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

Abril de 2026

DOCUMENTO/ ARCHIVO	
Código:	**Informe Gestión - Unión Temporal Gestión TIC 2023**
Nombre Archivo:	**Informe Gestión - Unión Temporal Gestión TIC 2023 – abril 2026**
Fecha:	8/05/2026
Versión:	1

REGISTRO DE CAMBIOS			
Versión	**Páginas**	**Fecha Modificación**	**Motivo del cambio**
1	185	8/05/2026	Elaboración del documento

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

Índice

Introducción 11
Objetivo 11
Alcance 11
Definición de Siglas y Expresiones Técnicas 12
1 GERENCIA Y/O ADMINISTRACIÓN 13
2 LÍNEA DE GESTIÓN DE SERVICIOS 13
2.1. Gestión del Servicio 13
2.1.2. Prácticas ITIL 4 19
2.1.2.1. Práctica Acuerdos Niveles de Servicio (ANS) 21
2.1.2.2. Práctica Habilitación de Cambios 22
2.1.2.3. Práctica Gestión de Activos 23
2.1.2.4. Práctica Catálogo de servicios 25
2.1.2.5. Práctica de Problemas 27
2.1.2.6. Práctica de Incidentes 29
2.1.2.7. Práctica de Requerimientos 36
2.1.2.8. Práctica de Eventos 41
2.1.2.9. Práctica de Disponibilidad 59
2.1.2.10. Práctica de Implementación 62
2.2 Mesa de Servicios y Soporte en Sitio 63
3 LINEA DE SERVICIOS CENTRALES 73
3.1 Datacenter Principal 73
3.1.1 Datacenter Alterno y DRP 76
3.1.2 Procesamiento almacenamiento y respaldo Servicio Windows y Office 365. 82
3.1.3 Procesamiento, almacenamiento y respaldo - Nube Privada 87
3.1.4 Aplicaciones Especializadas 95
3.1.5 No aplica 109
3.1.6 Seguridad Informática 109
3.1.6.1 Firewalls de nueva generación 109
3.1.6.2 Sandbox – Amenazas día 0 115
3.1.6.3 SIEM - Solución de correlación de eventos de seguridad, disponibilidad y recursos 118
3.1.6.4 WAF - Servicio de tipo “Firewall de Aplicaciones Web” 123
3.1.6.5 Solución de Anti-DDoS 124
3.1.6.6 Casos atendidos de los servicios de seguridad 125
3.1.6.7 Análisis de riesgo 127
3.1.6.8 Políticas y procedimiento de seguridad 128
3.1.7 Licenciamiento 128
3.1.8 Administración, soporte y monitoreo 129
3.2 No aplica 130
3.3 Conectividad WAN, SDWAN e Internet 130
3.3.1 Canales WAN 130
3.3.1.1 Incidentes de Conectividad 132
3.3.1.2 Topología Actual 133
3.3.2 Canales SDWAN e Internet Dedicado 133
4 LINEA DE SERVICIOS EN SEDE 137
4.1.1.1 Equipos de Cómputo de usuario final 137
4.1.2 Equipos de Escritorio 142
4.1.3 Equipos Portátiles 142
4.2 Conectividad LAN y WLAN 142
4.2.1 Switch CORE Sede Principal 144

4.2.2 Switch para conexiones perimetrales (EDGE) en sede principal 144
4.2.3 Switch de acceso 24 puertos 144
4.2.4 Switch de acceso 48 puertos 145
4.2.5 Puntos de Acceso 146
4.3 Telefonía IP 147
4.3.1 Teléfono Gama Media 147
4.3.2 Teléfono Gama Baja 147
4.3.3 Troncales SIP 148
4.3.4 No Aplica 148
4.3.5 No Aplica 148
4.3.6 Módems 4G – Con plan de 50 Gbps 148
4.4 Energía Regulada UPS 154
4.4.1 UPS 10 kVA 154
4.4.2 UPS 15 kVA 155
4.4.3 UPS 20 kVA 155
4.5 No aplica 158
4.6 Outsourcing de Impresión 158
4.6.1 No aplica 161
4.6.2 Multifuncional B/N rango medio – Cargo fijo mensual 162
4.6.3 Impresora Color rango medio – Cargo fijo mensual 162
4.6.4 No aplica 162
4.6.5 Multifuncional B/N rango medio – Clic de impresión 162
4.6.6 Impresora Color rango medio – Clic de impresión 162
4.7 Antivirus 163
4.7.1 Instalaciones de antivirus en servidores 163
4.7.2 Instalación de antivirus PCs usuarios final 164
4.7.3 Top 10 Virus Detectados 165
4.7.4 Servicio de Vulnerabilidades 170
4.7.4.1 Inventario y licenciamiento 171
4.7.4.2 Escaneos programados 171
4.7.4.3 TOP 10 – Vulnerabilidades más explotables 172
4.7.4.4 Estrategia de remediación y/o mitigación 173
4.7.4.5 Resumen de mitigación efectuada 174
5 GESTIÓN DE CALIDAD DE INFORMACIÓN 176
5.1 Evaluación calidad documental de casos 176
5.2 Evaluación de calidad de llamadas 177
5.3 Práctica de Mejora 179
6 GESTION DE RIESGOS 180
7 BOLSA DE RECURSOS 183
8 MEDICIÓN DE ACUERDOS DE NIVEL DE SERVICIO 183
9 ANEXOS 185

Índice de Tablas

Tabla 1 Atención de solicitudes por Grupo de Especialista 20
Tabla 2 Medición Indicador Porcentaje de Cumplimiento de ANS 21
Tabla 3 Tipificación de los cambios 22
Tabla 4 Medición Indicador Porcentaje de Cambios Exitosos 22
Tabla 5 KPI Práctica Catálogo de Servicios 27
Tabla 6 Consolidado problemas identificados 27
Tabla 7 Categorización de Incidentes por Servicio 32

Tabla 8 Top 10 Incidentes 33
Tabla 9 Incidentes Suspendidos 33
Tabla 10 Medición de KPIs 34
Tabla 11Estados de Requerimientos 37
Tabla 12 Estados de Tareas de requerimientos 37
Tabla 13 Seguimiento del Backlog Suspendidos 37
Tabla 14 Top 10 de Solicitudes 38
Tabla 15 Detalle de KIP Practica de Requerimientos 39
Tabla 16 Casos reabiertos 41
Tabla 17 KPI Práctica de Eventos 59
Tabla 18 Consolidado disponibilidad de servidores 59
Tabla 19 Consolidado disponibilidad de Directorio Activo 59
Tabla 20 Desagregado de Disponibilidad Directorio Activo 60
Tabla 21 Consolidado disponibilidad de equipos Datacenter principal 60
Tabla 22 Desagregado de Disponibilidad Datacenter Principal 60
Tabla 23 Consolidado disponibilidad de equipos Datacenter alterno 60
Tabla 24 Desagregado Disponibilidad de equipos Datacenter alterno 60
Tabla 25 Consolidado disponibilidad de equipos redes y conectividad 60
Tabla 26 Consolidado disponibilidad de equipos de seguridad 61
Tabla 27 Disponibilidad de equipos Seguridad de la Información 61
Tabla 28 Consolidado disponibilidad de equipos de telefonía 61
Tabla 29 Consolidado disponibilidad de plataforma antivirus 61
Tabla 30 Llamadas Atendida por la Mesa de Servicio 63
Tabla 31 casos suspendidos 65
Tabla 32 Casos Atendidos usuarios VIPs 70
Tabla 33 Casos Atendidos usuarios 70
Tabla 34 Visitas a sedes sin Soporte en Sitio 72
Tabla 35 Medición de ANS Mesa de servicios 73
Tabla 36 Pruebas realizadas 78
Tabla 37 Capacidades iniciales 92
Tabla 38 Capacidades modificatorio 92
Tabla 39 Total capacidades + servers desaprovisionamiento 92
Tabla 40 Total capacidades consumidas 93
Tabla 41 Total capacidades sin servers de pruebas 93
Tabla 42 Total capacidades ambientes pruebas 93
Tabla 43 Consumos totales 94
Tabla 44 *Suma Instancias* 104
Tabla 45 Total Docs 105
Tabla 46 Total Radicados 105
Tabla 47 Dimensionamiento Servers IBM - Virtualización Optima 106
Tabla 48 Apps & DDBB Oracle 109
Tabla 49 Tendencia de uso de ancho de banda 110
Tabla 50 usuarios con mayor consumo de ancho de banda 111
Tabla 51 Top de usuarios por sesiones 112
Tabla 52 Top de aplicaciones 113
Tabla 53 Consolidado de indicadores 115
Tabla 54 métricas EPS 119
Tabla 55 Tipos de incidentes 120
Tabla 56 Hosts e IPs Implicados 120
Tabla 57 Usuarios con Mayor Actividad de Riesgo 121

Tabla 58 Aplicaciones por Ancho de Banda 121
Tabla 59 Tipo de ataque 124
Tabla 60 Reporte de requerimientos abril 127
Tabla 61 Vulnerabilidades en la infraestructura 127
Tabla 62 Vulnerabilidades en la infraestructura 127
Tabla 63 ataques de phishing 127
Tabla 64 Licenciamiento 129
Tabla 65 Medición ANS Datacenter 130
Tabla 66 Medición ANS Nube Pública 130
Tabla 67 Incidentes de conectividad 132
Tabla 68 Medición de ANS Conectividad WAN e Internet 136
Tabla 69 Desagregado sedes con novedad un solo enlace 137
Tabla 70 Desagregado sedes con novedad con doble enlace 137
Tabla 71 Cantidades de equipos Contractual – Instalados - Almacén 138
Tabla 72 Cantidades de equipos asignados nivel nacional 138
Tabla 73 Cantidades de equipos por devolución nivel nacional 139
Tabla 74 Estado de casos de garantía. 139
Tabla 75 ANS casos de garantía. 139
Tabla 76 ANS Relación casos de garantía 140
Tabla 77 Equipos en siniestro 141
Tabla 78 Solicitudes de Equipos Usuario Final – Según Grupo Responsable 142
Tabla 79 Solicitudes de Equipos Usuario Final – Según Grupo Responsable 142
Tabla 80 Medición ANS Equipos de Usuario Final 142
Tabla 81 Top 5 de categorías en el Servicio de conectividad LAN-WLAN 143
Tabla 82 Distribución y Cantidades de switch 24 puertos 145
Tabla 83 Distribución y Cantidades de Switch 48 puertos 145
Tabla 84 Distribución de puntos de acceso 146
Tabla 85 Medición ANS LAN y WLAN 147
Tabla 86 Equipos gama media 147
Tabla 87 Sedes cerradas 148
Tabla 88 Consolidado de teléfonos gama baja 148
Tabla 89 Consolidado equipos MIFI 148
Tabla 90 Minutos, consumos 150
Tabla 91 Top llamadas nacionales 151
Tabla 92 Top 5 consumo de llamadas 151
Tabla 93 Top 5 llamadas LDI 152
Tabla 94 Top 5 llamadas Celular 152
Tabla 95 Top 5 llamadas locales 153
Tabla 96 Medición ANS Telefonía IP 154
Tabla 97 Inventario de UPS – 10kVA 155
Tabla 98 Inventario de UPS – 20Kva 156
Tabla 99 Casos gestionados – Energía Eléctrica Regulada UPS 157
Tabla 100 Medición ANS Energía Eléctrica UPS 158
Tabla 101 Inventario de impresoras para el servicio 158
Tabla 102 Consumo de impresiones y copias por usuario - Impresoras B/N 159
Tabla 103 Top 10 de impresoras con mayor uso 159
Tabla 104 Top usuarios impresión a color 160
Tabla 105 Top oficinas 160
Tabla 106 Top 10 impresoras más usadas del servicio de fotocopiado 161
Tabla 107 Ampliación de cuota de impresión 161

Tabla 108 Despacho de papel a sedes del Ministerio del Trabajo 161
Tabla 109 Cargo mensual multifuncional rango medio 162
Tabla 110 Cargo mensual impresora color 162
Tabla 111 Clics de impresión de marzo 2026 – Multifuncional B/N 162
Tabla 112 Tendencia de consumo de clics B/N 162
Tabla 113 Clics de Impresión – Impresora Color 162
Tabla 114Tendencia de consumo de clics color 163
Tabla 115 Medición ANS Outsourcing de Impresión 163
Tabla 116 Medición de ANS Antivirus 176
Tabla 117 KPI Practica de Mejora 180
Tabla 118 Gestión de Riesgos 183
Tabla 119 Bolsa de Recursos 183
Tabla 120 Medición de Acuerdos de Niveles de Servicio 184

Índice de Ilustraciones

Ilustración 1 Estado final de casos al corte del período 20
Ilustración 2 Socialización matriz de escalamiento 25
Ilustración 3 Estados Incidentes 29
Ilustración 4 Categorización de Incidentes por Servicio 30
Ilustración 6 Top 10 Incidentes 32
Ilustarcion 7 Incidentes Suspendidos 33
Ilustración 8 Efectividad de resolución de incidentes 35
Ilustración 9 Porcentaje de incidentes abiertos 36
Ilustración 10 KPI Efectividad de Resolución de Requerimientos de Servicio 39
Ilustración 11 Requerimientos de Reabiertos en el periodo 40
Ilustración 12 Resumen de incidentes 43
Ilustración 13 Sedes afectadas por router 43
Ilustración 14 Causas de eventos generados por router 44
Ilustración 15 Casos suspendidos VS. Casos solucionados/Cerrados de Router 45
Ilustración 16 Sedes afectadas por Switch 46
Ilustración 17 Top 9 Sedes afectadas por Access Point 47
Ilustración 18 Causa de eventos generados por AP 47
Ilustración 19 Casos suspendidos VS. Casos solucionados de AP 48
Ilustración 20 Top 10 Sedes afectadas por Starlink 49
Ilustración 21 Causas de eventos generados por Starlink 50
Ilustración 22 Casos suspendidos VS. Casos solucionados de Starlink 51
Ilustración 23 Top 5 Sedes afectadas por FortiGate 51
Ilustración 24 Causas de eventos generados por FortiGate 52
Ilustración 25 Casos suspendidos VS. Casos solucionados de FortiGate 53
Ilustración 26 Estado de casos escalados a Proveedor 54
Ilustración 27 Causas de alarmas Servidores Windows 54
Ilustración 28 TOP 10 de servidores Windows con mas alarmas 55
Ilustración 29 Casos suspendidos VS. Solucionados o cerrados Servidores Windows 56
Ilustración 30 Causas de alarmas Servidores Linux 56
Ilustración 31 TOP 10 de servidores Linux con mas alarmas 57
Ilustración 32 Casos suspendidos VS. Solucionados o cerrados Servidores Linux 57
Ilustración 33 Grafica CPU 58
Ilustración 34 Grafica memoria 58
Ilustración 35 Seguimiento de Pruebas de Disponibilidad 2026 62
Ilustración 36 Seguimiento Práctica Implementación 63
Ilustración 37 Llamadas Atendidas 64

Ilustración 39 Incidentes solucionados soporte en sitio 66
Ilustración 40 Incidentes solucionados soporte territoriales 66
Ilustración 41 requerimientos solucionados mesa de servicios 67
Ilustración 42 requerimientos solucionados soporte en sitio 67
Ilustración 43 requerimientos solucionados soporte territoriales 68
Ilustración 44 Requerimientos Cerrados por la Mesa de Servicios 68
Ilustración 46 Casos Cerrados por Soporte en Sitio 69
Ilustración 47 Casos Cerrados por Territoriales 69
Ilustración 48 Medios de Ingreso de Casos 70
Ilustración 49 Gestión Casos - SC 73
Ilustración 50 Gestión SC - Por Grupo 74
Ilustración 51 Comportamiento SWCORE Datacenter Colombia XV 75
Ilustración 53 Sincronización HA de los Switch Core 75
Ilustración 54 Grafica de consumo canal Internet Datacenter 76
Ilustración 55 máquinas virtuales DRP 77
Ilustración 56 Escenario pruebas Apps DRP 78
Ilustración 58 Extremo DC Bogotá 79
Ilustración 59 Extremo DC Cali 79
Ilustración 60 Estado canal de Internet DC Cali 79
Ilustración 61 Estado SWCORE Datacenter alterno 80
Ilustración 62 Estado HA SWCORE Datacenter alterno 81
Ilustración 63 Consumo canal MPLS DC Alterno 81
Ilustración 64 Estado Router MPLS DC Alterno 82
Ilustración 65 Gestión de Casos Windows 83
Ilustración 66 Cumplimiento WSUS 84
Ilustración 67 Block Legacy Authentication 85
Ilustración 68 Fechas de Soporte 87
Ilustración 69 Licencias asignadas 87
Ilustración 70 Gestión Nube Privada 91
Ilustración 71 Nuevo entorno ACEDOC 97
Ilustración 72 Gestión Apps Especializadas 97
Ilustración 73 Arquitectura final Apps 99
Ilustración 74 Distribución Sitios IIS 100
Ilustración 75 Gestión Casos IBM 103
Ilustración 76 Licenciamiento adicional componente IBM 106
Ilustración 77 Gestión DDBB 107
Ilustración Estado Bases de Datos 108
Ilustración 79 Firewall de nueva generación. 109
Ilustración 80 Comportamiento ancho de banda 110
Ilustración 81 Tendencia de uso de ancho de banda 111
Ilustración 82 Top de usuarios por números de sesiones 112
Ilustración 83 Top de aplicaciones 113
Ilustración 84 Top de Autenticación 114
Ilustración 85 sesiones fallidas 115
Ilustración 86 Reporte mensual 116
Ilustración 87 Captura de pantalla perfomance 117
Ilustración 88 licencia sandbox 118
Ilustración 90 Detalle servidores 122
Ilustración 91 Top attack types 123
Ilustración 92 Top de ataques 125

Ilustración 93 Políticas y procedimientos 128
Ilustración 94 Consumo canal MPLS DC Principal 131
Ilustración 95 Estado Router MPLS DC Principal 132
Ilustración 97 Topología actualizada 133
Ilustración 98 Interface Fortimanager 134
Ilustración 99 Interface MPLS HUB SDWAN 134
Ilustración 100 Interface Internet HUB SDWAN 135
Ilustración 101 VPN SDWAN establecidas 135
Ilustración 103 Estado HUB SDWAN Datacenter 135
Ilustración 104 Estado HA HUB Sdwan 135
Ilustración 105 Recursos Fortimanager 136
Tabla 74 Estado de casos de garantía. 139
Tabla 76 ANS Relación casos de garantía 140
Tabla 80 Medición ANS Equipos de Usuario Final 142
Ilustración 109 Estado de casos Redes y Conectividad 144
Tabla 84 Distribución de puntos de acceso 146
Tabla 86 Equipos gama media 147
Ilustración 112 Asignación de licencias 149
Ilustración 113 Comportamiento de tráfico 150
Tabla 92 Top 5 consumo de llamadas 151
Ilustración 115 llamada internacional de prueba 151
Tabla 93 Top 5 llamadas LDI 152
Ilustración 117 Top Celular 152
Tabla 94 Top 5 llamadas Celular 152
Ilustración 119 Top Local 152
Tabla 95 Top 5 llamadas locales 153
Ilustración 121 Requerimientos por garantía 153
Ilustración 122 Disponibilidad y Continuidad TOIP 154
Tabla 97 Inventario de UPS – 10kVA 155
Tabla 99 Casos gestionados – Energía Eléctrica Regulada UPS 157
Tabla 102 Consumo de impresiones y copias por usuario - Impresoras B/N 159
Tabla 103 Top 10 de impresoras con mayor uso 159
Tabla 104 Top usuarios impresión a color 160
Tabla 106 Top 10 impresoras más usadas del servicio de fotocopiado 161
Tabla 107 Ampliación de cuota de impresión 161
Tabla 109 Cargo mensual multifuncional rango medio 162
Tabla 111 Clics de impresión de marzo 2026 – Multifuncional B/N 162
Tabla 113 Clics de Impresión – Impresora Color 162
Tabla 115 Medición ANS Outsourcing de Impresión 163
Ilustración 134 Equipos consola antivirus 164
Ilustración 135 Gestión consola antivirus – equipos usuario final 165
Ilustración 136 Top 10 virus detectado 166
Ilustración 137 Descripción de virus 166
Ilustración 138Top 5 Equipos 168
Ilustración 139 BODSDIAZR 168
Ilustración 140 BOPEOVIEDO 168
Ilustración 141 UDACAICEDO 169
Ilustración 142 PEDDBEDOYA 169
Ilustración 143 Eventos Ransomware 169
Ilustración 144 captura eventos ransonware 170

Ilustración 145 Licenciamiento 170
Ilustración 146 *Gestión consola Nessus* 171
Ilustración 147 *Escaneos programados* 172
Ilustración 148 TOP 10 - Activos más explotables 173
Ilustración 149 Vulnerabilidades gestionadas vs en remediación 174
Ilustración 150 revisión configuraciones 175
Ilustración 151 captura envío de correo gestión de vulnerabilidades 175
Tabla 116 Medición de ANS Antivirus 176
Ilustración 153 Resultado General 176
Ilustración 154 Resultado de criterios y parámetros - Calidad de llamadas 178
Ilustración 155 Seguimiento Práctica Mejora 179
Ilustración 156 Resultado de Cumplimiento AM 180

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 abril 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 posterior envío de diferentes comunicados y divulgación de información a través de la cuenta de Soporte MT, los comunicados se orientaron a:

- **Incidentes mayores e intermitencias** presentadas en la operación de los servicios de TI y/o aplicaciones.
- **Ventanas de mantenimiento programadas** sobre la infraestructura tecnológica y/o aplicaciones avaladas bajo los lineamientos de la práctica de habilitación de cambios:
  - Mantenimiento sobre servidores de aplicaciones que involucran SIAS, Filco, APP2, Moodle, Cobro Coactivo, Tramites, SIAS, Observatorio, PQRSD, entre otras
  - Mantenimiento del servicio de conectividad en Nivel Central.
  - Mantenimiento del portal WEB.
  - Mantenimiento BD Gestor Documental
  - Mantenimiento SIRITI
- Aspectos claves para **creación de contraseñas seguras** de acceso a la red, los sistemas de información y aplicaciones; así mismo, se recuerda que no se deben almacenar contraseñas en navegadores de equipos de cómputo por seguridad de la información y para evitar el bloqueo de usuarios en el dominio por políticas internas.



¡INFORMACIÓN
IMPORTANTE - LINEA

- Promoción del **diligenciamiento de la encuesta de satisfacción de los servicios de tecnologías de la información**, se brindan indicaciones de como diligenciarla.



¡INFORMACIÓN
IMPORTANTE ENCUE

- 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 AGENT

- 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 PORTA

b. Traslados y novedades de sedes:

- **Segovia / Antioquia:** Se hizo traslado de la inspección de trabajo 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:** La sede no cuenta con usuario asignado por pensión, los equipos a cargo de la UT se encuentran en la sede apagados, a espera de asignación de los nuevos funcionarios.
- **Cañas Gordas / Antioquia:** La sede no cuenta con funcionario asignado, no se tiene información hasta que fecha. Los equipos a cargo de la UT se encuentran en la sede apagados.
- **IT Pitalito:** Inactiva por vacaciones desde el 1 de abril hasta el 6 de mayo 2026.
- **IT La Plata:** Inactiva por permiso del usuario los días 6, 7 y 8 de abril. Se reintegra el jueves 9 de abril 2026.
- **IT San Marcos - IT Líbano:** Inactivas por permisos entre el 1 y 9 de abril 2026.
- **El Doncello:** Usuario trabaja en sede una semana al mes, el resto de tiempo se desplaza a la DT.
- **Tibú:** Usuario trabaja algunos días en la semana, el resto de tiempo se desplaza a la DT.
- **IT Ipiales:** Requiere adecuación del cableado estructurado en la sede, el cable está pegado al piso de la oficina con cinta pegante.

- Novedades de las sedes trasladadas en los últimos meses según disposiciones de la entidad:
    - **Anserma / Caldas:** Por remodelación física de la alcaldía del municipio, la sede estuvo en lugar temporal entre el 8/03/2025 y el 29/01/2026, al volver a Casa de Justicia a sede fue ubicada en una oficina diferente por disposición de la alcaldía. La sede actual no cuenta con puntos de red ni puntos de energía cercanos a los puestos de trabajo, los puntos de energía se solventaron con extensiones y se dejaron equipos cerca al fortinet. Se habilita medio de conectividad temporal ya que en los arreglos hicieron corte de la fibra.
    - **Tumaco / Nariño** se trasladó el 16/01/2026 presentándose novedades que fueron reportadas al Coordinador del Grupo de Soporte Informático. La sede no cuenta con puntos de red para la conexión adecuada de los dispositivos, se realizó conexión de equipos con patchcord cerca del equipo Fortinet.

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

- Práctica Acuerdos de Nivel de Servicio en los Servicios de Tecnologías de Información.
- Práctica Requerimientos en los Servicios de Tecnologías de Información.
- Práctica Disponibilidad en los Servicios de Tecnologías de Información.

d. Disposición de RAEES y Residuos Electrónicos: Durante el periodo se gestionaron permisos para la salida de elementos o residuos tecnológicos, así:

- El **10 de abril de 2026** se gestiona salida de elementos por parte del soporte Cristian David Rocha Rodriguez (DT Santander) para ser entregados al proveedor (SUMA Desarrollo Ambiental.

Residuo	CANTIDAD
Diademas Lenovo - RAEE	1
Unidad Fusora Impresoras- RAEE	1
Unidades de Tambor Impresoras- RAEE	5
Cartuchos y tóner de impresoras de oficina	33

e. Implementación IPV6 en Dual Stack: A continuación, se relaciona el avance durante el período de la fecha en la implementación del protocolo IPV6 en Dual Stack para los servicios de TI definidos por la UT en el alcance:

- **SOC:** En conjunto con el SOC, se continúan ajustando las políticas de seguridad para la red de pruebas, se viene trabajando con ellos en sesiones programadas según disponibilidad para replicar el modelo de enrutamiento a las demás redes y posteriormente replicar también las políticas.
- **Para el servicio de SD-WAN:** Luego de los laboratorios y configuraciones realizadas por el equipo, se completa fase 2 de la VPN y se logra tener conectividad hacia el Data Center Alterno. Se esta replicando la configuración en el DC Principal

y adicional, se continua la labor de configuración en interfaces y equipos. Se esta realizando pruebas de la plantilla para aplicar la configuración a nivel general.

- **Para el servicio de conectividad LAN / WLAN:** Ya se efectuó la configuraron en los switches, se está realizando el proceso la configuración de access point con un avance del 80% de esta actividad.
- **Para el servicio de telefonía:** Se tiene un avance del 80% en la de la VLAN de voz en direcciones territoriales, ya cuenta con DHCP habilitado.
- **Para la infraestructura centralizada**: se están realizando pruebas de publicación de la página por parte del equipo de infraestructura, ya que se requiere realizar configuración en el balanceador para recepción de tráfico IPV6 y liberación hacía los servidores de aplicación, en seguimiento de los resultados. Se continúa avanzando en la configuración para algunas máquinas de los segmentos que se asignaron. Se encuentra en revisión con los especialistas la habilitación de servicios web sobre IPv6, incluyendo la configuración de resolución DNS mediante registros AAAA, actualmente existe un registro de tipo AAAA con un direccionamiento en la zona DNS de mintrabajo, pero posiblemente haga referencia a un pool con el que la entidad ya no cuenta, por lo que habría que realizar otra creación de DNS y eliminación del registro existente.
- **Para el servicio de impresión:** Se realiza despliegue de configuración de IPV6 en las impresoras de OE e IT, así se concluye la activación de lo requerido en los equipos.

f. Otras actividades

- **Lineamientos de Oficina TICs para gestión de usuarios e incidentes de seguridad**
  El 06/11/2025 y 11/11/2025 se remitió vía correo electrónico a la Oficina de TICs las observaciones a los documentos ***Lineamiento Específico Gestión de Cuentas de Usuario y Cuentas Especiales y ODI POLÍTICA DE GESTION DE INCIDENTES DE SEGURIDAD y ODI PROCEDIMIENTO GESTION DE INCIDENTES*** **emitido por la Oficina TICs**, debido a que se tenían varias actividades que no se encontraban definidas en cuanto a roles y entregables por parte de la UT y del Grupo de Soporte Informático.
  Se recibe versión final del documento de la gestión de cuentas de usuario, el cual está siendo revisado desde la práctica de requerimientos para ajustar los flujos que sean requeridos para el cumplimiento de los lineamientos.

  A espera de recibir retroalimentación al documento de Incidentes de Seguridad, y a que se divulguen los documentos finales con el usuario final.

- **Red WiFi para visitantes**
  Se genera divulgación de la disponibilidad de la red WiFi para los invitados y terceros que ingresen a las oficinas de la entidad, lineamientos de como solicitar el acceso, el tiempo de conexión, entre otros.



¡INFORMACIÓN
IMPORTANTE ACCES(

- **Gestión de información de residuos tecnológicos y entrega de papel**
  El 1/04/2026 vía correo electrónico se da respuesta a Maria Camila Acosta del Grupo de Recursos Físicos, Gestión y Administración de Bienes del Ministerio del Trabajo con información de Enero, Febrero y Marzo 2026 relacionado con el manejo ambiental: Bitácora de residuos tecnológicos, Manifiestos y certificados de disposición final, cronograma de capacitación al personal de la UT sobre el manejo de residuos del proyecto, envío de papel a nivel nacional, control de recarga de papel en impresoras de Nivel Central - DT Bogotá y Territorio, clics de impresión por sede.


RE_ SOLICITUD DE INFORMACIÓN_ REP(


RE_ SOLICITUD DE INFORMACIÓN_ REP(

- 13/04/2026: Con el apoyo de la Ing. Derly Milena Cocunubo – Jefe Oficina TICs, se replicó con todas las direcciones territoriales un **Memorando con los LINEAMIENTOS PARA LA PRESERVACIÓN Y PROTECCIÓN DE LA INFORMACIÓN INSTITUCIONAL** sugerido por la UT, dadas las novedades recientes de movimiento de personal y la necesidad de salvaguardar la información institucional de cada rol, asegurando la sincronización de la información en la nube y que no contenga archivos de carácter personal.


SEGURIDAD DE LA INFORMACIÓN Y USO

- **Equipo golpeado en IT Ipiales a causa de cableado estructurado**
  22/04:2026: Se reporta vía correo electrónico al coordinador del Grupo de Soporte Informático novedad que se presentó en la IT Ipiales, con el propósito que internamente en la entidad se pueda notificar a la dependencia responsable de hacer los ajustes correspondientes del cableado de la oficina y normalizar las conexiones, para evitar que la situación se presente de nuevo. Un funcionario se **tropezó con un cable de red pegado al piso, generando que el equipo de cómputo portátil presentara daños por la caída**, se relacionan los datos de la situación, equipo y el registro fotográfico para conocimiento de los interesados.


RE_ Reporte de incidente con cablead

g. Divulgaciones con el equipo de trabajo

- El 7/04/2026 desde la práctica de requerimientos se realizan varias sesiones de socialización al equipo de soporte técnico en sitio y mesa de servicios el flujo de devolución de bienes (refuerzo) y se incluye el flujo asociado a traslado de sede de un usuario o cambio de rol.


Socialización de Flujo de Devolución de Equ


Socialización de Flujo de Devolución de Equ

- 8/04/2026: Se realiza una mejora de los Lineamientos para la Asignación de CI - Requerimientos e Incidentes para las solicitudes relacionadas con cambio de

contraseñas, cuotas de impresión, novedades de equipos de cómputo y lineamientos generales de solicitudes de O365.

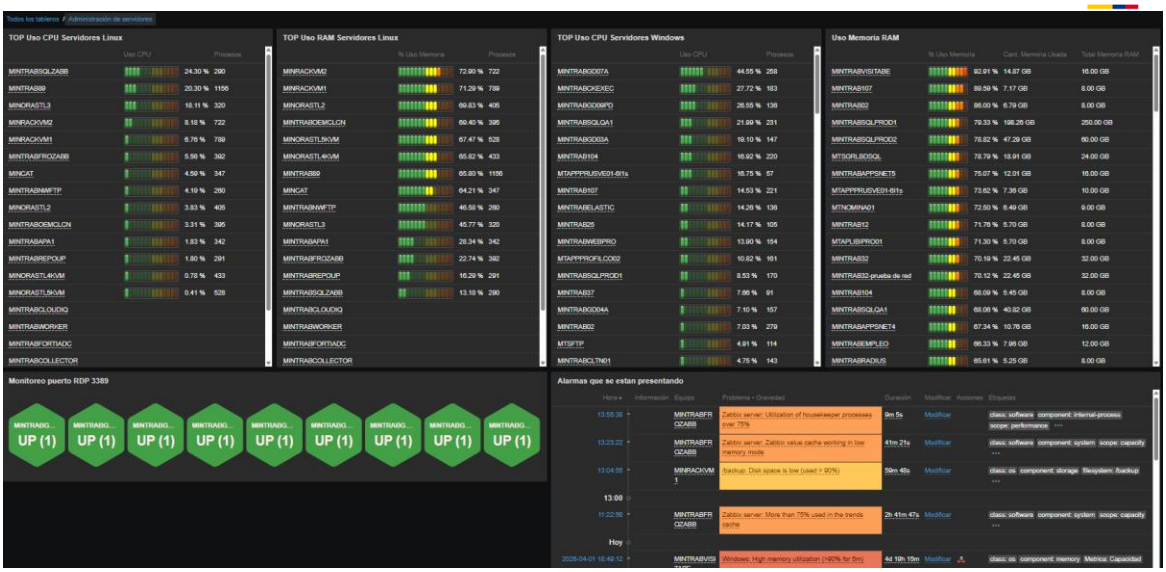


Alcance_ Mejora de
Lineamientos para la

2.1.1. Herramienta de Gestión ITSM

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

- Por medio del RFC-197712 se realiza la actualización de versión de AQM 9.42.0 para la visualización de reportes.
- Se realizó la creación de una herramienta de análisis ortográfico para auditar casos, esto permite agilizar las auditorias de casos y aumentar la calidad de la documentación de los casos. Esta herramienta puede utilizar modelos LLM locales o públicos.
- Se realizo la implementación de la asignación automática de 1 tarea cuando la categoría de un caso es creación de usuario.
- Se realizo ajuste de dependencia para los hosts dado que se identificó que algunas de ellas no estaban aplicando según lo esperado.
- Se creo un reporte en AQM que permite listar de manera rápida todos los Ci´s que actualmente se tienen configurados en la CMDB.
- Se realizo la implementación de la asignación automática de 9 tareas cuando la categoría de un caso es cambio de sede o asignación de rol.
- Se implemento una política de directorio activo que se encargara de actualizar los agentes de ADM en los equipos de los funcionarios. Esta tarea es de afinamiento para el despliegue rápido de la versión actual.
- Se creo reporte de AQM que presentara la información de los casos que sean creados por medio del portal de autogestión, este reporte trae los mismos campos que la sabana de casos general.
- Se adiciono una columna a la sabana de datos general llamada fecha de última nota, la cual como su nombre lo indica traerá la fecha en la cual se adiciono la última nota a un caso.
- Se modifico la columna ANS de la sabana de casos general, esta indicara que el ANS no aplica cuando el tipo de caso sea una tarea.
- 6/04/2026: El administrador de herramientas realiza la creación del tablero de monitoreo para el servicio de administración de servidores según lo solicitado por el líder de infraestructura, este es el link de acceso directo al tablero. http://observabilidad.mintrabajo.gov.co/zabbix/zabbix.php?action=dashboard.view&dashboardid=336



- 10/04/2026: Se realiza el cambio de tiempos de sincronización de Aranda ASMS (herramienta ITSM de gestión de casos) con el AD de mintrab, se encontraba a 5 min y pasó a 360 min, lo anterior debido a que estos tiempos tan cortos generaban cargas innecesarios y fuertes sobre la base de datos de la aplicación. Esto como acción de mejora del servicio, y aplica para cuando se cree, modifique o inactive un usuario en AD el cambio se verá reflejado en Aranda hasta que se active el proceso de sincronización cada 6 horas + el tiempo que tarde la sincronización.
- 21/04/2026: Se gestiona cambio para la actualización de Aranda ASMS a la versión 9.12.0.

2.1.2. Prácticas ITIL 4

Volumetría de Solicitudes Gestionadas:

En el mes de abril 2026 se registraron en la herramienta ITSM 6175 solicitudes asociadas a la prestación de los servicios de TI por parte de la UT.

- Tipificación según la volumetría de casos:
  - Requerimientos de Servicio: 4878
  - Incidentes y Eventos: 754 (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): 515
  - Cambios: 28
  - Problemas: No se registran.
- Casos Anulados: 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 abril 2026:

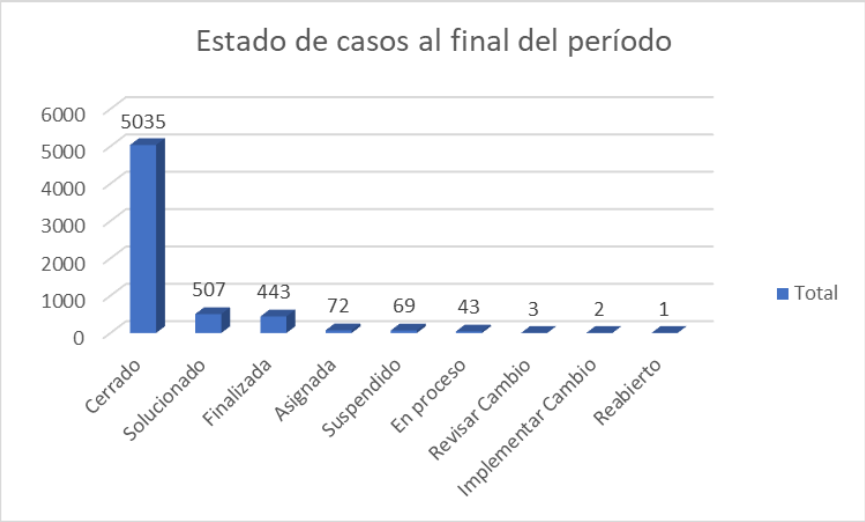


Ilustración 1 Estado final de casos al corte del período

- Gestión por parte de los grupos de especialistas:

Grupo Responsable	Cantidad de casos gestionados	Porcentaje (%)
Responsable_Soporte_Territoriales	1821	29,49
Responsable_Soporte_Bogota	1451	23,50
Responsable_Mesa_De_Servicio	998	16,16
Especialistas_IBM	556	9,00
NOC	418	6,77
Responsable_Soporte_Impresoras	395	6,40
SOC	175	2,83
Responsable_De_Servidores_Windows	90	1,46
Especialista_Telefonía_IP	64	1,04
Especialista Herramientas de Gestion	55	0,89
Especialista Nube Privada	37	0,60
Gestor de Inventarios	31	0,50
Responsable Garantías Equipos	27	0,44
Especialista Base de datos	21	0,34
Especialista Redes	15	0,24
Liferay	4	0,06
Especialista Nube Publica	4	0,06
Almacenamiento y Backups	4	0,06
Gestión del Servicio	4	0,06
Especialista Aplicaciones .Net	2	0,03
Responsable_de_Energia Electrica Regulada - UPS	2	0,03
Especialista Aplicaciones JAVA	1	0,02
Total	**6175**	**100,0**

Tabla 1 Atención de solicitudes por Grupo de Especialista

2.1.2.1. Práctica Acuerdos Niveles de Servicio (ANS)

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

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

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

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

Tabla 2 Medición Indicador Porcentaje de Cumplimiento de ANS

La medición mensual evidenció que, en términos generales, los Acuerdos de Niveles de Servicio (ANS) se mantuvieron dentro de los niveles de cumplimiento esperados, alcanzando un resultado del **95,12%**, lo cual supera la meta establecida del **95%**.
Este resultado refleja una adecuada gestión operativa, contribuyendo a la continuidad, estabilidad y confiabilidad de los servicios tecnológicos prestados, así como al cumplimiento de los compromisos definidos con las partes interesadas.
No obstante, el análisis detallado permitió identificar desviaciones puntuales en indicadores específicos relacionados con la continuidad y disponibilidad del servicio de red WAN. Estas desviaciones, aunque no representaron un impacto significativo en la operación global, constituyen oportunidades de mejora para fortalecer la resiliencia de la infraestructura.

- **Indicadores con Desviaciones Identificadas**

Las desviaciones detectadas corresponden a 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.
-

El detalle técnico y el desglose de los resultados asociados a estos indicadores se encuentra documentado en el archivo soporte **“ANS Internet – MPLS”**, el cual contiene la información base para el análisis realizado.

En conclusión, el desempeño general de los ANS durante el mes de abril de 2026 fue satisfactorio, evidenciando un alto nivel de cumplimiento y la efectividad de los mecanismos implementados para el control, seguimiento y medición del servicio.
Asimismo, se destaca que:

- Se mantuvo la estabilidad de los servicios tecnológicos.
- No se presentaron afectaciones significativas en la operación del negocio.
- Los mecanismos de monitoreo y gestión permitieron identificar oportunamente desviaciones.
- Se cuenta con insumos suficientes para la implementación de acciones de mejora continua orientadas a fortalecer la disponibilidad de la red WAN.

2.1.2.2. Práctica Habilitación de Cambios

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

- **Tipificación de los cambios**

Durante el mes de abril de 2026 se gestionaron 28 casos tipificados como Cambios, clasificados en las siguientes categorías:

Servicio	Cantidad	Porcentaje
Administración de Bases de Datos	9	32,14%
Administración de servidores	6	21,43%
Redes y Conectividad	4	14,29%
Seguridad informática	4	14,29%
Aplicaciones Especializadas	3	10,71%
Herramientas de Gestión	2	7,14%
Total	**28**	**100,00%**

Tabla 3 Tipificación de los cambios

- **Relación casos registrados**

A continuación, se presenta la relación de casos registrados en abril de 2026, en total se crearon 28 casos de los cuales se gestionaron 14 como cambios normales, 10 cambios como de emergencia y 4 cambios como estándar

- **Cambios por estado**

Al corte de abril de 2026, 23 casos quedaron estado Cerrado, 2 casos quedaron estado Implementar Cambio y 2 casos quedaron en Revisar 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: 26/28*100 PCE: 92,86 %

Tabla 4 Medición Indicador Porcentaje de Cambios Exitosos

Durante el periodo evaluado se implementaron 28 cambios, de los cuales 26 finalizaron exitosamente y 2 concluyeron en estado fallido, correspondientes a los RFC-202880 y RFC-199545. Estos cambios fallidos estuvieron asociados a inconvenientes durante la actualización del Supervisor de FortiSIEM, específicamente por fallas en la base de datos que impidieron completar correctamente el proceso.

El resultado del indicador fue 92,86 %, calculado mediante la fórmula PCE = (26 / 28) * 100. Este resultado supera la meta establecida del 80 %, evidenciando un desempeño favorable en la gestión e implementación de cambios durante el periodo evaluado.
Aunque se presentaron dos cambios no exitosos, estos fueron gestionados de manera controlada mediante la reversión al último snapshot disponible, dejando el sistema en el estado previo a la ventana de mantenimiento. Esta acción permitió mitigar el impacto operativo y garantizar la recuperación del servicio.

Adicionalmente, los eventos fallidos fueron documentados y escalados al fabricante Fortinet para su análisis, lo que permite fortalecer el seguimiento técnico y prevenir la recurrencia de situaciones similares. La evidencia registrada confirma que la falla estuvo relacionada con la actualización del esquema de base de datos, la cual permaneció en una versión anterior.

En conclusión, el indicador refleja un nivel adecuado de efectividad en la gestión de cambios, dado que la mayoría de las implementaciones fueron exitosas y las fallas presentadas contaron con acciones de contención oportunas. Se recomienda mantener las validaciones previas, los respaldos y los planes de reversa en cambios críticos, con el fin de asegurar la continuidad del servicio y mejorar continuamente el proceso.

2.1.2.3. Práctica Gestión de Activos

Durante el mes de abril de 2026, la Práctica de Gestión de Activos desarrolló 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:

- **Socializaciones de automatización Flujo de Devolución de Equipos para traslados en sede, cambio de equipo y roles – Aranda:**

Con el objetivo de optimizar y hacer más efectivo el trabajo de los profesionales, se procedió a seguir automatizando del flujo de devolución de equipos para traslados en sede, cambio de equipo y roles en Aranda. Actualmente, este proceso contempla 10 actividades que deben ser creadas manualmente entre las áreas de MDS y Soporte en Sitio, lo que generaba una alta carga operativa al gestionar múltiples procesos para atender una sola solicitud y las tareas no puedan ser eliminadas en ningún flujo de trabajo y que el caso solo pueda cerrarse una vez se haya completado el 100% de las actividades, garantizando así

el cumplimiento de todos los pasos definidos para este tipo de solicitudes. Con esta automatización se espera reducir la carga operativa, mejorar la trazabilidad del proceso y aumentar la eficiencia en la gestión de las solicitudes.

Por lo anterior, se procede a realizar las socializaciones al equipo de trabajo de Mesa de Servicio, Soporte Bogotá y Soporte Territoriales para seguir los nuevos lineamientos de devolución de equipos para traslados en sede, cambio de equipo y roles, según las novedades presentadas de personal de la entidad.

- **Plan de trabajo del Aplicativo SGU y Documentación de la Administración de Inventarios:**

Durante el abril, se ha ido desarrollando el aplicativo de inventarios de SGU, con la finalidad de automatización y actualización real de los movimientos de equipos de los servicios de Operación en Sede (Conectividad, Telefonía, Energía eléctrica y regulada, Infraestructura y equipos de cómputo).
Según las actividades propuesta se han ideo desarrollando con el equipo de la Práctica de activos y administrador de la aplicación:

- Modificaciones de los formatos de actas de asignación y devolución de equipos
- Actualización de estados de los activos
- Realización de las pruebas de funcionalidad de los campos, la correcta actualización del inventario, el manejo de los estados y actualización de actas.
- Actualización del procedimiento de Asignación y devolución de activos
- Actualización del procedimiento de Garantías de equipos
- Actualización del procedimiento de Mantenimientos preventivos de equipo de impresión.

- **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.

- **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.

2.1.2.4. Práctica Catálogo de servicios

Dentro de la práctica de Catálogo de Servicios, se busca consolidar y mantener una fuente única, actualizada y confiable de los servicios disponibles para el Ministerio del Trabajo. Esta práctica permite mejorar la visibilidad de los servicios, facilitar su gestión y asegurar una adecuada alineación con las necesidades de la entidad y de la operación TI.
Durante el mes de abril de 2026, se adelantaron actividades orientadas al fortalecimiento, actualización y control del Catálogo de Servicios, así como al mejoramiento de la calidad de la información registrada en la herramienta de gestión.

- **Automatización y socialización de la matriz de escalamiento**

Durante el mes de abril se llevó a cabo la actualización de la matriz de escalamiento, incorporando ajustes relevantes, como parte del fortalecimiento de la práctica ITIL de Catálogo de Servicios, se realizó la automatización de dicha matriz, permitiendo su consulta a través del tablero dispuesto para tal fin. Posteriormente, la matriz fue socializada mediante correo electrónico a todo el equipo de la Unión Temporal —UT—, con el propósito de garantizar:

- La correcta identificación de los niveles de escalamiento.
- La adecuada gestión de incidentes y requerimientos.
- La optimización de los tiempos de respuesta y atención.
- El fortalecimiento de los canales de comunicación interna.

A través del tablero de la matriz de escalamiento, el equipo puede consultar información clave para la operación, entre ella:

- El listado de contactos de los integrantes del equipo de trabajo.
- Los usuarios VIP de la entidad.
- Las categorías configuradas en la herramienta Aranda, mediante el uso de filtros.

Esta actividad contribuye a fortalecer la gestión operativa de los servicios, facilitar la identificación de responsables y asegurar una atención más oportuna y organizada de los casos registrados.

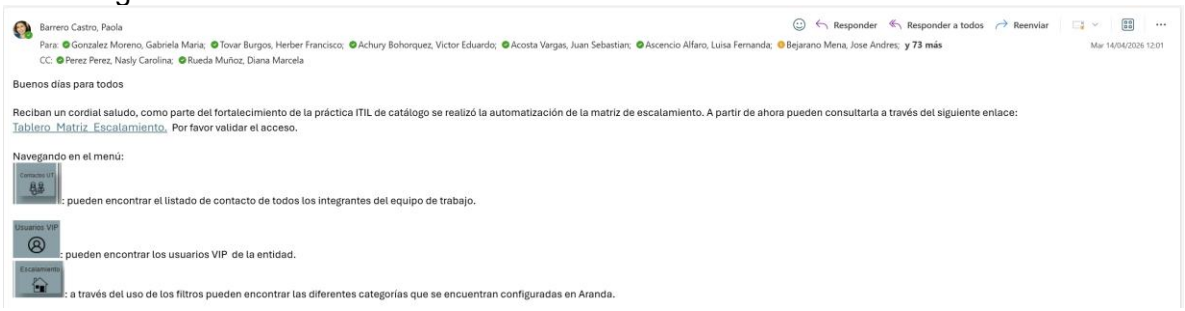


Ilustración 2 Socialización matriz de escalamiento

Se comparte la matriz para consulta y navegación través del siguiente enlace: Tablero_Matriz_Escalamiento.



Matriz de
escalamiento MinTrab

- **Solicitud de creación de categorías en el Catálogo de Servicios**

Con el propósito de fortalecer la gestión del Catálogo de Servicios, durante el mes de abril se solicitó la creación de nuevas categorías asociadas al servicio de Aplicaciones Especializadas, específicamente para el Portal MinTrabajo.
Las categorías solicitadas fueron las siguientes:

Servicio	Especialista	Categoría	ANS
Aplicaciones especializadas	Especialista Liferay / María Elena Lucumí Acevedo	Reportar una solicitud / Portal MinTrabajo / Solicitud de permisos	Tiempo de solución: 84 horas hábiles
Aplicaciones especializadas	Especialista Liferay / María Elena Lucumí Acevedo	Reportar una solicitud / Portal MinTrabajo / Acceso restringido	Tiempo de solución: 84 horas hábiles
Aplicaciones especializadas	Especialista Liferay / María Elena Lucumí Acevedo	Reportar una solicitud / Portal MinTrabajo / Creación y/o modificación de elementos del portal	Tiempo de solución: 84 horas hábiles
Aplicaciones especializadas	Especialista Liferay / María Elena Lucumí Acevedo	Reportar una solicitud / Portal MinTrabajo / Contenidos	Tiempo de solución: 84 horas hábiles

Estas solicitudes permiten ampliar y precisar las opciones disponibles en el Catálogo de Servicios, facilitando una mejor clasificación de los casos y una atención más alineada con las necesidades de los usuarios.

- **Seguimiento a la categorización de casos**

En el marco de las auditorías de calidad, se realizó el seguimiento a la correcta categorización de los casos registrados en la herramienta de gestión, verificando su adecuada clasificación conforme al Catálogo de Servicios definido.

Como resultado de este ejercicio:

- Se identificaron oportunidades de mejora en la categorización.
- Se brindó retroalimentación (feedback) a los equipos involucrados.
- Se promovió la estandarización en el registro de la información.

Estas acciones permiten mejorar la calidad de los datos, facilitar la trazabilidad de los casos y fortalecer la toma de decisiones basada en información confiable.

- **Ajuste los usuarios VIP en la herramienta de gestión.**

Durante el periodo evaluado, se realizó el ajuste y actualización de los usuarios VIP en la herramienta de gestión.
Esta actividad permite mantener actualizada la información de usuarios priorizados, facilitando su identificación dentro de la operación y contribuyendo a una atención más oportuna conforme a los criterios definidos para este tipo de usuarios.

- **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 silencio).	90%	Mensual	CPS= (2/2) *100 EF= 100%

Tabla 5 KPI Práctica Catálogo de Servicios

El resultado obtenido para el mes de abril fue del **100% de cumplimiento**, superando la meta establecida del **90%**. Este resultado evidencia una gestión efectiva en la atención y solución de las solicitudes relacionadas con la actualización del Catálogo de Servicios.
Asimismo, se destaca:

- La oportunidad en la gestión de cambios del catálogo.
- La adecuada articulación entre los equipos responsables.
- La mejora en la organización y disponibilidad de la información de servicios.
- El cumplimiento de las solicitudes recibidas durante el periodo evaluado.

2.1.2.5. Práctica de Problemas

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

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

CI afectado	# casos creados	Estado de los casos
Controlador de dominio	1	Solución definitiva - cierre
Módulo de radicación - Gestor documental	3 3 1	Error conocido Solución Temporal Solución definitiva - cierre
MINTRABGD01A - Gestor documental	1	Solución definitiva - cierre
Office 365	1	Error conocido
Página web	1	Solución definitiva - cierre
servicio de relay en el ISS	1	Solución Temporal
SISINFO	1	Solución Temporal
Telefonía	1	Solución definitiva - cierre
UPS Manizales	1	Solución Temporal
UPS sedes central	1	Investigación y diagnóstico
Total	14	

Tabla 6 Consolidado problemas identificados

Durante el mes de abril se realizó seguimiento al caso 174025 asociado con el Gestor Documental. De acuerdo con la sesión de trabajo realizada el 7 de abril se definieron las acciones que se va a adelantar:

Acciones propuestas y la nueva hoja de ruta:

1. De acuerdo con la revisión realizada por el especialista DBA Oracle de la respuesta de IBM relacionada con base de datos frente al uso de índices compuestos se concluye que se cumple a cabalidad, existen algunas mejoras que pueden explorarse a futuro.
2. Diligenciar RFC para la ventana de BBDD y realizar la desinstalación de java de la máquina. Responsables: Especialista DBA Oracle. Especialistas de servidores fecha: miércoles 8 de abril de 2026
3. Consecución de VoBo de la entidad para la ventana de BBDD Responsable: Lider de servicios centrales fecha: miércoles 8 de abril de 2026
4. Presentación del cambio de emergencia ante la práctica de habilitación de cambios : jueves 9 de abril de 2026 Responsables Especialista DBA Oracle. Especialistas de servidores
5. Realización de ventana de mantenimiento 10 al 12 de abril de 2026
6. Reapertura de caso ante IBM Responsables: Especialistas IBM fecha: 8 de abril de 2026
7. Consecución de mesa técnica con IBM, se trabaja en dos frentes: consulta realizada por Especialistas IBM y consulta realizada por Gerente de proyecto
8. Sesión de seguimiento 21 de abril a las 4 p.m

Se realizó nuevo seguimiento el 22 de abril con los siguientes compromisos:

1. Reapertura de caso ante IBM Responsable: Especialista IBM fecha: 23 de abril de 2026
2. Consecución de mesa técnica con IBM, se trabaja en dos frentes: consulta realizada por Especialista IBM y consulta realizada por gerente de proyecto.
3. Tareas en curso:

- Continuar con la prueba de concepto de la herramienta de monitoreo: Responsable: Especialista de servidores
- A nivel de BBDD continuar con las tareas de mantenimiento recurrente, actualización de estadísticas, revisión de índices e identificación de tablas candidatas a asignar nuevos índices. Responsable: Especialista DBA Oracle

4. Sesión de seguimiento 7 de mayo a las 4 p.m

Durante el mes de abril se realizó seguimiento al caso 174025 asociado con las tarjetas de las UPS que no permiten el monitoreo:

- Se han realizado cuatro (4) visitas técnicas a los equipos UPS ubicados en la sede del Ministerio de Trabajo, con el fin de diagnosticar las fallas reportadas en su operación.
- Durante las intervenciones realizadas, se evidenció la no funcionalidad de las tarjetas de red instaladas en los equipos. Como parte de las acciones correctivas iniciales, se efectuó la actualización de firmware de las UPS, sin lograr restablecer la comunicación ni la operación adecuada de las tarjetas.

- Dado lo anterior, el ingeniero especialista, representante autorizado de la marca Ablerex, procedió con el retiro de la tarjeta de red para su respectivo análisis y diagnóstico en laboratorio especializado del fabricante.

2.1.2.6. Práctica de Incidentes

En abril de 2026 se gestionaron en la Herramienta de Gestión 6175 solicitudes a nivel general. De este total, el 12,21% que corresponden a 754 tickets, fueron tipificados como Incidentes.

Este volumen incluye:

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

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

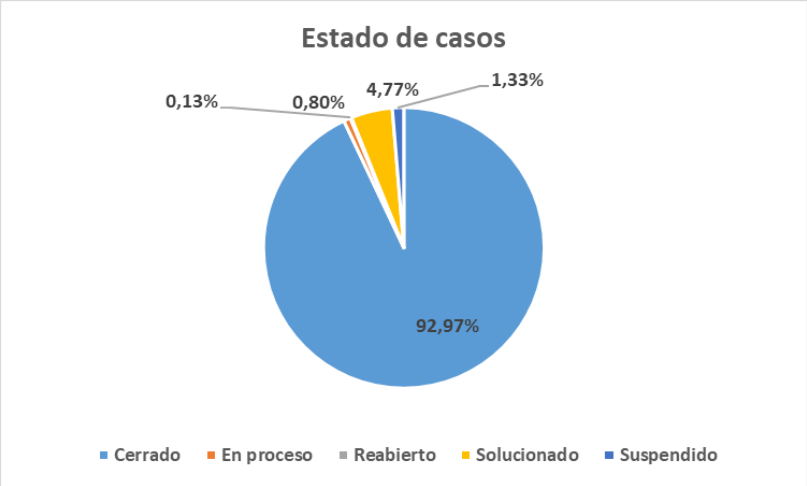


Ilustración 3 Estados Incidentes

- **Categorización de Incidentes por Servicio**

A continuación, se presenta la distribución de los 754 incidentes registrados, clasificados de acuerdo con el servicio afectado, lo que permite identificar los principales focos de impacto en la operación:

Durante el periodo analizado se registraron 754 casos en total, distribuidos en diferentes servicios tecnológicos. La mayor concentración de eventos se presentó en el servicio de Redes y Conectividad, con 407 casos, lo que representa aproximadamente el 53,98% del

total general. Este resultado evidencia que la disponibilidad de los componentes de red continúa siendo uno de los principales factores de afectación operativa.
Dentro de esta categoría, el evento con mayor recurrencia fue Alarma Zabbix.Router, con 225 casos, equivalente al 29,84% del total. También se destacan las alarmas asociadas a Starlink, con 74 casos y 9,81%, y FortiGate, con 68 casos y 9,02%. Esto permite concluir que una parte significativa de los incidentes corresponde a alertas de monitoreo sobre infraestructura de comunicaciones, posiblemente relacionadas con intermitencias, pérdida de conectividad, disponibilidad de enlaces o comportamiento anómalo de equipos de red.

El segundo grupo con mayor volumen corresponde a Soporte Microinformática, con 165 casos, equivalentes al 21,88% del total. En esta categoría sobresalen las fallas relacionadas con impresoras, principalmente atascos, con 34 casos, y no imprime, con 28 casos. También se identifican incidentes en equipos de cómputo, especialmente por fallas o errores de conexión a red, con 29 casos. Esto indica que los usuarios presentan una demanda importante de soporte en dispositivos finales, impresión, conectividad local y herramientas de productividad.

En tercer lugar, se encuentra el servicio de Aplicaciones Especializadas, con 154 casos, correspondiente al 20,42% del total general. La mayor parte de estos eventos está relacionada con el Gestor Documental, especialmente por falla funcional, con 69 casos, equivalente al 9,15%, y falla de radicación, con 33 casos, equivalente al 4,38%. Estos datos muestran que el Gestor Documental concentra una proporción relevante de incidentes funcionales, lo cual puede impactar directamente los procesos de radicación, aprobación, producción documental y atención de trámites.

Por otra parte, los servicios de Administración de Servidores, Energía Eléctrica Regulada - UPS, Telefonía IP y Herramientas de Gestión presentan una participación baja frente al total general. Administración de servidores registra 19 casos, principalmente por alarmas en servidores Windows y Linux. Energía eléctrica regulada y Telefonía IP registran 4 casos cada uno, mientras que Herramientas de Gestión presenta 1 caso. Aunque su volumen es menor, estos eventos deben mantenerse bajo seguimiento debido a que pueden afectar la continuidad de servicios críticos si evolucionan o se presentan de manera recurrente.

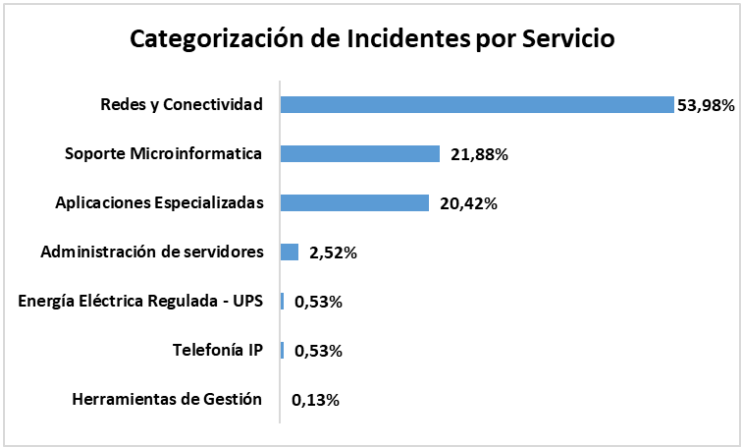


Ilustración 4 Categorización5 de Incidentes por Servicio

Servicio	Categoria	No	Porcentaje
Administración de servidores		**19**	
	Alarma Zabbix.Servidor Windows	17	2,25%
	Alarma Zabbix.Servidor Linux	2	0,27%
Aplicaciones Especializadas		**154**	
	Gestor Documental.Falla Funcional	69	9,15%
	Gestor Documental.Falla radicacion	33	4,38%
	Gestor Documental.No permite Aprobar y radicar	18	2,39%
	Gestor Documental.Caida - Degradacion	8	1,06%
	Gestor Documental.No permite ingresar datos	8	1,06%
	Gestor Documental.Falla error - Producir documento	5	0,66%
	Gestor Documental.Lentitud gestor	4	0,53%
	Gestor Documental.Falla - Error PQRSD	3	0,40%
	Gestor Documental.Falla Error - Datacap	2	0,27%
	Gestor Documental.PDF en blanco	1	0,13%
	Gestor Documental.No se encuentra radicado	1	0,13%
	Gestor Documental.Falla al cargar archivos	1	0,13%
	Gestor Documental.No genera sticker	1	0,13%
Energía Eléctrica Regulada - UPS		**4**	
	Alarma Zabbix.UPS	4	0,53%
Herramientas de Gestión		**1**	
	Monitoreo Zabbix.Alarma desde Zabbix	1	0,13%
Redes y Conectividad		**407**	
	Alarma Zabbix.Router	225	29,84%
	Alarma Zabbix.Starlink	74	9,81%
	Alarma Zabbix.FortiGate	68	9,02%
	Alarma Zabbix.AP	25	3,32%
	Alarma Zabbix.Switch	12	1,59%
	Incidente Mayor	1	0,13%
	LAN.Falla Equipo Activo	1	0,13%
	Internet.Sin servicio	1	0,13%
Soporte Microinformatica		**165**	
	Falla impresora.Atasco	34	4,51%
	Equipo de computo.Falla - Error conexión a red	29	3,85%
	Falla impresora.No imprime	28	3,71%
	Aplicaciones Office 365.Envio y recepción de correos	14	1,86%
	Equipo de computo.Lentitud - Bloqueo	10	1,33%
	Equipo de computo.Falla - error	8	1,06%
	Equipo de computo.No enciende	5	0,66%
	Navegadores.Lentitud	3	0,40%
	Navegadores.Falla - Error	3	0,40%
	Ofimatica.Falla Excel	3	0,40%
	Escaner.Falla - error	3	0,40%
	One Drive.Error sincronizacion	3	0,40%
	VPN.Falla aplicación	3	0,40%
	Microsoft Teams.Intermitencia - Lentitud	2	0,27%
	Mouse - Teclado - Base - Diadema.Daño fisico	2	0,27%
	Ofimatica.Falla Aplicaciones Office 365	2	0,27%
	Mouse - Teclado - Base - Diadema.Falla General	2	0,27%
	Ofimatica.Falla Word	1	0,13%
	Equipo de computo.Falla de sistema operativo	1	0,13%
	Software Adicional.Falla de instalacion	1	0,13%
	Navegadores.Falla Cargue pagina web	1	0,13%
	Ofimatica.Falla PDF	1	0,13%
	Falla impresora.Impresión deficiente	1	0,13%
	Navegadores.Bloqueo Navegador	1	0,13%
	Ofimatica.Falla - Error	1	0,13%
	Falla impresora.Daño fisico	1	0,13%

	Falla impresora.No Escanea	1	0,13%
	Monitor Pc.Falla- Error	1	0,13%
Telefonía IP		**4**	
	Servicios.No ingresan llamadas	3	0,40%
	Servicios.Falla de codigo de llamadas nacional	1	0,13%
Total general		**754**	**100%**

Tabla 7 Categorización de Incidentes por Servicio

- **Top 10 de Incidentes**

El análisis de los incidentes evidencia que la mayor afectación del servicio se concentra en la infraestructura de red, particularmente en dispositivos como routers, firewalls, Starlink y puntos de acceso monitoreados por Zabbix, los cuales representan el 65,01% del total de incidentes registrados. Se destacan 225 incidentes (37,31%) asociados a routers, 74 incidentes (12,27%) relacionados con Starlink, 68 incidentes (11,28%) asociados a FortiGate y 25 incidentes (4,15%) correspondientes a AP.

Las principales causas identificadas corresponden a fallas eléctricas, seguidas por incidentes asociados a proveedores de conectividad, equipos apagados en sede y ventanas de mantenimiento, condiciones que generan indisponibilidad e intermitencia en los servicios de red, impactando directamente la operación de los usuarios.

Además, se observa que parte de los incidentes está relacionada con el comportamiento propio de las herramientas de monitoreo, como la generación de alertas múltiples o dependencias entre dispositivos, especialmente ante eventos de caída de enlaces o reinicios no controlados de la infraestructura tecnológica.

De manera complementaria, se identifican incidentes asociados a aplicaciones y equipos de usuario final, principalmente relacionados con procesos funcionales del Gestor Documental, fallas de impresión y errores de conectividad en estaciones de trabajo, los cuales presentan un impacto limitado frente a la afectación global del servicio.

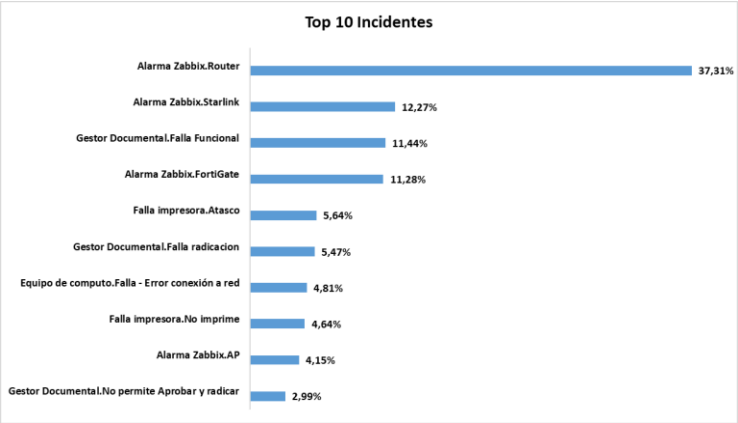


Ilustración 6 Top 10 Incidentes

Tipo de incidente	No	%	Observación
Alarma Zabbix.Router	225	37,31%	La mayor afectación corresponde a incidentes asociados a conectividad WAN y fallas en la red del proveedor de servicios, generando indisponibilidad e intermitencia en la comunicación de las sedes.
Alarma Zabbix.Starlink	74	12,27%	Se evidencian incidentes relacionados con fallas del proveedor de conectividad, intermitencia y lentitud en la red, así como desconexiones físicas de equipos y afectaciones ocasionadas por fallas de energía eléctrica en sede.
Gestor Documental.Falla Funcional	69	11,44%	Se presentan incidentes funcionales en el Gestor Documental
Alarma Zabbix.FortiGate	68	11,28%	Los eventos reportados corresponden principalmente a fallas en la conectividad del proveedor, afectando la disponibilidad y estabilidad de los servicios de seguridad y acceso a la red.
Falla impresora.Atasco	34	5,64%	Los incidentes registrados corresponden a atascos de papel
Gestor Documental.Falla radicación	33	5,47%	Se identifican fallas durante el proceso de radicación documental.
Equipo de cómputo.Falla - Error conexión a red	29	4,81%	Los usuarios reportan inconvenientes de conexión a la red corporativa, asociados a configuraciones de red.
Falla impresora.No imprime	28	4,64%	Los incidentes corresponden a fallas de impresión relacionadas con configuración, conectividad, controladores o estado operativo de los equipos.
Alarma Zabbix.AP	25	4,15%	Las alertas de puntos de acceso inalámbrico se asocian a desconexiones físicas, interrupciones eléctricas y fallas en la conectividad del proveedor de red.
Gestor Documental.No permite Aprobar y radicar	18	2,99%	Se presentan incidentes funcionales que impiden la aprobación y radicación de documentos.
Total general	**603**	**100,00%**	

Tabla 8 Top 10 Incidentes

- **Casos Suspendidos**

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

Grupo	Abril
NOC	6
Responsable_de_Energia Eléctrica Regulada - UPS	2
Especialista Redes	1
Responsable Garantías Equipos	1
Total general	**10**

Tabla 97 Incidentes Suspendidos

La principal causa de suspensión corresponde a dependencias externas con proveedores de conectividad y soporte de última milla, donde los casos permanecen en seguimiento mientras se reciben validaciones técnicas, RFO, restablecimiento de enlaces o atención por parte de terceros. Asimismo, se identificaron incidentes ocasionados por fallas eléctricas y picos de energía en sede, generando afectaciones en equipos UPS, dispositivos de red y tarjetas de comunicación.
Además, algunos casos fueron suspendidos debido a condiciones operativas en el sitio, como ausencia de funcionarios, equipos apagados o necesidad de coordinación para validaciones presenciales, lo que limita la continuidad inmediata de las actividades técnicas.

También se evidencian casos menores asociados a garantías y logística de entrega de equipos de usuario final, como dispositivos periféricos pendientes por transporte o reposición.
En términos generales, los casos suspendidos obedecen principalmente a factores externos, dependencias con terceros y condiciones de infraestructura en sede, manteniéndose bajo seguimiento y control operativo por parte de las áreas responsables hasta su normalización.

- **Incidentes Mayores**

Durante el mes de abril no se presentaron incidentes mayores que afectaran la continuidad de los servicios o la operación del cliente. Se mantuvo el monitoreo y seguimiento continuo sobre la infraestructura y los servicios críticos, garantizando la atención oportuna ante cualquier eventualidad identificada.

- **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 la Guía Operacional 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 abril
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=5528/5541*100 EF= 99,77%
Porcentaje de Incidentes Reabiertos en el Periodo	RRP: Porcentaje de casos Reabiertos en el periodo. IFS: Incidentes solucionadas en el período. IFR: Incidentes Reabiertos en el período.	<2%	Mensual	RRP= 1/5541*100 RRP= 0,02%

Tabla 10 Medición de KPIs

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

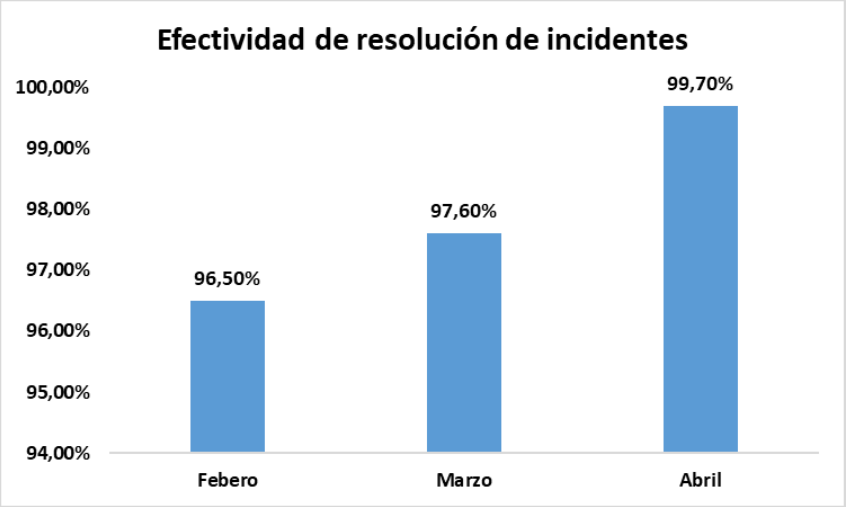


Ilustración 8 Efectividad de resolución de incidentes

Durante los últimos 3 meses, la efectividad en la resolución de incidentes se mantuvo por encima del indicador de cumplimiento del 80%, con los siguientes resultados:

- Febrero: 96,5%
- Marzo: 97,6%
- Abril: 99,7%

Para el mes de abril, la efectividad en la resolución de incidentes alcanzó un 99,7%, superando ampliamente el indicador de cumplimiento establecido del 80%. Este resultado evidencia una mejora significativa en la gestión operativa, el monitoreo proactivo y el seguimiento oportuno de los casos reportados.

El comportamiento del indicador refleja una mayor capacidad de atención y resolución de incidentes por parte de los equipos de soporte, permitiendo minimizar el impacto sobre la operación de los servicios tecnológicos y garantizar una mayor continuidad en la prestación del servicio. Asimismo, se evidencia un fortalecimiento en la gestión de incidentes asociados a infraestructura, conectividad y soporte a usuarios.

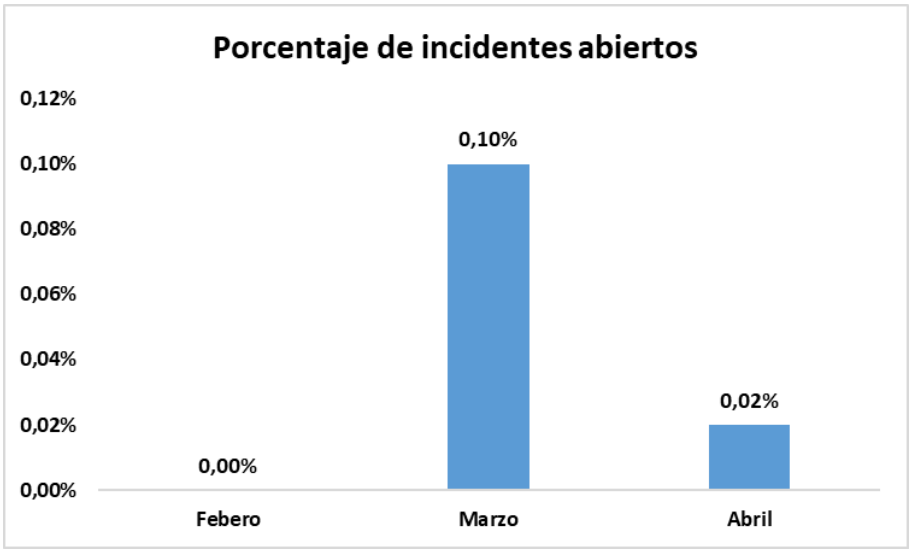


Ilustración 9 Porcentaje de incidentes abiertos

Durante el período evaluado, el indicador de incidentes reabiertos presentó un comportamiento estable y controlado, manteniéndose ampliamente por debajo de la meta definida del 2%. Este resultado evidencia la efectividad de los procesos de atención, diagnóstico y cierre implementados por el equipo de soporte, garantizando soluciones adecuadas desde la primera intervención y reduciendo la necesidad de reprocesos.

Los resultados obtenidos fueron los siguientes:

- Febrero: 0,00%
- Marzo: 0,10%
- Abril: 0,02%

El comportamiento observado demuestra una adecuada validación de las soluciones aplicadas antes del cierre de los casos, así como un seguimiento oportuno a los incidentes reportados por los usuarios. Aunque en marzo se presentó una variación mínima frente a los demás meses, esta se mantuvo dentro de niveles óptimos y no representó impacto significativo en la operación ni en el cumplimiento del indicador.
En términos generales, los resultados reflejan un alto nivel de calidad en la gestión del servicio, fortaleciendo la continuidad operativa y la satisfacción del cliente mediante la disminución de reincidencias y reaperturas de casos.

2.1.2.7. Práctica de Requerimientos

Dar a conocer las actividades de la Práctica de Requerimientos correspondientes al mes de abril 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 4878 casos tipo requerimiento quedando en los siguientes estados:

Estado	Casos
Cerrado	4311
Solucionado	471
Suspendido	59
En proceso	37

Tabla 11Estados de Requerimientos

- Durante el mes, se realizaron socializaciones de refuerzo de los flujos automatizados para la gestión de requerimientos de devolución de equipos para traslados en sede, cambio de equipos y Roles, con el fin de optimizar el control y seguimiento de las solicitudes, por lo tanto, se configuró la generación automática de tareas dentro de los requerimientos, permitiendo una mejor organización de las actividades y mayor trazabilidad en el proceso.

  Por lo anterior, se generaron 515 tareas, las cuales fueron gestionadas en los siguientes estados:

Estado	Task
Asignada	72
Finalizada	443

Tabla 12 Estados de Tareas de requerimientos

- Durante el mes, no se presentó casos en estado anulado.
- 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 marzo al periodo actual.

Grupo Responsable	Marzo	Abril
Especialista Redes	1	0
SOC	1	3
Especialista Aplicaciones.NET	1	0
Especialistas IBM	3	0
Responsable Garantías Equipos	8	12
Responsable_De_Servidores_Windows	2	2
Responsable_Mesa_de_Servicio	22	26
Responsable_Soporte_Bogotá	21	7
Responsable_Soporte_Impresoras	15	3
Gestor de Inventarios	0	1
Responsable_Soporte_Territoriales	10	3
Especialista Nube Publica	7	1
Total por Periodo	**91**	**59**

Tabla 13 Seguimiento del Backlog Suspendidos

En el inicio del período, se identificaron 126 casos suspendidos correspondientes al backlog del mes de marzo de 2026. Se realizaron seguimientos semanales de las solicitudes en estado abierto, logrando la solución de 32 casos a través de la herramienta de Gestión Aranda de los anteriores periodos de los servicios de MDS, Soporte en Sitio, Soporte Impresoras, IBM y Nube Publica. Para el cierre del mes, se encuentran pendientes 59 casos

en abril, los cuales se identificaron por: inactivación de usuarios, realización de Backup, cambio de contraseña, asignación de radicado, devolución de equipo, asignación de equipo, a espera de contactar al usuario, por garantía a espera de respuesta del proveedor.

- 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	618
Radicar una solicitud.Directorio activo.Inactivar usuario	436
Radicar una solicitud.Alarma Zabbix.Impresora	278
Radicar una solicitud.Impresora.Instalacion - Configuracion	227
Radicar una solicitud.Impresora.Aumento de cuota	195
Radicar una solicitud.Directorio activo.Cambiar contraseña	193
Radicar una solicitud.Gestor documental.Relanzamiento	168
Radicar una solicitud.Gestor documental.Asignar Radicado TYS	139
Radicar una solicitud.VPN.Instalacion y configuracion VPN	122
Radicar una solicitud.Equipo de computo.Traslado de Sede, Cambio Equipo o Rol	122

Tabla 14 Top 10 de Solicitudes

- De acuerdo con el TOP 10 de solicitudes, se evidencia que las categorías con mayores solicitudes son del servicio de Impresión con las categorías de cargué de papel en impresora con 618 tickets, inactivación de usuario 436 tickets y Alarma Zabbix Impresora por apagado de equipos o intermitencias eléctricas 278 ticktes.
- 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.

De acuerdo con la Guía Operacional de la Práctica de Requerimientos, se estableció 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 del Periodo
Porcentaje de efectividad en resolución de Requerimientos de servicio.	**EF=(RFS/RFR) *100**	80%	Mensual	**EF=** 4867/4878 *100
	EF: Efectividad en solución de Requerimientos.			
	RFS: Requerimientos solucionados que cumplen el ANS en el período.			**EF= 99,77%**
	RFR: Requerimientos registradas en el período.			

Nombre	Descripción / Fórmula	Meta	Periodicidad	Resultado del Periodo
Porcentaje de Requerimientos Reabiertos en el Periodo	**RRP:** Porcentaje de casos Reabiertos en el periodo.	<2%	Mensual	**RRP=** 4/4782*100
	RFR: Requerimientos Reabiertos en el período.			**RRP= 0,08%**
	RFS: Requerimientos solucionadas en el período.			

Tabla 15 Detalle de KIP Practica de Requerimientos

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

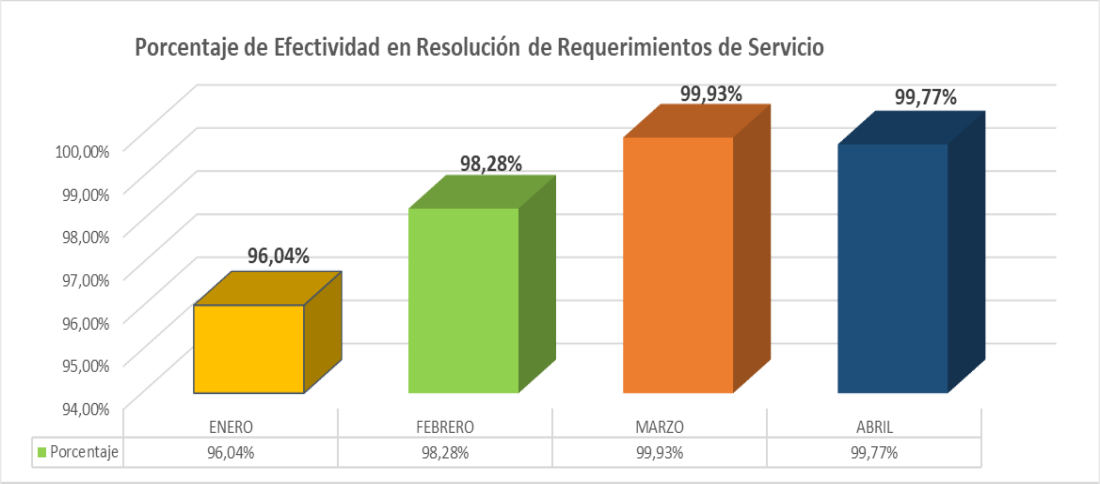


Ilustración 10 KPI Efectividad de Resolución de Requerimientos de Servicio

Durante el periodo evaluado, se evidencia el cumplimiento de la meta establecida para el mes de abril, alcanzando un porcentaje del 99,77%. Asimismo, se observa una disminución en la efectividad de las soluciones a comparación al periodo anterior del 0,16% con respecto al mes anterior. Para este mes, se presentó una disminución en el número de casos en estado suspendido y un mayor número de casos solucionados en comparación con el mes anterior.

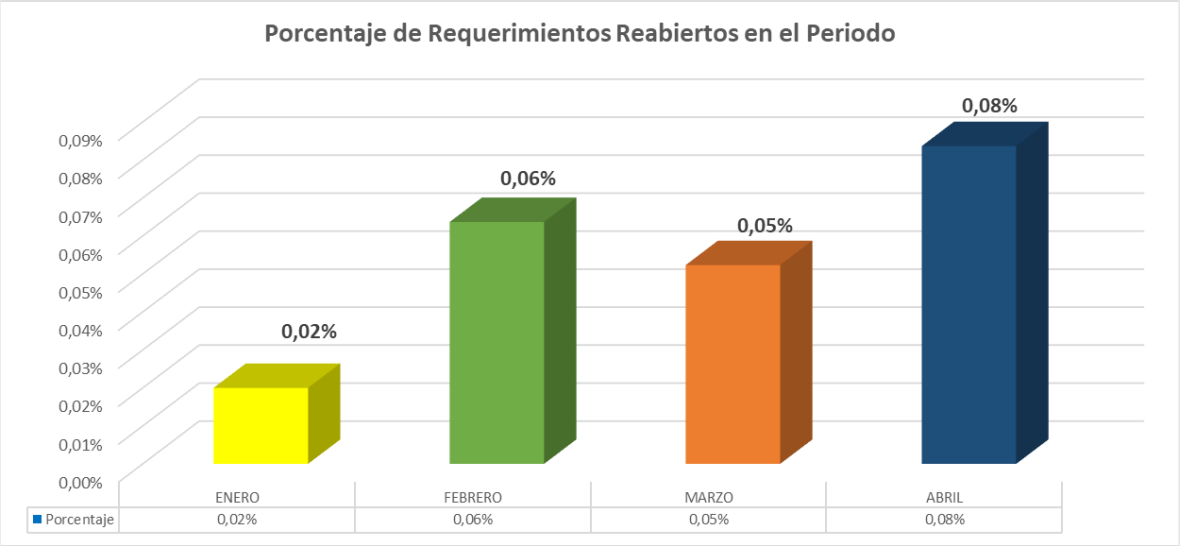


Ilustración 11 Requerimientos de Reabiertos en el periodo

Durante el periodo se realizó seguimiento a los requerimientos reabiertos por los usuarios, evidenciando este mes se presentó un aumento disminución frente al periodo anterior de 2026, lo cual se presentaron 4 casos con reapertura asociados requerimientos por; documentación no clara, errores de aplicación del estado y inconformidades por parte de los usuarios frente a la respuesta entregada por los especialistas, por lo tanto, desde la práctica se realizaron retroalimentaciones para fortalecer la atención al usuario y la calidad del registro de las soluciones.

Se relaciona 4 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-203158	Radicar una solicitud.Gestor documental.Asignar Radicado TYS	Especialistas IBM	Se solicita asignar radicados del Gestor Documental al perfil de jefe de asignación de radicados de ventanilla única, esto teniendo en cuenta que no me deja asignar estos radicados a los funcionarios de la Oficina Especial de Barrancabermeja.	Por parte del especialista, se indicó inicialmente que el requerimiento fue resuelto, señalando que la reasignación debía ser realizada por la jefe de Asignación, Laura Muñoz Angarita. Posteriormente, el equipo de Soporte en Sitio reabrió el caso, informando que el responsable es el jefe de la Oficina Bucaramanga, Carlos Andrés Cuadrado Mayoral. En consecuencia, se realizó una nueva revisión, aclarando que la reasignación debe ser gestionada por la jefe de Asignación, quien posteriormente remitirá el caso al jefe de la Oficina correspondiente.

RF-200418	Radicar una solicitud.Gestor documental. Solicitud depuración carpeta	Especialistas IBM	Se solicita la eliminación o anulación del radicado en Gestor Documental 04EE2026717300100000464 , ya que se encuentra duplicado.	Se realizó la revisión por parte del especialista, evidenciando que el caso fue abierto el 09/04/2026 con el fin de gestionar la eliminación correspondiente, para lo cual se generó el ticket respectivo. Como solución, se informó: “Se realizó la verificación correspondiente y se procedió con la terminación del radicado. Actualmente, no se encuentran tareas activas asociadas al mismo de la usuaria.” Con base en lo anterior, el caso fue marcado como solucionado. Sin embargo, la usuaria manifestó en la encuesta la siguiente observación: “La solicitud se realizó el 4 de febrero y fue resuelta el 10 de abril; considero que fue mucho tiempo para dar respuesta”, lo cual generó la reapertura del caso. Posteriormente, el especialista realizó una nueva revisión de los tickets eliminados, confirmando que no se evidencian duplicados y que la solución aplicada fue efectiva.
RF-204388	Radicar una solicitud.Impresora.Asesoria - Consulta	Responsable_ Soporte_Territoriales	La usuaria solicita asesoría sobre como configurar impresora RICOH-MOCOA para escanear de manera manual a dos caras.	El soporte en sitio atendió el caso y se asesoró a la usuaria para que pueda realizar los ajustes en el escáner de la multifuncional RICOH-MOCOA y escanear archivos manuales a doble cara y se le brinda paso a paso para la configuración, lo cual, la usuaria puede realizar el proceso y finalmente se soluciona el caso, pero al realizar la aplicación del estado, se generar un error y queda en estado reabierto, por tal motivo se soluciona el caso nuevamente.
RF-200237	Radicar una solicitud. Teléfono IP.Instalación - Configuracion	Responsable_Soporte_Territoriales	Se reporta que la línea telefónica no funciona y al intentar llamar aparece un círculo reiniciando.	Se realiza la gestión del caso, lo cual se confirma parte del especialista ya está funcionando, pero al confirmar el Soporte en Sitio y usuario la novedad persiste, lo cual se reabre el caso y el especialista revisa nuevamente indicando la siguiente respuesta: Se efectuaron las acciones necesarias para restablecer el servicio, quedando la línea telefónica funcionando con normalidad y se soluciona el caso.

Tabla 16 Casos reabiertos

2.1.2.8. Práctica de Eventos

La labor del equipo del Centro de Diagnóstico y Operaciones (CDO) permitió identificar y gestionar oportunamente un total de 403 incidentes, lo cual evidencia una alta capacidad operativa y de respuesta ante eventos críticos.

Los Routers fueron el componente con mayor incidencia, concentrándose 205 casos (50,87% del total). Esto está asociado a factores como la inestabilidad de la red eléctrica en zonas remotas o condiciones ambientales adversas. Se recomienda evaluar la continuidad del servicio con proveedores alternos o implementar mecanismos de respaldo más robustos.

Para este mes se evidencia una leve disminución en los casos reportados por antenas Starlink, los cuales se encuentran en el segundo lugar, representando 74 (18,36% del total) de los casos. Se evidencia que estas antenas son mayormente afectadas por temas eléctricos en las sedes, de igual forma una intervención humana con el apagado de los equipos.

Los dispositivos FortiGate presentaron una disminución en la cantidad de incidentes durante este mes, representando el 12,90% de los casos registrados (52 incidentes). Los eventos identificados estuvieron asociados principalmente a fallas en el suministro de energía comercial, apagado de equipos por parte de funcionarios e intermitencias en el servicio WAN en horarios no hábiles. Es importante resaltar que los equipos mantienen una operación estable y adecuada; sin embargo, las alertas generadas corresponden principalmente a factores externos de conectividad y energía. En los eventos presentados fuera del horario hábil no fue posible determinar la causa raíz.

Los servidores Windows Server ocuparon el cuarto lugar en la categorización de incidentes, con 32 casos registrados, equivalentes al 7,94% del total.
Los eventos reportados en servidores Windows estuvieron relacionados principalmente con alarmas informativas por consumo de memoria, disco y CPU las cuales son gestionadas por los especialistas quienes realizan acciones de depuración de procesamiento, detención de tareas programadas o cierre de sesiones que consumen recursos, una vez liberados los umbrales vuelven a los limites definidos. La atención de estos casos se muestra de forma detallada en la práctica de incidentes.

Por su parte, los incidentes relacionados con servidores Linux mantuvieron un comportamiento estable durante el periodo evaluado, sin impactos significativos sobre la continuidad de los servicios.

Los Access Points ocupan el 5to lugar con un 5,71% (23 casos) del total de los incidentes, cifra la cual es mayor en comparación con el mes anterior ya que en este aumento 11 casos.

Los dispositivos Switches reflejan una baja incidencia del 1,74% (7) del total de los casos, lo cual muestra para este mes un leve aumento en los casos a comparación de meses anteriores.

Este informe respalda el compromiso del equipo NOC en mantener la continuidad operativa de los servicios TI mediante una gestión proactiva, eficiente y orientada a la mejora continua.

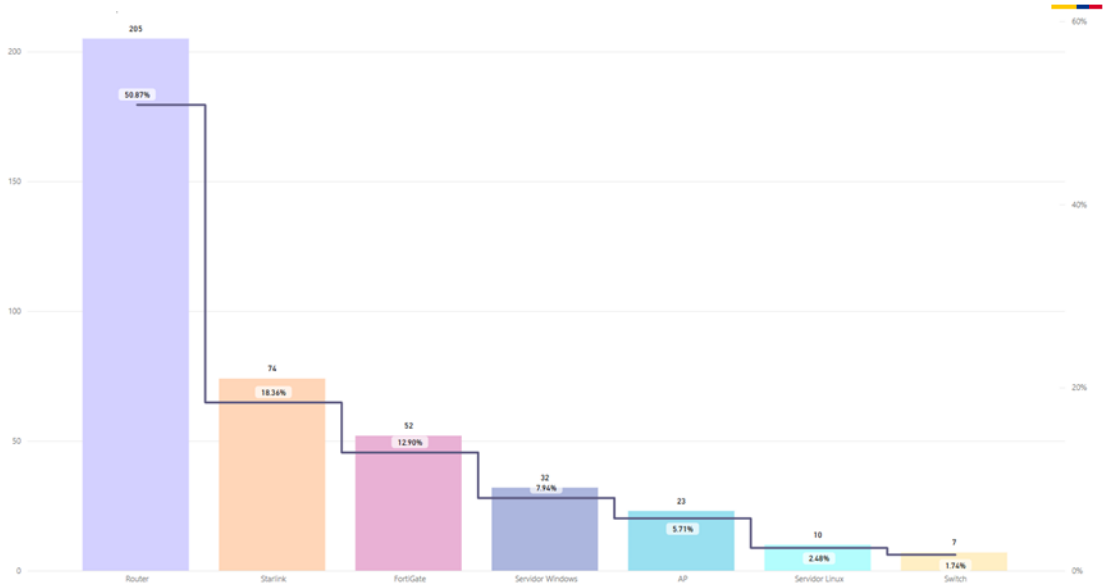


Ilustración 12 Resumen de incidentes

Redes y conectividad

- **Routers**

Desde el centro de operaciones NOC durante el mes de abril se gestionaron 205 incidentes relacionados con equipos de red Routers en diferentes sedes a nivel nacional, los cuales representaron el 50,87% de los casos.

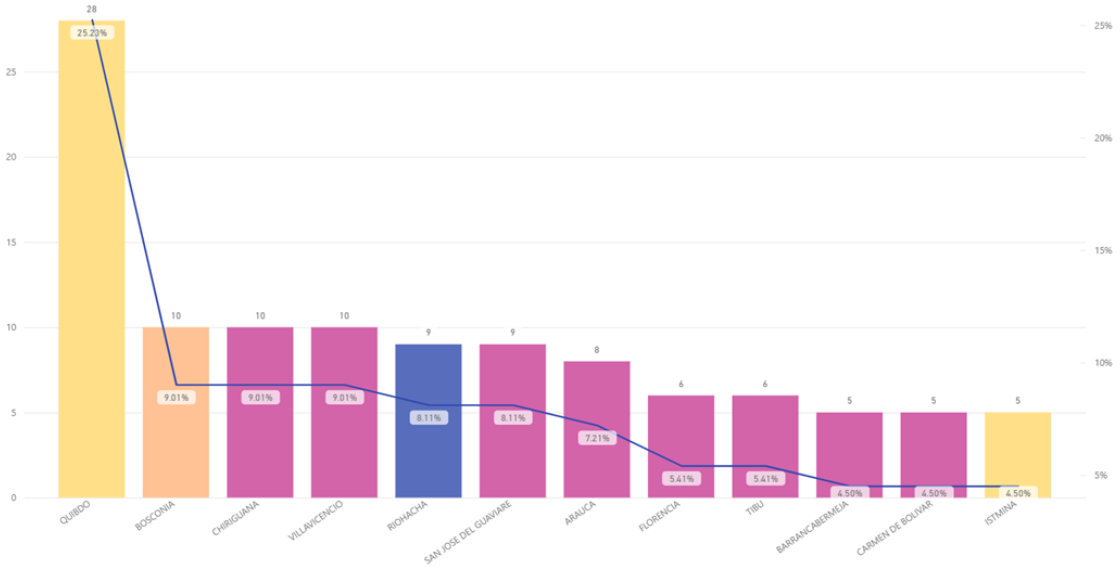


Ilustración 13 Sedes afectadas por router

- Para este mes se evidencia una alta cantidad de casos en la sede de Quibdó ocupando el primer lugar, reportando su principal causa por falla de energía eléctrica. En su gran mayoría esta sede reporta como fallas eléctricas en la sede o en la zona que afectan el servicio.

- Las sedes de Bosconia, Chiriguana y Villavicencio ocupan el 2 lugar ya que igualan con 10 casos cada una. Estas sedes reportan caídas en su mayoría por causa de falla energía eléctrica, desconexión/apagado físico de equipos en sede y falla en red de proveedor en la sede de Villavicencio.
- En 3er lugar encontramos a Riohacha y San José del Guaviare las cuales igualan en número de casos (10 casos) y el mayor porcentaje de incidencias son por fallas eléctricas y un mínimo por Falla en Red de Proveedor e Intermitencia/Lentitud en la red.
- En 4to lugar encontramos a Arauca, sede que presenta su mayor número de incidencias por falla energía eléctrica, seguido por falla en red de proveedor.
- Florencia y Tibú se ubican en 5to lugar igualando en cantidad de eventos (6) reportados, representando la mayoría de los eventos por causa de falla energía eléctrica.

- Carmen de Bolívar e Istmina se ubicaron en el sexto lugar, con 5 casos registrados cada una, la causa común de los incidentes correspondió a fallas en el servicio de energía eléctrica en las respectivas zonas.

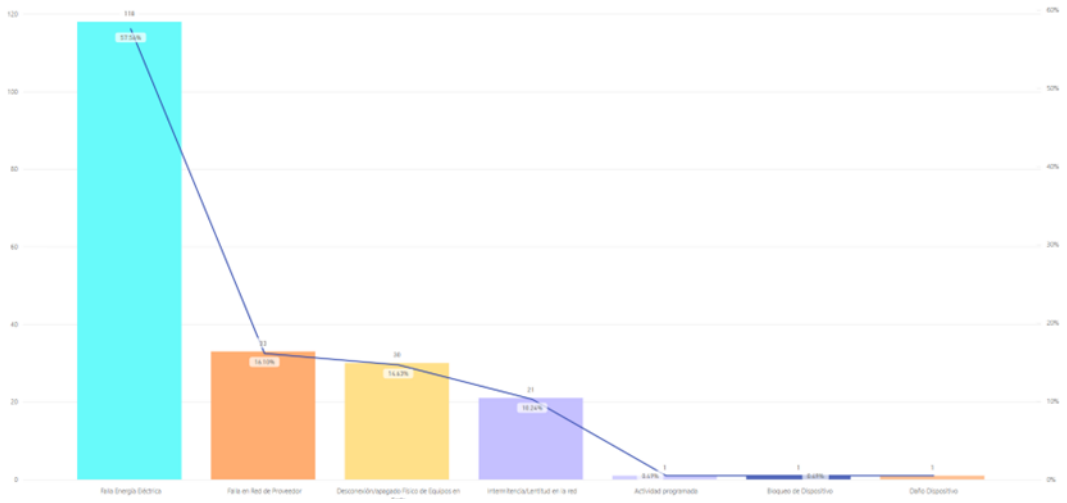


Ilustración 14 Causas de eventos generados por router

- Se evidencia que la causa principal del total de eventos para la categoría de Routers es por falla energía eléctrica ocupando el primer lugar con 118 casos (57,56%), seguido de Falla en red de proveedor con 33 casos (16,10%), en tercer lugar se evidencia desconexión/apagado físico de Equipos en Sede con 30 casos (14,63%), en cuarto lugar, se evidencia Intermitencia/Lentitud en la red con 21 casos (10,24%), por último y en quinto lugar se ubican las categorías actividad programada, bloqueo de dispositivo y daño dispositivo las cuales igualan con 1 caso cada una. A comparación de meses anteriores, se mantienen en un porcentaje bajo.
- Las fallas por energía eléctrica representan el 57,56% de los casos (118), afecta principalmente a zonas remotas o sin tecnología de respaldo como Quibdó, Bosconia, Riohacha, entre otras, donde la red eléctrica es inestable o está sujeta a

cortes constantes. En muchos casos, las sedes no cuentan con sistemas de respaldo energético (UPS, generadores o paneles solares y banco de baterías), lo que provoca apagones completos de la infraestructura de red. Recomendación crítica: Priorizar la implementación de UPS en sedes con alta recurrencia de fallas eléctricas para garantizar la continuidad del servicio y reducir alarmas innecesarias.

- El 16,10% (33) de los casos están relacionados a falla en red de proveedor, siendo Villavicencio y Quibdo las sedes con mayor número de eventos registrados por esta causa. Por esta causa registran 3 casos en estado suspendido y a espera de RFO por parte de ETB, dos de Quibdo y uno de San Jose, todos los demás están en estado cerrado o solucionado por distintas causas en la infraestructura de la red del proveedor.
- El 30% (14,63) de los casos están relacionados a desconexión apagado físico de equipos en sede, siendo Chiriguana y seguida por Bosconia, las sedes que registran mayor cantidad de eventos para esta categoría, los cuales son ocasionados porque los funcionarios apagan los equipos al salir de turno con el fin de prevenir la afectación de los dispositivos por picos altos en el servicio de energía.
- El 10,24% (21) de los casos están asociados a intermitencia/lentitud en la red, este tipo de incidencias se concentra en regiones con interrupciones del servicio de energía o en la red de datos de proveedor, sin embargo, estas se han registrado en su mayoría en horario no hábil y las cuales no han durado más de 20 a 30 minutos activas. Las sedes con mayor número de eventos por esta causa son Carmen de Bolivar y Riohacha.
- Por último, el 1,47% (1 caso cada una) de los casos es por bloqueo de dispositivo, actividad programada y daño de dispositivo que en conjunto suman este porcentaje.

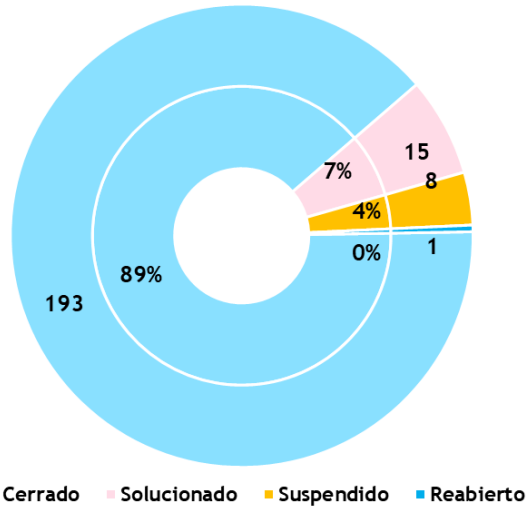


Ilustración 15 Casos suspendidos VS. Casos solucionados/Cerrados de Router

Se evidencia que del total de eventos generados (205) para la categoría de Routers durante el mes de abril; registran entre cerrados y solucionados representan el 98,05% (201), 4 casos en estado suspendido.

- Los casos suspendidos corresponden a sedes como

- San Marcos, relacionado al servicio principal donde se está a la espera que el funcionario retorne al punto.
- San Jose del Guaviare, relacionado al servicio principal y está a la espera de RFO por parte de ETB.
- Fundacion, relacionado al servicio principal y está a la espera de RFO por parte de ETB.
- Quibdo, relacionado al canal de internet y está a la espera de RFO por parte de ETB.

- **Switches**

Desde el Centro de Operaciones (NOC), durante el mes de abril se generaron 7 casos referentes a Switches en la herramienta de monitoreo Zabbix en diferentes sedes, los cuales representan el 1,74% del total de los casos, donde se evidencia un leve aumento de casos en comparación con el mes pasado.

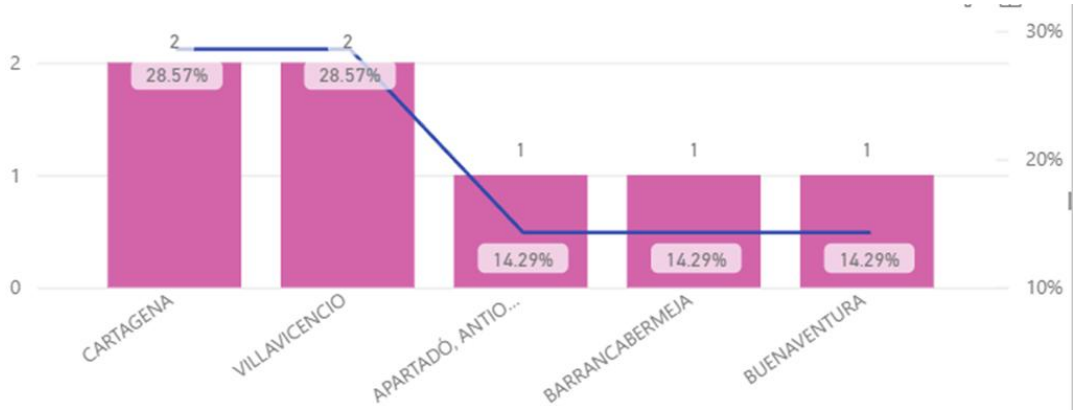


Ilustración 16 *Sedes afectadas por Switch*

De los 7 eventos registrados para la categoría de Switches en el mes de abril, los 7 registran en estado cerrado, cumpliendo de esta manera el 100% de los casos gestionados por parte del centro de operaciones NOC.

- **Access Point**

Desde el Centro de Operaciones (NOC), durante el mes de abril se gestionaron 23 incidentes asociados a equipos de red WLAN – Access Point en distintas sedes a nivel nacional, los cuales representan el 5.7% del total de casos reportados. Estos eventos fueron abordados dentro de los niveles de servicio establecidos, sin afectación crítica a la operación general de la red.

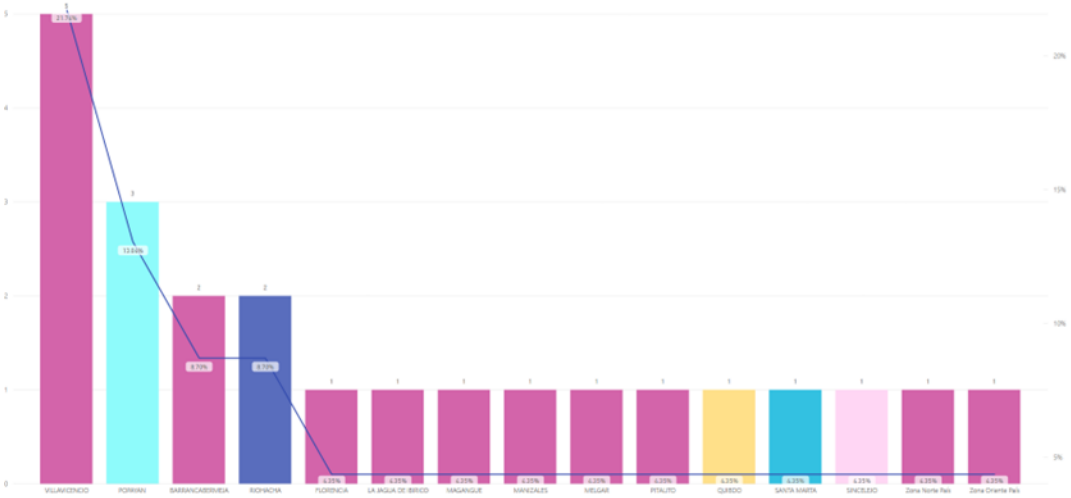


Ilustración 17 Top 9 Sedes afectadas por Access Point

Para este mes ser observa un aumento de casi el doble de casos a comparación del mes anterior, sin embargo, se evidencia de igual forma que la causa por falla eléctrica también subió de forma considerable, posicionándose en el TOP 1 en las causas.

Las sedes mas afectadas por estas fallas son Villavicencio, que presento múltiples intermitencias eléctricas un lapso de tiempo corto, seguido de Popayán con 3 casos, Barrancabermeja y Riohacha, sedes que también representan una alta incidencia por temas eléctricos.

A pesar de que solo tienen un 1 y una representación del 4% cada una, sedes como Florencia, La Jagua, Magangué y Manizales, también reportan fallas eléctricas en sus AP. Sedes como Melgar, Pitalito, Quibdo y Sincelejo presentan incidentes variados relacionados a desconexión de equipos e intermitencias.

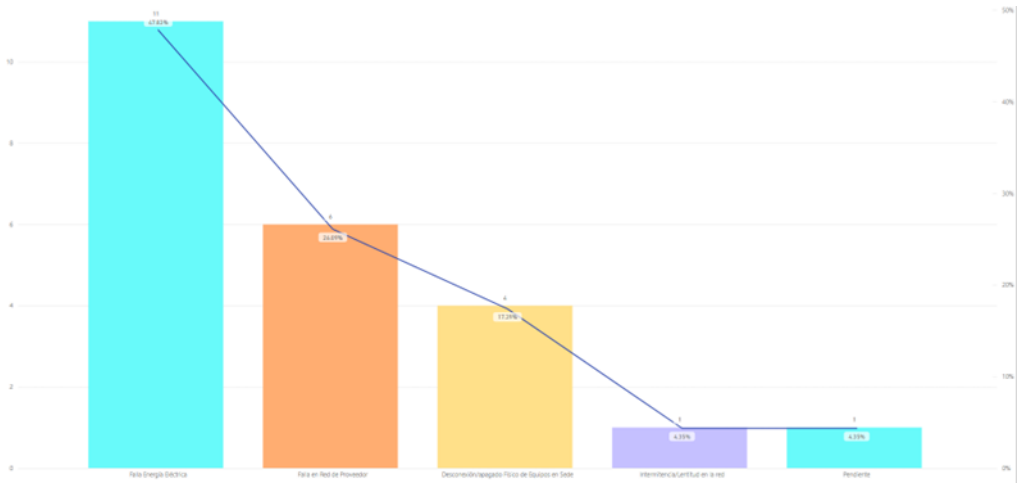


Ilustración 18 Causa de eventos generados por AP

El 52% de los incidentes en APs se relacionan a fallas eléctricas, especialmente por una sede que se alarmo repetidamente en un lapso muy corto. Sin embargo, a pesar de omitir esta sede, la cifra continúa siendo alta.
A pesar de que el número de incidencias es realmente bajo, con 6 casos y una representación del 26%, fallas en proveedor se presenta en el TOP 3, siendo la sede de Villavicencio la más afectada, seguida solo de Quibdo.

Para finalizar este TOP encontramos intermitencias o lentitudes relacionada a solo la sede Melgar, la cual no duro mas de 15 minutos, razón por la cual no se conoce una causa real que pudiese confirmar el motivo real de la falla.

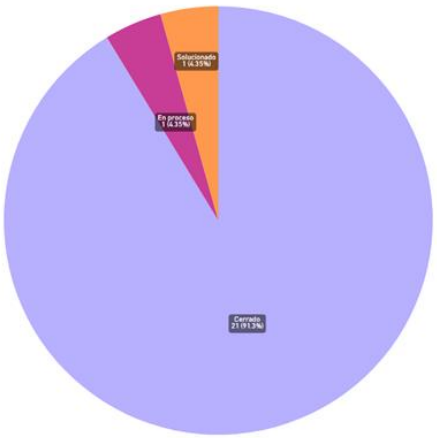


Ilustración 19 Casos suspendidos VS. Casos solucionados de AP

Según lo registrado de los 23 eventos generados por Access Point durante el mes de abril con relación a los casos suspendidos VS. Casos cerrados, se evidencian los 21 casos en estado cerrado, representando el 91% de gestión de casos, por otro lado, contamos con 2 casos aun en gestión para esta categoría.

- **Starlink**

Desde el centro de operaciones NOC durante el mes de abril se gestionaron 74 incidentes relacionados con equipos de red Starlink en diferentes sedes a nivel nacional, los cuales representan el 18% del total de los casos.

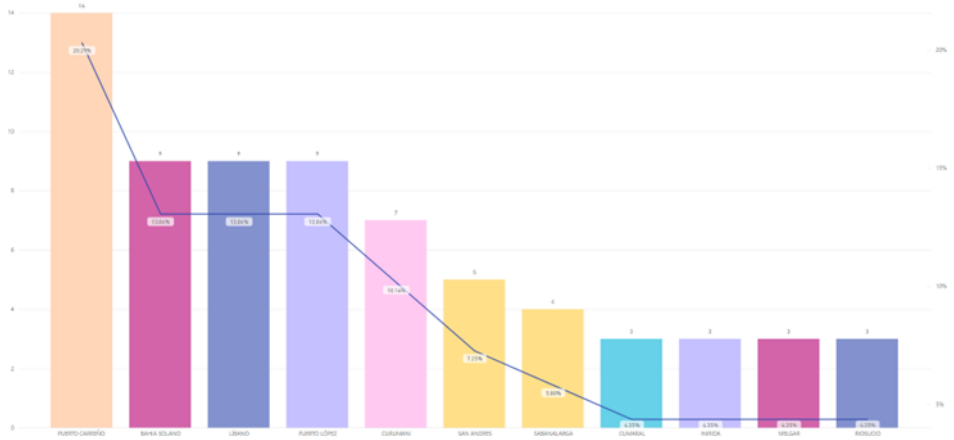


Ilustración 20 Top 10 Sedes afectadas por Starlink

Para el mes de abril el TOP 10 de las sedes con mayor número de eventos generados para la categoría de Starlink fueron Puerto Carreño con 14 eventos, la cual se mantiene en el TOP 1 por varios meses, siendo la sede en la que más se evidencian diferentes fallas eléctricas con un 57%, ya sea por tormentas, mantenimientos o incluso por la misma infraestructura de la sede, a pesar de que también se evidencian otro tipo de fallas, estas se dividen en concentraciones más bajas.

Bahia Solano, Puerto López y Libano con 9 eventos cada una, representando un 13% cada una, en estas sedes también se observan múltiples caídas eléctricas, e intermitencias, pero estas últimas en una menor medida. Las fallas eléctricas son la principal causa de indisponibilidad a nivel de red en las regionales.

Curumani en tercera posición con 7 casos y un peso del 10% en el TOP, es la única sede que no reporta fallas eléctricas, sin embargo, la desconexión de equipos abarca el 100% de los casos, debido a que los funcionarios apagan los dispositivos al finalizar su jornada laboral.

San Andrés con 5 eventos y un peso de 7%, junto con Sabanalarga con 5 eventos representando 5%, reportan por partes iguales novedades a nivel eléctrico y de desconexión física.
Finalizando el TOP encontramos ciudades como Cumaral, Inirida, Melgar y Riosucio, las cuales reportan 3 casos cada una con un peso del 4% de forma individual, también presentan una alta incidencia a fallas a nivel eléctrico, seguido de desconexiones físicas en el caso.

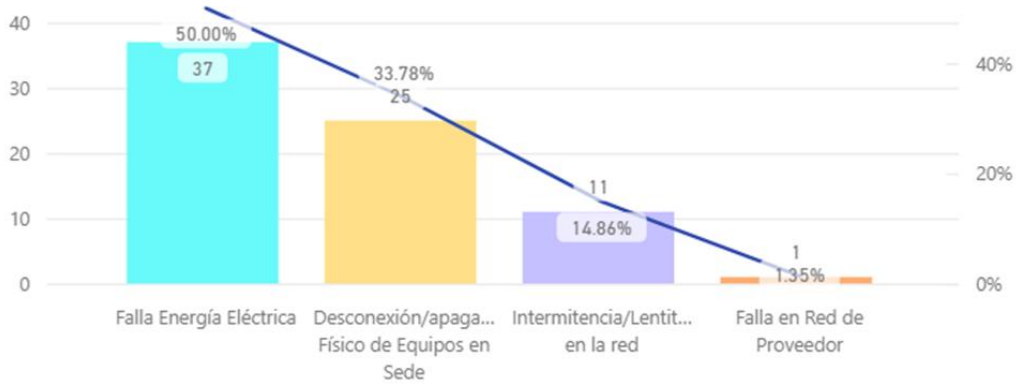


Ilustración 21 Causas de eventos generados por Starlink

Las fallas relacionadas a energía eléctrica sigue siendo la causa número uno en el TOP, para este mes representa un 50% de los casos relacionados al CI Starlink, se ha evidenciado que las zonas más remotas del país son las más afectadas, ya sean por tormentas, lluvias, mantenimientos, daños de terceros, racionamiento o hasta por falta de pago; siendo la sede Puerto Carreño la más afectada en el día a día, esta sede en los últimos meses ha ocupado el TOP 1, Bahía Solano, Líbano y Puerto López, a pesar de que varían en la posición, han estado presente en el TOP 10 el último año. por esta razón, consideramos importante que se contemple la posibilidad de sistemas de respaldo en estas sedes.
La desconexión de equipos de manera física para este mes muestra una disminución de casos, sin embargo, sigue ocupando la posición 2 en el TOP, con una representación del 33%, correspondiente a 33 eventos. A pesar de que es una práctica conocida entre los funcionarios la desconexión de los dispositivos no siempre es recomendable, razón por la cual se recomienda la opción de estabilizadores en las sedes, con el objetivo de evitar picos de voltaje y evitar eventos.

En el TOP 3, la causa de intermitencias o lentitudes, a pesar de que han disminuido, esta causa sigue representado un 14% del total, con 11 casos, siendo las sedes de Puerto Carreño, Bahía Solano, San Andrés y Cumaral las sedes más afectadas, con alarmas no superiores a 30 minutos y mínimo de 15 minutos.
Al final del TOP, en la posición 4, encontramos fallas de proveedor, siendo Curumani la sede afectada. Su presentación es menor con un 1% equivalente a 1 caso.

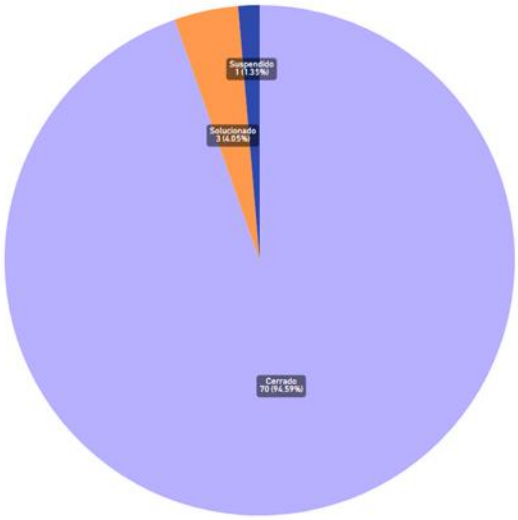


Ilustración 22 Casos suspendidos VS. Casos solucionados de Starlink

Según lo registrado se evidencia que los casos suspendidos VS. casos solucionados o cerrados del total de los 74 eventos registrados para la categoría Starlink durante el mes de abril, se reportan que el 98% de los casos fueron solucionados y el 1% (1 caso) se encuentra pendiente en estado suspendido, ya que la falla fue escalada al proveedor de las antenas y aún estamos a la espera de respuesta.

- **FortiGate**

Desde el centro de operaciones NOC durante el mes de abril se gestionaron 52 incidentes relacionados con equipos de red FortiGate en diferentes sedes a nivel nacional, los cuales representaron el 12.90% del total de los casos, ocupando el tercer lugar.

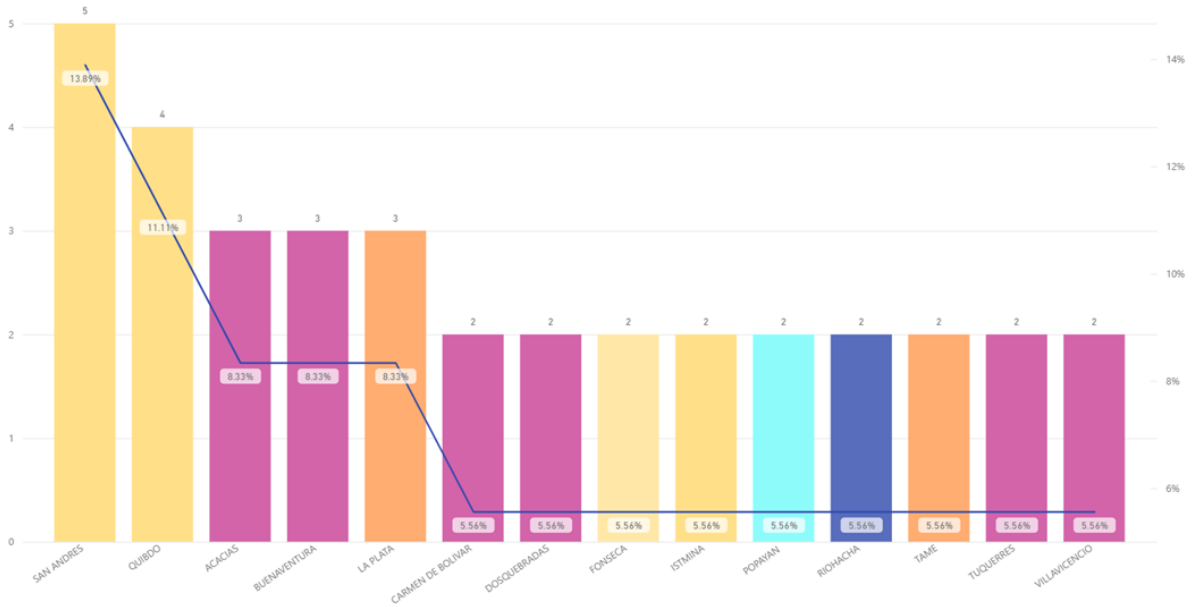


Ilustración 23 Top 5 Sedes afectadas por FortiGate

En comparación con el mes anterior, la categoría de FortiGate subió en la cantidad de casos en 7 puntos; se observa en el TOP 10 que 11 sedes reportan con 2 casos en promedio y 5 casos como máximo. Siendo la sede San Andrés la que ocupa la posición 1, con 5 casos representando el 13%; Quibdó es la segunda sede con más casos reportados, representando el 11.11% (4 casos). Se observa que el 77.78% de los eventos reportados están atribuidos a fallas con energía eléctrica, fallas que podrían mitigarse con la instalación de sistemas de respaldo.

Dentro del promedio con 3 casos, encontramos Acacias, Buenaventura y La Plata, las cuales representan un 8.33% cada una. Para este grupo de sedes, también se observa que las fallas eléctricas interrumpen la operación de las sedes, representando un 55.56%, sin embargo, la desconexión de equipos con un 44% también esta presente, siendo este último un tipo de actividad controlada por el funcionario en sede.

Al final del TOP 10, encontramos con 2 casos las sedes de Carmen de Bolivar, Dosquebradas, Fonseca, Istmina, Popayán, Riohacha, Tame, Tuquerres y Villavicencio, representando un 5.56% cada una. Para este grupo se sedes, se observan igualmente fallas eléctricas que afectan la operación, con 44% de los casos, seguido de desconexión de equipos, actividad realizada por funcionarios, representando un 27% y también relevante intermitencias y lentitudes con un peso del 16%.

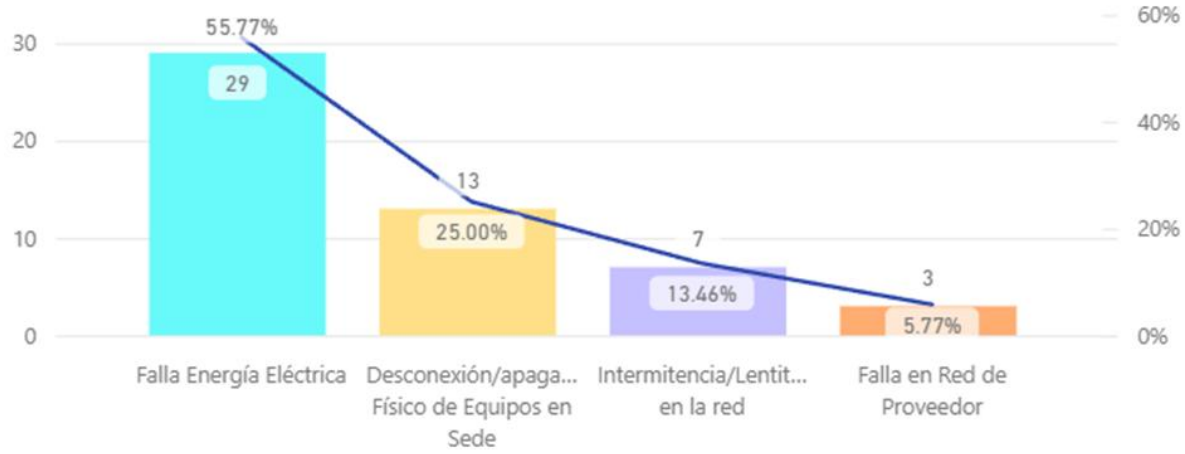


Ilustración 24 Causas de eventos generados por FortiGate

Durante el mes de abril, los dispositivos SD-WAN presentaron una tasa alta en cuanto a la causa de fallas en energía eléctrica, representando más de la mitad de los casos con un 55.77%; desconexión o apagado de equipos para este mes disminuyo caso a la mitad con 13 eventos registrados, representados con el 25% del total de los casos para esta categoría, los funcionarios en sede, se manera manual realizan la desconexión de los dispositivos, con el fin de evitar, según ellos, fallas en el servicio o daños en los equipos por picos de energía que se puedan presentar durante el horario no hábil; intermitencia y/o lentitud continua estable con una baja incidencia con 7 casos, representando un 13%.

Por otro lado, la causa de falla en red de proveedor se mantiene estable y relativamente baja en comparación con meses anteriores, con 3 casos lo cual representa solo el 5% de las fallas, es importante resaltar que esta disminución se debe a los ajustes que se han realizado con los reportes de Zabbix junto con Aranda.



Ilustración 25 Casos suspendidos VS. Casos solucionados de FortiGate

De los 52 eventos reportados en el mes, se evidencia que 51 casos se encuentran en estado cerrado representando el 98%, mientras que con 1.9% encontramos un caso suspendido debido a que el funcionario encargado de la sede Dosquebradas se encuentra de vacaciones y no es posible para soporte en sitio validar el estado del servicio, por lo tanto el NOC no tiene alcance de gestión hasta junio que retorna el funcionario.

Casos Escalados a Proveedor de Telecomunicaciones

Durante el mes de abril se registraron 27 casos que fueron escalados y gestionados con proveedor de telecomunicaciones de los cuales quedan 23 (85%) que registran en estado solucionado o cerrado y 4 (15%) en estado suspendido, en proceso o en espera de RFO.

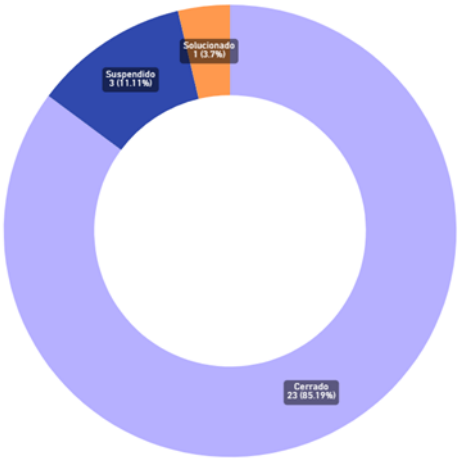


Ilustración 26 Estado de casos escalados a Proveedor

- El caso en Aranda IM-204467 se relaciona al servicio Router_Puerto_Berrio, el cual está escalado a UM, quien se encuentra realizando el diagnóstico de la falla.
- El caso en Aranda IM-204692 se relaciona al servicio RInternet_ETB_Quibdo, el cual está a la espera del RFO para cierre.
- El caso en Aranda IM-204829 se relaciona al servicio Router_San_Jose_del_Guaviare, el cual está a la espera del RFO para cierre.
- El caso en Aranda IM-204944 se relaciona al servicio Router_Fundacion, el cual está a la espera del RFO para cierre.

Servicios centrales

Servidores Windows

Durante abril, el Centro de Operaciones de Red (NOC) gestionó 32 incidentes asociados a servidores Windows, equivalentes al 7% del total de casos registrados durante el mes.

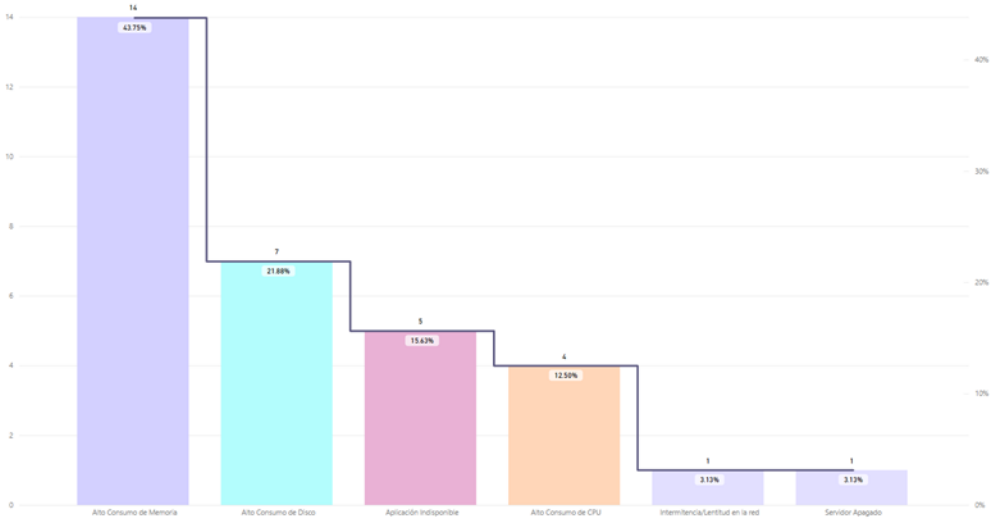


Ilustración 27 Causas de alarmas Servidores Windows

Se evidencia que para el mes de abril la causa principal y con mayor número de eventos es por alto consumo de memoria con 14 eventos registrados y representando el 43%, a pesar de que la cantidad de eventos bajo en comparación con el mes anterior, esta causa sigue siendo el top 1; seguido encontramos alto consumo en disco con 7 casos, representando el 21%, esta causa a comparación del mes anterior aumento su número de incidencias para abril; seguido encontramos 4 eventos que representan el 15%, donde los 5 eventos se relacionan a la Disponibilidad SFT (tolerancia a fallos de software), el cual ha estado presente en los reportes del último año; seguido encontramos consumo de CPU que para este mes presenta una baja incidencia con 4 casos y un peso del 12%; para este mes también observamos que con 1 evento, se reporta que el MINTRAB03 presento fallas a nivel de red, de igual forma se presenta 1 evento de apagado con el servidor MINTRABSQLQA1.

Es recomendable la revisión de las aplicaciones que se están viendo afectadas. Por lo tanto, enfocar las acciones correctivas en las causas principales permitirá lograr una reducción significativa en la ocurrencia de incidentes y un mejoramiento clave en la estabilidad operativa del sistema, de igual forma, se recomienda dejar en estado mantenimiento los servidores que tengan actividades programadas con el fin de evitar alertamientos.

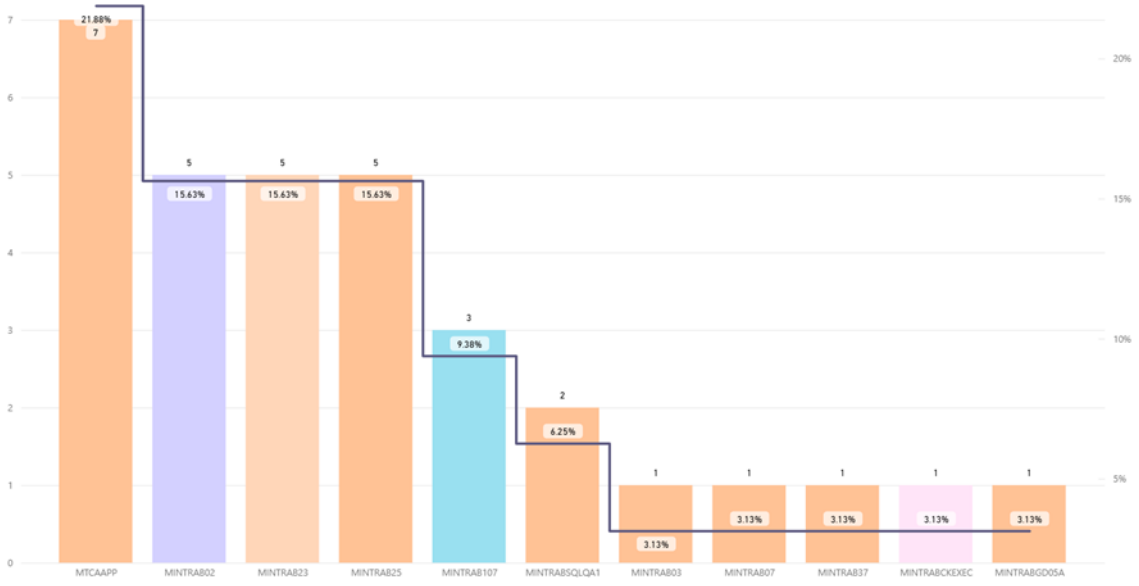


Ilustración 28 TOP 10 de servidores Windows con mas alarmas

El servidor MTCAAPP (7 casos) representa el 21% de los eventos reportados, siendo el primer mes que este servidor se encuentra en el top 1, en las causas se evidencian múltiples reportes de memoria y consumos de CPU; MINTRAB02 y MINTRAB23 con 5 casos cada uno, para este mes representan el 15% c/u, observando altos consumos en memoria para ambos casos y 1 evento de consumo de CPU para MINTRAB23, este último presenta en el 90% de sus casos indisponibilidad con SFT; por otro lado tenemos servidores con poca presencial en casos como MINTRABSQLQA1, MINTRABGD05A, MINTRABCKEXEC y MINTRAB37, los cuales reportan diversos tipos de causas, como consumo en disco, CPU, memoria, entre otras.

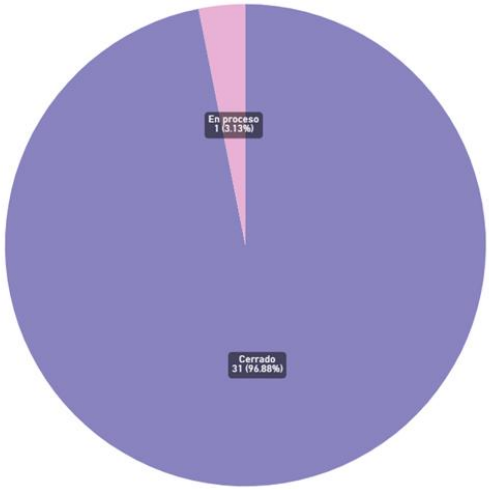


Ilustración 29 Casos suspendidos VS. Solucionados o cerrados Servidores Windows

Se evidencia que de los 32 eventos registrados durante el mes de abril, 31 estan en estado cerrado y solucionado, mientras que 1 caso, se encuentra en estado en proceso relacionado al servidor MINTRAB02, y categorizado como alto consumo de memoria, sin embargo, este caso no tiene documentación por parte del especialista.

- **Servidores Linux**

Durante abril se presentaron 10 casos a servidores Linux, los cual es una cifra muy alta a comparación de los últimos 4 meses, donde esta categoria solo presentaba máximo 3 casos.

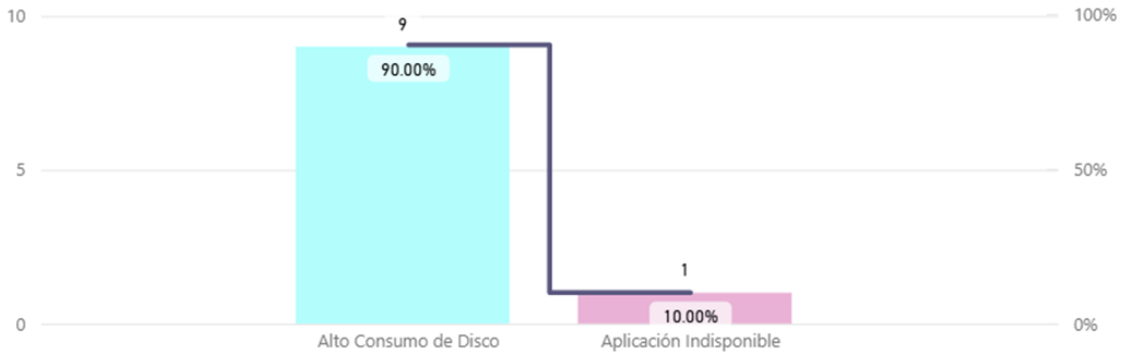


Ilustración 30 Causas de alarmas Servidores Linux

En abril se observa que el 90% de los casos pertenecen a consumo de disco duro en solo 2 servidores MINTRAB60 y MINTRAB32, lo cual corresponde a un incremento en procesamiento, por otro lado se presenta 1 alerta relacionada con el servidor de Zabbix.

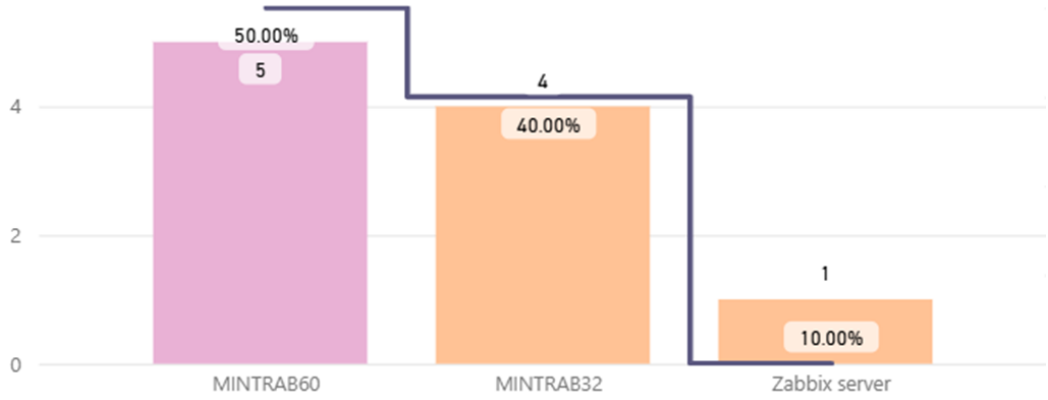


Ilustración 31 TOP 10 de servidores Linux con mas alarmas

Para este mes se evidencia que el consumo de disco estuvo muy presente en los servidores Linux MINTRAB60 y MINTRAB32, representando el 90% de los casos (9 de 10 casos), donde el primer servidor reporta 5 eventos, mientras que el segundo reporta 4; Zabbix server presento novedad, representando el 10% de los casos.

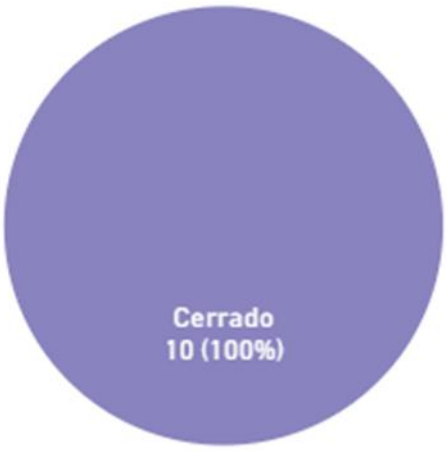


Ilustración 32 Casos suspendidos VS. Solucionados o cerrados Servidores Linux

Se evidencia que los 10 (100%) casos reportados para abril, todos fueron cerrados y documentados de forma correcta, por lo general los casos de esta categoría, se gestionan con celeridad.

- **Graficas de CPU zabbix de todo el mes sobre servidores**

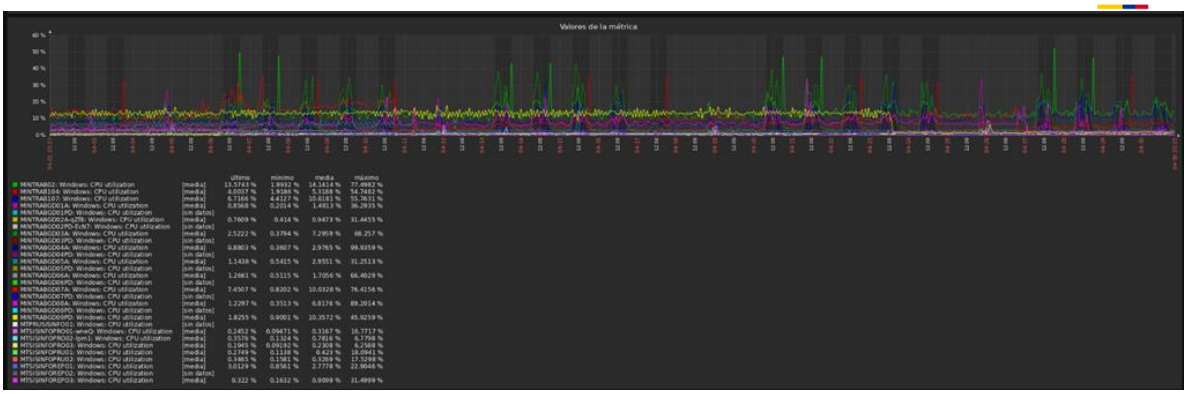


Ilustración 33 Grafica CPU

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. MINTRAB02 14.1414%
2. MINTRAB107 10.6181%
3. MINTRABGD09PD 10.3572%
4. MINTRABGD07A 10.0328%
5. MINTRABGD03A 7.2959%

- **Grafica de MEMORIA zabbix de todo el mes sobre servidores**

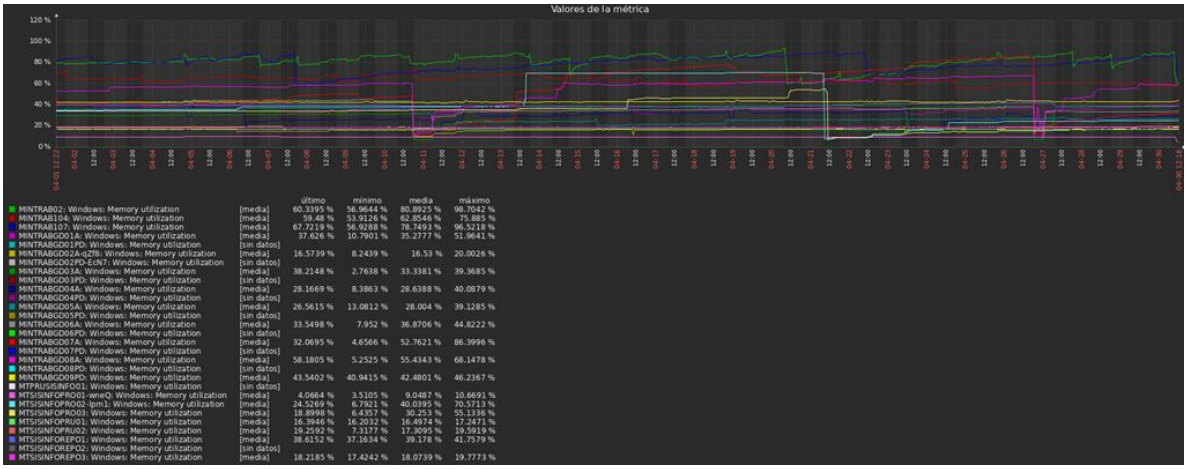


Ilustración 34 Grafica memoria

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

- **MEMORIA**

1. MINTRAB02 80.8925%
2. MINTRAB107 78.7493%
3. MINTRAB104 62.8546%
4. MINTRABGD08A 55.4343%
5. MINTRABGD07A 52.7621%

- **Datacenter (Cali - Bogotá)**

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

- **Indicadores (KPI) Efectividad de la Gestión de eventos**

Nombre	Descripción / Fórmula	Meta	Periodicidad	Resultado
Efectividad de la Gestión de eventos	ECE: (CEA/ CEC) *100 ECE: Porcentaje de eficacia de los tickets generados por alarmas CEC: Cantidad de tickets creados por alarmas en el periodo. CEA: Cantidad de tickets solucionados por alarmas en el periodo	80%	Mensual	ECE= (396/403) *100 EF= 98,26%

Tabla 17 KPI Práctica de Eventos

Durante el período evaluado, el indicador de Efectividad de la Gestión de Eventos presentó un resultado de 98,26%, superando ampliamente la meta establecida del 80%. Este resultado evidencia una gestión eficiente y oportuna de los eventos generados a partir de alarmas monitoreadas en la plataforma.

En total, se registraron 403 tickets creados por alarmas, de los cuales 396 fueron solucionados dentro del período, demostrando una alta capacidad de atención, seguimiento y cierre efectivo por parte del equipo operativo.
El cumplimiento alcanzado refleja un monitoreo continuo, una adecuada priorización de incidentes y una respuesta ágil ante las alertas detectadas, contribuyendo a minimizar afectaciones en la operación y garantizar la estabilidad de los servicios soportados.

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 30 de abril de 2026.

Servidores

Cantidad de dispositivos	Disponibilidad consolidada
122	100%

Tabla 18 Consolidado disponibilidad de servidores

Directorio Activo

Cantidad de dispositivos	Disponibilidad consolidada
3	100,00%

Tabla 19 Consolidado disponibilidad de Directorio Activo

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

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

Tabla 20 Desagregado de Disponibilidad Directorio Activo

Datacenter Principal

Cantidad de dispositivos	Disponibilidad consolidada
8	100,00%

Tabla 21 Consolidado disponibilidad de equipos Datacenter principal

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

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

Tabla 22 Desagregado de Disponibilidad Datacenter Principal

Datacenter Alterno

Cantidad de dispositivos	Disponibilidad consolidada
4	100%

Tabla 23 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 24 Desagregado Disponibilidad de equipos Datacenter alterno

Redes y conectividad

Cantidad de dispositivos	Disponibilidad consolidada
487	98,72%

Tabla 25 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	99,99%

Tabla 26 Consolidado disponibilidad de equipos de seguridad

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

Equipo	Disponible
MINTRABSUPERVISOR	99,93%
MINTRABVULNE01	100,00%
SOC_Fortianalyzer	100,00%
SOC_FortiDDOS	100,00%
SOC_SandBox	100,00%
SOC_WAF	100,00%
SDWAN-FG600F-SCENTRAL	99,99%
FGT-2200-ColombiaXV	100,00%

Tabla 27 Disponibilidad de equipos Seguridad de la Información

Telefonía

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

Tabla 28 Consolidado disponibilidad de equipos de telefonía

Antivirus

Cantidad de dispositivos	Disponibilidad consolidada
1	100%

Tabla 29 Consolidado disponibilidad de plataforma antivirus

Actividades de la Practica de Disponibilidad:

- Seguimiento a los resultados de los cambios presentados en el CAB por partes de especialistas que afecten la disponibilidad del servicio.
- Durante el periodo, se realizó seguimiento a los resultados de las pruebas de disponibilidad de los canales de conmutación de sede Chiquinquirá RFC-199435 y RFC-202881 Pruebas de Alta disponibilidad LAN, las cuales fueron exitosas y sin novedades.
- Se realizó seguimiento y revisión de la documentación y cronograma de las pruebas del DRP con los servicios infraestructura y redes.
- Actualización del tablero de Power BI de los % de disponibilidad de operación del consolidado del 2026.

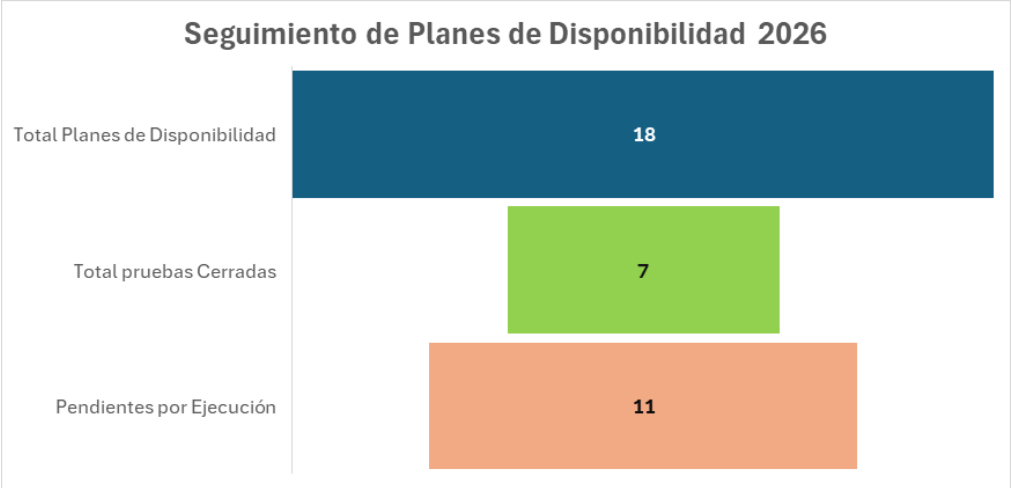


Ilustración 35 Seguimiento de Pruebas de Disponibilidad 2026

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 30 de abril de 2026.

Actividades en curso:

- Revisión de los cambios (RFC) ejecutados durante el periodo, para los cuales (23) cambios fueron aprobados su cierre, ya que cuentan con las evidencias completas de los planes de Pruebas Previas y Posteriores, al corte del 30/04/2026 se encuentra (5) casos abiertos (en implementación) a la espera de entrega de las evidencias por parte los especialistas.

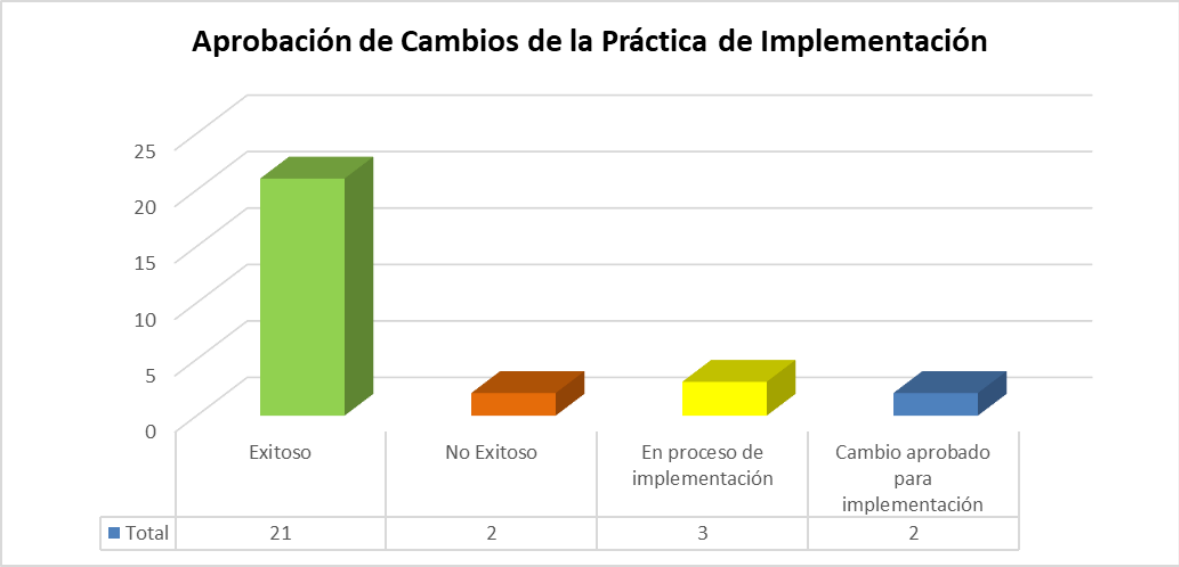


Ilustración 36 Seguimiento Práctica Implementación

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

2.2 Mesa de Servicios y Soporte en Sitio

A continuación, se presenta la gestión desarrollada durante el mes de abril 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 abril a la MDS ingresaron 321 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 No Atendidas umbral	Abandonadas	No Atendidas
COL - Mintrabajo-equipo compu	211	211	207	0	0	0
COL - Mintrabajo-Gestor-documental	69	69	66	0	0	0
COL - Mintrabajo-office365	28	28	28	0	0	0
COL - mintrabajo-Impresora	13	12	12	0	1	0
TOTAL	321	320	313	0	1	0

Tabla 30 Llamadas Atendida por la Mesa de Servicio

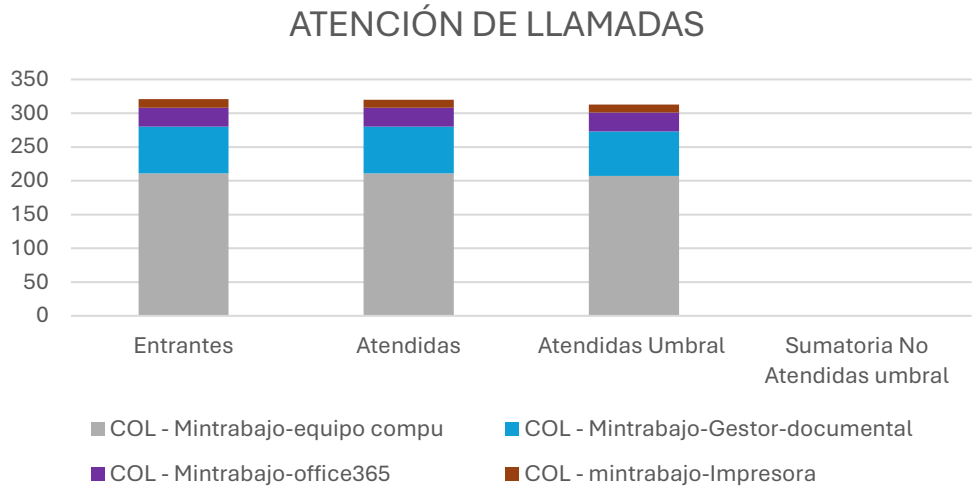


Ilustración 3738 Llamadas Atendidas

El servicio más solicitado a través de la atención de llamadas es: Equipo de cómputo con 321 llamadas entrantes, se atendieron 320 solicitudes se observan: 1 llamada abandonada antes de los 20 segundos.

- **Casos Registrados por Categoría de Servicio**

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

- **Análisis de Casos Anulados por Servicio**

Para este periodo se tienen 40 casos anulados para los siguientes servicios:

CASOS ANULADOS	TOTAL
Herramientas de Gestión	39
Administración de servidores	1
Total general	**40**

Los casos anulados por Herramientas de Gestion se deben al monitorio proactivo de alarmas de Zabbix con 39 casos.

El caso anulado por Administración de servidores se debe a un cambio duplicado que se generó.

- **Análisis de Casos Suspendidos por Servicio**

Para el periodo del mes de abril, se dio una disminución de casos suspendidos del 36,70% que corresponde a 40 casos para un total de este mes de 69 casos de los siguientes servicios:

CASOS SUSPENDIDOS	TOTAL
Soporte Microinformatica	35
Administración de servidores	21
Redes y Conectividad	7
Seguridad informatica	4
Energía Eléctrica Regulada - UPS	2
Total general	69

Tabla 31 casos suspendidos

- **Soporte Microinformática:** 35 casos suspendidos debido a que se ha solicitado información complementaria a los usuarios o están pendientes por disponibilidad del usuario: Equipo Escritorio y Asesoría – Consulta con 6 casos; Traslado de Sede, Cambio Equipo o Rol y Backup con 4 casos cada categoría; Cambio Toner, Equipo Periférico con 3 casos cada categoría; Solicitud Backup, Equipo Portátil con 2 casos de cada categoría; Configuración, Traslado - Movimiento, Asignación de equipo (portátil o PC), Falla General, Instalación – Configuración con 1 caso cada categoría.
- **Administración de servidores**: 21 casos suspendidos por: Inactivar usuario con 11 casos, Crear/Modificar/Eliminar con 2 casos; Configuración, Mantenimiento preventivo, Asesoría - Consulta, Asignación de licencia, Informes y Reportes, Cambiar contraseña, Administración de equipos, Cambio de grupo con 1 caso para cada categoría.
- **Redes y Conectividad:** 7 casos suspendidos debido a: Router con 5 casos; Starlink y FortiGate con 1 casos cada categoría.
- **Seguridad informática:** 4 casos suspendidos: Seguridad Informática con 2 casos, Análisis de Correos y Ajuste de configuraciones (Crear - Eliminar) con 1 caso para cada categoría.
- **Energía Eléctrica Regulada - UPS:** 2 casos suspendidos por alarmas proactivas de Zabbix en UPS de Barrancabermeja.

- **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 39 Incidentes solucionados soporte en sitio

Incidentes solucionados por Soporte Territoriales: Para este periodo quedaron 11 incidentes en estado solucionado.

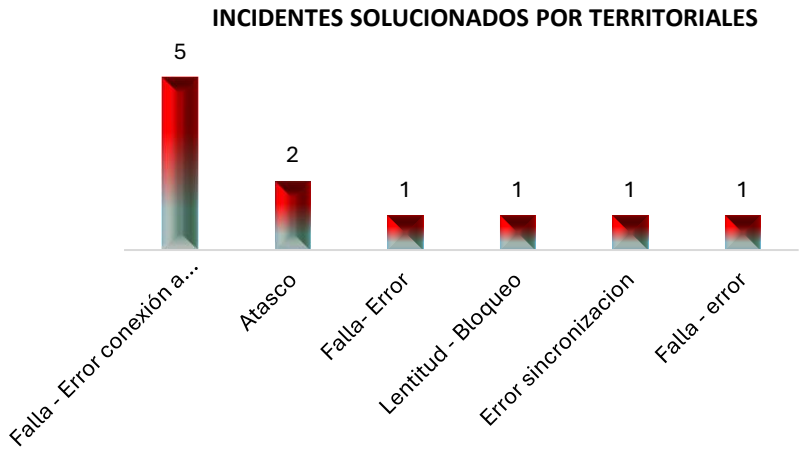


Ilustración 40 Incidentes solucionados soporte territoriales

Requerimientos solucionados por la Mesa de Servicios:
En el mes de abril quedaron 61 requerimientos en estado solucionado.

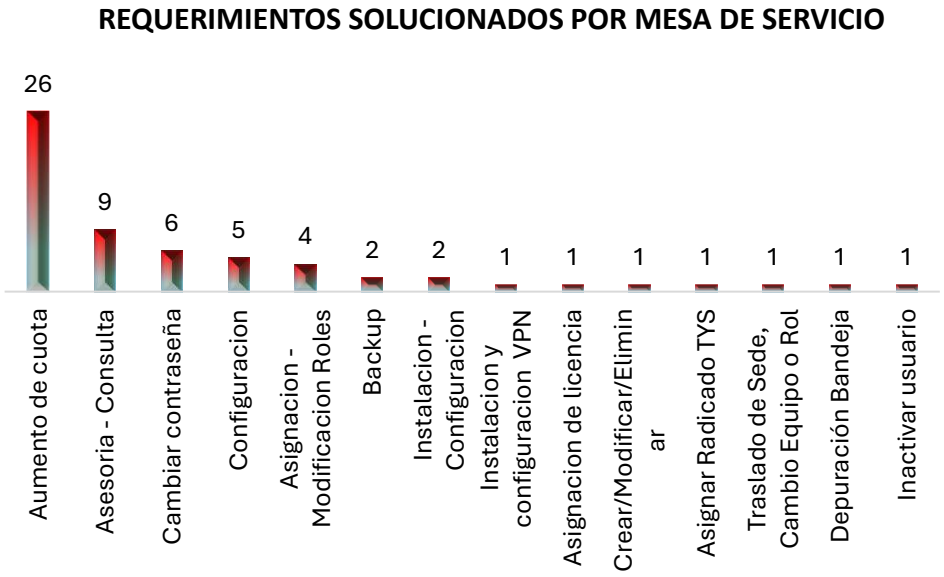


Ilustración 41 requerimientos solucionados mesa de servicios

Requerimientos solucionados por Soporte en sitio Bogotá: En el mes de abril quedaron 88 requerimientos en estado solucionado.

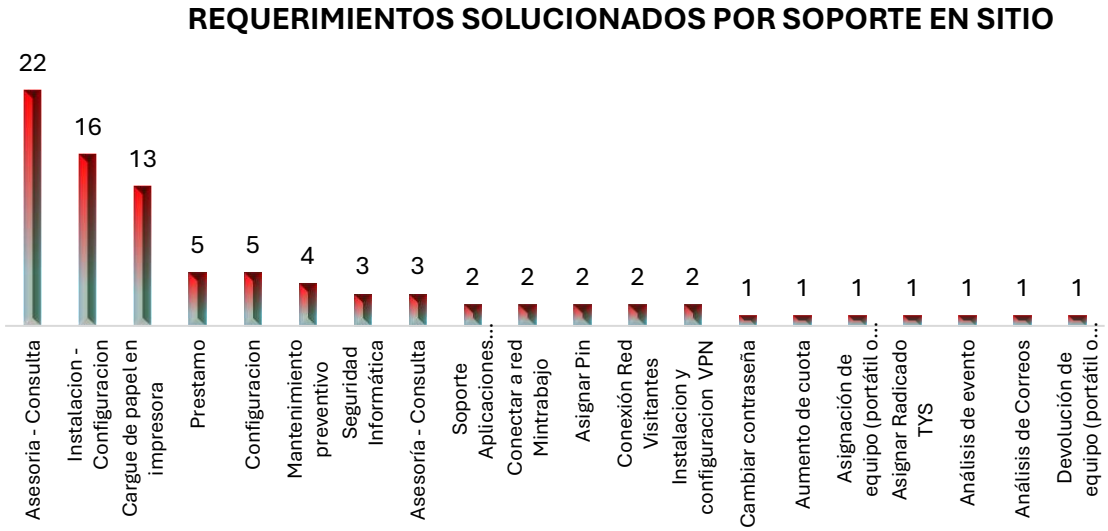


Ilustración 42 requerimientos solucionados soporte en sitio

Requerimientos solucionados por Soportes Territoriales: Para el mes de abril quedaron 232 requerimiento en estado solucionado.



Ilustración 43 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 abril se cerraron 724 casos, discriminados así: Asesoría - Consulta 156 casos, Asesoría – Aumento de cuota 146 casos, Cambio de grupo 44 casos, Creación de usuario 38 casos, Inactivar usuario y Instalación y configuración VPN 26 casos para cada categoría, Configuración 18 casos, Asignar Radicado TYS 15 casos, Instalación – Configuración y Habilitar usuario 8 casos para cada categoría.

En comparación del mes anterior se nota una disminución de casos cerrados por la mesa de un 23,78% que es equivalente a 226 casos.

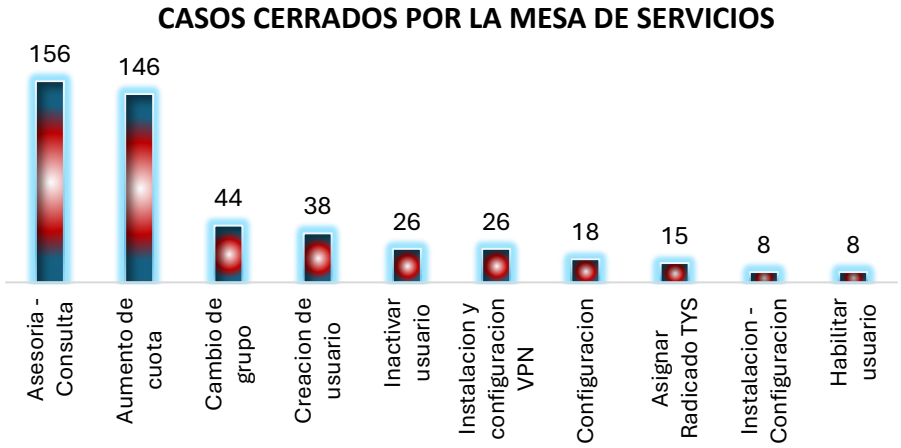


Ilustración 4445 Requerimientos Cerrados por la Mesa de Servicios

Casos Cerrados por Soporte en Sitio: Se indica el top 10 de Requerimientos cerrados por soporte en sitio, para el mes de abril se cerraron 1215 casos discriminados así: Cargue de papel en impresora con 332 casos, Asesoría – Consulta con 183 casos, Instalación - Configuración con 159 casos, Configuración con 122 casos, Préstamo con 56 casos, Soporte Aplicaciones Office 365 con 39 casos, Análisis de evento 35 casos, Conectar a red Mintrabajo 34 casos, Seguridad Informática 30 casos, Instalación y configuración VPN con 28 casos.

En comparación con el mes anterior se tiene una disminución del 11,11% que corresponde a 152 casos.

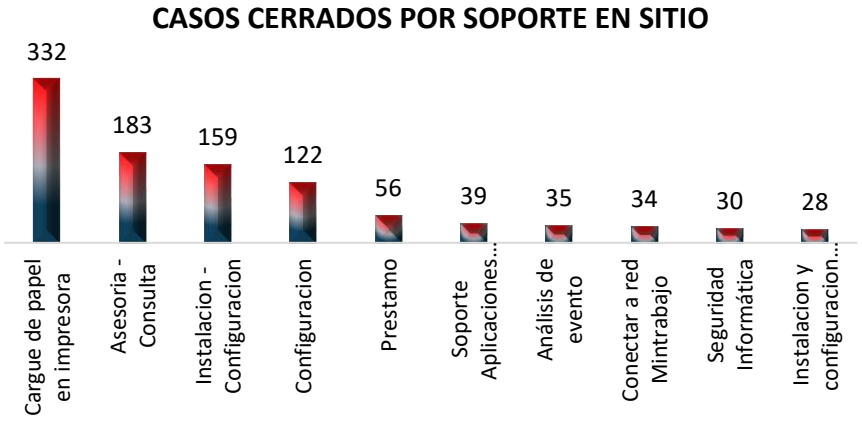


Ilustración 46 Casos Cerrados por Soporte en Sitio

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 abril se cerraron 1502 casos, discriminados así: Asesoría – Consulta con 262 casos, Cargue de papel en impresora 226 casos, Instalación - Configuración 148 casos, Configuracion100 casos, Asesoría Excel 73 casos, Asesoría PDF 71 casos, Mantenimiento preventivo 64 casos, Instalación y configuración VPN 62 casos, Soporte Aplicaciones Office 365 52 casos, Asesoría Word 43 casos.

En comparación con el mes anterior se tiene una disminución del 12,26% que corresponde a 210 casos.

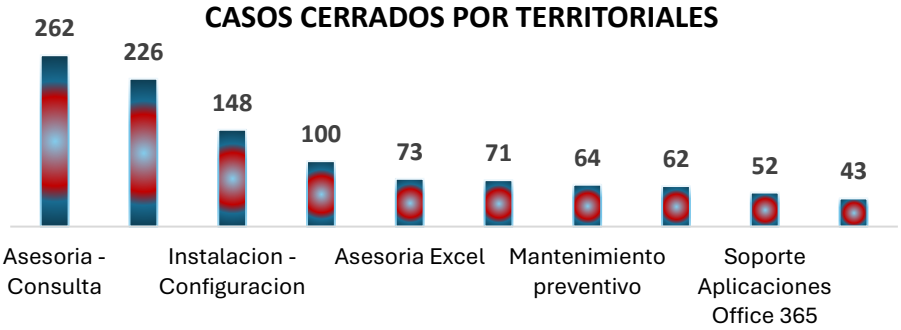


Ilustración 47 Casos Cerrados por Territoriales

- **Casos Atendidos a Usuarios VIPS**

Durante este periodo se crearon 38 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
Incidentes	3		3
Requerimientos	35	0	35
Total general	**38**	**0**	**38**

Tabla 32 Casos Atendidos usuarios VIPs

Se atendieron 11276 solicitudes para el resto de los usuarios discriminados así:

TIPO DE CASO-NO-VIPS	CUMPLIMIENTO	NO_CUMPLE	TOTAL
Incidentes	59	1	60
Requerimientos	1215	1	1216
Total general	**1274**	**2**	**1276**

Tabla 33 Casos Atendidos usuarios

- **Medio de Ingreso de Casos**

Durante el período ingresaron a la mesa de servicio 5653 casos a través de los diferentes medios que se tiene habilitados para la atención de solicitudes, como son Gestión Técnica, Correo SoporteMT, alarma de Zabbix, Llamadas Telefónicas, alarma de Fortisiem, Portal Autogestión, casos creados de forma automática por las diferentes herramientas:

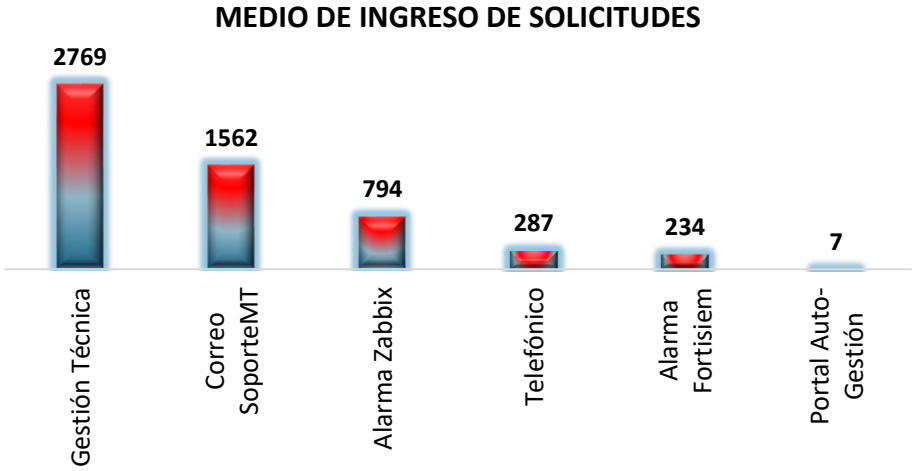


Ilustración 48 Medios de Ingreso de Casos

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

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

Se Inicia mantenimiento de las impresoras de sede central.

Se entregan 2 manuales para la revisión de calidad: Manual de configuración de impresoras para equipos personales y Manual de configuración de firma Outlook escritorio y web en equipos personales.

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

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

Se realizan cinco 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 interviene en 1821 casos, dentro de los que se destacan: Asesoría-Consulta sobre el software instalado, Cargues de Papel en las impresoras de las diferentes Sedes, Inactivación de usuarios, Configuración de hardware y Línea Base, Instalación-Configuración de línea base, Intervención de impresoras, Aumento de cuotas de impresión, Cambio de contraseña, Relanzamiento de tareas de usuario final y Asignación de Radicados T y S.

Se inicia con el mantenimiento semestral de las impresoras Ricoh en las Sedes e Inspecciones de todo el país.

Validación y pruebas funcionales de la antena Starlink en Buenaventura.

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
Abril 26	Magdalena	El Plato	Fortinet - Conectividad e Internet	Se realiza visita a inspección, se verifica funcionamiento del equipo Fortinet, concluyendo que se debe reemplazar el equipo actual por uno nuevo	RF-200762
Abril 26	Cundinamarca	Villeta	Devolución de equipo de cómputo MBARRERA	Se procede a dejar constancia de la información recibida y se indica que, por temas de trazabilidad y tiempos de gestión, los casos actuales se cerrarán y se generará posteriormente un nuevo caso relacionado, en el cual se realizará la gestión solicitada de inactivación en Villeta y activación en Mosquera.	RF-199423
Abril 26	Apartadó	Turbo	Pruebas sobre el firewall	Se identificó que la falla correspondía al conector de la fuente de poder del equipo Fortinet, el cual presentaba falso contacto. Se realizó ajuste/reconexión, restableciendo el servicio con normalidad.	IM-200963
Abril 26	Magdalena	Plato	Visita inspección por cambio de equipo Fortinet	Se realiza cambio de equipo Fortinet, se retomaron las conexiones de red que usaba el equipo anterior, dejando en funcionamiento el nuevo equipo firewall	RF-203318 RF-203315
Abril 26	Meta	Granada	Lentitud en equipo de escritorio JDIAZG	Se realiza validación del rendimiento del sistema, evidenciando posible consumo elevado de recursos, archivos temporales acumulados y/o programas en segundo plano que afectan el desempeño.	RF-203761

Tabla 34 Visitas a sedes sin Soporte en Sitio

- Medición ANS Mesa de Servicios

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

Área	Nombre del Indicador	Resultado	Meta
Mesa de Servicio	Tiempo de atención de solicitudes por soporte en sitio	100,00%	95,00%
	Tiempo de solución de incidentes por soporte en sitio	99,45%	90,00%
	Tiempo de solución de requerimientos por soporte en sitio	99,86%	90,00%
	Tiempo de respuesta de la mesa de servicio	99,06%	85,00%
	Abandono de llamadas	0,00%	Máximo 8,00%

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

Tabla 35 Medición de ANS Mesa de servicios

3 LINEA DE SERVICIOS CENTRALES

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

3.1 Datacenter Principal

Se realizó la gestión efectiva de los requerimientos de servicio, Línea de Servicios centrales realizó atención de un total de 719 casos distribuidos en requerimientos de servicios, incidentes, cambios y problemas. Así como la siguiente distribución de casos por estado, grupo de especialistas y atención de acuerdo con el tipo de usuario.

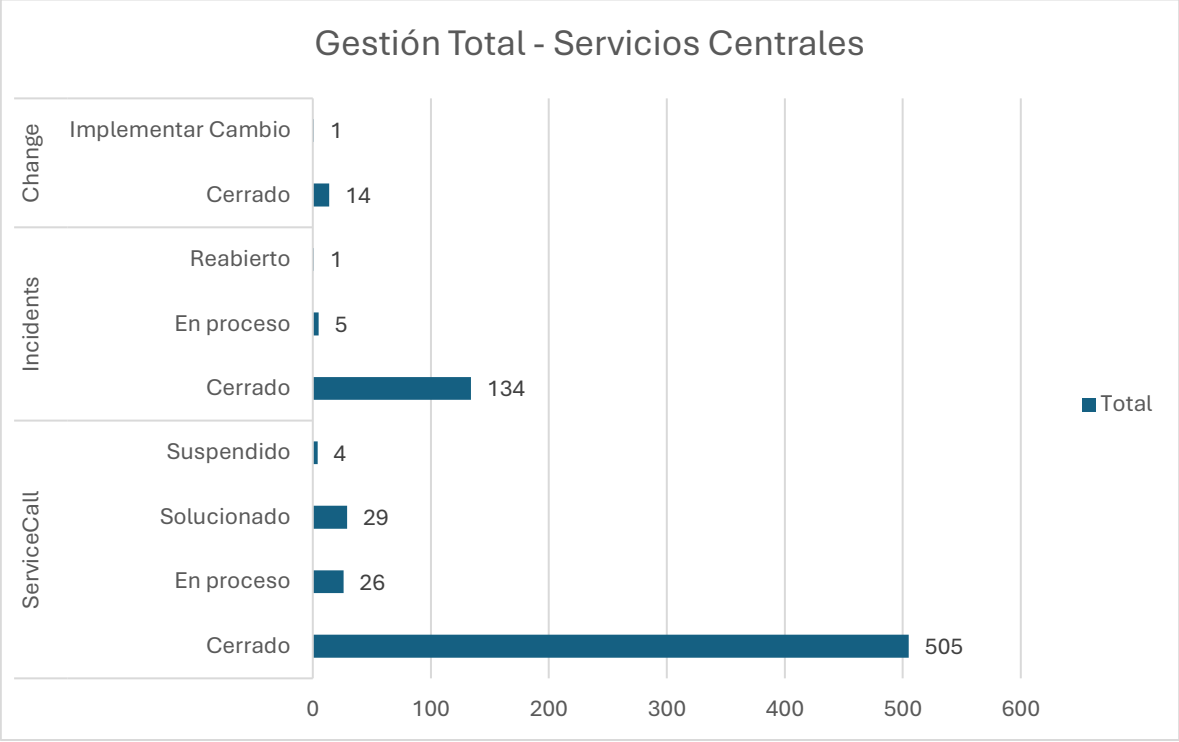


Ilustración 49 Gestión Casos - SC

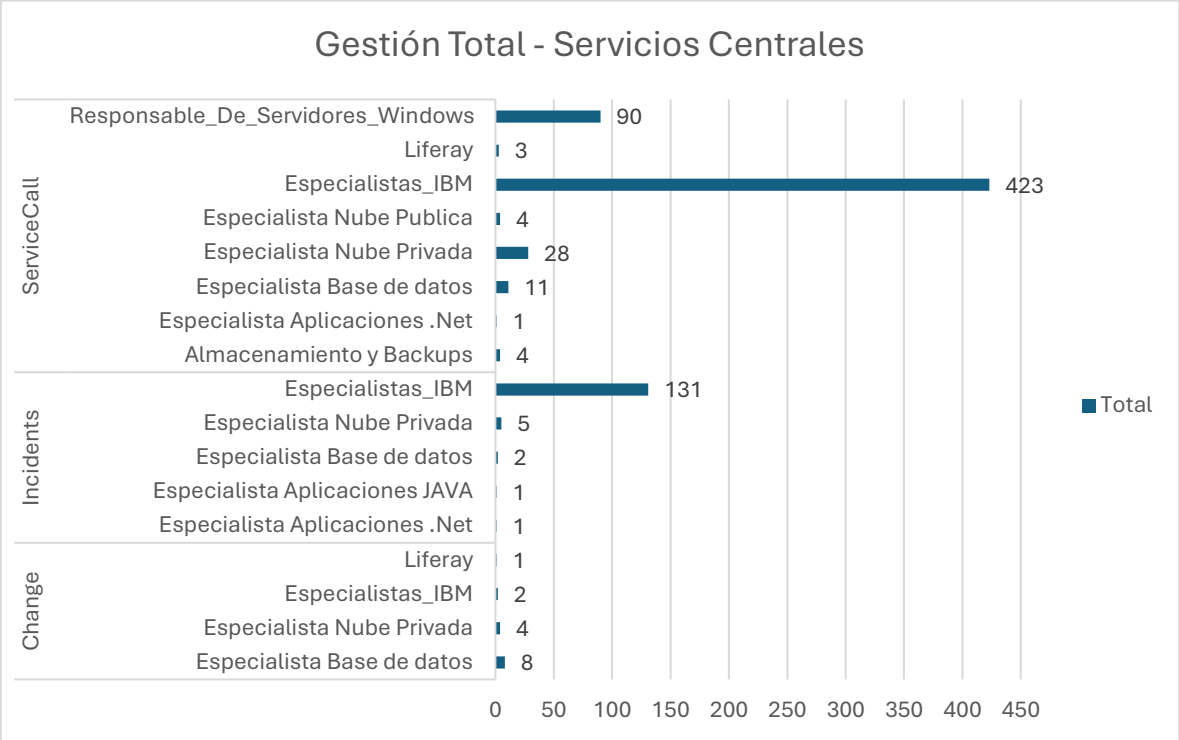


Ilustración 50 Gestión SC - Por Grupo

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 5152 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

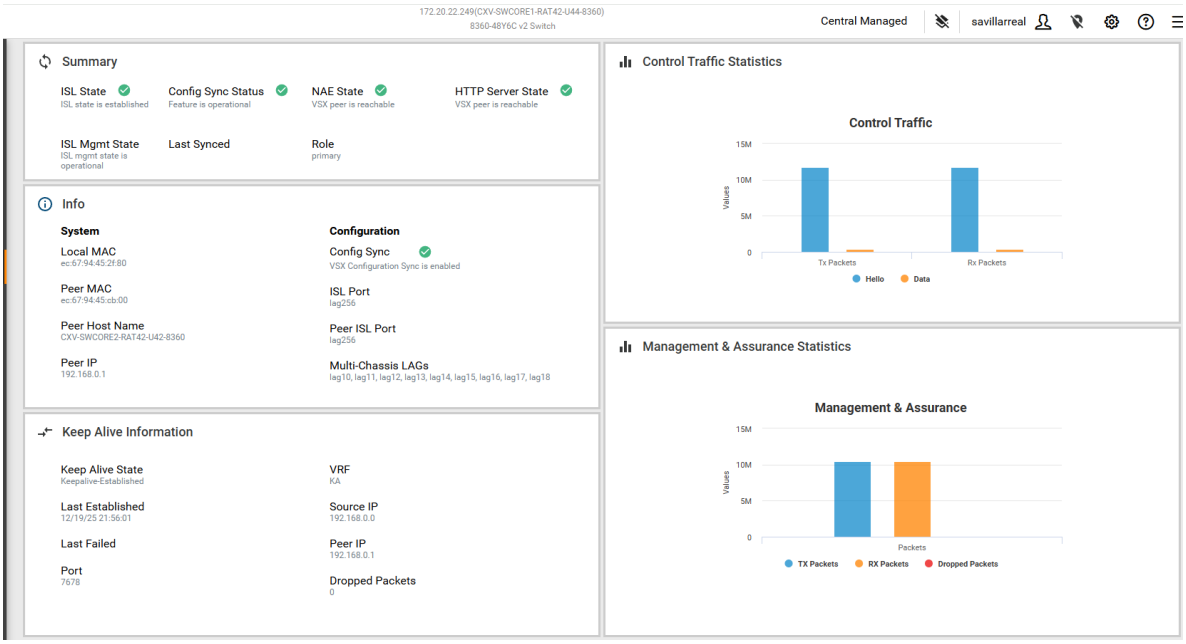


Ilustración 53 Sincronización HA de los Switch Core

-

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 trafico total de 332 Mbps, no se han presentado picos de consumo, que no afectan la estabilidad del cana ya que no se mantienen.

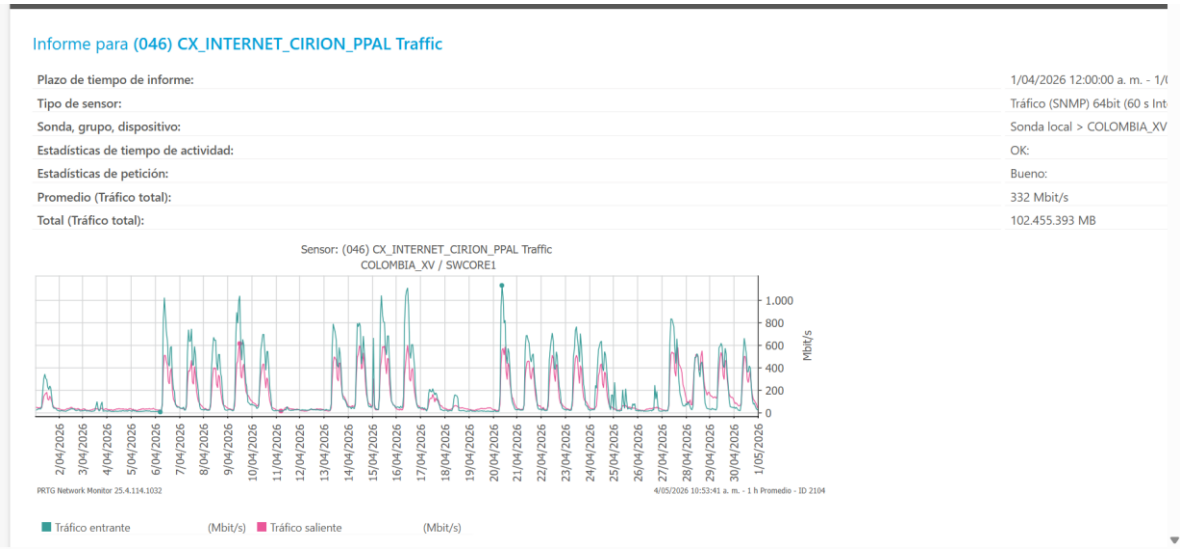


Ilustración 54 Grafica de consumo canal Internet Datacenter

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 continuó con 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:

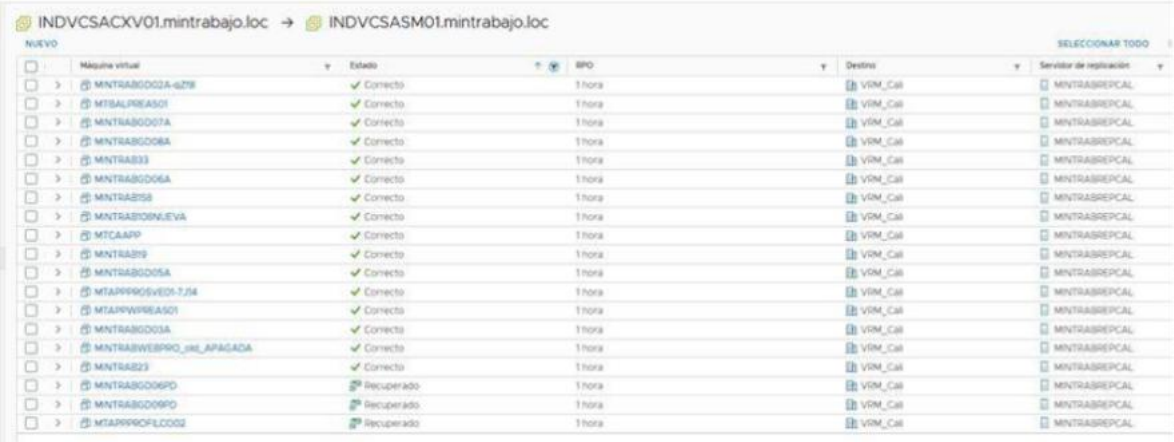


Ilustración 55 máquinas virtuales DRP

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

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

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

La prueba se realizó para las siguientes bases de datos:

No.	Base de Datos	Aplicación
1	MT_EVENTOS	Observatorio Laboral
2	ARCHSINDICAL	Archivo Sindical
3	Bancos	Tesorería
4	CalculadoraLaboral	Calculadora Laboral
5	ESTADOJOVEN	Estado Joven

No.	Base de Datos	Aplicación
6	Infraestructura	Cobro Coactivo
7	MTRCobroCoactivo	Cobro Coactivo
8	Siriti2018	Siriti

Tabla 36 Pruebas realizadas

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

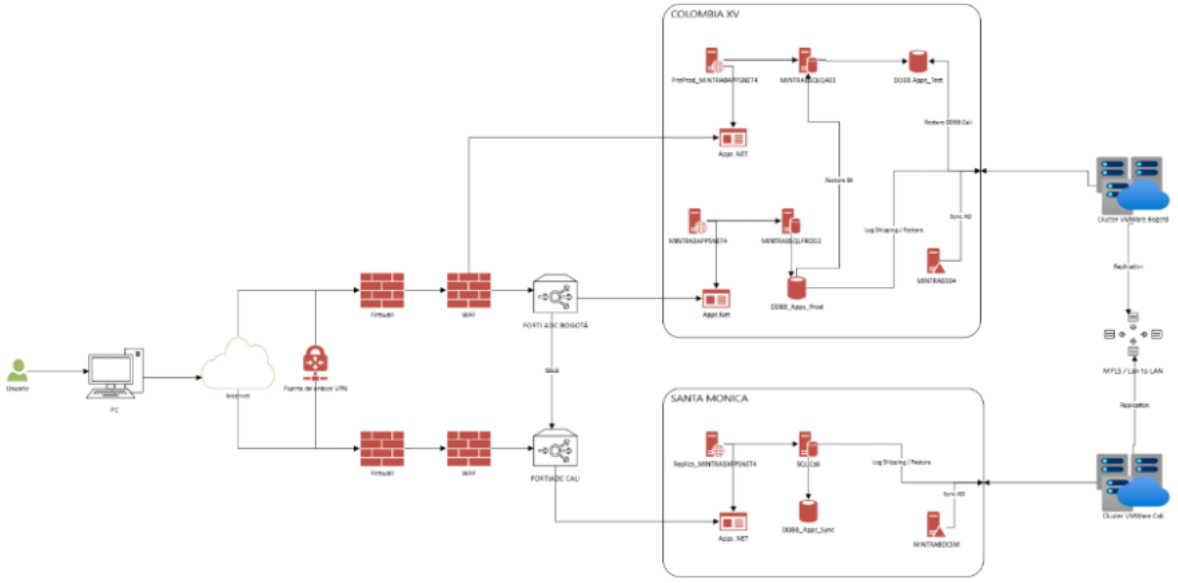


*Ilustración 5*657 Escenario pruebas Apps DRP

A nivel de comunicaciones en DC alterno, se observa que la conexión del LAN to LAN entre los dos Datacenter funcionó correctamente, 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 178Mbps. Tambien se observa que se presentó alto consumo durante el mes, esto debido a que por parte del equipo de infraestructura enviaron las maquianas de QA del gestor documental.

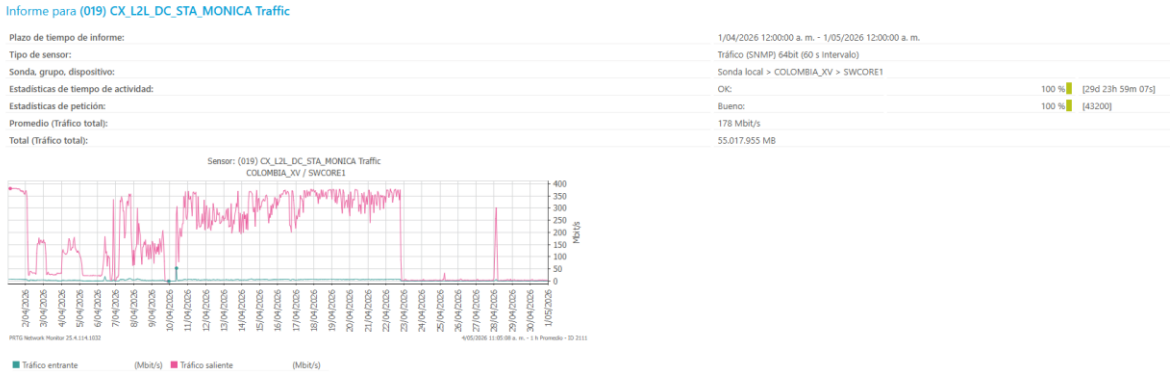


Ilustración 58 Extremo DC Bogotá

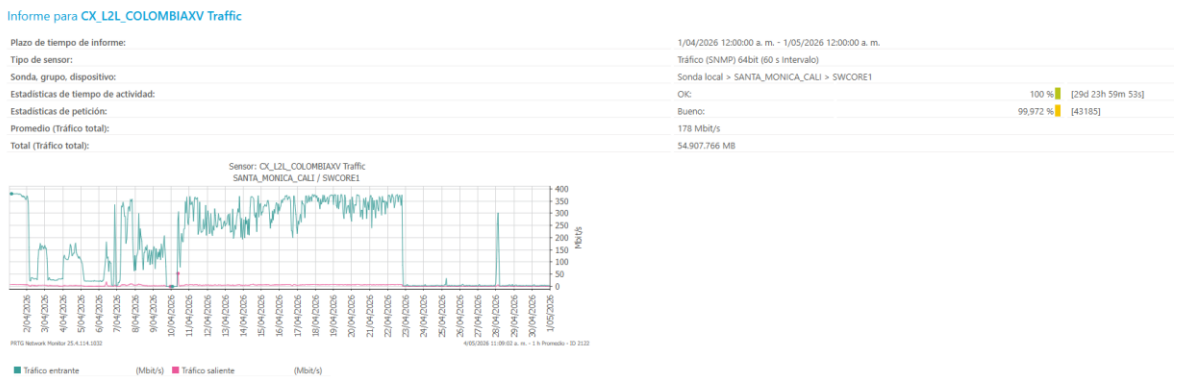


Ilustración 59 Extremo DC Cali

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 0.23 Mbps.

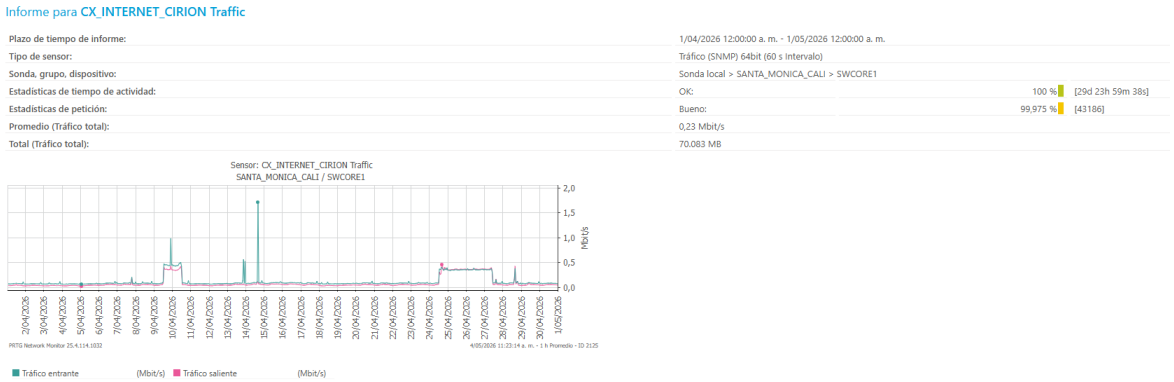


Ilustración 60 Estado canal de Internet DC Cali

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

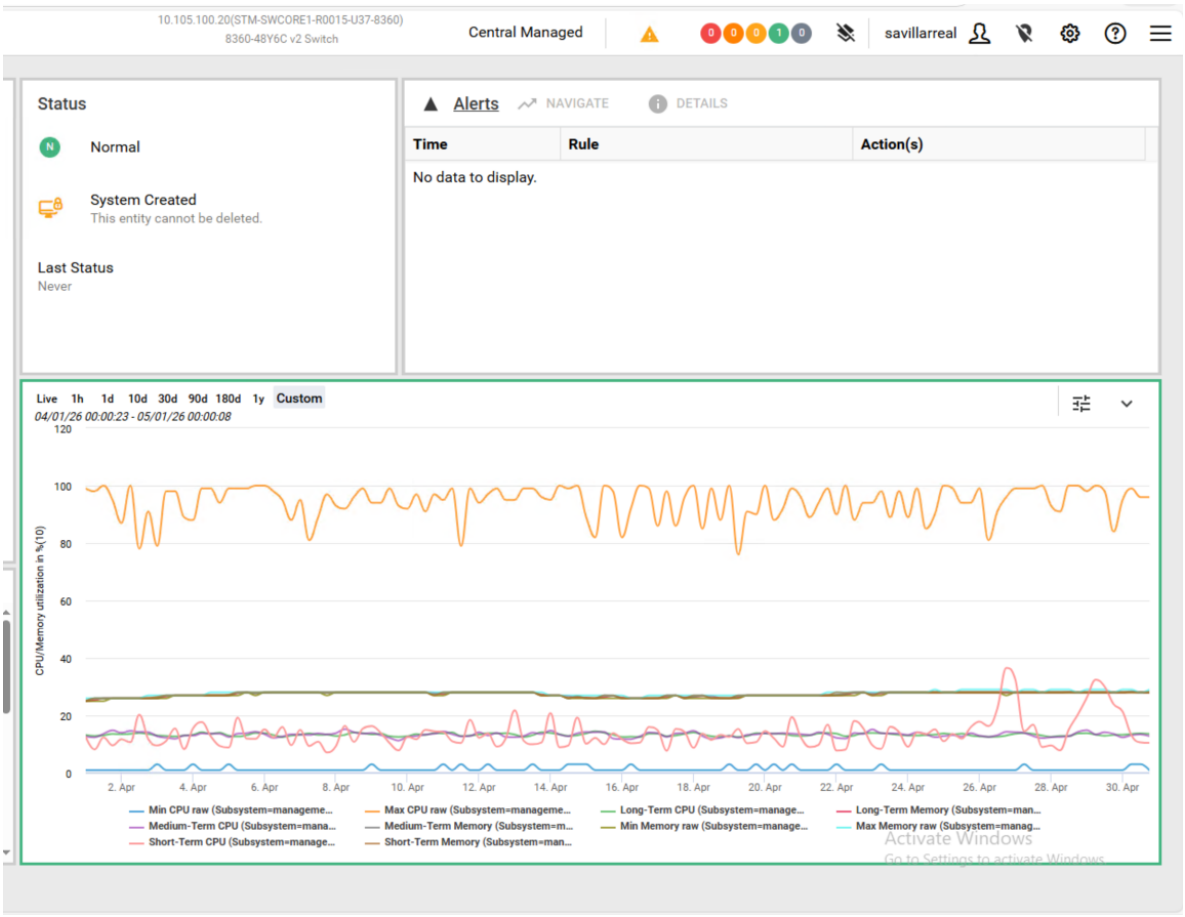


Ilustración 61 Estado SWCORE Datacenter alterno

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

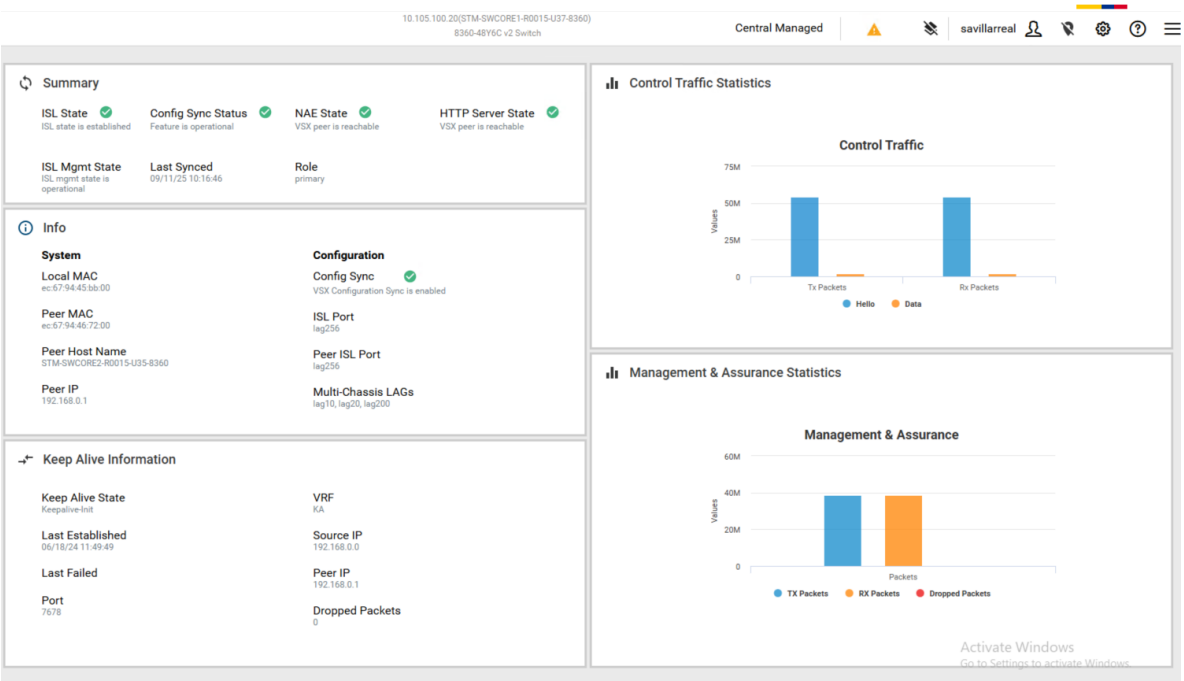


Ilustración 62 Estado HA SWCORE Datacenter alterno

Se verifica el canal MPLS de datacenter alterno, el cual se observa que se ha mantenido activo durante el mes de abril, 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 0.061 Mbps.

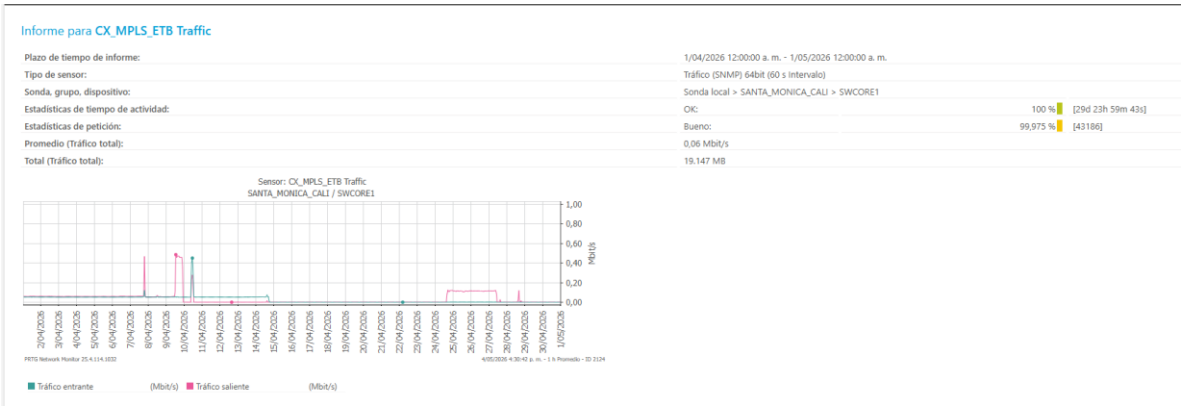


Ilustración 63 Consumo canal MPLS DC Alterno

Se verifica estado del equipo, donde se observa que presenta un uptime de 1 año y 4 semanas, el equipo no ha tenido problemas en procesamiento y memoria. Este equipo recibe la conexión MPL de respaldo del DC principal, en caso de algún evento en este punto.

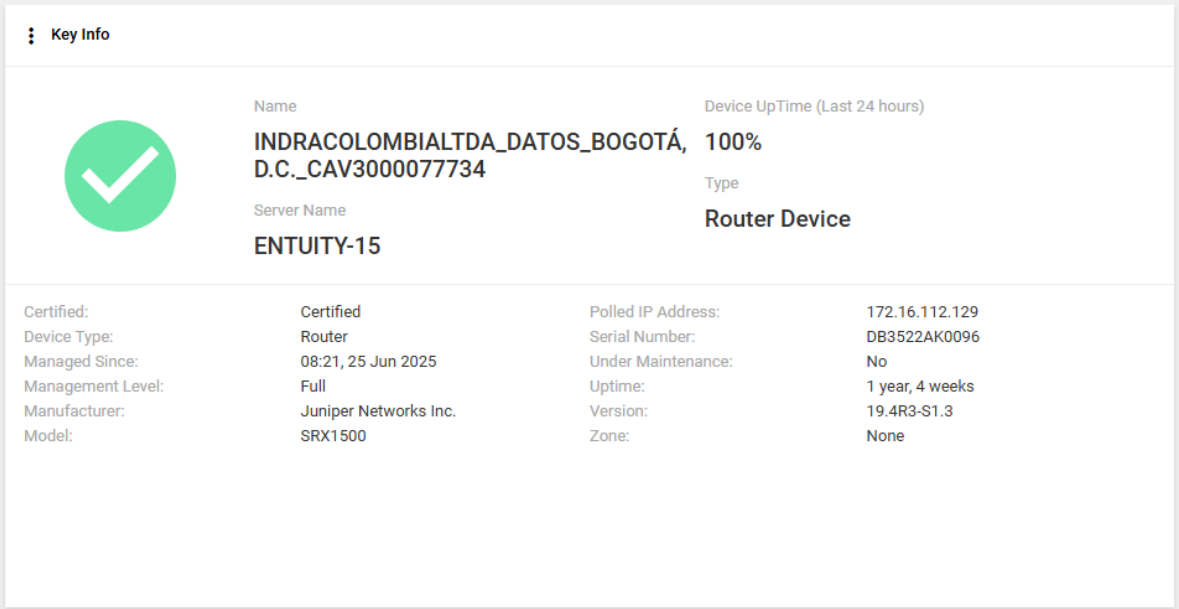


Ilustración 64 Estado Router MPLS DC Alterno

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 empresariales. Esta validación garantiza la escalabilidad y la flexibilidad del sistema para adaptarse a futuros cambios en la infraestructura o en los requisitos del negocio, esto en el marco de la implementación de nueva infraestructura tecnológica y de la sincronización de máquinas virtuales al nuevo vCenter de VMWare.

Se observó un comportamiento de crecimiento la asignación de licencias de Office 365 reportados a través de ARANDA, donde se realizó la atención de 90 requerimientos asociados a esta categoría del servicio de Windows, así como la creación, modificación de usuarios que mantiene su reporte en 13 casos para el mes de abril. De la mano de asignación de licencias se atendieron 7 requerimientos, obteniendo una disminución considerable con respecto a los meses anteriores, con respecto a los casos asociados a configuración de MFA se observa que se mantiene en 19 casos adicionales de apoyo en configuraciones del servicio de Office 365. 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. Se ha incrementado el reporte de asignación de licencias por creación de cuentas de servicio por parte de las áreas teniendo en cuenta los movimientos en áreas y estructura organizacional de la entidad.
Durante el mes de abril de 2026, se surten los procesos de inactivación, reactivación o creación de usuarios de acuerdo con las necesidades y ajustes requeridos por cada dependencia de la entidad, dentro de los tiempos establecidos y bajo la práctica referenciada desde la Oficina de Tecnologías de la Información.

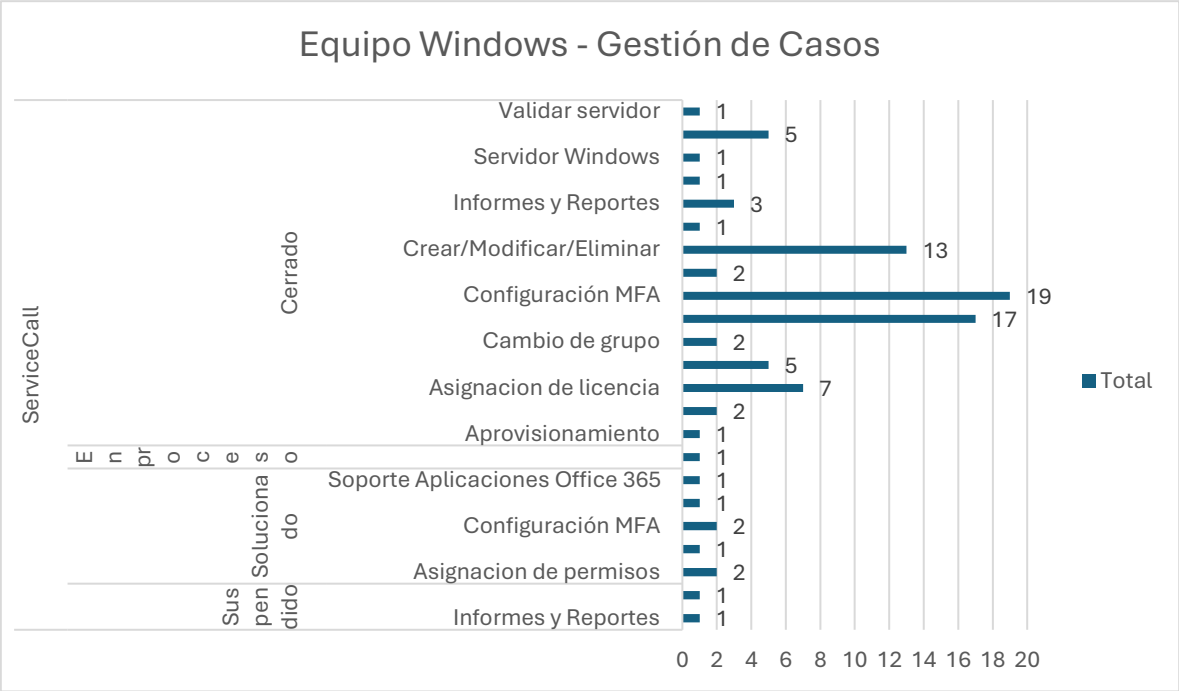


Ilustración 65 Gestión de Casos Windows

Es importante que la entidad remita bimestral o trimestralmente informes relacionados con la desvinculación de funcionarios y contratistas 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 trabajando con la Oficina de Tecnologías de la Información para fortalecer este punto en específico e implementar un plan de calidad de la información de Directorio activo. Actualmente se está a espera del envío de la información de manera formal por parte de la entidad, pero se ha trabajado de manera articulada con la Oficina de Tecnologías de la Información, para fortalecer este ítem dentro de la entidad. Es importante que esta actividad se priorice para los meses de enero y febrero debido a la desvinculación de contratistas de la entidad por cierre de gestión. Lo anterior alineado al nuevo lineamiento de gestión y creación de usuarios emitido por la OTIC.

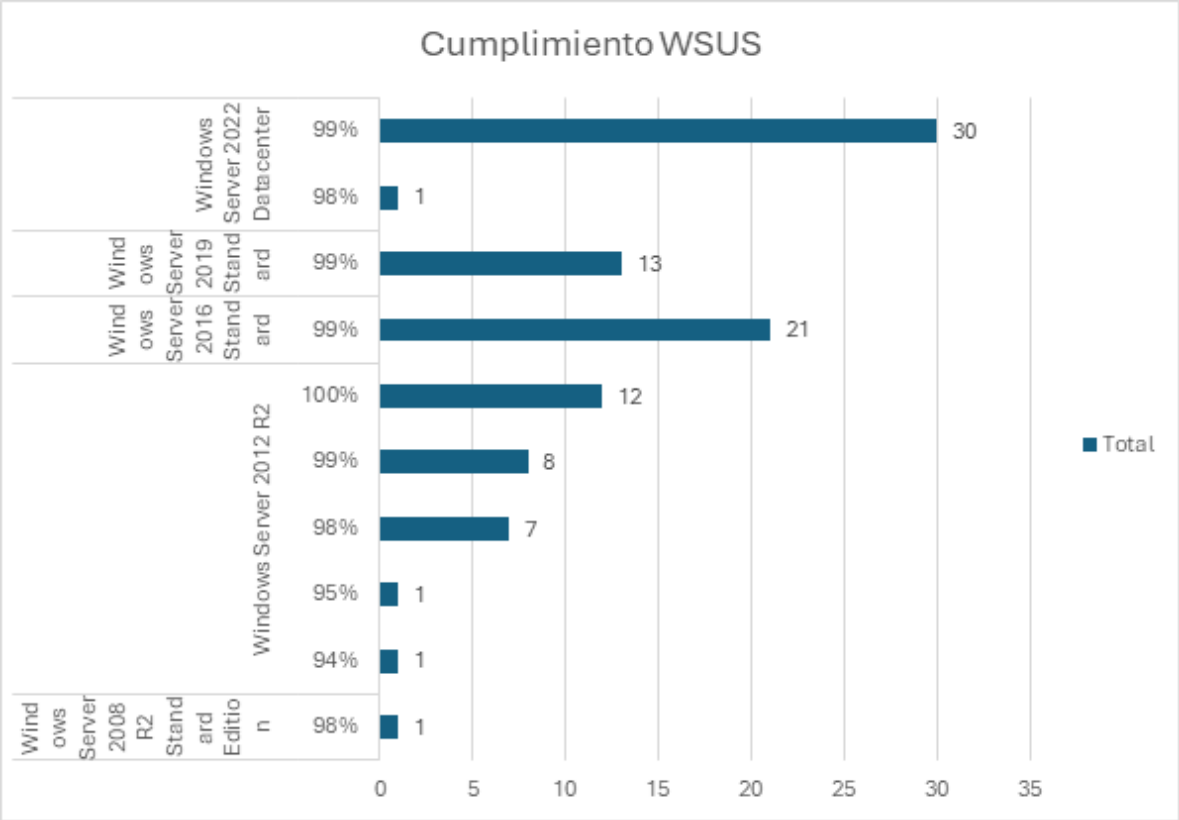


Ilustración 66 Cumplimiento WSUS

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.

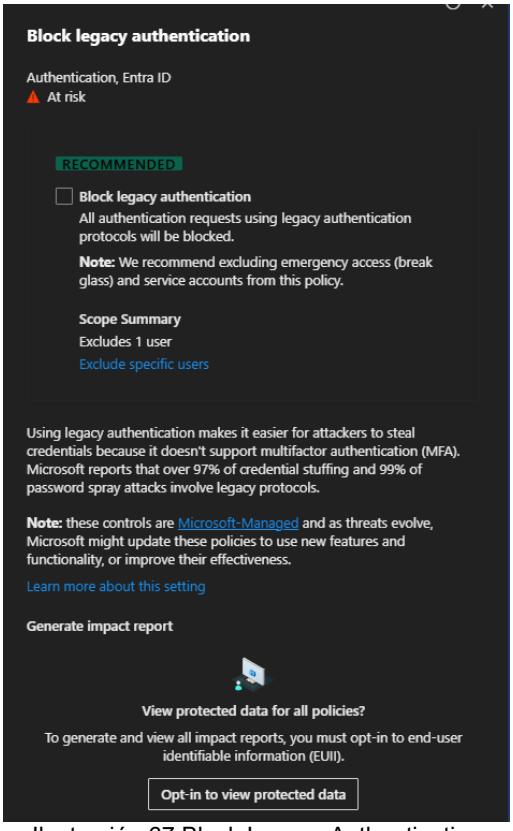


Ilustración 67 Block Legacy Authentication

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

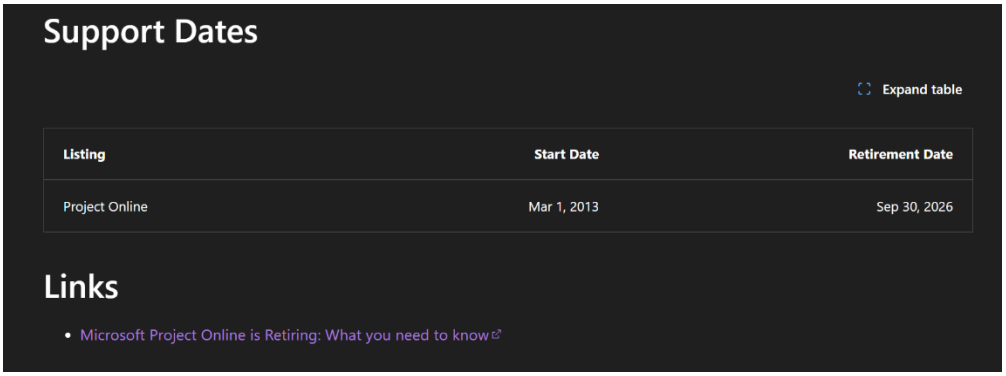


Ilustración 68 Fechas de Soporte

Licencias asignadas

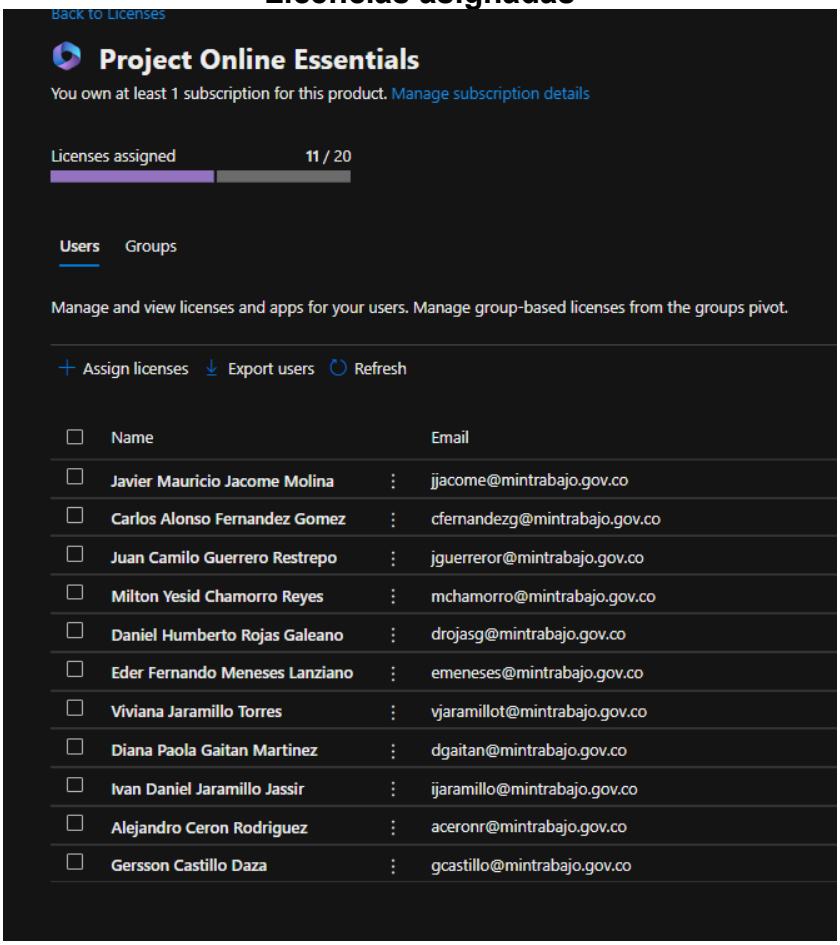


Ilustración 69 Licencias asignadas

3.1.3 Procesamiento, almacenamiento y respaldo - Nube Privada

Se continúa con la ejecución del plan de backups en donde se generan respaldos completos de todas las máquinas virtuales críticas alojadas en VMWare, este plan de backup en la actualidad se ejecuta los viernes en la noche generando un backup full de la semana de cada máquina y su almacenamiento, garantizando 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 ha permitido como operador de servicios tecnológicos, identificar diversas acciones de mejora que se han venido ejecutando de manera transversal desde el inicio del contrato, pero es importante dar visibilidad de los escenarios observados. Durante los procesos de afinamiento y egreso de equipos no productivos en Datacenter se logra visualizar componentes en estado sensible que podrían poner en riesgo la disponibilidad de servicios críticos como lo es el sistema de información histórica de nómina. Se observa que el servidor físico que aloja la máquina MINTRAB13 es un Dell (PowerEdge 2950) con fecha de salida a mercado 19/10/2015 y cuenta con un OS SUSE Linux Enterprise Server 11 (i586) con fecha de salida al mercado 24/10/2016.

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

Se dio visibilidad de esta situación para realizar las maniobras técnicas correspondientes de manera coordinada con el proveedor de este software a la entidad durante el mes de julio de 2024 se realizó esta sesión, en donde se identifican los servidores productivos como parte del escenario de virtualización de la entidad y que su proceso de migración a nuevos servidores de aplicación puede surtirse de la mano del área funcional. Actualmente se está a espera que el área funcional nuevamente permita un espacio de socialización para lograr entender el paradigma de consulta y validar que es posible migrar bajo una modalidad más simple y dejar la dependencia de esta infraestructura en estado de obsolescencia. Para el servidor MINTRAB13, el cual aloja una copia histórica del anterior aplicativo y base de datos de nómina de la entidad, el proveedor nos confirma que no tiene administración y ningún tipo de gestión sobre el recurso y la

información que esta aloja. La entidad confirma tener acceso de consulta a una base de datos y solo es consultada por demanda, pero no está asociada a ningún sistema de información productivo.

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

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

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

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

Es importante mencionar que la entidad no ha fortalecido o establecido una ruta para la retención de los backups de manera clara y concisa, por lo cual el equipo de trabajo creo el plan de backups y se definieron tiempos de retención de estos orientados a Infraestructura de acuerdo con las buenas prácticas y experiencia del equipo de trabajo. No se definen tiempos claros para estos recursos ni para documentos virtuales, file server o backups de usuario final por parte de la entidad.
Se ha solicitado Instrucción a la entidad instrucción con respecto a los siguientes recursos los cuales se encuentran alojados en la Nube Privada de la entidad y por su grado de Obsolescencia crítico y debido a que el sistema Operativo en el que se encuentran aprovisionados estos recursos se encuentra totalmente fuera de soporte, se requiere de una instrucción precisa y clara del cómo proceder con los siguientes recursos:

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

Ambas aplicaciones dependen de la Subdirección de IVC.

- Actualización MINTRAB25: La máquina fue migrada a Windows 2022 y fue separada la base de datos en un servidor independiente, se están realizando pruebas de conectividad de la aplicación. A la fecha la

aplicación está estabilizada y solo restaría la validación del área funcional y el visto bueno para apagado y reemplazar el servidor.

Con respecto a los requerimientos del servicio de Nube privada su categorización nos indica que el comportamiento de reportes asociados a servidores Windows es de mayor demanda en el proyecto, asociado a configuraciones de servicios, revisión de consumo de capacidades a través de alertamientos de la herramienta de Monitoreo Zabbix o solicitud de accesos a carpetas compartidas del servicio de File Server. Se ha venido trabajando articuladamente con la Coordinación de Soporte Informático manteniendo informado del comportamiento de la nube privada y sus capacidades. Así como el apoyo transversal en los proyectos escalados por las áreas funcionales. Es importante mencionar que se ha venido creando diferentes VM asociados a nuevos servicios que aprovisionará el Ministerio del Trabajo, pero en principio se encuentran en su fase de pruebas por lo cual solo se han creado VM de pruebas. Algunas VM ya fueron intervenidas, pero hasta el momento no son productivas debido a que se está a espera de VB o revisiones de las áreas funcionales.

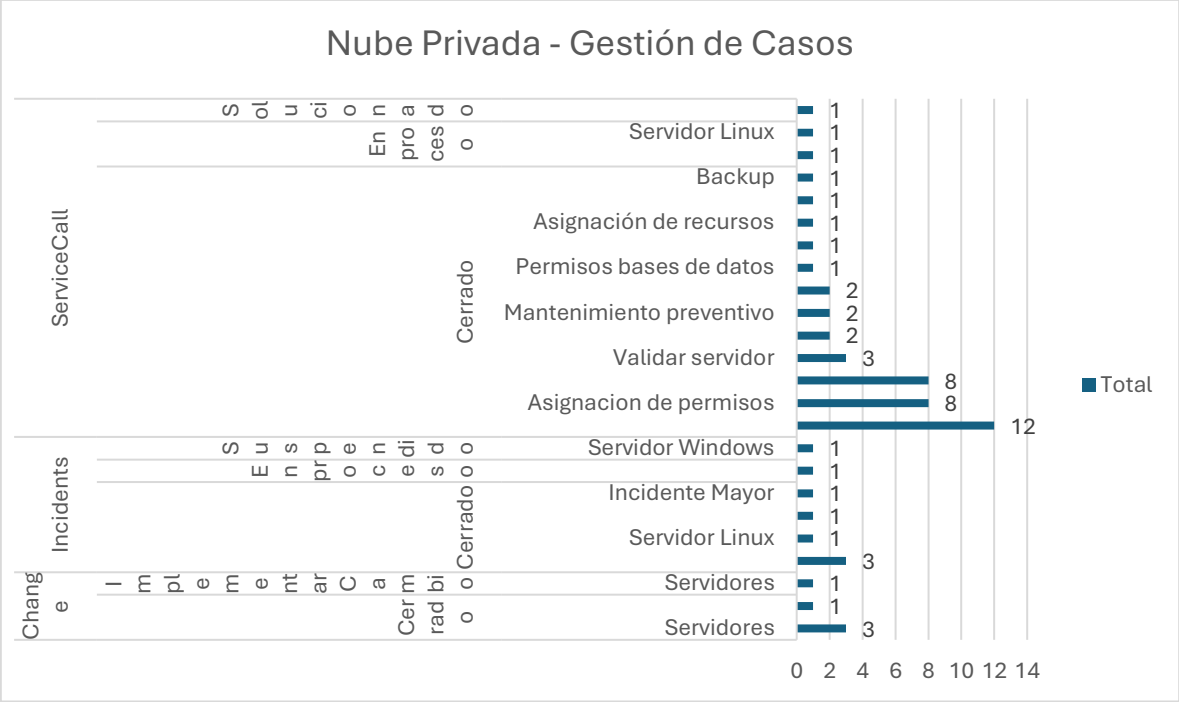


Ilustración 70 Gestión Nube Privada

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 37 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 38 *Capacidades modificatorio*

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

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

Tabla 39 *Total capacidades + servers desaprovisionamiento*

Total MinT (Sin servidores para desaprovisionar con ambientes de pruebas)	
Descripción - características	Total
vCPU	716
RAM	3.01 TB
Almacenamiento	130 TB
Numero de Servidores	106

Tabla 40 *Total capacidades consumidas*

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

Tabla 41 Total capacidades sin servers de pruebas

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

Tabla 42 Total capacidades ambientes pruebas

- vCPU Ficha: **854** a vCPU consumida: **716 (83.4%)**
- Memoria Ficha: **3.3 TB** a Memoria consumida: **3.0 TB (88.7%)**
- Almacenamiento Ficha: **156 TB** a Almacenamiento consumido: **130 TB (83.3%)**
- Número de Servidores Ficha: **106** a Numero de Servidores disponibles: **106**

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

revisión, nuevamente entraría el ítem de almacenamiento superando la capacidad contratada.

Es importante mencionar que la entidad cuenta con 10 Servidores de pruebas nuevos asociados a nuevas aplicaciones y existe una redundancia de servidores del servicio SIAS, ya que se aprovisionaron los 3 nuevos servidores de pruebas para este servicio, pero no se encuentran en uso actualmente, por lo cual en cuanto se realice el cambio de los servidores antiguos a los nuevos, se reducirán las capacidades consumidas, así como el servidor creado de manera temporal para el Asessment realizado para aplicaciones a migrar hacía Azure ya fue desaprovisionado tras autorización de la OTIC. De igual forma no se restan las capacidades de estos servidores al no estar en escenario productivo o pruebas pero dan la visual a la entidad de que no están superando su holgura de crecimiento.

vCPUs		RAM - TB	Capacidad Disco
Consumos	**716**	**3.0 TB**	**130 TB**

Tabla 43 *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

A nivel de aplicaciones especializadas se realizó la validación de diversos componentes tecnológicos que se han identificado como en desuso, obsoletos o alojados en máquinas virtuales desasignadas o sin acceso por no asignación de interfaces de red, por lo cual se realizó actualización de inventario de componente virtualizado y su impacto a nivel de aplicación, esto permitió definir procesos para exclusión de estos como complemento de los procesos de afinamiento de máquinas virtuales asociadas a aplicaciones, así como la atención de requerimientos e incidentes asociados a aplicaciones misionales y funcionales JAVA y .Net.

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

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

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

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

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

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

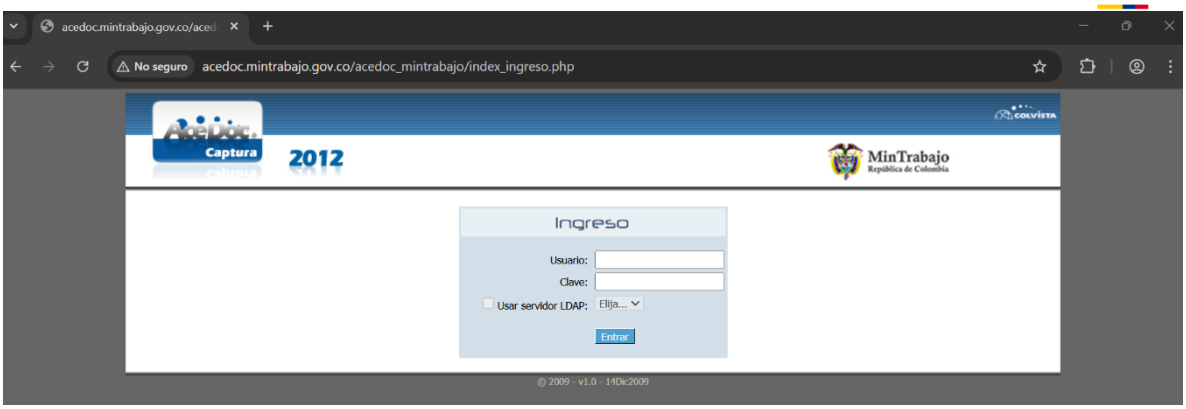


Ilustración 71 Nuevo entorno ACEDOC

Se adjunta la información de gestión de casos por categoría del servicio de aplicaciones especializadas.

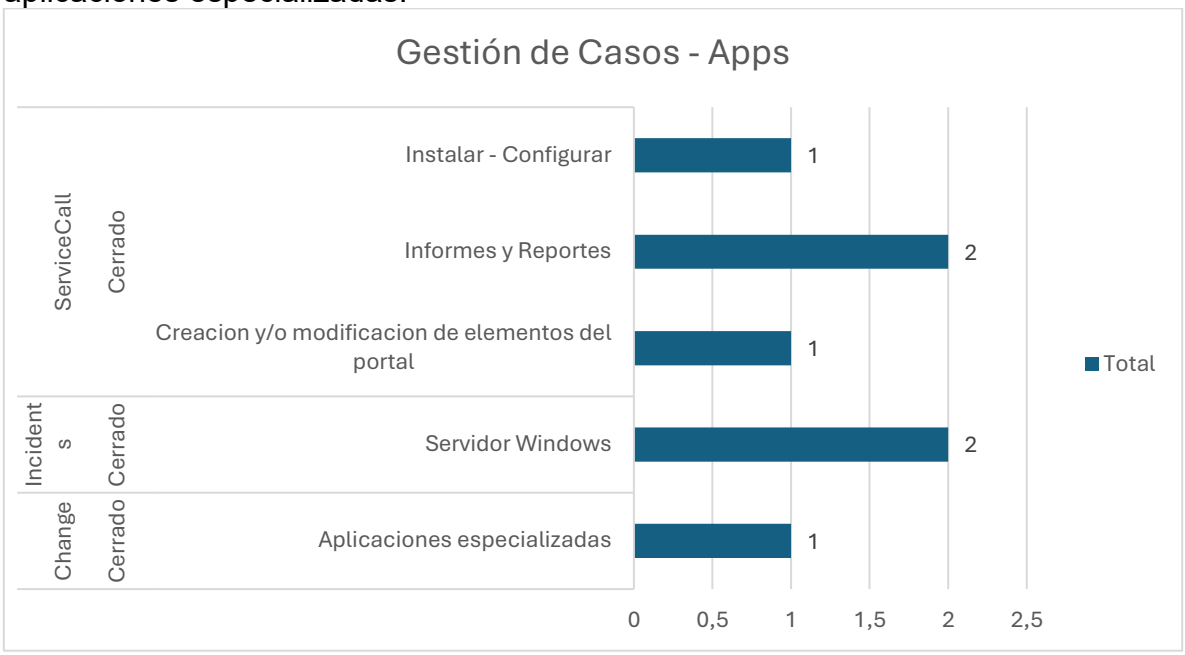


Ilustración 72 Gestión Apps Especializadas

Migración Aplicaciones .NET

Se comunica que la información suministrada de lideres funcionales fue remitida en noviembre del año anterior y se desconocía si los líderes de estos aplicativos aún conservan su rol o si de lo contrario continúan ejerciendo este rol dentro de la entidad, esto en el marco de los cambios organizacionales que tiene la entidad constantemente. Por ende, se solicitó confirmación a la coordinación de Soporte Informático con el fin de corroborar esta información ya suministrada para realizar un solo contacto y evitar reprocesos en la comunicación hacía las áreas funcionales.

Es importante mencionar que este ejercicio se realiza de esta forma ya que la dinámica para cada aplicación a nivel de migración no sería la misma, por lo cual una sesión con todas las personas de todas las áreas con sistemas de información distintos que no interoperan entre sí no sería totalmente productiva para el ejercicio de la migración, por lo cual se solicitó a la entidad esta información para realizar sesiones y seguimientos independientes a cada área funcional. El catálogo de sistemas de información fue actualizado de manera satisfactoria de la mano de la OTIC.

También es importante para nosotros como proveedor de servicios tecnológicos abrir estos espacios con las áreas funcionales de manera independiente, porque abre las puertas a una comunicación más fluida como administradores técnicos de los repositorios de estas aplicaciones, ya que permite mantener un canal de comunicación directo, actualización de fichas de servicio e identificar los actores necesarios para socializaciones con las gestiones ITIL, por ende es importante establecer estos canales de comunicación directos no solo para las pruebas de migración, sino también para conocer a detalle la dinámica de las áreas con los sistemas de información y articular la gestión realizada desde las gestiones ITIL con cada área responsable de cada aplicativo que se traduce en un CI dentro de la herramienta de gestión ARANDA.

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

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

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

Actualmente solo restan las aplicaciones Observatorio, nómina y cobro coactivo para migración a nuevo entorno. De igual forma por solicitud de la entidad, se dan de baja las siguientes aplicaciones:

- Censo Sindical
- BIBLIOTECA VIRTUAL DE TRABAJO
- BVT
- MIGESTION
- SIPGES
- SIMPC

Se sostuvo reunión con área de nómina y su proveedor y comparten las nuevas capacidades para dar continuidad al proceso de migración de la aplicación de nómina. Las máquinas virtuales fueron aprovisionadas de manera satisfactoria y se está a espera de configuración conjunta con el proveedor de la aplicación.
Se socializó el estado final a nivel de arquitectura con la entidad:

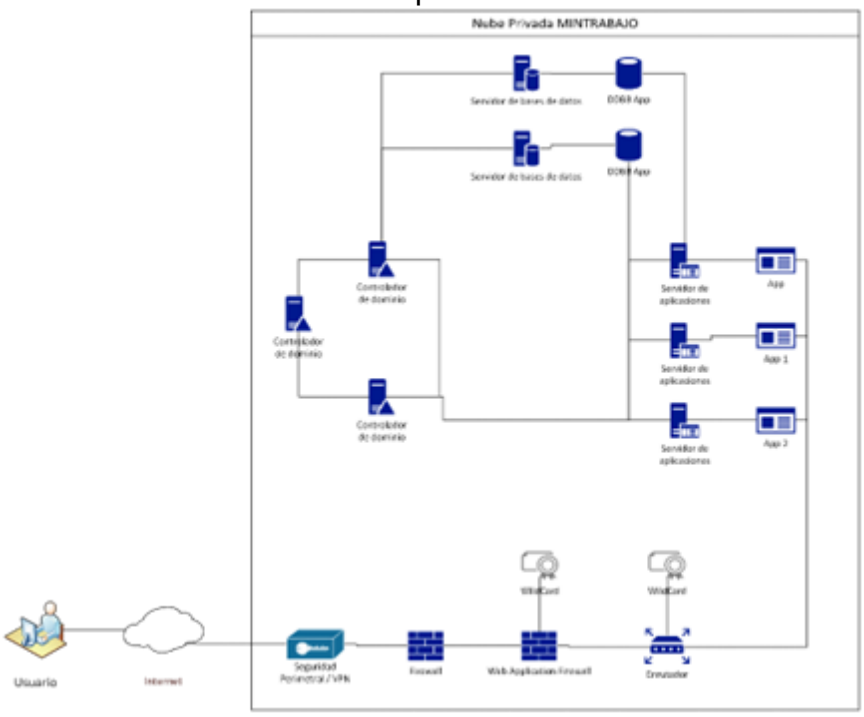


Ilustración 73 Arquitectura final Apps

Y la reorganización de los sitios de manera independiente:

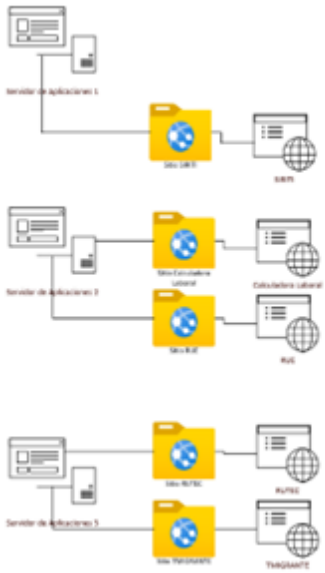


Ilustración 74 Distribución Sitios IIS

Haciendo énfasis en los siguientes ítems:

- Renovación tecnológica de los entornos productivos que contienen las aplicaciones especializadas de la entidad.
- Independizar las aplicaciones para garantizar un espacio individualizado por sistema de información.
- Segmentar el tráfico de red para cada aplicación o sistema de información.
- Suprimir la dependencia entre sistemas de información a nivel de controles de cambios.
- Remediar y evitar vulnerabilidades por versionamiento de componentes obsoletos.
- Mejora significativa en el performance de cada sistema de información.

Migración Portal Web

En atención a los compromisos definidos en la sesión del día 26 de febrero de 2025 categorizados de la siguiente forma:

- Se realizó la migración de forma exitosa a versión 7.3 sin afectación del servicio o corrupción de información
- Envío de Información/Ajustes por parte del equipo de Empleo sobre los tableros de FILCO publicados en el ambiente de pruebas de la página web de la entidad para que los cambios puedan aplicarse en el marco de la migración y puedan salir a producción con la nueva versión del portal. Se sostiene reunión a espera de formalización de los ajustes requeridos

- La entidad se encuentra en validación para creación de un equipo de experiencia de usuario 100% Ministerio del trabajo.
- La revisión de links rotos sigue en cabeza de la entidad.
- Actualmente se encuentra en fase de pruebas el versionamiento de LifeRay 7.3, Tomcat y versión de Oracle DB 19c.
- Se ejecuta paso a producción de las últimas versiones mencionadas en julio de 2025 de manera satisfactoria y sin errores en su despliegue.
- En etapa de pruebas para versión 7.4.
- Se está apoyando el desarrollo de un nuevo Organigrama para publicación en el portal. En validación de plantillas.
- Se están apoyando procesos de creación y templates para nuevos micrositios, así como actualización de la imagen institucional en todo el portal.
- Se ejecuta migración de versión en febrero 2026 de manera correcta, finalizando con todas las actualizaciones de versión del portal.

IBM-Gestor Documental

A nivel de mantenimientos del gestor documental no se realizaron actividades técnicas de mantenimiento en el marco de proceso de afinamiento y optimización, esto de acuerdo con la solicitud de ejecución por parte de la entidad, se plasman como evidencia los siguientes procedimientos:
Se hace entrega de información que justifica los procesos de mantenimiento del gestor documental

Plataforma – Aplicaciones

- Consultas lentas a los índices sobre los objetos de búsqueda de las tareas que se tiene en el portal de trabajo.
- Lentitud en la carga de información sobre las diferentes pantallas del proceso.
- Tener instancias innecesarias activas de proceso, generan peso a la aplicación ya que tiene toda la información cargada en el cache del servidor.
- No realizar borrado de los Documentos temporales de los File System en los diferentes servidores, se llenarían los espacios de almacenamiento y no permiten carga de más documentos y ejecución correcta de la plataforma.
- El no reinicio de las diferentes instancias del servidor de aplicaciones, ocasiona que se queden hilos pegados y hace que el procesamiento de los servidores físicos, estén en un alto procesamiento, esto genera lentitud y bloqueo de la plataforma.
- Se realiza ejecución productiva del módulo de envío de notificaciones el cual permite que el usuario tenga visibilidad de que radicados posee hace más de tres meses sin interacción y envía reporte notificando de que

serán inactivadas de su perfil con el objeto de liberar la carga transacciona de la base de datos de la aplicación.
- Se ha observado un alto flujo de transacciones hacia la base de datos en comparación a meses anteriores, lo cual genera degradación del servicio si se analizan los aspectos como transacciones inactivas, sesiones sin tráfico, radicados sin gestión, alto flujo de carga documental.
- Se está explorando alternativas de redistribución de capacidades así como distribución de licenciamiento para optimizar la carga de los servidores.

La falta de actualización del Caché (componente de hardware o software que guarda datos para que las solicitudes futuras de esos datos se puedan atender con mayor rapidez) de las diferentes instancias de proceso de las JVM's de los servidores de aplicación, generarían HeapSize, y pondría la memoria del servidor en alto consumo.

Este evento de concurrencia que se está presentando corresponde a que el número de sesiones que ingresan a la base de datos por medio del usuario BPMDBA estén consultando repetidamente el objeto tabla LSW_TASK el cual almacena las tareas creadas por el sistema BPM, sumando el tamaño actual de la tablas la operaciones normales se irán degradando (Tiempo de ejecución) de manera paulatina, es necesario realizar los procesos de borrado, desfragmentación y reconstrucción de índices para que las consultas sean más rápidas sobre estos objetos.

Uno de los objetivos que se tienen en el mantenimiento es poder eliminar las instancias de tipo 2 y 4 lo anterior es necesario para eliminar registros innecesarios sobre la tabla BPMDBA.LSW_BPD_INSTANCE, al tener menos registros redundantes la búsqueda de los registros será más optima y los tiempos de resolución de consultas (Querys) de la aplicación serán mucho mejores. Lo anterior debe ser acordado con el cliente según los tiempos de retención.

Los tamaños de los tablespaces tienden a consumir más espacio antes de los periodos de los mantenimientos, aunque los valores de uso de los tablespaces están en valores de alerta y es necesario mantener valores amplios de estos objetos para periodos de alta demanda transaccional de la aplicación, esto garantiza que las transacciones y procesos del gestor documental puedan ser gestionados óptimamente y garantizando la disponibilidad 100%. Históricamente los tiempos de resolución de solicitudes de la aplicación mejoran considerablemente después de las tareas de mantenimiento, los tiempos pueden mejorar de manera significativa si se realiza los mantenimientos de forma periódica, esto con el fin de mantener la aplicación en todos sus componentes funcionando de la mejor manera para brinda un mejor servicio.

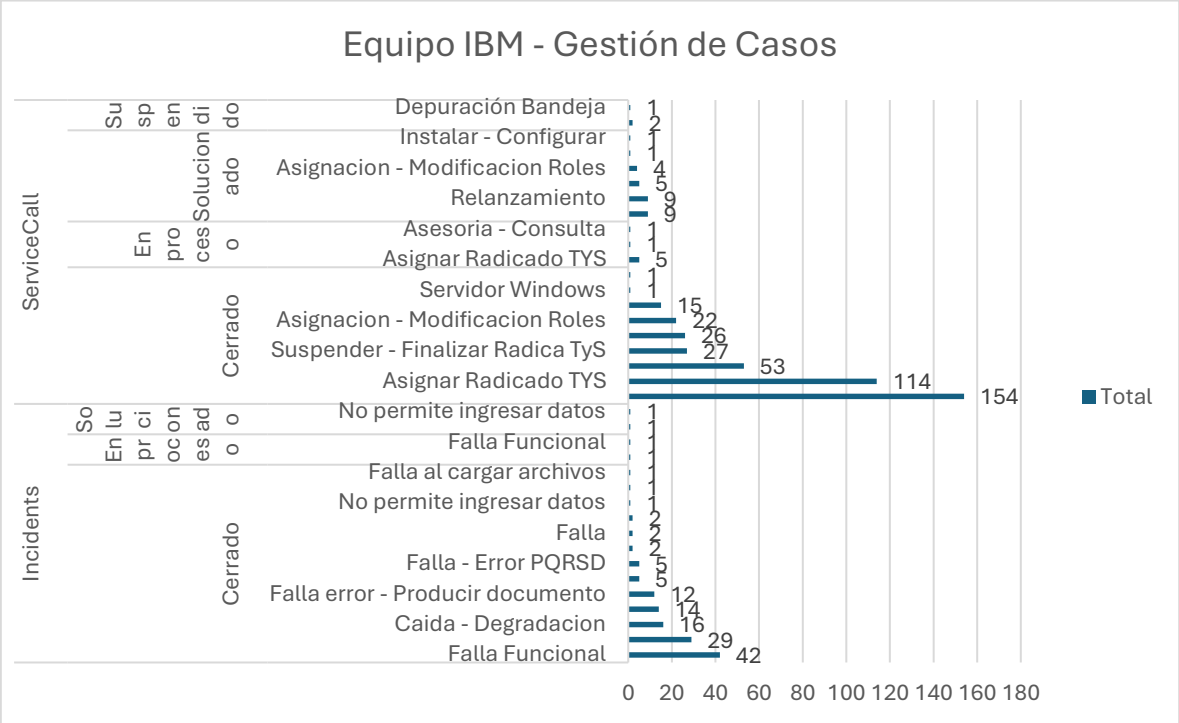


Ilustración 75 Gestión Casos IBM

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 (109 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.
- Radicar una solicitud - Depuración de Bandeja (54 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 (56 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.
- Falla radicación (56 casos): Requerimientos a fallas en los procesos de radicación, errores asociados a este proceso, ya sea por mal procedimiento, problemas en conectividad, falta de roles para ejecución de actividades o temas aislados que se tratan de manera diferencial.

De acuerdo con la serie de sesiones sostenidas con el equipo IBM y el Ministerio del Trabajo, se remiten las capacidades mínimas para el aprovisionamiento de un ambiente de pruebas en condiciones para la entidad, ya que actualmente el escenario de licenciamiento no permite el aprovisionamiento de este entorno.

El objetivo de esta arquitectura es asegurar la capacidad para:

Simular escenarios de pruebas de carga.

- Realizar pruebas exhaustivas de actualizaciones de los diferentes componentes.
- Soporte de alta transaccionalidad y balanceo.

Maquinas Gestor Desarrollo - Pruebas				
Rol Servidor	Cores por Server	Tipo de licenciamiento	PVCs por Core / PVU's por Core	total
WASND	6	PVU	70	420
WASND	6	PVU	70	420
BUS - AppConnect	6	PVU	70	420
ODM	4	PVC	5	20
DATACAP	5	PVC	5	25
DATACAP	5	PVC	5	25
BAW	6	PVC	5	30
BAW	6	PVC	5	30
Filenet FRONT	7	PVC	5	35
Filenet BACK	7	PVC	5	35
			Total PVU's	1260
			Total PVC's	200

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

Mes	Suma de Total Instancias
Diciembre 2025	109540
Enero 2026	83242
Febrero 2026	148858
Marzo 2026	151041
Abril 2026	139558
Total acumulado	632.239

Tabla 44 *Suma Instancias*

Mes	Suma de Total Documentos
Diciembre 2025	174277
Enero 2026	136435
Febrero 2026	177295
Marzo 2026	202780
Abril 2026	175530
Total acumulado	866.317

Tabla 45 Total Docs

Mes	Suma de Total radicados
Diciembre 2025	**59671**
Enero 2026	53821
Febrero 2026	68311
Marzo 2026	74463
Abril 2026	68784
Total, acumulado	325.050

Tabla 46 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 47 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 76 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 realizó el cargue de los archivos planos recibidos vía FTP desde el Ministerio de Salud dicha tarea se realizó sobre las tablas que ya están definidas para ser cargadas en la Base de Datos de PILA.

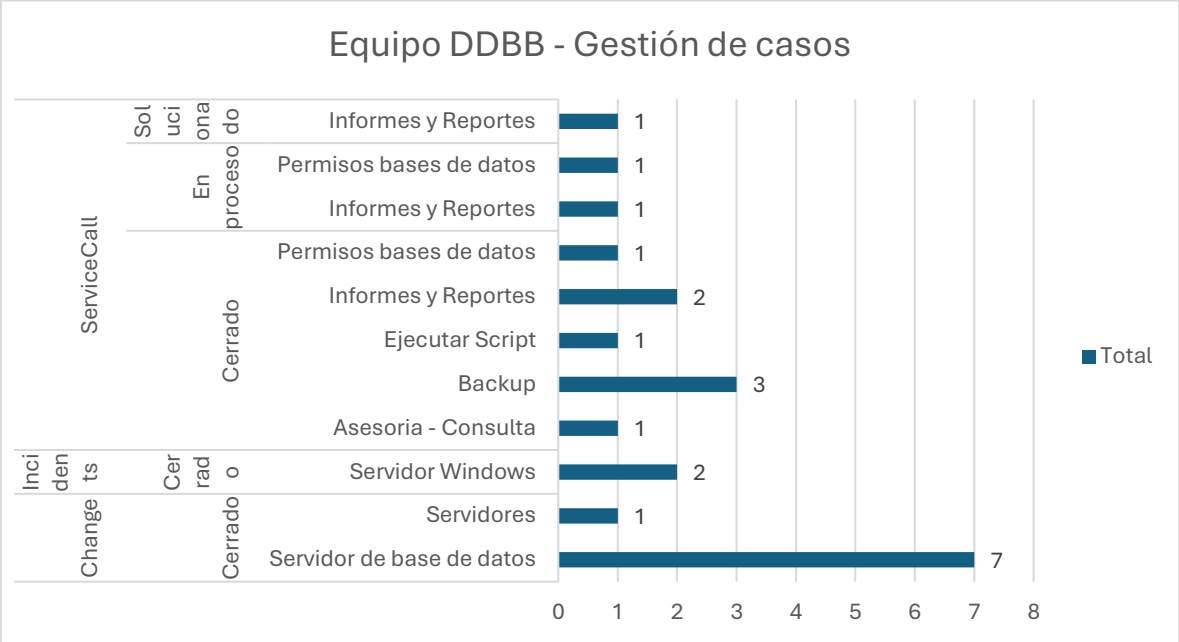


Ilustración 77 Gestión DDBB

A nivel de los procesos de migración y actualización de versión de MSSQL Server, ya se encuentran aprovisionados los servidores y ya se realizaron las pruebas de restauración en nuevos entornos, se garantiza interoperabilidad con las DDBB de MSSQL que consumen servicios de Oracle y ya se encuentran varias bases de datos en el nuevo entorno y se encuentran productivas. Durante el mes de Julio se migró casi el 85% de las DDBB de producción y pruebas y se encuentran operando en los nuevos servidores de MSSQL Server. Debido al cambio de versión, se realizaron cambios dentro de las configuraciones para obtener una compatibilidad completa en versión 2022. Todo de manera satisfactoria y sin indisponibilidades no controladas.

- Estado de las Bases de Datos – Oracle Gestor Documental

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

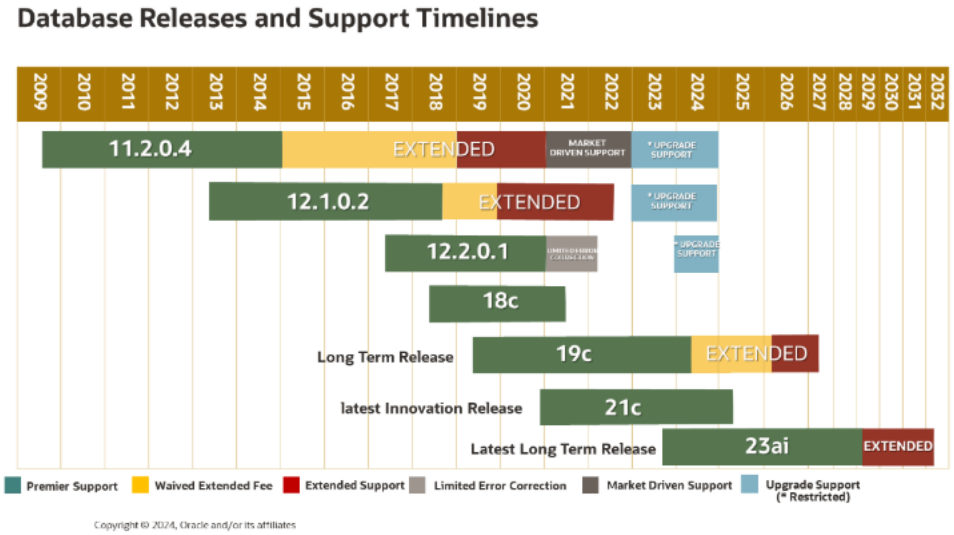


Ilustración 78 Estado Bases de Datos

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	*poliferay*	*Liferaypro, liferaypru, filcodev, filcopru*	*Producción - desarrollo*

Tabla 48 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 abril 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.

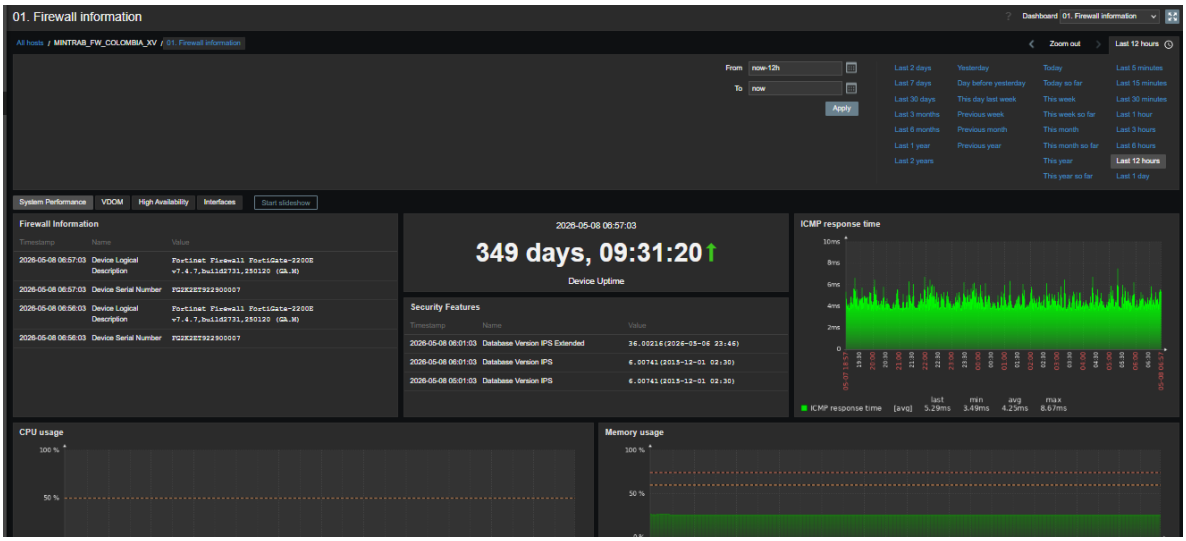


Ilustración 79 Firewall de nueva generación.

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 abril. 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 adaptada al gráfico
Tendencia general	El comportamiento del tráfico es estable y predecible durante todo el período analizado, con oscilaciones regulares y sin picos abruptos. No se identifican patrones anómalos asociados a eventos de exfiltración, abuso de red o transferencia masiva no autorizada.
Volumen promedio	El volumen total diario (tráfico enviado + recibido) se mantiene dentro de rangos operativos esperados, con valores aproximados entre 5 TB y 10 TB. La predominancia del tráfico recibido es coherente con un entorno institucional orientado al consumo de servicios externos y plataformas centralizadas.
Tráfico recibido (azul)	El tráfico recibido muestra variaciones periódicas, con picos que alcanzan aproximadamente 5–10 TB en determinados días. Este comportamiento es compatible con consumo de servicios en la nube, acceso a portales institucionales, actualizaciones de plataformas y sincronización de información corporativa.
Tráfico enviado (amarillo)	Se mantiene estable y controlado, con valores promedio cercanos a 1 – 5 TB diarios. No se evidencian incrementos súbitos que sugieran cargas atípicas, respaldos masivos no planificados o posibles fugas de información.
Días de mayor actividad	Se identifican incrementos puntuales del tráfico recibido hacia la segunda y tercera semana del período analizado, sin ruptura de tendencia. Estos picos son consistentes con ventanas operativas, procesos de actualización, sincronización de datos y uso intensivo de servicios como plataformas colaborativas y portales gubernamentales.
Días de menor tráfico	Se identifican valles claros en el tráfico total, asociados probablemente a fines de semana, menor actividad operativa o mantenimientos programados, sin impacto negativo sobre la disponibilidad del servicio.
Comportamiento esperado / Riesgo	El patrón de tráfico refleja un entorno controlado, balanceado y estable, sin señales de congestión, saturación o actividad maliciosa. Desde una perspectiva de gestión del riesgo, el comportamiento observado se considera normal y aceptable, sin indicios de compromiso a la confidencialidad, integridad o disponibilidad de la información.

Tabla 49 Tendencia de uso de ancho de banda

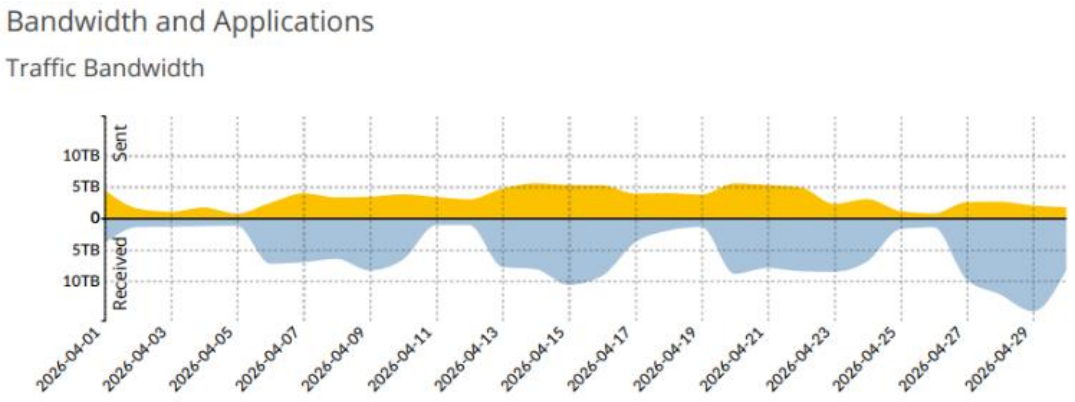


Ilustración 80 Comportamiento ancho de banda

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 abril. La identificación de los 10 principales usuarios de ancho de banda proporciona información valiosa sobre los patrones de uso de la red y los puntos críticos de congestión.
A continuación, se detallan los hallazgos más relevantes:

N°	Usuario/IP	Total, de datos (aprox.)	Observaciones
1	172.25.0.131	**47.72 TB**	Tráfico extremadamente alto, servidor de almacenamiento, backup (MINTRABCKEXEC.mintrabajo.loc).
2	172.20.22.167	**16.68 TB**	
3	172.20.22.27	**11.92 TB**	Servidos de aplicaciones
4	172.20.22.251	**10.97 TB**	Documental Usuario con alto consumo. Requiere validar si se relaciona con actividades administrativas o técnicas (por ejemplo, transferencia de informes o copias de respaldo).
5–10	Resto de IPs internas	Entre **1–2 TB** cada una	Tráfico normal para estaciones o servidores secundarios. "ADMINBCK" (10.º) destaca como usuario de **respaldo**, con ~1 TB.

Tabla 50 usuarios con mayor consumo de ancho de banda

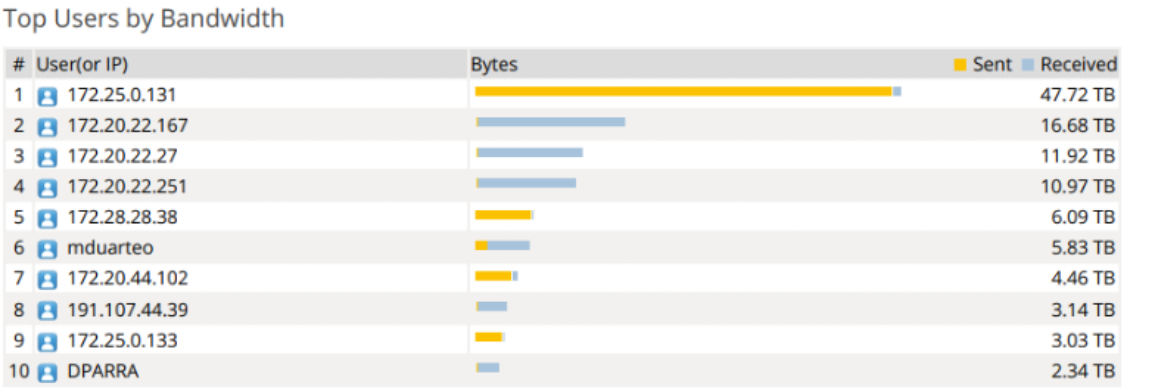


Ilustración 81 Tendencia de uso de ancho de banda

Top de usuarios por número de sesiones

La imagen corresponde al apartado "Top Users by Sessions" del informe perimetral de abril 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.

Top Users by Sessions

#	User (or IP)	Sessions
1	172.25.0.5	196,246,317
2	mduarteo	86,843,914
3	172.20.22.234	31,859,636
4	FORTINET	18,769,998
5	172.20.22.3	17,806,742
6	172.16.27.125	16,583,944
7	172.20.22.40	15,219,727
8	192.168.133.203	12,748,812
9	172.20.22.228	12,615,177
10	172.16.34.125	12,065,890

Ilustración 82 Top de usuarios por números de sesiones

Análisis Top Users by Sessions

N°	Usuario/IP	Sesiones	Observaciones
1	**172.25.0.5**	**196.246.137**	IP con la mayor cantidad de conexiones. Muy probablemente corresponde a un **servidor interno o sistema de autenticación/proxy**, encargado de canalizar solicitudes de múltiples usuarios.
2	**mduarteo**	86.843.914	Usuario con actividad muy elevada. Puede estar vinculado a gestion de alguna plataforma(Mireya Duarte Osma)
3	**172.20.22.234**	31,859,636	Servidor interno asociado a un controlador de dominio.
4	**FORTINET**	**18,769,998**	Tráfico legítimo del sistema de seguridad (firewall, antivirus o gestión de eventos).
5	**Resto de IPs internas (rango 172.16–172.22)**	Entre **12 y 18 millones de sesiones**	Volumen esperado para servicios de autenticación, proxy, o endpoints activos de red.

Tabla 51 Top de usuarios por sesiones

Top Applications by Bandwidth

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

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	HTTPS			62.71 TB
2	TCP/31031			51.26 TB
3	SMB			24.72 TB
4	TCP/UDP_1436			16.68 TB
5	TCP/445			12.42 TB
6	TCP/902			10.72 TB
7	SYSLOG			8.50 TB
8	TCP/1521			8.38 TB
9	Microsoft.SharePoint			7.90 TB
10	Microsoft.365.Portal			7.46 TB

Ilustración 83 Top de aplicaciones

Aplicación	Tamaño	Descripción
2HTTPS	62.71 TB	Tráfico web cifrado — servicios cloud, correo, portales institucionales. Representa la base del tráfico corporativo seguro.
3. SMB (Server Message Block)	24.72 TB	Protocolo de compartición de archivos en red. Muestra alto uso de repositorios compartidos internos.
4. TCP/445	12.42 TB	Asociado también a SMB y autenticación Windows (Active Directory). Indica intenso intercambio de archivos y autenticaciones.
1. TCP/902	10.72 TB	Puerto comúnmente usado para VMware ESXi (administración de máquinas virtuales). Indica alto volumen de sincronización o replicación de entornos virtualizados.
5. SYSLOG	8.50 TB	Transmisión de logs desde dispositivos hacia el FortiAnalyzer o SIEM. Tráfico esperado y saludable para monitoreo de seguridad.
6. TCP/1521	8.38 TB	Puerto usado por Oracle Database. Indica consultas o réplicas intensivas en bases de datos institucionales.

Tabla 52 Top de aplicaciones

Top 15 Authenticated Logins by VPN Connections

La imagen corresponde al apartado “Authenticated Logins” del informe perimetral de abril 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	2026-04-01 07:28:16	188	187:24:06
2	ediazb	ssl-tunnel	2026-04-06 18:06:56	99	47:29:43
3	ypineros	ssl-tunnel	2026-04-01 13:13:07	80	135:45:48
4	idjimenez	ssl-tunnel	2026-04-01 09:49:36	79	37:15:50
5	ivaldes	ssl-tunnel	2026-04-01 09:57:42	74	58:15:51
6	jmaestre	ssl-tunnel	2026-04-01 14:51:45	73	116:43:40
7	magarcia	ssl-tunnel	2026-04-01 03:12:27	72	46:02:58
8	RMURCIA	ssl-tunnel	2026-04-01 05:42:44	71	96:16:21
9	mvanegasc	ssl-tunnel	2026-04-01 17:44:22	70	112:57:21
10	srvxroadinterop	ssl-tunnel	2026-04-01 00:04:22	69	109:04:09
11	agente6	ssl-tunnel	2026-04-01 00:02:48	64	137:57:34
12	eordonez	ssl-tunnel	2026-04-01 18:01:18	63	90:47:37
13	cmcamelo	ssl-tunnel	2026-04-01 08:24:16	63	168:34:39
14	dosma	ssl-tunnel	2026-04-06 09:03:35	62	58:48:32
15	jecheverryb	ssl-tunnel	2026-04-02 03:16:48	62	46:59:54

Ilustración 84 Top de Autenticación

Indicador	Descripción actualizada
Tipo de conexión	El 100 % de las sesiones identificadas se realizaron mediante SSL-Tunnel, evidenciando el uso de la VPN segura FortiGate como mecanismo principal de acceso remoto a la red institucional.
Usuarios más activos (por duración)	Los usuarios con mayor tiempo acumulado de conexión son: contaccenter (~187:24 h), cmcamelo (~168:34 h), ypineros (~135:45 h), agente6 (~137:57 h) y srvxroadinterop (~109:04 h). Este comportamiento es consistente con roles operativos, soporte extendido y actividades de monitoreo o administración remota.
Mayor duración total	El mayor tiempo acumulado corresponde a contaccenter (~187 horas), seguido de cmcamelo (~168 horas) y agente6 (~137 horas), lo que indica accesos persistentes asociados a operación continua o soporte técnico crítico.
Mayor cantidad de conexiones	Los usuarios con mayor número de conexiones son: contaccenter (188 conexiones), ediazb (99), ypineros (80), idjimenez (79) y iviales (74). Este patrón es típico de usuarios con múltiples reconexiones o turnos operativos distribuidos.
Duraciones elevadas (>100 h)	Se identifican usuarios con actividad superior a 100 horas: contaccenter, cmcamelo, ypineros, agente6 y srvxroadinterop, lo cual debe estar alineado con funciones de operación continua, soporte o monitoreo 24/7.
Duraciones medias (50 h – 100 h)	Usuarios con uso recurrente de la VPN: RMURCIA (~96 h), eordonez (~90 h), iviales (~58 h) y dosma (~58 h). Corresponden a trabajo remoto frecuente y soporte técnico periódico.

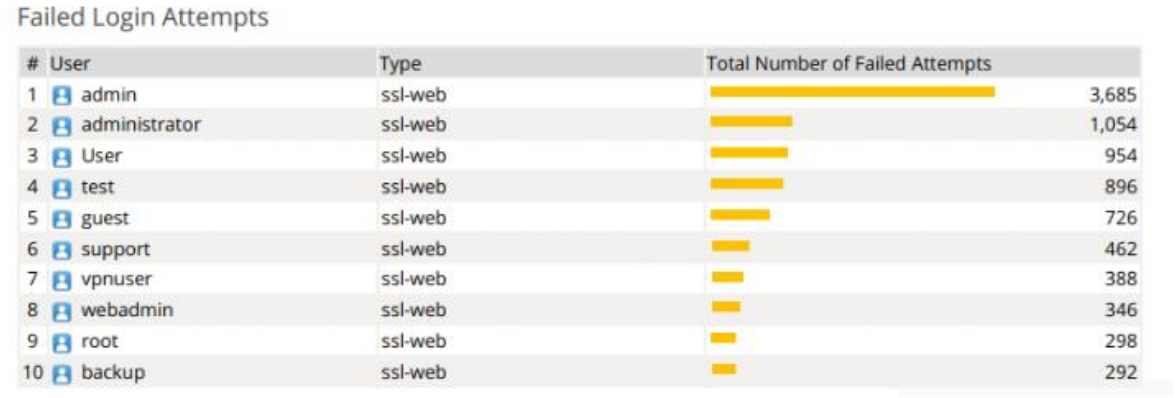
Duraciones bajas (<50 h)	Usuarios como ediazb (~47 h), magarcia (~46 h), jecheverryb (~46 h) e idjimenez (~37 h) presentan accesos más puntuales, lo que sugiere uso ocasional o actividades específicas de soporte.

Tabla 53 Consolidado de indicadores

Failed Login Attempts by User

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

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


Failed Login Attempts

#	User	Type	Total Number of Failed Attempts
1	admin	ssl-web	3,685
2	administrator	ssl-web	1,054
3	User	ssl-web	954
4	test	ssl-web	896
5	guest	ssl-web	726
6	support	ssl-web	462
7	vpnuser	ssl-web	388
8	webadmin	ssl-web	346
9	root	ssl-web	298
10	backup	ssl-web	292

Ilustración 85 sesiones fallidas

Análisis
Durante abril 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 abril de 2026, se generaron 66 eventos analizados, los cuales fueron limpiados de algún tipo de amenazas

Scan Statistics - Last 4 Weeks

Inputs	Pending	Processing	Malicious	High Risk	Medium Risk	Low Risk	Clean	Other	Total
Device	0	0	0	0	0	0	66	0	66
Adapter	0	0	0	0	0	0	0	0	0
On Demand	0	0	0	0	0	0	0	0	0
Network Share	0	0	0	0	0	0	0	0	0
Sniffer	0	0	0	0	0	0	0	0	0
URL	0	0	0	0	0	0	0	0	0
All Sources	0	0	0	0	0	0	66	0	66

File Scan - Last 4 Weeks

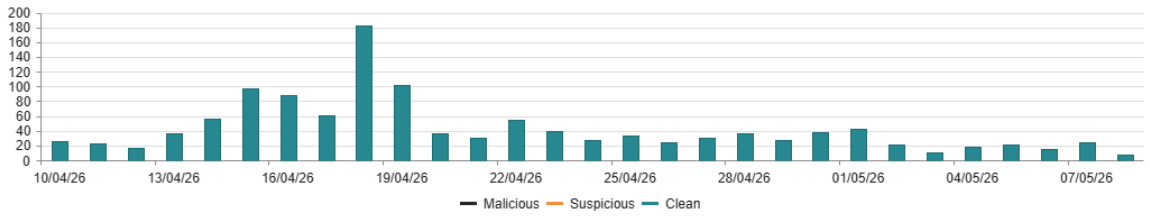


Ilustración 86 Reporte mensual

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

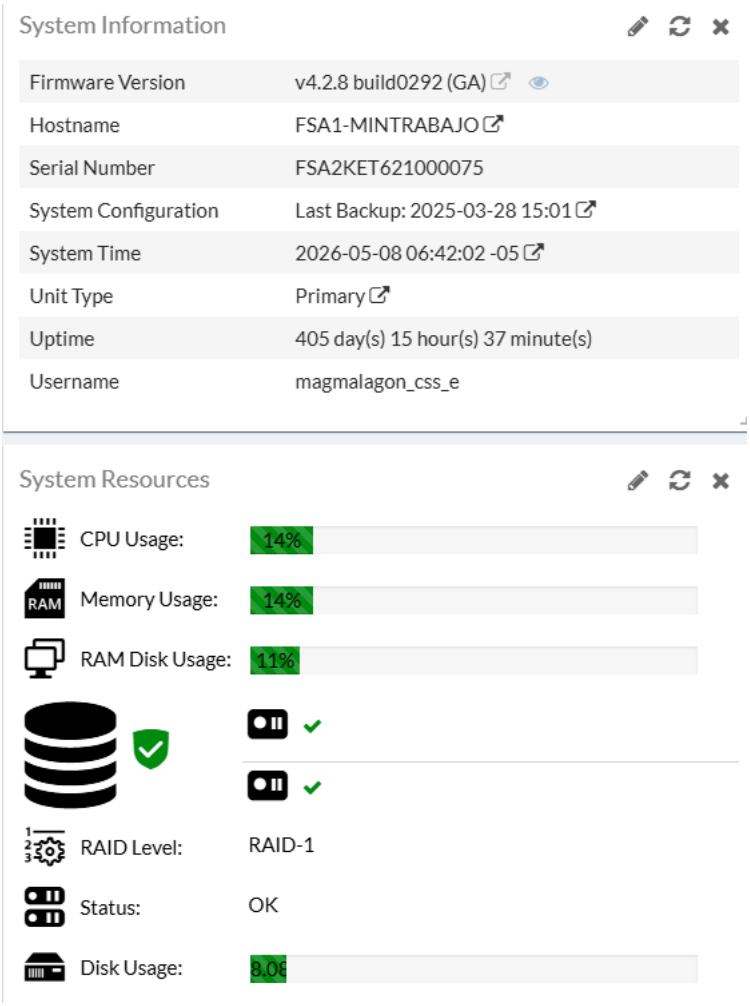


Ilustración 87 Captura de pantalla perfomance

Licencia Sandbox

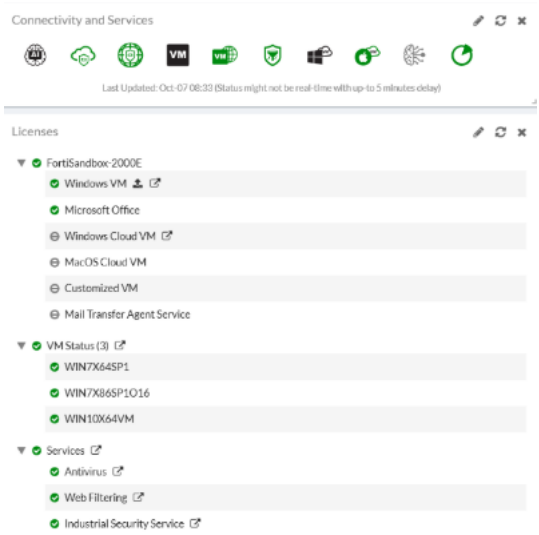


Ilustración 8889 licencia sandbox

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

El presente informe consolida los hallazgos y métricas operacionales del Centro de Operaciones de Seguridad (SOC) del Ministerio de Trabajo durante el mes de abril de 2026, con base en la telemetría procesada por la plataforma FortiSIEM.

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

4.584	431	6.864	200 TB
EPS Pico máximo (eventos/segundo)	EPS Promedio sostenido del mes	Incidentes totales detectados	Tráfico total procesado (ISAKMP)

HALLAZGO PRIORITARIO: 767 eventos de 'Large Outbound Transfer'

Se detectaron 767 eventos de transferencia saliente masiva de datos. Este indicador, combinado con los 5.022 casos de violaciones de política web, constituye el perfil de riesgo más relevante del período. Se requiere correlación con usuarios específicos y validación de DLP (Data Loss Prevention).

Conclusiones del período:

•El SIEM FortiSIEM operó con estabilidad, procesando eventos dentro de márgenes normales (pico 4.584 EPS, promedio 431 EPS).

•El tipo de incidente más frecuente fue 'Website access policy violation' con 5.022 casos, indicando brechas en la aplicación de la política de uso aceptable.

•Se detectaron 767 eventos de transferencia saliente de gran volumen, un indicador de riesgo de exfiltración que requiere investigación.

•Office 365 registró 1.075 eventos de 'SendAs/SendOnBehalf', lo que puede indicar suplantación de identidad en el correo corporativo.

•El tráfico de red está dominado por ISAKMP (VPN IPsec) con 200 TB, indicando uso intensivo de acceso remoto seguro.

•Los servidores monitoreados presentan alta disponibilidad con latencia mínima (RTT promedio 1 ms), sin degradaciones reportadas.

3.1.6.3.1 Métricas de Events Per Second (EPS)

Los Events Per Second (EPS) son el indicador principal de carga operacional del SIEM.

Un EPS elevado sostenido puede generar pérdida de eventos si supera la capacidad de ingesta de la plataforma; un EPS promedio muy bajo puede indicar fuentes de log desconectadas.

Métrica EPS	Valor Abril 2026	Evaluación
Pico máximo de eventos indexados	**4.584 EPS**	Normal – no supera umbral crítico de la plataforma
Promedio sostenido mensual	**431 EPS**	Estable – comportamiento dentro de márgenes normales
Relación Pico / Promedio	**10.6x**	Indica eventos en ráfaga (picos de actividad anómalos en fechas específicas)

Tabla 54 métricas EPS

Dispositivos Fuente de Eventos (Reporting Devices)

El volumen de eventos generados por cada dispositivo permite identificar fuentes de alta carga y validar que todos los activos críticos están enviando telemetría al SIEM. La ausencia de un dispositivo en los reportes puede indicar una fuente de log desconectada o una brecha de visibilidad.

- Los dispositivos con mayor volumen de EPS generado son los firewalls FortiGate (VD_DMZ, VD_INTERNET, VD_MINTRAB) y la plataforma TrendMicro WFBS.
- Se recomienda establecer una línea base (baseline) de EPS por dispositivo para detectar desviaciones que indiquen comprometimiento o mal funcionamiento.
- Validar mensualmente que el inventario de dispositivos fuente en FortiSIEM coincide con el inventario de activos TI del ministerio.

3.1.6.3.2 Incidentes por Tipo

Los incidentes registrados en FortiSIEM durante abril de 2026 provienen tanto de reglas de correlación automáticas como de reglas configuradas manualmente. La siguiente tabla presenta los tres tipos de incidentes con mayor frecuencia:

#	Tipo de Incidente	Casos	Severidad	Análisis y Recomendación
1	**Website Access Policy Violation**	**5.022**	**MEDIA**	Usuarios acceden a categorías bloqueadas por política. Indica fallas de cumplimiento de AUP. Requiere revisión de categorías y campaña de concientización.
2	**Office365: Mailbox SendAs / SendOnBehalf**	**1.075**	**ALTA**	Posible suplantación de identidad en correo corporativo o delegación de buzón no autorizada. Verificar si las delegaciones son legítimas con el área de RRHH/Legal.
3	**Large Outbound Transfer**	**767**	**ALTA**	Transferencias de datos salientes de gran volumen. Riesgo de exfiltración. Correlacionar con usuarios implicados (casanabriap, dtboyaca) e investigar destinos.

Tabla 55 Tipos de incidentes

RIESGO ALTO: Delegación de buzón en Office 365 (SendAs/SendOnBehalf)
1.075 eventos de delegación de correo en un mes es un volumen elevado para una entidad pública. Este tipo de configuración, si no es autorizada explícitamente, puede ser utilizada por un atacante que haya comprometido una cuenta para enviar correos suplantando a funcionarios del ministerio, incluyendo directivos. Se recomienda auditoría inmediata de delegaciones activas en Office 365.

3.1.6.3.3. Hosts e IPs Implicados

Los siguientes activos concentran la mayor parte de los incidentes detectados durante el período. Su presencia recurrente en múltiples tipos de incidentes es un indicador de que requieren atención prioritaria:

Tipo	Activo	Incidentes Asociados	Acción Recomendada
Host	**Mintrab02.mintrabajo.loc**	Múltiples tipos	Auditar actividad de usuario local, revisar parches pendientes y logs de autenticación
Host	**mintrab107.mintrabajo.loc**	Política web + transferencias	Identificar usuario asignado, aplicar DLP y revisar contenido transferido
Host	**mintrabgd08a.mintrabajo.loc**	Alta frecuencia de alertas	Determinar si es servidor o estación; evaluar aislamiento preventivo para análisis
IP Externa	**201.234.143.90**	Tráfico sospechoso	Verificar si es C2 conocido (Mirai), bloquear en perimetral si no está ya bloqueada
IP Interna	**172.20.22.40 / .3**	Origen frecuente en alertas	Identificar propietario del activo, revisar comportamiento en el SIEM los últimos 90 días

Tabla 56 Hosts e IPs Implicados

3.1.6.3.4. Usuarios con Mayor Actividad de Riesgo

Usuario	Patrón Detectado	Recomendación
casanabriap	Asociado a Large Outbound Transfer y alertas de política	Revisión de archivos transferidos, entrevista con el área de gestión humana, posible restricción temporal de accesos
dtboyaca	Incidentes recurrentes durante el mes	Análisis de actividad en el SIEM (últimos 90 días), correlación con solicitudes de acceso a información sensible
(Empty / Sin usuario)	Mayoría de los registros sin autenticación asociada	Revisar fuentes de log que no envían usuario; mejorar cobertura de autenticación en registros de eventos del sistema

Tabla 57 Usuarios con Mayor Actividad de Riesgo

3.1.6.3.5. Aplicaciones por Ancho de Banda

El análisis del tráfico de red de abril de 2026 muestra una infraestructura dominada por comunicaciones cifradas, servicios VPN corporativos y plataformas de seguridad cloud. El siguiente cuadro resume las aplicaciones de mayor consumo:

#	Aplicación / Protocolo	Total	Sent / Recv Predominante	Evaluación de Seguridad
1	**ISAKMP – IPsec VPN (Network.Service)**	**~200.94 TB**	Balanceado S/R	Muy elevado. Uso intensivo de túneles VPN site-to-site. Verificar que todos los túneles activos sean autorizados.
2	**TrendMicro WFBS (Cloud.IT)**	**~85.37 TB**	Enviado: 81.06 TB	Alto tráfico saliente hacia consola cloud de seguridad. Confirmar que el volumen corresponde solo a telemetría de endpoints.
3	**SSL/TLS v1.3 (Network.Service)**	**~77.04 TB**	Recibido: 67.81 TB	Normal – descarga de contenido HTTPS/cloud. Configurar inspección SSL en el firewall para visibilidad interna.
4	**DTLS – UDP cifrado (Network.Service)**	**~36.54 TB**	Recibido: 30.66 TB	Consistente con videoconferencia y colaboración (Teams/Zoom). Verificar que los destinos sean corporativos.
5	**SSL/TLS v1.2 + PQC (Network.Service)**	Relevante	Variado	Presencia de TLS 1.3 PQC sugiere compatibilidad con criptografía post-cuántica. Validar configuración intencional.

Tabla 58 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 abril 2026. Ofrece información valiosa sobre los patrones de disponibilidad de servidores en lo relacionado con la última fecha de reinicio. A continuación, se presentan los hallazgos más relevantes:
Los servidores con mayor tiempo de disponibilidad continua en los últimos 30 días sin presentar eventos son:

Hallazgos relevantes:

- Servidores como MINTRAB03 y MINTRAB94 presentan más de 190 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.

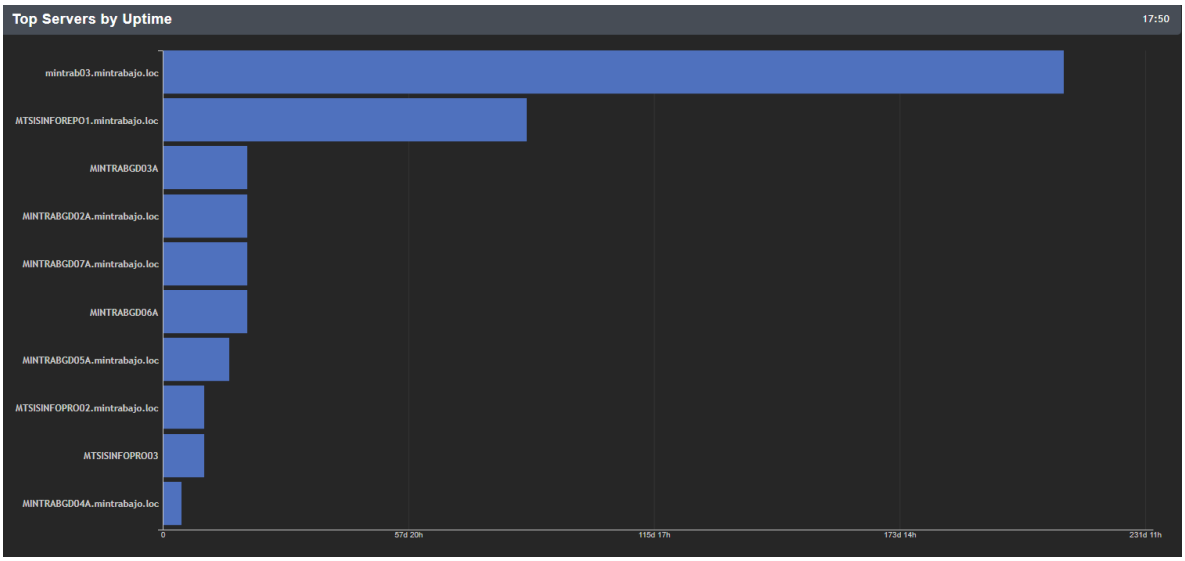


Ilustración 90 Detalle servidores

El período de abril de 2026 presenta un SOC operacionalmente estable en métricas de plataforma, pero con hallazgos de riesgo ALTO que requieren seguimiento activo por parte del Ministerio de Trabajo.

✓ La plataforma FortiSIEM opera con estabilidad. El pico de 4.584 EPS y el promedio de 431 EPS son coherentes con la capacidad contratada. La disponibilidad de servidores supera el 99.9% sin incidentes reportados.

! Los 767 eventos de 'Large Outbound Transfer' y los 1.075 eventos de delegación de buzón en Office 365 son los hallazgos de mayor riesgo. Ninguno ha sido cerrado formalmente a la fecha de este informe. Requieren investigación con prioridad ALTA.

→ Los 5.022 casos de violación de política web indican que las herramientas de bloqueo están funcionando, pero la cultura de uso aceptable requiere refuerzo. Se recomienda un programa de concientización mensual con métricas de evolución.

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

Durante el mes de abril 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.

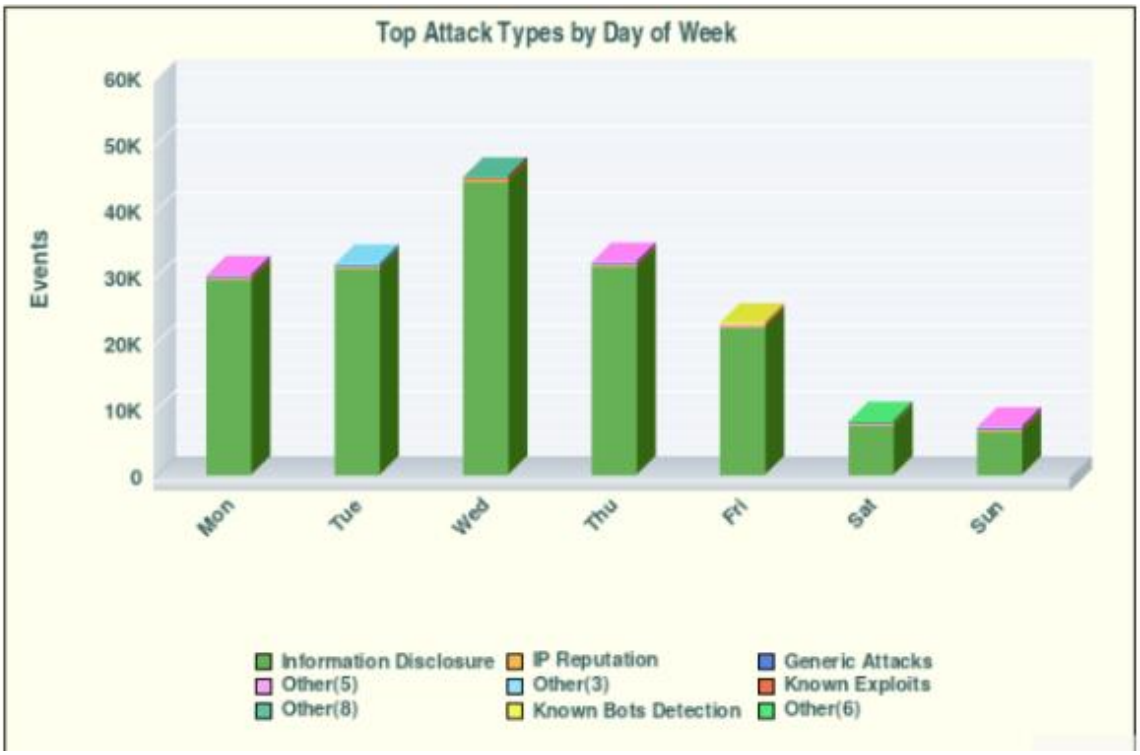


Ilustración 91 Top attack types

Análisis

Análisis	Descripción
Distribución de ataques por día	La mayor concentración de eventos se presenta entre **martes, miércoles y jueves**, alcanzando picos cercanos a **45.000 – 48.000 eventos**, siendo **miércoles el día con mayor volumen**. Esto evidencia una mayor actividad de ataques durante los días laborales de mayor operación.
Inicio de semana	El **lunes** registra aproximadamente **30.000 – 32.000 eventos**, lo que refleja un nivel alto de actividad desde el inicio de la semana, asociado a la reactivación de servicios institucionales.
Mitad de semana	Entre **martes y miércoles** se observa un incremento significativo (**~35.000 a ~48.000 eventos**), consolidando el miércoles como el punto máximo, lo que indica un **patrón intensivo de escaneo y explotación automatizada**.
Jueves	Se presenta una ligera reducción frente al pico del miércoles, con aproximadamente **33.000 – 35.000 eventos**, manteniéndose en niveles altos y estables.
Viernes	Se evidencia una disminución del volumen (**~25.000 eventos**), aunque continúa siendo representativo dentro del comportamiento semanal.
Fin de semana	Los **sábados y domingos** presentan una reducción significativa (**~8.000 – 10.000 eventos**), consistente con la menor actividad operativa y menor exposición de usuarios.
Tipo de ataques predominantes	Predominan los eventos de **Information Disclosure**, seguidos por **IP Reputation, Known Exploits y Generic Attacks**, lo que indica principalmente **recolección de información, escaneo automatizado y explotación de vulnerabilidades conocidas**.
Eventos asociados a reputación IP	Se mantienen eventos asociados a **IP Reputation**, provenientes de direcciones con historial malicioso, lo que confirma la presencia de **tráfico automatizado desde Internet**.
Interpretación de riesgo	El comportamiento corresponde a una **actividad constante, automatizada y no dirigida**, típica de servicios expuestos públicamente. No se identifican anomalías críticas ni campañas dirigidas, manteniéndose el riesgo en un nivel **controlado y esperado**.

Tabla 59 Tipo de ataque

3.1.6.5 Solución de Anti-DDoS

Durante el período del mes de abril, se registraron eventos 4 de ataques de denegación de servicio distribuido (DDoS) a las aplicaciones publicadas en internet por el Ministerio de Trabajo.

Top Attacked Subnets

Subnet	SPP	Direction	Drops	Events
PAGINA_MINTRABAJO	PAGINA_MINTRABAJO	Outbound	62	5
GESTOR_DOC_MINT	GESTOR_DOC_MINT	Outbound	35	2
SOMINTRABAJO	Acceso_Web	Outbound	1	1

Ilustración 92 Top de ataques

Análisis Detallado:

PAGINA_MINTRABAJO también muestra un número bajo de intentos salientes bloqueados (62), lo que sugiere riesgo bajo en aplicaciones web institucionales.

3.1.6.5.1 Login Fallidos

Durante el mes de abril 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 abril 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 175 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-202880	21/04/2026 10:48	Ventana Mantenimiento y Actualización FortiSIEM de Mintrabajo	SOC	Firewall
RFC-199550	7/04/2026 10:00	RFC Upgrade Firmware Firewall Fortigate Cali	SOC	Firewall
RFC-202879	21/04/2026 10:48	Upgrade Firmware Firewall FortiWeb	SOC	Firewall de aplicaciones Web - WAF
RFC-199545	7/04/2026 9:52	RFC : correspondiente a la actividad de Mantenimiento y Actualización de FortiSIEM	SOC	Firewall de aplicaciones Web - WAF
RF-202357	20/04/2026 8:36	Eliminar licencia de antivirus	SOC	Desinstalacion

RF-199158	6/04/2026 9:03	SOLICITUD DE ACTIVACION DE PUERTOS DE MI COMPUTADOR PARA MEMORIA USB	SOC	Habilitación Puertos USB
RF-199290	6/04/2026 12:55	SOLICITUD APERTURA DE PUERTOS USB	SOC	Habilitación Puertos USB
RF-199375	6/04/2026 15:43	Habilitación puertos USB computador portátil DT Amazonas	SOC	Habilitación Puertos USB
RF-199948	8/04/2026 9:19	Habilitación puertos USB y backup	SOC	Habilitación Puertos USB
RF-200278	9/04/2026 11:02	Habilitar puerto USB	SOC	Habilitación Puertos USB
RF-200369	9/04/2026 14:43	Fw: Solicitud de habilitación de puertos USB en equipo asignado	SOC	Habilitación Puertos USB
RF-200470	10/04/2026 7:39	RV: Actualización de la autorización del puerto USB	SOC	Habilitación Puertos USB
RF-201235	14/04/2026 8:27	Habilitación puertos USB computador portátil DT Amazonas	SOC	Habilitación Puertos USB
RF-201255	14/04/2026 8:50	RV: SOLICITUD URGENTE	SOC	Habilitación Puertos USB
RF-202547	20/04/2026 11:38	Habilitación puerto USB , Doctor: JUAN SEBASTIAN ESCOBAR MOLINA - DT RDA	SOC	Habilitación Puertos USB
RF-203403	22/04/2026 17:17	RV: ACTIVACION USUARIO PARA IMPRESION Y CUENTA	SOC	Habilitación Puertos USB
RF-204266	27/04/2026 14:02	Habilitación de utilización puertos USB en el equipo de servidora CPOLO.	SOC	Habilitación Puertos USB
RF-203928	24/04/2026 12:47	RV: URGENTE – Reporte de incidente de seguridad digital – Solicitud de eliminación y protección de datos personales	SOC	Análisis de evento
TK-201594	15/04/2026 9:27	Eliminar licencia de antivirus	SOC	Inactivar usuario
TK-202111	16/04/2026 15:25	Habilitación de Puertos con Líder de Seguridad Informática	SOC	Inactivar usuario
TK-202112	16/04/2026 15:25	Habilitación de Puertos Revisión de equipo	SOC	Inactivar usuario
TK-202113	16/04/2026 15:25	Eliminar licencia de antivirus	SOC	Inactivar usuario
TK-202398	20/04/2026 9:21	Eliminar licencia de antivirus	SOC	Inactivar usuario
RF-200233	9/04/2026 9:59	FortiSIEM Alert: TLP:RED - Mintrabajo - Traffic to Emerging Threat IP List	SOC	Seguridad Informática
RF-200795	12/04/2026 15:05	FortiSIEM Alert: TLP:RED - Mintrabajo - Multiple Logon Failures: VPN	SOC	Seguridad Informática
RF-200796	12/04/2026 15:51	FortiSIEM Alert: TLP:RED - Mintrabajo - Multiple Logon Failures: VPN	SOC	Seguridad Informática
RF-200797	12/04/2026 16:07	FortiSIEM Alert: TLP:RED - Mintrabajo - Multiple Logon Failures: VPN	SOC	Seguridad Informática
RF-200798	12/04/2026 16:37	FortiSIEM Alert: TLP:RED - Mintrabajo - Multiple Logon Failures: VPN	SOC	Seguridad Informática
RF-200799	12/04/2026 19:03	FortiSIEM Alert: TLP:RED - Mintrabajo - Multiple Logon Failures: VPN	SOC	Seguridad Informática
RF-200801	13/04/2026 2:23	FortiSIEM Alert: TLP:RED - Mintrabajo - Multiple Logon Failures: VPN	SOC	Seguridad Informática
RF-200802	13/04/2026 2:35	FortiSIEM Alert: TLP:RED - Mintrabajo - Multiple Logon Failures: VPN	SOC	Seguridad Informática
RF-201500	14/04/2026 17:19	FortiSIEM Alert: TLP:RED - Mintrabajo - Multiple Logon Failures: VPN	SOC	Seguridad Informática
RF-202023	16/04/2026 12:22	FortiSIEM Alert: TLP:RED - Mintrabajo - Traffic to Emerging Threat IP List	SOC	Seguridad Informática
RF-202158	16/04/2026 16:31	FortiSIEM Alert: TLP:RED - Mintrabajo - Traffic to Emerging Threat IP List	SOC	Seguridad Informática
RF-203029	21/04/2026 15:51	FortiSIEM Alert: TLP:RED - Mintrabajo - Multiple Logon Failures: VPN	SOC	Seguridad Informática
RF-203231	22/04/2026 11:47	FortiSIEM Alert: TLP:RED - Mintrabajo - Traffic to Emerging Threat IP List	SOC	Seguridad Informática
RF-203232	22/04/2026 11:56	FortiSIEM Alert: TLP:RED - Mintrabajo - Traffic to Emerging Threat IP List	SOC	Seguridad Informática
RF-203455	22/04/2026 22:04	Mintrabajo - Traffic to Emerging Threat IP List	SOC	Seguridad Informática
RF-203477	22/04/2026 22:29	Mintrabajo - Traffic to Emerging Threat IP List	SOC	Seguridad Informática
RF-203478	22/04/2026 22:37	Mintrabajo - Traffic to Emerging Threat IP List	SOC	Seguridad Informática
RF-203479	22/04/2026 22:47	Mintrabajo - Traffic to Emerging Threat IP List	SOC	Seguridad Informática
RF-203480	22/04/2026 22:53	Mintrabajo - Traffic to Emerging Threat IP List	SOC	Seguridad Informática
RF-203548	23/04/2026 10:12	Mintrabajo - Traffic to Emerging Threat IP List	SOC	Seguridad Informática

RF-203554	23/04/2026 10:18	Mintrabajo - Traffic to Emerging Threat IP List	SOC	Seguridad Informática
RF-203555	23/04/2026 10:21	Mintrabajo - Traffic to Emerging Threat IP List	SOC	Seguridad Informática
RF-203559	23/04/2026 10:26	Mintrabajo - Traffic to Emerging Threat IP List	SOC	Seguridad Informática
RF-203673	23/04/2026 13:57	Mintrabajo - Traffic to Emerging Threat IP List	SOC	Seguridad Informática
RF-203701	23/04/2026 14:47	FortiSIEM Alert: TLP:RED - Mintrabajo - Traffic to Emerging Threat IP List	SOC	Seguridad Informática
RF-203707	23/04/2026 14:58	FortiSIEM Alert: TLP:RED - Mintrabajo - Traffic to Emerging Threat IP List	SOC	Seguridad Informática
RF-203715	23/04/2026 15:23	FortiSIEM Alert: TLP:RED - Mintrabajo - Traffic to Emerging Threat IP List	SOC	Seguridad Informática
RF-203718	23/04/2026 15:28	FortiSIEM Alert: TLP:RED - Mintrabajo - Traffic to Emerging Threat IP List	SOC	Seguridad Informática
RF-203747	23/04/2026 16:03	FortiSIEM Alert: TLP:RED - Mintrabajo - Traffic to Emerging Threat IP List	SOC	Seguridad Informática

Tabla 60 Reporte de requerimientos abril

3.1.6.7 Análisis de riesgo

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

- **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 61 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 62 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 63 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.
- Se realiza

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 activades realizadas en el mes de abril 2026, se realizó la revisión, ajuste, observaciones de algunos procedimientos y políticas que describimos a continuación

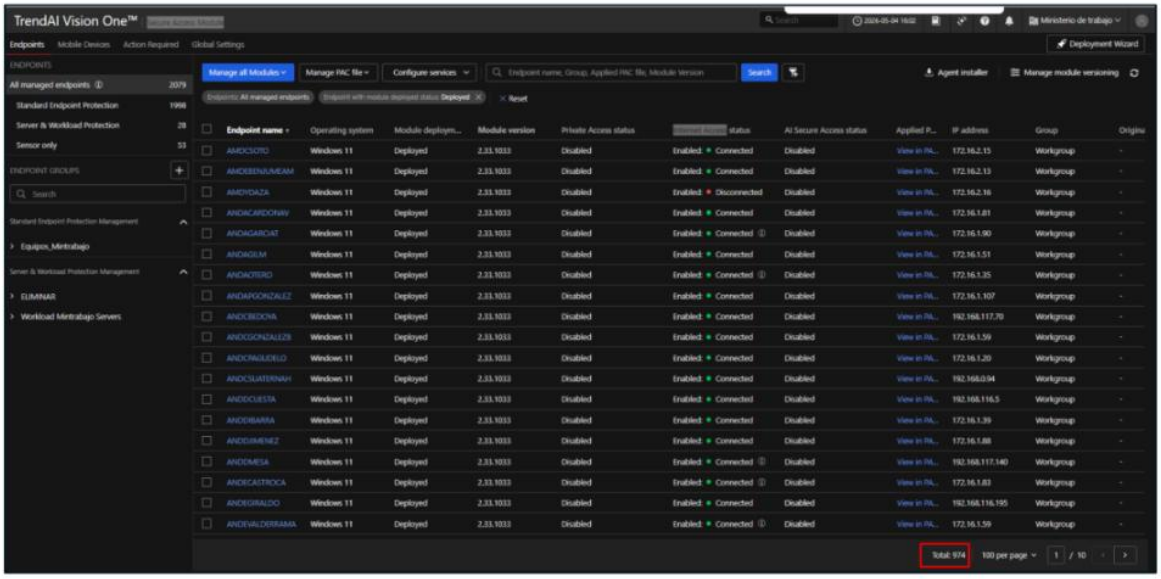


Ilustración 93 Políticas y procedimientos

Actualmente, el servicio de Zero Trust Network Access (ZTNA) se encuentra en proceso de ajuste y optimización de las reglas de acceso a Internet. A la fecha, se han desplegado 974 agentes funcionales en las distintas Direcciones Territoriales (DTs), lo cual ha permitido establecer una capa adicional de protección frente a amenazas cibernéticas y prevenir posibles fugas de información. Esta implementación fortalece significativamente los mecanismos de control de acceso y seguridad en los equipos de la entidad

3.1.7 Licenciamiento

A continuación, se presenta la información del licenciamiento:

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

Tabla 64 Licenciamiento

3.1.8 Administración, soporte y monitoreo

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

Nube pública

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

DDBB

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

Almacenamiento

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

Medición ANS Datacenter y Nube Pública

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

ID	Indicadores	Resultado	Meta
DC-1	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
DC-2	Continuidad y disponibilidad del datacenter principal	100,00%	99.95%
DC-3	Continuidad y disponibilidad del datacenter alterno	100,00%	99,60%
DC-4	Continuidad y disponibilidad de la plataforma de procesamiento, almacenamiento y respaldo	100,00%	99,70%
DC-5	Tiempo de solución de incidentes asociado a los servicios de aplicaciones especializadas	98,72%	90,00%
DC-6	Tiempo de solución de requerimientos asociado a los servicios de aplicaciones especializadas	100,00%	90,00%
DC-7	Continuidad y disponibilidad de los servicios de directorio activo	100,00%	99,60%
DC-8	Continuidad y disponibilidad de los servicios de seguridad informática	100,00%	99,90%
DC-9	Tiempo de solución de incidentes asociado a los servicios de administración, soporte y monitoreo	100,00%	90,00%
DC-10	Tiempo de solución de requerimientos asociado a los servicios de administración, soporte y monitoreo	99,87%	90,00%
DC-11	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 65 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 66 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 abril, 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.

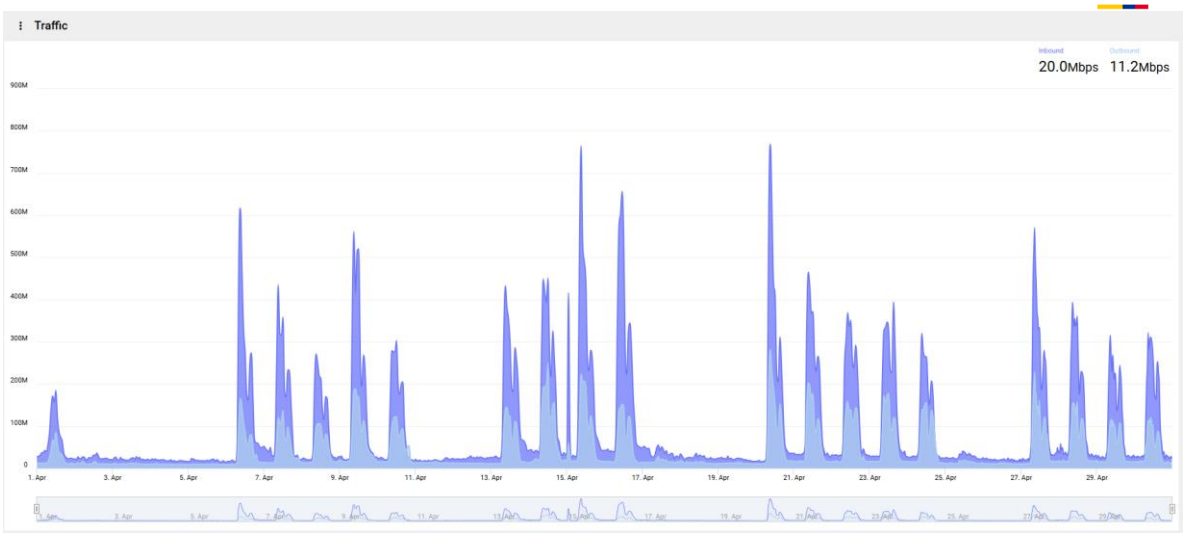


Ilustración 94 Consumo canal MPLS DC Principal

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

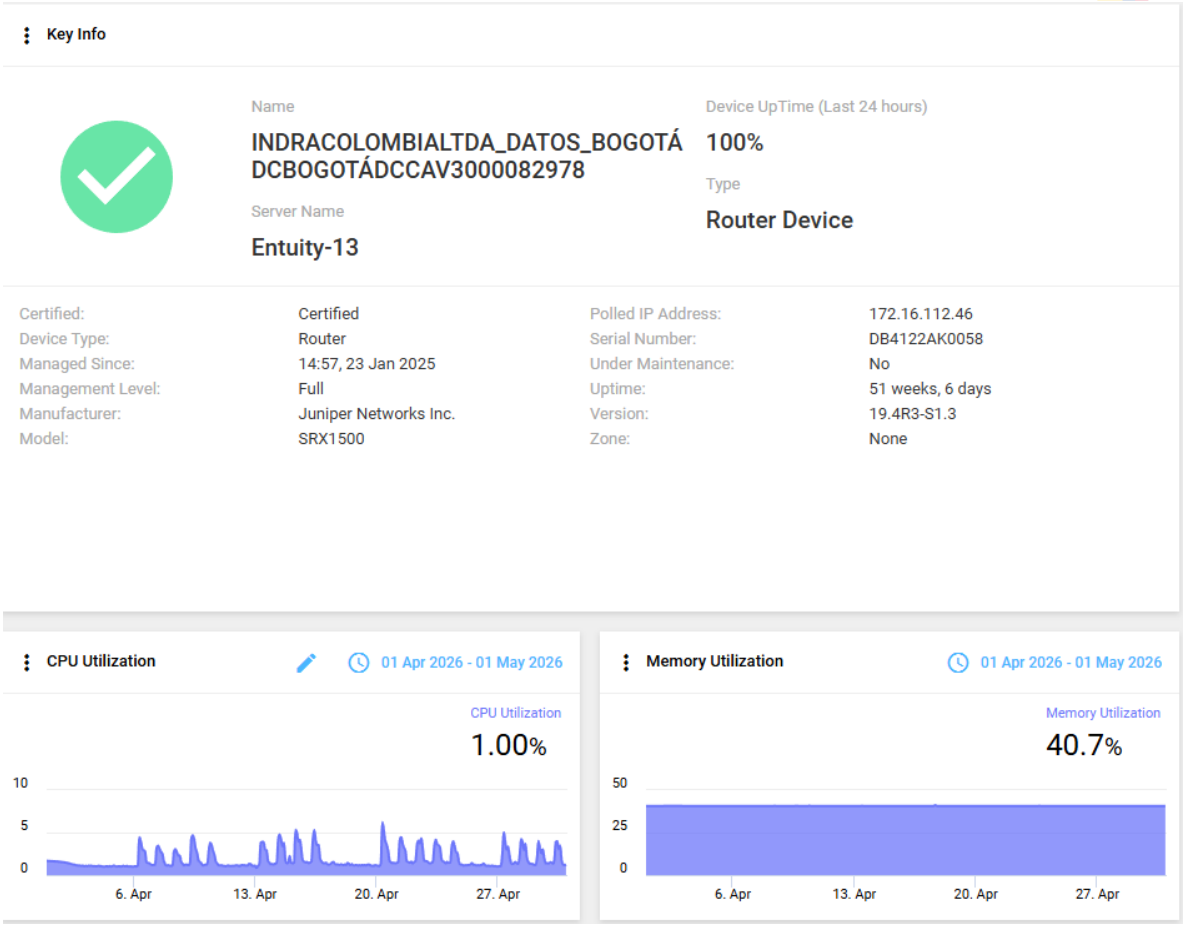


Ilustración 9596 Estado Router MPLS DC Principal

3.3.1.1 Incidentes de Conectividad

Durante el mes de abril, 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
Sede Territorial Arauca	IM-201046 IM-203164	99,16%
Sede Territorial San José del Guaviare	IM-199882 IM-204829	98,67%
Sede Territorial Quibdó	IM-199001	95,01%
Plato	IM-199197	46,83%
Sede Territorial Bucaramanga	IM-200243	97,84%
Salamina	IM-201310	95,67%
Guapi	IM-202333	90,88%
Tuquerres	IM-200309	97,03%
Turbo	IM-200186	85,83%
Palmira	IM-200480	99,08%

Tabla 67 Incidentes de conectividad

3.3.1.2 Topología Actual

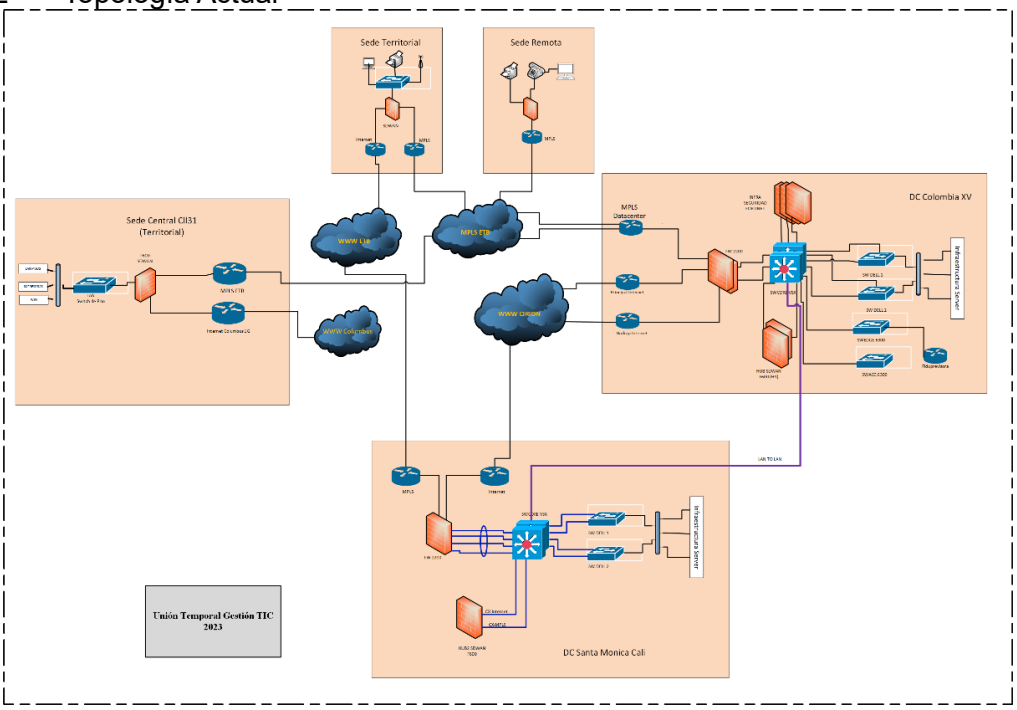


Ilustración 97 Topología actualizada

3.3.2 Canales SDWAN e Internet Dedicado

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

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

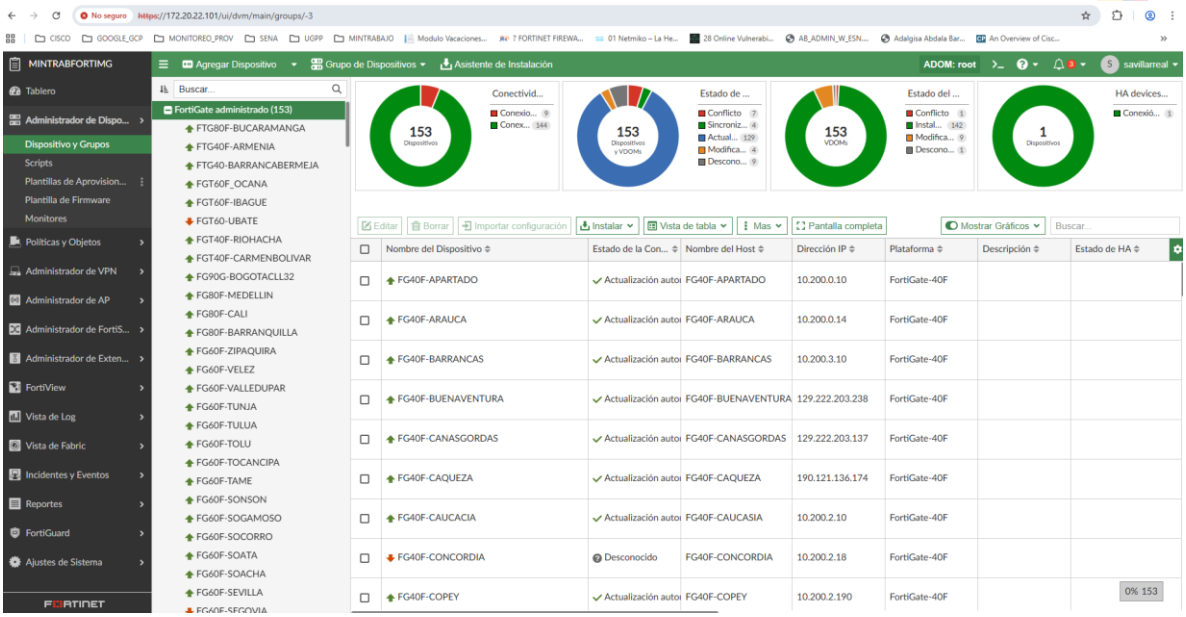


Ilustración 98 Interface Fortimanager

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 178.35 Mbps de consumo con un máximo de 1.25 Gbps, este canal es de 2GB, con el tráfico generado se observa que no presentó saturación durante el mes.

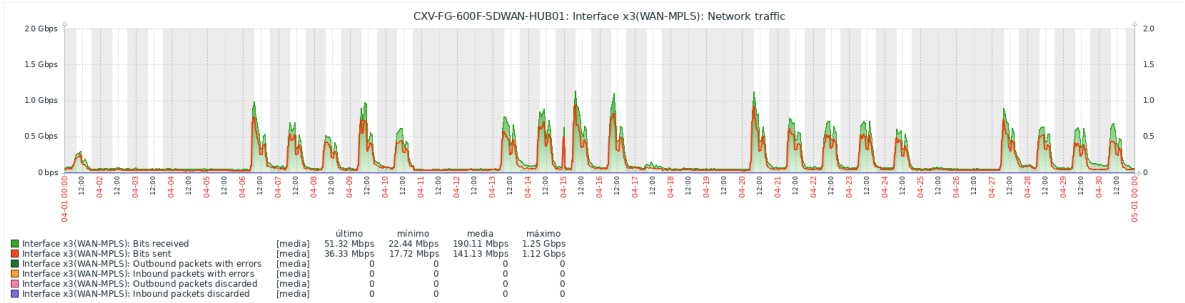


Ilustración 99 Interface MPLS HUB SDWAN

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 71.94 Mbps de consumo en el mes donde se tuvo un máximo de 542.92 Mbps. Este canal es de 1GB, con el tráfico generado en el mes, no se presentó saturación.

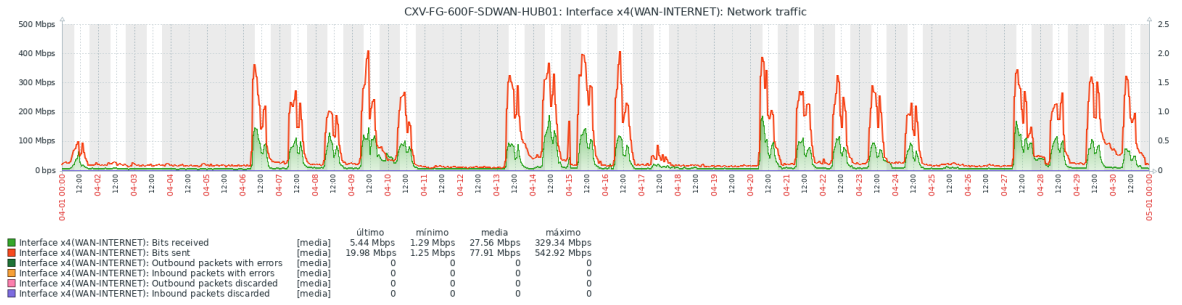


Ilustración 100 Interface Internet HUB SDWAN

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

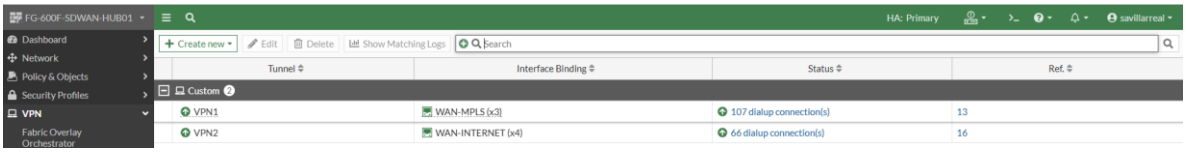


Ilustración 101102 VPN SDWAN establecidas

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.

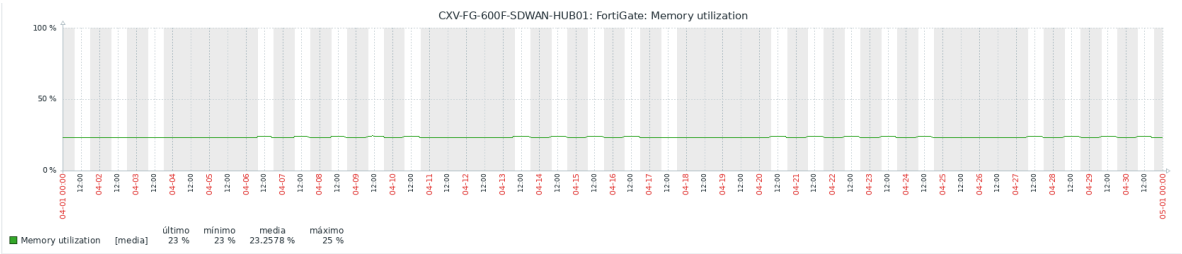


Ilustración 103 Estado HUB SDWAN Datacenter

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.

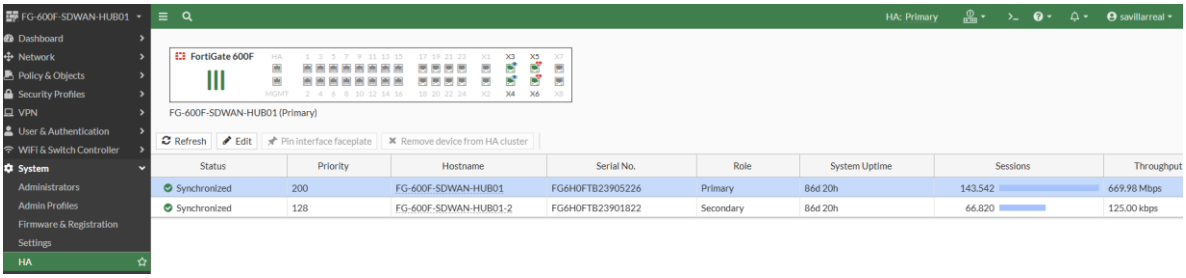


Ilustración 104 Estado HA HUB Sdwan

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 105 Recursos Fortimanager

Otras novedades del servicio:

A continuación, se relacionan las novedades relevantes en el servicio.

- Durante el mes de abril, el equipo de infraestructura realizó el envío de las máquinas de QA del gestor documental a DC alterno Santa Mónica, esto se vio reflejado en el aumento de tráfico a través del enlace LAN TO LAN.
- 10/04/2026: Se ejecut el RFC-199435, en el cual se realizaron pruebas DRP en la sede Chiquinquirá, donde se verificó el correcto funcionamiento del servicio operando a través del canal de Internet del DC alterno Santa Mónica en Cali.
- Se está llevando a cabo el retiro de los equipos de conectividad asociados al proveedor ETB y sus aliados de última milla, los cuales pertenecen a enlaces que han sido retirados y/o reemplazados por otros proveedores.

IM-191302 Revisión
Canales Internet Terri

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 68 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 abril:

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

Dirección Territorial	Caso Asociado	% de Disponibilidad	% Penalidad	Valor Penalidad un enlace
Plato	IM-199197	46,83%	100%	$ 317.255
Salamina	IM-201310	95,67%	3%	$ 9.518
Guapi	IM-202333	90,88%	10%	$ 31.725
Tuquerres	IM-200309	97,03%	3%	$ 9.518
Turbo	IM-200186	85,83%	10%	$ 31.725
Palmira	IM-200480	99,08%	3%	$ 9.518
Total				**$ 409.259**

Tabla 69 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
Sede Territorial Arauca	IM-201046 IM-203164	99,16%	10%	$ 83.699
Sede Territorial San José del Guaviare	IM-199882 IM-204829	98,67%	3%	$ 12.555
Sede Territorial Quibdó	IM-199001	95,01%	3%	$ 37.664
Sede Territorial Bucaramanga	IM-200243	97,84%	3%	$ 62.774
Total				**$ 196.692**

Tabla 70 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 solicitudes relacionadas con la revisión, pruebas, retiro y asignación de equipos de cómputo. Así mismo, se brindó soporte a las novedades presentadas en el parque computacional Lenovo.

- **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**	1148	24
Equipos portátiles	**1000**	955	165
Equipos portátiles adicionales	**120**		
Total	**2292**	**2103**	**189**

Tabla 71 Cantidades de equipos Contractual – Instalados - Almacén

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

Durante el período, se dejó de realizar la asignación de equipos a contratistas, pasantes, casos de doble asignación a funcionarios, así como a salas de conciliación, entre otros, una vez se recibió el aval por parte del Coordinador del Grupo de Soporte Informático.

- **Gestión de Inventario**:

Se atendieron las solicitudes de retiro, traslados y asignación de equipos de cómputo según los requerimientos de los usuarios.

ASIGNACION DE EQUIPOS ABRIL		
SEDE	**TIPO DE ELEMENTO**	**CANTIDAD**
DT Arauca	Escritorio	1
DT Boyacá	Escritorio	1
DT Córdoba	Escritorio	1
DT Huila	Portátil	1
DT Santander	Portátil	2
Nivel Central	Escritorio	3
Nivel Central	Portátil	34
TOTAL		**43**

Tabla 72 Cantidades de equipos asignados nivel nacional

DEVOLUCION DE EQUIPOS ABRIL		
SEDE	**TIPO DE ELEMENTO**	**CANTIDAD**
DT Antioquia	Escritorio	2
DT Antioquia	Portátil	1
DT Arauca	Portátil	1
DT Bogotá	Portátil	2
DT Boyacá	Escritorio	2
DT Cauca	Portátil	1
DT Córdoba	Escritorio	1
DT Norte de Santander	Escritorio	1
DT Putumayo	Escritorio	1
DT Santander	Escritorio	1
DT Santander	Portátil	2

DT Valle del Cauca	Portátil	2
DT Valle del Cauca	Escritorio	2
DT Nivel Central	Escritorio	6
DT Nivel Central	Portátil	12
TOTAL		**37**

Tabla 73 Cantidades de equipos por devolución nivel nacional

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

- **Gestión de Garantías:**

Durante el mes de abril se reportó un total de 24 casos de garantía. A continuación, se detallan los estados asociados a estos casos:

Estado de caso	Cantidad
Cerrado	13
Suspendido	11
Total	**24**

106 Tabla 74 Estado de casos de garantía.

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

ANS	Cerrado	Suspendido	Total
CUMPLE	13	11	24
NO CUMPLE			
Total	**13**	**11**	**24**

Tabla 75 ANS casos de garantía.

Fecha de Reporte	Serial	Parte	Falla	Sede	No. Caso	Estado
27/04/2026		Equipo Portátil	Garantía Equipo portátil por problema en serial.	Mocoa	RF-204377	Cerrado
22/04/2026	HC3BBN84	Diadema	Garantía Diadema HC3BBN84	Piso 9	RF-203370	Cerrado
21/04/2026	HC3BBLK6	Diadema	Revision de periféricos por posibles daños internos.	Piso 19	RF-202912	Cerrado
21/04/2026	HC3BAHHN	Diadema	Garantía Diadema HC3BAHHN	Piso 9	RF-202888	Cerrado
21/04/2026	HC3BBNDX	Diadema	falla diadema s/n: HC3BBNDX	Antioquia	RF-202878	Cerrado
21/04/2026	HC3BBM37	Diadema	Garantía de Diadema	Calle 32	RF-202790	Cerrado
14/04/2026	HC3BBMA0	Diadema	Garantía Diadema HC3BBMA0	Piso 9	RF-201456	Cerrado
14/04/2026	VNAA622K	Monitor	Garantía Monitor S-N VNAA622K por fallas de imagen	Santander	RF-201227	Cerrado
13/04/2026	VNAA64AH	Monitor	Garantía Monitor S-N VNAA64AH por fallas de imagen	Santander	RF-200939	Cerrado
9/04/2026	HC3BBLXR	Diadema	Solicitud garantía de diadema	Huila	RF-200354	Cerrado
6/04/2026	HC3BBMTJ	Diadema	solicitud revisión diadema	Piso 10	RF-199451	Cerrado

6/04/2026	AVLC3C5A2HN	Teclado	Garantía de teclado AVLC3C5A2HN	Piso 8	RF-199345	Cerrado
14/04/2026	VNAA62P0	Equipo Escritorio	Solicitud de garantía de monitor - VNAA62P0	Choco	RF-201289	Cerrado
24/04/2026	PW0A36YC	Equipo Portátil	Solicitud de garantía – Portátil ThinkPad 14 G6 ABP	Cali	RF-203982	Suspendido
22/04/2026	PW0A3BE5	Equipo Portátil	Colaboración con garantía de equipo portatil	Ipiales	RF-203182	Suspendido
23/04/2026	HC3BBMST	Diadema	Gestionar garantía diadema	Atlántico	RF-203612	Suspendido
23/04/2026	HC3BBMYK	Diadema	cambio de diadema por garantía	Guajira	RF-203573	Suspendido
22/04/2026	HC3BBNFH	Diadema	Garantía diadema	Guateque	RF-203322	Suspendido
29/04/2026	MJ0LS5Y0	Equipo Escritorio	No da imagen	Piso 22	RF-204867	Suspendido
29/04/2026	VNAA62A8	Monitor	Presenta Líneas	Buenaventura	RF-204836	Suspendido
27/04/2026	VNAA64B5	Monitor	Falla en pantall	Guajira	RF-204271	Suspendido
20/04/2026	VNAA64G6	Monitor	Monitor presenta colores y rayas horizontales. SERIAL VNAA64G6	Guapi	RF-202390	Suspendido
10/04/2026	MJ0LS58H	Equipo Escritorio	Equipo enciende, pero no da video MJ0LS58H	Planeta Rica	RF-200596	Suspendido
9/04/2026	VNAA625B	Equipo Escritorio	Valoración de pantalla, presenta colores y rayas horizontales SERIAL VNAA625B	Santander de Quilichao	RF-200221	Suspendido

Tabla 76107 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_2025_3256134/2025046910//2023159675
Bernardo Ardila Fernández	PW09Z34H	Valledupar	Golpes en esquinas	Aseguradora hace entrega de equipo	PRG_2025_4160592
Galia Lena Álvarez Hernández	PW0A3CHL	Nivel Central	Golpes en esquinas	Aseguradora realizó la reposición del equipo con serial PW09ZT67 /se realiza entrega de equipos dañado	
Henrry Samir Gómez Ortiz	PW0A36X6	Nivel central	Robo	Denegada aseguradora no cubre	

Ana Mireya Escobar Tierradentro	MJ0LS5TW	Popayán/	No enciende	Se deja una cpu de reposición/Aseguradora/ 09/05/2025 Se realiza reposición de equipos MZ01E5KG	PRG_2025_1766918
Lacides Manuel Morales Ortega	MJ0LS5XL	Sincelejo/ San Marcos	Se apaga y no enciende	Se realiza reposición de equipo MZ01E5KA	PRG_2025_1921454
Jesús Manuel Martínez Franco	PW0A3BEY	Montería	Golpes en esquinas	Aseguradora hace entrega de equipo PW0A370B.	PRG_2025_4160302
Adriana Patricia Martínez Arévalo	PW09Z369	Nivel central	Equipo no da imagen	Se adjunta acta de asignación de equipo de reposición por aseguradora PW09ZT6N 05/08/2025	PRG_2025_2251570
Miguel Ángel Izquierdo Hospital	PW0A3BFT	Nivel Central	Falla en puerto de carga	Aseguradora realizó la reposición del equipo con serial PW09ZT78, se realiza devolución de equipo dañado	PRG_2025_4159804
William Ricardo Álvarez Gómez	PW0A3CK3	Nivel Central	Robo	Se deja equipo de reposición en bodega dado que ya se le había asignado PW0A3AVL al funcionario.	PRG_2025_3861658
Amber Duran Lozano	PW0A3BJM	Nivel central	Reporta varias grietas en el equipo portátil	Aseguradora realizó la reposición del equipo con serial PW0A3BPJ	PRG_2025-4611910
Maria Isabel Cuenca Mendoza	PW0A3BPB	Cali Valle	no responde correctamente a comandos del teclado integrado	Aseguradora realiza reposición de equipo PF68AZS3	PRG_2026_2853
Laura Estefanía Mendoza Quintero	PW0A3CKM	DT Quindío	Robo	Se realiza envió de portátil PW0A3BHA de contingencia/ Se realiza reposición de equipo PF68B03K	
Valeria Márquez Pereira	PW0A3AZW	Nivel central	Robo	Se realiza asignación de equipo de contingencia PW0A36XS/Se realiza reposición de equipo PF68AZRT	PRG_2024_1504426
Silvia Patricia Rojas Ardila	MJ0LS5CD	B/manga	Robo	Se envía documentación para trámite ante aseguradora.	PRG_2025_4989622
Cindy Julieth Feria Molina	PW0A0FN2	Nivel Central 8	Robo	Se realiza asignación de equipo PW09ZT6H/Se realiza reposición de equipo PF68B03E	PRG_2026_62277
Jhonny Santander Cerinza	PW0A3AWT	DT Santander	Golpe en cover	Lenovo realiza visita que no cubre garantía por que el equipo sufrió un golpe 27/02/2026 se envía documentación para proceso con aseguradora	
Viviana Stephanys Plaza Amador	MJ0LS534	La Jagua	No enciende	Se envía documentación para proceso con aseguradora	
Brenny Liliana Martinez Gomez	PW0A3CF5	DT Santander	Existe un objeto extraño alojado en su interior	Se envía documentación para proceso con aseguradora	

Tabla 77 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 24 solicitudes tipificadas así:
  - Incidentes: 0 casos

- Requerimientos: 24 casos

- Al corte de mes quedaron en estado:
  - Cerrado: 13 casos.
  - Suspendido: 11 casos.

- 24 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	23
Gestor de inventarios	1
Total, general	24

Tabla 78 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	24
Equipo Periférico	14
Equipo Escritorio	7
Equipo Portátil	3
Total	24

Tabla 79 Solicitudes de Equipos Usuario Final – Según Grupo Responsable

4.1.2 Equipos de Escritorio

Durante el mes de abril, se continuó la gestión y atención de los equipos de cómputo de escritorio asignados a los usuarios de la entidad, en el nivel central y en las sedes territoriales.

4.1.3 Equipos Portátiles

Durante el mes de abril 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 80 108 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:

- 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.
- 10/04/2026: Se presenta novedad de conectividad de la IT Plato / Magdalena, se realiza reporte al proveedor de conectividad pero confirma funcionalidad y respuesta del router, en diagnóstico a nivel de la LAN, se identifica posible daño del adaptador o del equipo Fortinet. Se deja la sede operativa a través de la MPLS, se gestiona el cambio del equipo SDWAN en la sede. Se configuró e instaló nuevo equipo SN. FGT40FTK2309BCM4 normalizando las conexiones LAN en la sede.
- Se corrigieron vulnerabilidades en los switches asegurando los protocolos de acceso https y SSH.
- Se ejecutó RFC de pruebas del plan de disponibilidad de Red LAN.
- 16 y 17/04/2026: Se realiza la actualización de firmware en Switches (a la versión 10.13.11.61) y Access Point Aruba (a la versión 8.13.1.2_9514) de acuerdo con las recomendaciones de fábrica. Se trabajo bajo los casos RFC-201337 y RFC-201516.

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

- Los especialistas gestionaron un total de 15 solicitudes escaladas a través de la herramienta Aranda. Al corte del mes 12 casos quedaron en estado Cerrado, 2 casos en estado en Proceso y 1 en Suspendido. los casos obedecen a revisión de alertas sobre caída de servicios de conectividad, degradación y lentitud sobre los canales, habilitar puntos de red en puestos de trabajo, ejecución de RFCs para elaboración de planes de disponibilidad y actualización de firmware de dispositivos. Los demás casos relacionados con el servicio se gestionaron por parte del NOC, los detalles se relacionan en el apartado 2.1.2.8. Práctica de Eventos de este mismo documento.

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

Categoría	Cantidad de solicitudes
Router	2
Starlink	2
FortiGate	2
Revisión estado del canal	1
Asesoría - Consulta	1

Tabla 81 Top 5 de categorías en el Servicio de conectividad LAN-WLAN

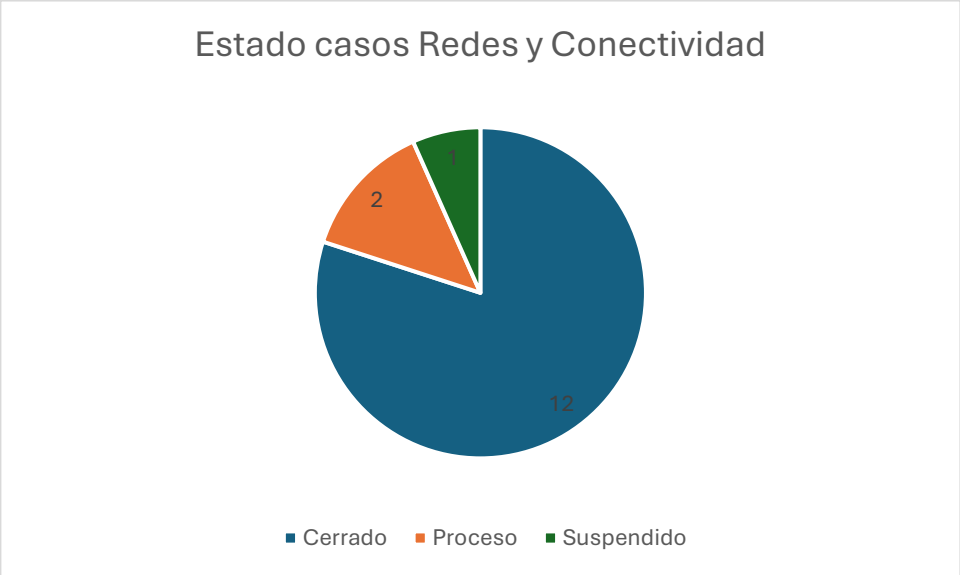


Ilustración 109 Estado de casos Redes y Conectividad

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

Dirección Territorial	Población y/o ciudad de ubicación	Cantidad switches 24 puertos
Territorial Valle	CALI	2*
Sede Nivel Central	BOGOTA	7
	Total	**24**

Tabla 82 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
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 83 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	4
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
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	**110**

Tabla 84110 Distribución de puntos de acceso

Territorial Norte de Santander - Cúcuta: El AP fue enviado e instalado en la DT Santander / Bucaramanga
Calle 32: 5 Access Point se desinstaló por cierre de oficina y se instaló en sede central.
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.

Sede Nivel Central: Se retiró AP del piso 12 debido a que el ministerio debía entregar al edificio zona BID, se deja AP en Stock.

- **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 85 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 86111 Equipos gama media

(*) Novedades en la instalación de teléfonos

Nivel Central disponibilidad de 3 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 87 Sedes cerradas

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

Tabla 88 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 89 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 abril 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 disponibles según cada referencia.
- Se continúa el monitoreo sobre las troncales para las opciones 2 y 0 configuradas en el IVR para atención al ciudadano con el nuevo aliado BPM.
- En seguimiento al caso RF-188953, se informa que se mantiene monitoreo diario sobre la línea 1080 correspondiente a la mesa de servicios, con el objetivo de verificar continuamente el comportamiento del servicio; adicionalmente, se están recopilando y almacenando de forma permanente las trazas y evidencias técnicas derivadas de las pruebas realizadas, permitiendo un control detallado de la operación y garantizando la estabilidad y disponibilidad del servicio, sin evidenciarse a la fecha anomalías en la infraestructura.



Validación caso
RF-188953 - Falla de

- Durante el mes en curso se realizó el proceso de configuración y aprovisionamiento de extensión y asignación de licencia de Teams Phone Standard en el tenant de Microsoft Teams para un usuario solicitado. Los cambios fueron aplicados exitosamente. Se adjuntaron manuales de soporte y configuración para referencia. Estado actual: Todos los usuarios se encuentran activos – casos RF-198952 – RF-200467 – RF– 2022889 – RF-204405 – RF-205007.

- **Asignación de Licencias – Extensiones**

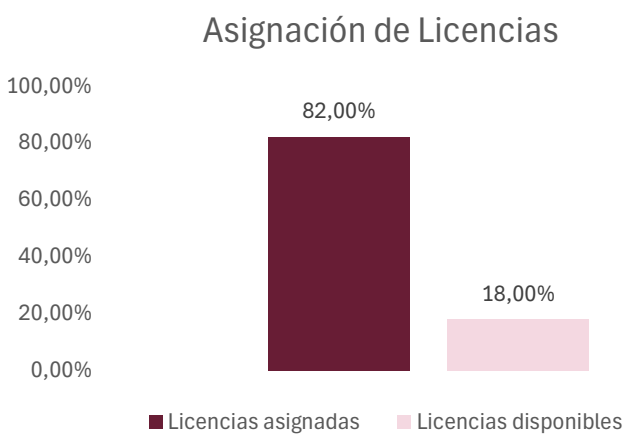


Ilustración 112 Asignación de licencias

Durante el mes en gestión, se han asignado un total de 490 extensiones a nivel nacional. Actualmente, permanecen disponibles 110 extensiones.

- **Estadísticas de Tráfico**

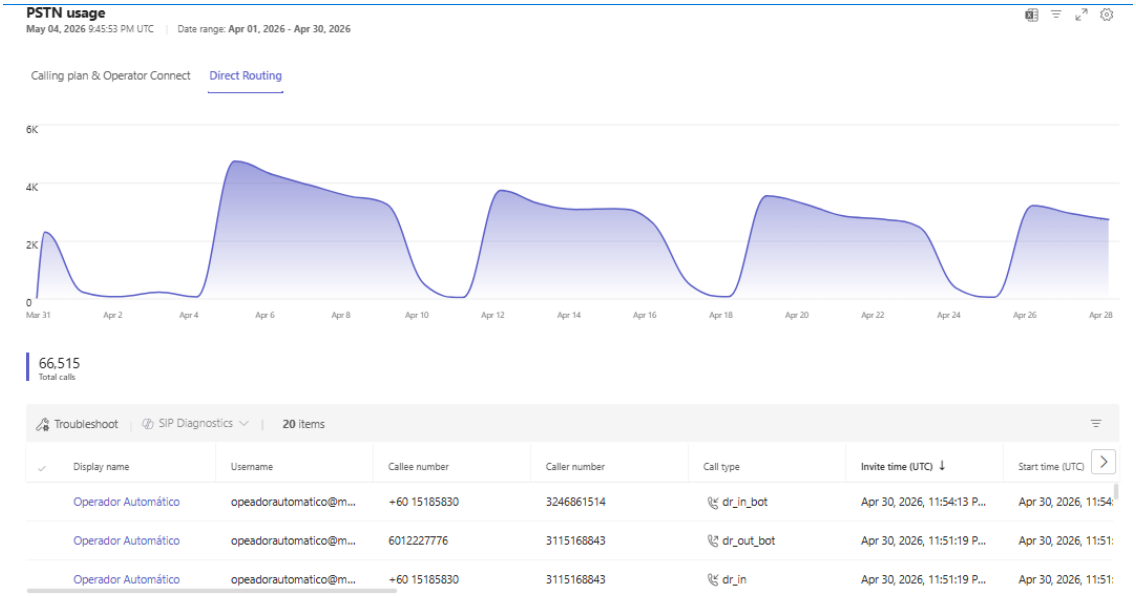


Ilustración 113 Comportamiento de tráfico

En la gráfica anterior se visualizan las tendencias de uso del servicio, en el periodo correspondiente al mes de abril de 2026, donde se atendieron un total de 66,515 llamadas.

Servicio	Minutos Disponibles	Minutos Utilizados
Locales	Ilimitados	1410.11
Celular	1000	910.23
Nacional	Ilimitados	771.15
Internacional	700	6.31
Total		3097,79

Tabla 90 Minutos, consumos

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

Con respecto a las llamadas realizadas a destinos larga distancia nacional en el mes de abril de 2026, se identifica que se realizaron llamadas con una duración total de 771.15 minutos.

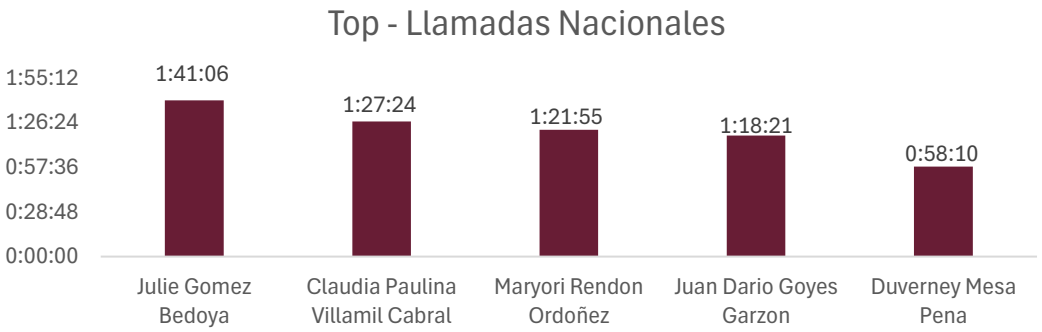


Tabla 91 Top llamadas nacionales

N°	Usuario	Área	Tiempo llamadas
1	Julie Gomez Bedoya	Grupo De Atención Al Ciudadano Y Tramites – DT Cauca	1:41:06
2	Claudia Paulina Villamil Cabral	Grupo Interno de Trabajo de Análisis y Monitoreo de la Información	1:27:24
3	Maryori Rendon Ordoñez	Digitalizadora O.E Barrancabermeja	1:21:55
4	Juan Dario Goyes Garzon	Dialogo Social DT Antioquia	1:18:21
5	Duverney Mesa Pena	Inspector de Municipios Antioquia	0:58:10

Tabla 92 114 Top 5 consumo de llamadas

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

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

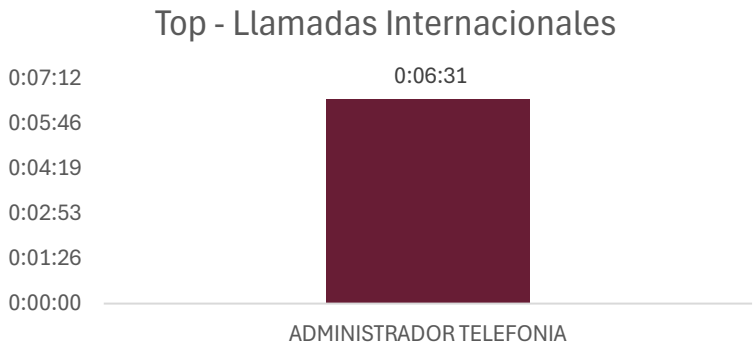


Ilustración 115 llamada internacional de prueba

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

N°	Usuario	Área	Tiempo llamadas
1	Administrador Telefonía	UT	0:06:31

Tabla 93116 Top 5 llamadas LDI

- **Consumo de llamadas destinos celulares**

Con respecto a las llamadas realizadas a celular en el mes de abril de 2026, se identifica que se realizaron llamadas con una duración total de 910.23 minutos (15,17 horas).

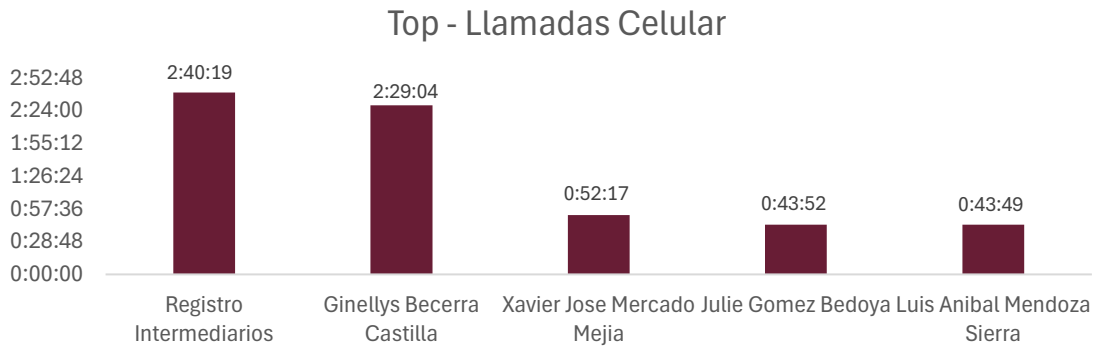


Ilustración 117 Top Celular

N°	Usuario	Área	Tiempo llamadas
1	Registro Intermediarios	Cuenta de servicios Registro de Intermediarios Bogotá	2:40:19
2	Ginellys Becerra Castilla	Comunicaciones GEEG Bogotá	2:29:04
3	Xavier Jose Mercado Mejia	Inspector de Municipios Antioquia	0:52:17
4	Julie Gomez Bedoya	Grupo De Atención Al Ciudadano Y Tramites – DT Cauca	0:43:52
5	Luis Anibal Mendoza Sierra	Inspector de Municipios Antioquia	0:43:49

Tabla 94 118 Top 5 llamadas Celular

- **Consumo de llamadas locales**

Con respecto a las llamadas realizadas a destinos locales en el mes de abril de 2026, se identifica que se realizaron llamadas con una duración total de 1410.11 minutos (23,50 horas).

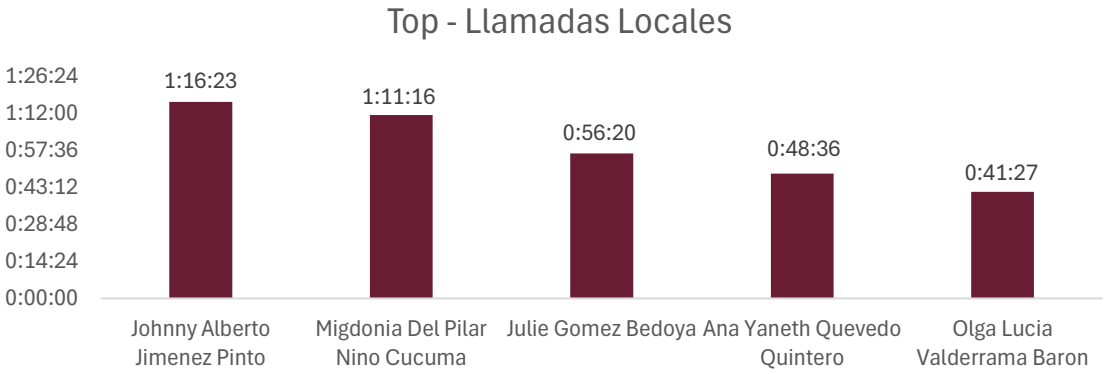


Ilustración 119 Top Local

N°	Usuario	Área	Tiempo llamadas
1	Johnny Alberto Jimenez Pinto	Defensa Judicial DT Bogotá	1:16:23
2	Migdonia Del Pilar Nino Cucuma	Dirección de Generación y Protección de Empleo y Subsidio Familiar Bogotá	1:11:16
3	Julie Gomez Bedoya	Grupo de Atención al Ciudadano y Tramites DT Valle del Cauca	0:56:20
4	Ana Yaneth Quevedo Quintero	Dirección de Pensiones y Otras Prestaciones Bogotá	0:48:36
5	Olga Lucia Valderrama Baron	Dirección de Inspección Vigilancia Control y Gestión Territorial Bogotá	0:41:27

Tabla 95120 Top 5 llamadas locales

- **Capacitaciones y divulgaciones**

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

- **Mejores Prácticas**

Se adelantarán procesos de capacitación y divulgación sobre el uso de la nueva herramienta de telefonía. Paralelamente, avanza la liberación de licencias a nivel nacional por demanda y se continuará con la validación de los respaldos de grabaciones de las llamadas que ingresan a la mesa de servicios.

- **Medición de ANS – Telefonía IP**

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

TIP-1 Tiempo de solución de requerimientos de garantía



Ilustración 121 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

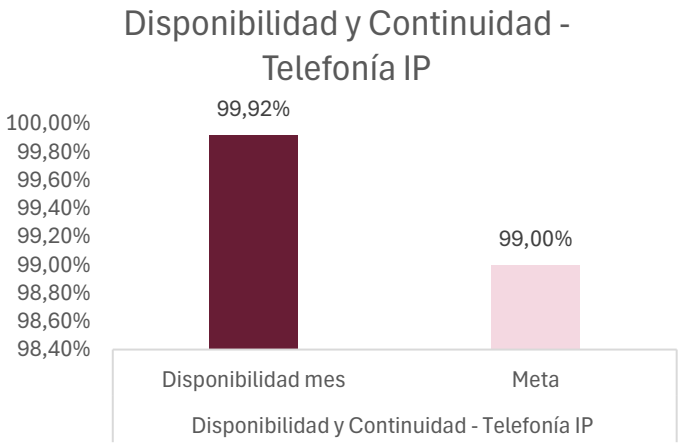


Ilustración 122 Disponibilidad y Continuidad TOIP

En el periodo correspondiente al mes de abril, 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 96 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 97 123 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 98 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. Las novedades generadas obedecen a caídas prolongadas del servicio de energía en las sedes.

A continuación, se relacionan los casos gestionados:

No. Caso	Tipo de Caso	Descripción	Solución / Avance	Estado
IM-200133	Incidents	Se ha detectado un evento en el sistema de monitoreo Zabbix. A continuación, se detallan los datos del evento: Nombre del Host: UPS_Barrancabermeja IP del Host: 172.16.34.10 Tipo de Equipo: UPS Evento: UPS en estado Baterias Severidad: Disaster Fecha y Hora del Evento: 2026.04.08 15:53:18 Descripción del Problema: Valor Actual del Ítem: Baterias (5) Por favor, toma las medidas necesarias para solucionar este problema lo antes posible.	Al restablecerse el servicio electrico la UPS enciende y las baterías empiezan a cargarse, no se presentan novedades con el equipo. Se realiza seguimiento a caso y se confirma que el daño pudo haber sido ocasionado por los picos eléctricos presentados en la sede	Suspendido
IM-200150	Incidents	Se ha detectado un evento en el sistema de monitoreo Zabbix. A continuación, se detallan los datos del evento: Nombre del Host: UPS_Barrancabermeja IP del Host: 172.16.34.10 Tipo de Equipo: UPS Evento: Generic SNMP: Unavailable by ICMP ping Severidad: Disaster Fecha y Hora del Evento: 2026.04.08 21:02:17 Descripción del Problema: Problema de comunicación con el dispositivo Valor Actual del Ítem: Down (0) Por favor, toma las medidas necesarias para solucionar este problema lo	Al restablecerse el servicio electrico la UPS enciende y las baterías empiezan a cargarse, no se presentan novedades con el equipo. Se realiza seguimiento a caso y se confirma que el daño pudo haber sido ocasionado por los picos eléctricos presentados en la sede	Suspendido
IM-202778	Incidents	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: 2026.04.20 21:32:45 Descripción del Problema: Valor Actual del Ítem: Baterias (5) Por favor, toma las medidas necesarias para solucionar este problema lo antes posible.	Soporte en sitio informa que la UPS estaba apagada, recién la puso en marcha nuevamente, la alerta se solventa	Cerrado

IM-202779	Incidents	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: Generic SNMP: Unavailable by ICMP ping Severidad: Disaster Fecha y Hora del Evento: 2026.04.20 22:01:44 Descripción del Problema: Problema de comunicación con el dispositivo Valor Actual del Ítem: Down (0) Por favor, toma las medidas necesarias para solucionar este problema lo antes po	Soporte en sitio informa que la UPS estaba apagada, recién la puso en marcha nuevamente. se solventa la alerta	Cerrado

Tabla 99124 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 realizo 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 Fisicos 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.

  - Se continúa verificando con fábrica una inconsistencia que se tiene con seis (6) de las UPS intervenidas en Nivel Central en el mantenimiento preventivo, ya que se encuentran operativas y funcionales, pero no se tiene alcance a la IP de monitoreo de su tarjeta de red. Se han efectuado cuatro (4) visitas técnicas bajo ventanas de mantenimiento con el propósito de: hacer revisión de las tarjetas bajo la práctica de cambios, se remiten evidencias y pruebas para el escalamiento con el fabricante Ablerex, intentar reconfiguración de las tarjetas.

  Durante el período del informe se efectuó la actualización de firmware de la UPS de Piso 18, sin lograr restablecer la comunicación ni la operación adecuada de las tarjetas. Dado lo anterior, el ingeniero Santiago Murillo, representante autorizado de la marca Ablerex, procedió con el retiro de la tarjeta de red para su respectivo análisis y diagnóstico en laboratorio especializado del fabricante. Se registran avances en el caso PM-193636.

- 9/04/2026: 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.

- **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 100 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 101 Inventario de impresoras para el servicio

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

- Para el mes de abril, el responsable del servicio gestionó un total de 395 solicitudes escaladas a través de Aranda. Al corte del mes, 388 casos quedaron en estado Cerrado/Solucionado, 7 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 33% de la capacidad total del almacenamiento (capacidad total 100gb).
- El administrador del servicio de outsourcing de impresión remitió semanalmente vía correo electrónico al Coordinador del Grupo de Soporte Informático e interesados el consolidado de consumo de clics acumulado durante el período, lo anterior con el propósito de notificar el momento en que se supera el umbral definido de consumo establecido para el servicio.

- Se realizó la asignación de cuotas de clics de impresión de usuarios finales bajo el caso Aranda RF-198844; 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 15/04/2026 se realizó el cambio de la impresora en la DT Vichada, debido a fallas presentadas por el equipo anterior. La nueva impresora instalada cuenta con el número de serie SN: 3353PB50307.
- El 28/04/2026 se da inicio al mantenimiento preventivo de las impresoras a nivel central y en algunas DT, con el fin de garantizar un buen funcionamiento sobre las impresoras y la calidad de las impresiones. Esta actividad se gestiona en el marco de las obligaciones contractuales y el mantenimiento semestral que se les debe hacer a los equipos.

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

Nombre de la impresora	Ubicación	Nombre de Usuario	Nombre Completo	Blanco y negro
ricohpiso23b	Bogotá sede central	lpanche	Luis Fernando Panche Chiquiza	6.114
ricohpiso9a	Bogotá sede central	criverad	Carlos Jose Rivera Daza	3.983
ricoh-apartado-piso2-c	Apartado	mibarguen	Maria Dolores Ibarguen Torres	3.171
ricohpiso19b	Bogotá sede central	sleonm	Sandrith Mariana Leon Martinez	2.734
ricoh-guadalaraja-buga-insp	Guadalaraja buga	vfierro	Viviana Fierro Herrera	2.668
ricoh-ibague-radicacion	Ibague	jgonzalezcu	Jose Eugenio Gonzalez Cuella	2.608
ricohpiso17a	Bogotá sede central	pvergara	Pedro Jean Paul Vergara Nino	2.527
ricohpiso19a	Bogotá sede central	pnustes	Patricia Celestial Nustes Barrera	2.490
ricoh-bmanga-ofc205	Bucaramanga	ybeltran	Yerson Daniel Beltran Martinez	2.456
ricohpiso23a	Bogotá sede central	ekecan	Eliana Karolina Kecan Torres	2.345

Tabla 102*125* Consumo de impresiones y copias por usuario - Impresoras B/N

Clics por usuario.xlsx

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

Nombre de la impresora	Ubicación	Blanco y negro
ricohpiso23a	Bogotá Sede Central	17.256
ricohpiso23b	Bogotá Sede Central	15.910
ricohpiso9a	Bogotá Territorial	14.838
ricoh-bmanga-ofc205	Bucaramanga	14.581
ricohcl32-rcc	Bogotá Territorial	12.328
ricohpiso5a	Bogotá Sede Central	11.544
ricoh-cali-piso3	Cali	11.330
ricoh-cali-piso4	Cali	11.025
ricoh-cali-piso2-atc	Cali	9.134
ricohpiso21a	Bogotá Sede Central	8.896

Tabla 103126 Top 10 de impresoras con mayor uso

Top Impresoras.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	790
ricohpiso25c	Bogotá Sede Central	bhernandez	Bibiana Hernandez Hernandez	198
ricohpiso25c	Bogotá Sede Central	jrey	Julian Andres Rey Reina	30

Tabla 104127 Top usuarios impresión a color

Piso25C.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	1.020	165.977	120.570	46.427	166.997	40.359	272,5
D.T. Valle del Cauca	0	48.635	35.248	13.387	48.635	12.561	89,7
D.T. Santander	0	36.295	27.178	9.117	36.295	9.556	108
D.T. Antioquia	0	24.311	17.540	6.771	24.311	6.961	80,1
D.T. Bogotá	0	21.750	13.466	8.284	21.750	6.407	26,1
OE	0	20.690	14.306	6.384	20.690	5.082	82,8
D.T. Atlántico	0	18.528	10.942	7.586	18.528	5.897	47,6
D.T. Cundinamarca	0	18.154	10.778	7.376	18.154	4.632	121,6
D.T. Norte de Santander	0	15.130	10.098	5.032	15.130	4.449	87,6
D.T. Tolima	0	14.997	9.996	5.001	14.997	3.719	57,4

Tabla 105 Top oficinas

Oficinas.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	2.699
RICOH-BMANGA-OFC205	D.T. Santander	COPY	1.682
RICOH-CAQUETA-PISO1-PPAL	D.T. Caqueta	COPY	1.039
RICOHPISO23B	Nivel Central	COPY	796
RICOH-LETICIA	D.T. Amazonas	COPY	774
RICOH-MEDELLIN-PISO1	D.T. Antioquia	COPY	740
RICOH-PEREIRA-PISO5-IVC	D.T. Risaralda	COPY	737
RICOHPISO9A	Nivel Central	COPY	728

RICOHGAU-A	D.T. Bogotá	COPY	704
RICOH-MONTERIA-PISO2	D.T. Cordoba	COPY	686

Tabla 106*128* Top 10 impresoras más usadas del servicio de fotocopiado

Copia.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
scelya	Samuel Cely Alvarez	ADJUST	11.180	7
lpanche	Luis Fernando Panche Chiquiza	ADJUST	11.910	6
dzubieta	Diana Marcela Zubieta Nuñez	ADJUST	11.006	6
ekecan	Eliana Karolina Kecan Torres	ADJUST	10.180	6
pbetancourt	Paula Andrea Betancourt Nocua	ADJUST	10.180	5
ysanchezs	Yudi Nathalia Sanchez Salamanca	ADJUST	10.180	5
jamunoz	Jarrison Alexander Muñoz Vargas	ADJUST	10.000	5
jmrojas	Juan Manuel Rojas Moreno	ADJUST	10.000	5
mvargasm	Maye Liliana Vargas Manosalva	ADJUST	10.000	5
mzambrano	Michell Andrea Zambrano Garcia	ADJUST	10.000	5

Tabla 107129 Ampliación de cuota de impresión

Aumento de Cuota.xlsx

- Despacho de papel, tóner y unidades a nivel nacional

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

	feb-26		mar-26		abr-26	
	Resmas Carta	Resmas Oficio	Resmas Carta	Resmas Oficio	Resmas Carta	Resmas Oficio
Total, Resmas	490	432	252	229	669	386
Total, Cajas por Tamaño	49,00	43,20	25,20	22,90	66,90	38,60
Total, Cajas Enviadas	**92,20**		**48,10**		**105,50**	

Tabla 108 Despacho de papel a sedes del Ministerio del Trabajo

Durante el período, se despacharon a sedes del ministerio un total de 24 toners para impresora B/N IM430, 6 unidades de imagen y 2 unidades fusoras.

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 109130 Cargo 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 110 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 abril de 2026:

MES	DETALLE	CANTIDAD
Abril	Multifuncional blanco y negro rango medio - Clic de impresión tóner y papel carta	**523.019**
	TOTAL	**523.019**

Tabla 111131 Clics de impresión de abril 2026 – Multifuncional B/N

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

Mes 2026	Febrero	Marzo	Abril
Cantidad de clics consumidos	584.994	593.134	523.019

Tabla 112 Tendencia de consumo de clics B/N

El consumo mensual establecido para el servicio es de **450.000** clics de impresión en B/N a nivel nacional; para el período del informe se presentó un consumo de **490.533** clics de impresión (esto incluye **2.608** de la impresora de contratos piso 8) y **32.486** de fotocopias para un total de **523.019** 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 abril de 2026:

MES	DETALLE	CANTIDAD
Abril	Impresora color rango medio - Cargo fijo mensual - Clic de impresión tóner y papel carta	1.018
Total		1.018

Tabla 113132 Clics de Impresión – Impresora Color

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

Mes	Febrero	Marzo	Abril
Cantidad de clics consumidos	555	1.083	1.018

Tabla 114Tendencia 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 **1.018** clics para este servicio, por lo cual no se superó dicho consumo.

- Medición de ANS Outsourcing de impresión

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

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

Tabla 115133 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 abril 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.

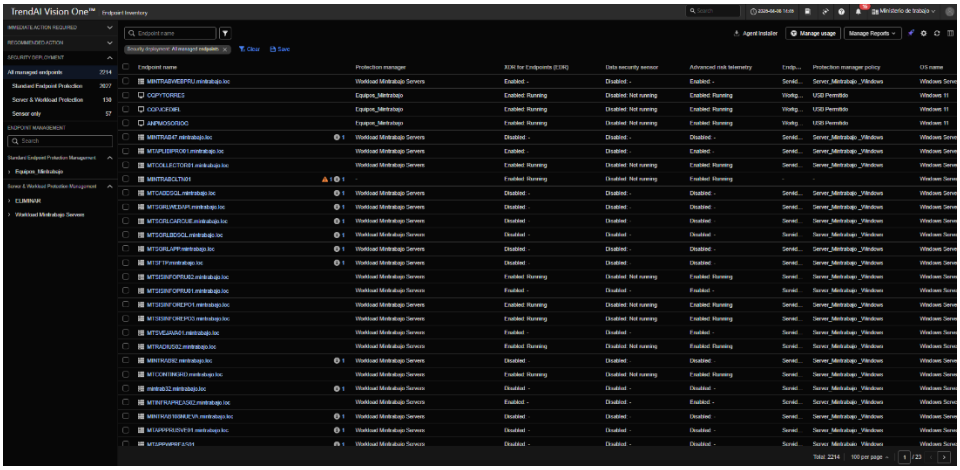


Ilustración 134 Equipos consola antivirus

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 (2104) de Mintrabajo, se cuenta con 2255 licencias, se tienen disponibles 151.

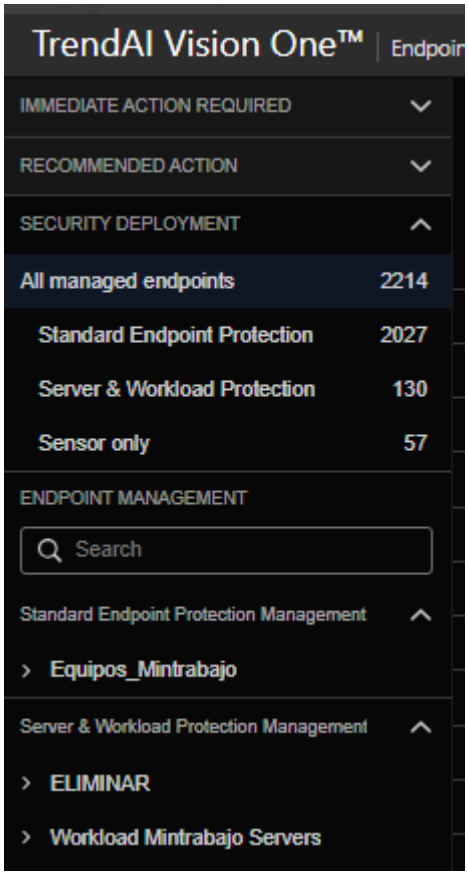


Ilustración 135 Gestión consola antivirus – equipos usuario final

4.7.3 Top 10 Virus Detectados

Durante el mes analizado, los eventos detectados por la plataforma TrendMicro se detectaron un total de 205 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:

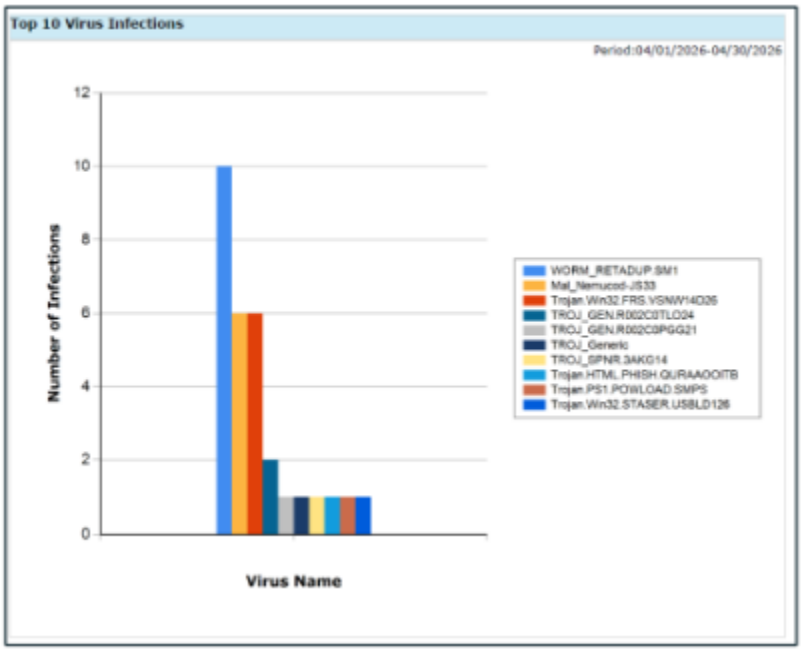


Ilustración 136 Top 10 virus detectado

Top 10 Virus Infections		
Virus Name	# of Infections	Detected By
WORM_RETADUP.SM1	10	Desktop (10)
Mal_Nemucod-JS33	6	Desktop (6)
Trojan.Win32.FRS.VSNW14D26	6	Desktop (6)
TROJ_GEN.R002C0TLO24	2	Desktop (2)
TROJ_GEN.R002C0PGG21	1	Desktop (1)
TROJ_Generic	1	Desktop (1)
TROJ_SPNR.3AKG14	1	Desktop (1)
Trojan.HTML.PHISH.QURAAOOITB	1	Desktop (1)

Ilustración 137 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.

WORM_RETADUP.SM1: esta amenaza corresponde a una variante del gusano conocido como Retadup worm, una amenaza diseñada para propagarse automáticamente entre

sistemas y ejecutar actividades maliciosas sin intervención del usuario, estas detecciones se realizaron en unidad removible F:/ y fueron eliminadas por parte del antivirus.

Mal_Nemucod-JS33: Variante de la familia Nemucod, caracterizada por distribuirse mediante archivos JavaScript adjuntos en campañas de phishing. Actúa como downloader, contactando servidores remotos para descargar y ejecutar malware adicional (frecuentemente ransomware o troyanos bancarios). La detección se presentó en los equipos BODSDIAZR, GUDACAICEDO. Las detecciones fueron controladas por la solución.

Trojan.Win32.FRS.VSNWI4D26: Esta es la detección genérica de Trend Micro para archivos que presentan un comportamiento sospechoso y que podrían dañar los sistemas. Los troyanos son una clasificación general de malware que engloba archivos, aplicaciones o programas maliciosos que se descargan habitualmente de Internet. estos troyanos también descargan o instalan otro malware y acceden a URL para enviar y recibir comandos de un atacante remoto. Los atacantes remotos pueden controlar los sistemas y hacer que realicen acciones maliciosas sin el conocimiento del usuario.

TROJ_GEN.R002C0TL024: Esta es la detección genérica de Trend Micro para archivos que presentan un comportamiento sospechoso y que podrían dañar los sistemas. Los troyanos son una clasificación general de malware que engloba archivos, aplicaciones o programas maliciosos que se descargan habitualmente de Internet. estos troyanos también descargan o instalan otro malware y acceden a URL para enviar y recibir comandos de un atacante remoto. Los atacantes remotos pueden controlar los sistemas y hacer que realicen acciones maliciosas sin el conocimiento del usuario.

TROJ_GEN.R002COPGG21: Esta es la detección genérica de Trend Micro para archivos que presentan un comportamiento sospechoso y que podrían dañar los sistemas. Los troyanos son una clasificación general de malware que engloba archivos, aplicaciones o programas maliciosos que se descargan habitualmente de Internet. estos troyanos también descargan o instalan otro malware y acceden a URL para enviar y recibir comandos de un atacante remoto. Los atacantes remotos pueden controlar los sistemas y hacer que realicen acciones maliciosas sin el conocimiento del usuario.

TOP 5 EQUIPOS

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

HOST	Cantidad	Virus/malware
BODSDIAZR	4	Mal_Nemucod-JS33
BOPFOVIEDO	4	Trojan.Win32.FRS.VSNW14D26
GUDACAICEDO	2	Mal_Nemucod-JS33
PEDDBEDOYA	2	Trojan.Win32.FRS.VSNW14D26
BYDDNITOLAC	2	TROJ_GEN.R002C0TLO24
PTDLMORA	1	TROJ_GEN.R002C0PGG21
DESKTOP-3CFF	1	Trojan.Win32.STASER.USBLD126
SNPVMENDEZ	1	Trojan.HTML.PHISH.QURAAOOITB
BOPCMENDIETA	1	TROJ_Generic
BADORAMOS	1	Trojan.PS1.POWLOAD.SMPS

Ilustración 138Top 5 Equipos

BODSDIAZR

En el equipo se registran 4 detecciones asociadas a la amenaza reconocida como Mal_Nemucod-JS33 los archivos fueron sanitizados de manera correcta por parte del antivirus.

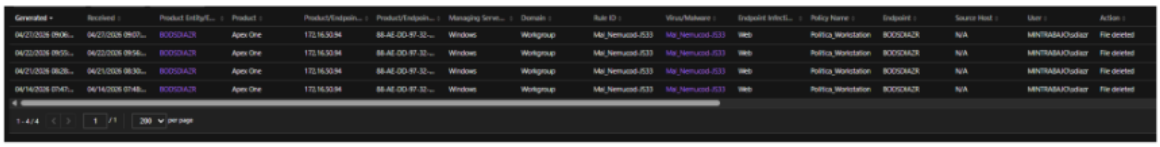


Ilustración 139 BODSDIAZR

BOPEOVIEDO

En el equipo se registran 4 detecciones asociadas a la amenaza reconocida como Trojan.Win32.FRS.VSNWI4D26 los archivos fueron sanitizados de manera correcta por parte del antivirus. Adicional el equipo y no fue necesario ejecutar acciones adicionales en el equipo

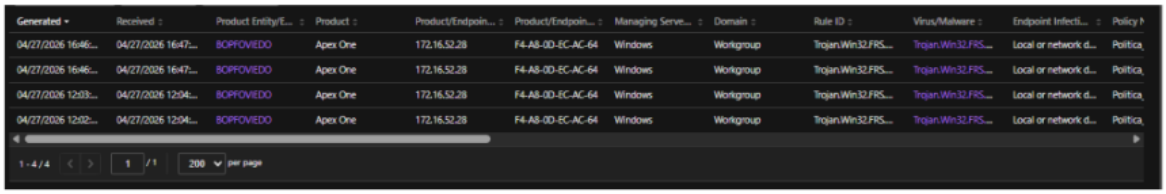


Ilustración 140 BOPEOVIEDO

UDACAICEDO

En el equipo se reportan 11 detecciones de la amenaza de una amenaza denominada Mal_Nemucod-JS33 los archivos fueron eliminados de manera

correcta por parte del antivirus

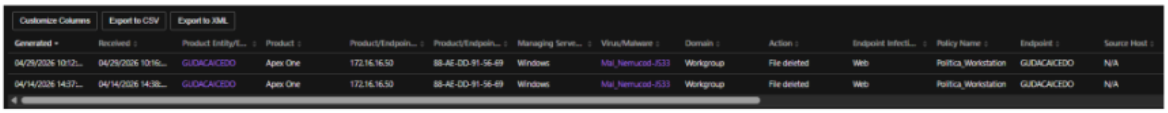


Ilustración 141 UDACAICEDO

PEDDBEDOYA

En el equipo se reportan 2 detecciones de la amenaza de un troyano de tipo genérico que corresponden a clasificación general de malware para archivos, aplicaciones o programas maliciosos que se descargan comúnmente de Internet.

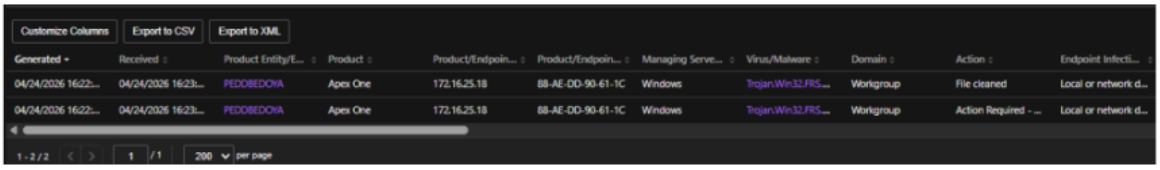


Ilustración 142 PEDDBEDOYA

Eventos Ransomware

Ransomware es una de las amenazas cibernéticas más críticas y costosas de la actualidad. Se trata de un tipo de malware que cifra o bloquea el acceso a los sistemas y datos corporativos, exigiendo un rescate económico para su liberación. Su impacto va mucho más allá de la pérdida de archivos: puede paralizar operaciones, dañar la reputación y generar pérdidas millonarias.

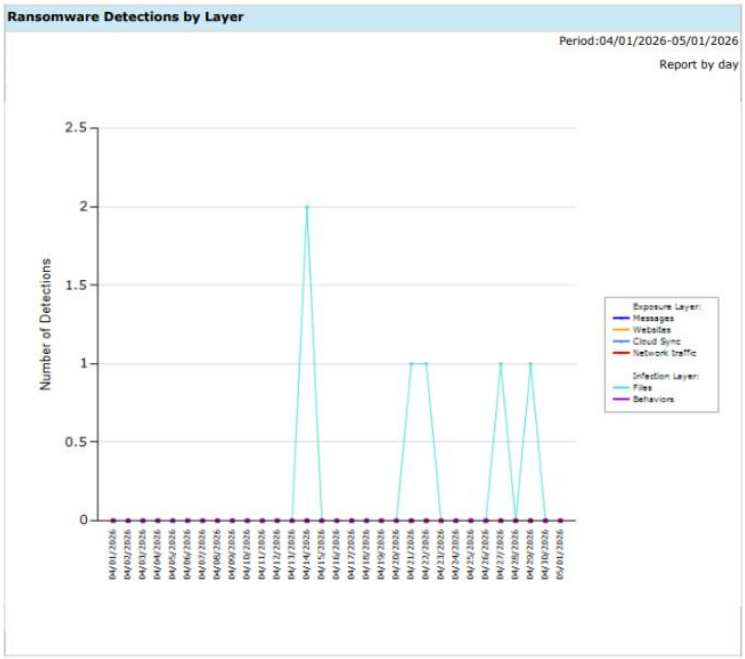


Ilustración 143 Eventos Ransomware

En el mes de abril 2026, se presentaron eventos 6 eventos escalados por detección de malware Ransomware, estas detenciones se realizaron en los hosts: GUDACAICEDO, BODSDIAZR.
Los eventos indicados fueron contenidos por la solución de Trend Micro en el transcurso del mes, sin embargo, los eventos están asociados al manejo de navegación, no a una materialización o intento de ataque por alguna familia de Malware.
.

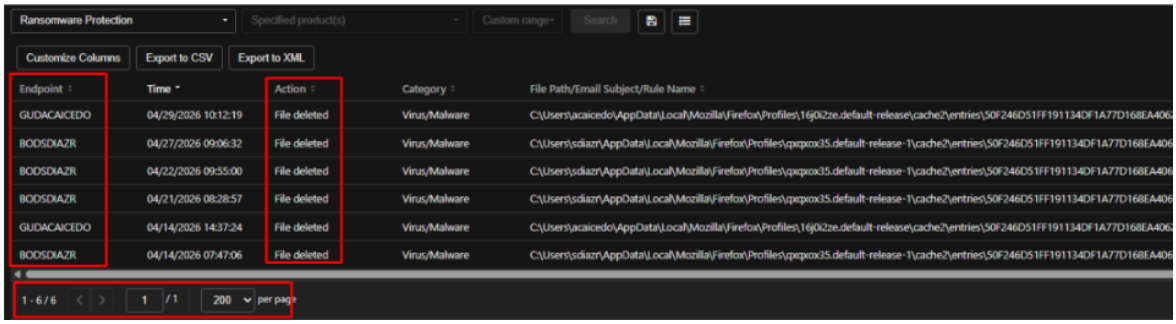


Ilustración 144 captura eventos ransonware

Licenciamiento

Actualmente se cuenta con los módulos activos de la solución y licenciamiento activo hasta 31-07-2026.

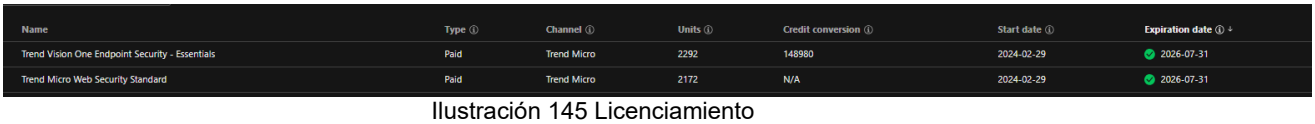


Ilustración 145 Licenciamiento

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 abril 2026 sobre la infraestructura tecnológica registrada del Ministerio de Trabajo, con el objetivo de identificar los hallazgos a nivel de vulnerabilidades que pueden alterar el nivel de exposición cibernética del negocio.

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

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

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

Validación: Realizar pruebas exhaustivas antes de implementar parches en entornos de producción.

4.7.4.1 Inventario y licenciamiento

El inventario de activos registrado en la herramienta Tenable Nessus Professional, se basa en la priorización y selección de aquellos activos que son críticos o core del negocio para el **Ministerio del Trabajo** y los resultados del escaneo "TCP Discovery" inicial, con el fin de validar el alcance desde el servidor Nessus. Al cierre de abril del 2026 se tienen registrados 319 activos TI, de los cuales, se registró un alcance sobre 305 (97%) activos.

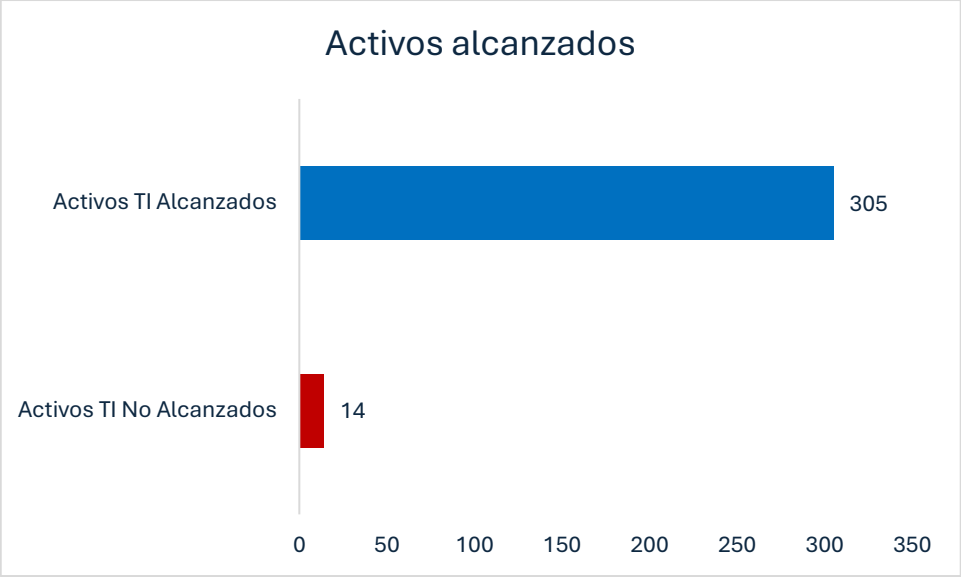


Ilustración 146 *Gestión consola Nessus*

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 - WEEKLY I 2026 SEMANAL I - LINUX	Vulnerability	Weekly on Sun at 8:00 PM	May 3 at 9:27 PM
2026 - WEEKLY I 2026 SEMANAL I - FORTISIEM	Vulnerability	Weekly on Sun at 6:00 PM	May 3 at 6:47 PM
2026 - WEEKLY I 2026 SEMANAL I - WINDOWS	Vulnerability	Weekly on Sat at 8:00 PM	May 3 at 3:41 AM
2026 - WEEKLY I 2026 SEMANAL I - NETWORKING	Vulnerability	Weekly on Sat at 2:00 AM	May 2 at 3:37 AM
2026 - WEEKLY I 2026 SEMANAL I - NO AUTH	Vulnerability	Weekly on Sat at 1:00 AM	May 2 at 1:18 AM

Ilustración 147 *Escaneos programados*

Clasificación de Prioridad de Vulnerabilidad por Instancias Totales (VPR)
La plataforma Tenable io calcula un VPR (Vulnerability Priority Rating) dinámico para la mayoría de las vulnerabilidades. El VPR es un complemento dinámico de los datos proporcionados por la puntuación CVSS de la vulnerabilidad, ya que Tenable actualiza el VPR para reflejar el panorama de amenazas actual a nivel mundial. Los valores de VPR oscilan entre 0,1 y 10; un valor más alto representa una mayor probabilidad de explotación.

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

4.7.4.3 TOP 10 – Vulnerabilidades más explotables

Al cierre de abril del 2026, el activo TI con la mayor cantidad de vulnerabilidades identificadas corresponde al host (172.20.22.188), con un total de 2.035 hallazgos, corresponde a un servidor Red Hat Enterprise Linux Server release 7.9 (Maipo) y la mayoría de las vulnerabilidades están asociadas a Unpatched, es decir, son actualizaciones de paquetes pendientes que no se pueden desplegar debido a que el proveedor no las ha autorizado en los repositorios originales de Red Hat.

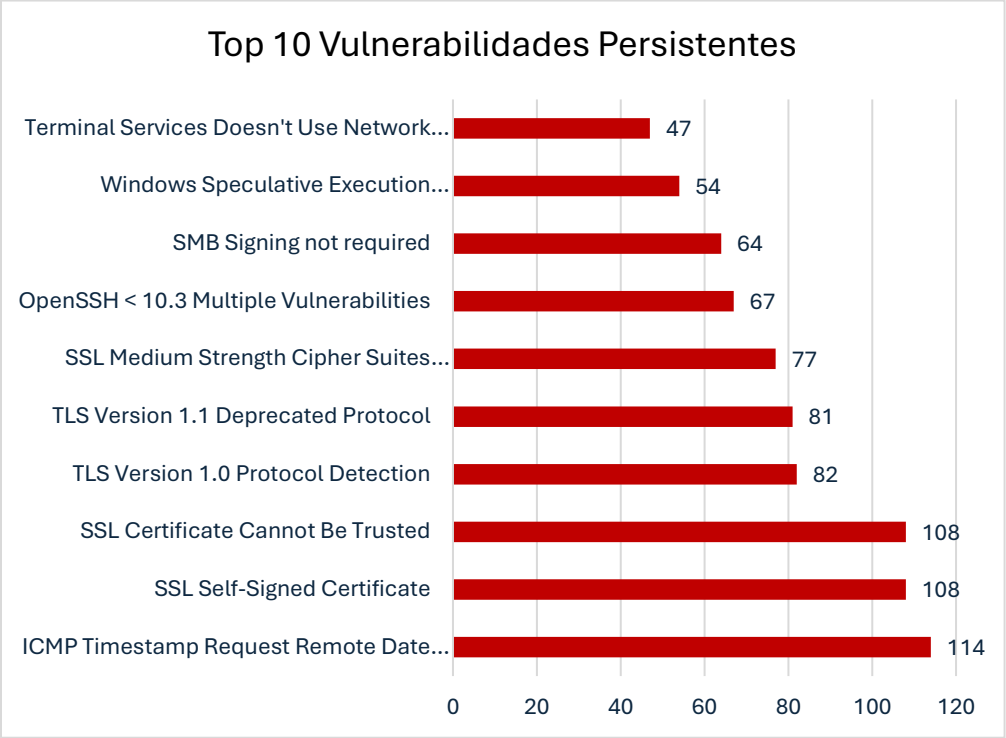


Ilustración 148 TOP 10 - Activos más explotables

Al cierre de abril del 2026, la vulnerabilidad identificada con la mayor cantidad de persistencias corresponde a (ICMP Timestamp Request Remote Date Disclosure), con un total de 114 hallazgos, consiste en un tipo de paquete ICMP, específicamente tipo 13 y 14, los cuales le permiten a un ciberdelincuente conocer la fecha y hora del dispositivo que responde a la solicitud.

4.7.4.4 Estrategia de remediación y/o mitigación

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

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

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

4.7.4.5 Resumen de mitigación efectuada

A continuación, se contrasta un resumen de las actividades relacionas con la gestión de vulnerabilidades correspondientes al Snapshot del semestre I 2026, el cual reportó un total de 4.323 vulnerabilidades TI en las severidades:

490 vulnerabilidades críticas.
1.506 vulnerabilidades altas.
1.965 vulnerabilidades medias.
362 vulnerabilidades bajas.

Durante el periodo de abril del 2026, se remediaron un total de 165 vulnerabilidades, de las cuales, 7 fueron de severidad crítica, 71 de severidad alta, 14 de severidad media y 73 de severidad baja. Por otro lado, con relación a indicadores semestrales, se gestionaron un total de 773 vulnerabilidades, de las cuales, 80 fueron de severidad crítica, 375 de severidad alta, 172 de severidad media y 146 de severidad baja.

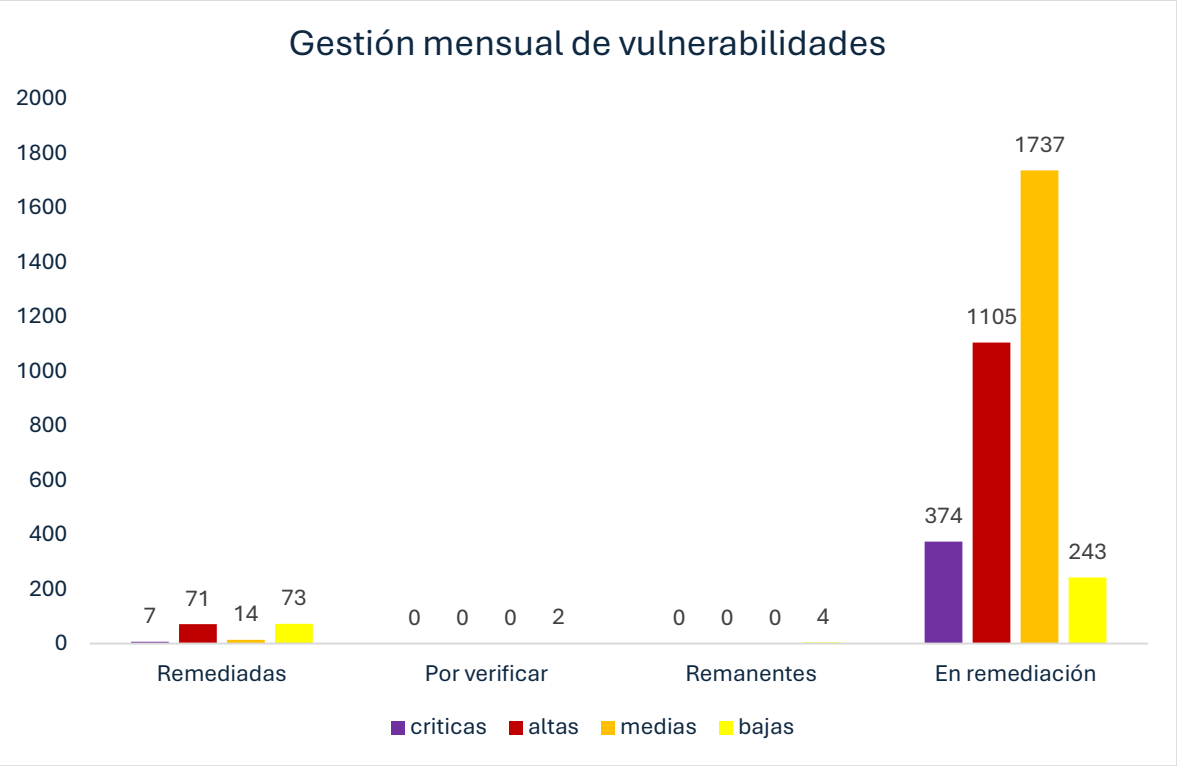


Ilustración 149 Vulnerabilidades gestionadas vs en remediación

Ethical Hacking del **primer semestre 2026**
Se informa el inicio de la segunda fase del Ethical Hacking correspondiente al primer semestre de 2026 para el proyecto del Ministerio del Trabajo, conforme al cronograma de ejecución establecido.

Esta fase tiene como objetivo la validación de los requerimientos técnicos necesarios para la ejecución de las pruebas, incluyendo:

Validación del alcance definido sobre los activos objetivo
Verificación de credenciales de autenticación (dado que la prueba se realizará bajo enfoque de caja blanca)
Revisión de configuraciones a nivel de equipos de red y dispositivos perimetrales

FASE	RIESGO	RESPONSABLE	PROGRESO	FECHA INICIO	FECHA FIN	DÍAS
Levantamiento de Información	Bajo	Daniel Castillo	100%	Marzo 30, 2026	Abril 1, 2026	3
Planeación de la Prueba	Bajo	Daniel Castillo	100%	Abril 6, 2026	Abril 24, 2026	15
Ejecución de la Prueba	Alto	Daniel Castillo	0%	Abril 27, 2026	Mayo 8, 2026	9
Documentación	Medio	Daniel Castillo	0%	Mayo 11, 2026	Mayo 22, 2026	9
Presentación de Resultados	Bajo	Daniel Castillo	0%	Mayo 25, 2026	Mayo 29, 2026	5

Ilustración 150 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 abril 2025, se adjunta informe socializado.

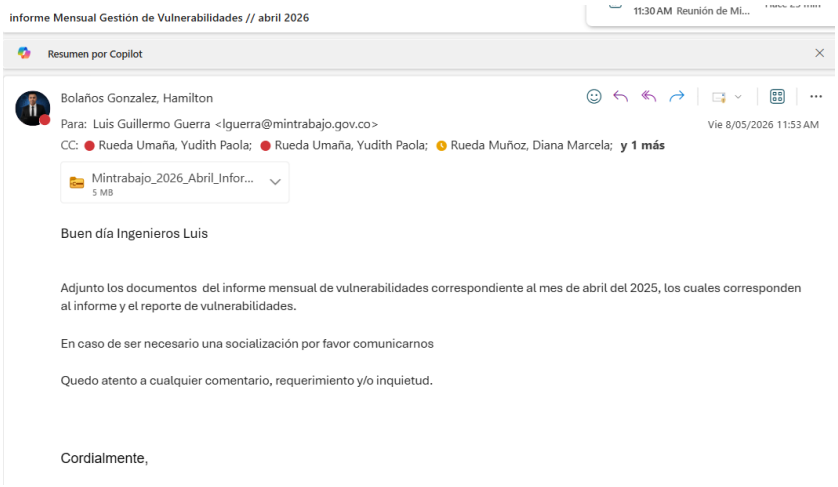


Ilustración 151 captura envío de correo gestión de vulnerabilidades

- Medición de ANS Antivirus

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

ID	Indicadores	Resultado	Meta
AV-1	Cobertura de antivirus	96,82%	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 116152 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 abril 2026, se realizó la evaluación cuantitativa de la muestra de 267 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:

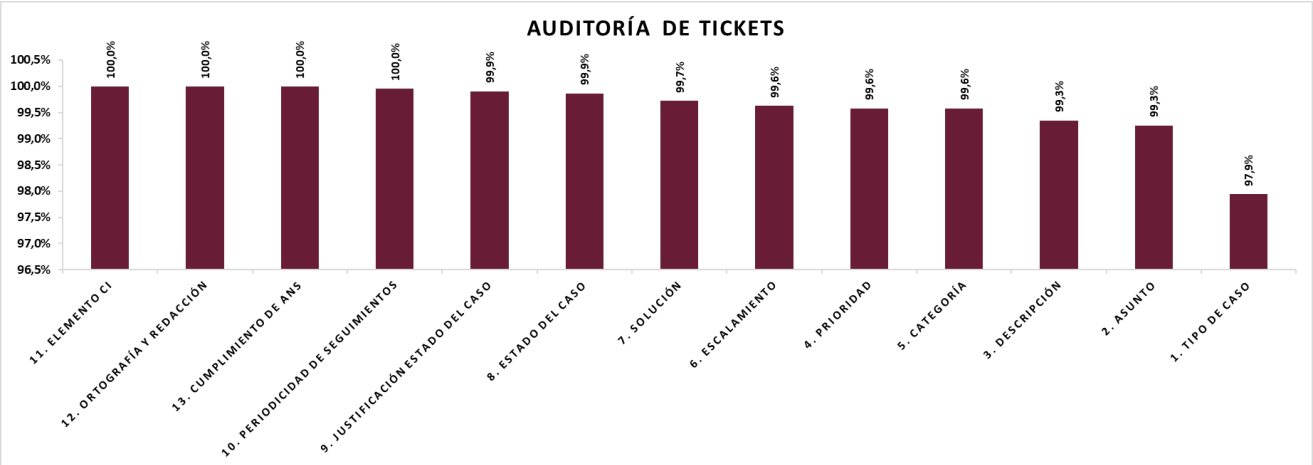


Ilustración 153 Resultado General

Durante el mes de abril de 2026 se ejecutaron 267 auditorías de calidad al servicio del Ministerio de Trabajo, identificándose 77 afectaciones, lo que permitió alcanzar un indicador de cumplimiento (PDA) del 96,40%, manteniéndose dentro de los niveles esperados de calidad y control operativo.

Los resultados evidencian que los criterios relacionados con Elemento CI, Ortografía y redacción y Cumplimiento de ANS alcanzaron un desempeño del 100%, reflejando una adecuada gestión documental, claridad en los registros y cumplimiento oportuno de los acuerdos de servicio establecidos.

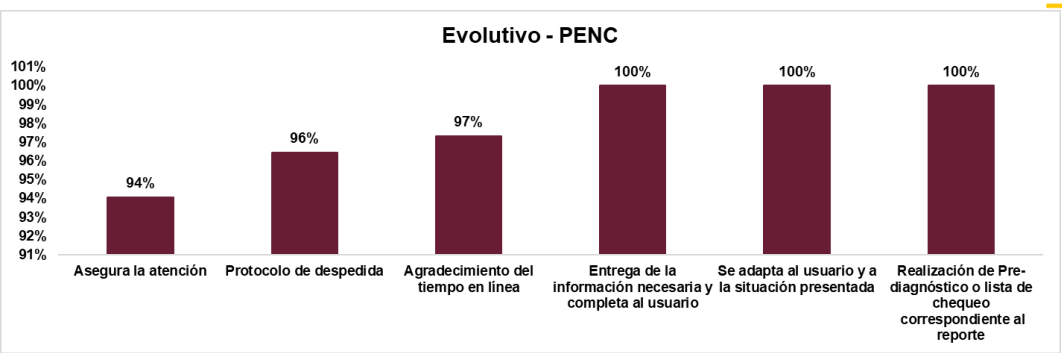
Las principales oportunidades de mejora se concentraron en el diligenciamiento de campos operativos y de clasificación de los casos, especialmente en el criterio “Tipo de caso”, el cual registró 44 afectaciones, seguido de “Asunto” con 16 casos y “Descripción” con 14 casos. Estas novedades estuvieron asociadas principalmente a errores de categorización, selección incorrecta del tipo de requerimiento y registros incompletos en la descripción inicial del caso, situaciones que no generaron impacto en la atención ni en el cumplimiento de los ANS, pero sí representan oportunidades de fortalecimiento en la calidad del registro y trazabilidad de la información.

Adicionalmente, se identificaron oportunidades menores en los criterios de Prioridad, Categoría, Escalamiento y Solución, asociadas a inconsistencias puntuales en la tipificación y actualización de casos durante la operación diaria. Estas afectaciones corresponden principalmente a errores operativos derivados del volumen transaccional y de la ejecución manual de algunos registros en herramienta.

Como acciones de mejora, se reforzarán las jornadas de retroalimentación con el equipo operativo, enfocadas en la correcta clasificación y documentación de los casos, así como en la validación de información antes del cierre de los tickets. De igual forma, se continuará realizando seguimiento periódico a los hallazgos recurrentes con el fin de mantener la tendencia positiva de cumplimiento y fortalecer continuamente los niveles de calidad del servicio.

5.2 Evaluación de calidad de llamadas

En el mes de abril 2026, se realizó la evaluación cuantitativa de la muestra de las llamadas presentadas con una duración mayor a 1:30 minutos
Para el cálculo de llamadas, se evaluaron 28 llamadas con los siguientes criterios definidos, obteniendo el siguiente resultado:



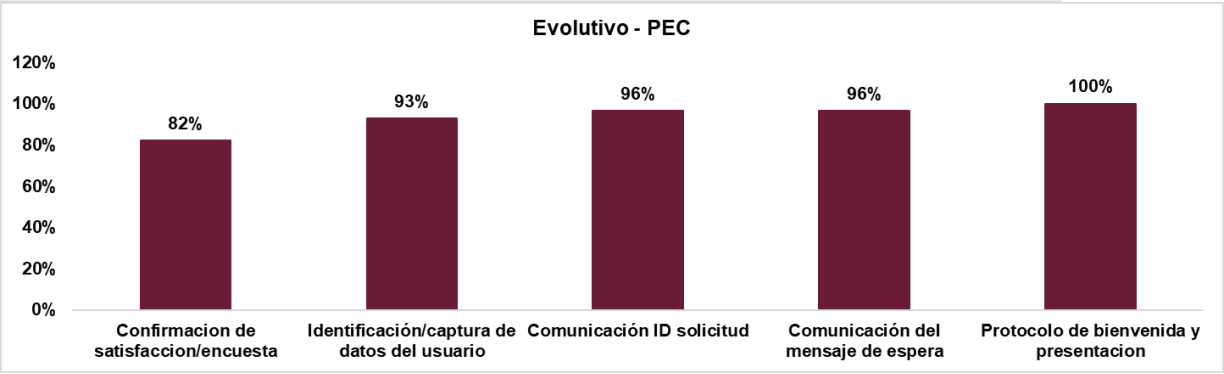


Ilustración 154 Resultado de criterios y parámetros - Calidad de llamadas

Durante el mes de abril de 2026 se realizaron 28 monitoreos de calidad sobre las llamadas gestionadas en la operación, obteniendo un resultado de 97,97% en Precisión de Error No Crítico (PENC) y 93,57% en Precisión de Error Crítico (PEC), evidenciando un adecuado nivel de cumplimiento en los lineamientos de atención y comunicación con el usuario.

En los criterios asociados a errores no críticos, los resultados reflejan una adecuada adherencia a los protocolos establecidos, destacándose con cumplimiento del 100% los ítems relacionados con la entrega de información completa al usuario, adaptación a la situación presentada y realización del prediagnóstico o lista de chequeo correspondiente.

Las principales oportunidades de mejora en PENC estuvieron concentradas en el criterio “Asegura la atención”, con 5 hallazgos sobre 84 oportunidades evaluadas, seguido de “Agradecimiento del tiempo en línea” con 3 casos y “Protocolo de despedida” con 1 caso. Estas situaciones estuvieron asociadas principalmente a omisiones parciales en el cierre de la interacción o en la validación completa de la atención antes de finalizar la llamada, sin generar afectación en la solución brindada al usuario.

En cuanto a los errores críticos (PEC), el criterio con mayor oportunidad de mejora fue “Confirmación de satisfacción/encuesta”, registrando 5 hallazgos y alcanzando un cumplimiento del 82%, evidenciando que en algunos casos no se realizó de manera completa la invitación o confirmación de participación en

encuesta al finalizar la atención. Asimismo, se identificaron hallazgos menores en “Identificación/captura de datos del usuario”, “Comunicación ID solicitud” y “Comunicación del mensaje de espera”, asociados principalmente a omisiones operativas durante la gestión de llamadas.

Es importante resaltar que el criterio “Protocolo de bienvenida y presentación” alcanzó un cumplimiento del 100%, reflejando el adecuado inicio de las interacciones y la correcta identificación por parte de los analistas.
Como parte de las acciones de mejora, se fortalecerán las sesiones de retroalimentación enfocadas en el cumplimiento integral del protocolo de atención telefónica, especialmente en las actividades de cierre de llamada, confirmación de satisfacción y validación de información suministrada al usuario.
Adicionalmente, se continuará realizando seguimiento continuo a los hallazgos recurrentes para mantener y mejorar los indicadores de calidad del servicio.

5.3 Práctica de Mejora

Dar a conocer las actividades de la Práctica de Mejora Continua correspondientes a abril de 2026. Este apartado contiene información relevante sobre las acciones de mejora identificadas por los Servicios TIC y Prácticas ITIL.

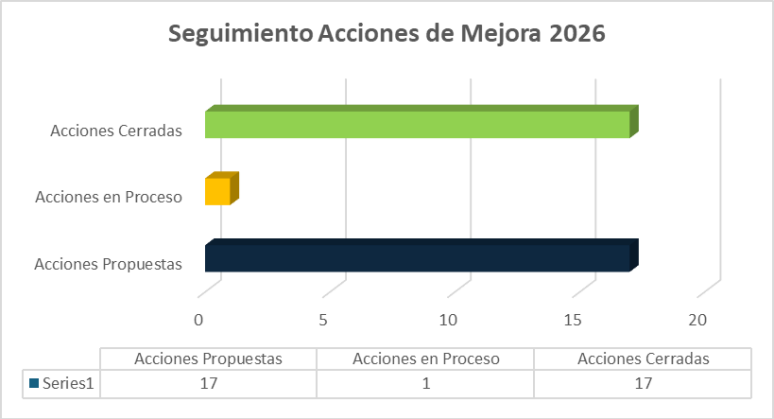


Ilustración 155 Seguimiento Práctica Mejora

En el anterior gráfico, se evidencia de las (17) acciones de mejora identificadas, se observa el cumplimiento de 94%, al corte del 30 de abril de 2026 se encuentran cerradas (16) y cumplen con las evidencias entregadas por los responsables de cada acción y en proceso de implementación (1) acción de mejora.

Durante el inicio de la Práctica de mejora, se realizaron diferentes actividades de socialización y capacitación, con el fin de establecer mecanismos de identificación y participación de los diferentes Servicios TIC, por lo tanto, para dar una medición al su cumplimiento de las acciones propuestas, se estableció el siguiente indicador 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 **AMI**: Cantidad de Acciones ejecutadas en el periodo. **TAM:** Total de Acciones planificadas para el período.	>= 70%	Trimestral

Tabla 117 KPI Practica de Mejora

De acuerdo con el indicador establecido, se ha realizado la medición durante enero a marzo de 2026 de manera trimestral y sus resultados han sido los siguientes:

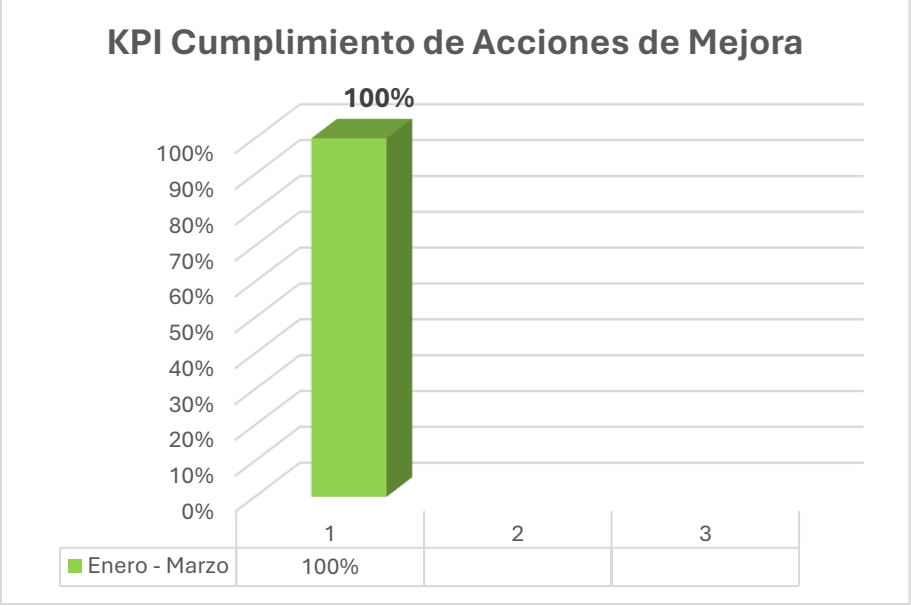


Ilustración 156 Resultado de Cumplimiento AM

Durante el trimestre, se realiza seguimiento de las (50) acciones de mejora del proyecto, las cuales solo se encuentran pendientes (1) pendientes del 2025 y se seguirá consultando de manera periódica al grupo responsable de las acciones, con el fin de realizar el cierre durante el 2 trimestre del 2026.

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

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

SERVICIO/ PRÁCTICA	NOMBRE	DESCRIPCIÓN	¿MATERIALIZADO ?	ACCIONES PARA REALIZAR
Todos	Indisponibilidad de la nube privada que afecte la prestación de servicios de TI	Falla en la prestación de los servicios de TI por falla en la infraestructura de TI provista por la UT	NO	Se dispuso de la infraestructura y recursos que soportan las estrategias de contingencia y recuperación. El suministro del servicio de energía eléctrica fue normal en los sitios alternos. Se realización copias de respaldo de las bases de datos, información y sistemas de información se realiza de acuerdo con la política institucional de copias de respaldo.
Todos	Pérdida de información	Falla en la generación de las copias de respaldo de la información centralizada	NO	Se realizan pruebas de restauración de backups generados por la herramienta definida para el proyecto
Todos	Pérdida de disponibilidad	Perdida de disponibilidad de la infraestructura que soporta los servicios y activos de información de TI	NO	No se ha presentado dicha situación.
Todos	Pérdida de integridad	La ausencia de actualizaciones de seguridad en las aplicaciones podría poner en riesgo la integridad y disponibilidad de los sistemas, permitiendo la ejecución de código malicioso.	NO	Se realizó la planeación del primer ejercicio de Ethical Hacking. Se ejecutaron de manera oportuna y permanente las actualizaciones y controles necesarios para remediar las vulnerabilidades detectadas durante las pruebas de seguridad.
DRP	Indisponibilidad de servicios de TI	Indisponibilidad de la Infraestructura principal alojada en Datacenter Cirion Colombia XV	NO	Se dispuso de la infraestructura y recursos que soportan las estrategias de contingencia y recuperación. El suministro del servicio de energía eléctrica fue normal en los sitios alternos. Se realización de copias de respaldo de las bases de datos, información y sistemas de información se realiza de acuerdo 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,	NO	El personal asignado estuvo disponible durante el periodo.

SERVICIO/ PRÁCTICA	NOMBRE	DESCRIPCIÓN	¿MATERIALIZADO ?	ACCIONES PARA REALIZAR
		administrar y operar los servicios.		
Telefonia 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 118 Gestión de Riesgos

7 BOLSA DE RECURSOS

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

Descripción	Cantidad	Precio total antes de IVA
Switch de acceso 48 puertos	8	$4.068.408
Clics adicionales B/N	73019	$10.514.736
	Subtotal	$14.583.144

Tabla 119 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	100,00%	95,00%
	Tiempo de solución de incidentes por soporte en sitio	99,45%	90,00%
	Tiempo de solución de requerimientos por soporte en sitio	99,86%	90,00%
	Tiempo de respuesta de la mesa de servicio	99,06%	85,00%
	Abandono de llamadas	0,00%	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	96,82%	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	100,00%	90,00%
	Tiempo de solución de requerimientos asociado a los servicios de aplicaciones especializadas	98,72%	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	100,00%	90,00%
	Tiempo de solución de requerimientos asociado a los servicios de administración, soporte y monitoreo	100,00%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	99,87%	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	99,92%	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 120 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 abril
- Detalle_llamadas_recibidas_(01.04.2026-30.04.2026)
- Datos_Mintrabajo_abril
- Informe Sistema Nacional de Registro de Trabajadores - SNRT

FIN DEL DOCUMENTO