win32.ZYX.USBLGF26 estas presentan características compatibles con un troyano, las detecciones no identifican un malware concreto, sino un archivo cuyo comportamiento o estructura coincide con patrones maliciosos. Los eventos y archivos son controlados por la herramienta y se lleva la eliminación de estos.

Generated	Received	Product Entity/E...	Product	Product/Endpoin...	Product/Endpoin...	Managing Serve...	Domain	Action	Rule ID	Virus/Malware	Endpoint Infecti...
08/07/2026 18:15:...	08/07/2026 18:17:...	BOPMFTRIANA	Apex One	172.16.64.19	80-E8-2C-BC-49-AA	Windows	Workgroup	File deleted	TROJ_FAKEAV.SMVP	TROJ_FAKEAV.SMVP	Local or network d...
08/07/2026 18:08:...	08/07/2026 18:09:...	BOPMFTRIANA	Apex One	172.16.64.19	80-E8-2C-BC-49-AA	Windows	Workgroup	File deleted	TROJ_FAKEAV.SMVP	TROJ_FAKEAV.SMVP	Local or network d...
08/06/2026 19:07:...	08/06/2026 19:07:...	BOPMFTRIANA	Apex One	172.16.64.19	80-E8-2C-BC-49-AA	Windows	Workgroup	File deleted	Trojan.Win32.ZYX....	Trojan.Win32.ZYX....	Local or network d...
08/06/2026 19:07:...	08/06/2026 19:07:...	BOPMFTRIANA	Apex One	172.16.64.19	80-E8-2C-BC-49-AA	Windows	Workgroup	File deleted	Trojan.Win32.ZYX....	Trojan.Win32.ZYX....	Local or network d...
08/06/2026 19:07:...	08/06/2026 19:07:...	BOPMFTRIANA	Apex One	172.16.64.19	80-E8-2C-BC-49-AA	Windows	Workgroup	File deleted	Trojan.Win32.ZYX....	Trojan.Win32.ZYX....	Local or network d...
08/06/2026 19:06:...	08/06/2026 19:07:...	BOPMFTRIANA	Apex One	172.16.64.19	80-E8-2C-BC-49-AA	Windows	Workgroup	File deleted	TROJ_GEN.R002C0...	TROJ_GEN.R002C0...	Local or network d...
08/06/2026 19:06:...	08/06/2026 19:07:...	BOPMFTRIANA	Apex One	172.16.64.19	80-E8-2C-BC-49-AA	Windows	Workgroup	File deleted	TROJ_GEN.R002C0...	TROJ_GEN.R002C0...	Local or network d...
08/06/2026 19:06:...	08/06/2026 19:07:...	BOPMFTRIANA	Apex One	172.16.64.19	80-E8-2C-BC-49-AA	Windows	Workgroup	File deleted	TROJ_SPNR.02B713	TROJ_SPNR.02B713	Local or network d...
08/06/2026 19:06:...	08/06/2026 19:07:...	BOPMFTRIANA	Apex One	172.16.64.19	80-E8-2C-BC-49-AA	Windows	Workgroup	File deleted	TROJ_GEN.R002C0...	TROJ_GEN.R002C0...	Local or network d...
08/06/2026 19:06:...	08/06/2026 19:07:...	BOPMFTRIANA	Apex One	172.16.64.19	80-E8-2C-BC-49-AA	Windows	Workgroup	File deleted	TROJ_GEN.R002C0...	TROJ_GEN.R002C0...	Local or network d...
08/06/2026 19:06:...	08/06/2026 19:07:...	BOPMFTRIANA	Apex One	172.16.64.19	80-E8-2C-BC-49-AA	Windows	Workgroup	File deleted	TROJ_GEN.R002C0...	TROJ_GEN.R002C0...	Local or network d...
08/06/2026 19:06:...	08/06/2026 19:07:...	BOPMFTRIANA	Apex One	172.16.64.19	80-E8-2C-BC-49-AA	Windows	Workgroup	File deleted	TROJ_SPNR.02B713	TROJ_SPNR.02B713	Local or network d...
08/06/2026 19:06:...	08/06/2026 19:07:...	BOPMFTRIANA	Apex One	172.16.64.19	80-E8-2C-BC-49-AA	Windows	Workgroup	File deleted	TROJ_SPNR.03D613	TROJ_SPNR.03D613	Local or network d...
08/06/2026 19:06:...	08/06/2026 19:07:...	BOPMFTRIANA	Apex One	172.16.64.19	80-E8-2C-BC-49-AA	Windows	Workgroup	File deleted	TROJ_SPNR.03DA13	TROJ_SPNR.03DA13	Local or network d...
08/06/2026 18:34:...	08/06/2026 18:35:...	BOPMFTRIANA	Apex One	172.16.64.19	80-E8-2C-BC-49-AA	Windows	Workgroup	File deleted	Trojan.Win32.ZYX....	Trojan.Win32.ZYX....	Local or network d...
08/06/2026 18:34:...	08/06/2026 18:35:...	BOPMFTRIANA	Apex One	172.16.64.19	80-E8-2C-BC-49-AA	Windows	Workgroup	File deleted	Trojan.Win32.ZYX....	Trojan.Win32.ZYX....	Local or network d...
08/06/2026 18:34:...	08/06/2026 18:35:...	BOPMFTRIANA	Apex One	172.16.64.19	80-E8-2C-BC-49-AA	Windows	Workgroup	File deleted	Trojan.Win32.ZYX....	Trojan.Win32.ZYX....	Local or network d...
08/06/2026 18:34:...	08/06/2026 18:35:...	BOPMFTRIANA	Apex One	172.16.64.19	80-E8-2C-BC-49-AA	Windows	Workgroup	File deleted	TROJ_GEN.R002C0...	TROJ_GEN.R002C0...	Local or network d...
08/06/2026 18:34:...	08/06/2026 18:35:...	BOPMFTRIANA	Apex One	172.16.64.19	80-E8-2C-BC-49-AA	Windows	Workgroup	File deleted	TROJ_GEN.R002C0...	TROJ_GEN.R002C0...	Local or network d...

Ilustración 102 BOPMFTRIANA

ANPJCHERNANDEZM

En el equipo se registraron tres detecciones asociadas a la amenaza Backdoor.JS.XWORM.YXGHKZ, identificada por Trend Micro como un backdoor (puerta trasera) desarrollado en JavaScript. Este tipo de amenaza puede proporcionar a un atacante capacidades de ejecución remota o control sobre un sistema comprometido, así como permitir la ejecución de acciones maliciosas adicionales, dependiendo de las funcionalidades de la muestra. Los eventos fueron gestionados y controlados mediante las acciones de remediación de la solución de seguridad: un archivo fue limpiado, un segundo

archivo fue eliminado y, en el tercer caso, fue necesario reiniciar el host para completar su eliminación. Estas acciones permitieron contener las detecciones identificadas en el equipo

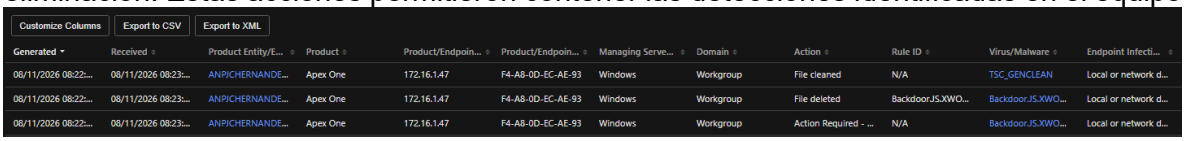


Ilustración 103 ANPJCHERNANDEZM

ARDMGIRALDO

En el equipo se reportan 3 detecciones de una amenaza denominada Trojan.Win32.HIJACKLOADER.YXGEFZ, asociadas a un troyano de tipo HijackLoader, una familia de malware utilizada como cargador para facilitar la ejecución o distribución de otras amenazas en sistemas Windows. Este tipo de malware puede emplear técnicas de manipulación o secuestro de procesos legítimos para evadir mecanismos de seguridad y ejecutar código malicioso.

Los eventos fueron gestionados y controlados mediante las acciones de remediación de la solución de seguridad: un archivo fue limpiado, un segundo archivo fue eliminado y, en el tercer caso, fue necesario reiniciar el host para completar su eliminación. Estas acciones permitieron contener las detecciones identificadas en el equipo.

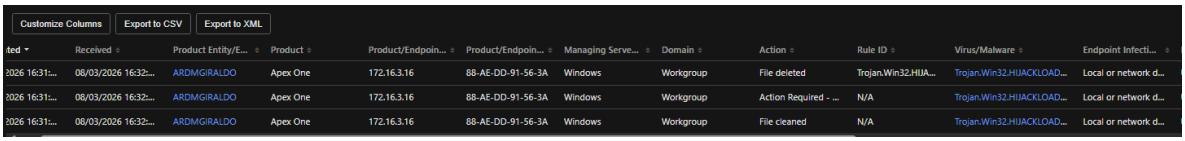


Ilustración 104 ARDMGIRALDO

CTDJORTEGAJ

En el equipo se reportan 2 detecciones de la amenaza de una amenaza denominada Trojan.Win32.ZYX.USBLFC26, asociadas a la categoría de troyanos para sistemas Windows. La identificación ZYX.USBLFC26 corresponde a una clasificación utilizada por el motor de detección para identificar archivos que presentan características compatibles con código o comportamiento potencialmente malicioso. Los eventos fueron gestionados y controlados mediante las acciones de remediación de la solución de seguridad: un archivo fue limpiado, para el segundo archivo fue necesario reiniciar el host para completar su eliminación. Estas acciones permitieron contener las detecciones identificadas en el equipo

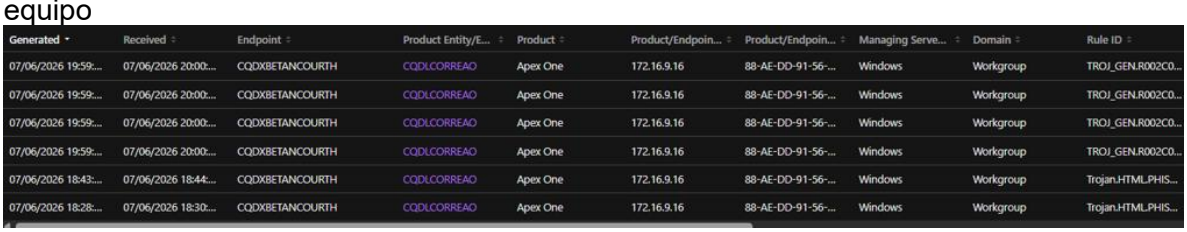


Ilustración 105 CTDJORTEGAJ

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 agosto 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 segundo 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 agosto del 2026 se tienen registrados 345 activos TI, de los cuales, se registró un alcance sobre 316 (92%) activos

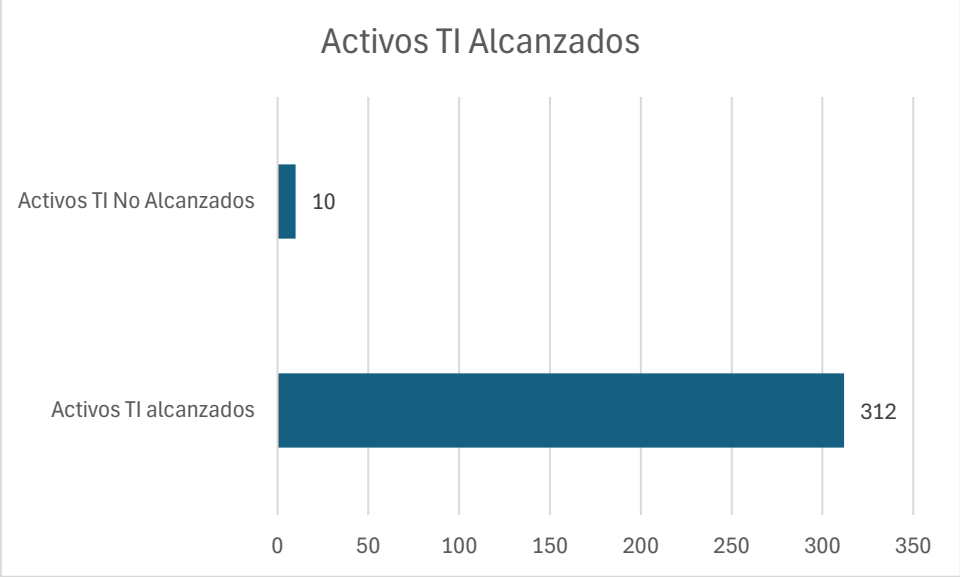
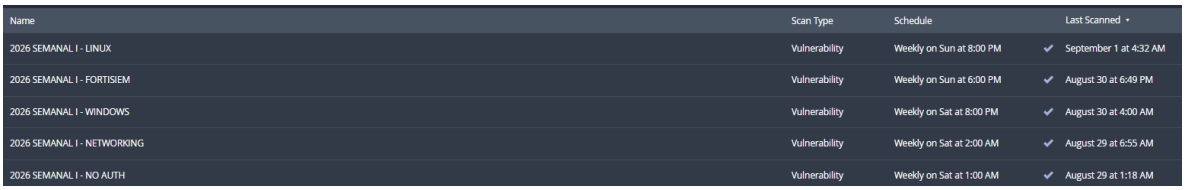


Ilustración 106 *Gestión consola Nessus*

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.



Name	Scan Type	Schedule	Last Scanned
2026 SEMANAL I - LINUX	Vulnerability	Weekly on Sun at 8:00 PM	September 1 at 4:32 AM
2026 SEMANAL I - FORTISIEM	Vulnerability	Weekly on Sun at 6:00 PM	August 30 at 6:49 PM
2026 SEMANAL I - WINDOWS	Vulnerability	Weekly on Sat at 8:00 PM	August 30 at 4:00 AM
2026 SEMANAL I - NETWORKING	Vulnerability	Weekly on Sat at 2:00 AM	August 29 at 6:55 AM
2026 SEMANAL I - NO AUTH	Vulnerability	Weekly on Sat at 1:00 AM	August 29 at 1:18 AM

Ilustración 107 *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 Identificación y Clasificación de vulnerabilidades

De los procesos de escaneo realizados durante el periodo de agosto del 2026 se muestran a continuación datos estadísticos de los resultados obtenidos en la plataforma Tenable Nessus Professional.

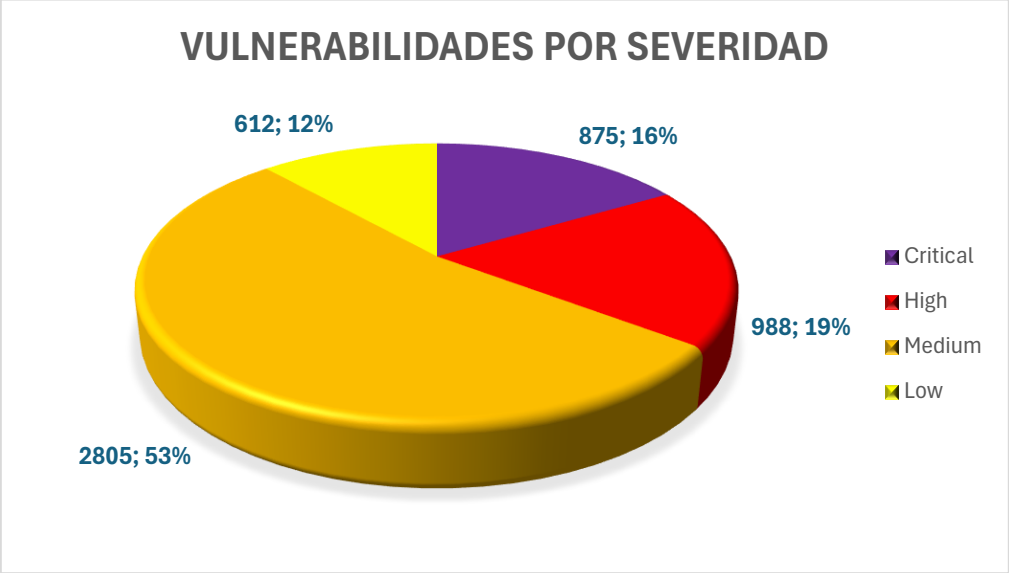


Ilustración 108 TOP 10 - Vulnerabilidades por severidad

Al cierre de agosto del 2026, se identificaron un total de 5.280 vulnerabilidades, de las cuales 875 clasificaron a la severidad crítica, 988 a la severidad alta, 2.805 a la severidad media y 612 a la severidad baja.

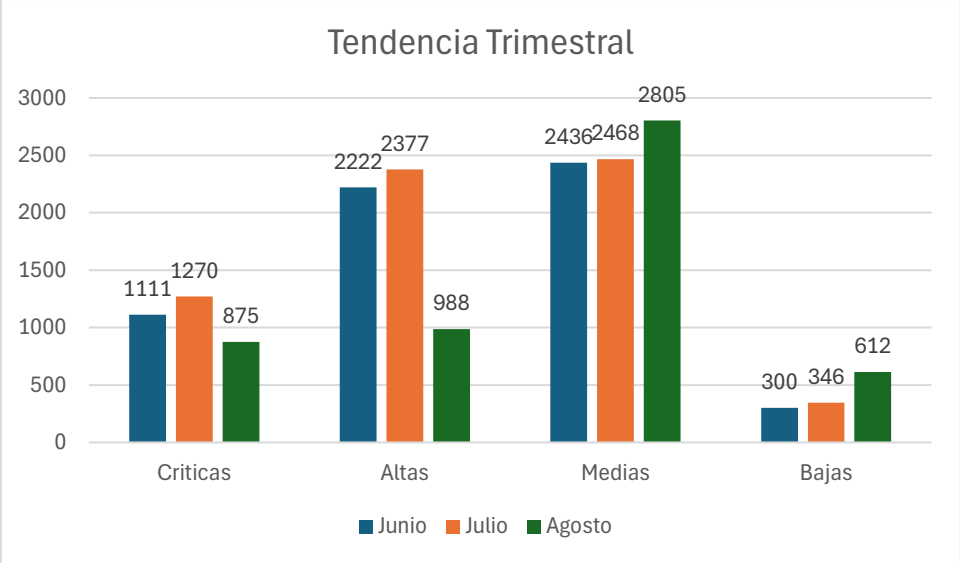


Ilustración 109 Tendencia de vulnerabilidades trimestral

Al cierre de agosto del 2026, se evidenció una **tendencia trimestral incremental** en las severidades crítica, alta y media, mientras que la **severidad baja decrementó**. Actividad justificada por la disminución de actividades de explotación de vulnerabilidades altas y la aplicación de actualizaciones de seguridad para Software Microsoft y configuraciones de Regedit

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 agosto del 2026, se remediaron un total de **51 vulnerabilidades**, de las cuales, 9 fueron de severidad crítica, 15 de severidad alta, 15 de severidad media y 12 de severidad baja. Por otro lado, con relación a **indicadores semestrales**, se gestionaron un total de **86 vulnerabilidades**, de las cuales, 12 fueron de severidad crítica, 8 de severidad alta, 22 de severidad media y 14 de severidad baja.

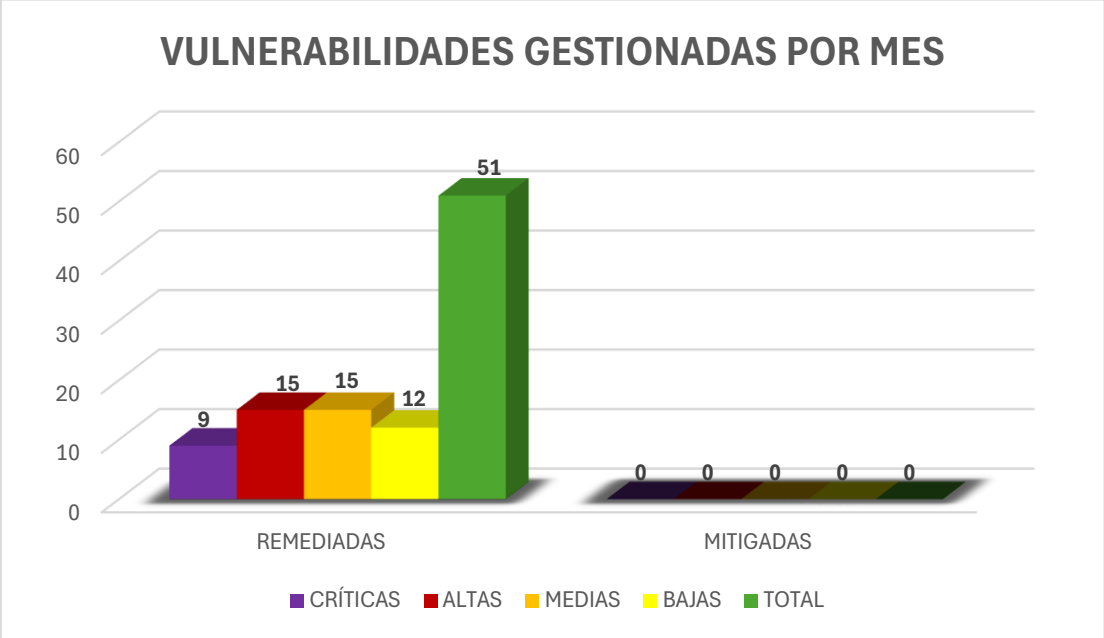


Ilustración 110 Vulnerabilidades gestionadas vs en remediación

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 111 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 agosto 2027, se adjunta informe socializado.



Ilustración 112 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	99,39%	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 118 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 179 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:

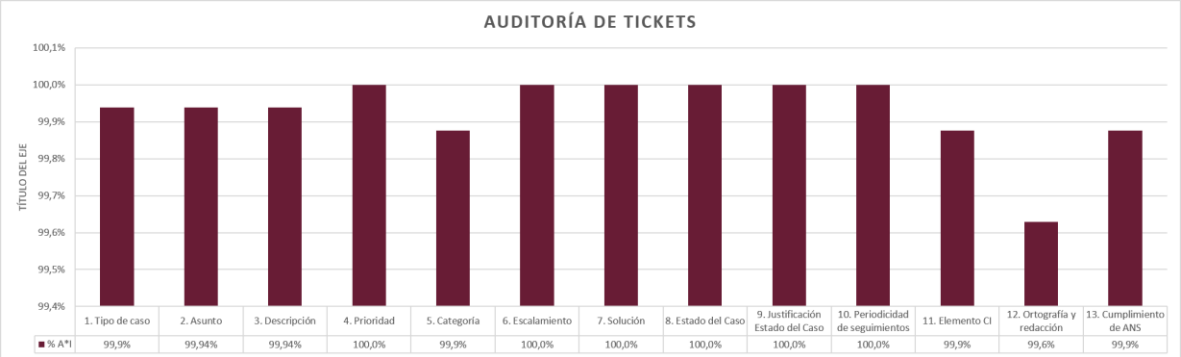


Ilustración 113 Resultado General

Durante el período evaluado, la calidad documental de los casos registró un desempeño superior al 99,07% 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 6 hallazgos, alcanzando un cumplimiento del 99,6%. Esto evidencia la necesidad de fortalecer la correcta redacción y revisión de la ortografía al solucionar los tickets.

También se presentaron hallazgos menores en Categoría (2), Elemento CI (2), Cumplimiento de ANS (2), Tipo de caso (1), Asunto (1) y Descripción (1); 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 99,07% 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 24 llamadas, considerando los criterios definidos para el proceso de aseguramiento de la calidad.

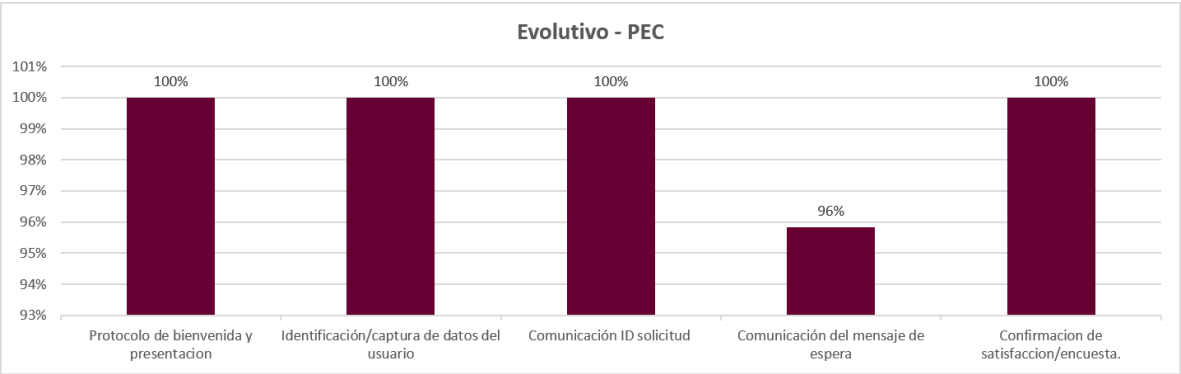


Ilustración 114 Resultado de criterios y parámetros - Calidad de llamadas

Adicionalmente, durante el período se efectuaron 24 monitoreos de calidad sobre las llamadas gestionadas en la operación. Como resultado, se obtuvo un cumplimiento del 99,2%

- 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 Agosto 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.

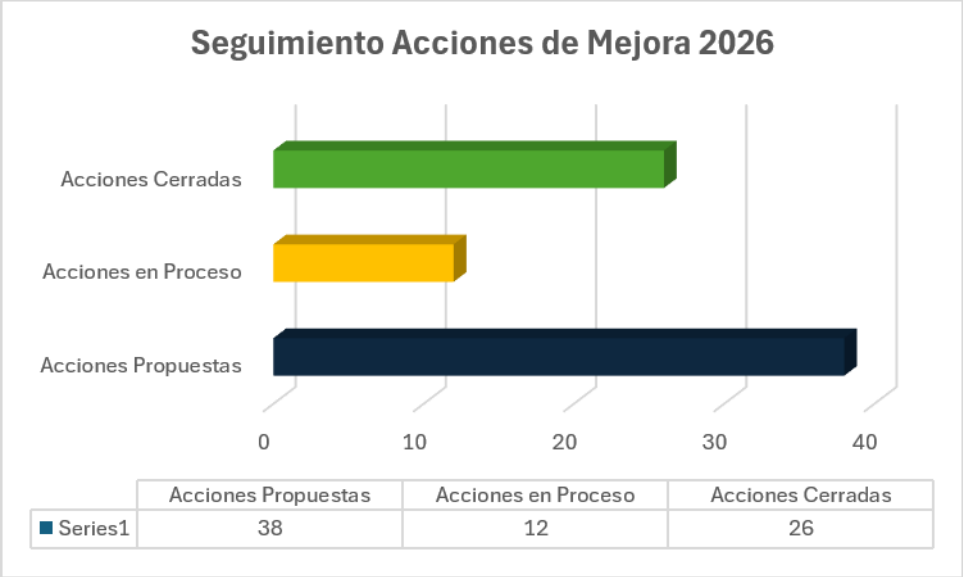


Ilustración 115 Seguimiento Práctica Mejora

En la gráfica anterior se observa el seguimiento a las acciones de mejora identificadas durante 2026. Al corte del 31 de Agosto de 2026, de un total de 38 acciones de mejora, 26 se encuentran cerradas, lo que representa un avance del 68,42%, 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 119 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.

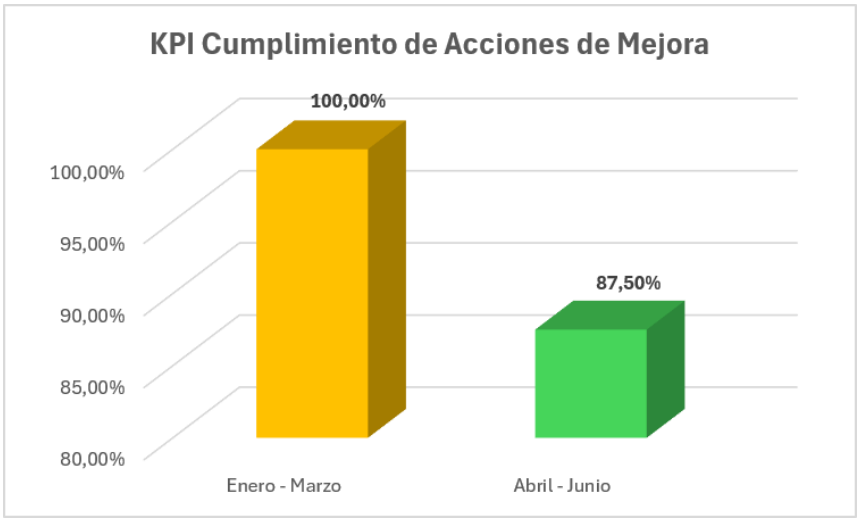
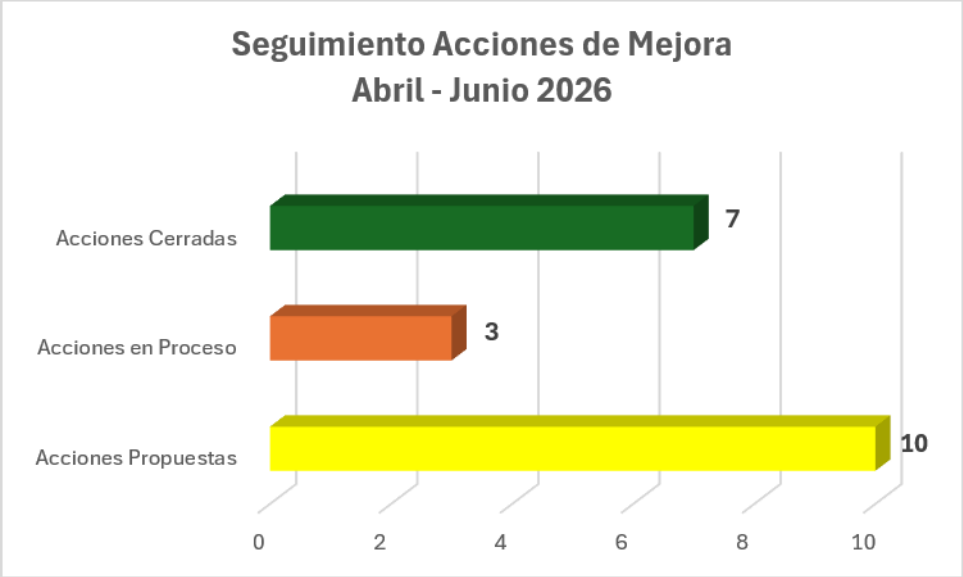


Ilustración 116 Resultado de Cumplimiento AM

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 agosto 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.

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

SERVICIO/ PRÁCTICA	NOMBRE	DESCRIPCIÓN	¿MATERIALIZADO?	ACCIONES PARA REALIZAR
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	SI	La creación manual de la solicitudes de los usuarios
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.
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,	NO	Se realizó la planeación del primer ejercicio de Ethical Hacking. Se ejecutaron de manera oportuna y permanente las

SERVICIO/ PRÁCTICA	NOMBRE	DESCRIPCIÓN	¿MATERIALIZADO?	ACCIONES PARA REALIZAR
		permitiendo la ejecución de código malicioso.		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 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 120 Gestión de Riesgos

7 BOLSA DE RECURSOS

Para el período del informe no se realizó consumo de la 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	99,25%	95,00%
	Tiempo de solución de incidentes por soporte en sitio	98,89%	90,00%
	Tiempo de solución de requerimientos por soporte en sitio	98,64%	90,00%
	Tiempo de respuesta de la mesa de servicio	98,04%	85,00%
	Abandono de llamadas	2,17%	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	99,39%	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	97,25%	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	98,85%	90,00%
	Tiempo de solución requerimientos asociado a los servicios de administración, soporte y monitoreo	99,15%	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 121 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 agosto
- Detalle_llamadas_recibidas_(01.08.2026-31.08.2026)
- Datos_Mintrabajo_agosto
- Certificado Licenciamiento IBM
- Certificado Licenciamiento Liferay

FIN DEL DOCUMENTO