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

Enero de 2026

DOCUMENTO/ ARCHIVO	
Código:	**Informe Gestión - Unión Temporal Gestión TIC 2023**
Nombre Archivo:	**Informe Gestión - Unión Temporal Gestión TIC 2023 – enero 2026**
Fecha:	9/02/2026
Versión:	1

REGISTRO DE CAMBIOS			
Versión	**Páginas**	**Fecha Modificación**	**Motivo del cambio**
1	238	9/02/2026	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 23
2.1.2.1. Práctica Acuerdos Niveles de Servicio (ANS) 23
2.1.2.2. Práctica Habilitación de Cambios 24
2.1.2.3. Práctica Gestión de Activos 26
2.1.2.4. Práctica Catálogo de servicios 26
2.1.2.5. Práctica de Problemas 28
2.1.2.6. Práctica de Incidentes 29
2.1.2.7. Práctica de Requerimientos 37
2.1.2.8. Práctica de Eventos 40
2.1.2.9. Práctica de Disponibilidad 54
2.1.2.10. Práctica de Implementación 57
2.2 Mesa de Servicios y Soporte en Sitio 58
3 LINEA DE SERVICIOS CENTRALES 69
3.1 Datacenter Principal 69
3.1.1 Datacenter Alterno y DRP 74
3.1.2 Procesamiento almacenamiento y respaldo Servicio Windows y Office 365. 80
3.1.3 Procesamiento, almacenamiento y respaldo - Nube Privada 86
3.1.4 Aplicaciones Especializadas 106
3.1.5 No aplica 158
3.1.6 Seguridad Informática 158
3.1.6.1 Firewalls de nueva generación 158
3.1.6.2 Sandbox – Amenazas día 0 164
3.1.6.3 SIEM - Solución de correlación de eventos de seguridad, disponibilidad y recursos 167
3.1.6.4 WAF - Servicio de tipo “Firewall de Aplicaciones Web” 173
3.1.6.5 Solución de Anti-DDoS 175
3.1.6.6 Casos atendidos de los servicios de seguridad 175
3.1.6.7 Análisis de riesgo 177
3.1.6.8 Políticas y procedimiento de seguridad 178
3.1.7 Licenciamiento 179
3.1.8 Administración, soporte y monitoreo 179
3.2 No aplica 180
3.3 Conectividad WAN, SDWAN e Internet 180
3.3.1 Canales WAN 180
3.3.1.1 Incidentes de Conectividad 182
3.3.1.2 Topología Actual 183
3.3.2 Canales SDWAN e Internet Dedicado 183
4 LINEA DE SERVICIOS EN SEDE 188
4.1.1 Equipos de Cómputo de usuario final 188
4.1.2 Equipos de Escritorio 192
4.1.3 Equipos Portátiles 192
4.2 Conectividad LAN y WLAN 192
4.2.1 Switch CORE Sede Principal 194

4.2.2 Switch para conexiones perimetrales (EDGE) en sede principal 194
4.2.3 Switch de acceso 24 puertos 194
4.2.4 Switch de acceso 48 puertos 195
4.2.5 Puntos de Acceso 196
4.3 Telefonía IP 197
4.3.1 Teléfono Gama Media 197
4.3.2 Teléfono Gama Baja 197
4.3.3 Troncales SIP 198
4.3.4 No Aplica 198
4.3.5 No Aplica 198
4.3.6 Módems 4G – Con plan de 50 Gbps 198
4.4 Energía Regulada UPS 204
4.4.1 UPS 10 kVA 204
4.4.2 UPS 15 kVA 205
4.4.3 UPS 20 kVA 205
4.5 No aplica 208
4.6 Outsourcing de Impresión 208
4.6.1 No aplica 212
4.6.2 Multifuncional B/N rango medio – Cargo fijo mensual 212
4.6.3 Impresora Color rango medio – Cargo fijo mensual 212
4.6.4 No aplica 212
4.6.5 Multifuncional B/N rango medio – Clic de impresión 212
4.6.6 Impresora Color rango medio – Clic de impresión 213
4.7 Antivirus 214
4.7.1 Instalaciones de antivirus en servidores 214
4.7.2 Instalación de antivirus PCs usuarios final 214
4.7.3 Top 10 Virus Detectados 215
4.7.4 Servicio de Vulnerabilidades 221
4.7.4.1 Inventario y licenciamiento 221
4.7.4.2 Escaneos programados 222
4.7.4.3 TOP 10 – Vulnerabilidades más explotables 223
4.7.4.4 Estrategia de remediación y/o mitigación 223
4.7.4.5 Resumen de mitigación efectuada 224
5 GESTIÓN DE CALIDAD DE INFORMACIÓN 225
5.1 Evaluación calidad documental de casos 226
5.2 Evaluación de calidad de llamadas 227
5.3 Práctica de Mejora 227
6 GESTION DE RIESGOS 229
7 BOLSA DE RECURSOS 232
8 MEDICIÓN DE ACUERDOS DE NIVEL DE SERVICIO 232
9 ANEXOS 234

Índice de Tablas

Tabla 1 Atención de solicitudes por Grupo de Especialista 22
Tabla 2 Medición Indicador Porcentaje de Cumplimiento de ANS 24
Tabla 3 Tipificación de los cambios 25
Tabla 4 Medición Indicador Porcentaje de Cambios Exitosos 25
Tabla 5 KPI Práctica Catálogo de Servicios 28
Tabla 6 Consolidado problemas identificados 28
Tabla 7 Estados Incidentes 29
Tabla 8 Top 10 Incidentes 30

Tabla 9 Incidentes Suspendidos 31
Tabla 10 Incidentes Mayores 35
Tabla 11 Medición de KPIs 35
Tabla 12 Estados de Requerimientos 37
Tabla 13 Seguimiento del Backlog Suspendidos 38
Tabla 14 Top 10 de Solicitudes 38
Tabla 15 Detalle de KIP Practica de Requerimientos 39
Tabla 16 Casos reabiertos 40
Tabla 17 KPI Práctica de Eventos 41
Tabla 18 Consolidado disponibilidad de servidores 55
Tabla 19 Consolidado disponibilidad de Directorio Activo 55
Tabla 20 Desagregado de Disponibilidad Directorio Activo 55
Tabla 21 Consolidado disponibilidad de equipos Datacenter principal 55
Tabla 22 Desagregado de Disponibilidad Datacenter Principal 55
Tabla 23 Consolidado disponibilidad de equipos Datacenter alterno 55
Tabla 24 Desagregado Disponibilidad de equipos Datacenter alterno 56
Tabla 25 Consolidado disponibilidad de equipos redes y conectividad 56
Tabla 26 Consolidado disponibilidad de equipos de seguridad 56
Tabla 27 Disponibilidad de equipos Seguridad de la Información 56
Tabla 28 Consolidado disponibilidad de equipos de telefonía 56
Tabla 29 Consolidado disponibilidad de plataforma antivirus 57
Tabla 30 Llamadas Atendida por la Mesa de Servicio 58
Tabla 31 Casos anulados por Servicio 59
Tabla 32 casos suspendidos 61
Tabla 33 Casos Atendidos usuarios VIPs 64
Tabla 34 Casos Atendidos usuarios 65
Tabla 35 Medios de Ingreso de Casos 65
Tabla 36 Visitas a sedes sin Soporte asignado 68
Tabla 37 Medición de ANS Mesa de servicios 69
Tabla 38 Sesiones Servicios Centrales 71
Tabla 39 Capacidades iniciales 94
Tabla 40 Capacidades modificatorio 95
Tabla 41 Total capacidades + servers desaprovisionamiento 95
Tabla 42 Total capacidades consumidas 95
Tabla 43 Total capacidades sin servers de pruebas 95
Tabla 44 Total capacidades ambientes pruebas 96
Tabla 45 Consumos totales 96
Tabla 46 Suma Instancias 130
Tabla 47 Total Docs 130
Tabla 48 Total Radicados 130
Tabla 49 Dimensionamiento Servers IBM - Virtualización Optima 131
Tabla 50 Apps & DDBB Oracle 134
Tabla 51 Escenario de Capacidades Oracle - Estado de consumo Actual 135
Tabla 52 Escenario de Capacidades Oracle - Total de recursos empleados 135
Tabla 53 Tendencia de uso de ancho de banda 160
Tabla 54 usuarios con mayor consumo de ancho de banda 161
Tabla 55 Top de usuarios por sesiones 162
Tabla 56 Top de aplicaciones 162
Tabla 57 Consolidado de indicadores 164
Tabla 58 Tipos de incidentes 171
Tabla 59 Tipo de ataque 174
Tabla 60 Reporte de requerimientos enero 177
Tabla 61 Vulnerabilidades en la infraestructura 177
Tabla 62 Vulnerabilidades en la infraestructura 177
Tabla 63 ataques de phishing 177
Tabla 64 Licenciamiento 179

Tabla 65 Medición ANS Datacenter 180
Tabla 66 Medición ANS Nube Pública 180
Tabla 67 Incidentes de conectividad 182
Tabla 68 Medición de ANS Conectividad WAN e Internet 186
Tabla 69 Desagregado sedes con novedad un solo enlace 187
Tabla 70 Desagregado sedes con novedad con doble enlace 188
Tabla 71 Cantidades de equipos Contractual – Instalados - Almacén 188
Tabla 72 Cantidades de equipos asignados nivel nacional 189
Tabla 73 Cantidades de equipos por devolución nivel nacional 189
Tabla 74 Estado de casos de garantía. 189
Tabla 75 ANS casos de garantía. 190
Tabla 76 ANS Relación casos de garantía 190
Tabla 77 Equipos en siniestro 191
Tabla 78 Solicitudes de Equipos Usuario Final – Según Grupo Responsable 192
Tabla 79 Solicitudes de Equipos Usuario Final – Según Grupo Responsable 192
Tabla 80 Medición ANS Equipos de Usuario Final 192
Tabla 81 Top 5 de categorías en el Servicio de conectividad LAN-WLAN 193
Tabla 82 Distribución y Cantidades de switch 24 puertos 195
Tabla 83 Distribución y Cantidades de Switch 48 puertos 195
Tabla 84 Distribución de puntos de acceso 196
Tabla 85 Medición ANS LAN y WLAN 197
Tabla 86 Equipos gama media 197
Tabla 87 Sedes cerradas 198
Tabla 88 Consolidado de teléfonos gama baja 198
Tabla 89 Consolidado equipos MIFI 198
Tabla 90 Minutos, consumos 200
Tabla 91 Top 5 consumo de llamadas 201
Tabla 92 Top 5 llamadas LDI 201
Tabla 93 Top 5 llamadas Celular 202
Tabla 94 Top 5 llamadas locales 203
Tabla 95 Medición ANS Telefonía IP 204
Tabla 96 Inventario de UPS – 10kVA 205
Tabla 97 Inventario de UPS – 20Kva 206
Tabla 98 Casos gestionados – Energía Eléctrica Regulada UPS 207
Tabla 99 Medición ANS Energía Eléctrica UPS 208
Tabla 100 Inventario de impresoras para el servicio 208
Tabla 101 Consumo de impresiones por usuario - Impresoras B/N 209
Tabla 102 Top 10 de impresoras con mayor uso 210
Tabla 103 Top usuarios impresión a color 210
Tabla 104 Top oficinas 210
Tabla 105 Top 10 impresoras más usadas del servicio de fotocopiado 211
Tabla 106 Ampliación de cuota de impresión 211
Tabla 107 Despacho de papel a sedes del Ministerio del Trabajo 212
Tabla 108 Cargo mensual multifuncional rango medio 212
Tabla 109 Cargo mensual impresora color 212
Tabla 110 Clics de impresión de enero 2026 – Multifuncional B/N 212
Tabla 111 Tendencia de consumo de clics B/N 213
Tabla 112 Clics de Impresión – Impresora Color 213
Tabla 113 Tendencia de consumo de clics color 213
Tabla 114 Medición ANS Outsourcing de Impresión 213
Tabla 115 Top 5 Equipos 218
Tabla 116 Medición de ANS Antivirus 225
Tabla 117 Errores cometidos 226
Tabla 118 Resultado de criterios y parámetros - Calidad de llamadas 227
Tabla 119 KPI Practica de Mejora 228
Tabla 120 Gestión de Riesgos 232

Tabla 121 Bolsa de Recursos 232
Tabla 122 Medición de Acuerdos de Niveles de Servicio enero 2026 233

Índice de Ilustraciones

Ilustración 1 Consolidado encuesta de percepción soporte en sitio 20
Ilustración 2 Estado final de casos al corte del período 21
Ilustración 3 Captura de pantalla mantenimientos en Zabbix 23
Ilustración 4 Socialización matriz de escalamiento 27
Ilustración 5 Efectividad de resolución de incidentes 36
Ilustración 6 Porcentaje de incidentes abiertos 37
Ilustración 7 KPI Efectividad de Resolución de Requerimientos de Servicio 39
Ilustración 8 Requerimientos de Reabiertos en el periodo 40
Ilustración 9 Top de incidentes por sedes 42
Ilustración 10 Top de incidentes por sedes 43
Ilustración 11 Eventos por sedes routers 45
Ilustración 12 Top de causas por sedes switches 45
Ilustración 13 Top de eventos por sedes Access Point 46
Ilustración14Top de causas por sedes Access point 47
Ilustración 15 Top de eventos por sedes Starlink 47
Ilustración 16 Top de causas por sedes Starlink 48
Ilustración 17 Top de incidentes por sedes fortigate 49
Ilustración 18 Top de causas por sedes fortigate 50
Ilustración 19 Top de eventos Windows 51
Ilustración 20 Top de servidores Windows 51
Ilustración 21 Top de causas eventos linux 52
Ilustración 22 Top de servidores linux 53
Ilustración 23 Gráficas CPU Zabbix 53
Ilustración 24 Gráfica memoria servidores 54
Ilustración 25 Seguimiento Práctica Implementación 57
Ilustración 26 Llamadas Atendidas 58
Ilustración 27 Evidencia creación masiva de casos 59
Ilustración 28 Correos generados masivamente 60
Ilustración 29 Depuración de correos enviados masivamente 60
Ilustración 30 Requerimientos Solucionados por Soporte en Sitio 62
Ilustración 31 Requerimientos Solucionados por Territoriales 62
Ilustración 32 Requerimientos Solucionados por la Mesa de Servicios 63
Ilustración 33 Casos Cerrados por Soporte en Sitio 64
Ilustración 34 Casos Cerrados por Territoriales 64
Ilustración 35 Medio de ingreso solicitudes 65
Ilustración 36 Gestión Casos - SC 72
Ilustración 37 Gestión SC - Por Grupo 72
Ilustración 38 Gestión Sc - Por Tipo De Usuario 73
Ilustración 39 Comportamiento SWCORE Datacenter Colombia XV 73
Ilustración 40 Sincronización HA de los Switch Core 74
Ilustración 41 Grafica de consumo canal Internet Datacenter 74
Ilustración 42 máquinas virtuales DRP 75
Ilustración 43 Escenario pruebas Apps DRP 76
Ilustración 44 Extremo DC Bogotá 77
Ilustración 45 Extremo DC Cali 77
Ilustración 46 Estado canal de Internet DC Cali 78
Ilustración 47 Estado SWCORE Datacenter alterno 78
Ilustración 48 Estado HA SWCORE Datacenter alterno 79
Ilustración 49 Consumo canal MPLS DC Alterno 79
Ilustración 50 Estado Router MPLS DC Alterno 80
Ilustración 51 Gestión de Casos Windows 81
Ilustración 52 Cumplimiento WSUS 82

Ilustración 53 Block Legacy Authentication....84
Ilustración 54 Fechas de Soporte....86
Ilustración 55 Licencias asignadas....86
Ilustración 56 Gestión Nube Privada....92
Ilustración 57 App Service1....100
Ilustración 58 App Service2....100
Ilustración 59 - SQL Database BDMT_MS_REPORT....101
Ilustración 60 - SQL Database dev_sqldb_direccion_ivc....101
Ilustración 61 Tabla de recursos....102
Ilustración 62 Mayor consumo de recursos....102
Ilustración 63 Relación de suscripciones....103
Ilustración 64 cuenta perfil catálogo....104
Ilustración 65 Captura configuración del portal....104
Ilustración 66 Validación de buzones....105
Ilustración 67 Nuevo entorno ACEDOC....108
Ilustración 68 Gestión Apps Especializadas....109
Ilustración 69 Grafica umbral servidor....110
Ilustración 70 Gráfica umbral servidor2....111
Ilustración 71 Arquitectura final Apps....114
Ilustración 72 Distribución Sitios IIS....114
Ilustración 73 Gestión Casos IBM....122
Ilustración 74 Diagrama BP....125
Ilustración 75 Diagrama ODM....125
Ilustración 76 Diagrama WASND....126
Ilustración 77 Diagrama FileNet Front....126
Ilustración 78 Diagrama Datacap....127
Ilustración 79 Diagrama App Connect....127
Ilustración 80 Arquitectura Gestor Documental....128
Ilustración 81 Capacidades VM Gestor Documental....128
Ilustración 82 Licenciamiento Oracle....129
Ilustración 83 IBM Licenciamiento....130
Ilustración 84 Gestión DDBB....132
Ilustración 85 Estado Bases de Datos....133
Ilustración 86 Información base de datos – Servidor....136
Ilustración 87 Estadísticas CPU....136
Ilustración 88 Estadísticas Memoria....136
Ilustración 89 Estadísticas Pool compartido....137
Ilustración 90 Tamaño DDBB....137
Ilustración 91 Tamaño Esquema DDBB....137
Ilustración 92 Rendimiento DDBB....138
Ilustración 93 DDBB por Server....138
Ilustración 94 Host e Instancia CPU....138
Ilustración 95 Estadísticas Memoria....139
Ilustración 96 Estadística Shared Pool....139
Ilustración 97 Tamaño DDBB DBMINTRA....139
Ilustración 98 Tamaño Esquema DDBB....139
Ilustración 99 Rendimiento DDBB MINTRASG....140
Ilustración 100 Información DDBB PLIFERAY....140
Ilustración 101 Host e Instancia CPU....140
Ilustración 102 Estadísticas Memoria....141
Ilustración 103 Estadísticas Shared Pool....141
Ilustración 104 Tamaño DDBB PLifeRay....141
Ilustración 105 Tamaño Esquemas DDBB....141
Ilustración 106 Rendimiento DDBB PlifeRay....142
Ilustración 107 Información DDBB SIGEP....142
Ilustración 108 Firewall de nueva generación.....159

Ilustración 109 Comportamiento ancho de banda....160
Ilustración 110 Tendencia de uso de ancho de banda....161
Ilustración 111 Top de usuarios por números de sesiones....161
Ilustración 112 Top de aplicaciones....162
Ilustración 113 Top de Autenticación....163
Ilustración 114 sesiones fallidas....164
Ilustración 115 Reporte mensual enero....165
Ilustración 116 Captura de pantalla perfomance....166
Ilustración 117 licencia sandbox....167
Ilustración 118 licencia sandbox....168
Ilustración 119 Detalle de latencia o errores....168
Ilustración 120 detalle de problemas en servicios....169
Ilustración 121 Detalle casos de uso....169
Ilustración 122 Detalle de alertas....170
Ilustración 123 Detalle de alertas....170
Ilustración 124 Detalle de incidentes....171
Ilustración 125 Detalle servidores....172
Ilustración 126 Detalle fortigate....173
Ilustración 127 Top attack types....174
Ilustración 128 Top de ataques....175
Ilustración 129 Consumo canal MPLS DC Principal....181
Ilustración 130 Estado Router MPLS DC Principal....181
Ilustración 131 Topología actualizada....183
Ilustración 132 Interface Fortimanager....184
Ilustración 133 Interface MPLS HUB SDWAN....184
Ilustración 134 Interface Internet HUB SDWAN....185
Ilustración 135 VPN SDWAN establecidas....185
Ilustración 136 Estado HUB SDWAN Datacenter....185
Ilustración 137 Estado HA HUB Sdwan....186
Ilustración 138 Recursos Fortimanager....186
Ilustración 139 Estado de casos Redes y Conectividad....194
Ilustración 140 Asignación de licencias....199
Ilustración 141 Comportamiento de tráfico....200
Ilustración 142 Top llamadas nacionales....200
Ilustración 143 llamada internacional de prueba....201
Ilustración 144 Top Celular....202
Ilustración 145 Top Local....202
Ilustración 146 Requerimientos por garantía....203
Ilustración 147 Disponibilidad y Continuidad TOIP....204
Ilustración 148 Equipos consola antivirus....214
Ilustración 149 Gestión consola antivirus – equipos usuario final....215
Ilustración 150 Top 10 virus detectado....216
Ilustración 151 Descripción de virus....216
Ilustración 152 DFGARCIA....218
Ilustración 153 URPEASPRILLA....219
Ilustración 154 ANDJYPEREZ....219
Ilustración 155 BOPCBUSTAMANTE....219
Ilustración 156 Eventos Ransomware....220
Ilustración 157 captura eventos ransonware....220
Ilustración 2158. Licenciamiento....221
Ilustración 159 *Gestión consola Nessus*....222
Ilustración 160 *Escaneos programados*....222
Ilustración 161 TOP 10 - Activos más explotables....223
Ilustración 162 Vulnerabilidades gestionadas vs en remediación....224
Ilustración 163 captura envío de correo gestión de vulnerabilidades....225
Ilustración 164 Resultados auditoria de casos....227

Ilustración 165 Seguimiento Práctica Mejora 228
Ilustración 166 Resultado de Cumplimiento AM 229

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 enero 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 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 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 Preventivo de UPS en Tunja, Ibagué, Pereira, Bucaramanga, Medellín. Revisión de tarjetas de red de UPS en Nivel Central. Servidores de bases de datos (Sistema de Procedimiento Sancionatorio IVC SISINFO, entre otros), Bases de datos del Gestor Documental, Conectividad de red, Portal WEB.
- 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 CONTR

- Aspectos importantes para el **buen uso de One Drive como repositorio de la información institucional** a cargo de cada usuario, la importancia de verificar la sincronización de la información, trabajar los archivos con la opción de autoguardado habilitado y recordar que es de uso institucional y no para guardar datos personales.




¡INFORMACIÓN IMPORTANTE USO DI ¡INFORMACIÓN IMPORTANTE LINEAM

- 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

- Se continúa replicando mensaje de la Oficina TICs en Soporte MT relacionado con el **lineamiento de bloqueo de puertos USB en los equipos institucionales** con el fin de mitigar los riesgos de fuga de información y accesos no autorizados.



¡INFORMACIÓN IMPORTANTE PORTA

b. Traslados y novedades de sedes:

– **Anserma / Caldas:** Por remodelación física de la alcaldía del municipio, la sede fue trasladada temporalmente el 8/03/2025 a un local cercano mientras terminan las adecuaciones. El 29/01/2026 la UT asiste a la sede para reacomodación de los equipos a su cargo encontrando que
  - La sede no cuenta con puntos de red ni puntos de energía cercanos a los puestos de trabajo. Los puntos de energía se solventaron con extensiones.
  - Se realiza ubicación del equipo de cómputo, impresora y equipos de comunicaciones, todos muy cerca del Fortinet para poder hacer conexión con patchcord.
  - **La oficina asignada a la inspección no es la misma que se tenía en el 2025**, por lo que en los arreglos hicieron corte de la fibra. Debemos gestionar con el proveedor de conectividad la manera de solventar la situación, ya se realizó el escalamiento con ETB (26431610) para ver el modo de proceder luego de una

visita en la sede. Informaremos las novedades del caso según lo que informe el proveedor.

- Se hizo validación de los elementos pero **no se encuentra el adaptador del Fortinet**. Nos podrías apoyar por favor para que el personal de la sede pueda realizar una búsqueda exhaustiva dentro de los elementos de oficina que están organizando.



Reapertura IT
Anserma _ Caldas.msg

- **Segovia / Antioquia:** Informan que 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

- **DT Vaupés / Mitú:** El 13/11/2025 sin previa notificación, se realiza el acompañamiento por parte de la UT Gestión TIC 2023 para el traslado de sede de la DT Vaupés a una nueva ubicación. La sede no cuenta con cableado estructurado, por lo que los dos equipos que quedaron conectados están físicamente cerca al Fortinet y conectados mediante patchcord. El 3/12/2025 la UT entrega cotización de la adecuación de puntos requeridos para la sede, no se tienen novedades o respuesta por parte de la entidad. El director encargado reporta al SS que se debe solventar la situación.

- Se dejan varias sedes en mantenimiento prolongado en la herramienta de monitoreo Zabbix durante el período por ausencia de usuarios por vacaciones: San Marcos, Puerto Asís, Pasto, Manzanares.
- **Cumaral / Meta**: Se deja en mantenimiento en Zabbix la sede ya que el funcionario asignado estará de vacaciones desde el 29/01/2026 y hasta el 9/02/2026.
- Durante diciembre 2025 la entidad solicitó coordinar lo correspondiente para el traslado de las sedes IT Cisneros, IT Tumaco, IT Riosucio / Choco, OE Buenaventura, DT Cesar para mediados de enero 2026. Se realiza la gestión pertinente por parte de la UT.
  - **Rio Sucio / Choco** se trasladó el 16/01/2026 sin contratiempos, sede queda completamente funcional con Starlink instalada y conectada al FW para conectividad LAN.



Informe traslado de
equipos – Sede Riosu

  - **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; además, se requiere un cable más extenso para la instalación de la antena Starlink ya que se debe ubicar en la terraza del predio. El cable de la antena es comprado en Bogotá y remitido a la inspección.



RE_ Solicitud de traslado de soporte te

- **Cisneros / Antioquia** se trasladó el 19/01/2026 presentándose como novedad que el modem para la conexión temporal de internet que se tenía en la sede no fue encontrado, fue necesario esperar que la auxiliar administrativa de la inspección regresara de sus vacaciones para que fuera encontrado.
- **OE Buenaventura** se trasladó el 23/01/2026 y durante esa semana. La UT apoyo el ponchado de cables en el centro de cableado ya que el tercero no dejo listos ni marcados los puntos, además se apoyó la instalación del punto y el Access Ppint. La sede tiene unas solicitudes de elementos adicionales que se notificaron al Coordinador del Grupo de Soporte Informático para revisión y respuesta por parte de la entidad.





RE_ Traslado de OE Buenaventura.msg RE_ Traslado de OE Buenaventura.msg RE_ Traslado de OE Buenaventura.msg

- **DT Cesar:** Aun se encuentran en proceso de ubicar un inmueble y concretar los procesos administrativos, continúan en la sede habitual.

c. **Plan de trabajo documentos SIG para publicación en la SVE:** Durante el período, Cesar Augusto Valencia de la Oficina Asesora de Planeación (OAP) vía correo electrónico da el visto bueno para que los documentos entregados para revisión el mes anterior, continúen flujo en la SVE:

- Procedimiento Práctica Habilitación de cambios en los Servicios de Tecnologías de Información.
- Formato Solicitud de Cambio en los Servicios de Tecnologías de Información – RFC
- Procedimiento Práctica Problemas en los Servicios de Tecnologías de Información.
- Procedimiento Práctica Acuerdos de Nivel de Servicio en los Servicios de Tecnologías de Información.
- Procedimiento Práctica Implementación en los Servicios de Tecnologías de Información.
- Procedimiento Práctica Requerimientos en los Servicios de Tecnologías de Información.
- Procedimiento Práctica Disponibilidad en los Servicios de Tecnologías de Información.




RE_ Plan de trabajo documentos SIG Acue RE_ Plan de trabajo documentos SIG Acue

El 13/01 se remite correo electrónico a Cindy Feria del Grupo de Soporte Informático relacionando las capturas de pantalla de los documentos que ya fueron registrados

en la SVE para publicación, ella a su vez remite correo a Cesar Valencia de la OAP ya que para la aprobación del Coordinador del Grupo no se visualizan los documentos en su perfil de la SVE. El 30/01/2026 se envía correo a Cesar Valencia con los documentos editables y pidiendo la retroalimentación respctiva.


RV_ Registro de documentos SVE.msg


RE_ Plan de trabajo documentos SIG Acue

d. Disposición de RAEES y Residuos Electrónicos: Durante el periodo no se gestionaron permisos para la salida de elementos o residuos tecnológicos por parte del proveedor SUMA Desarrollo Ambiental para disposición final.

El 23/01/2026: Se da respuesta vía correo electrónico a Maria Camila Acosta del Grupo de Recursos Físicos, Gestión y Administración de Bienes del Ministerio del Trabajo con información de Diciembre 2025 del manejo ambiental: Despacho de resmas a nivel nacional, control de recargas de resmas en territorio y Nivel Central y clics de impresión por sede.


RE_ SOLICITUD DE APOYO REPORTE DE I

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:

- Se realiza ajuste del plan de trabajo de implementación de IPV6 en Dual Stack, se mapean en el documento las rutas del SharePoint de la entidad donde se están consolidando los soportes y evidencias.
- Se ajusta plan de direccionamiento y se inicia fase de entrega de segmentos a los administradores de servicios.
- Se registró el caso CS0566094 con Cirion, se aplicó la configuración IPv6 en los equipos CPE del DC CXV, quedando de la siguiente manera:
  Subred CX Cirion: 2801:15:400::/64
  CPE Principal: 2801:15:400::2
  CPE Backup: 2801:15:400::3
- Se está gestionando ventana de mantenimiento en conjunto con el proveedor bajo el caso CS0586631para realizar ajustes en los equipos de backbone para asociar el direccionamiento mencionado al **AS BGP 274265** entre Backbone Cirion y CPE Principal / Backup.
- Para el servicio de telefonía, se asignó el prefijo y se configuró la VLAN de voz en IPV6 para Nivel Central, el especialista del servicio está realizando pruebas, replicación de la VLAN en el teléfono, se encuentra en curso. Adicional los SBC que está en Azure ya está dual stack.
- Para el servicio de impresión, la VLAN 18 es la asignada, se está verificando el paso en todas las impresoras (tarea manual), se tiene equipo de prueba y se está validando lo requerido a nivel del server.

- Para los equipos de cómputo de usuario final, se hizo una prueba base de asignación de DHCP en IPV6 que resultó satisfactoria en Piso 22 Nivel Central.
- Para la infraestructura centralizada, se entrega al responsable el Gateway, DNS y segmentos asignados para la configuración de Servidores- iSCSI, en proceso de verificación para distribución del direccionamiento.



IPV6_Dual_Stack -
Min Trabajo .msg

f. Divulgaciones con el equipo de trabajo

- Se genera y envía a los equipos de MDS y SS un **Manual de validación y actualización de BIOS** para estandarización con el equipo de trabajo, y que los lineamientos sean aplicados correctamente durante los procesos de revisión en cada una de las sedes del cliente.



Manual de validación
y actualización de BIO

- El 7/01/2026: Se realizó sesión presencial con el equipo de soportes de Bogotá para reiterar el flujo de actividades y responsables de la Gestión de Devolución de Equipos y reiterar apoyo en actividades masivas de actualización de agentes, BIOS y SO. El 9 de enero se realiza la misma sesión al personal de soporte técnico de territorio vía Microsoft Teams.



Socialización de
Devolución de Equipo

- El 14/01/2026 la gestora de la práctica de requerimientos notifica al SOC y al equipo una modificación del flujograma del proceso **Habilitación de puertos USB**, el cual se podrá realizar en los siguientes escenarios a partir del 15/01/2025:
  Aplicar Excepción de Habilitación de puertos: Debe ser enviada por el jefe de dependencia y contener la justificación de la excepción de habilitación de puertos así como los usuarios a los cuales se aplicará la excepción.
  Backup equipo de cómputo: El caso debe ser creado únicamente por parte del Soporte en Sitio para el proceso de devolución de equipos, lo relacionado con el Backup físico y que no cuente habilitado los puertos USB, se solicitará la autorización de la habilitación temporal por (5 días hábiles).



Modificación del
Flujo habilitación de p

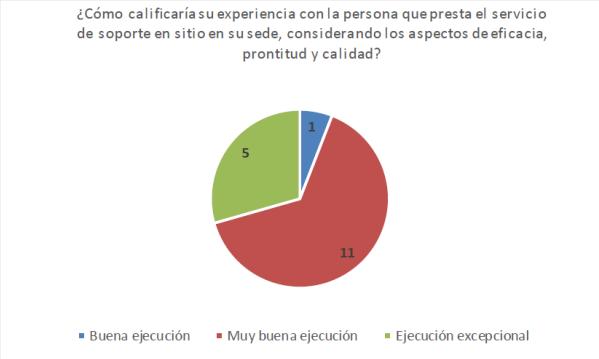
g. Otras actividades

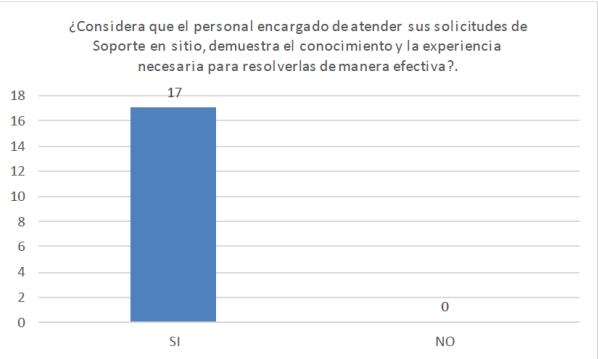
- Referente a la **Encuesta de percepción del personal de Soporte en Sitio Territorial** el 16/01/2026 se envía correo electrónico al Coordinador del Grupo de Soporte Informático el informe de resultados luego del diligenciamiento de diez y siete (17) Directores Territoriales: Cauca, Buenaventura, Nariño, Casanare,

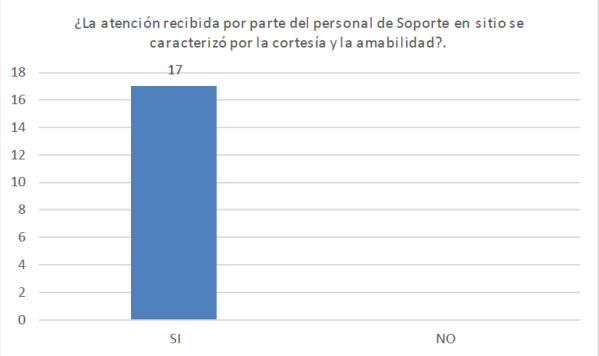
Amazonas, Cesar, Magdalena, Guainía, Caquetá, Vichada, Caldas, Barrancabermeja, Boyacá , Valle Del Cauca, Choco, Santander y Guajira.

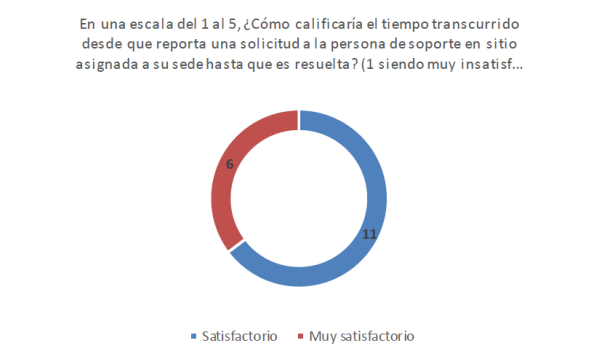
A continuación, se comparte los resultados más representativos y el correo remitido con el documento adjunto:

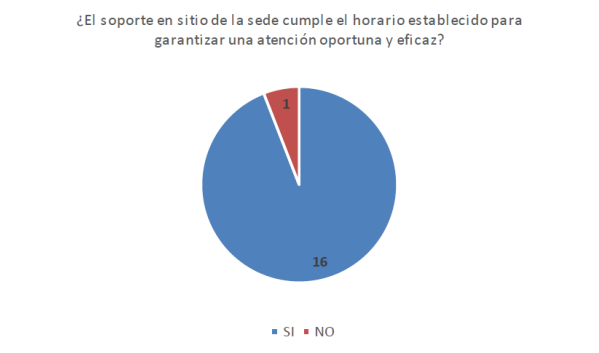
RE_ Encuesta de percepción de soporte

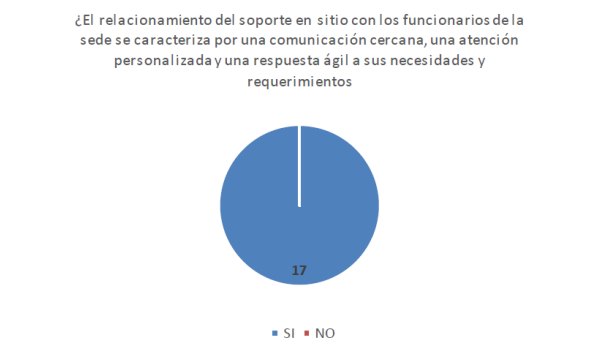












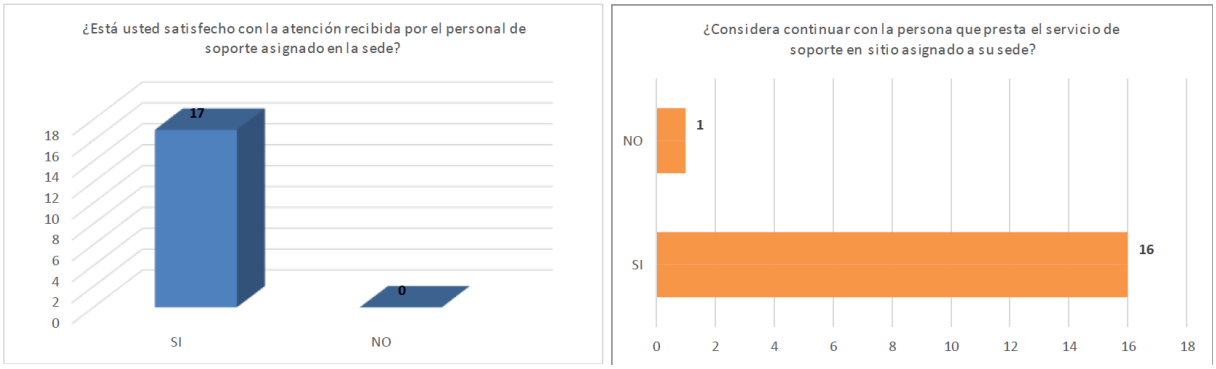


Ilustración 1 Consolidado encuesta de percepción soporte en sitio

Para el personal de soporte en sitio de DT Magdalena, se realizó sesión de retroalimentación de los resultados identificando las oportunidades de mejora y los apoyos que se brindan desde la línea de servicios en sede para continuar con seguimiento para fortalecer los conocimientos en la gestión del servicio al cliente y la adopción de los lineamientos para la prestación de los servicios.

También se realiza sesión con todo el personal de soporte para presentar los resultados obtenidos:

ResultadosencuestaS S2025.pptx

- 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. A espera de recibir retroalimentación de esta oficina, y a que se divulguen los documentos finales con el usuario final.

h. Volumetría de Solicitudes Gestionadas:

En el mes de enero 2026 se registraron en la herramienta ITSM 6106 solicitudes asociadas a la prestación de los servicios de TI por parte de la UT, en el apartado 2.1.2.8. Práctica de Eventos de este mismo documento se muestra la volumetría asociada a la gestión de eventos resultantes del monitoreo 7x24 de la infraestructura a cargo de la UT.

- Tipificación según la volumetría de casos:
  - Requerimientos de Servicio: 5329
  - Incidentes: 754
  - Cambios: 23

- 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 enero 2026:

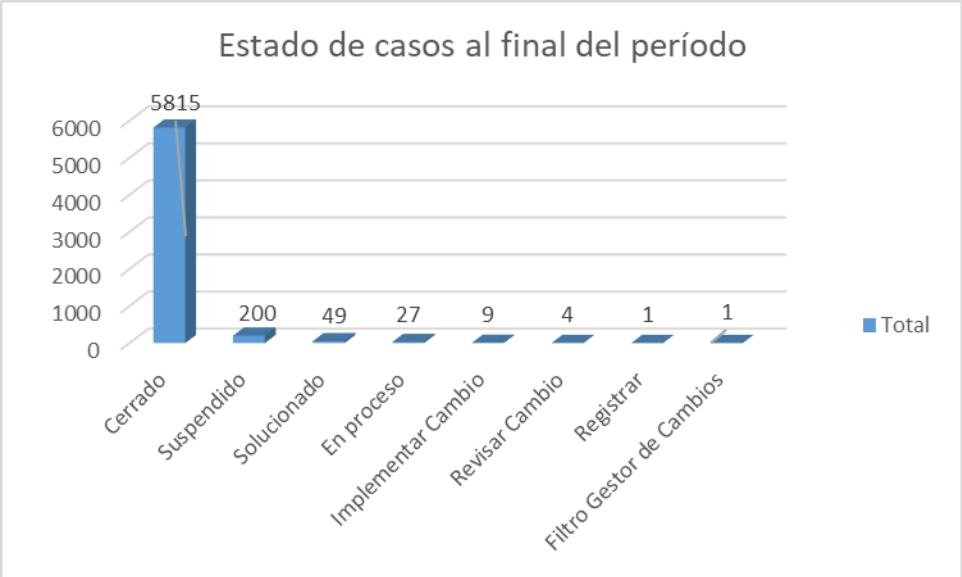


Ilustración 2 Estado final de casos al corte del período

- Gestión por parte de los grupos de especialistas:

Grupo Responsable	Cantidad de casos gestionados	Porcentaje (%)
Responsable_Soporte_Territoriales	1564	25,61
Responsable_Mesa_De_Servicio	1320	21,62
Responsable_Soporte_Bogota	1315	21,54
NOC	520	8,52
Responsable_Soporte_Impresoras	485	7,94
Especialistas_IBM	337	5,52
Responsable_De_Servidores_Windows	142	2,33
Especialista_Telefonía_IP	98	1,60
SOC	97	1,59
Gestor de Inventarios	55	0,90
Especialista Herramientas de Gestion	39	0,64
Especialista Nube Privada	38	0,62
Responsable Garantías Equipos	24	0,39
Especialista Redes	21	0,34
Especialista Base de datos	14	0,23
Gestión del Servicio	10	0,16
Responsable_de_Energia Electrica Regulada - UPS	7	0,11
Especialista Nube Publica	6	0,10
Especialista Aplicaciones .Net	4	0,07
Especialista Aplicaciones JAVA	4	0,07
Liferay	2	0,03

Responsable Antena Starlink	2	0,03
Almacenamiento y Backups	2	0,03
TOTAL	**6106**	**100,00**

Tabla 1 Atención de solicitudes por Grupo de Especialista

2.1.1. Herramienta de Gestión ITSM

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

- Afinamiento de métricas para toma del estado del puerto 3389 en los servidores del gestor documental.
- Se realizaron mejoras sobre el Visor ZMTM creado para la gestión centralizada y ágil de los mantenimientos solicitados en zabbix, dentro de las mejoras se incluyó:
    - La autenticación con usuario y clave de zabbix (este se puede unir al directorio activo).
    - Se agrego seguridad a la extensión de mantenimiento solo para aquellas personas que hagan parte de un grupo especifico en zabbix.
    - Se agrego la visual de cantidad de host y/o grupos afectados para dar mejor visibilidad del impacto del mantenimiento.
    - Se agregaron filtros de búsqueda, ahora se puede buscar por nombre, por orden alfabético y por estado (activo, próximo a vencer en 24 horas, programados y todos).
    - Se pueden organizar por menor tiempo restante, fin cercano y alfabéticamente A - Z.
    - Se agregó funcionalidad de exportar a csv
    - Los mantenimientos con menos de 1 día para vencerse se podrán extender agregando días, horas, minutos y un motivo de manera obligatoria.
    - Se agrego caracterización por colores donde se indica la criticidad cuando el mantenimiento está próximo a vencerse, no tiene descripción o fue extendido.
    - Se muestra los motivos cuando un mantenimiento fue extendido.

- Se corrigieron errores de posicionamiento de cursor cuando se está extendiendo un mantenimiento.

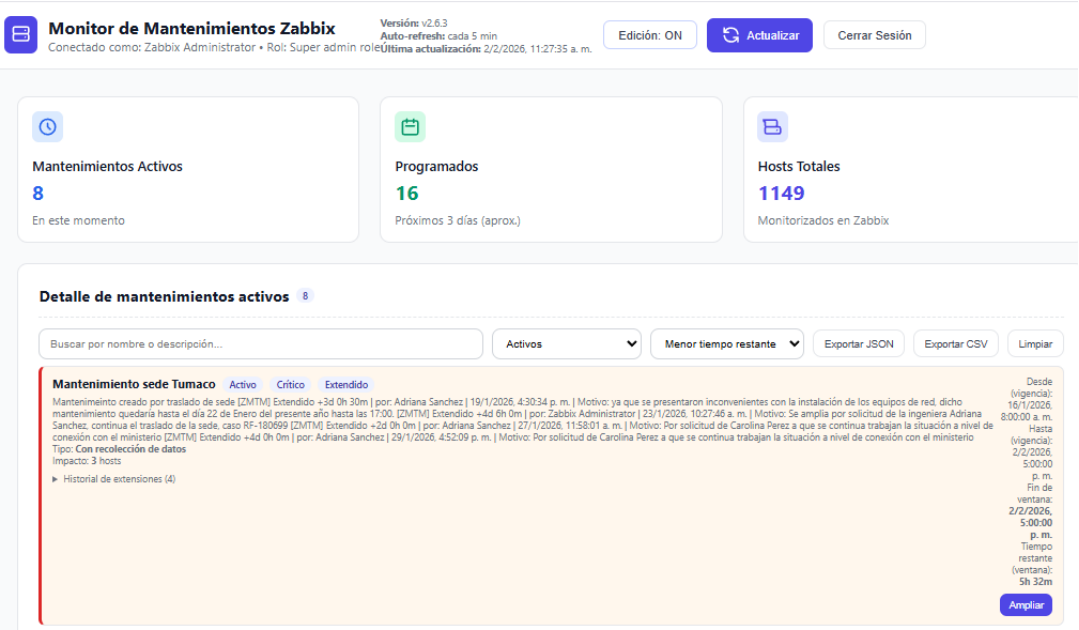


Ilustración 3 Captura de pantalla mantenimientos en Zabbix

- El 28/01/2026 se realiza la actualización de ADM a la versión 9.41.2.3 bajo el cambio RFC-181585.
- Se realizo afinamiento en las reglas que obligan a la asignación de notas cuando un caso pasa a estado suspendido.
- Se realizo la creación de 2 nuevas categorías en la CMDB asociados a la antena Starlink y varios para la clasificación de los CI´s.
- Se creo el Grupo Indra para indicar que son los responsables de los CI´s

2.1.2. Prácticas ITIL 4

2.1.2.1. Práctica Acuerdos Niveles de Servicio (ANS)

Durante el periodo comprendido entre el 1 y el 31 de enero de 2026, se llevó a cabo el seguimiento, control y medición de los Acuerdos de Niveles de Servicio (ANS) parametrizados en la herramienta de gestión, en articulación con los líderes de cada servicio. Esta actividad se desarrolló con el propósito de validar el nivel de cumplimiento de los compromisos contractuales establecidos, conforme a lo definido en el Numeral 7. Medición de Acuerdos de Nivel de Servicio.

- **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 dent ro 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 ANS se mantuvieron dentro de los niveles de cumplimiento esperados, contribuyendo a la continuidad y estabilidad de la operación de los servicios tecnológicos. No obstante, se identificaron desviaciones puntuales en los indicadores asociados a la continuidad y disponibilidad del servicio de red WAN.

El detalle de los resultados obtenidos para los indicadores de continuidad y disponibilidad se encuentra desagregado en el archivo “ANS Internet – MPLS”, el cual soporta la información analizada. Las desviaciones detectadas corresponden específicamente 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.

En conclusión, el desempeño general de los ANS durante el mes de enero de 2026 fue satisfactorio, manteniéndose la estabilidad de los servicios y reafirmando la efectividad de los mecanismos de control, seguimiento y mejora continua, sin impacto significativo en la operación del negocio.

2.1.2.2. Práctica Habilitación de Cambios

Dar a conocer las actividades de la Práctica Habilitación de Cambios correspondientes al periodo del 1 al 31 de enero de 2026. Este apartado contiene información relevante sobre actividades realizadas y novedades presentadas.

- **Tipificación de los cambios**

Durante el mes de enero de 2026 se gestionaron 23 casos tipificados como Cambios, clasificados en las siguientes categorías:

Servicio	No	Porcentaje
Herramientas de Gestión	1	4,35%
Administración de Bases de Datos	6	26,09%
Administración de servidores	8	34,78%

Servicio	No	Porcentaje
Energía Eléctrica Regulada - UPS	8	34,78%
Total	**23**	**100,00%**

Tabla 3 Tipificación de los cambios

- **Relación casos registrados**

A continuación, se presenta la relación de casos registrados del 1 al 31 de enero de 2026, en total se crearon 23 casos de los cuales se gestionaron 11 como cambios estándar, 5 cambios como de emergencia y 6 cambios como estándar

Sesion_HC_Enero2026.xlsx

- **Cambios por estado**

Al corte del 31 de enero 2026, 9 casos quedaron estado Cerrado, 9 casos quedaron estado Implementar Cambio y 5 quedaron en estado revisar cambio.

- **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: 21/23*100 PCE: 91,30 %

Tabla 4 Medición Indicador Porcentaje de Cambios Exitosos

Durante el periodo comprendido entre el 1 y el 31 de enero de 2026, se gestionaron 23 cambios implementados, de los cuales 21 fueron clasificados como exitosos, alcanzando un resultado del 91,30 %, valor que supera la meta establecida del 80 %.

Los dos cambios no exitosos corresponden a los **RFC-180220 y RFC-178197**, asociados a la actividad **"Revisión UPS Sede Central – Continuación Revisión".** En estos casos, no fue posible restaurar la comunicación por red de las UPS, debido a que las actividades planificadas no arrojaron los resultados esperados. De acuerdo con el proveedor, se identificó la necesidad de solicitar a fábrica una tarjeta de red nueva y certificada, con el fin de garantizar su correcta instalación y funcionamiento. En consecuencia, se gestionará un nuevo RFC para la ejecución de una nueva ventana de mantenimiento que permita completar la actividad de forma satisfactoria.

Es importante resaltar que estos cambios no exitosos no generaron afectaciones críticas al servicio, se encontraban debidamente controlados, contaban con planes de mitigación definidos y fueron gestionados conforme al procedimiento establecido, asegurando la trazabilidad y el análisis de causa correspondiente.

2.1.2.3. Práctica Gestión de Activos

Durante el mes de enero 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:

- **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.

- **Socialización del flujo de devolución de equipos – Soporte en sitio**

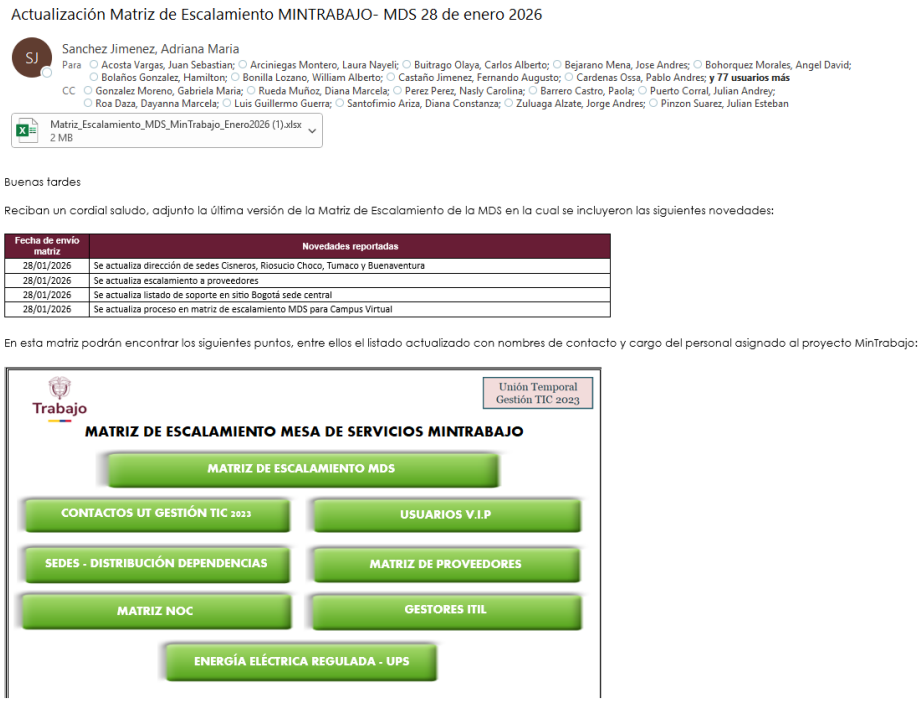
Entre el 07 y el 09 de enero, se realizó la socialización del flujo de devolución de equipos al equipo de soporte en sitio, con el objetivo de estandarizar el proceso, clarificar roles y responsabilidades, y reforzar los criterios para la correcta devolución, recepción y registro de los activos tecnológicos. Esta actividad contribuyó a reducir reprocesos, fortalecer la trazabilidad de los equipos, mejorar el control del inventario y asegurar el cumplimiento de los procedimientos definidos por la Entidad.

2.1.2.4. Práctica Catálogo de servicios

Dentro de la práctica de catálogo de servicios, se busca tener una fuente única de la lista de servicios disponibles para Ministerio del Trabajo. A continuación, se indican las acciones adelantadas:

- **Actualización y Socialización de matriz de Escalamiento**

El pasado 6 y 28 de enero de 2026, se realizó la actualización y socialización de la matriz de escalamiento vía correo electrónico a todo el equipo de la UT, en esta se tuvo en cuenta la actualización de los técnicos de soporte en sitio Bogotá, actualización de las direcciones de sedes a nivel nacional, se actualizó la matriz de proveedores y la matriz de escalamiento en la MDS para la gestión del campus virtual.



Actualización Matriz de Escalamiento MINTRABAJO- MDS 28 de enero 2026

Sanchez Jimenez, Adriana Maria

Para Acosta Vargas, Juan Sebastian; Arciniegas Montero, Laura Nayeli; Buitrago Olaya, Carlos Alberto; Bejarano Mena, Jose Andres; Bohorquez Morales, Angel David; Bolaños Gonzalez, Hamilton; Bonilla Lozano, William Alberto; Castaño Jimenez, Fernando Augusto; Cardenas Ossa, Pablo Andres; **y 77 usuarios más**

CC Gonzalez Moreno, Gabriela Maria; Rueda Muñoz, Diana Marcela; Perez Perez, Nasly Carolina; Barrero Castro, Paola; Puerto Corral, Julian Andrey; Roa Daza, Dayanna Marcela; Luis Guillermo Guerra; Santofimio Ariza, Diana Constanza; Zuluaga Alzate, Jorge Andres; Pinzon Suarez, Julian Esteban

Matriz_Escalamiento_MDS_MinTrabajo_Enero2026 (1).xlsx
2 MB

Buenas tardes

Reciban un cordial saludo, adjunto la última versión de la Matriz de Escalamiento de la MDS en la cual se incluyeron las siguientes novedades:

Fecha de envío matriz	Novedades reportadas
28/01/2026	Se actualiza dirección de sedes Cisneros, Riosucio Choco, Tumaco y Buenaventura
28/01/2026	Se actualiza escalamiento a proveedores
28/01/2026	Se actualiza listado de soporte en sitio Bogotá sede central
28/01/2026	Se actualiza proceso en matriz de escalamiento MDS para Campus Virtual

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

Ilustración 4 Socialización matriz de escalamiento

- **Creación Categoría**

Se crea la siguiente categoría, con el fin de gestionar y registrar adecuadamente los casos cuando se presente la inhabilitación de un usuario por renuncia o despido, de acuerdo con los lineamientos establecidos para la devolución de equipos.

- Servicio: Soporte Microinformática
- Categoría: ***Radicar una solicitud. Impresora. Deshabilitación de usuario***



- En las auditorias de calidad, se realizó seguimiento a la correcta categorización de casos y así mismo se realiza feedback de acuerdo con novedades encontradas
- De acuerdo con ausencias de especialistas o soportes en sitio, se solicita la inhabilitación de usuario en aranda para evitar la asignación de tickets y vencimientos de los mismos.

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 enero
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= (1/1)*100 EF= 100%

Tabla 5 KPI Práctica Catálogo de Servicios

2.1.2.5. Práctica de Problemas

Dar a conocer las actividades de la Práctica de Problemas correspondientes al periodo de enero 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
Total	13	

Tabla 6 Consolidado problemas identificados

Durante el mes de enero se realizó seguimiento al caso 174025 asociado con el Gestor Documental.

De acuerdo con la sesión de trabajo realizada el 19 de enero se definieron las acciones que se va a adelantar:

1. Documentar logs en el caso actual de IBM (19 de enero) – Especialistas IBM
2. Revisión de información adicional con IBM que pueda aclarar aspectos relacionados con el problema (19- 23 enero) Especialistas IBM.
3. Coordinar sesión con Alex para revisión de consultas altas en BBDD (19 – 23 enero) Especialistas IBM, Especialista DBA Oracle
4. Coordinar sesión equipo Windows búsqueda de políticas GPO (19 – 23 enero) Especialistas Windows- Especialistas Nube Privada.
5. Presentación esta semana de RFC para ventana de mantenimiento Filenet (ejecutar 30-31 de enero)- Especialistas IBM
6. Revisión de posible aplicación de herramienta para captura de logs (observabilidad) y herramienta DELL (19-23 enero) Líder Servicios Centrales.

2.1.2.6. Práctica de Incidentes

Este apartado presenta un resumen de las actividades realizadas en el marco de la Práctica de Incidentes durante el periodo de enero 2026. Se incluye información relevante sobre los incidentes registrados, las acciones ejecutadas y las novedades ocurridas.

Durante el período del informe, se registraron 754 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:

Estado	Cantidad
Cerrado	719
En proceso	1
Solucionado	18
Suspendido	16
Total general	754

Tabla 7 Estados Incidentes

De acuerdo con los incidentes generados en el mes de medición, a continuación, se comparte el detalle del TOP 10

Tipo de incidente	Total	Observación

Reportar una falla.Alarma Zabbix.Router	271	Incidentes generados en el servicio de redes y conectividad por afectaciones en infraestructura del proveedor. Adicional, novedades por equipos apagados por parte de los usuarios
Reportar una falla.Alarma Zabbix.FortiGate	96	Casos generados por alarmas en Zabbix debido a intermitencias a nivel de red, dispositivos apagados en sede cuando no se encuentran los funcionarios en la misma y fallas a nivel eléctrico
Reportar una falla.Alarma Zabbix.Starlink	83	Intermitencias presentadas por: condiciones climáticas adversas (tormentas, nubes densas), obstrucciones físicas (techos, árboles), fluctuaciones eléctricas y ajustes en la cobertura satelital en regiones específicas.
Reportar una falla.Falla impresora.No imprime	34	Novedades presentadas por desconfiguración de impresora, bloqueo de impresora, errores en archivo origen, impresora sin conexión a la red, tamaño de papel erróneo al momento de imprimir. Etc
Reportar una falla.Alarma Zabbix.Switch	34	Novedades presentadas por cortes de energía, equipos apagados y novedades con la red del proveedor. En este caso, es posible que Zabbix verifique primero los hosts dependientes y después los host padres, si esto se presenta lo más posible es que Zabbix cree los casos correspondientes a cada uno de los hosts alertados, es decir, que en esta situación las dependencias no actuarían.
Reportar una falla.Gestor Documental.Falla Funcional	33	El 94% de los casos corresponde a errores en la aplicación del gestor documental. Se destacan reprocesos, relanzamientos y sobrecarga del sistema debido al desconocimiento de los flujos por parte de los usuarios.
Reportar una falla.Alarma Zabbix.AP	26	Novedades presentadas por cortes de energía, equipos apagados y novedades con la red del proveedor. En este caso, es posible que Zabbix verifique primero los hosts dependientes y después los host padres, si esto se presenta lo más posible es que Zabbix cree los casos correspondientes a cada uno de los hosts alertados, es decir, que en esta situación las dependencias no actuarían.
Reportar una falla.Gestor Documental.Falla radicacion	21	Novedades presentadas debido a errores generados en el radicado, extensiones de archivo erróneas, lentitud presentada con el gestor documental
Reportar una falla.Falla impresora.Atasco	19	Casos generados por atasco de papel en impresoras
Reportar una falla.Alarma Zabbix.Servidor Windows	11	Se identificó que la redirección desde la aplicación SFT hacia la aplicación del Sistema Nacional de Cualificaciones estaba fallando debido a la indisponibilidad temporal de esta última, alertamientos por actividad programada en RFC-179327

Tabla 8 Top 10 Incidentes

- **Casos Suspendidos**

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

Grupo Resolutor	noviembre	diciembre	enero

Especialista Redes			2
NOC			12
Responsable_de_Energia Electrica Regulada - UPS	6	1	
Especialistas_IBM			1
Soporte Microinformática			1
Responsable_Soporte_Impresoras			1
Total	6	1	17

Tabla 9 Incidentes Suspendidos

El backlog de enero se concentra principalmente en:

NOC, con 12 casos, siendo el grupo con mayor impacto y el principal generador del backlog actual debido a casos escalados al proveedor de telecomunicaciones de los cuales varios están pendientes de cierre a espera del RFO. Especialista Redes, con 2 casos, que, aunque menor, muestra aparición de backlog frente a meses anteriores.
Otros grupos (Especialistas IBM, Soporte Microinformática y Responsable Soporte Impresoras) presentan 1 caso cada uno.
El grupo Responsable de Energía Eléctrica Regulada – UPS, que concentraba el backlog en meses anteriores, no presenta casos suspendidos en enero.

- **Incidentes Mayores**

Del total de incidentes reportados, los siguientes casos fueron registrados como incidentes mayores afectando los servicios Office 365 (1), redes y conectividad (4) los cuales se detallan a continuación:

Incidente Aranda	Estado Ticket Aranda	Novedad	Causa Raíz	Acciones Realizadas para restablecer el servicio	Usuarios Afectados	Fecha/Hora inicio	Fecha/Hora Fin	Tiempo de Indisponibilidad
IM-180563	Cerrado	Incidente Mayor Novedad en Office 365	Una parte de la infraestructura de servicios dependientes en la región de Norteamérica no está procesando el tráfico como se esperaba.	Se realiza validación con Microsoft e indican que la novedad es global la cual se está gestionando con MO1221364, mencionan como avance que se tiene una degradación en la infraestructura de servicios dependientes de Microsoft 365, que afecta el flujo de transporte de correo de Exchange Online y el acceso a portales asociados (Microsoft Defender XDR y Microsoft Purview). 22 de enero de 2026, 4:32 p. m. GMT-5 Hemos implementado una solución de balanceo de tráfico en una porción limitada de la infraestructura y la telemetría muestra resultados exitosos. Estamos aplicando esta solución de forma gradual en toda la infraestructura afectada para garantizar que el entorno permanezca equilibrado mientras continúa la recuperación. Estamos optimizando activamente las configuraciones de balanceo de carga para abordar desequilibrios residuales	General	22/01/2026 2:30	23/01/2026 7:30	17 H

				y reforzar los esfuerzos de recuperación, al tiempo que tomamos precauciones adicionales para minimizar el riesgo de que se presenten nuevos problemas relacionados con la recuperación. Esta actualización rápida tiene como objetivo brindar la información más reciente sobre este incidente. Hemos confirmado que la infraestructura afectada ha regresado a un estado saludable y está operando según lo esperado. Continuaremos monitoreando de cerca las acciones de remediación implementadas y realizaremos los ajustes necesarios para mantener la estabilidad. Si los usuarios experimentan problemas residuales, limpiar las cachés DNS locales o reducir temporalmente los valores de TTL de DNS puede ayudar a garantizar una remediación más rápida.				
IM-177142	Cerrado	Incidente Mayor Intermitencias Equipos SDWAN	falla de un atenuador defectuoso el cual fue reemplazado y de esta forma se soluciona la falla presentada	falla de un atenuador defectuoso el cual fue reemplazado y de esta forma se soluciona la falla presentada	Ninguno	6/01/2026 14:00	6/01/2026 17:30	3h 30m
IM-178039	Cerrado	Incidente Mayor Afectación Antenas Starlink	Saturación o reinicio no registrado	e presentó afectación temporal del servicio de conectividad a internet en varias sedes a nivel nacional que cuentan con enlaces Starlink, con una duración aproximada de una (1) hora. Durante la atención del Incidente Mayor se realizó validación técnica con el proveedor Soingtel, quien confirmó que, según la plataforma de monitoreo de Starlink, las antenas asociadas a los servicios afectados se mantuvieron en estado en línea, sin evidenciar caídas de enlace, indisponibilidad ni alertas relacionadas con fallas del servicio. De acuerdo con la información suministrada por el proveedor, la afectación reportada no se asocia a una falla del servicio Starlink, por lo que se presume una condición de origen interno o un evento transitorio ajeno a la operación del proveedor. El servicio se restableció de forma automática, sin requerir intervención directa por parte del proveedor. Se realizaron notificaciones a los usuarios afectados y se deja como acción preventiva la revisión de equipos de red, energía y configuraciones locales en las sedes impactadas. Se procede con el cierre del Incidente Mayor, dejando el evento en observación y	Sabanalarga Curumani Melgar BAHIASOLANO Acacias PuertoCarreno SanAndres: la sede cuenta con internet mediante canal de tigo Riosucio choco Canasgordas Fusagasuga Cañasgordas	13/01/2026 14:44	13/01/2026 13:48	1 Hr 4 Min

				seguimiento en caso de presentarse recurrencia.				
IM-181044	Cerrado	Incidente Mayor Novedad en Internet Zona Sur	apertura óptica en enlace Yumbo San Bernardino a 56 km ópticos desde San Bernardino y además se observa corte aproximadamente a 500 mts de Torca	: Se realizó validación del enlace de fibra óptica Yumbo – San Bernardino, identificando una apertura óptica a 56 km desde el punto de San Bernardino. Adicionalmente, se evidenció un corte de fibra aproximadamente a 500 metros del sector de Torca. El proveedor ejecutó las labores correctivas correspondientes sobre el tramo afectado, normalizando los niveles ópticos del enlace y restableciendo la conectividad del servicio. Servicio operando con normalidad al momento del cierre.	Router_Facatativa Router_Monteria Router_Manizales Router_Turbo Router_Yarumal Router_Sonson Router_Santa_Rosa_de_Osos Router_Santa_Barbara Router_Rionegro Router_Puerto_Berrio Router_Guarne Router_Caucasia Router_Santa_Rosa_de_Cabal Router_Cali Router_Sincelejo Router_Barrancabermeja Router_Pereira UPS_Medellin Router_Santa_Marta Router_Apartado Router_Medellin SDWAN-FG80F-MEDELLIN RInternet_ETB_Medellin RInternet_ETB_Sincelejo RInternet_ETB_Monteria RInternet_ETB_Apartad	26/01/2026 9:31	26/01/2026 14:47	5 H 16 min Aproximadamente

					o SW6200 - MINTRABAJO-MEDLL4 SW6200 - MINTRABAJO-MEDLL3 SW6200 - MINTRABAJO-MEDLL2 SW6200 - MINTRABAJO-MEDLL1 Router_Sevilla RInternet_ETB_Cali RInternet_ETB_Pereira RInternet_ETB_Manizales Router_Cartago Router_Santander_de_Quilichao Router_Tulua Router_La_Dorada Router_Roldanillo Router_Palmira Router_Bugalagrande Router_La_Virginia Router_Dosquebradas Router_Villeta Router_Armenia Router_Popayan Router_Santa_Fe_de_Antioquia				
IM-182457	Cerrado	Incidente Mayor Sin internet zona Sur	Falla en enlaces troncales: Apertura del BB Primario Saldaña-Neiva	Se corrigió fallas por apertura de fibra.	Huila La Plata CAV3000077645 INC0000142765	30/01/2026 10:35	30/01/2026 11:32	57 m	

			Neiva-Bogota BB secundario Prado-Flandes Tramo: Purificacion-Prado y TK (2851906) Apertura BB primario Popayán – Manizales, Popayán – Yumbo. Tramo: Santander de Quilichao – Yumbo, apertura del BB secundario, Santander de Quilichao – Popayán.		90 Huila Pitalito CAV300 0077634 - INC000 0142766 25 Nariño La Unión CAV300 0077656 - INC000 0142766 34 Putuma yo Mocoa CAV300 0077669 - INC000 0142766 44				

Tabla 10 Incidentes Mayores

- **Otras Actividades**

  - Se realizó seguimiento a incidentes en backlog, para la documentación y cierre de casos pendientes de gestión.
  - Desde la gestión ITIL se realizaron auditorias de casos en los que se ha evidenciado oportunidades de mejora, las cuales son compartidas mediante correo a los especialistas a quienes se les realiza retroalimentación, con base a las novedades encontradas en cada caso.
  - Se envía tip de conocimiento sobre el correcto uso de las mayúsculas en la documentación de los casos.

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 enero
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=729/756*100 EF= 9,4%
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= 0/731*100 RRP= 0,2%

Tabla 11 Medición de KPIs

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

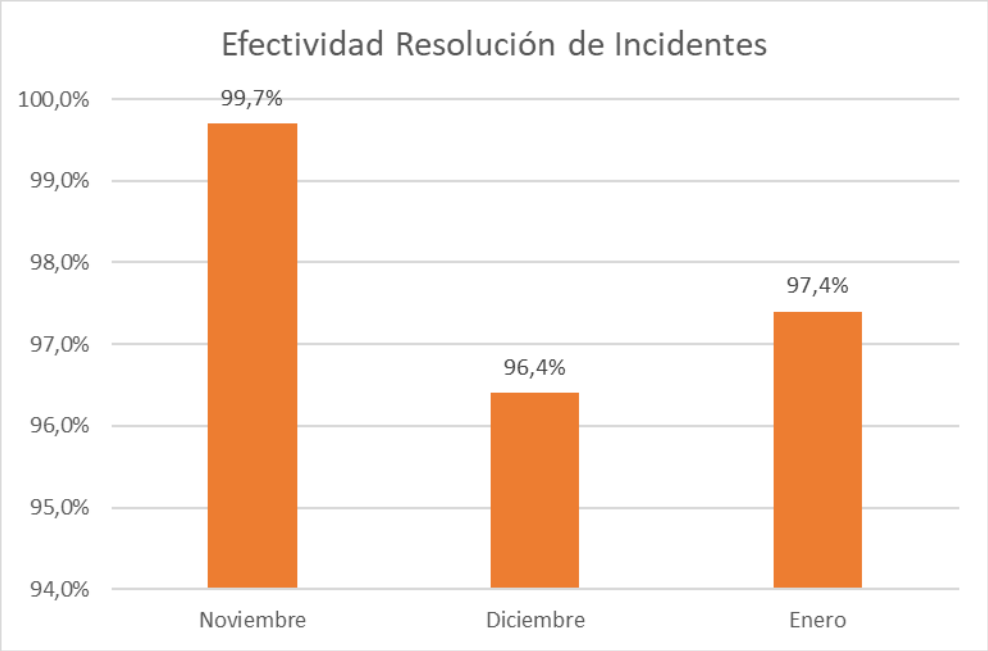


Ilustración 5 Efectividad de resolución de incidentes

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:

- Noviembre: 99,7%
- Diciembre: 96,4%
- Enero: 97,4%

Se identificó disminución en el cálculo del KPI debido a que 2 casos presentaron afectación del ANS y 17 quedaron en proceso y en suspendido a corte del 31 de enero. Es importante mencionar que el cálculo mensual depende de la cantidad de incidentes reportados en la herramienta de gestión durante cada mes, el desempeño sigue siendo satisfactorio. Como parte de la gestión de la práctica, se realizó retroalimentación con el equipo haciendo énfasis en la documentación y cumplimiento de los ANS definidos por cada servicio.

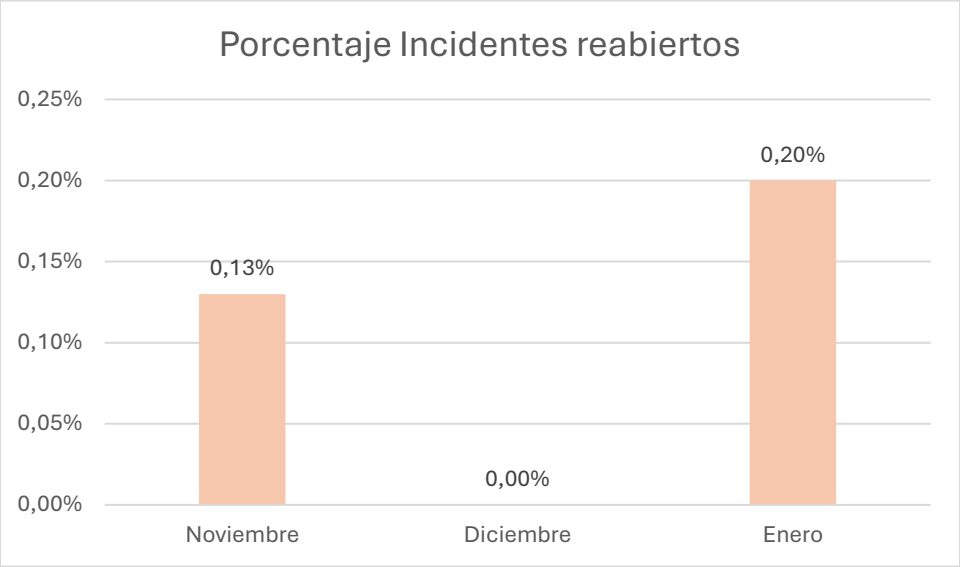


Ilustración 6 Porcentaje de incidentes abiertos

Durante el tercer trimestre, el porcentaje de casos reabiertos se mantuvo muy por debajo de la meta del 2%, para el mes de enero.

- Noviembre: 0.13%
- Diciembre: 0,0%
- Enero: 0.2%

El resultado sigue siendo favorable y refleja una adecuada gestión de incidentes.

2.1.2.7. Práctica de Requerimientos

Dar a conocer las actividades de la Práctica de Requerimientos correspondientes al mes de enero 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 5329 casos tipo requerimiento quedando en los siguientes estados:

Estado	Casos
Cerrado	5087
Solucionado	31
Suspendido	184
En proceso	26
Registrado	1

Tabla 12 Estados de Requerimientos

- Durante el mes, se presentaron 972 casos en estado anulado relacionados con respuesta automática a la solución de requerimientos que quedaron almacenados en la herramienta de gestión y fueron liberados el 1 de enero de 2026, se escaló el caso a fabricante para su solución.
- 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 noviembre al periodo actual.

Grupo Responsable	Diciembre	Enero
Especialista Redes	0	1
SOC	1	9
Especialistas IBM	0	4
Responsable Garantías Equipos	9	8
Responsable_De_Servidores_Windows	1	2
Responsable_Mesa_De_Servicio	6	98
Responsable_Soporte_Bogotá	6	42
Responsable_Soporte_Impresoras	1	6
Gestor de Inventarios	0	1
Responsable_Soporte_Territoriales	0	13
Especialista Base de datos	1	0
Total por Periodo	**25**	**184**

Tabla 13 Seguimiento del Backlog Suspendidos

En el inicio del período, se identificaron 25 casos suspendidos correspondientes al backlog del mes de noviembre de 2025. Se realizaron seguimientos semanales de las solicitudes en estado abierto, logrando la solución de 17 casos a través de la herramienta de Gestión Aranda de los anteriores periodos. Para el cierre del mes, se encuentran pendientes 184 casos en el mes de enero, 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	583
Radicar una solicitud.Alarma Zabbix.Impresora	348
Radicar una solicitud.Impresora.Instalacion - Configuracion	268
Radicar una solicitud.Directorio activo.Cambiar contraseña	221
Radicar una solicitud.Impresora.Aumento de cuota	195
Radicar una solicitud.Correo Electronico.Asesoria - Consulta	185
Radicar una solicitud.Directorio activo.Habilitar usuario	157
Radicar una solicitud.Equipo de computo.Actualización Bios	115
Radicar una solicitud.Equipo de computo.Devolución de equipo (portátil o PC)	109
Radicar una solicitud.Equipo de computo.Configuracion	102

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 583 tickets, Alarma Zabbix Impresora con 348 tickets, instalación y configuración con 268 tickets, y aumento de cuota con 195 tickets.
- Se realizó seguimiento a requerimientos en backlog, enviando correos a los especialistas para la documentación y cierre de casos pendientes.
- Desde la Práctica de ITIL se realizan auditorias de casos en los que se evidencian oportunidades de mejora, compartidas por correo a los especialistas a quienes se les hace retroalimentación, con base en las novedades encontradas en cada ticket.

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=** 5118/5329 *100
	EF: Efectividad en solución de Requerimientos.			
	RFS: Requerimientos solucionados que cumplen el ANS en el período.			**EF= 96.04%**
	RFR: Requerimientos registradas en el período.			
Porcentaje de Requerimientos Reabiertos en el Periodo	**RRP:** Porcentaje de casos Reabiertos en el periodo.	<2%	Mensual	**RRP=** 1/5118*100
	RFR: Requerimientos Reabiertos en el período.			**RRP= 0,020%**
	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:

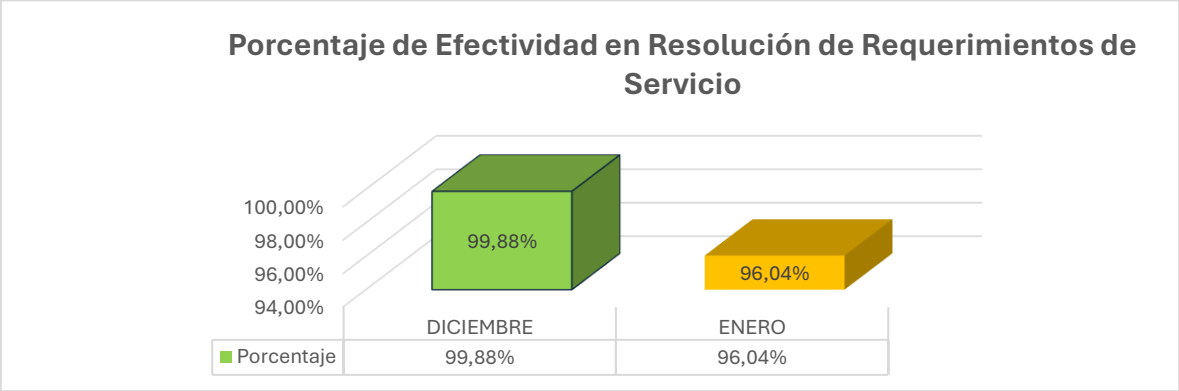


Ilustración 7 KPI Efectividad de Resolución de Requerimientos de Servicio

Durante el periodo, se evidencia el cumplimiento de la meta propuesta para el mes de enero con un porcentaje de 96.04% con un decrecimiento con respecto al mes anterior de 3.84%, para este mes se presentó un incremento en el número de casos en estado suspendido relacionados con inactivación de usuarios, realización de backups.

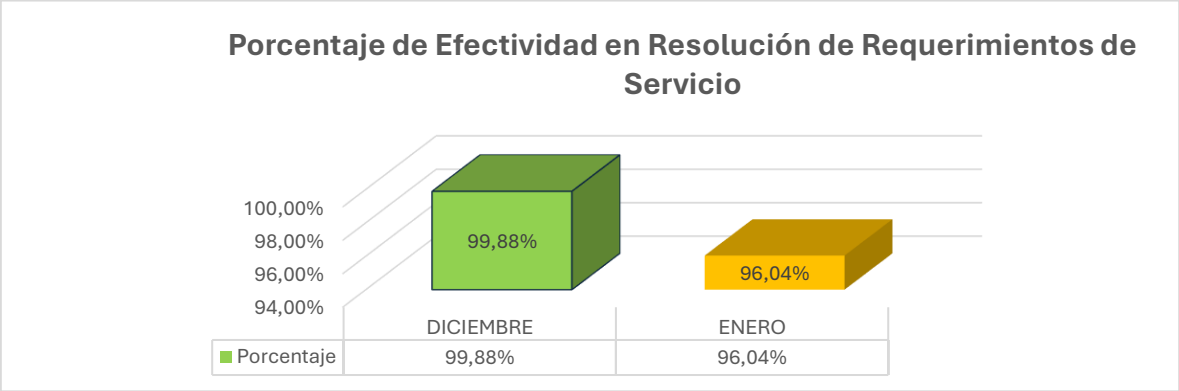


Ilustración 8 Requerimientos de Reabiertos en el periodo

Durante el periodo, se realizó el seguimiento de los requerimientos reabiertos por los usuarios y se ha presentado disminución de reaperturas en comparación de meses anteriores, debido la revisión del backlog desde la Práctica de requerimientos con los servicios TIC.

Para enero se presentó 1 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-180299	Radicar una solicitud.Correo Electronico.Configuracion	Responsable_De_Servidores_Windows	solicito se corrobore el informe de recuperación de mensaje de correo electrónico se realizó como se evidencia en las imágenes adjuntas.	El especialista reabre el caso para ampliar el contenido de la solución del caso precisando "Confirmación que el usuario cfuquen@mintrabajo.gov.co NO leyó el correo electrónico." 4. Confirmación expresa de NO lectura – cfuquen@mintrabajo.gov.co Tras la revisión detallada de los registros asociados al buzón cfuquen@mintrabajo.gov.co, se confirma de manera concluyente que: NO existen eventos de lectura, apertura o acceso al mensaje No se registran eventos tipo Read, Opened, MailItemsAccessed o equivalentes No hubo interacción del usuario con el contenido del correo No existe evidencia de exposición del mensaje en el buzón Por lo anterior, queda técnicamente confirmado que el usuario cfuquen@mintrabajo.gov.co NO leyó el correo electrónico. 5.Conclusión El proceso de recuperación fue ejecutado correctamente. El usuario cfuquen@mintrabajo.gov.co no recibió ni leyó el mensaje. No existe evidencia técnica de acceso o exposición del contenido en dicho buzón.

Tabla 16 Casos reabiertos

2.1.2.8. Práctica de Eventos

Para el mes de enero, se realizó validación de los casos generados en Aranda los cuales son reportados por el NOC con asunto “PROACTIVO NOC ZABBIX MINTRABAJO – xxxxxx” un total de 548 casos escalados mediante la herramienta de gestión de los cuales 347 alarmas fueron gestionadas por el NOC, los casos restantes corresponden a casos

generados por incidentes masivos que se relacionaron a los mismos o casos creados por los diferentes CI que hacen parte de una misma sede

- **Actividades ejecutadas por el líder de herramientas con Apoyo de Gestor de Eventos**

- Cambios en nombres e IP de Host de impresión.
- Inhabilitación de monitoreo para equipos apagados desde infraestructura.
- Creación de monitoreo para host de redes.
- Creación de dependencias para nuevos hosts recibidos.
- Categorización por sede, tipo y ubicación para los nuevos hosts.
- Optimización de la automatización de creación de mantenimientos, mejoras de la seguridad, los parámetros, personalización de nombres, timeout.
- Ajuste de mantenimientos ya programados para inspecciones, servicio de impresión
- Programación de mantenimientos en zabbix por ausencias de usuarios debido a permisos, vacaciones o estadía en territoriales.
- Se realizó afinación en las reglas que obligan a la asignación de notas cuando un caso pasa a estado suspendido.
- Se realizó la creación de 2 nuevas categorías en la CMDB antena Starlink y varios para la clasificación de los CI´s.
- Se creó el Grupo Indra para indicar que son los responsables de los CI´s

- **Actividades realizadas desde la Gestión de Eventos:**

- Se realizó seguimiento a casos en backlog
- Se realizó seguimiento de alarmas diarias en Zabbix y se envía reporte diario con apoyo del equipo NOC
- Solicitud de mantenimiento de sedes en las que los funcionarios apagan los equipos y/o se ausentan de las mismas
- Solicitud de Mantenimientos de acuerdo con RFC aprobados.
- Se valido con el equipo de redes las alarmas recurrentes y se tomaron acciones a nivel de monitoreo
- Se valido con soporte impresión las alarmas recurrentes y se tomaron acciones a nivel de impresión

De acuerdo con la Guía Operacional de la Práctica de Eventos, 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 enero
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= (546/548)*100 EF= 99,6%

Tabla 17 KPI Práctica de Eventos

- **Informe Operación NOC**

La labor del equipo del Centro de Diagnóstico y Operaciones (CDO) permitió identificar y gestionar oportunamente un total de 347 incidentes, lo cual evidencia una alta capacidad operativa y de respuesta ante eventos críticos.
Los Routers fueron el componente con mayor incidencia, concentrándose 180 casos (52% del total). Esto está asociado a factores como la inestabilidad de la red eléctrica en zonas remotas o condiciones ambientales adversas.
Para este mes se evidencia una disminución en los casos reportados por Antenas Starlink, los cuales se encuentran en el segundo lugar, representando 70 (20% 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 presentan disminución para este mes representaron el 13% de los casos (45 incidentes), eventos causados por falla en la energía comercial, apagado de equipos por parte de los funcionarios e intermitencias en el servicio en horario no hábil. En los eventos que se presentaron en horario no hábil no se logró determinar la causa raíz. A comparación de meses anteriores se ha visto una mejoría en la operación de los FortiGate.
Los servidores Windows en cuarto lugar representados 30 (9% del total) de los incidentes, evidenciando este mes disminución de eventos en comparación con el mes anterior, aunque, son considerablemente altos en comparación con los Servidores Linux con solo 1 caso, representando el 0% del total de los casos.
Los Access Points ocupan el 5to lugar con un 3% (11 casos) del total de los incidentes, cifra la cual es similar en comparación con los meses anteriores ya que en este aumento solo un caso.
Los dispositivos Switches reflejan una baja incidencia del 3% (10) del total de los casos, lo cual muestra una baja incidencia en fallas relacionadas a estos equipos.

Redes y Conectividad

Routers: Desde el centro de operaciones NOC durante el mes de enero se gestionaron 180 incidentes relacionados con equipos de red Routers en diferentes sedes a nivel nacional, los cuales representaron el 52% de los casos.

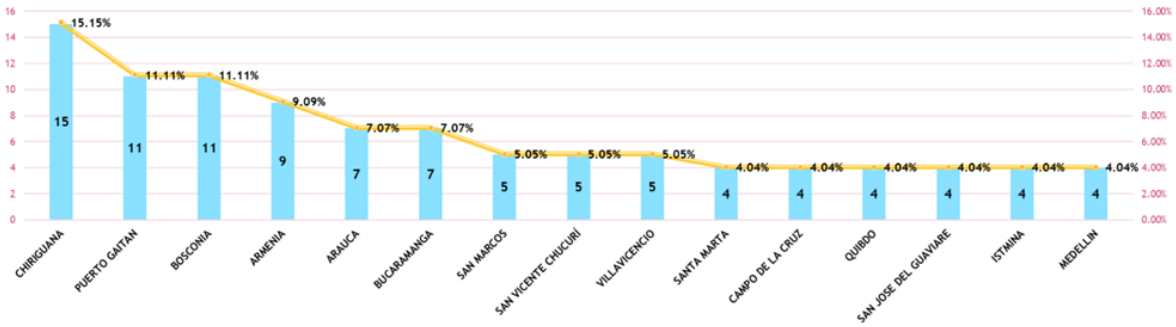


Ilustración 9 Top de incidentes por sedes

– Para el mes de febrero se evidencia que la sede Chiriguaná tiene el mayor número de incidentes, registrando 15 casos, representando el (15,15%) del total de esta categoría. La causa predominante en la mayoría (13 de los 15 casos) es la

desconexión o apagado físico de equipos por parte de los funcionarios al finalizar su jornada laboral, lo que genera alarmas en Zabbix fuera del horario hábil.

- Puerto Gaitán y Bosconia ocupan el segundo lugar con 11 casos cada una, que sumando en conjunto representan el (22,22%) corresponden en su mayoría (12 de los 22 casos) a Falla Energía Eléctrica, seguida por Desconexión/apagado Físico de Equipos en Sede (7 de los 22 casos) y los 3 casos restantes corresponden a Falla en Red de Proveedor.
- Armenia ocupa el tercer lugar con 9 casos (9,09%) de los cuales 4 son por falla de energía eléctrica, 3 por Intermitencia/Lentitud en la red, 1 por Falla en Red de Proveedor y 1 por Bloqueo de Dispositivo.
- Arauca y Bucaramanga se posicionan en el cuarto lugar del TOP 10 con 7 casos cada una (7,07% C/U). La causa principal de los incidentes en Arauca para este mes está dividida en dos, por un lado 4 casos por Intermitencia/Lentitud en la red y 3 casos por Falla Energía Eléctrica. Por otro lado, Bucaramanga presento 4 causas, las principales fueron Actividad programada, Falla Energía Eléctrica e Intermitencia/Lentitud en la red cada una con 2 eventos registrados y el restante por Falla en Red de Proveedor.
- Las sedes de San Marcos, San Vicente Chucuri y Villavicencio, las tres con 5 casos cada una relacionados a Routers. En San Marcos 4 de los 5 incidentes se relacionan a Desconexión/apagado Físico de Equipos en Sede y el restante a Falla Energía Eléctrica. San Vicente Chucuri registro 2 casos relacionados a Falla Energía Eléctrica, 2 por Intermitencia/Lentitud en la red y 1 por Desconexión/apagado Físico de Equipos en Sede. Villavicencio registro 3 casos por Falla Energía Eléctrica y 2 por falla en red de proveedor.
- Por último, tenemos las sedes de Santa Marta, Campo de la Cruz, Quibdó, San José del Guaviare, Istmina y Medellín cada una con 4 incidentes registrados que sumados en conjunto representan 24 casos y el 24,24% del total de los casos para esta categoría. La causa común entre estas sedes y que predomina con 12 de los 24 casos en conjunto son por Falla Energía Eléctrica.

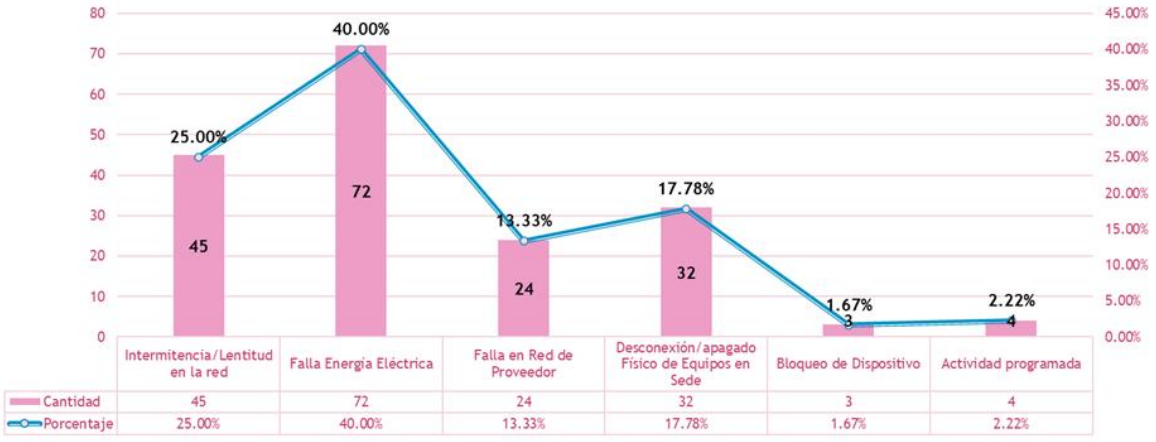


Ilustración 10 Top de incidentes por sedes

- Se evidencia que la causa principal del total de eventos para la categoría de Routers es por Falla Energía Eléctrica ocupando el 40,00% y seguido por la falla en

Intermitencia/Lentitud en la red y este último con un 25,00% del total de los casos para esta categoría.

- Las fallas por energía eléctrica representan el 40,00% de los casos (72), afecta principalmente a zonas remotas o sin tecnología de respaldo como Bosconia, Puerto Gaitán y Armenia, entre otras, donde la red eléctrica es inestable o está sujeta a cortes constantes.
- El 25,00% (45) 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 Arauca y Armenia.
- El 17,78% (32) de los casos están relacionados a desconexión apagado físico de equipos en sede, siendo Bosconia y Chiriguana 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 13,33% (24) de los casos están relacionados a Falla en Red de Proveedor, siendo Puerto Gaitán la sede con mayor número de eventos registrados (3) por esta causa y seguido por Mariquita, Medellín y Pasto cada una con 2 casos. De estos registra 1 caso de Mariquita en estado suspendido y escalado con el tercer nivel de ETB, todos los demás están en estado cerrado o solucionado por diferentes causas en la infraestructura de la red del proveedor.

- El 3,89% (7) de los casos es por bloqueo de dispositivo y actividad programada que en conjunto suman este porcentaje. Siendo actividad programada la categoría con mayor número de eventos (4), seguida de bloqueo de dispositivo con 3 eventos representando el 1,67%. En varios casos, el bloqueo ocurre tras eventos eléctricos o fluctuaciones de red.
- Se evidencia que del total de eventos generados (180) para la categoría de Routers durante el mes de enero registran entre cerrados y solucionados representan el 97% (174) y 6 en estado suspendido, debido a:
- IM-182296 Pendiente asistencia técnica el día 3 de febrero por parte de ETB.
- IM-182442 Servicio en validación con el proveedor
- IM-176971 A espera de encendido de equipos.
- IM-178808 A espera que regresen los funcionarios el 4 de febrero.
- IM-182038 Está siendo validado por 3cer nivel, a espera de nuevos avances.
- IM-182063 A la espera de RFO por parte de UM.

Switches

Desde el Centro de Operaciones (NOC), durante el mes de enero se generaron 10 casos referentes a Switches en la herramienta de monitoreo Zabbix en diferentes sedes, los cuales representan el 3% del total de los casos, donde se evidencia un leve aumento de 5 casos en comparación con el mes pasado. Se identifico que es posible que zabbix verifique

primero los hosts dependientes y después los host padres, al presentarse, zabbix crea los casos correspondientes a cada uno de los hosts alertados, es decir, que en esta situación las dependencias no actuarían.

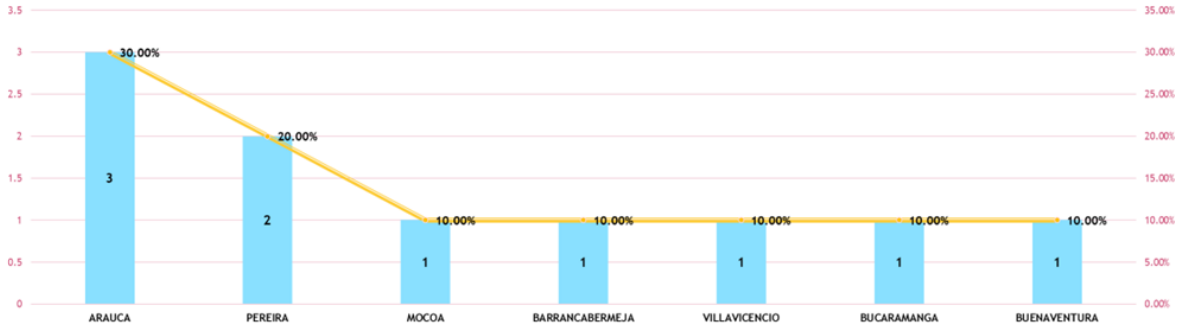


Ilustración 11 Eventos por sedes routers

- Por parte del grupo NOC en el mes de enero, se evidencia que, de los 10 eventos registrados sobre Switches, la sede con mayor número de eventos fue a Arauca con 3 eventos (30,00%), Facatativá, en según lugar esta Pereira con 2 eventos (20,00%) y por último tenemos a Mocoa, Barrancabermeja, Villavicencio, Bucaramanga y Buenaventura cada una con 1 evento registrado y representando el 10% de forma individual.

A continuación, se relacionan las causas que generaron las alarmas:

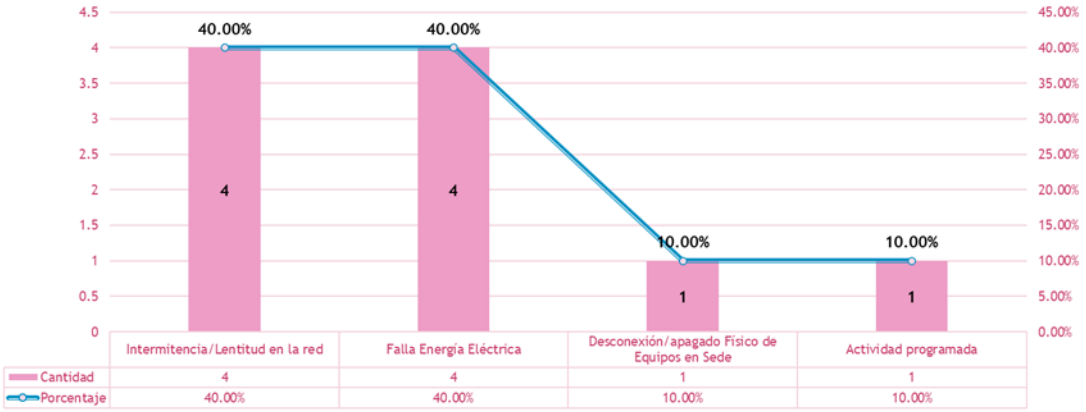


Ilustración 12 Top de causas por sedes switches

- Se listan 4 diferentes causas para la categoría de Switches registradas durante el periodo del mes de enero.
- Para el mes de enero tenemos una igualdad entre las categorías de Intermitencia/Lentitud en la red y Falla Energía Eléctrica ya que cada una registra 4 eventos, representando el 40,00% del total de los casos para esta categoría de forma individual.
- Por último, también se evidencia una igualdad entre las categorías Desconexión/apagado Físico de Equipos en Sede y Actividad programada las cuales registran 1 evento cada una, representando el 10,00% de forma individual.

El evento por actividad programada se produjo por una actividad controlada en la UPS de la sede.

Esta distribución refuerza nuevamente el patrón observado en otros tipos de dispositivos: la inestabilidad del suministro eléctrico es el factor predominante que impacta la disponibilidad de la infraestructura de red, incluso en equipos pasivos como los Switchs.

De los 10 eventos registrados para la categoría de Switches en el mes de enero, los 10 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 enero se gestionaron 11 incidentes asociados a equipos de red WLAN – Access Point en distintas sedes a nivel nacional, los cuales representan el 3% 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.

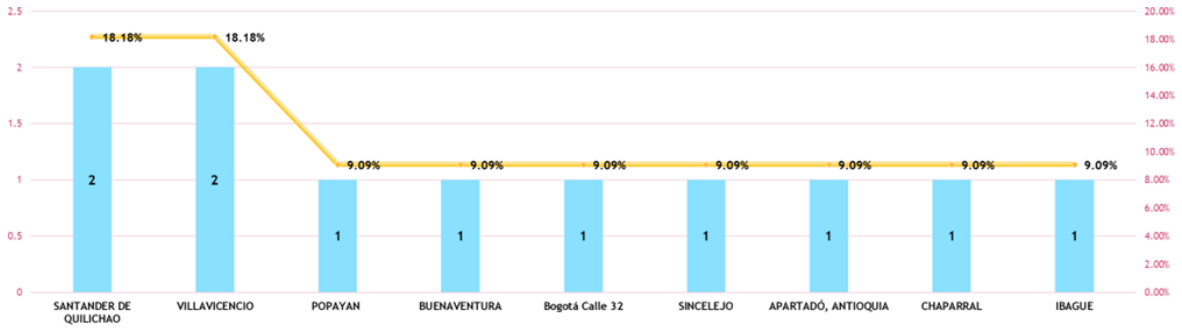


Ilustración 13 Top de eventos por sedes Access Point

Durante el mes de enero se evidencia que las sedes con mayor número de eventos relacionados con Access Point es Santander de Quilichao y Villavicencio, las dos igualando con 2 casos cada una que representa el 18,18% cada una del total de los casos, conservando el primer y segundo lugar en el TOP. Estas también igualan en eventos por categoría ya que Villavicencio presenta 2 por falla de energía eléctrica y Santander de Quilichao 2 por Intermitencia/Lentitud en la red.

Por otro lado, las sedes restantes como Popayán, Buenaventura, Bogotá calle 32, Sincelejo, Apartado Antioquia, Chaparral e Ibagué presentaron cada una con 1 evento, representando el 9.09% de forma individual. Los casos de las sedes de Buenaventura, Sincelejo e Ibagué registran bajo la causa de Desconexión/apagado Físico de Equipos en Sede, los casos de las sedes de Popayán, Bogotá calle 32 y Chaparral registran bajo la causa de Intermitencia/Lentitud en la red y el caso restante de Apartado Antioquia registra bajo la causa de Falla Energía Eléctrica.

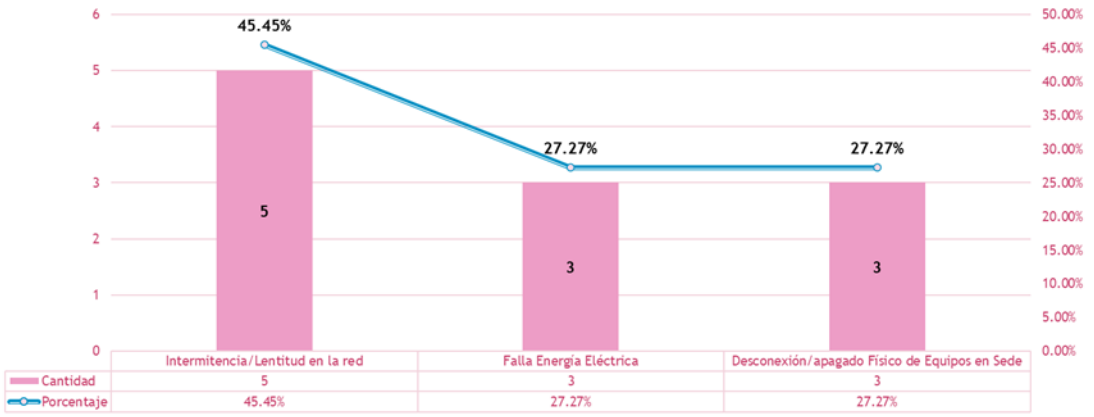


Ilustración14Top de causas por sedes Access point

Se evidencian 3 causas de fallas para el periodo del mes de enero con relación a los dispositivos Access Point.

El 45,45% de los incidentes en APs (5 de 11) están directamente relacionados con Intermitencia/Lentitud en la red. El 27,27% relacionados a Falla Energía Eléctrica y Desconexión/apagado Físico de Equipos en Sede en donde se registró 3 eventos por cada causa de forma individual debido a que los funcionarios apagan equipos cuando salen de sede.

Starlink

Desde el centro de operaciones NOC durante el mes de enero se gestionaron 70 incidentes relacionados con equipos de red Starlink en diferentes sedes a nivel nacional, los cuales representan el 20% del total de los casos.

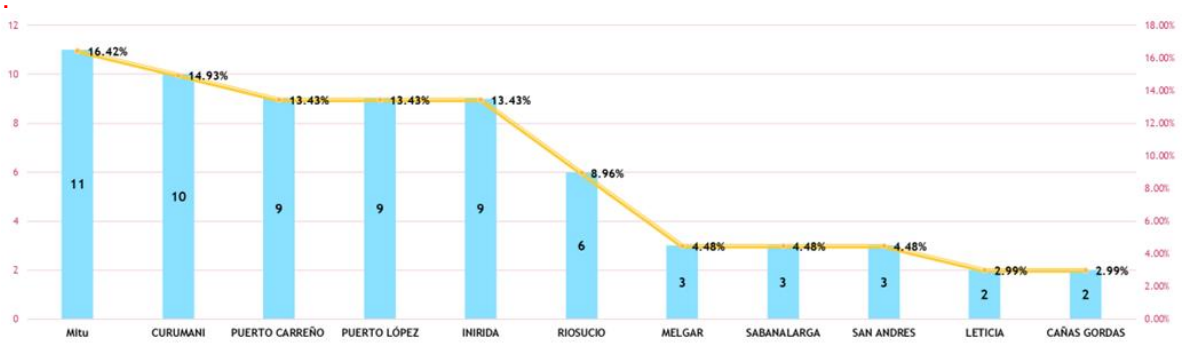


Ilustración 15 Top de eventos por sedes Starlink

Para el mes de enero el TOP 10 de las sedes con mayor número de eventos generados para la categoría de Starlink fueron Mitú con 11 eventos, representando un 16,42% la cual

puntea en primer lugar. Curumaní con 10 eventos, representando un 16,42%. Puerto Carreño, Puerto López e Inírida con 9 eventos cada una, representando un 13,43% de forma individual. Riosucio con 6 eventos, representando un 8,96%. Melgar, Sabana Larga y San Andrés con 3 eventos cada una, representando un 4,48% de forma individual. Leticia y Cañas Gordas con 2 eventos cada una, representando el 2,99% de forma individual.

Los eventos por Falla Energía Eléctrica son la causa predominante con 40 casos en la mayoría de las sedes del TOP de equipos Starlink, representando el 57,14% del total de los casos para esta categoría, estas ocasionadas por interrupción en el servicio durante pocos minutos sin diagnostico en sitio.

En este mes Mitú puntea con mayor número de eventos (10 casos) y seguido de Inírida con 9 eventos relacionados con Falla Energía Eléctrica.

La segunda causa que predomina es por Desconexión/apagado Físico de Equipos en Sede con 18 casos en la mayoría de las sedes del TOP de equipos Starlink, representando el 25,71% del total de los casos para esta categoría.

Las sedes con mayor número de eventos por Desconexión/apagado Físico de Equipos en Sede para este mes son Curumaní con 9 eventos. Sabana Larga y Puerto López con 3 eventos cada una de forma individual.

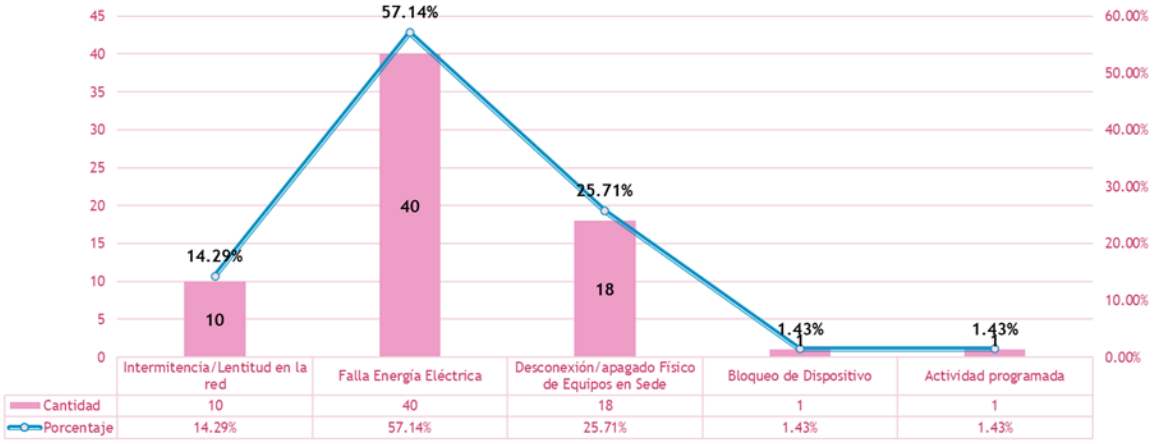


Ilustración 16 Top de causas por sedes Starlink

En tercer lugar, tenemos la causa de Intermitencia/Lentitud en la red con 10 eventos registrados del TOP de equipos Starlink, representando el 14,29% del total de los casos para esta categoría, estas ocasionadas por interrupción en el servicio durante pocos minutos sin diagnostico en sitio.

Se evidencia que las sedes con mayor número de eventos registrados por Intermitencia/Lentitud en la red son Rio Sucio, Puerto Carreño y San Andrés las cuales igualan con 2 casos registrados cada una para esta causa sobre esta categoría de Starlink.

Durante el mes de enero se pudo observar que la falla en dichos puntos con este dispositivo Starlink se debió a efectos climáticos y por energía eléctrica, lo que ocasiono constantes caídas en este servicio.

Hay casos que se evidenciaron durante el horario no hábil y, por lo tanto, no se determinaron las causas reales de las alarmas, debido a que estas subieron a los pocos minutos; estas fallas se atribuyen a intermitencias causadas por malas condiciones climáticas que del mismo modo afectan el servicio de energía.

Según lo registrado se evidencia que los casos suspendidos VS. Casos solucionados o cerrados del total de los 70 eventos registrados para la categoría Starlink durante el mes de enero, se reportan que el 99% de los casos fueron solucionados y el 1% (1 caso) se encuentra pendiente por validaciones y en estado suspendido hasta que se encienda el dispositivo por parte de los funcionarios.

Fortigate

Desde el centro de operaciones NOC durante el mes de enero se gestionaron 45 incidentes relacionados con equipos de red FortiGate en diferentes sedes a nivel nacional, los cuales representaron el 13% del total de los casos, ocupando el tercer lugar.

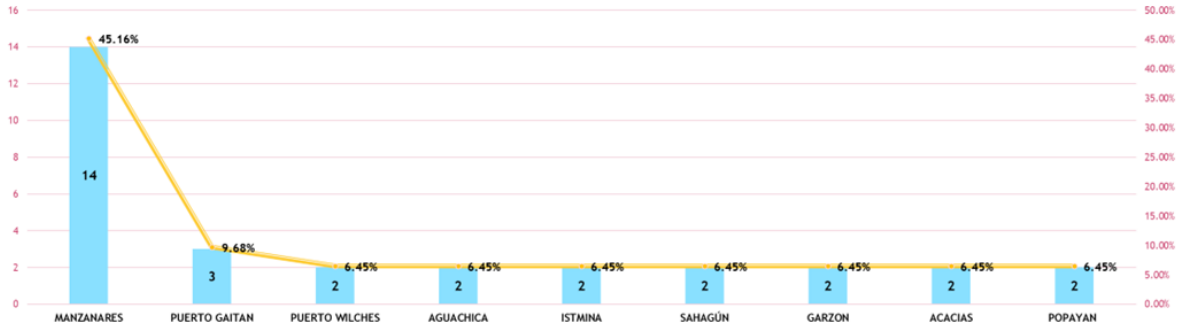


Ilustración 17 Top de incidentes por sedes fortigate

Durante el análisis del comportamiento de la red SD-WAN en el mes de enero, se identificó una mayor frecuencia de afectación y se presentó en la sede de Manzanares la cual está ocupando el primer lugar con 45,16% (14 casos) del total de casos para esta categoría, en segundo lugar esta Puerto Gaitán con un 9,68% (3 casos) y por ultimo tenemos el resto de sedes (Puerto Wilches, Aguachica, Istmina, Sahagún, Garzon, Acacias y Popayán) que registran una baja tasa de eventos, cada una con 2 (6,45%) eventos registrados.

La causa con mayor número de eventos registrados en Manzanares fue Desconexión/apagado Físico de Equipos en Sede con 12 casos, que afectan directamente la disponibilidad de los enlaces SD-WAN ya que los funcionarios desconectan los dispositivos de forma preventiva. Se recomienda evaluar medidas de mitigación como implementación de respaldo energético (UPS o plantas). Los dos casos restantes registran por Intermitencia/Lentitud en la red.

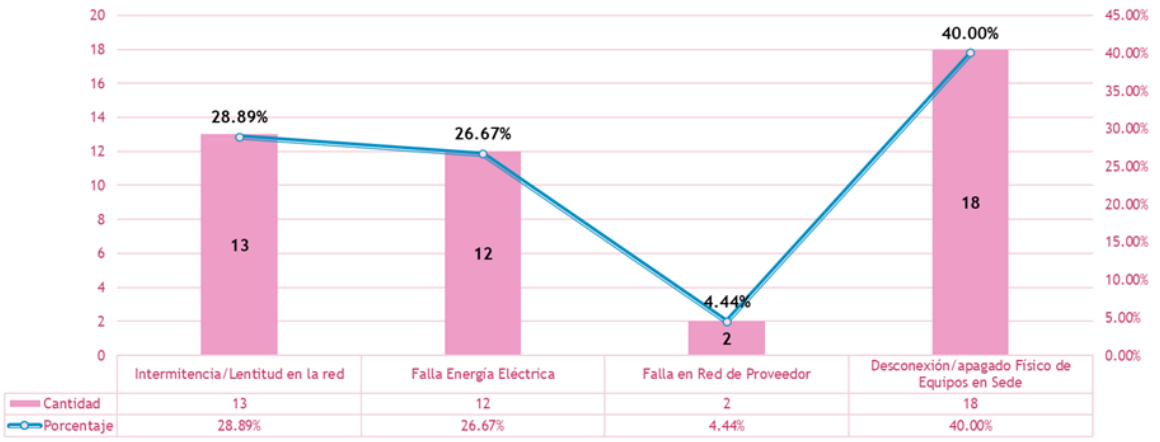


Ilustración 18 Top de causas por sedes fortigate

Durante el mes de enero, los dispositivos SD-WAN presentaron una tasa alta en cuanto a la causa de Desconexión/apagado Físico de Equipos en Sede con 18 eventos registrados, representados con el 40,00% del total de los casos para esta categoría. que se atribuyen al apagado de los equipos por parte de los funcionarios al salir de labores para evitar daños por picos altos en la energía.

Un 28,89% (13 casos) de las alarmas correspondieron a Intermitencia/Lentitud en la red Estas ocasionadas por condiciones climáticas adversas, validadas por el soporte en sitio y algunas fuera de horario hábil.

En tercer lugar, tenemos un 26,67% (12 casos) de los eventos registrados durante el mes a Falla Energía Eléctrica que se atribuyen a interrupciones en horario hábil y otros en horario no hábil.
Por otro lado, el 4,44% (2 casos) de los eventos registrados se atribuyen a Falla en Red de Proveedor en donde se realizaron las labores correctivas por parte de Claro y de este modo queda nuevamente operativo el servicio.
De los 45 casos relacionados con los dispositivos SD-WAN, 40 se encuentran a fecha de corte cerrados exitosamente, representando un 89% de resolución operativa dentro del mes por parte del centro de operaciones NOC. Mientras que el 11% (5) de los casos se encuentran en estado suspendido de los cuales 2 (Agua Chica y Acacias) están a espera de validaciones con soporte en sitio, 1 (Agustín Codazzi) a espera que retorne el servicio de energía, 1 (Puerto Asís) a espera que el funcionario retorne a labores el día 4 de febrero y el caso restante (Tumaco) a la espera de la llegada de los accesorios para la instalación de la antena Starlink. Información con corte al cierre de enero.

Casos Escalados a Proveedor de Telecomunicaciones

Durante el mes de enero se registraron 25 casos que fueron escalados y gestionados con proveedor ETB y TIGO de los cuales el 100% quedaron en estado solucionado o cerrado.

Servicios Centrales

Servidores Windows

Durante enero, el Centro de Operaciones de Red (NOC) gestionó 30 incidentes asociados a servidores Windows, equivalentes al 9% del total de casos registrados durante el mes.

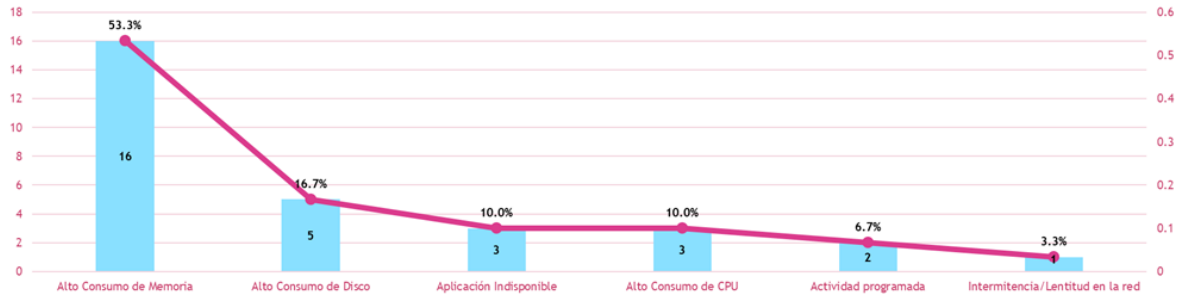


Ilustración 19 Top de eventos Windows

Se evidencia que para el mes de enero la causa principal y con mayor número de eventos es por Alto Consumo de Memoria con 16 eventos registrados y representando el 53,3%, seguido por Alto Consumo de Disco con 5 eventos registrados, representando el 16,7%, en tercer lugar tenemos a Alto Consumo de CPU, representando el 20,0% , en cuarto lugar tenemos a Actividad Programada con 2 eventos registrados, representando 6,7% y por último en quinto lugar tenemos a Intermitencia/Lentitud en la red con 1 evento, representando 3,3%.

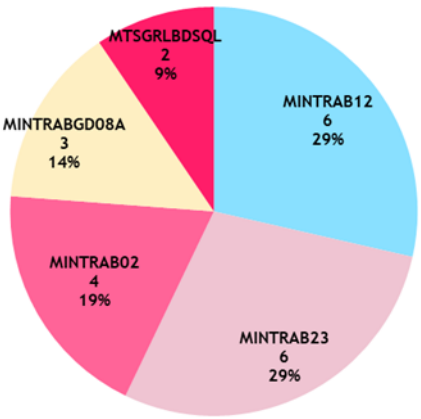


Ilustración 20 Top de servidores Windows

El servidor MINTRAB23 para este mes representan el 29% (6 casos) del total de los casos para esta categoría, se reporta que en su mayoría (3) los casos están relacionados a aplicación indisponible; el servidor MINTRAB12 representa el 29% (6 casos) todos relacionados a alto consumo de memoria, el servidor MINTRAB02 registra 4 eventos, representando el 19% y todos están relacionados a alto consumo de memoria. El servidor MINTRABGD08A registra 3 eventos, representando el 14% y están relacionados a alto consumo de CPU, memoria y disco. Por último, el servidor MTSGRLBDSQL registra 2 eventos y representa el 9%, de los cuales 2 están relacionados a alto consumo de memoria. Estas VM están relacionadas a parchados realizados durante el mes de enero, se parcho la versión de SQL Server, lo cual generaba una indisponibilidad controlada de las aplicaciones, realizado a través de RFC, De igual forma estas VM son de appp y ddbb sql, los demás son servidores de alto consumo, gestor documental, SQL productivo, aplicaciones .NET que normalmente tienen mucho trafico
Se evidencia que de los 30 eventos registrados durante el mes de enero, los 30 están en estado cerrado y solucionado. Lo cual refleja una efectiva y oportuna gestión por parte de los especialistas con los eventos reportados, reflejando un porcentaje del 100% de gestión de los casos.

Servidores Linux

Durante enero, el Centro de Operaciones de Red (NOC) gestionó 1 incidente asociado a servidores Linux, equivalentes al 0% del total de casos registrados en el mes.

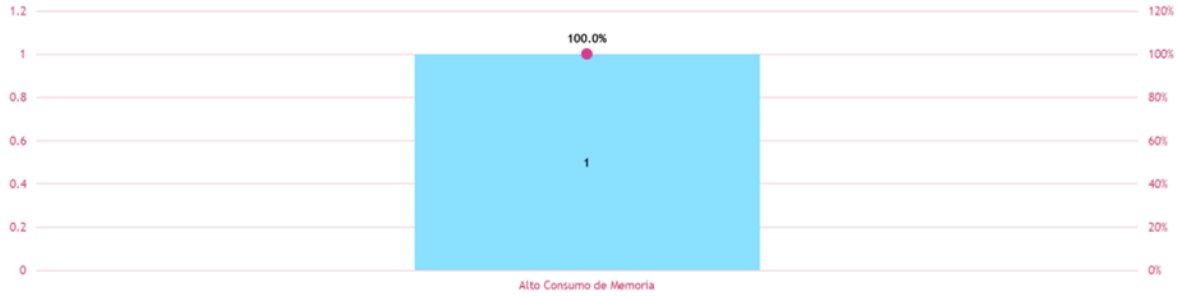


Ilustración 21 Top de causas eventos linux

La causa principal de los eventos registrados muestra que todos están asociadas a factores conocidos y potencialmente controlables. El alto consumo de memoria representando un 100% ya que fue el único evento registrado para el mes de enero sobre esta categoría de servidores Linux.

En comparación con meses anteriores, la cantidad de casos es baja, sin embargo, se puede obtener una clara oportunidad de mejora en la gestión operativa. Una revisión proactiva de protocolos de encendido/apagado, reinicios, programación de tareas y manejo de dispositivos puede tener un impacto significativo en la prevención de eventos y en la mejora general de la disponibilidad y estabilidad del sistema.

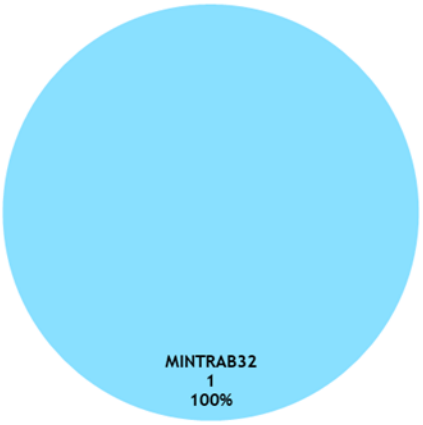


Ilustración 22 Top de servidores linux

Para este mes se observa que el caso reportado tiene un solo servidor relacionado, por lo tanto, es el único servidor en la gráfica. El evento presentado fue por alto consumo de memoria.

Gráficas de CPU Zabbix de todo el mes sobre servidores

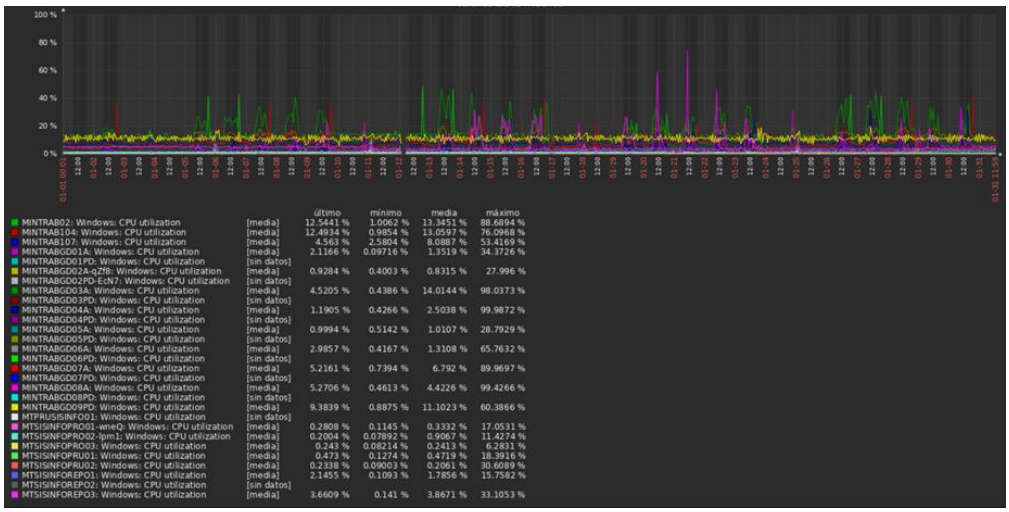


Ilustración 23 Gráficas CPU Zabbix

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

CPU

MINTRABGD03A	14.0144%
MINTRAB02	13.3451%
MINTRAB104	13.0597%
MINTRABGD09PD	11.1023%
MINTRAB107	8.0887

Gráfica de MEMORIA Zabbix de todo el mes sobre servidores



Ilustración 24 Gráfica memoria servidores

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

MEMORIA

MINTRAB104	78.2882%
MINTRAB02	75.4456%
MINTRAB107	73.6235%
MINTRABGD09PD	45.6436%
MINTRABGD07A	42.0308%

Datacenter (Cali - Bogotá)

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

2.1.2.9. Práctica de Disponibilidad

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

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

Servidores

Cantidad de dispositivos	Disponibilidad consolidada
113	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
5	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%
STM-FG-600F-SDWAN-HUB02	100%

Tabla 24 Desagregado Disponibilidad de equipos Datacenter alterno

Redes y conectividad

Cantidad de dispositivos	Disponibilidad consolidada
493	98,66%

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
6	100,00%

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	100,00%
MINTRABVULNE01	100,00%
SOC_Fortianalyzer	100,00%
SOC_FortiDDOS	100,00%
SOC_SandBox	100,00%
SOC_WAF	100,00%
SOC_FW_Sede_Central	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.
- Se elaboró plan de disponibilidad para la vigencia 2026

2.1.2.10. Práctica de Implementación

Dentro de la aplicación de la práctica, se desarrollaron procesos para apoyar a planificar, programar, ejecutar, controlar, aplicar pruebas e implementar nuevos servicios o incluir modificaciones de las funcionalidades de los aplicativos o sistemas de información en producción.
A continuación, se muestra la información correspondiente a la práctica de implementación para el periodo del 1 al 31 de enero de 2026.

Actividades en curso:

Revisión de los RFC ejecutados durante el periodo, para los cuales (14) cambios fueron aprobados su cierre, ya que cuentan con las evidencias completas de los planes de Pruebas Previas y Posteriores, al corte del 31/01/2026 se encuentra (9) casos abiertos (en proceso de revisión) a la espera de entrega de las evidencias por parte los especialistas.

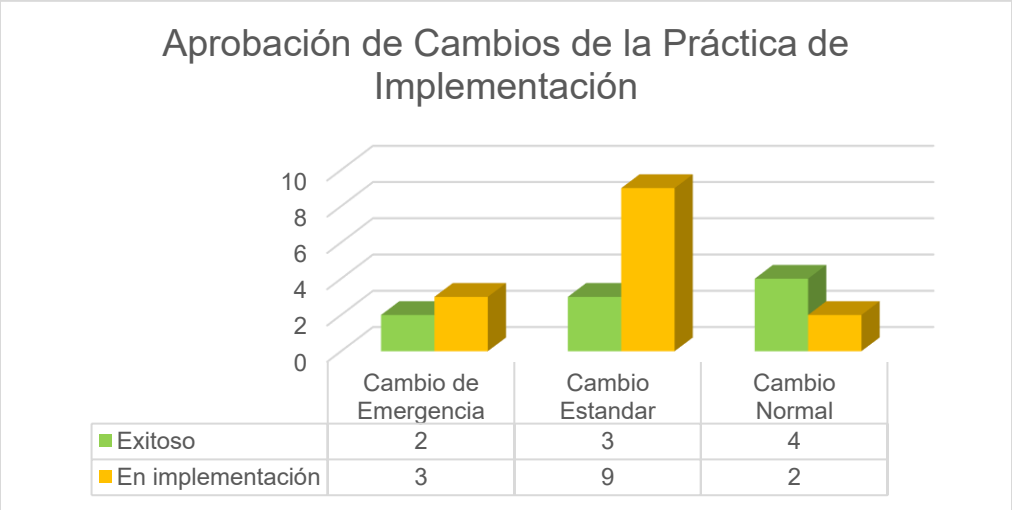


Ilustración 25 Seguimiento Práctica Implementación

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

Seguimiento%20de
%20cambios%20Imp

2.2 Mesa de Servicios y Soporte en Sitio

A continuación, se presenta la gestión desarrollada durante el mes de enero 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 enero, a la MDS ingresaron 367 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	261	259	258	0	2	0
COL - Mintrabajo-Gestor-documental	55	54	53	0	1	0
COL - Mintrabajo-office365	34	34	33	0	0	0
COL - mintrabajo-Impresora	17	16	16	0	1	0
TOTAL	367	363	360	0	4	0

Tabla 30 Llamadas Atendida por la Mesa de Servicio

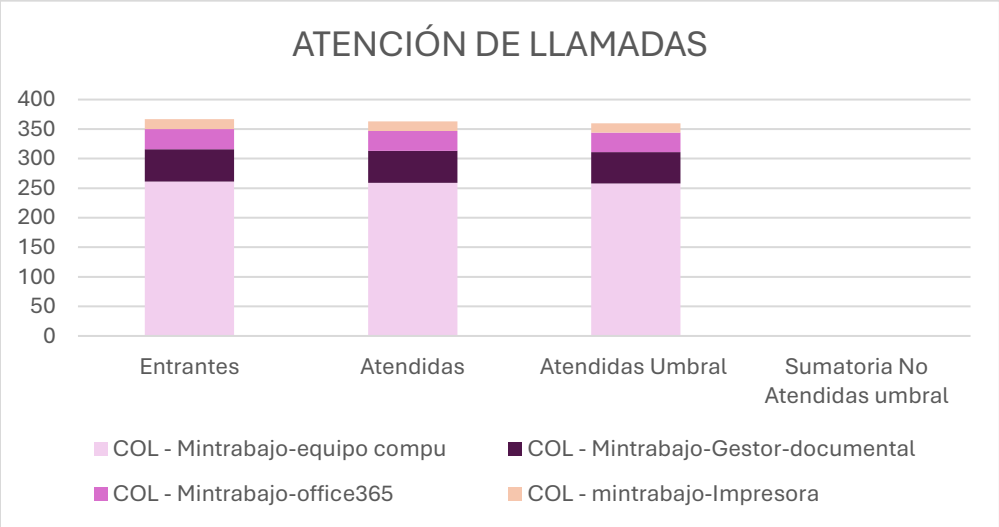


Ilustración 26 Llamadas Atendidas

El servicio más solicitado a través de la atención de llamadas es: Equipo de cómputo con 261 llamadas entrantes, se atendieron 259 solicitudes se observan: 4 llamadas Abandonadas 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_ENERO.xlsx pestaña *categoría.*

- **Análisis de Casos Anulados por Servicio**

Para este periodo se tiene 974 casos anulados de los siguientes servicios:

CASOS ANULADOS	TOTAL
Creación de Servicio	972
Herramientas de Gestión	2
Total general	**974**

Tabla 31 Casos anulados por Servicio

- **Creación de Servicio:** se tiene 972 casos debido a generación masiva de casos, realizando la validación de los correos enviados se encontró que estos son el resultado de casos ya solucionados y de envió encuestas masivas, al verificar la configuración se encontró un recordatorio de encuesta el cual fue el encargado de reenviar correos pendientes por encuestas. Adjunto las evidencias enviadas por fabrica, se tomaron estas acciones para evitar que se repita la situación.

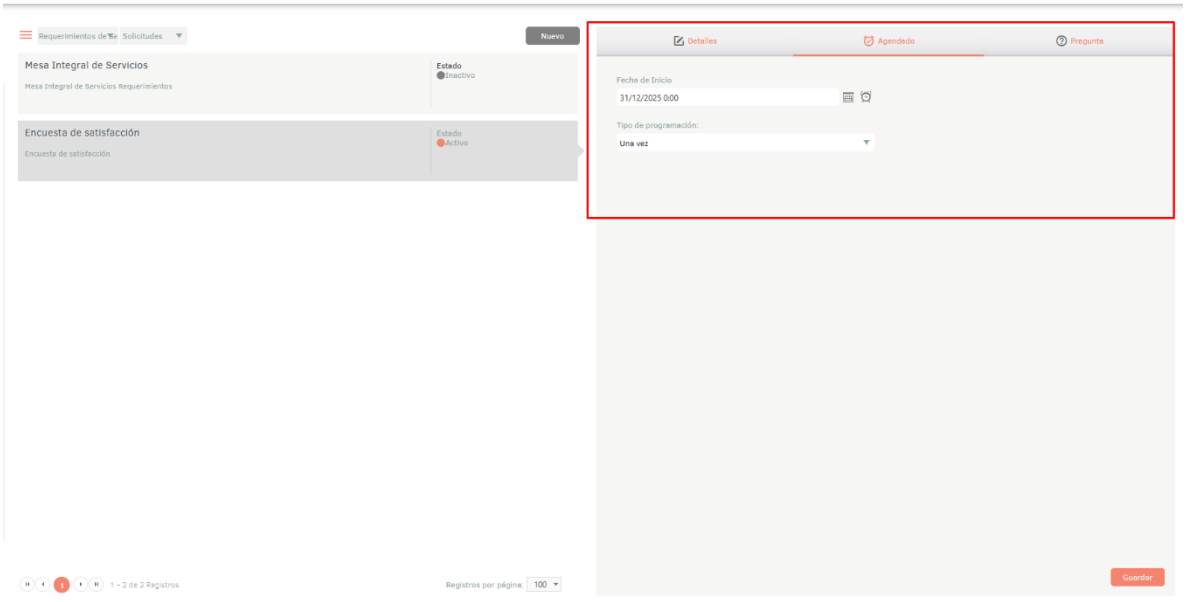


Ilustración 27 Evidencia creación masiva de casos

- Esta configuración lo que realiza es enviar un correo de "recordatorio" de las encuestas de los casos de ese modelo que aplico esa encuesta que no se han respondido hasta el momento.

    - Viendo los correos, todos estos se generaron el día 1 de enero,

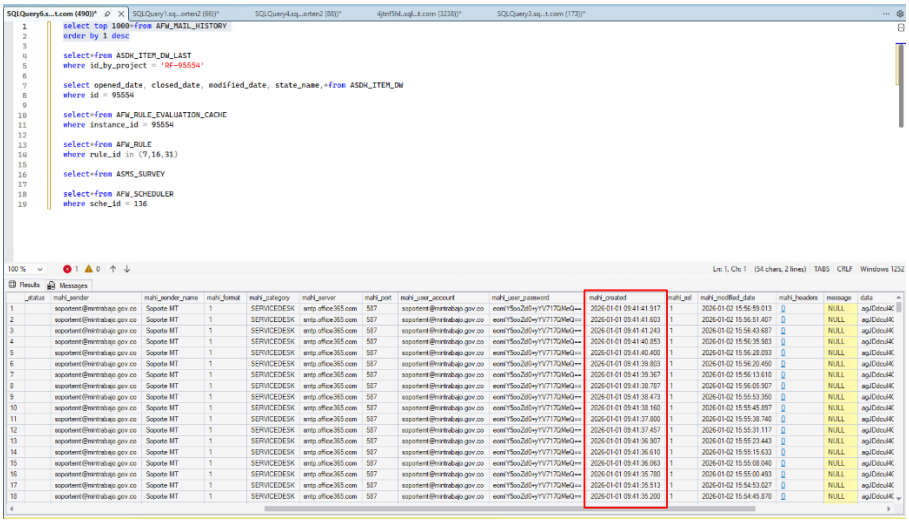


Ilustración 28 Correos generados masivamente

- Se evidencia que aún hay correos en cola generados y por lo anterior se realizó su depuración.

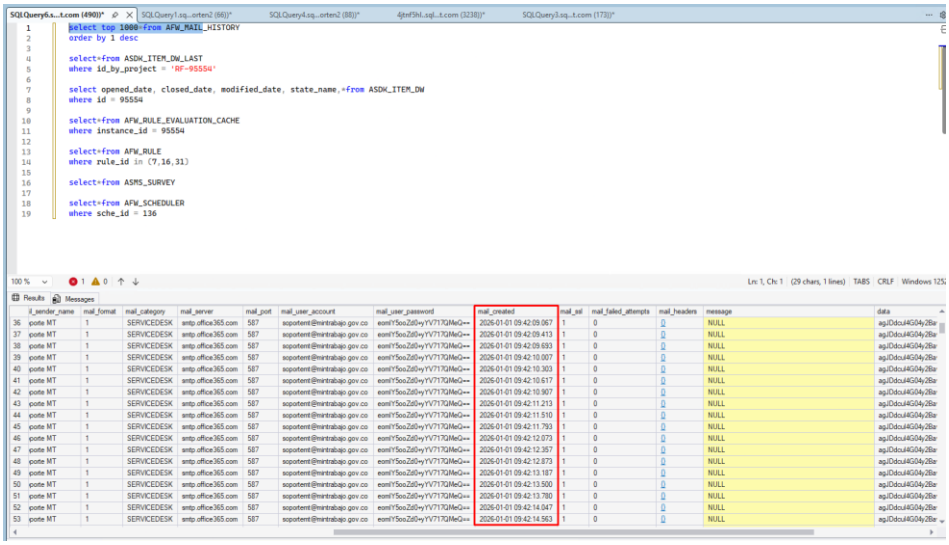


Ilustración 29 Depuración de correos enviados masivamente

- **Herramientas de Gestión:** se tienen 2 casos de Reporte de falla de monitoreo Zabbix.

- **Análisis de Casos Suspendidos por Servicio**

Para el periodo del mes de enero, se dio un aumento de casos suspendidos del 79% que corresponde a 158 casos para un total de este mes de 200 casos de los siguientes servicios:

CASOS SUSPENDIDOS	TOTAL
Soporte Microinformática	108
Administración de servidores	52
Seguridad informática	15
Redes y Conectividad	15
Aplicaciones Especializadas	10
Total general	**200**

Tabla 32 casos suspendidos

- **Soporte Microinformática:** 108 casos suspendidos debido a que se ha solicitado información complementaria a los usuarios o están pendientes por disponibilidad del usuario:, Backup 43 casos Asignación de equipo (portátil o PC) con 14 casos, Devolución de equipo (portátil o PC) con 13 casos, Solicitud Backup con 11 casos, Cambio Toner con 5 casos, Equipo Portátil, Instalación – configuración, Préstamo con 3 casos cada categoría, Asesoría – Consulta, Soporte Aplicaciones Office 365, Equipo Periférico, Equipo Escritorio con 2 casos cada categoría, desinstalación, configuración. Traslado – Movimiento, Cambio de unidad fusara, Daño físico con 1 caso cada categoría.

- **Administración de servidores**: 52 casos suspendidos por: Inactivar usuario con 45 casos, Backup con 4 casos, Habilitar usuario, Cambiar contraseña, Configuración MFA 1 caso para cada categoría.

- **Seguridad informática:** 15 casos suspendidos: Permitir accesos con 4 casos, Validación Habilitación Puertos USB y Análisis de Malware con 2 casos cada categoría, instalación, Seguridad Informática, Análisis de Correos, Ajuste de configuraciones (Crear - Eliminar), Generación de reportes, Accesos por fuerza bruta y Creación de VPN con 1 caso de cada categoría.

- **Redes y Conectividad:** 15 casos suspendidos debido a: Router y FortiGate con 6 casos cada categoría, Degradación, Starlink y Equipo Conectividad internet con 1 caso cada categoría

- **Aplicaciones Especializadas:** 10 casos suspendidos debido a: Asignar Radicado TYS con 5 casos , Relanzamiento 3 casos, Falla Funcional y Depuración Bandeja con 1 caso cada categoría.

- **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 quedo 1 incidente en estado solucionado.

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

Requerimientos solucionados por la Mesa de Servicios: en el mes de enero no quedaron requerimientos en estado solucionado.

Requerimientos solucionados por Soporte en sitio Bogotá: en el mes de enero quedaron 5 requerimientos discriminados de la siguiente manera:

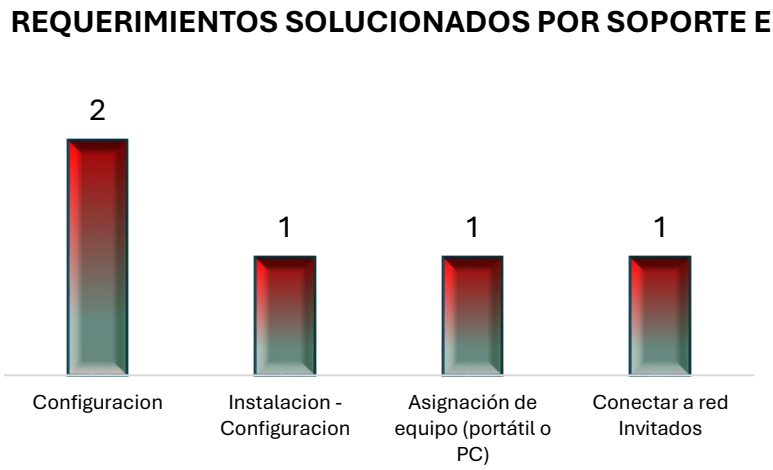


Ilustración 30 Requerimientos Solucionados por Soporte en Sitio

Requerimientos solucionados por Soportes Territoriales: Para el mes de enero quedaron 5 requerimientos discriminados de la siguiente manera:

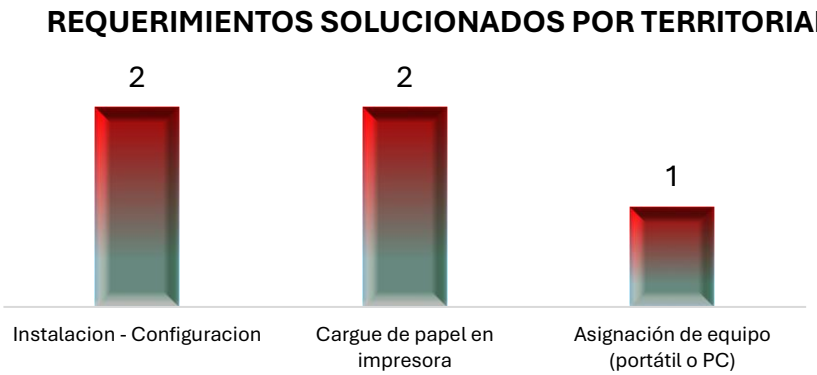


Ilustración 31 Requerimientos Solucionados por Territoriales

- **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 enero se cerraron 1219 casos, discriminados así: Asesoría – Consulta con 310 casos, Cambiar contraseña con 202 casos, Aumento de cuota con 159 casos, Habilitar usuario 155 casos, Creación de usuario 85 casos, Backup 49 casos, Inactivar usuario 47 casos, Cambio de grupo con 35 casos, Eliminar Hostname con 32 casos y Instalación-Desinstalación con 26 casos.

En comparación del mes anterior se nota un aumento de casos cerrados por la mesa de un 19% que es equivalente a 194 casos.

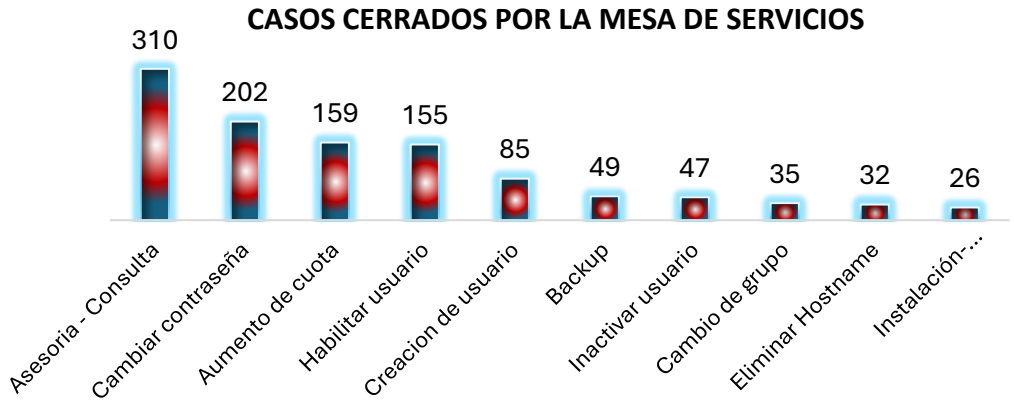


Ilustración 32 Requerimientos Solucionados por la Mesa de Servicios

Casos Cerrados por Soporte en Sitio: Se indica el top 10 de Requerimientos cerrados por soporte en sitio, para el mes de enero se cerraron 1265 casos discriminados así: Cargue de papel en impresora con 377 casos, Instalación - Configuración con 142 casos, Asesoría - Consulta con 135 casos, Configuración con 120 casos, Solicitud Backup con 56 casos, Actualización BIOS 42 casos, Devolución de equipo (portátil o PC) 40 casos, Soporte Aplicaciones Office 365 39 casos, Asignación de equipo (portátil o PC) 34 casos y Borrado seguro Portátil 30 casos.

En comparación con el mes anterior se tiene una disminución del 6% que corresponde a 78 casos.

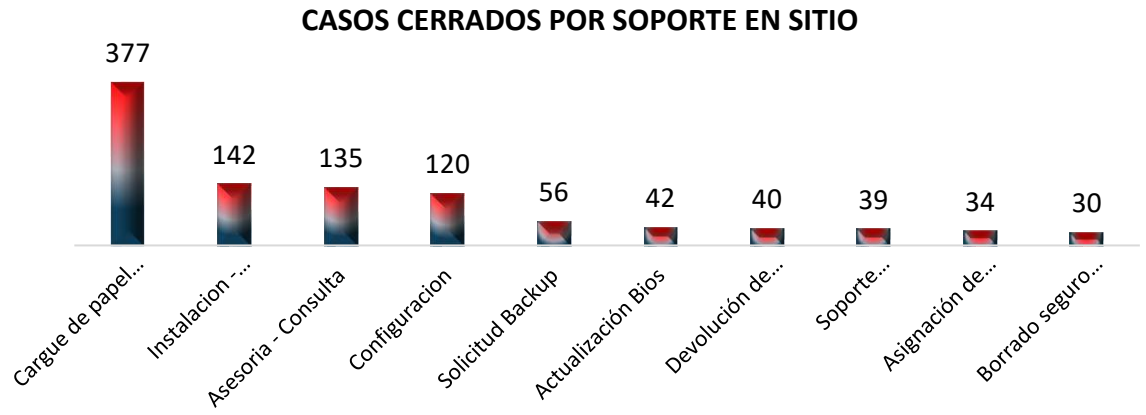


Ilustración 33 Casos Cerrados por Soporte en Sitio

Casos Cerrados por soporte en sitio Territoriales: Se indica el top 10 de Requerimientos cerrados por soporte en Territorio, para el mes de enero se cerraron 1541 casos discriminados así: Asesoría – Consulta con 272 casos, Cargue de papel en impresora con 192 casos, instalación – Configuración con 188 casos, Configuración con 137 casos, Mantenimiento preventivo con 87 casos, Asesoría Excel con 74 casos, Actualización BIOS con 73 casos, Soporte Aplicaciones Office 365 con 49 casos, Asesoría PDF 43 casos, Asesoría Word con 40 casos.

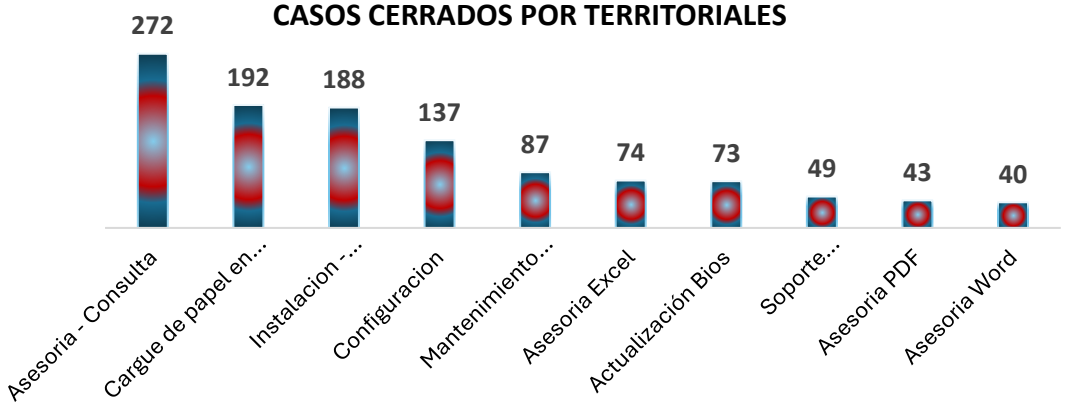


Ilustración 34 Casos Cerrados por Territoriales

- **Casos Atendidos a Usuarios VIPS**

Durante este periodo se crearon 86 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
Incidente	4	0	4
Requerimiento	81	1	82
Total general	**85**	**1**	**86**

Tabla 33 Casos Atendidos usuarios VIPs

Se atendieron 1299 solicitudes para el resto de los usuarios discriminados así:

TIPO DE CASO-NO-VIPS	CUMPLIMIENTO	NO_CUMPLE	TOTAL
Incidentes	39	0	39
Requerimientos	1190	0	1190
Total general	**1299**	**0**	**1299**

Tabla 34 Casos Atendidos usuarios

- **Medio de Ingreso de Casos**

Durante el período ingresaron a la mesa de servicio 6104 casos a través de los diferentes medios que se tiene habilitados para la atención de solicitudes, como son correo, extensión telefónica, portal de autogestión, alarma de Zabbix, casos creados de forma automática por las diferentes herramientas:

MEDIO DE INGRESO DE CASOS	TOTAL
Gestión Técnica	2745
Correo SoporteMT	1981
Alarma Zabbix	991
Telefónico	347
Alarma Fortisiem	35
Portal Auto-Gestión	4
Case Creator Mesa de Servicios	1
Total general	**6104**

Tabla 35 Medios de Ingreso de Casos

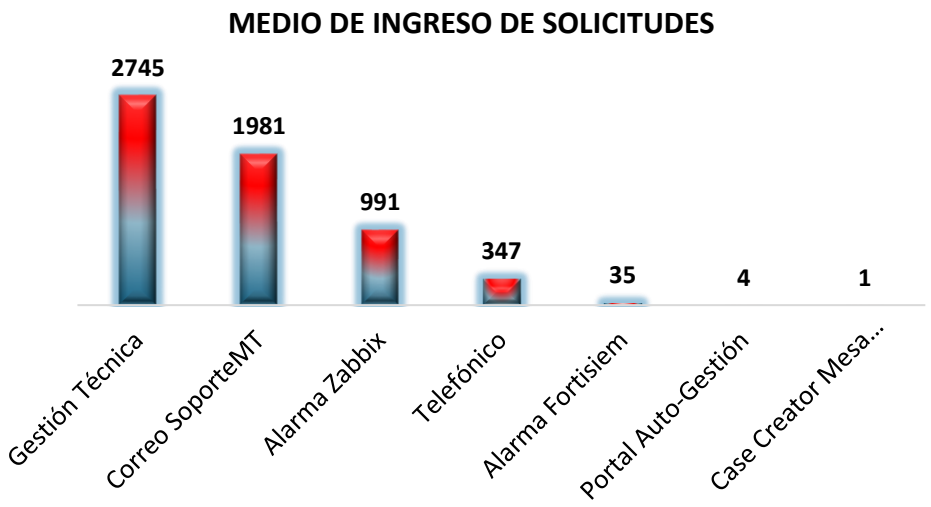


Ilustración 35 Medio de ingreso solicitudes

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 realiza mantenimiento y depuración de la información de las carpetas compartidas de Mintra60 y Mintra19 que contienen export de los funcionarios.

Se realiza modificación de jornada y adaptación del personal de soporte en sitio al área de Contratación, con jornadas de soporte adicionales hasta las 10:00 p.m. Desde el 16 de enero hasta el 30 de enero.

- Novedades de la operación – Soporte en sitio Territoriales

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

18 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 el mantenimiento de impresoras

Intervención en 1564 casos, dentro de los que se destacan: Asesoría-Consulta sobre el software instalado, Cargues de Papel en las impresoras de las diferentes Sedes, Instalación-Configuración, Configuración de hardware, Mantenimiento de Impresoras, Asesoría Excel, Actualización de BIOS, Soporte en aplicaciones Office Asesorías en PDF y Asesoría Word.

Traslado de antenas starlink requeridas por los especialistas de redes y conectividad

Traslado de equipos de cómputo, impresoras, racks e instalación de los mismos en las nuevas instalaciones de 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
Ene-26	Santander	Puerto Wilches	Revisión y mantenimiento completo de la impresora	Se realiza el mantenimiento de la impresora RICOH así como la validación de la actualización de su software y la interfaz	RF-180335 RF-180336
Ene-26	Meta	Granada	Revisión y mantenimiento completo de la impresora	Se realiza el mantenimiento de la impresora RICOH así como la validación de la actualización de su software y la interfaz	RF-179307 RF-179408 RF-179411 RF-179415
Ene-26	Meta	Acacias	Revisión y mantenimiento completo de la impresora	Se realiza el mantenimiento de la impresora RICOH así como la validación de la actualización de su software y la interfaz	RF-179752 RF-179751 RF-179728 RF-179726 RF-179724
Ene-26	Guajira	Barrancas	Revisión y mantenimiento completo de la impresora	Se realiza el mantenimiento de la impresora RICOH así como la validación de la actualización de su software y la interfaz	RF-180676
Ene-26	Atlántico	Campo de la Cruz	Revisión y mantenimiento completo de la impresora	Se realiza el mantenimiento de la impresora RICOH así como la validación de la actualización de su software y la interfaz	RF-179991 RF-179992 RF-179993
Ene-26	Huila	Garzón	Devolución de equipo de cómputo	Se realiza alistamiento de PC en su respectiva caja original para retorno, una vez se realizó el borrado seguro se reinstalo el sistema operativo	RF-177585
Ene-26	Valle	Buenaventura	Revisión y mantenimiento completo de la impresora	Se realiza mantenimiento preventivo de impresora RICOH Se adjunta acta de mantenimiento y registro fotográfico del antes y después del mantenimiento.	RF-180173 RF-180170
Ene-26	Santander	San Vicente de Chucurí	Actualización de BIOS	Se intervino el equipo escritorio y se realizó la respectiva actualización de la BIOS a la versión M46KT58A con el fin de corregir errores, mejorar la compatibilidad con hardware y optimizar el rendimiento del equipo.	RF-180803
Ene-26	Santander	Sabana de Torres	Actualización de BIOS	Se intervino el equipo escritorio y se realizó la respectiva actualización de la BIOS a la versión MJ0LS5CF con el fin de corregir errores, mejorar la compatibilidad con hardware y optimizar el rendimiento del equipo.	RF-180973 RF-180975 RF-180980
Ene-26	Cesar	Codazzi	Revisión y mantenimiento completo de la impresora	Se realiza mantenimiento preventivo de impresora RICOH-AGUSTINCIDAZZI Se adjunta acta de mantenimiento y registro fotográfico del antes y después del mantenimiento.	RF-181162
Ene-26	OE Buenaventura	Buenaventura	Solicitud de traslado de equipos por cambio de sede	Se efectuó el traslado de los equipos de escritorio con las medidas de protección necesarias, garantizando que cada equipo llegara en condiciones óptimas a la nueva sede. Posteriormente se validó la integridad de los equipos y periféricos, confirmando que el	RF-181370

				procedimiento se realizó con éxito y que la solicitud quedó atendida	
Ene-26	Cesar	Bosconia	Revisión y mantenimiento completo de la impresora	Se realiza mantenimiento preventivo de impresora RICOH-BOSCONIA Se adjunta acta de mantenimiento y registro fotográfico del antes y después del mantenimiento.	RF-181819
Ene-26	Caldas	Anserma	Visita para Inspección Técnica	Se procede a revisar cada equipo de cómputo de cada funcionario, los procesos de imprimir, escanear y copiar en la impresora, el funcionamiento del internet y correcta navegación	RF-182393
Ene-26	Cesar	La Jagua de Ibirico	Revisión y mantenimiento completo de la impresora	Se realiza mantenimiento preventivo de impresora RICOH-JAGUA-IBIRICO-INSP Se adjunta acta de mantenimiento y registro fotográfico del antes y después del mantenimiento	RF-181620
Ene-26	Meta	Puerto Gaitán	Funcionaria requiere soporte en sitio debido que manifiesta que el internet le está presentando mucha intermitencia al abrir las páginas corporativas	Se realizo visita técnica a la inspección para validar la falla que manifiesta la funcionaria con el servicio de internet de los cuales se realizan las validación del servicio, se evidencia que el internet en donde está ubicada la funcionaria está operativo. Se adjuntan pantallazos y se genera informe sobre la visita a sede central	RF-178633
Ene-26	OE Buenaventura	Buenaventura	Revisión de cableado	Se realiza el ponchado de los cables de red con los RJ45, luego de esto se comprueba el correcto funcionamiento de los puntos, del Intranet y la correcta navegación.	RF-182308
Ene-26	Cordoba	Cereté	Actualización de BIOS de la versión M46KT4DA a la M46KT57A para Desktop	Se intervino el equipo escritorio y se realizó la respectiva actualización de la BIOS a la versión más reciente del equipo MOTEROR con el fin de corregir errores, mejorar la compatibilidad con hardware y optimizar el rendimiento del equipo.	RF-180182
Ene-26	Cordoba	Sahagún	Actualización de BIOS de la versión M46KT4DA a la M46KT57A para Desktop	Se intervino el equipo escritorio y se realizó la respectiva actualización de la BIOS a la versión más reciente del equipo MFVEGA con el fin de corregir errores, mejorar la compatibilidad con hardware y optimizar el rendimiento del equipo.	RF-181321

Tabla 36 Visitas a sedes sin Soporte asignado

- 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	99,21%	90,00%
	Tiempo de solución de requerimientos por soporte en sitio	99,70%	90,00%
	Tiempo de respuesta de la mesa de servicio	99,72%	85,00%
	Abandono de llamadas	0,00%	Máximo 8,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 37 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

Durante el mes de enero de 2026 desde la línea de servicios centrales se atendieron las siguientes sesiones o reuniones:

Se realizó la gestión efectiva del Directorio Activo, implementando las siguientes actividades:

Día	Hora	Asunto de la Sesión	Agendada por	Ubicación	Objetivo
6/01/2026	11:00 a. m.	Seguimiento Vulnerabilidades Interno	Servicios Centrales	Microsoft Teams	Seguimiento Interno del Equipo de Servicios Centrales, para revisión de avances en cuestión de mitigación de vulnerabilidades y planes anuales de gestión de Seguridad Informática.
7/01/2026	9:00 a. m.	MINTRABAJO | Validación SISINFO	Servicios Centrales	Microsoft Teams	Revisión con el equipo de desarrollo de IVC y Aplicaciones Especializadas - DDBB para revisar tópicos relacionados con la migración de DDBB de SISINFO.
8/01/2026	11:00 a. m.	Contextualización del proyecto Migración Aplicativos para asignación Recursos y Permisos	Oficina TIC	Microsoft Teams	Contextualización del proyecto de migración de Aplicaciones RUE, RUTEC y CEN hacía Azure, prerrequisitos y demás.
8/01/2026	3:00 p. m.	Transferencia de Conocimiento Vulnerabilidades y Seguridad MinTrabajo	Servicios Centrales	Microsoft Teams	Sesión de seguimiento y socialización de resultados a la Oficina TIC y Soporte informático de las actividades realizadas relacionados con Seguridad informática.
9/01/2026	2:00 p. m.	Revisión técnica-DA-Ministerio Trabajo	Oficina TIC	Microsoft Teams	Sesión para validación de privilegios en el Tenant de

					Office 365 para el proveedor Caro, revisión de proyecto Power Apps/Automate.
13/01/2026	11:00 a. m.	Seguimiento Vulnerabilidades Interno	Servicios Centrales	Microsoft Teams	Seguimiento Interno del Equipo de Servicios Centrales, para revisión de avances en cuestión de mitigación de vulnerabilidades y planes anuales de gestión de Seguridad informática.
14/01/2026	10:00 a. m.	MINTRABAJO | Validación Migración OS Apps .NET	Servicios Centrales	Microsoft Teams	Seguimiento y planteamiento de migración de aplicaciones - Independización de DNS por App.
15/01/2026	10:00 a. m.	Socialización Resultado Auditoria de Calidad de Casos Mensual	Servicios en Sede	Microsoft Teams	Socialización interna de gestión de casos del proyecto.
15/01/2026	11:00 a. m.	Validación CI en la CMDB Servicios Centrales	Servicios en Sede	Microsoft Teams	Revisión de CI asociados a los servicios de la Línea de servicios centrales - ARANDA
15/01/2026	3:00 p. m.	Transferencia de Conocimiento Vulnerabilidades y Seguridad MinTrabajo	Servicios Centrales	Microsoft Teams	Sesión de seguimiento y socialización de resultados a la Oficina TIC y Soporte informático de las actividades realizadas relacionados con Seguridad informática.
16/01/2026	11:00 a. m.	Continuación Migración Azure 3 APPs (PaaS)	Oficina TIC	Microsoft Teams	Validación prerrequisitos migración PaaS CEN, RUE, RUTEC.
19/01/2026	10:00 a. m.	Seguimiento PM 174025	Servicios Centrales	Microsoft Teams	Seguimiento a problema en servidor FileNet Freeze de servicios de Windows.
20/01/2026	11:00 a. m.	Seguimiento Vulnerabilidades Interno	Servicios Centrales	Microsoft Teams	Seguimiento Interno del Equipo de Servicios Centrales, para revisión de avances en cuestión de mitigación de vulnerabilidades y planes anuales de gestión de Seguridad informática.
20/01/2026	2:00 p. m.	MINTRABAJO | Nube Privada	Servicios Centrales	Microsoft Teams	Seguimiento interno a las actividades relacionadas con el servicio de Nube Privada.
22/01/2026	2:00 p. m.	MINTRABAJO | Validación Suscripción Dirección Empleo	Oficina TIC	Microsoft Teams	Revisión de inconvenientes presentados en la Suscripción de la Dirección de Empleo en Azure con el equipo de trabajo del BID.
22/01/2026	3:00 p. m.	Transferencia de Conocimiento Vulnerabilidades y Seguridad MinTrabajo	Servicios Centrales	Microsoft Teams	Sesión de seguimiento y socialización de resultados a la Oficina TIC y Soporte informático de las actividades realizadas relacionados con Seguridad informática.
23/01/2026	9:00 a. m.	MINTRABAJO | Validación Equipo IBM	Servicios Centrales	Microsoft Teams	Alineación interna para atención de requerimientos de servicio e incidentes para el servicio de Gestor Documental.
23/01/2026	10:00 a. m.	Plan de Capacitación IBM	Servicios Centrales	Microsoft Teams	Sesión para empalmar y capacitar al equipo de trabajo interno en la gestión de casos de Gestor documental.
23/01/2026	2:00 p. m.	Plan de Disponibilidad 2026	Servicios en Sede	Microsoft Teams	Sesión para determinar las pruebas de alta disponibilidad

					para la vigencia 2026 de la línea de servicios centrales.
26/01/2026	9:00 a. m.	Plan de acción Página Web 2026	Oficina TIC	Microsoft Teams	Sesión para validar los objetivos a cumplir para la vigencia 2026 en lo que respecta el portal web de la entidad.
26/01/2026	2:00 p. m.	MINTRABAJO | Validación Línea Base .NET	Servicios Centrales	Microsoft Teams	Validación de la documentación base de la línea de aplicaciones especializadas .NET
26/01/2026	3:00 p. m.	Revisión de actividades para base de datos productiva del Portal web	Servicios Centrales	Microsoft Teams	Revisión interna para determinar dependencias y actividades relacionadas con la migración de versión de LifeRay y parchado de DDBB Oracle del portal web.
27/01/2026	11:00 a. m.	Seguimiento Vulnerabilidades Interno	Servicios Centrales	Microsoft Teams	Seguimiento Interno del Equipo de Servicios Centrales, para revisión de avances en cuestión de mitigación de vulnerabilidades y planes anuales de gestión de Seguridad informática.
27/01/2026	2:00 p. m.	Seguimiento Servicios Centrales	Servicios Centrales	Presencial	Validación de ruta crítica para vigencia 2026 del equipo de trabajo de Servicios centrales de manera transversal a la ejecución del contrato.
27/01/2026	3:00 p. m.	Transferencia de Conocimiento GD IBM	Servicios Centrales	Microsoft Teams	Sesión para empalmar y capacitar al equipo de trabajo interno en la gestión de casos de Gestor documental.
29/01/2026	10:00 a. m.	MINTRABAJO | Transferencia de Conocimiento Pagina Web - LifeRay	Oficina TIC	Microsoft Teams	Socialización con Oficina TIC del funcionamiento del portal web con el nuevo equipo de contratistas.
29/01/2026	2:00 p. m.	Revisión Ambiente Gestor Documental MINTRABAJO	Servicios Centrales	Microsoft Teams	Revisión de funcionamiento de Ambientes de Gestor documental, Arquitectura e interoperabilidad.
29/01/2026	3:00 p. m.	Transferencia de Conocimiento Vulnerabilidades y Seguridad MinTrabajo	Servicios Centrales	Microsoft Teams	Sesión de seguimiento y socialización de resultados a la Oficina TIC y Soporte informático de las actividades realizadas relacionados con Seguridad informática.
30/01/2026	4:00 p. m.	MINTRABAJO | Transferencia de conocimiento DDBB Oracle	Servicios Centrales	Microsoft Teams	Revisión de arquitectura y documentación de la solución de DDBB Oracle.

Tabla 38 Sesiones Servicios Centrales

De acuerdo con lo anterior, la Línea de Servicios centrales realizó atención de un total de 549 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.

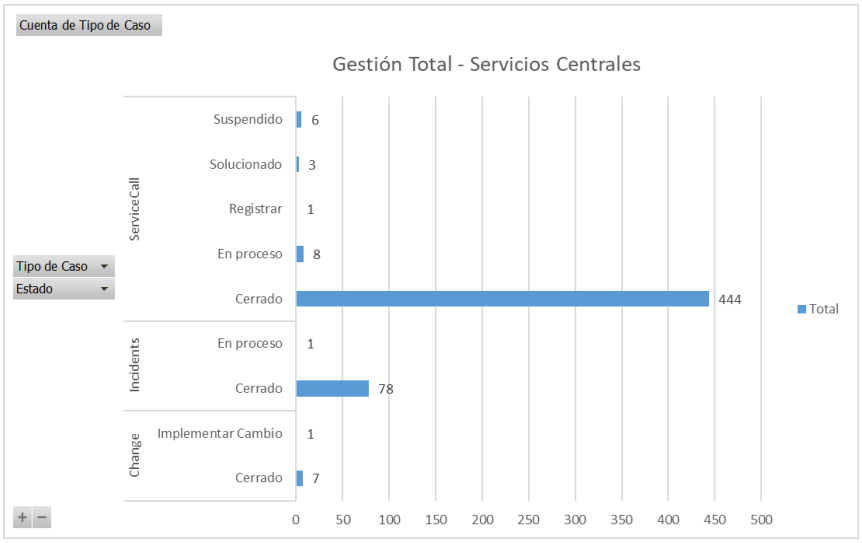


Ilustración 36 Gestión Casos - SC

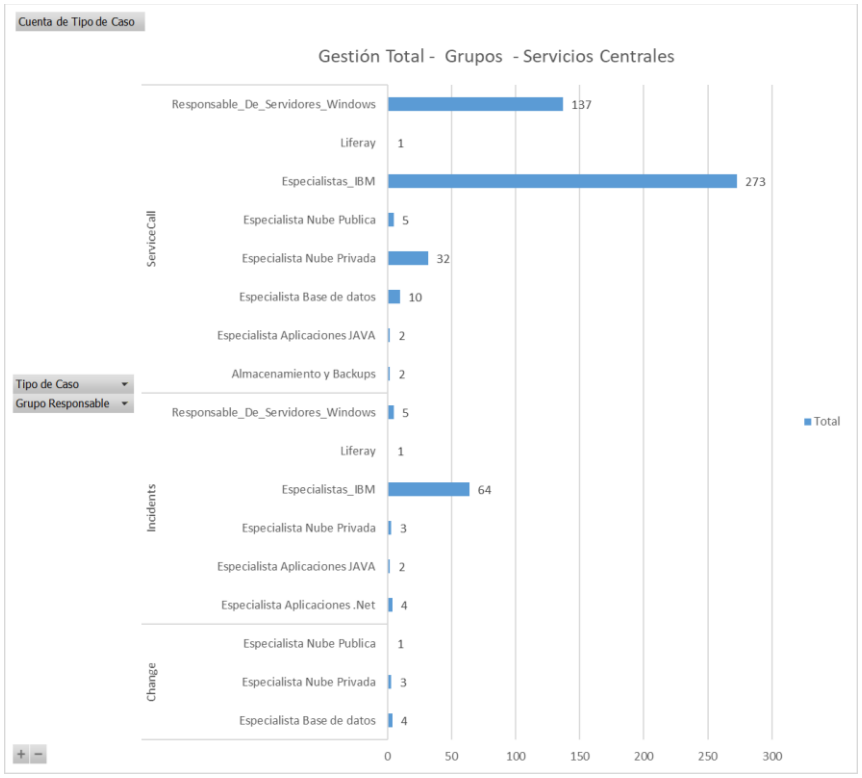


Ilustración 37 Gestión SC - Por Grupo

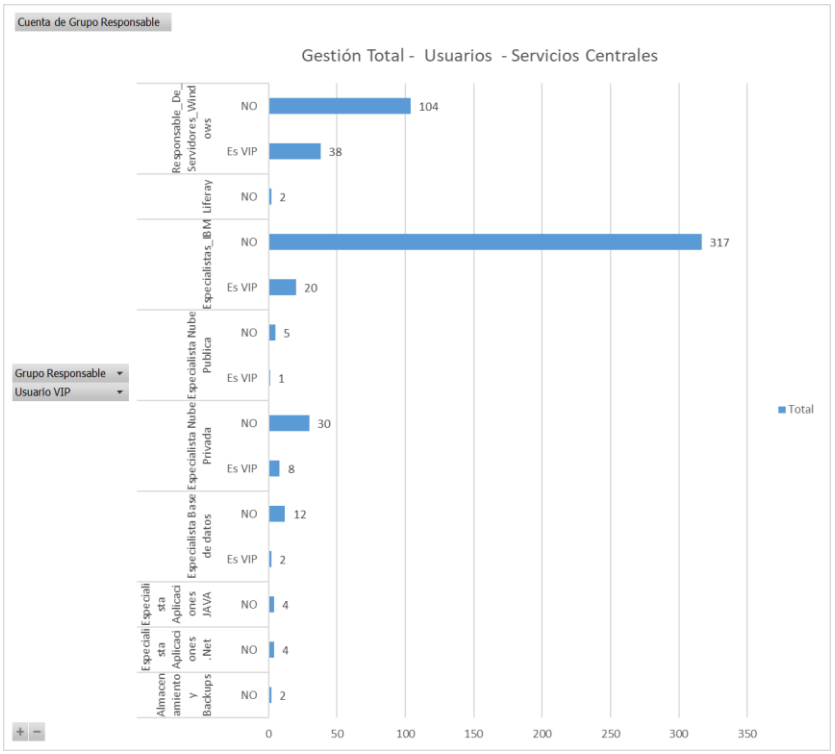


Ilustración 38 Gestión Sc - Por Tipo De Usuario

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.

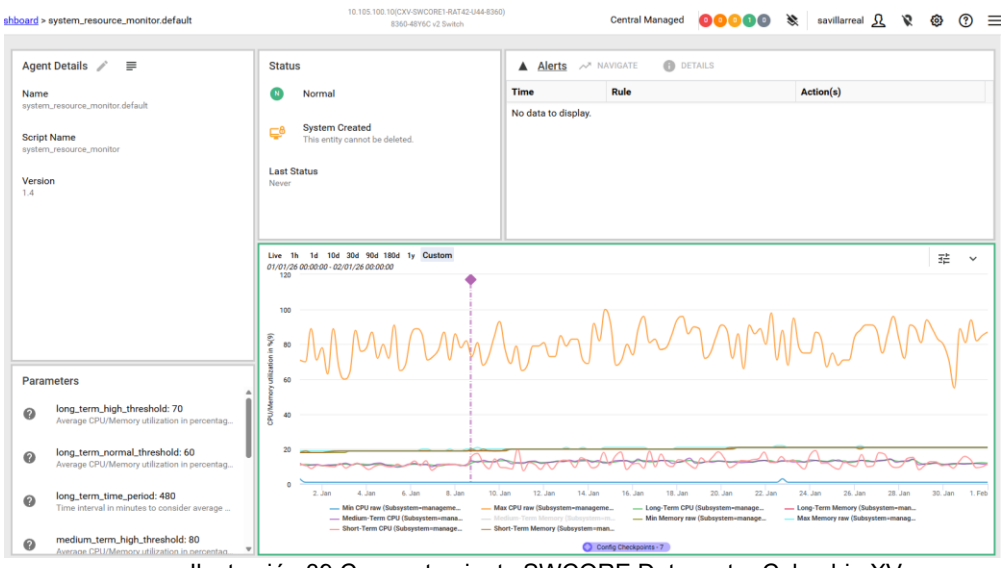


Ilustración 39 Comportamiento SWCORE Datacenter Colombia XV

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

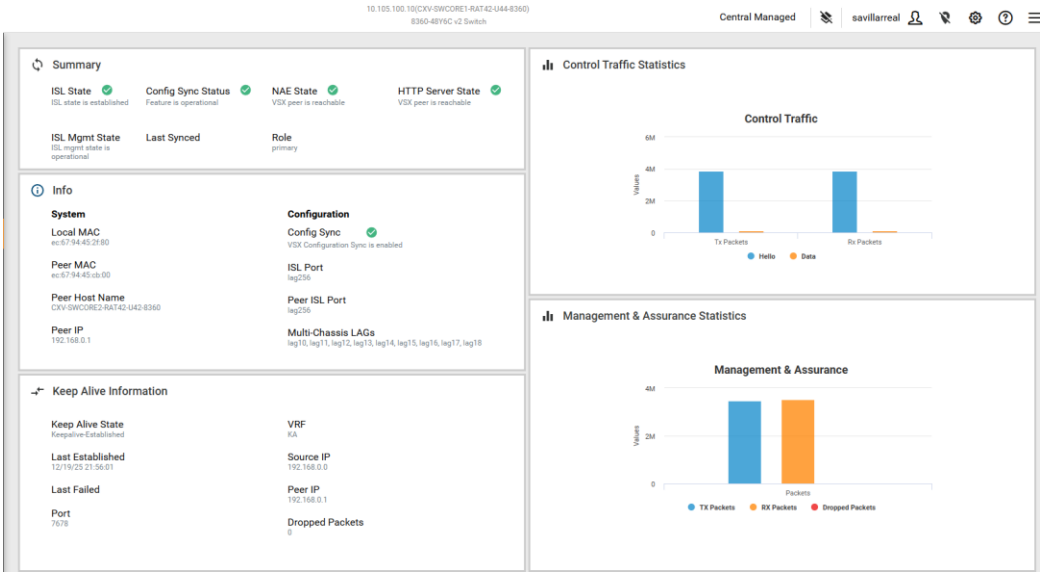


Ilustración 40 Sincronización HA de los Switch Core

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 pico de 1G de consumo sin afectar el rendimiento del canal, se observa un flujo estable de tráfico. El tráfico se ha mantenido con el mismo comportamiento de consumo de los últimos meses.

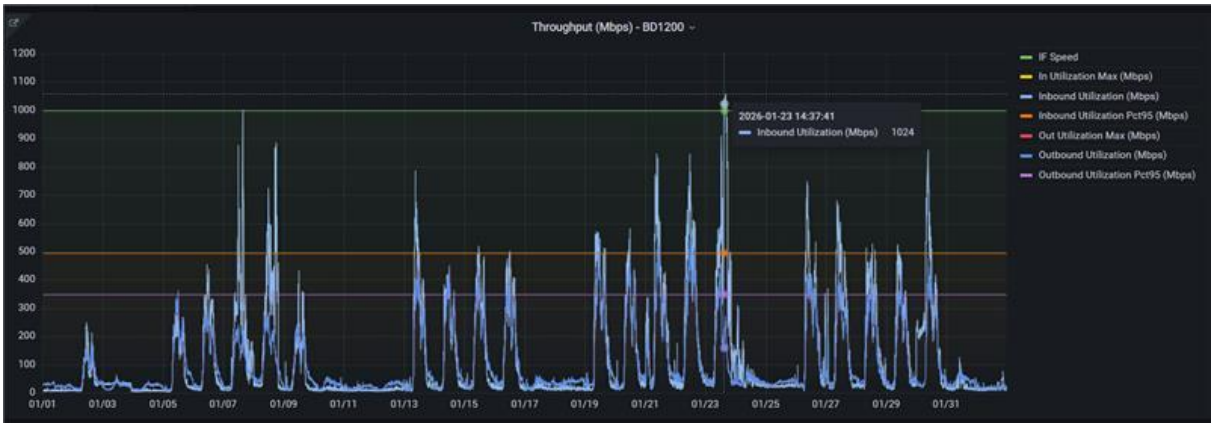


Ilustración 41 Grafica de consumo canal Internet Datacenter

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:

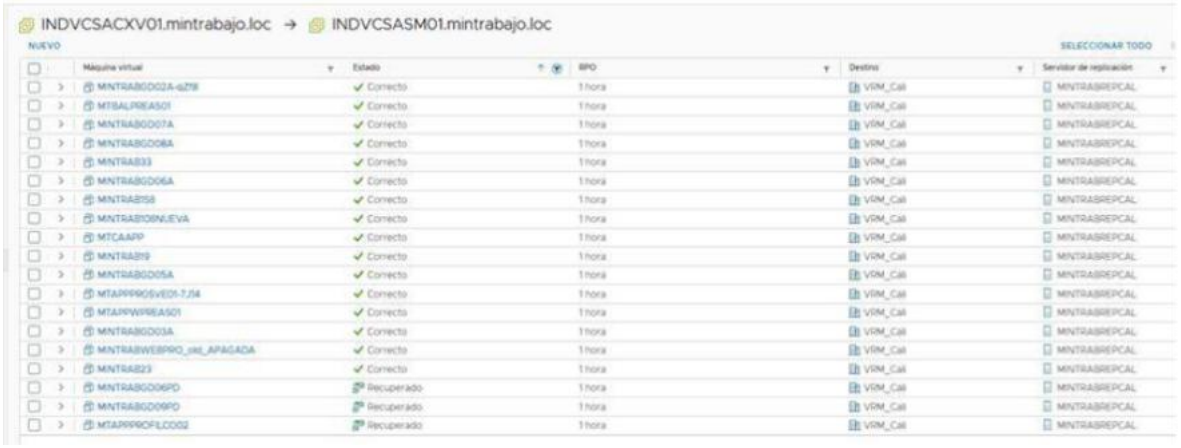


Ilustración 42 máquinas virtuales DRP

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 realizará para las siguientes bases de datos:

No.	Base de Datos	Aplicación
1	MT_EVENTOS	Observatorio Laboral
2	ARCHSINDICAL	Archivo Sindical

3	Bancos	Tesorería
4	CalculadoraLaboral	Calculadora Laboral
5	ESTADOJOVEN	Estado Joven
6	Infraestructura	Cobro Coactivo
7	MTRCobroCoactivo	Cobro Coactivo
8	Siriti2018	Siriti

- 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.

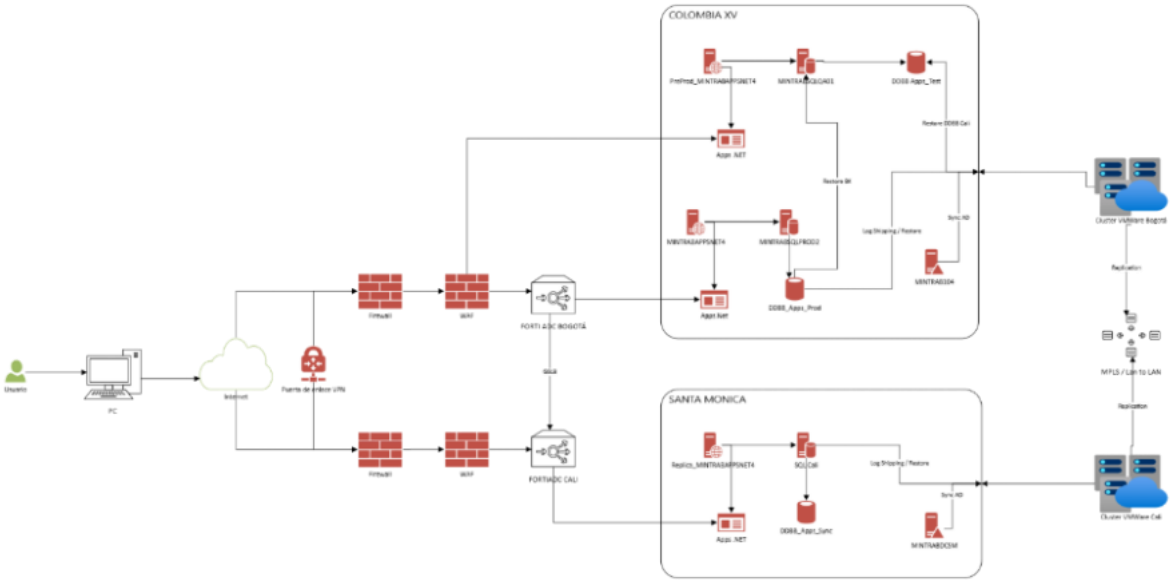


Ilustración 43 Escenario pruebas Apps DRP

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 bajo tráfico durante el mes. Se observa que se tuvo un pico máximo de 160 Mbps.

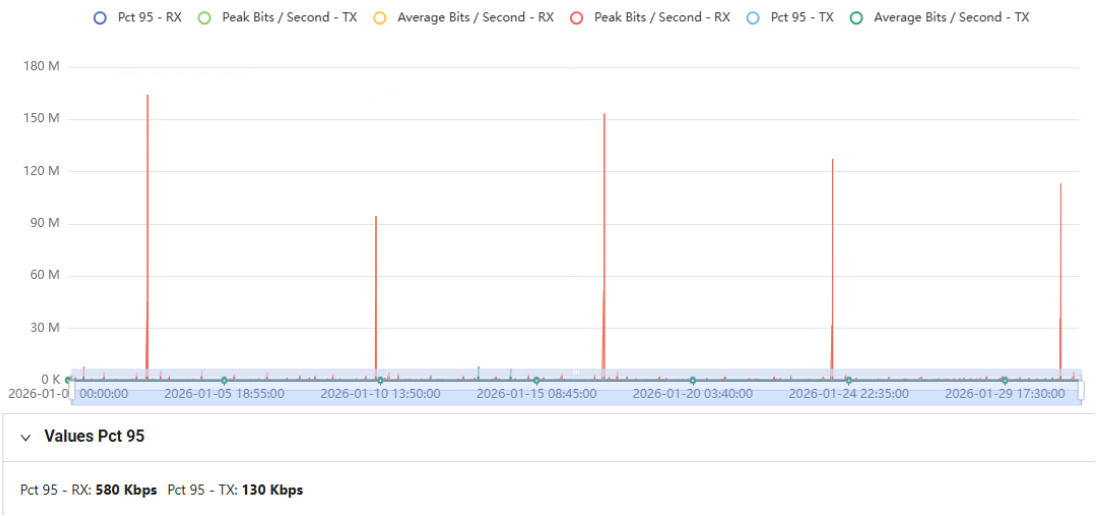


Ilustración 44 Extremo DC Bogotá

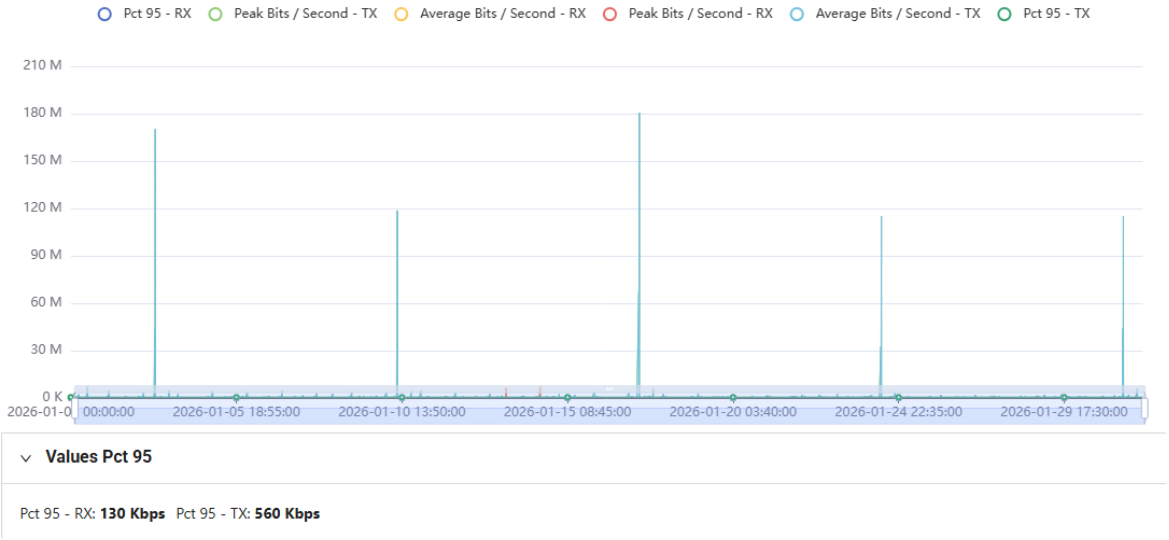


Ilustración 45 Extremo DC Cali

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 pico máximo de 12Mbps.

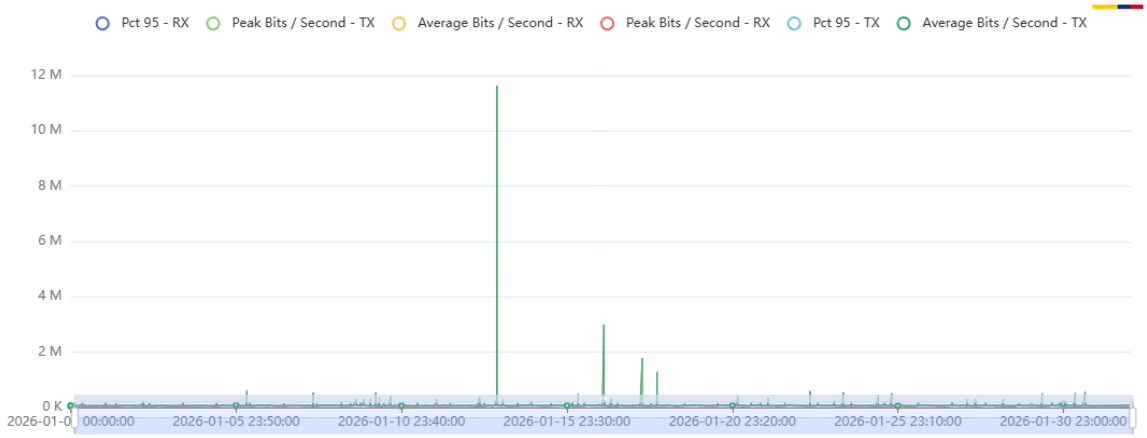


Ilustración 46 Estado canal de Internet DC Cali

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



Ilustración 47 Estado SWCORE Datacenter alterno

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

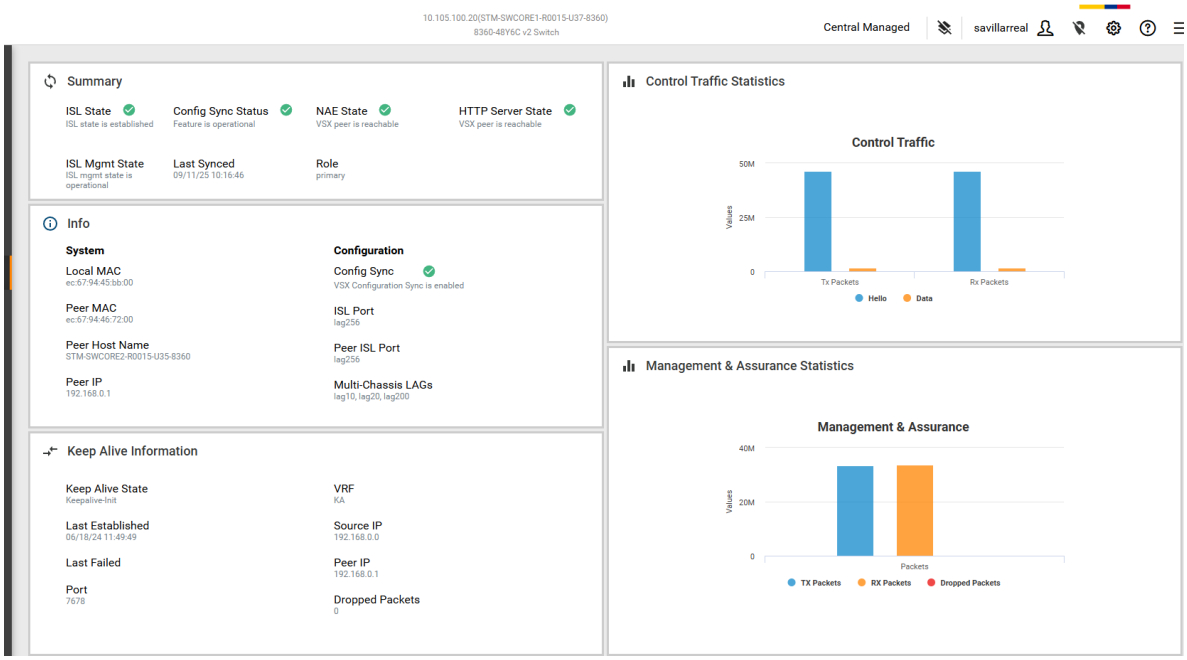


Ilustración 48 Estado HA SWCORE Datacenter alterno

Se verifica el canal MPLS de datacenter alterno, el cual se observa que se ha mantenido activo durante el mes de enero, 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 entrada de 43.7 Kbps y de salida de 54.7 Kbps.

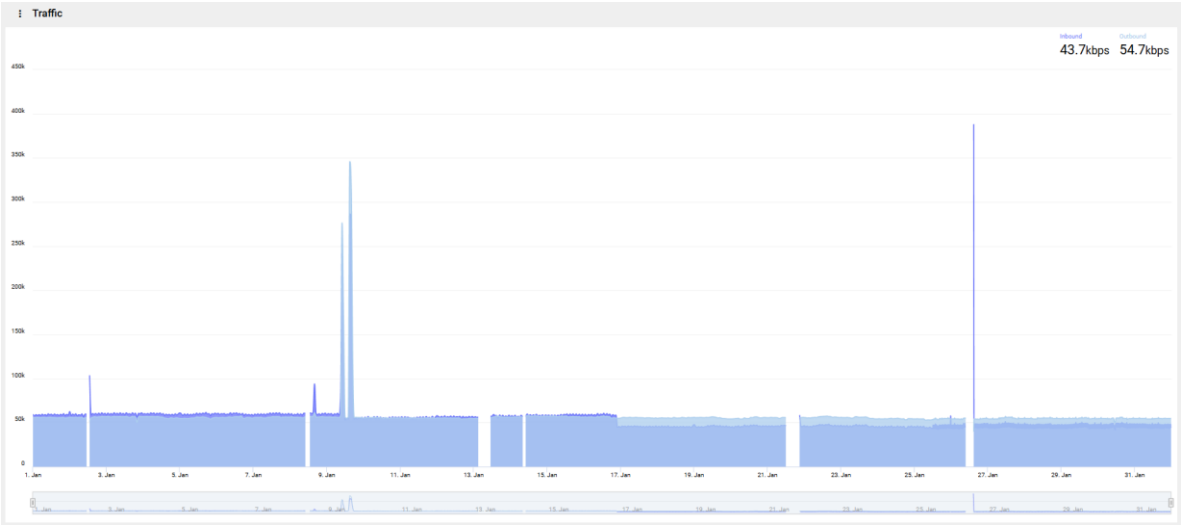


Ilustración 49 Consumo canal MPLS DC Alterno

Se verifica estado del equipo, donde se observa que presenta un uptime de 43 semanas con 4 días, con un promedio de utilización de memoria de 40.7% y de procesamiento de 1.33%, lo que nos indica que el equipo no presenta uso alto en procesamiento y memoria.

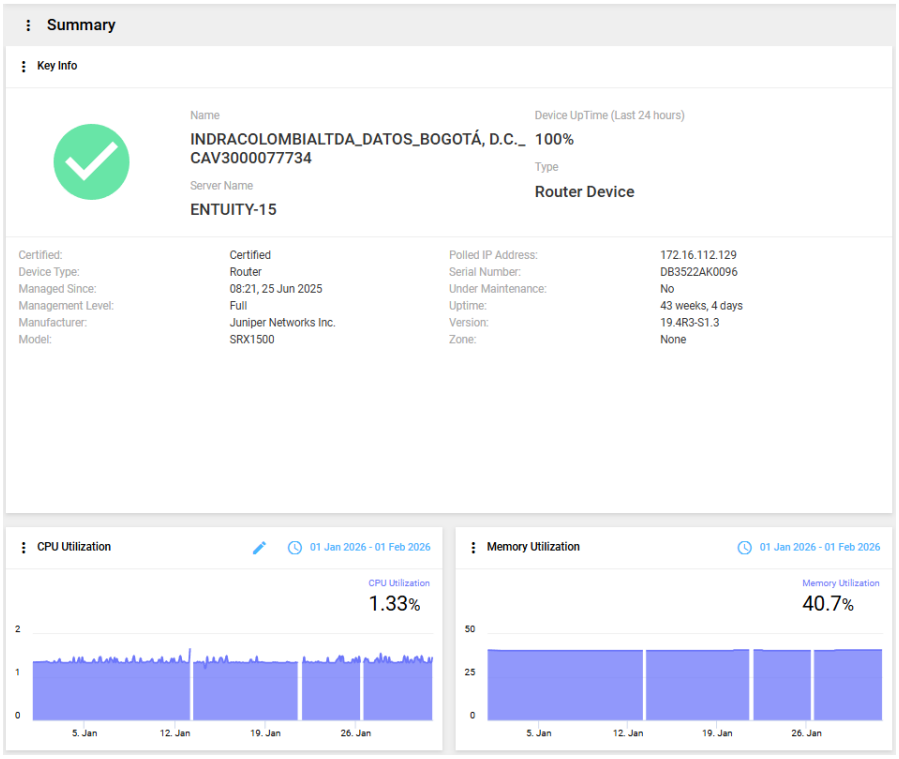


Ilustración 50 Estado Router MPLS DC Alterno

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 142 requerimientos asociados a esta categoría del servicio de Windows, así como la creación, modificación de usuarios que reduce su reporte a 19 casos para el mes de enero. De la mano de asignación de licencias se atendieron 61 requerimientos, obteniendo un incremento considerable con respecto a los meses anteriores, con respecto a los casos asociados a configuración de MFA se observa un ligero crecimiento a 18 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.

Durante el mes de enero 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.

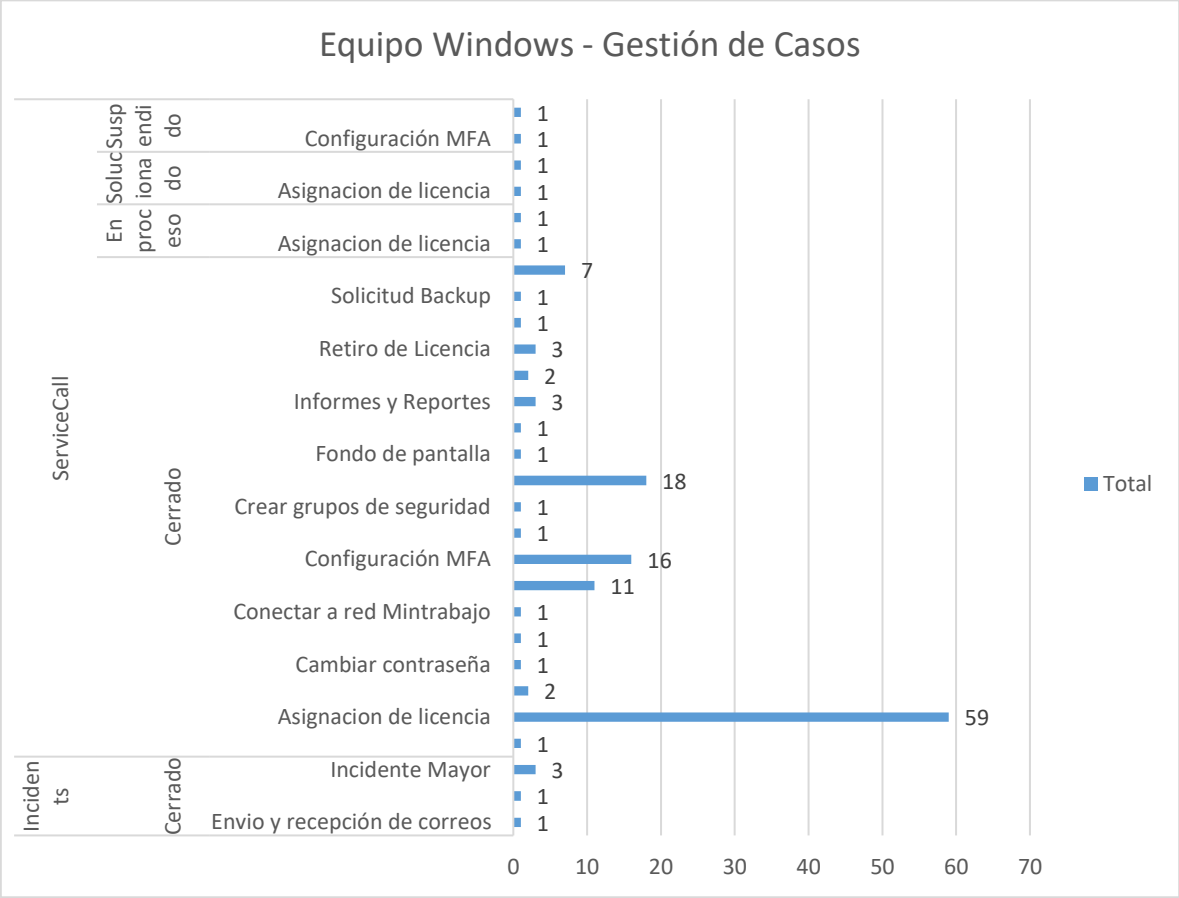


Ilustración 51 Gestión de Casos Windows

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.

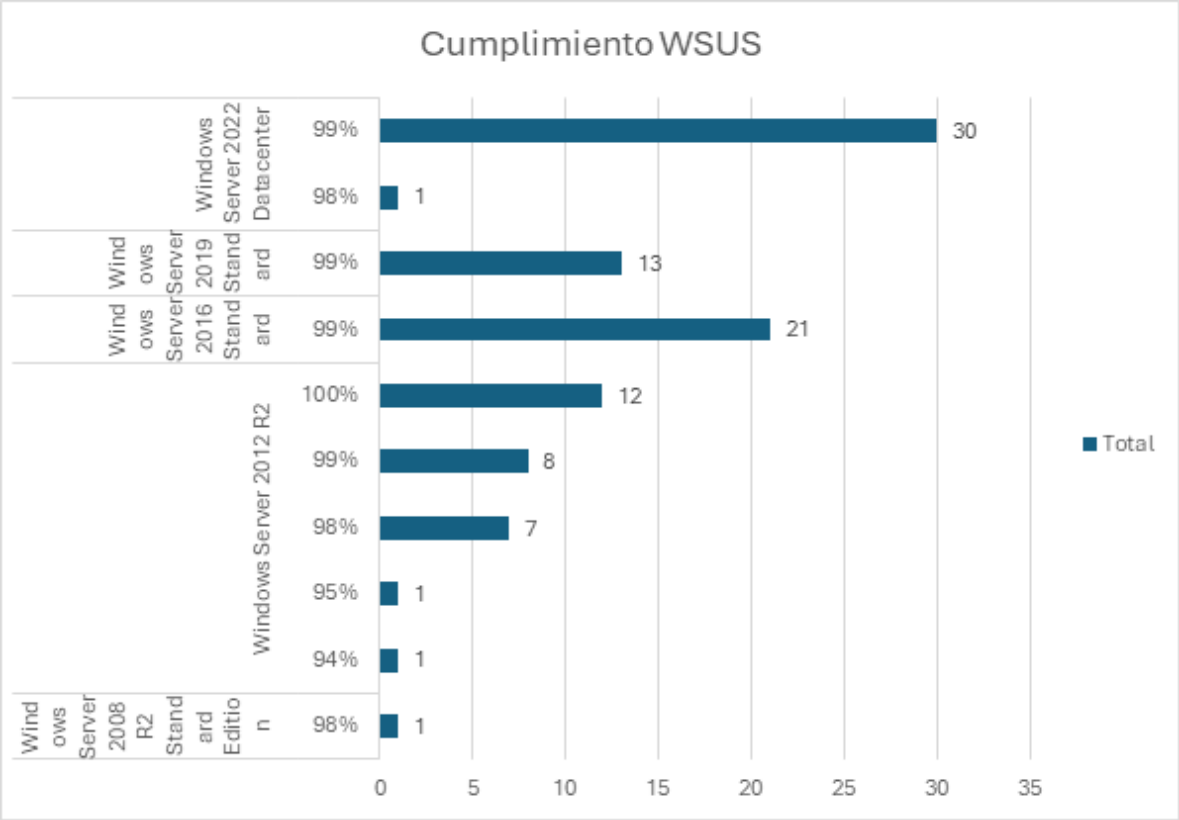


Ilustración 52 Cumplimiento WSUS

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 las 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.

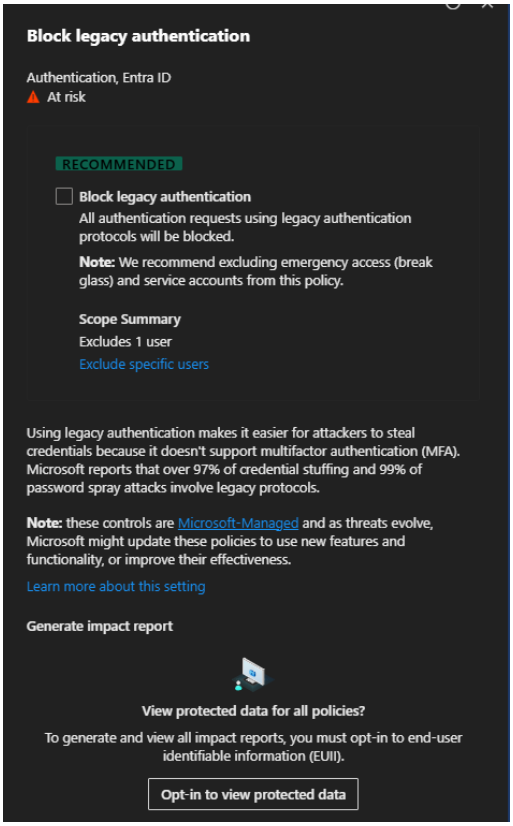


Ilustración 53 Block Legacy Authentication

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

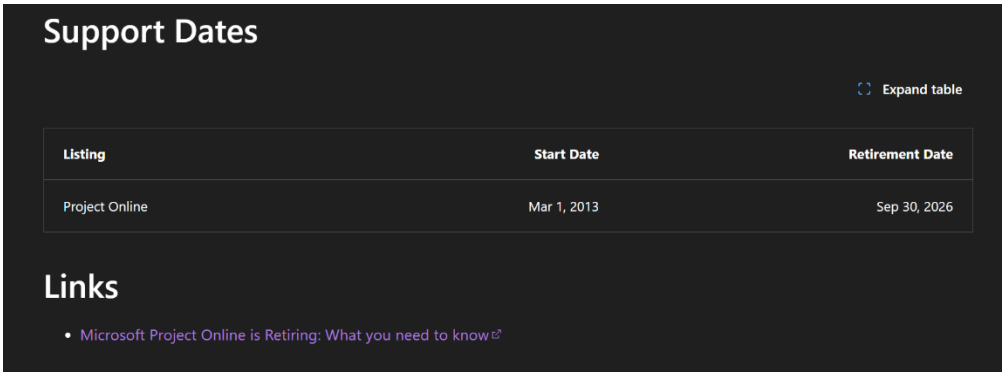


Ilustración 54 Fechas de Soporte

Licencias asignadas

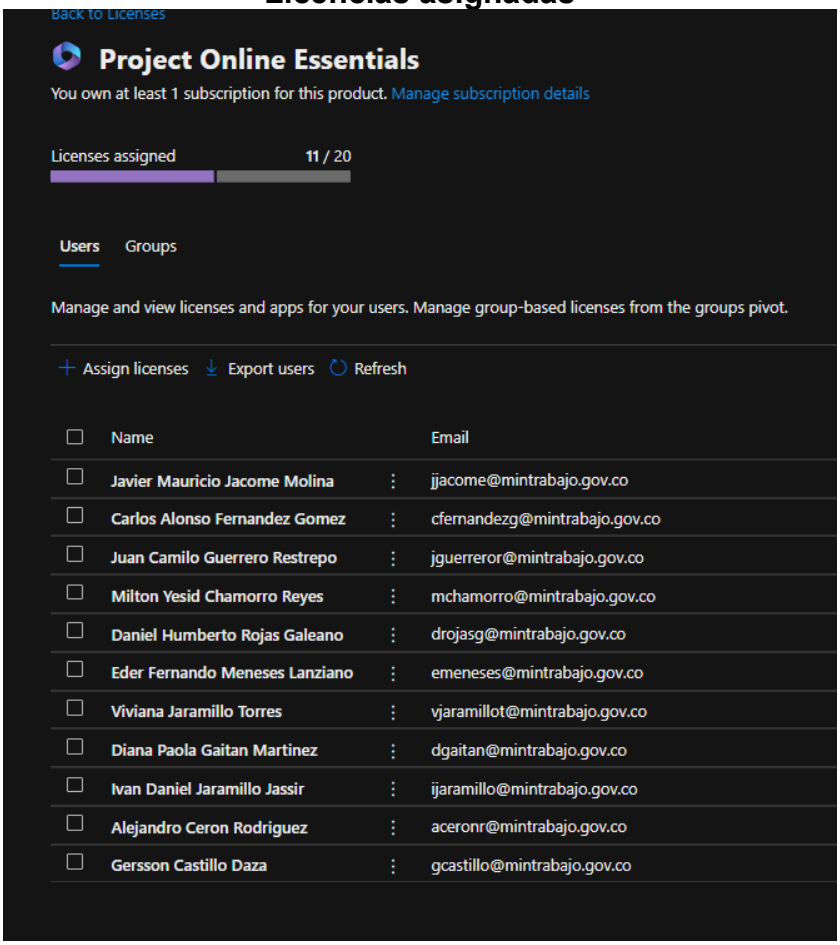


Ilustración 55 Licencias asignadas

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.

De igual forma, y articulado con el punto anterior a nivel de gobernanza de la infraestructura y de la mano con la implementación de buenas prácticas a nivel de procesos y administración de recursos tecnológicos, se da visibilidad del escenario de descentralización en donde diversos usuarios poseen diferentes accesos que pueden generar tiempos más largos en la identificación de causas raíces de incidencias o requerimientos presentados sobre las aplicaciones o infraestructura tecnológica de la entidad debido a este comportamiento en la asignación de privilegios sobre la infraestructura, servidores, aplicaciones o bases de datos. Lo anterior asociado a la propuesta de privilegio de acceso mínimo.

De la mano de los procesos de privilegios se trabajó en la mitigación de vulnerabilidades sobre la infraestructura virtualizada, en donde se observaban escenarios con protocolos deprecados o con versiones más recientes disponibles, máquinas virtuales en desuso que fueron postuladas para apagado ya sea por afinamiento de sus vulnerabilidades en otros entornos o por desuso de este recurso y aplican para procesos de Backup final y des aprovisionamiento. Se plantean diversas actividades para mitigación de vulnerabilidades:

Actualización de versiones de sistema operativo

- Cambio de repositorio de máquina virtual
- Actualización de componentes
- Habilitación y/o des habilitación de protocolos según corresponda
- Creación de políticas para servidores en AD

Entre otras actividades que han permitido una disminución significativa para la mitigación de vulnerabilidades.

Sin embargo durante estos procesos de mitigación, se han encontrado escenarios en donde el alcance contractual y técnico del equipo de trabajo, no permite realizar una mitigación total de las vulnerabilidades encontradas, sobre todo para el escenario de aplicaciones especializadas, por lo cual se consolidarán aquellas vulnerabilidades que por su naturaleza no pueden ser mitigadas con las actividades que se han propuesto y se han venido ejecutando, por lo cual se realizará una socialización y posterior entrega de aceptación del riesgo por parte de la entidad, ya que dentro de los escenarios encontrados, se observan obsolescencia de versiones de componentes que interoperan y permiten hacer funcional una aplicación que al intentar actualizarlos, indica que el código de la aplicación se

encuentra en un grado de obsolescencia y de uso de paradigmas de programación que ya no son soportados, por lo cual algunas de estas aplicaciones deben pasar por un proceso de re factorización total del código, que la entidad debe validar internamente, ya que esta actividad implica desarrollo de software de toda la aplicación y esto no se encuentra contemplado dentro de las actividades de mitigación de vulnerabilidades ni dentro del alcance contractual del servicio.

De acuerdo con este ítem, se ha venido trabajando articuladamente con la Oficina de Tecnologías de la Información con el fin de que a través de esta Oficina se realice el vínculo con las áreas funcionales y dar continuidad a los procesos de aceptación del riesgo.

Es importante mencionar que para el escenario de migración y estabilización de los file server eran servidores con las siguientes referencias:

- Dell Power Edge M820 a Fecha lanzamiento octubre 2012 | Fin de Soporte octubre 2017.
- Dell Power Edge M620 a Fecha lanzamiento junio 2012 | Fin de Soporte junio 2017.

Esta infraestructura poseía alertamientos en sus discos físicos, lo cual era un indicio de una posible falla futura que podría generar una indisponibilidad y perdida de la información alojada en los discos, lo cual significaba un alto riesgo para la integridad, disponibilidad y resguardo de la información alojada en estos recursos tecnológicos, teniendo en cuenta que esta información no poseía una redundancia que permitieran una recuperación oportuna o disponibilidad de los archivos digitales.

Esta infraestructura virtualizada expuesta, fue migrada a un entorno virtualizado con soporte de infraestructura vigente y bajo una administración centralizada y monitoreada, que permite tener visibilidad del estado actual de los recursos virtualizados. Actualmente la totalidad de la infraestructura se encuentra en la siguiente infraestructura:

- Dell Power Edge R6525 a Fecha lanzamiento junio 2021 | Fin de Soporte junio 2026

En estos 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. 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.

El equipo de nube privada gestionó y brindó apoyo en requerimientos escalados desde el área de riesgos laborales, requerimientos asociados a privilegios de acceso a recursos compartidos con terceros, traspaso de información, disponibilidad de servidores virtuales y depuración de permisos de acuerdo con lo requerido por el área solicitante.

Se ha realizado la actualización de los agentes de VMWare Tools de manera paulatina para evitar riesgos de seguridad asociados a versionamientos vulnerables de este agente sobre todas las máquinas virtuales del Ministerio del Trabajo.

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.

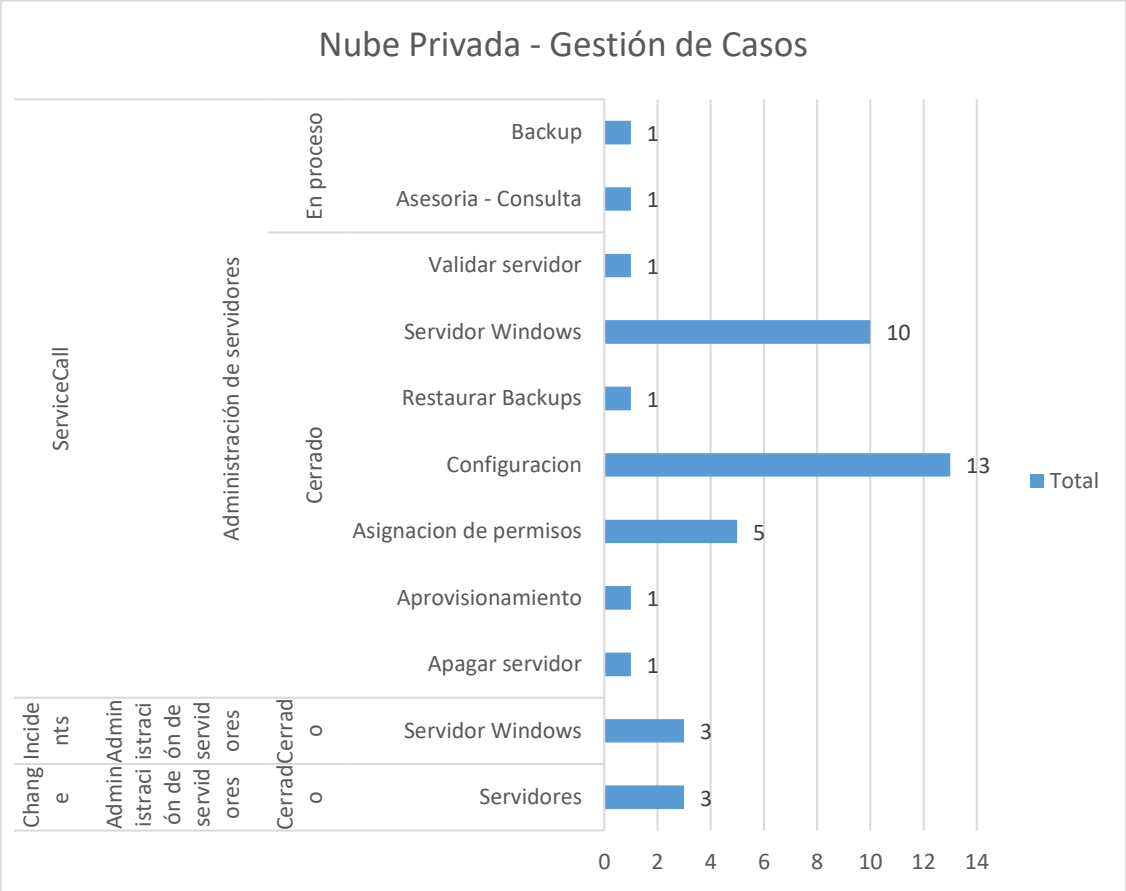


Ilustración 56 Gestión Nube Privada

Es importante precisar que la mayoría de 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 a lo anterior se deja claridad que la línea de Nube Privada esta compuesta por los componentes:

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

El servidor MINTRAB118 fue dispuesto inicialmente por el anterior proveedor de servicios tecnológicos como servidor de base de datos.

- Con el tiempo este servidor perdió su exclusividad para administración de este servicio y brindaron accesos para diferentes usuarios, perdiendo el control de los recursos y componentes alojados allí.

- Bajo esta premisa, tanto aplicaciones y bases de datos coexistían en el mismo servidor, como es de conocimiento de la Oficina de Tecnologías de la Información del Ministerio del trabajo, esto es una muy mala practica a nivel de seguridad y desarrollo. Ya que en el caso en donde el servidor o las credenciales del usuario sean vulnerado, no solo se vulnera la aplicación, código fuente, sino también las bases de datos de la aplicación alojadas allí.

- En el marco de los procesos de migración de base de datos a nuevos entornos, las bases de datos que actualmente se alojan en este servidor, serán migradas o en su defecto dadas de baja dependiendo de su criticidad y validación previa.

    - Esto teniendo en cuenta que se tenía una versión de OS y DDBB MSSQL Obsoleta, por lo cual es procedente realizar la baja de este servidor.

- No se dispondrá un servidor de desarrollo con control total, ya que esto abre la puerta a instalación de software no permitido, software no licenciado, malas practicas de acceso a la información y a los servidores virtuales.

    - Es importante mencionar que por este tipo de malas prácticas dentro de la entidad y en la administración de los recursos se materializaron escenarios de vulneración a sistemas de información y aplicaciones dentro de la entidad, documentadas y remitidas en su momento a las jefaturas de la Oficina de Tecnologías y áreas funcionales involucradas.

- En aras de conservar una correcta administración de los recursos de la entidad, evitar incidencias de seguridad como se han presentado por este tipo de incidencias y bajo la premisa de que la nube privada es para uso exclusivo de servidores virtuales y no para el uso de Escritorios virtuales, no

se han autorizado servidores para administración independiente y fuera del equipo de servicios centrales del Grupo de Soporte Informático de la entidad.

- Caso contrario para los escenarios en donde se exige un servidor de pruebas de aplicación, en donde la aplicación ya se encuentra desarrollada y la administración y accesos recaen en el equipo de Servicios Centrales.

- De acuerdo con lo anterior, en diferentes ocasiones y en conversación con la Jefatura de la Oficina TIC, se ha manifestado la necesidad de materializar el privilegio de mínimo acceso, en donde el acceso a los recursos tecnológicos de la entidad debe ser basado en roles y estrictamente el acceso a lo necesario para cada usuario, restringiendo accesos privilegiados o de administración a servidores virtuales, con el fin de reducir riesgos de seguridad anteriormente materializados y mantener integridad y seguridad en cada componente de la nube privada de la entidad.

- El servidor MINTRAB118 no se conservará en la infraestructura de la entidad, ya que como se mencionó, los componentes de DDBB fueron migrados a servidores nuevos de Win Server 2022, por lo cual la infraestructura WS2012 será dada de baja y no aplica para actualización, toda aplicación o servicio tecnológico alojado en 2012 es migrado a un servidor totalmente nuevo. Esto teniendo en cuenta que los procesos de actualización de sistema operativo en VM con OS tan obsoleto tienden a generar fallas y corromper archivos del sistema, estropeando procesos de correcta administración.
- Por lo cual, si se requiere un servidor virtual para desarrollar e instalar IDE de desarrollo se debe contar con la licencia respectiva del IDE para dejarlo aprovisionado en el servidor. De lo contrario si se requieren realizar pruebas funcionales de una aplicación o sistema de información en desarrollo, indicar las características necesarias para el servidor y los componentes (prerrequisitos) para dejar en funcionamiento la aplicación (IIS, versiones de .NET, Frameworks, Apache, NGNIX entre otros).
- De igual forma se pide concepto tanto a la Jefatura de OTIC como a la Coordinación de GSI para la creación de un escritorio virtual

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 39 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 40 *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 41 *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 42 *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 43 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 44 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 45 *Consumos totales*

Es importante mencionar que, en el proceso de redimensionamiento de la nube privada de la entidad, los ambientes de pruebas son los que están creciendo de manera continua (nuevos aprovisionamientos), por lo cual se debe entrar a revisar procesos de reducción de capacidades de estos entornos. De

igual forma se han reducido capacidades y desaprovisionado servidores para reducir los consumos sin afectar la disponibilidad de servicios productivos. En el escenario actual, la entidad tiene capacidad de crecimiento o ampliación de capacidades de los servicios ya aprovisionados. Se está en proceso de revisión para reducción de capacidades de servidores de aplicación como SISINFO por asignación de capacidades en RAM elevadas en contra parte con sus consumos.

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

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.

Se realiza sesión con la OTIC en donde se socializan los estados actuales y el camino a seguir para la continuidad de la implementación de Well Architected Framework, se da claridad de los escenarios para la correcta administración por parte de la UT, en donde se indica que NO se realizará recepción de ninguna cuenta de servicio, ya que el equipo de trabajo administra desde las cuentas de cada especialista que lidera cada servicio. Las cuentas de servicio deben estar bajo custodia de un funcionario de la entidad teniendo e cuenta la calidad de contratista de la UT. De igual forma se expone el escenario de Power BI y Microsoft Fabric y se da claridad de los componentes que se encuentran en funcionamiento, que deben ser ajustados, los que deben ser validados para conservar o desaprovisionar y se establece un plan de trabajo para la toma de decisiones con respecto a estos componentes. De Igual forma se establece una ruta para comparación de componentes, documentación y arquitectura para la recepción y migración de estas suscripciones al framework de arquitectura.

Se hizo envío de borrador de política de Privilegio de acceso mínimo y se incluyó a la nueva jefatura de TIC, así como la formalización del Lineamiento Implementación Infraestructura en Azure:

Objetivo: *El objetivo de esta política es garantizar que los empleados, contratistas y otros usuarios de los sistemas de información del Ministerio del trabajo tengan únicamente los privilegios necesarios para realizar sus funciones laborales, minimizando así los riesgos relacionados con el acceso no autorizado y la exposición de datos sensibles.*

Alcance: *Esta política es aplicable a todos los usuarios que interactúan con los sistemas de la organización, incluidos empleados, contratistas, proveedores, y cualquier otra parte externa que tenga acceso a los recursos informáticos de la empresa.*

El principio de privilegio de acceso mínimo es esencial para garantizar la seguridad operativa y proteger la integridad de los sistemas y datos de la organización. Todos los usuarios y administradores deben ser conscientes de su responsabilidad para mantener este principio y adherirse a los controles establecidos para gestionar los accesos de manera efectiva.

Principio del Privilegio de Acceso Mínimo: *La política de privilegio de acceso mínimo establece que los usuarios solo deben tener acceso a los recursos y datos que sean estrictamente necesarios para realizar sus tareas laborales. Esto implica:*

- *Asignación basada en roles: Los privilegios de acceso se deben asignar en función del rol específico del usuario dentro de la organización. No se debe otorgar acceso a más recursos de los que un usuario necesita para desempeñar su función.*
- *Acceso restringido a sistemas sensibles: El acceso a información crítica, confidencial o estratégica debe ser limitado solo a aquellos usuarios cuyo trabajo lo requiera. Los usuarios deben ser autorizados de forma explícita para acceder a estos sistemas, y la autorización debe ser revisada periódicamente.*
- *Revisión periódica de privilegios: Los privilegios de acceso deben ser revisados regularmente para asegurar que los usuarios mantengan únicamente los permisos necesarios para sus funciones actuales. Cualquier cambio en el rol o en las responsabilidades de un usuario debe conllevar una revisión inmediata de sus privilegios.*
- *Rechazo de accesos innecesarios: En ningún caso un usuario debe recibir acceso por defecto a sistemas, aplicaciones o datos que no estén directamente relacionados con sus responsabilidades. Todos los accesos adicionales deben ser solicitados, evaluados y aprobados por el responsable de seguridad. Importancia de Mantener el Principio de Privilegio de Acceso Mínimo*
  Mantener el principio de privilegio de acceso mínimo es crucial para la protección de la información sensible y la integridad de los sistemas de la organización. La asignación indebida de permisos o la falta de restricciones adecuadas puede dar lugar a los siguientes riesgos:
- *Acceso no autorizado: Usuarios con privilegios excesivos pueden acceder a información o sistemas para los cuales no están autorizados, exponiendo así datos confidenciales.*
- *Incremento de la superficie de ataque: Los usuarios con privilegios elevados, si se ven comprometidos, pueden proporcionar a los atacantes un punto de acceso para obtener más control sobre los sistemas de la organización.*
- *Errores humanos y mal uso: Incluso sin malicia, un usuario con privilegios innecesarios puede cometer errores que afecten la estabilidad o la seguridad de los sistemas, como la eliminación o modificación de datos importantes.*

Responsabilidades

Cada miembro de la organización debe:

- *Gestionar el acceso de acuerdo con los principios de esta política: Los administradores de sistemas y recursos son responsables de asegurarse de que los privilegios de acceso se asignen correctamente y se ajusten a las necesidades laborales de los usuarios.*
- *Solicitar cambios de privilegios a través de los canales adecuados: Cualquier solicitud para otorgar, modificar o eliminar privilegios debe ser canalizada a través del proceso formal de gestión de accesos de la organización.*
- *Reportar accesos sospechosos o actividades inusuales: Todos los usuarios deben estar atentos a comportamientos inusuales y reportarlos inmediatamente al departamento de seguridad o administración de sistemas.*
- *Seguridad: La seguridad de los sistemas y la protección de la información son fundamentales para el éxito y la continuidad de la organización. La implementación efectiva del principio de privilegio de acceso mínimo contribuye a la mitigación de los riesgos de seguridad, tales como:*

- *Prevención de brechas de seguridad: Limitar el acceso de los usuarios solo a los recursos necesarios reduce significativamente la probabilidad de que un atacante pueda obtener acceso a información sensible en caso de que una cuenta de usuario sea comprometida.*

- *Auditoría y trazabilidad: Al aplicar el principio de privilegio mínimo, es más fácil realizar auditorías y seguimientos de las actividades de los usuarios. Si un incidente de seguridad ocurre, la trazabilidad de accesos y actividades será más clara y se podrá tomar acción correctiva rápidamente.*

La implementación de este lineamiento está del lado de la Oficina de Tecnologías de la Información de la entidad. Aún se encuentra en espera de retroalimentación de esta Oficina a la UT y Soporte informático.

Se realizó la pausa de servicios de nube a través de una sesión técnica y funcional, con el fin de que el área de la oficina de TIC como encargada de administrar costos del tenant el Ministerio de Trabajo sea quien pause los componentes que se evalúen en la misma sesión. Hasta el momento GoToCloud como proveedor ha manifestado la intención de iniciar con la migración y esta en validación de la OTIC.

De acuerdo con el contexto anterior y dando un alcance adicional, desde el equipo de Nube Publica de Servicios Centrales, se remite el siguiente análisis de costos de la suscripción de Empleo que alberga algunos proyectos del BID, en promedio la suscripción está consumiendo 15.000 USD al mes. Este es detalle por grupo de recursos (este reporte se realiza con los consumos del mes de enero 2026).

Tras una validación proactiva del equipo de Nube Pública, nos permitimos realizar las siguientes observaciones a nivel de costos de una de las suscripciones (Analitica-Interoperabilidad) del Tenant Azure de la entidad:

Los siguientes recursos no generan un gasto considerable (solo algunos USD) pero son recursos redundantes que deben ser eliminados por buena práctica:

- appanalitica-bk - Web app
- appanalitica-bk2 – Web app
- appanalitica-bk - App Insigths
- appanalitica-bk2 – App Insigths
- appanalitica20231120115 - App Insigths
- appanalitica-prueba - App Insigths
- appanalitica-bk202311201036 - App Insigths

El App Service **ASP-RGANALITICAMT-b4ad** se encuentra sin uso, (no tiene apps desplegadas) y consume Aproximadamente 13 USD al mes:

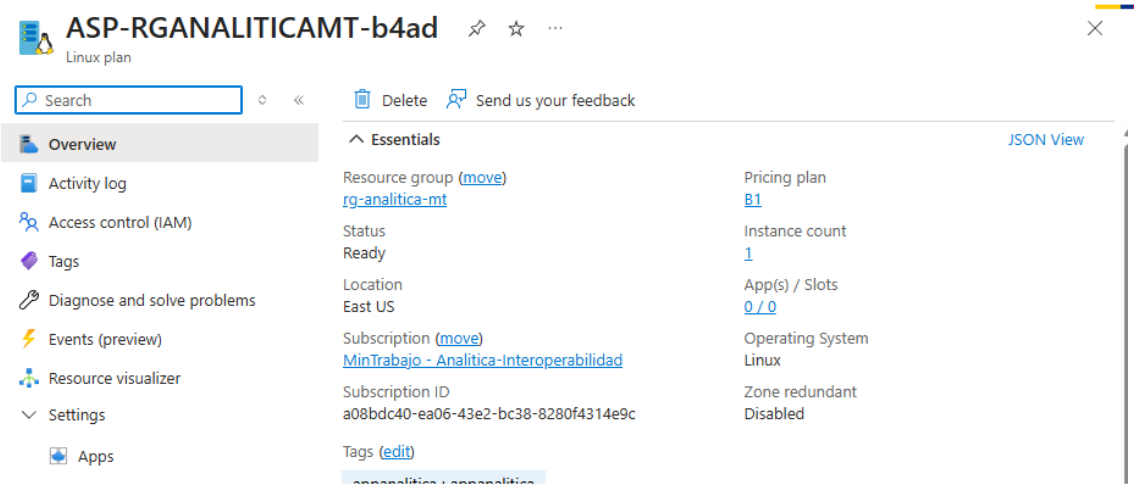


Ilustración 57 App Service1

El App service ASP-RGANALITICAMT-bd39 se encuentra sin uso, (no tiene apps desplegadas) y consume Aproximadamente 180 USD al mes:

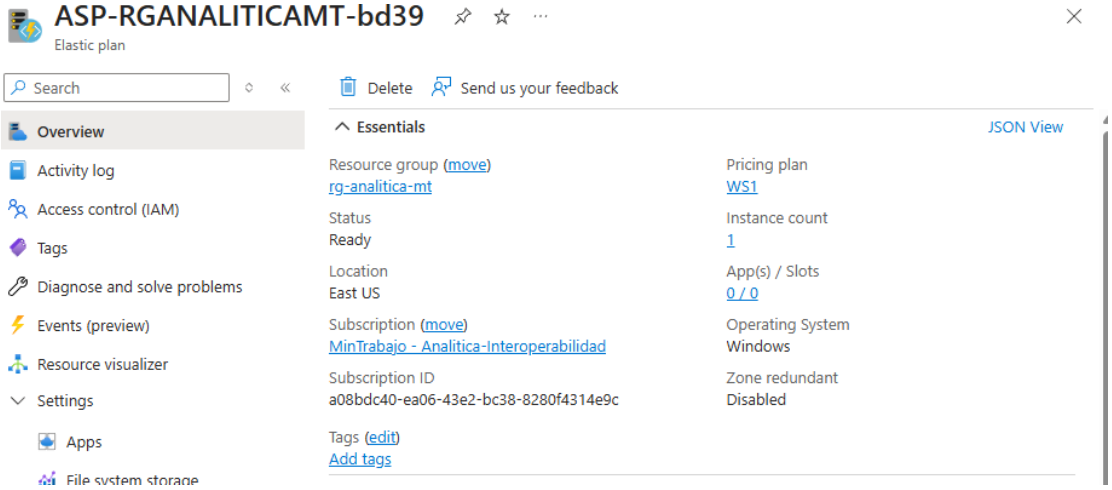


Ilustración 58 App Service2

Los siguientes recursos de Bases de datos se puede cambiar el modelo de consumo, de Instancias con vCores Fijos, a el modelo de DTU:

- SQL Database **BDMT_MS_REPORT (svmtsql/BDMT_MS_REPORT**) tiene un consumo promedio de 5 % de procesamiento en los últimos 7 días, tiene una configuración de General Purpose: Gen5, 2 vCores con un costo de 210 USD aprox, se recomienda realizar el cambio a una server en el modelo de DTU con 50 DTU (con un costo de 80 USD aprox) y validar el comportamiento para redimensionar el servidor de acuerdo al consumo final.

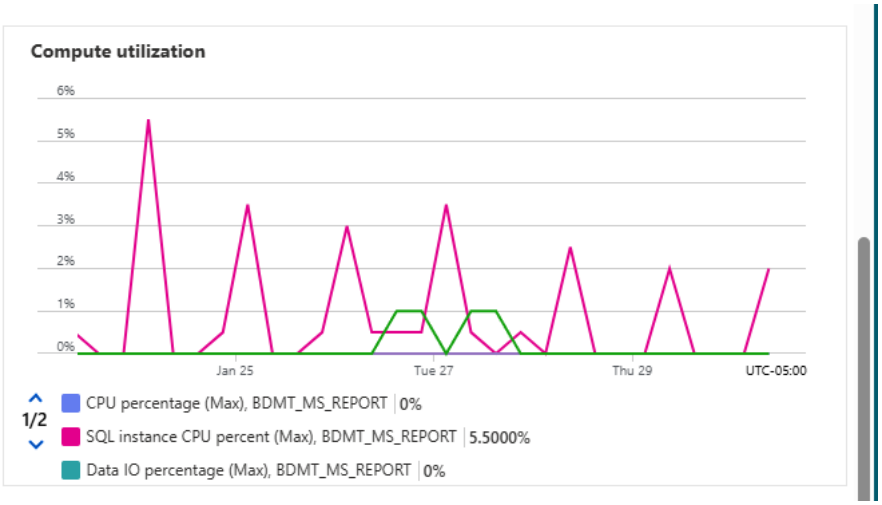


Ilustración 59 - SQL Database BDMT_MS_REPORT

- SQL Database **dev_sqldb_direccion_ivc Standard S2: 50 DTUs,** tiene un consumo de (77 USD Aprox) y de acuerdo a las métricas del último mes no se encuentra en uso (salvo por un consumo del 1 %). La primera recomendación es reducir la DB a 10DTU (15 USD Aprox) y validar si realmente se está en uso la DB

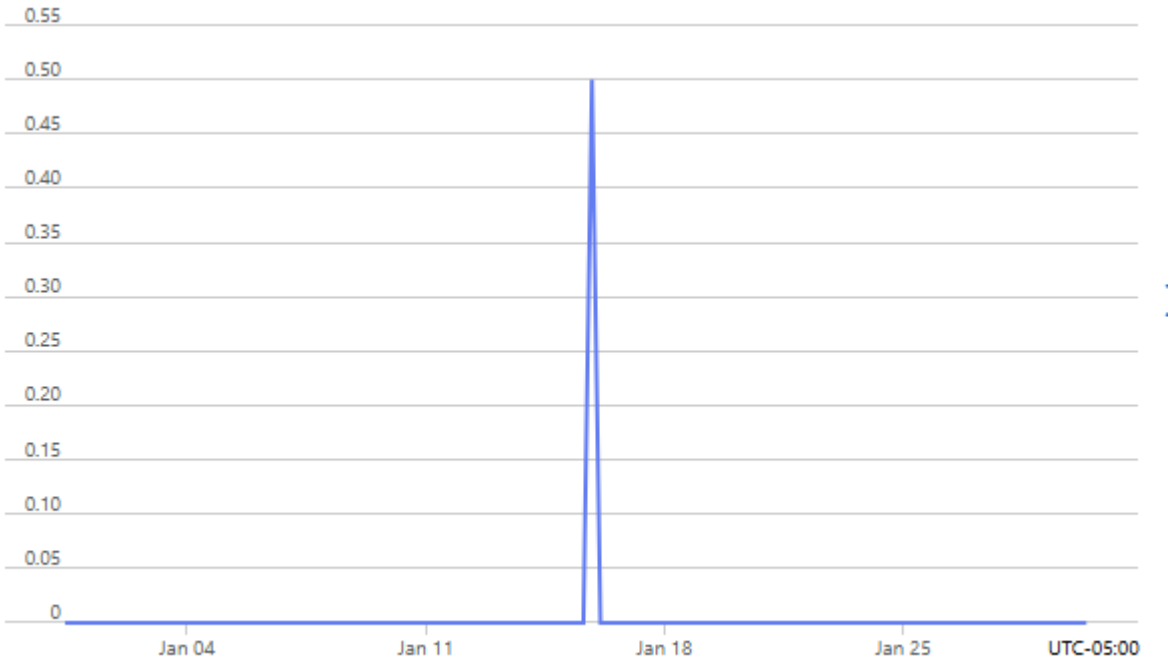


Ilustración 60 - SQL Database dev_sqldb_direccion_ivc

Las anteriores recomendaciones pueden generar un ahorro aproximado de 300 USD mensual.

ResourceGroup	SubscriptionName	CostUSD
az_rg_psncde_prd	Mintrabajo - Direccion de Empleo	$ 4.495,17
az_rg_sig_qa	Mintrabajo - Direccion de Empleo	$ 1.938,41
az_networking_all_01	Mintrabajo - Direccion de Empleo	$ 1.404,83
az_rg_sig_dev	Mintrabajo - Direccion de Empleo	$ 1.322,62
mc_az_rg_psnc_dev_az_aks_psnc_dev_eastus2	Mintrabajo - Direccion de Empleo	$ 1.269,14
az_rg_backend_prd_01	Mintrabajo - Direccion de Empleo	$ 1.162,42
az_rg_backend_qa_01	Mintrabajo - Direccion de Empleo	$ 745,31
az_rg_psnc_dev	Mintrabajo - Direccion de Empleo	$ 513,91
az_rg_shv_prd	Mintrabajo - Direccion de Empleo	$ 363,49
az_rg_webapps_qa_01	Mintrabajo - Direccion de Empleo	$ 342,21
aks-platformwale_eastus2	Mintrabajo - Direccion de Empleo	$ 252,87
az_rg_shv_qa	Mintrabajo - Direccion de Empleo	$ 249,59
az_rg_sena	Mintrabajo - Direccion de Empleo	$ 245,07
az_rg_webapps_prd_01	Mintrabajo - Direccion de Empleo	$ 235,47
az_monitoreo_tubio_ocupacol	Mintrabajo - Direccion de Empleo	$ 229,71
databricks-rg-dbricks-sig-qa-fghycz5wd63rg	Mintrabajo - Direccion de Empleo	$ 45,50
sig_dev_rg	Mintrabajo - Direccion de Empleo	$ 43,44
az_rg_iaas_all_01	Mintrabajo - Direccion de Empleo	$ 42,12
synapseworkspace-managedrg-169b47eb-b798-48b8-b67d-d072ef1c9b9d	Mintrabajo - Direccion de Empleo	$ 21,67
synapseworkspace-managedrg-5d77bdb5-7f9b-4b12-b98d-f146da7f9da6	Mintrabajo - Direccion de Empleo	$ 21,67
databricks-rg-azdbwsprd01-v4hv6ycuxi3f6	Mintrabajo - Direccion de Empleo	$ 14,87
cloud-shell-storage-southcentralus	Mintrabajo - Direccion de Empleo	$ 11,79
dbrickssigdev	Mintrabajo - Direccion de Empleo	$ 7,59
az_rg_aks_qa	Mintrabajo - Direccion de Empleo	$ 7,03
databricks-rg-azdbwsqa01-ii2qme4mj32a2	Mintrabajo - Direccion de Empleo	$ 5,58
databricks-rg-sig_dev_dbks-xac4zvgszu4dy	Mintrabajo - Direccion de Empleo	$ 5,58
az_rg_tfstate	Mintrabajo - Direccion de Empleo	$ 5,57
az_rg_api_qa	Mintrabajo - Direccion de Empleo	$ 3,99
az_monitoring_all_01	Mintrabajo - Direccion de Empleo	$ 0,61
defaultresourcegroup-eus	Mintrabajo - Direccion de Empleo	$ 0,10
	Mintrabajo - Direccion de Empleo	$ 237,20
Total		$ 15.244,54

Ilustración 61 Tabla de recursos

Estos son los recursos que consumen más de 500 USD:

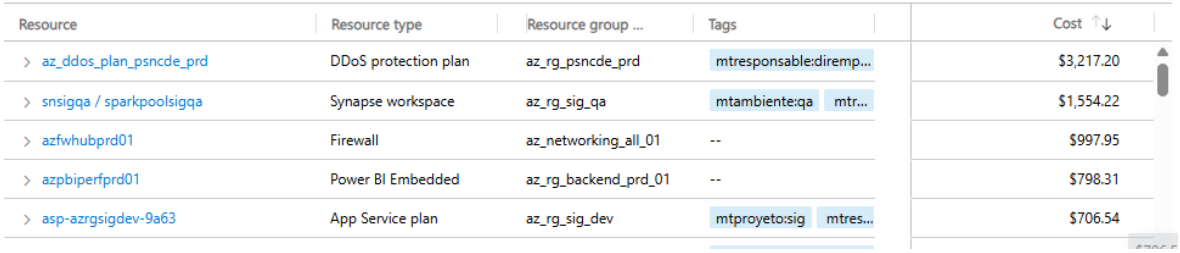


Ilustración 62 Mayor consumo de recursos

En función de la solicitud escalada por el equipo técnico Accenture y el BID, nos permitimos remitir la trazabilidad de lo ocurrido con la Suscripción de Dirección de Empleo alojada en el Tenant del Ministerio del Trabajo.

1. Inicialmente se reporta perdida de accesos y privilegios a los grupos de recursos y suscripción de dirección de Empleo, esto reportado por el equipo de Accenture.
2. Se inicia validación con el equipo de Administración y Arquitectura de nube publica, para validar los privilegios que tienen los diferentes usuarios hacía el Tenant de la entidad y la suscripción de Empleo.
    a. Se observa que desde los usuarios con los que la entidad dispone para administrar el Tenant, tampoco se visualiza la suscripción de Dirección de Empleo dentro de los grupos de administración del Tenant de Azure del Ministerio del Trabajo:

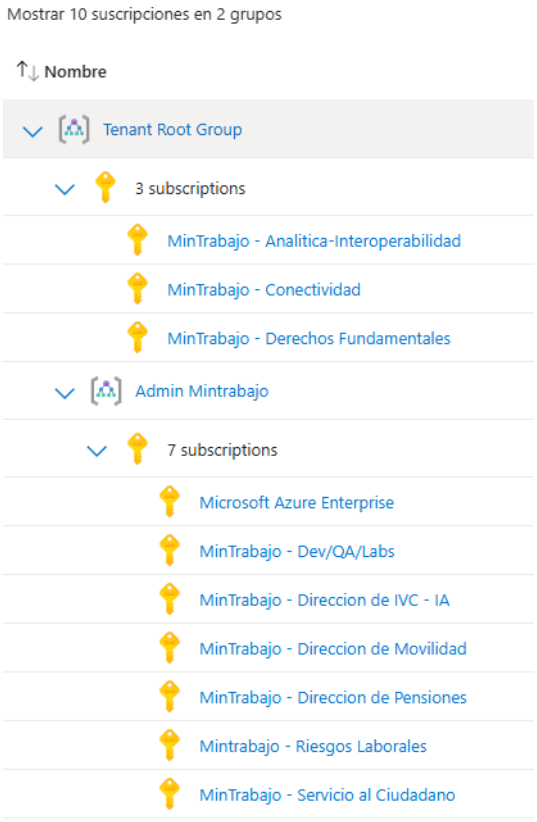


Ilustración 63 Relación de suscripciones

3. Se realizan sesiones técnicas para validar el usuario perfilcatalogo@mintrabajo.gov.co el cual es usado por el equipo BID para administrar los recursos alojados en la suscripción de Empleo.

a. Se presentan inconvenientes para acceder, pero finalmente se logra iniciar sesión al realizar exclusión de método de MFA con el fin de poder observar si este usuario también había perdido privilegios sobre la suscripción. (se observa que el usuario es usado por más de un usuario).

b. Al acceder con la cuenta perfil catálogo se observa que solamente tiene visibilidad de la suscripción DEV/QA del Tenant del Ministerio del Trabajo:

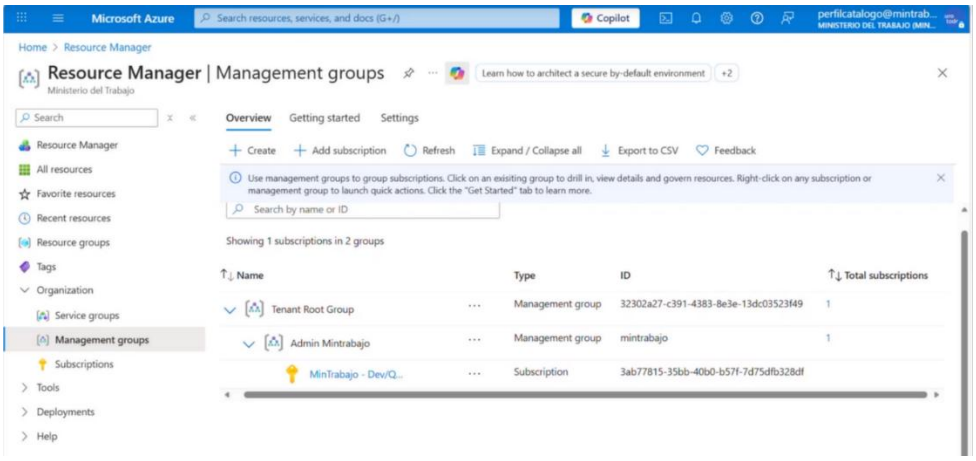


Ilustración 64 cuenta perfil catálogo

4. Tras validación de que privilegios poseía esta cuenta se observa que también posee acceso a un Tenant diferente al del Ministerio, con dominio SPEmpleo.onmicrosoft.com, el cual no es de administración del Ministerio del Trabajo:

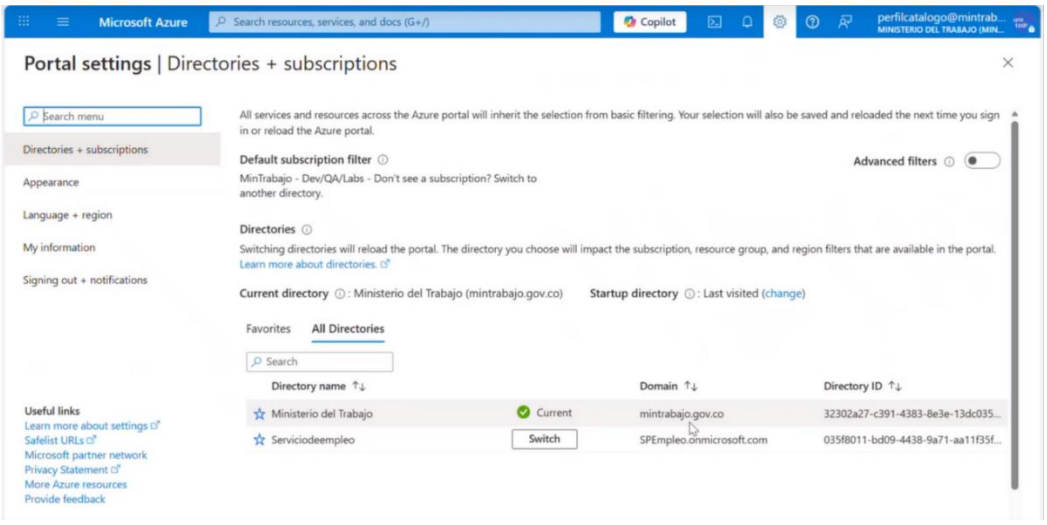


Ilustración 65 Captura configuración del portal

5. Al realizar validación de los buzones de las cuentas de administración del Tenant de Ministerio del Trabajo podemos observar lo siguiente:

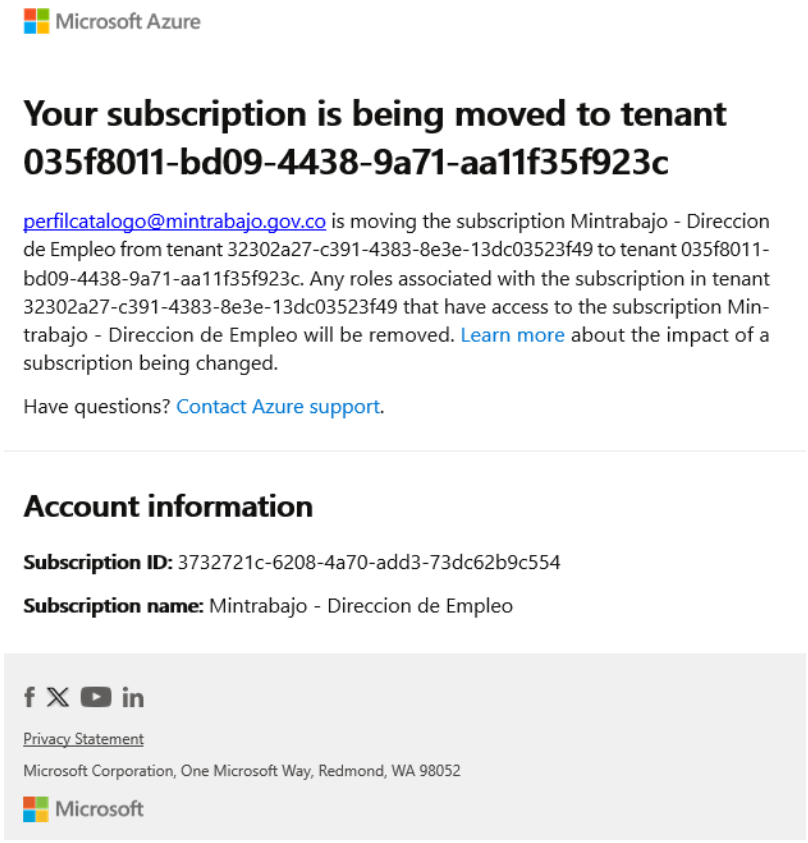


Ilustración 66 Validación de buzones

   a. Aquí se observa que a través de la cuenta de servicio perfilcatalogo@mintrabajo.gov.co que no esta bajo la custodia del Grupo de Soporte Informático ni de la Oficina de Tecnologías de la Información, se realizó el movimiento de toda la suscripción de la Dirección de Empleo del Tenant de Azure del Ministerio del Trabajo a un Tenant diferente (en el correo indica el ID del Tenant de Azure al que fue movida).

   b. Bajo esta premisa, el Ministerio del Trabajo perdió gestión y visibilidad de los recursos de esta suscripción y quedaron alojados en el Tenant con el id referenciado, posiblemente el Tenant con dominio SPEmpleo.onmicrosoft.com

6. Tras el contexto anterior, *se puede determinar la razón por la cual todos los usuarios, incluidos los administradores del Tenant del Ministerio del Trabajo perdieron acceso y visibilidad de la Suscripción de la Dirección de Empleo*.

Consideramos este comportamiento bastante grave, ya que este movimiento de recursos requiere de un control de cambios bajo la práctica de ITIL, previo a realizar este tipo de ajustes o cambios dentro del Tenant de la entidad, así como se debe justificar la maniobra de movimiento de suscripción entre Tenant, se debe radicar un RFC con el minuto grama, involucrados, actividades a realizar, actividades previas y rollback en caso de ser necesario. Pero por encima del cumplimiento de las buenas prácticas de gestión de cambios, se debió notificar a la entidad quien es propietaria de estos recursos, suscripciones y como se gestionan.

De igual forma y como se ha mencionado en repetidas ocasiones, el tipo de privilegios elevados a estas cuentas de servicio como *perfilcatalogo*, debe entrar en revisión y auditoria, ya que permite tomar decisiones sobre los recursos sin previa notificación a la Oficina de Tecnologías de la Información. Consideramos que, bajo la implementación del privilegio de mínimo de acceso, todos los usuarios y estrictamente las cuentas de servicio deben tener los permisos necesarios para trabajar, pero se deben considerar privilegios que permitan este tipo de maniobras, aprovisionamiento de recursos con grandes dimensiones, descentralizar la administración de las suscripciones entre otros puntos técnicos a revisar.

Finalmente, como se ha venido sugiriendo, es importante que el Ministerio del Trabajo, adopte un procedimiento o política de Gobernanza de la Nube**,** en donde estandarice este tipo de políticas y que se implementen y se realice seguimiento de manera transversal a todos los usuarios que posean acceso a recursos en la Nube, esto con el fin de mantener una buena práctica no solo en el acceso a los recursos e información en la nube, si no es la forma de aprovisionar, gestionar y administrar los proyectos alojados allí.

Es importante realizar el contacto con los usuarios que posean el acceso al Tenant del SPEmpleo.onmicrosoft.com para poder retornar la suscripción y volver a realizar la asignación de privilegios dentro del Tenant de la entidad.

Se dio continuidad a los procesos de creación de templates en Terraform para migrar aplicaciones y entorno completos a la nueva arquitectura de Azure, integrada con DevOps.

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 identificaron diversas aplicaciones que durante los procesos de afinamiento generaron indisponibilidad, pero no generaron un incremento o reporte de

requerimientos de servicio e incidencias, este comportamiento permite identificar qué tipo de aplicaciones se encuentran aprovisionadas, pero sin administración funcional lo cual dentro de los procesos de re dimensionamiento de aplicaciones e infraestructura virtualizada permiten una optimización de los recursos asignados a las aplicaciones que realmente requieren capacidades superiores para un correcto funcionamiento en ambientes productivos.

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

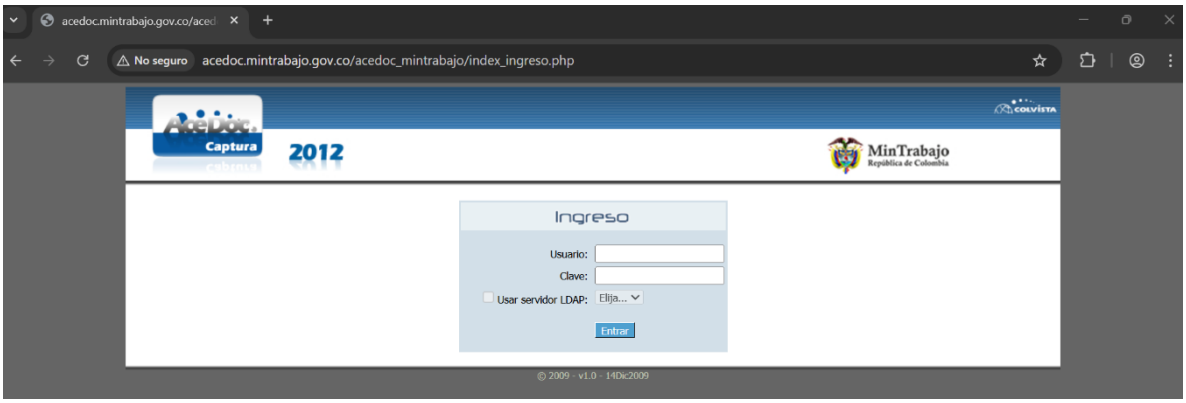


Ilustración 67 Nuevo entorno ACEDOC

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

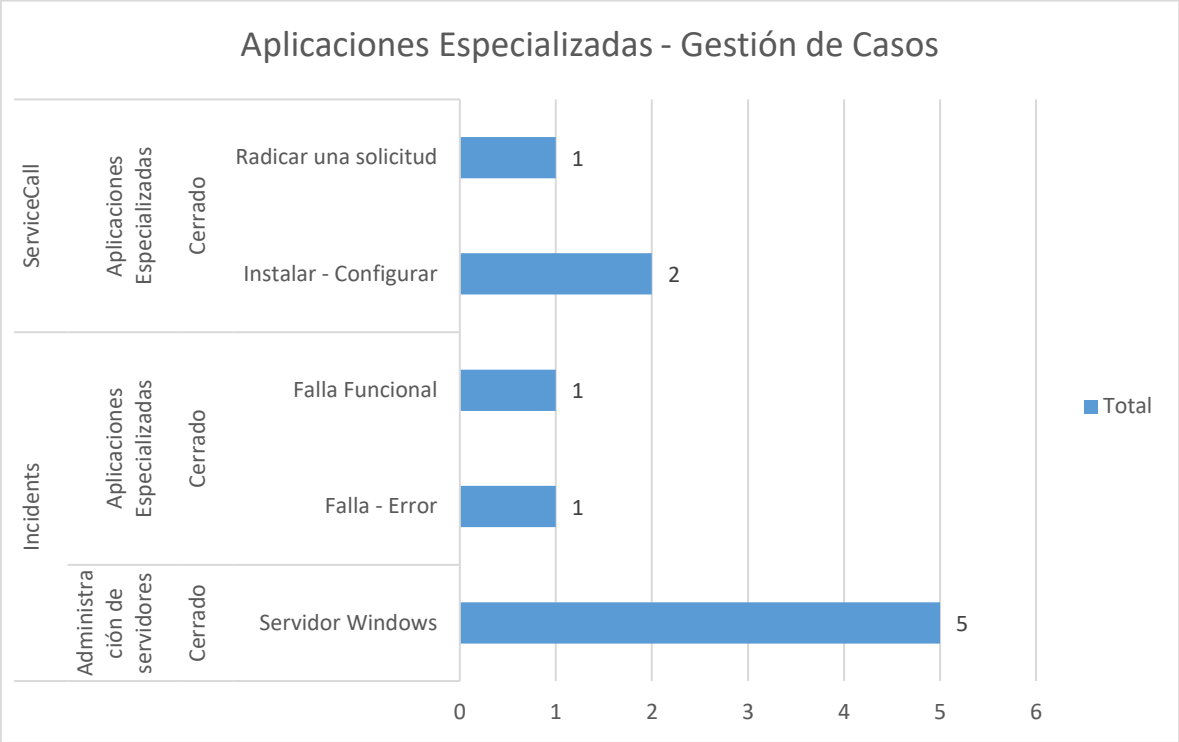


Ilustración 68 Gestión Apps Especializadas

Se definieron una serie de actividades para dar continuidad a la prestación de los servicios a nivel de aplicación para SIAS.

Escenario SIAS:

Pendientes:

- IVC recopilaría la información de los sindicatos que accederían al sistema para escalar la creación de usuarios VPN que tengan estrictamente acceso a SIAS y a ningún otro recurso tecnológico. Esta información actualmente no ha sido remitida para iniciar con el proceso de creación de usuarios. Fue descartado por IVC
- Entrega de sistema de información SIAS refactorizado el cual tienen presupuestado probar y poner en producción durante el mes de Julio de 2025. Nunca se envío información al respecto por parte de IVC.
- Se informan retrasos en los procesos de desarrollo del equipo de IVC y aún se está a espera de información hacía la Oficina TIC y el Grupo de Soporte Informático.
- Tras avance en el desarrollo, la entidad determina que el sistema no se encuentra listo para salir a producción.
- Se aprovisionaron las nuevas máquinas de SIAS en Windows 2022, esto está generando doble consumo de capacidades en la nube privada y se está a espera de confirmación para dar de baja los servidores antiguos. Los servidores fueron apagados para no generar doble consumo

de capacidades y se está a espera de instrucción por parte del área funcional. Las VM no han sido intervenidas ni han informado de avances significativos.

De acuerdo con los tickets RF-154278, RF-154044, RF-154384 y el IM-154045, se ha identificado que en el servidor 172.20.42.101 - MTAPPWPREAS01 el disco C: ha superado el umbral del 90% de ocupación.
La causa principal corresponde al crecimiento de la carpeta asociada a IIS, lo que incrementa el riesgo de que el sistema quede sin espacio disponible. Al tratarse de la unidad C:, donde reside el sistema operativo, esto podría generar indisponibilidad del servidor y afectar la continuidad del servicio.

Por lo anterior, se solicita la depuración de la carpeta de IIS para mitigar el riesgo y garantizar la estabilidad del servidor.

Se comparten las evidencias de dicho umbral.

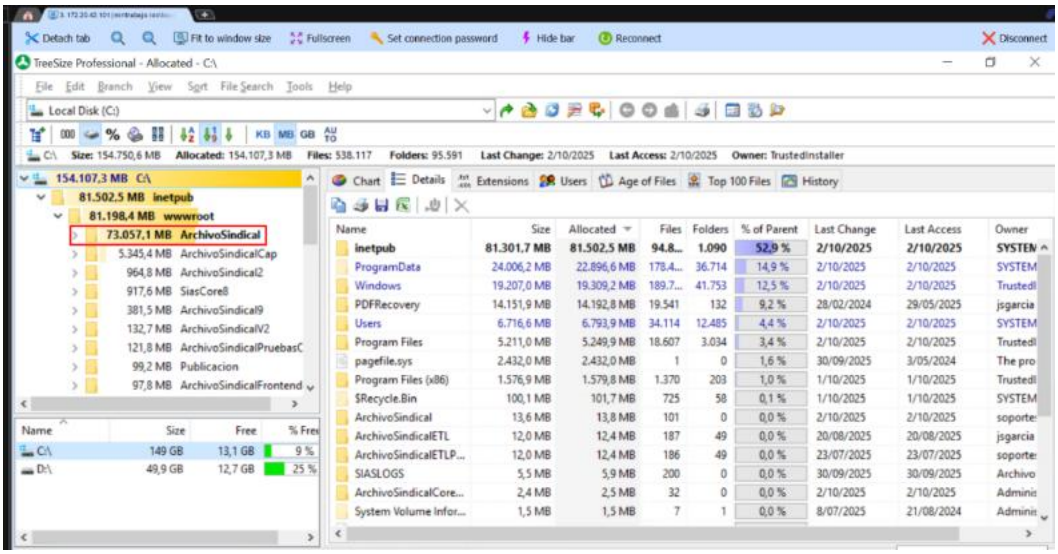


Ilustración 69 Grafica umbral servidor

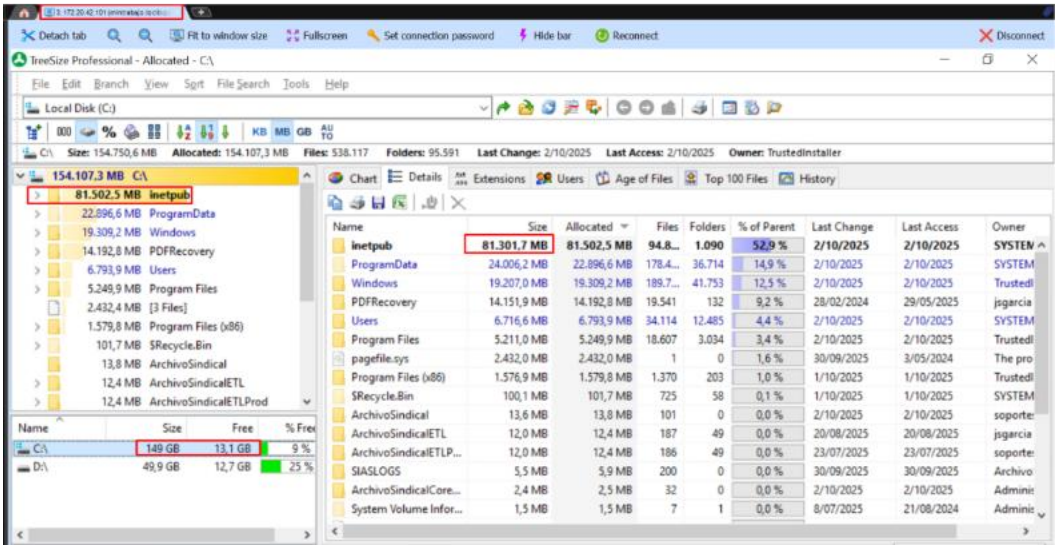


Ilustración 70 Gráfica umbral servidor2

El área funcional manifiesta un crecimiento adicional del 100GB sobre los servidores, tras autorización del Coordinación, se realiza el crecimiento necesario sobre los servidores

Escenario FILCO:

Pendientes:

- Queda pendiente el agendamiento de una sesión con el equipo de empleo para validar el funcionamiento de los DSpace para validar alternativas tanto en nube publica como en nube privada bajo los lineamientos de la entidad.
- Se da continuidad al proceso de DSpace de la mano de la Oficina de Tecnologías de la Información en donde se adoptan medidas de descartar formalmente el servicio de DSpace y usar herramientas licenciadas como lo son LifeRay y FileNet, se proponen alternativas de publicar los contenidos a través del Micrositio con el que cuenta actualmente FILCO en la Página Web de la entidad y que es administrado actualmente por el área de Empleo.
- Se logra conexión entre FileNet y LifeRay, en validación de conexión entre DSpace y LifeRay o FileNet en su defecto.
- tras la realización de validaciones internas con el equipo de trabajo, se pueden determinar los siguientes aspectos:
- No existe una forma directa de conectar FileNet a DSPace, requiere un desarrollo específico para lograr la conectividad entre estos dos componentes.
- Es posible conectar LifeRay con FileNet a través del consumo de servicios que expone FileNet, la conexión puede ser algo lenta ya que no se conecta puntualmente a un repositorio sino a toda la solución.
- Para poder conectar LifeRay con DSPace es necesario la URL del repositorio CMIS, servicio que expone DSPace para poder trackear la información.

- Es necesario crear los tipos documentales (Nombres y campos) por lo cual es requerida esta matriz de información de los documentos que se necesitan sincronizar con el micrositio de la página web.
- Se crea micrositio para alojar los documentos de la red ORMET y se está espera de aprobación funcional por parte del área de empleo.

Para poder dar continuidad a este proceso, es necesaria la información solicitada en los dos últimos ítems para iniciar pruebas de conectividad y creación de tipos documentales, quedamos atentos a su validación y análisis para dar continuidad a este procedimiento. Se está a espera de envío de información por parte de la entidad.

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. De igual forma se indica la información para ser validada y posteriormente realizar el contacto.

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. Las aplicaciones pendientes de aprobación y a las cuales se hace referencia en el presente correo para realizar pruebas y migración a un entorno de Windows Server 2022 son:

Banco de Información Regional de Empleo (BIRE)

- Formación Vocacional
- Tramites (es una aplicación diferente a tramites.mintrabajo.gov.co, posiblemente un sitio de pruebas ya que esta aplicación en concreto se encuentra alojada en MINTRAB23, servidor de aplicaciones NET y diferente de donde se aloja la página expuesta a la ciudadanía).

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:

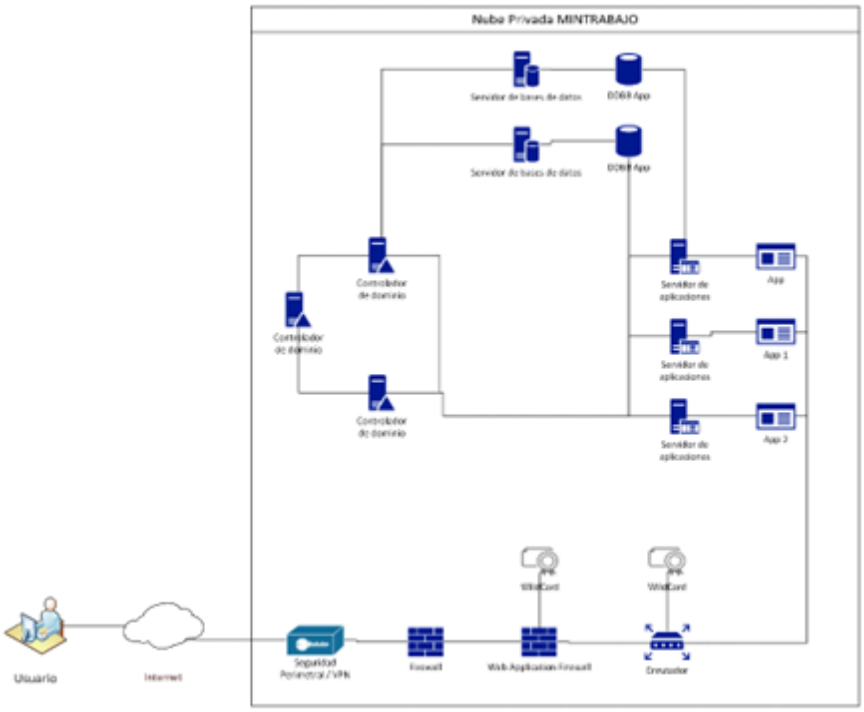


Ilustración 71 Arquitectura final Apps

Y la reorganización de los sitios de manera independiente:



Ilustración 72 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.

Como parte de las actividades contempladas, el equipo técnico de la Unión Temporal TIC recibió del Ministerio de Trabajo un medio físico (CD) que contenía el código fuente y archivos relacionados con el sistema SISGESTION. Este material constituye la base sobre la cual se realizó el proceso de despliegue de la aplicación en el entorno del Ministerio. El contenido del medio incluía la solución completa en formato de proyecto de Visual Studio, junto con las carpetas de código fuente organizadas por módulos y funcionalidades. Entre los elementos principales recibidos se destacan:

- Carpetas de módulos del sistema: AccesoDatos, Contratos, LogicaNegocio, PlaneacionInstitucional, SISGESTION.WebApp, Viaticos, entre otras, que contienen el código fuente estructurado.
- Carpeta SISGESTION.Entidades.Database: esta carpeta reviste especial importancia ya que incluye los scripts SQL necesarios para la creación y configuración de la base de datos del sistema. Contiene un total de 604 scripts SQL que abarcan la definición de tablas, procedimientos almacenados, funciones y otros objetos de base de datos requeridos para el funcionamiento completo de la aplicación.
- Archivos de configuración de automatización: scripts en PowerShell (como deploySisgestion.ps1) y archivos YAML para definición de pipelines (pipeline-aplicacionweb.yml, pipeline-sitioweb.yml, pipeline-sitiowebpr.yml), que facilitan procesos de despliegue continuo.
- Archivo de solución de Visual Studio: Sisgestion.sln, que permite cargar el proyecto completo en el entorno de desarrollo para su compilación y revisión.
- Otras dependencias: carpetas como dlls y packages, necesarias para la correcta compilación y ejecución de la aplicación.

Esta estructura permitió revisar y ejecutar el proceso de despliegue siguiendo las indicaciones provistas, aunque se identificaron aspectos del código que requerirían ajustes o refactorización para mejorar su funcionamiento o adaptarlo a cambios futuros.

A continuación, se presenta el cronograma de actividades realizadas para el despliegue del sistema SISGESTION. Este cronograma detalla las principales tareas ejecutadas, sus fechas y responsables, permitiendo evidenciar el cumplimiento de los compromisos establecidos.

El despliegue del sistema SISGESTION se realizó en un ambiente de pruebas controlado. La topología de red implementada incluye servidores de aplicaciones, base de datos y componentes necesarios para validar la instalación y el funcionamiento del sistema.

- El despliegue del sistema SISGESTION se llevó a cabo siguiendo una serie de pasos técnicos orientados a garantizar su correcta instalación, configuración y funcionamiento dentro del entorno de pruebas (QA). A continuación, se detallan las principales actividades ejecutadas durante el proceso:

  - Instalación del complemento de Reporting Services en Visual Studio Para asegurar la carga completa de todos los proyectos incluidos en la solución SISGESTION, fue necesario instalar el complemento correspondiente a Reporting Services, el cual habilita el soporte para reportes dentro del entorno de desarrollo.
  - Configuración de cadena de conexión Se actualizaron los datos de conexión dentro del archivo web.config de la aplicación, utilizando la información suministrada desde la parte de la base de datos, con el fin de enlazar correctamente la aplicación con la base de datos correspondiente.
  - Ajustes de seguridad en el archivo de configuración. Se realizaron modificaciones en los niveles de seguridad definidos por defecto en la aplicación, permitiendo la autenticación a través del protocolo HTTP. Para ello, se ajustó la propiedad correspondiente en el archivo web.config
  - Compilación y publicación del sitio. Con las configuraciones anteriores completadas, se procedió a compilar la solución en Visual Studio y publicar el sitio para su posterior despliegue en el entorno designado.
  - Despliegue en el servidor de pruebas (QA). La aplicación fue desplegada en el servidor correspondiente al ambiente de pruebas (QA), en el cual se realizan validaciones funcionales.
  - Creación del sitio en IIS y configuración de puerto de salida Finalmente, se creó el sitio correspondiente en el servidor web IIS (Internet Information Services), configurando un puerto de salida específico para asegurar su accesibilidad dentro de la red del Ministerio.

Este proceso se desarrolló de forma controlada, documentando cada paso técnico relevante y asegurando que el sistema quedara disponible para las pruebas funcionales y validación por parte del equipo del Ministerio de Trabajo

Durante el proceso de despliegue del sistema SISGESTION se identificaron varios aspectos relevantes que deben ser tenidos en cuenta para la continuidad del proyecto, su estabilización y eventual puesta en producción:

1. Reportes precargados con información desactualizada: Los reportes incluidos en la solución presentan un alto volumen de información precargada proveniente del Departamento Nacional de Planeación (DNP), lo cual limita su aplicabilidad directa en el contexto del Ministerio de Trabajo. Estos reportes requieren ser revisados y ajustados tanto a nivel de contenido como de formato para alinearse con las necesidades específicas del Ministerio.
2. Necesidad de depuración y actualización de datos: Se evidenció la presencia de datos "quemados" o estáticos en diversas secciones de la aplicación, incluyendo formularios, parámetros y reportes, lo que podría generar inconsistencias si no se actualizan adecuadamente. Será necesario un proceso de depuración para limpiar o sustituir esta información por datos oficiales y dinámicos.
3. Sesión técnico-funcional de entrega: Con el fin de formalizar la entrega del sistema SISGESTION a las áreas funcionales del Ministerio de Trabajo, se recomienda realizar una sesión técnica/funcional que tendría como objetivo presentar el estado final del despliegue, validar que el sistema se encuentra disponible en el ambiente de pruebas, y dejar constancia de los pendientes identificados durante la instalación. Esta sesión también permitirá oficializar la transferencia del sistema para su validación y uso por parte del equipo del Ministerio.
4. Alcance del despliegue: Es importante resaltar que el alcance de este despliegue corresponde únicamente a la instalación técnica del sistema y su puesta en marcha en un entorno de pruebas. Las actividades de ajuste funcional, adecuación del código fuente, integración con sistemas existentes y mejoras de rendimiento deberán contemplarse en fases posteriores.

El equipo de Servicios Centrales de la UT Gestión TIC 2023, se permitió dar visibilidad a la entidad de los siguientes aspectos para tener en cuenta con respecto al sistema de información a nivel técnico:

- El sistema de información tiene una implementación muy similar a varias aplicaciones desarrolladas en lenguaje .NET que posee actualmente la entidad.
- El sistema de información viene de una transición de versionamiento de sistemas operativos y base de datos deprecado (versiones 2012) que actualmente, la versión que está siendo desarrollada y por liberar por parte del DNP (versión 2.0) posee una actualización a versiones 2019.
- El equipo de Servicios Centrales de la UT se encuentra en proceso de actualización a versionamiento 2022 de Sistema Operativo Windows y de Base de datos SQL Server.
- SISGESTION tiene aval y despliegue correcto en sistema operativo y base de datos 2019, no se ha probado por parte del DNP en versión 2022. Pueden

existir problemas de compatibilidad, en principio debería funcionar de manera adecuada, pero lo ideal es que la aplicación sea probada en entornos 2022 para validar el funcionamiento adecuado en esta versión de sistema operativo y de base de datos.

- El sistema de información SISGESTION tiene una dependencia en su desarrollo con un componente INFRAGISTIC el cual es un componente que según informa el equipo de Tecnología de DNP, se encuentra fuera de soporte y se encuentran en etapa de desarrollo para eliminar la dependencia de este componente, el cual genera problemas de compatibilidad con los navegadores actuales (Google Chrome, Microsoft Edge y Mozilla Firefox) lo cual degrada la experiencia del usuario final, ya que la herramienta no se comporta de manera adecuada. o La versión que el DNP liberará (versión 2.0) posee actualizaciones que permite la compatibilidad y uso adecuado del sistema de información SISGESTION en Microsoft Edge y Google Chrome sin inconvenientes, pero es importante precisar que continua con el componente Infragistics que a futuro quedará obsoleto en un corto o mediano plazo.

    - La aplicación se encuentra desarrollada en .Net Framework 4.5 y la versión de SISGESTION que actualmente están liberando esta actualizada a versión .Net Framework 4.7. La última versión disponible de .Net Framework es 4.8.1. La recomendación para aplicaciones nuevas es la migración a .Net Core o .Net 6/8. o Lo anteriormente mencionado requiere un proceso de reescritura del código fuente de la aplicación. Esto en función de que la aplicación no se quede obsoleta al corto plazo por los versionamientos de componente .NET Framework. o Es importante precisar que la obsolescencia de este tipo de componentes se ven reflejadas en vulnerabilidades de seguridad sobre las aplicaciones por falta de soporte por parte de su fabricante, en este caso Microsoft, que recomienda el desarrollo y la actualización de las aplicaciones a los versionamientos mencionados.
    - El estado actual de .NET Framework 4.7 por parte de Microsoft es el siguiente:
    - Solamente recibe actualizaciones o parches de seguridad hasta 2027 como máximo.
    - Tiene soporte limitado por parte de fabricante (Microsoft)
    - Se recomienda migrar a .NET 4.8 o .NET 6/8
    - Es importante que las áreas funcionales/misionales de la entidad validen los flujos de cada proceso dentro del sistema de información y que estos se adecuen a su necesidad.
    - En caso de que exista alguna variante en el flujo, algún paso dentro del procedimiento, actividad adicional o que se deba eliminar implicaría intervenir el código de la aplicación. Es decir, la entidad debe contar con un equipo de desarrollo de software dedicado explícitamente a adecuar el sistema de información en términos de lógica de programación para que se alinee a las necesidades funcionales y misionales del Ministerio. o En caso de no recibir

actualizaciones del software por parte del DNP, este equipo de desarrollo de software debe realizar el mantenimiento de la aplicación a nivel de la capa de aplicación (en caso de que surjan necesidades adicionales, modificación de módulos existentes, creación de nuevos flujos y demás).

- Si la aplicación es intervenida en su lógica de programación por un equipo de Ministerio del Trabajo y en el futuro el DNP libera actualizaciones las cuales el Ministerio es aplicable, se deben realizar pruebas de compatibilidad entre las actualizaciones liberadas por el DNP y las adecuaciones realizadas por el equipo de Ministerio del Trabajo.
- El sistema de información del DNP cuenta con servicios de Firma electrónica con servicios de firma centralizada, el cual es un servicio que garantiza Integridad y autenticidad en los procesos de firma de documentos electrónicos.
- Actualmente el Ministerio no cuenta con estos servicios adquiridos por lo cual, si se quiere implementar SISGESTION con todas las funcionalidades que DNP posee actualmente y libera en su versión 2.0. Se deben adquirir los servicios de firma electrónica, firma centralizada y certificados digitales para los actores dentro de la entidad que actuarían como firmantes dentro del sistema de información.
- En caso de no acogerse a la modalidad de firma digital, se debería modificar el flujo para cambiar el paso de firma por un paso de aprobación o firma mecánica. Esto también implicaría modificar el software para que se adecue a la decisión que tome la entidad.
- Ejecución de Scripts para creación de roles Estándar de acuerdo con lo remitido por parte del equipo de DNP.
- Se realizó conexión exitosa con el LDAP de la entidad, por lo cual los usuarios creados en SISGESTIÓN pueden iniciar sesión con su usuario y contraseña de dominio tras la creación del usuario en SISGESTION con el mismo domain name.

Es importante mencionar que, se plantea el siguiente procedimiento, pero es decisión estrictamente de la entidad el proceder.

- Aspectos técnicos: ya fueron gestionados todos los ítems que pueden depender del Grupo de Soporte Informático y el equipo de servicios centrales de la UT.
- Ya se configuró todo el entorno de servidores y base de datos para pruebas.
- Se actualizó la imagen institucional del sistema.
- Se ejecutaron los scripts de creación de roles.
- Se realizó configuración con Active Directory.
- Se suministraron usuarios administradores para creación de usuarios.
- Aspectos funcionales: Se deben establecer los líderes funcionales del sistema de información y de los procedimientos asociados dentro del sistema de información.

- Se deben establecer los usuarios que se deben crear en SISGESTIÓN para asignación de roles para posterior interacción dentro del sistema de información.
- Se deben crear los flujos tanto internos como el ya existente dentro del sistema de información para definir una ruta crítica de los módulos o módulos de SISGESTION, así como inicio de las pruebas dentro del sistema de información por parte de los usuarios.

Como se mencionó anteriormente, esto es a modo de sugerencia, la entidad puede sugerir e implementar una ruta crítica totalmente diferente que se alinee con los intereses institucionales de la entidad.

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 programa migración de versión para mediados de diciembre de 2025, 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.

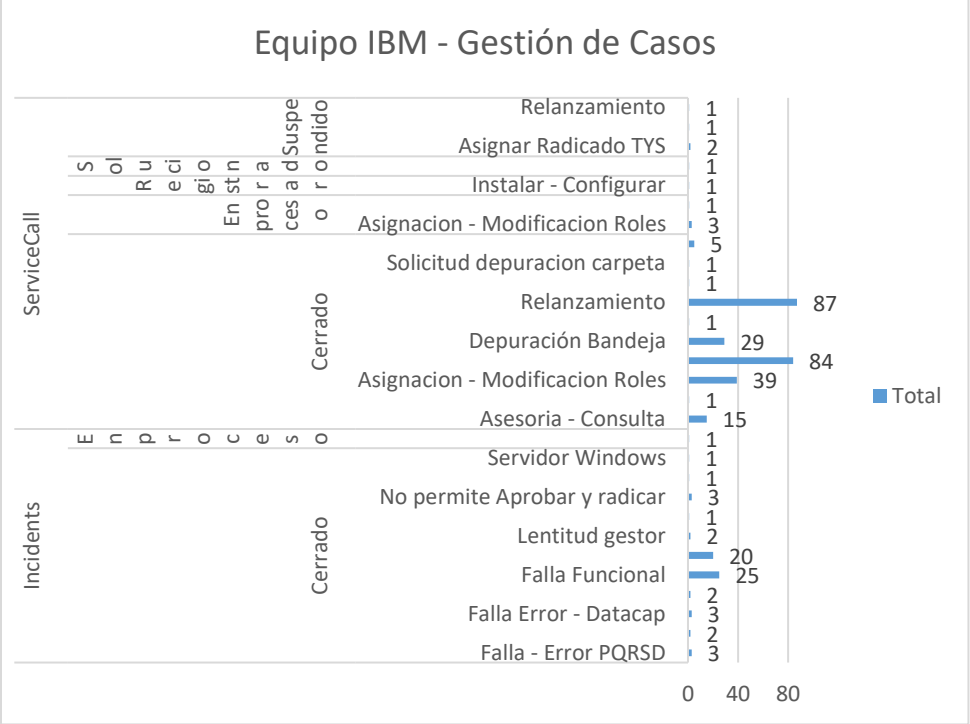


Ilustración 73 Gestión Casos IBM

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 (87 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 (84 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 2024.
- Radicar una solicitud - Depuración de Bandeja (29 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.
- Radicar una solicitud - Asesoría/Consulta (15 casos) Consultas relacionadas con procesos del Gestor Documental en las que los usuarios reportan errores durante la radicación o al intentar subir documentos, lo cual impide completar correctamente la solicitud.
- Falla radicación (20 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.

Se observa una disminución notable sobre el reporte de requerimientos del gestor documental.

Se realizó cambio de inactivación del campo referido de acuerdo con lo solicitado por el área funcional generando el siguiente comunicado: *Por medio de la presente, informamos que, a partir del* ***lunes 1 de diciembre de 2025****, la sección* ***"Radicados Referidos"*** *ha sido deshabilitada en todas las pantallas del proceso del gestor documental.*

Esta medida obedeció a la necesidad de garantizar la integridad y la precisión de los datos en los informes de gestión a nivel documental. Se identificó que la referenciación de radicados afectaba la trazabilidad y la consolidación de reportes.

La deshabilitación tuvo como finalidad fundamental estandarizar y formalizar los procedimientos de cierre de peticiones. A partir de ahora, todas las áreas de negocio del Ministerio.

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 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.

A continuación, se expone la arquitectura por componente de la solución de gestor documental:

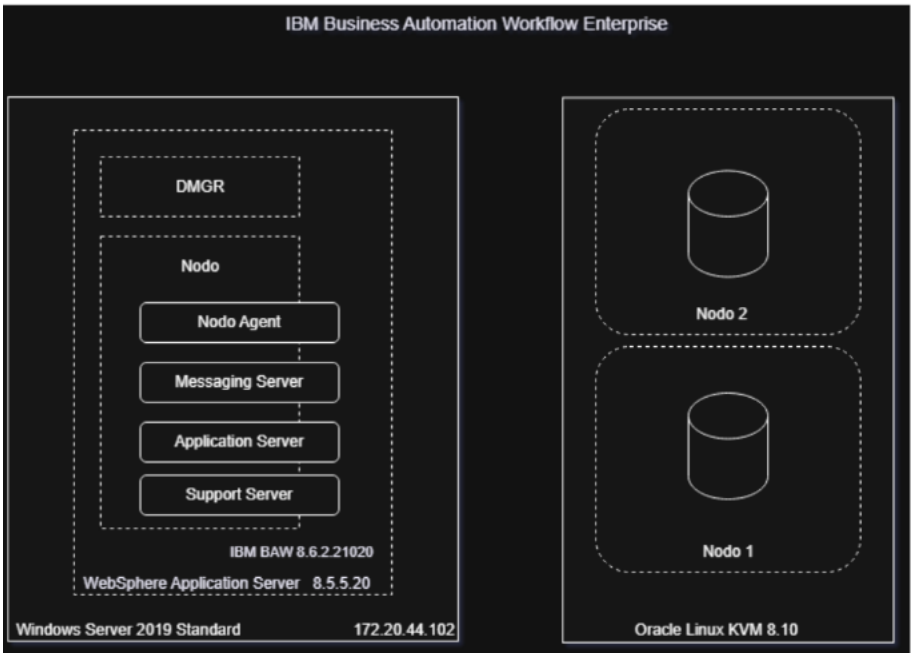


Ilustración 74 Diagrama BP

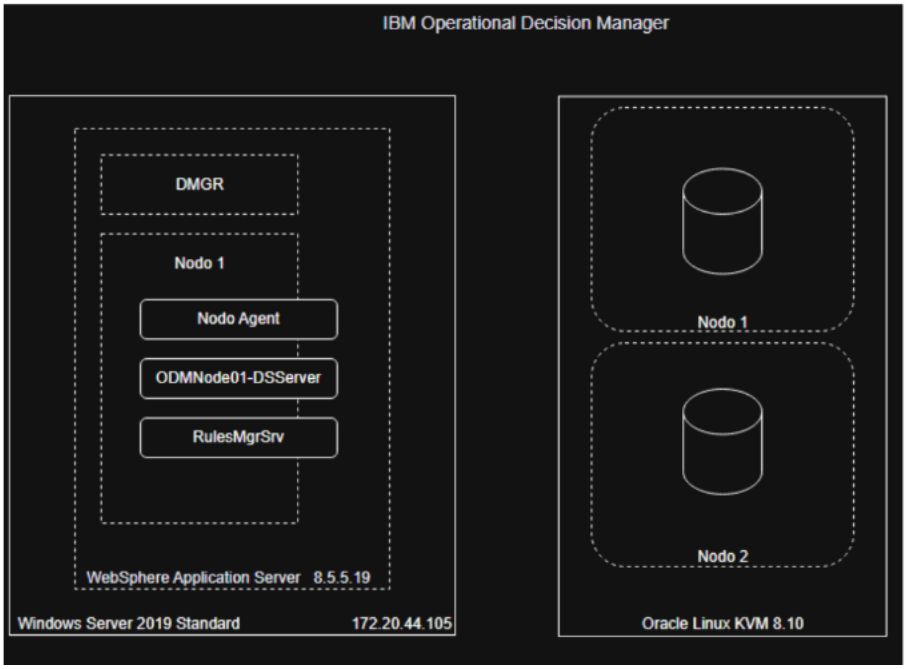


Ilustración 75 Diagrama ODM

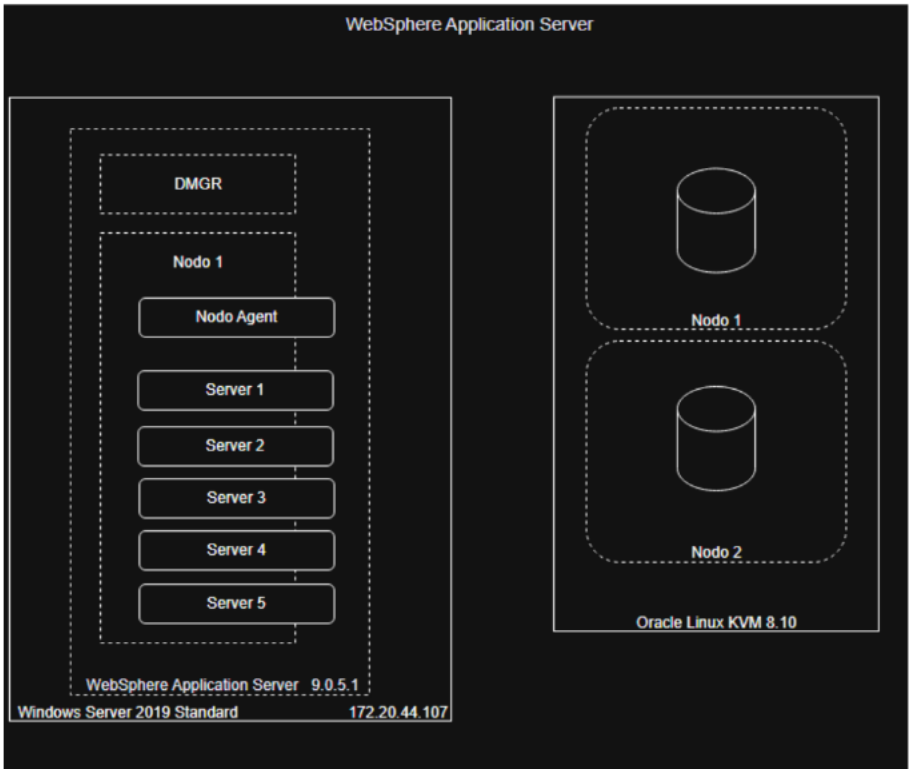


Ilustración 76 Diagrama WASND

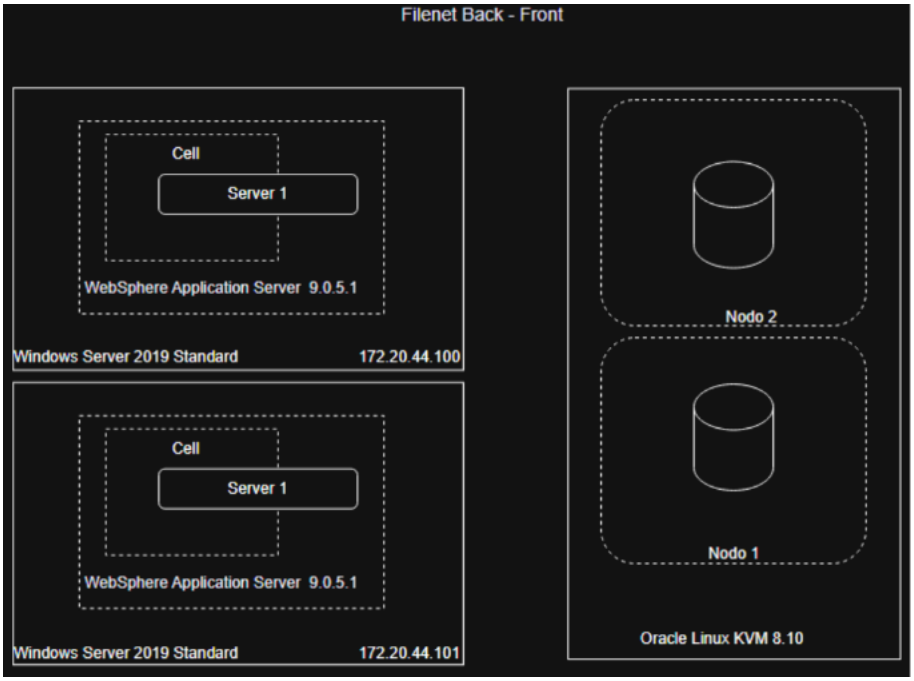


Ilustración 77 Diagrama FileNet Front

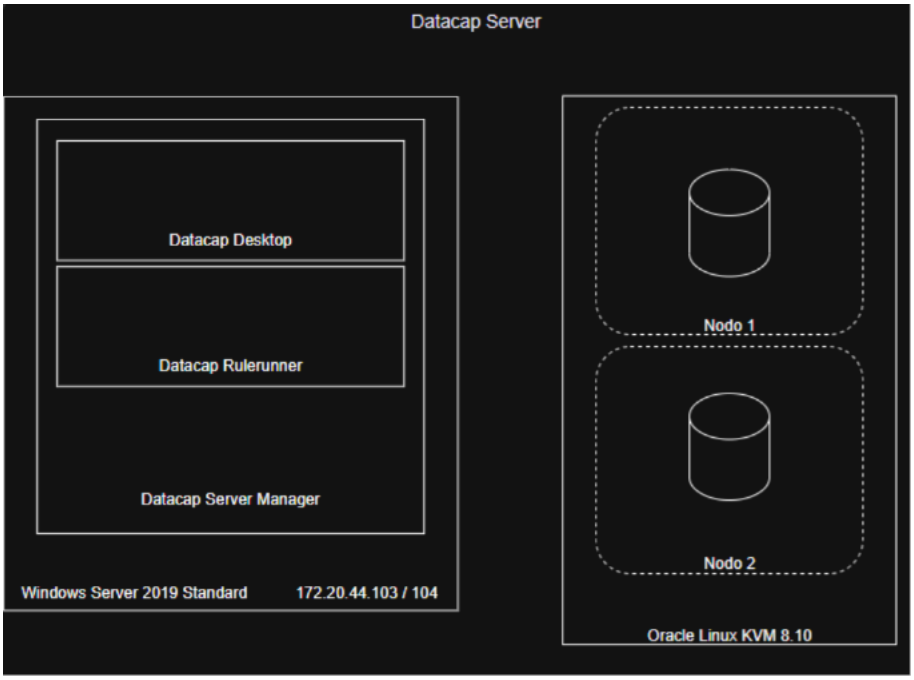


Ilustración 78 Diagrama Datacap

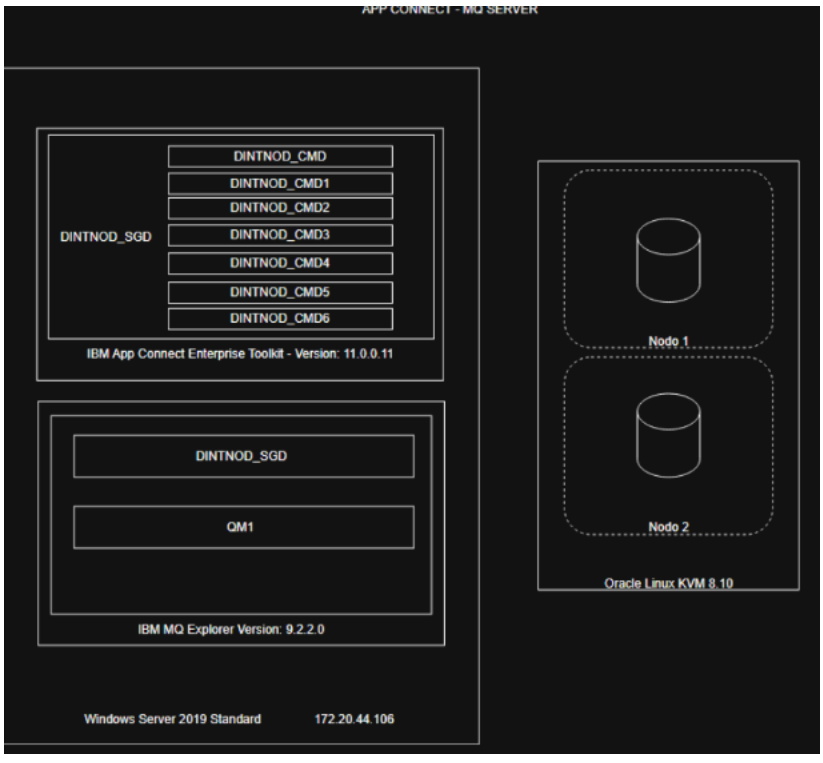


Ilustración 79 Diagrama App Connect

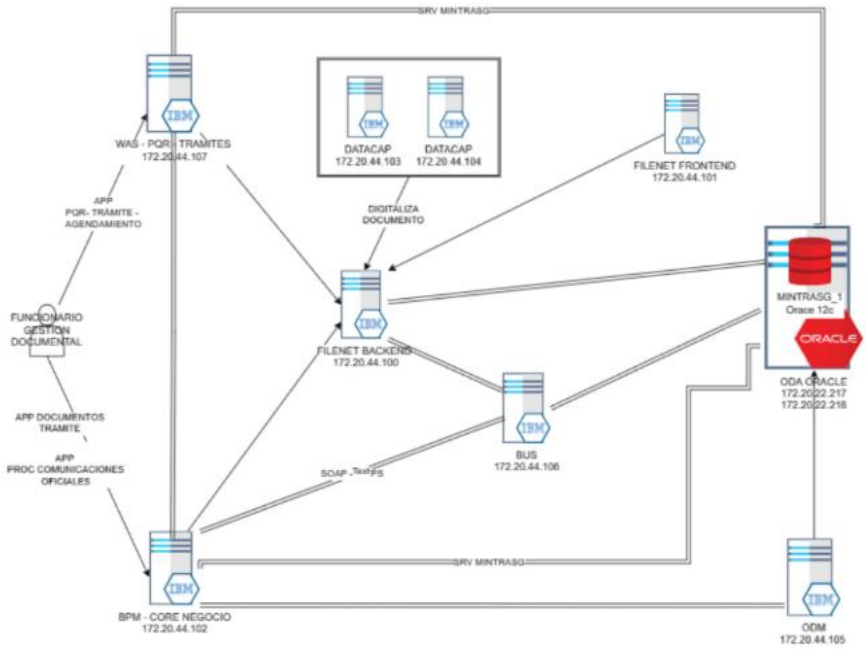


Ilustración 80 Arquitectura Gestor Documental

Rol	Recursos de la maquina	Discos	VCPU
WASND	Windows server 2019, Procesador AMD EPYC 7713 64-Core Processor	C: 170 GB, E: 100 GB	7
BUS - AppConnect	Windows server 2019, Procesador AMD EPYC 7713 64-Core Processor	C: 150 GB	3
ODM	Windows server 2019, Procesador AMD EPYC 7713 64-Core Processor	C: 100 GB, E: 50 GB	3
DATACAP	Windows server 2019, Procesador AMD EPYC 7713 64-Core Processor	C: 150 GB	5
DATACAP	Windows server 2019, Procesador AMD EPYC 7713 64-Core Processor	C: 100 GB, E: 50 GB, F 500 GB, H: 500 GB	8
BAW	Windows server 2019, Procesador AMD EPYC 7713 64-Core Processor	C: 150 GB, D: 100 GB	5
Filenet FRONT	Windows server 2019, Procesador AMD EPYC 7713 64-Core Processor	C: 150 GB , D: 119 GB	8
Filenet BACK	Windows server 2019, Procesador AMD EPYC 7713 64-Core Processor	C: 150 GB , D: 119 GB, E: 7TB	8

Ilustración 81 Capacidades VM Gestor Documental

Nivel de Servicio: Software Update License & Support

Descripción del Producto	CSI #	Cant.	Metrica de Licencia	Nivel/Tipo de Licencia
Oracle Database Enterprise Edition - Processor Perpetual	20331608	4		FULL USE
Oracle WebLogic Suite - Processor Perpetual	20331608	3		FULL USE
Oracle Database Enterprise Edition - Processor Perpetual	20941023	2		FULL USE
Oracle WebLogic Suite - Processor Perpetual	21069467	3		FULL USE
Oracle Diagnostics Pack - Processor Perpetual	22682625	4		FULL USE
Oracle Tuning Pack - Processor Perpetual	22682625	4		FULL USE
Oracle Database Enterprise Edition - Processor Perpetual	25055449	2		FULL USE

Ilustración 82 Licenciamiento Oracle

Business Partner de la transaccion: **Indra Colombia Ltda**

Cantidad	Número de Pieza	Descripción	Fecha de cobertura de la Subscripción y Soporte de Software
70	D03S0LL	IBM App Connect Standard Processor Value Unit (PVU) License + SW Subscription & Support 12 Months	29-Nov-2024 - 30-Nov-2025
3	D20RULL	IBM Cloud Pak for Business Automation Virtual Processor Core License + SW Subscription & Support 12 Months	29-Nov-2024 - 30-Nov-2025

www.rational.com/licensing

Número de Cliente de IBM: **323500**

Recursos Web importantes o útiles:
Información sobre Passport Advantage, acceso a sitios seguros del cliente, formación, etc.: **ibm.com/software/passportadvantage**
Acuerdo Internacional de Programas Bajo Licencia de IBM y documentos de Información sobre licencia del producto: **ibm.com/software/sla**
Sitio web de Soporte de Software de IBM: **https://www.ibm.com/software/support/handbook.html** *Número de Cliente de IBM:* **323500**

Cantidad	Número de Pieza	Descripción	Fecha de cobertura de la Subscripción y Soporte de Software
7	D20RULL	IBM Cloud Pak for Business Automation Virtual Processor Core License + SW Subscription & Support 12 Months	29-Nov-2024 - 30-Nov-2025

www.rational.com/licensing

70	D55WJLL	IBM WebSphere Application Server Network Deployment Processor Value Unit (PVU) License + SW Subscription & Support 12 Months	29-Nov-2024 - 30-Nov-2025

Cantidad	Número de Pieza	Descripción	Fecha de cobertura de la Subscripción y Soporte de Software
210	E04NRLL	IBM App Connect Standard Processor Value Unit (PVU) Annual SW Subscription & Support Renewal 12 Months	01-Dic-2024 - 30-Nov-2025
1	E0BRLLL	IBM Integration Designer per Authorized User Annual SW Subscription & Support Renewal	01-Dic-2024 - 30-Nov-2025

Cantidad	Número de Pieza	Descripción	Fecha de cobertura de la Subscripción y Soporte de Software
20	E0PMHLL	IBM Cloud Pak for Business Automation Virtual Processor Core Annual SW Subscription & Support Renewal 12 Months	01-Dic-2024 - 30-Nov-2025
www.rational.com/licensing			
136	D20RWLL	IBM Cloud Pak for Business Automation Virtual Processor Core from Eligible Programs Trade Up License + SW Subscription & Support 12	29-Nov-2024 - 30-Nov-2025
www.rational.com/licensing			
1.120	E025SLL	IBM WebSphere Application Server Network Deployment Processor Value Unit (PVU) Annual SW Subscription & Support Renewal	01-Dic-2024 - 30-Nov-2025

Ilustración 83 IBM Licenciamiento

Mes	Suma de Total Instancias
Diciembre 2025	109540
Enero 2026	83242
Total acumulado	192782

Tabla 46 Suma Instancias

Mes	Suma de Total Documentos
Diciembre 2025	174277
Enero 2026	136435
Total acumulado	310712

Tabla 47 Total Docs

Mes	Suma de Total radicados
Diciembre 2025	**59671**
Enero 2026	53821
Total, acumulado	113492

Tabla 48 Total Radicados

De acuerdo con el funcionamiento actual del sistema de gestión documental, se exponen las capacidades actuales contrastadas con las capacidades requeridas a nivel de Cores asignados a las máquinas virtuales aprovisionadas para la puesta en

marcha del Gestor documental. Es importante mencionar que estas capacidades solamente enmarcan ampliación para funcionamiento del escenario actual, es decir una optimización del sistema actual sin incluir nuevos desarrollos o funcionalidades ya que estas deben ser dimensionadas y expuestas de manera específica para plasmar el crecimiento de las capacidades de los contenedores del componente IBM.

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

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

De acuerdo con este esquema de licenciamiento (únicamente para base de datos) el licenciamiento de WebLogic, Diagnostic Pack y Tuning Pack no cambiaría y no incluiría el Oracle Premier Support for Systems que es el que soporta la infraestructura física del ODA X5, pero es importante que la entidad contemple el licenciamiento de la herramienta Oracle Cloud Control, que permite la visualización en tiempo real de las bases de datos, máquinas virtuales y capas medias de Oracle. Para ello, sugerimos la importancia de validar con el proveedor de estas licencias, para que realice la aclaración de acuerdo con este dimensionamiento y que el Ministerio del trabajo, tenga claridad del costo de las licencias que requiere renovar para la vigencia 2025-2026.

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

Tabla 49 Dimensionamiento Servers IBM - Virtualización Optima

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.

Se observó un comportamiento sobre las solicitudes relacionadas con acceso a bases de datos como dbOwner o acceso remoto donde reposan los motores de base de datos, lo cual puede volcar la memoria de estos recursos tecnológicos ya que múltiples sesiones remotas en el servidor sumando la limitada capacidad de la infraestructura tecnológica actual, podría generar intermitencias, problemas en el performance o inclusive indisponibilidades no controladas, por lo cual se sugiere a la Coordinación del Grupo de Soporte Informático realizar un control sobre este tipo de solicitudes a áreas misionales/funcionales con el fin de poder estabilizar y canalizar de la mejor manera estas solicitudes para evitar problemas dentro de las aplicaciones y las bases de datos de la entidad.

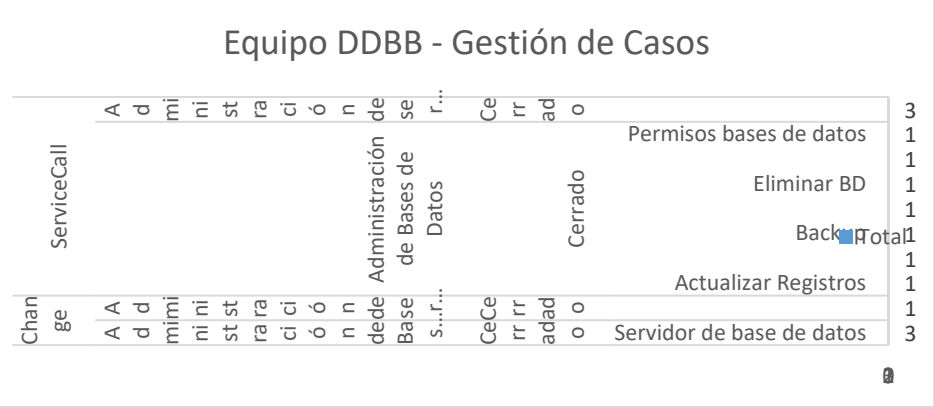


Ilustración 84 Gestión DDBB

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:

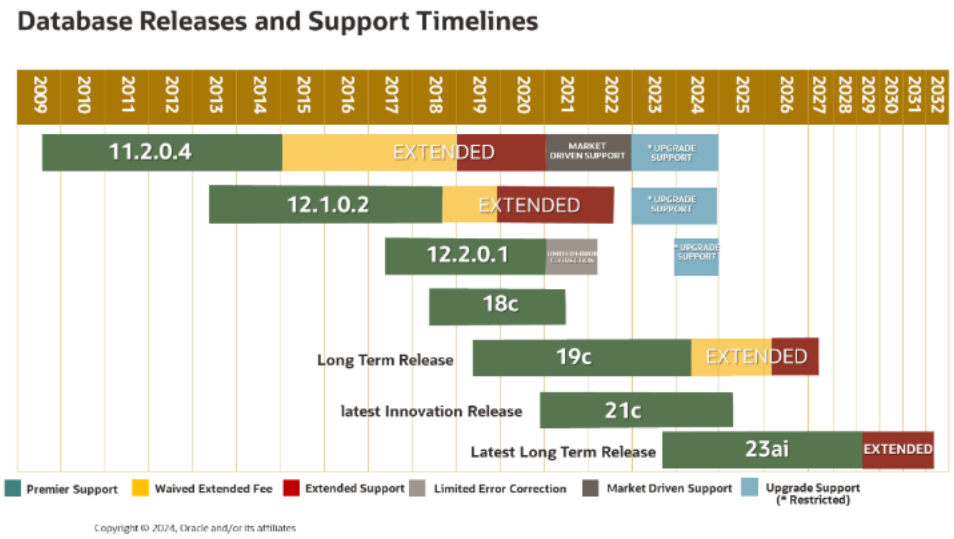


Ilustración 85 Estado Bases de Datos

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

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

Actualmente, el ministerio de trabajo tiene desplegadas sobre el ODA X5-2 un total de 7 bases de datos en versión 12c, estas bases de datos son productivas y

desarrollo en el siguiente apartado se mostrarán las aplicaciones que han sido mapeadas y que consumen conexiones sobre las bases de datos del ODA X5-2. En el siguiente apartado se listan las aplicaciones que hacen uso de las bases de datos de la entidad y que consumen su conexión mediante esquemas específicos:

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

Tabla 50 Apps & DDBB Oracle

En este apartado la información no es exacta dado que no se cuenta con un soporte donde se especifique que aplicaciones hacen uso de una base de datos o esquemas al detalle, lo que se tiene son las conexiones de servidores de aplicación Weblogic que tienen un apuntamiento sobre bases de datos del ODA x5-2 detalladamente.

Es importante mencionar, que ante un escenario de virtualización, las recomendaciones de fabrica a nivel de asignación de recursos/capacidades están asociadas a las capacidades de la infraestructura que ofrece como fabricante, es decir, las capacidades de un ODA X-10 HA suelen ser las recomendadas para cubrir un escenario de alta disponibilidad y de crecimiento de servicios. El crecimiento de las capacidades está directamente relacionado con el crecimiento de los componentes Oracle/DDBB de la propia entidad.

De acuerdo con el escenario actual de base de datos, se anexan las capacidades del ODA X-5 aprovisionado por la entidad y el uso de las capacidades para cada componente de DDBB, es decir lo disponible en el hardware de Oracle y el usado por las máquinas virtuales y bases de datos que permiten el funcionamiento actual tanto del gestor documental como de otras aplicaciones que tienen base de datos Oracle:

INST_NAME	IP	SERVER_NAME	AMBIENTE	Version_Motor	S.O	MEMORIA GB	CPU	STORAGE ASIGE GB	STORAGE USED GB	STORAGE FREE GB
mintrasg_1	172.20.22.217	mintrab89-pub	PRODUCCION	Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	Oracle Linux 4.9.2-6.2.0.3	40	12	5677	1713	3964

pliferay_1	172.20.22.217	mintrab89-pub	PRODUCCION	Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	Oracle Linux 4.9.2-6.2.0.3	4	2	235	139	95
dbmintra_1	172.20.22.217	mintrab89-pub	PRODUCCION	Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	Oracle Linux 4.9.2-6.2.0.3	8	4	2225	1967	257
DBPSIMPC_2	172.20.22.217	mintrab89-pub	PRODUCCION	Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	Oracle Linux 4.9.2-6.2.0.3	2	2	47	5	42
sigep_2	172.20.22.217	mintrab89-pub	PRODUCCION	Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	Oracle Linux 4.9.2-6.2.0.3	20	8	265	81	184
dliferay_2	172.20.22.217	mintrab89-pub	DESARROLLO	Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	Oracle Linux 4.9.2-6.2.0.3	4	4	151	71	80
mintrasd	172.20.22.217	mintrab89-pub	DESARROLLO	Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	Oracle Linux 4.9.2-6.2.0.3	2	16	390	186	204
Dbmintrab	172.20.22.107	mintrab32	PRODUCCION	Oracle Database 11g Enterprice edition Release 11.2.0.1.0	Windows Server 2012 R2	13	10	41	19	22
Inventarios	172.20.22.107	mintrab32	PRODUCCION	Oracle Database 11g Enterprice edition Release 11.2.0.1.0	Windows Server 2012 R2	13	10	14	7	7

Tabla 51 Escenario de Capacidades Oracle - Estado de consumo Actual

	MEMORIA GB	CPU	STORAGE ASIG GB	STORAGE USED GB	STORAGE FREE GB
TOTAL DE RECURSOS USADOS	**106**	**68**	**9043**	**4189**	**4855**

Tabla 52 Escenario de Capacidades Oracle - Total de recursos empleados

TRASACCIONALIDAD BASES DE DATOS PRODUCTIVAS ODA X5-2:

BASE DE DATOS MINTRASG (Gestor documental):

DB Name	DB Id	Instance	Inst num	Startup Time	Release	RAC
MINTRASG	941530115	mintrasg_1	1	30-Sep-24 20:09	12.1.0.2.0	YES

Host Name	Platform	CPUs	Cores	Sockets	Memory (GB)
mintrab89-pub	Linux x86 64-bit	16	16	1	157.15

	Snap Id	Snap Time	Sessions	Cursors/Session	Instances
Begin Snap:	65817	10-Oct-24 01:00:46	157	18.1	1
End Snap:	66017	18-Oct-24 09:00:42	331	37.2	1
Elapsed:		11,999.94 (mins)			
DB Time:		32,771.09 (mins)			

Ilustración 86 Información base de datos – Servidor

Estadísticas de uso de CPU: *Información referente a la carga que ha tenido la CPU a nivel de host como a nivel de instancia en el periodo de tiempo reportado.*

NUM_CORES_ASIGNADOS	DESCRIPTION
12	number of CPUs for this instance

Host CPU

CPUs	Cores	Sockets	Load Average Begin	Load Average End	%User	%System	%WIO	%Idle
16	16	1	31.49	46.70	15.2	6.2	72.3	78.2

Instance CPU

%Total CPU	%Busy CPU	%DB time waiting for CPU (Resource Manager)
8.4	38.6	0.0

Ilustración 87 Estadísticas CPU

Estadísticas de uso Memoria: Se puede observar el uso del recurso de memoria durante el periodo reportado.

Memory Statistics

	Begin	End
Host Mem (MB):	160,925.8	160,925.8
SGA use (MB):	36,864.0	36,864.0
PGA use (MB):	922.9	1,588.5
% Host Mem used for SGA+PGA:	23.48	23.89

Ilustración 88 Estadísticas Memoria

Estadísticas del shared pool: La siguiente estadística muestra el tamaño utilizado para el almacenamiento de las estructuras compartidas por la sesiones de la base de datos (sentencias sql, objetos de diccionario y estructuras de ejecución) como tal se puede dar un diagnóstico para poder evaluar el aumento de la SGA para optimizar el uso de memoria y diagnosticar problemas relacionados con la sobre carga o subutilización del shared pool, para el caso de la BD MINTRASG (Gestor Documental) se observa que los usos de la SGA son idénticos entre los snapshots del reporte.

Shared Pool Statistics

	Begin	End
Memory Usage %:	87.94	89.09
% SQL with executions>1:	96.50	95.79
% Memory for SQL w/exec>1:	95.37	93.86

Ilustración 89 Estadísticas Pool compartido

Tamaño base de datos MINSTRASG:



Ilustración 90 Tamaño DDBB

Actualmente la BD MINTRASG tiene parametrizada 5.7 TB a nivel de almacenamiento de los cuales 1,8 TB están en uso y se tiene libre 3,8 TB.

Tamaño de esquemas de base de datos:

ESQUEMA	SIZE_GB
BPMDBA	661,09
ERK	381,59
SGD	328,95
BDWDBA	195,48
AUDSYS	131,67
RPUA	76,38
SYS	59,8
FNT_OS	54,93
CORR_ENG	3,63
LIFERAYPRU	2,57
CORR_ADM	0,84
FNT_FPOS	0,59
SQLTXPLAIN	0,36
MEDBA	0,25
SYSTEM	0,12
FNT_GCD	0,09
CMNDBA	0,08
XDB	0,06
RMAN	0,02
WMSYS	0,01
FNT_ICN	0,01
CORRESPONDENCIA_FP	0
RESDB	0
CORRESPONDENCIA_ADM	0
NAVDBA	0
CORRESPONDENCIA_ENG	0
GSMADMIN_INTERNAL	0
OUTLN	0
ODMADMIN	0
DBSNMP	0

Ilustración 91 Tamaño Esquema DDBB

Los esquemas resaltados son los que tienen mayor consumo a nivel de almacenamiento sobre la base de datos.

Graficas de rendimiento de la Base de datos MINSTRASG



Ilustración 92 Rendimiento DDBB

2. BASE DE DATOS DBMINTRA:

Información base de datos – Servidor:

DB Name	DB Id	Instance	Inst num	Startup Time	Release	RAC
DBMINTRA	761112416	dbmintra_1	1	10-Sep-24 22:09	12.1.0.2.0	YES

Host Name	Platform	CPUs	Cores	Sockets	Memory (GB)
mintrab89-pub	Linux x86 64-bit	16	16	1	157.15

	Snap Id	Snap Time	Sessions	Cursors/Session	Instances
Begin Snap:	29927	10-Oct-24 01:00:09	146	1.6	1
End Snap:	30128	18-Oct-24 10:00:51	157	4.1	1
Elapsed:		12,060.70 (mins)			
DB Time:		3,683.80 (mins)			

Ilustración 93 DDBB por Server

Estadísticas de uso de CPU: Información referente a la carga que ha tenido la CPU a nivel de host como a nivel de instancia en el periodo de tiempo reportado.

NUM_CORES_ASIGNADOS	DESCRIPTION
4	number of CPUs for this instance

Host CPU

CPUs	Cores	Sockets	Load Average Begin	Load Average End	%User	%System	%WIO	%Idle
16	16	1	30.35	51.90	15.3	6.3	72.1	78.0

Instance CPU

%Total CPU	%Busy CPU	%DB time waiting for CPU (Resource Manager)
1.8	8.4	0.6

Ilustración 94 Host e Instancia CPU

Estadísticas de uso Memoria: Se puede observar el uso del recurso de memoria durante el periodo reportado.

Memory Statistics

	Begin	End
Host Mem (MB):	160,925.8	160,925.8
SGA use (MB):	8,192.0	8,192.0
PGA use (MB):	684.4	982.3
% Host Mem used for SGA+PGA:	5.52	5.70

Ilustración 95 Estadísticas Memoria

Shared pool, para el caso de la BD DBMINTRA (Gestor Documental) se observa que los usos de la SGA son idénticos entre los snapshots del reporte.

Shared Pool Statistics

	Begin	End
Memory Usage %:	89.41	92.91
% SQL with executions>1:	98.17	86.11
% Memory for SQL w/exec>1:	98.79	88.87

Ilustración 96 Estadística Shared Pool

Tamaño base de datos DBMINTRA:

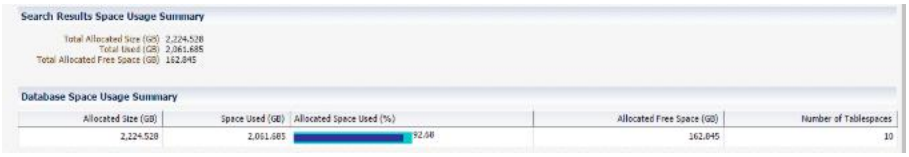


Ilustración 97 Tamaño DDBB DBMINTRA

Actualmente la BD DBMINTRA tiene parametrizada 2.2 TB a nivel de almacenamiento de los cuales 2,0 TB están en uso y se tiene libre 162,8 GB.

Tamaño de esquemas de base de datos:

ESQUEMA	SIZE_GB
IVCMI3	1936,81
NEWIVCMI	78,99
LIFERAYPRO	21,11
SIMPC	10,31
SYS	6,7
FILCODEV	4,23
IVCDASHBOARD	0,72
AUDSYS	0,3
RUI	0,09
RUIPRU	0,07
XDB	0,06
SYSTEM	0,03
DBRNFL	0,02
RMAN	0,01
WMSYS	0,01
SIMPCDES	0,01
DBSNMP	0
OUTLN	0
GSMADMIN_INTERNAL	0

Ilustración 98 Tamaño Esquema DDBB

Como se puede observar en la imagen anterior se muestra el tamaño de los esquemas de mayor a menor, para este caso el esquema IVCMT3 tiene el mayor tamaño de 1.9 TB

Graficas de rendimiento de la Base de datos MINSTRASG



Ilustración 99 Rendimiento DDBB MINTRASG

Esta base de datos se mantiene estable en los consumos, por lo cual los parámetros a nivel de memoria y CPU son óptimos para su funcionamiento.

BASE DE DATOS PLIFERAY (PORTAL WEB):

Información base de datos – Servidor:

DB Name	DB Id	Instance	Inst num	Startup Time	Release	RAC
PLIFERAY	1933304249	pliferay_1	1	10-Sep-24 22:09	12.1.0.2.0	YES

Host Name	Platform	CPUs	Cores	Sockets	Memory (GB)
mintrab89-pub	Linux x86 64-bit	16	16	1	157.15

	Snap Id	Snap Time	Sessions	Cursors/Session	Instances
Begin Snap:	65855	10-Oct-24 01:00:34	134	8.8	1
End Snap:	66056	18-Oct-24 10:00:40	129	6.6	1
Elapsed:		12,060.09 (mins)			
DB Time:		2,584.71 (mins)			

Ilustración 100 Información DDBB PLIFERAY

Estadísticas de uso de CPU: Información referente a la carga que ha tenido la CPU a nivel de host como a nivel de instancia en el periodo de tiempo reportado.

NUM_CORES_ASIGNADOS	DESCRIPTION
4	number of CPUs for this instance

Host CPU

CPUs	Cores	Sockets	Load Average Begin	Load Average End	%User	%System	%WIO	%Idle
16	16	1	31.10	52.69	15.3	6.3	72.1	78.0

Instance CPU

%Total CPU	%Busy CPU	%DB time waiting for CPU (Resource Manager)
1.2	5.4	0.5

Ilustración 101 Host e Instancia CPU

Estadísticas de uso Memoria: Se puede observar el uso del recurso de memoria durante el periodo reportado.

Memory Statistics

	Begin	End
Host Mem (MB):	160,925.8	160,925.8
SGA use (MB):	4,096.0	4,096.0
PGA use (MB):	1,141.2	822.6
% Host Mem used for SGA+PGA:	3.25	3.06

Ilustración 102 Estadísticas Memoria

Shared pool, para el caso de la BD PLIFERAY (Portal Web) se observa que los usos de la SGA son idénticos entre los snapshots del reporte.

Shared Pool Statistics

	Begin	End
Memory Usage %:	93.57	93.40
% SQL with executions>1:	93.41	96.69
% Memory for SQL w/exec>1:	92.14	92.26

Ilustración 103 Estadísticas Shared Pool

Tamaño base de datos PLIFERAY:



Ilustración 104 Tamaño DDBB PLifeRay

Actualmente la BD PLIFERAY tiene parametrizada 236,505 GB a nivel de almacenamiento de los cuales 60 GB están en uso y se tiene libre 94,4 GB.

Tamaño de esquemas de base de datos:

ESQUEMA	SIZE_GB
PERFSTAT	48,61
LIFERAYPRO	24,07
SIMPCPRU	23,92
LIFERAYPRU	23,79
FILCODEV	5,8
FILCODEV2020	5,35
FILCOPRU	5,21
SYS	3,41
AUDSYS	1,84
EMPRENDIMIENTOP	0,28
XDB	0,06
SYSTEM	0,05
WMSYS	0,01
RMAN	0,01
SDMX	0,01
DBSNMP	0
OUTLN	0
GSMADMIN_INTERNAL	0

Ilustración 105 Tamaño Esquemas DDBB

Como se puede observar en la imagen anterior se muestra el tamaño de los esquemas de mayor a menor, para este caso el esquema PERFSTAT, LIFERAYPRO, SIMPCPRU, LIFERAYPRU tiene el mayor consumo a nivel de almacenamiento.

Graficas de rendimiento de la Base de datos PLIFERAY

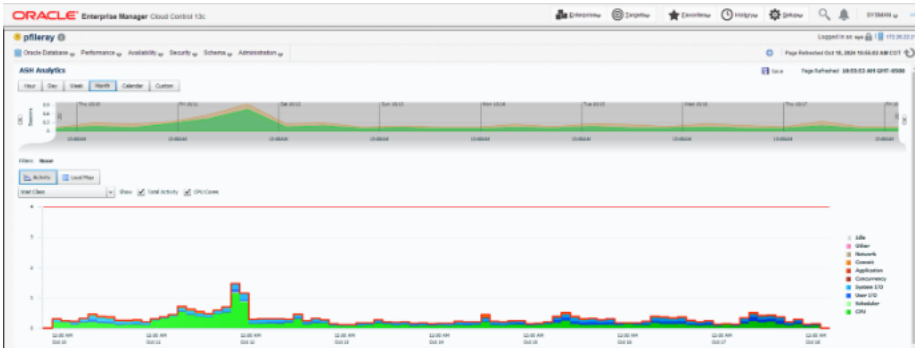


Ilustración 106 Rendimiento DDBB PlifeRay

La base de datos PLIFERAY se mantiene estable en los consumos, revisando el histórico de rendimiento se puede ver que sus cargar de uso están en promedio sobre 2 sesiones por lo cual los parámetros a nivel de memoria y CPU son óptimos para su funcionamiento.

BASE DE DATOS SIGEP (NOMINA):

Información base de datos – Servidor:

DB Name	DB Id	Instance	Inst num	Startup Time	Release	RAC
SIGEP	4059161030	sigep_1	1	14-Feb-20 21:02	12.1.0.2.0	YES

Host Name	Platform	CPUs	Cores	Sockets	Memory (GB)
mintrab90-pub	Linux x86 64-bit	16	16	1	157.15

	Snap Id	Snap Time	Sessions	Cursors/Session	Instances
Begin Snap:	17850	17-Feb-20 10:00:35	106	29.5	1
End Snap:	17851	17-Feb-20 11:00:44	114	35.2	1
Elapsed:		60.15 (mins)			
DB Time:		43.66 (mins)			

Ilustración 107 Información DDBB SIGEP

Estadísticas de uso de CPU: Información referente a la carga que ha tenido la CPU a nivel de host como a nivel de instancia en el periodo de tiempo reportado.

NUM_CORES_ASIGNADOS	DESCRIPTION
8	number of CPUs for this instance

Host CPU

CPUs	Cores	Sockets	Load Average Begin	Load Average End	%User	%System	%WIO	%Idle
16	16	1	24.09	20.40	75.3	8.4	1.0	15.0

Instance CPU

%Total CPU	%Busy CPU	%DB time waiting for CPU (Resource Manager)
1.2	1.4	0.0

Ilustración 92 Estadística Host e Instancia

Como se puede observar los consumos de CPU son en extremo bajos para esta base de datos, por lo cual es candidata para parametrizar a un CPU_COUNT=2.

Estadísticas de uso Memoria: Se puede observar el uso del recurso de memoria durante el periodo reportado.

Memory Statistics

	Begin	End
Host Mem (MB):	160,925.8	160,925.8
SGA use (MB):	18,432.0	18,432.0
PGA use (MB):	520.8	551.7
% Host Mem used for SGA+PGA:	11.78	11.80

Ilustración 93 Estadística Memoria

Shared pool, para el caso de la BD SIGEP (Nomina) se observa que los usos de la SGA son idénticos entre los snapshots del reporte.

Shared Pool Statistics

	Begin	End
Memory Usage %:	89.63	91.40
% SQL with executions>1:	73.75	77.02
% Memory for SQL w/exec>1:	81.62	79.97

Ilustración 94 Estadística Shared Pool

Tamaño base de datos SIGEP:

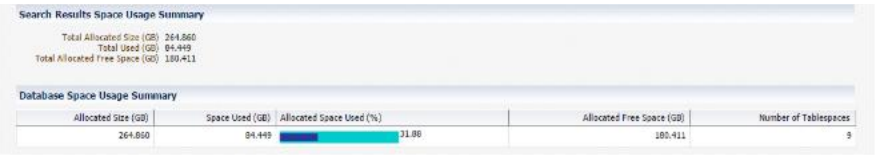


Ilustración 95 Tamaño DDBB SIGEP

Actualmente la BD SIGEP tiene parametrizada 264,860 GB a nivel de almacenamiento de los cuales 31 GB están en uso y se tiene libre 180,411 GB.

Tamaño de esquemas de base de datos:

ESQUEMA	SIZE_GB
SIGEP	25,93
DESSIGEP	24,95
PRESIGEP	24,88
SYS	5,4
SYSTEM	2,04
AUDSYS	1,4
SIPGES	0,15
HHGS_SIGEP	0,06
XDB	0,06
HV8007	0,04
HV_8007	0,03
RMAN	0,02
WMSYS	0,01
GSMADMIN_INTERNAL	0
OUTLN	0
OJVMSYS	0
SCOTT	0
DBSNMP	0

Ilustración 96 Tamaño Esquema DDBB

Como se observa en la imagen anterior se muestra el tamaño de los esquemas de mayor a menor, para este caso el esquema SIGEP, DESSIGEP, PRESIGEP tiene el mayor consumo a nivel de almacenamiento, se puede observar que en esta misma base de datos se está manejando ambientes tanto de producción, desarrollo y preproducción.

Graficas de rendimiento de la Base de datos SIGEP

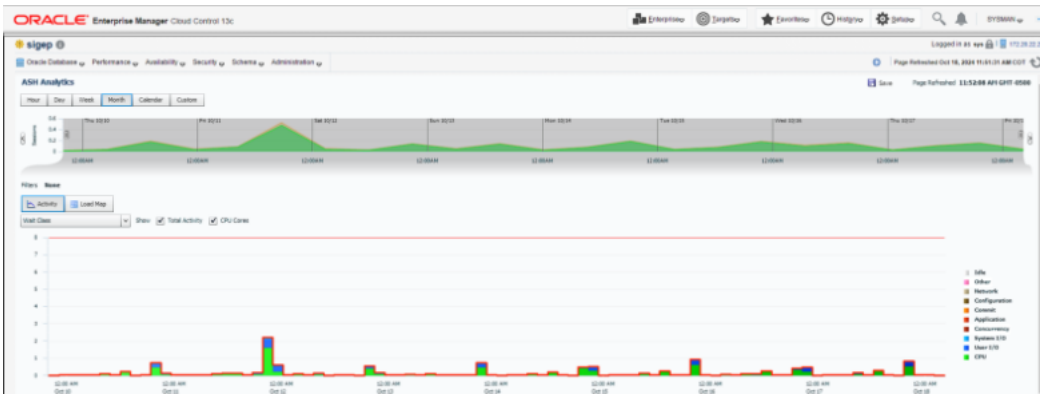


Ilustración 97 Rendimiento DDBB SIGEP

La base de datos PLIFERAY se mantiene estable en los consumos, revisando el histórico de rendimiento se puede ver que sus cargas de uso están en promedio sobre 1 a 2 sesiones por lo cual los parámetros a nivel de memoria y CPU pueden estar sobredimensionados, no obstante, como está actualmente la base de datos se comporta correctamente y tiene un óptimo funcionamiento.

BASE DE DATOS DBSIMPC (Catalogo RMAN):

Información base de datos – Servidor:

DB Name	DB Id	Instance	Inst num	Startup Time	Release	RAC
DBPSIMPC	3524191625	DBPSIMPC_2	2	10-Sep-24 22:09	12.1.0.2.0	YES

Host Name	Platform	CPUs	Cores	Sockets	Memory (GB)
mintrab89-pub	Linux x86 64-bit	16	16	1	157.15

	Snap Id	Snap Time	Sessions	Cursors/Session	Instances
Begin Snap:	45970	10-Oct-24 01:00:57	68	1.2	1
End Snap:	46173	18-Oct-24 12:00:23	70	1.2	1
Elapsed:		12,179.44 (mins)			
DB Time:		54.14 (mins)			

Ilustración 98 Información DDBB DBSIMPC

Estadísticas de uso de CPU: Información referente a la carga que ha tenido la CPU a nivel de host como a nivel de instancia en el periodo de tiempo reportado.

NUM_CORES_ASIGNADOS	DESCRIPTION
2	number of CPUs for this instance

Host CPU

CPUs	Cores	Sockets	Load Average Begin	Load Average End	%User	%System	%WIO	%Idle
16	16	1	31.88	53.84	15.6	6.3	71.8	77.7

Instance CPU

%Total CPU	%Busy CPU	%DB time waiting for CPU (Resource Manager)
0.1	0.5	1.1

Ilustración 99 Estadística CPU

Como observa en los consumos de CPU son en extremo bajos para esta base de datos, En este caso la base de datos esta con un CPU_COUNT=2 el cual está acorde según su funcionamiento.

Estadísticas de uso Memoria: Se puede observar el uso del recurso de memoria durante el periodo reportado.

Memory Statistics

	Begin	End
Host Mem (MB):	160,925.8	160,925.8
SGA use (MB):	2,048.0	2,048.0
PGA use (MB):	351.5	356.7
% Host Mem used for SGA+PGA:	1.49	1.49

Ilustración 100 Estadística Memoria

Shared pool, para el caso de la BD DBSIMPC (RMAN) se observa que los usos de la SGA son idénticos entre los snapshots del reporte.

Shared Pool Statistics

	Begin	End
Memory Usage %:	93.28	92.44
% SQL with executions>1:	90.97	94.94
% Memory for SQL w/exec>1:	94.34	96.09

Ilustración 101 Estadística Shared Pool

Tamaño base de datos DBSIMPC:



Ilustración 102 Tamaño DDBB SIMPC

Actualmente la BD DBSIMPC tiene parametrizada 46,6 GB a nivel de almacenamiento de los cuales 5 GB están en uso y se tiene libre 41,5 GB.

Tamaño de esquemas de base de datos:

ESQUEMA	SIZE_GB
SYS	2,13
SIMPCPRO	2,08
AUDSYS	0,62
RMAN	0,09
SID4	0,08
XDB	0,06
SYSTEM	0,03
WMSYS	0,01
GSMADMIN_INTERNAL	0
OUTLN	0
DBSNMP	0

Ilustración 103 Tamaño Esquema DDBB

Como observa en la imagen anterior se muestra el tamaño de los esquemas de mayor a menor, para este caso el esquema SYS, SIMPCPRO, AUDSYS, RMAN tiene el mayor consumo a nivel de almacenamiento, como tal la ocupación de dichos esquemas es muy baja, se detectó un esquema SIMPCPRO el cual tiene muy baja transaccionalidad.

Graficas de rendimiento de la Base de datos DBSIMPC

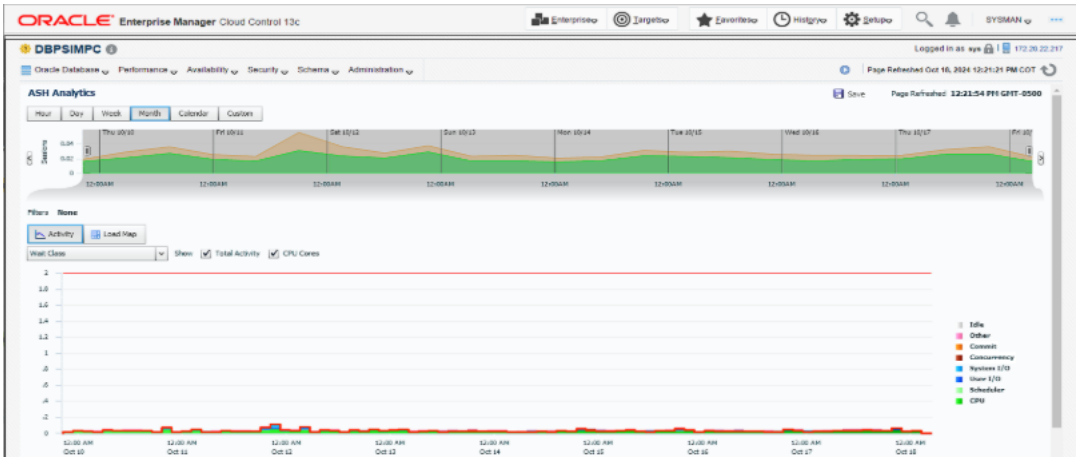


Ilustración 104 Rendimiento DDBB

La base de datos **DBSIMPC** mantiene un comportamiento muy bajo, como lo indica la gráfica el número de sesiones es caso nulo dado el que promedio de sesiones es de 0.02, el consumo está establecido con por el Catálogo de RMAN en momento de validar la catalogación de los trabajos de backups y el usuario SIMPCPRO

2. BASES DE DATOS DESARROLLO ODA X5-2

2.1 BASE DE DATOS MINTRASD (Gestor Documental):

Información base de datos – Servidor:

DB Name	DB Id	Instance	Inst num	Startup Time	Release	RAC
MINTRASD	1177930235	mintrasd	1	20-Sep-24 14:09	12.1.0.2.0	NO

Host Name	Platform	CPUs	Cores	Sockets	Memory (GB)
mintrab89-pub	Linux x86 64-bit	16	16	1	157.15

	Snap Id	Snap Time	Sessions	Cursors/Session
Begin Snap:	9195	13-Oct-24 01:00:27	54	5.6
End Snap:	9397	21-Oct-24 11:00:37	55	5.3
Elapsed:		12,120.17 (mins)		
DB Time:		1,682.96 (mins)		

Ilustración 105 Información servidor DBBB

Estadísticas de uso de CPU: Información referente a la carga que ha tenido la CPU a nivel de host como a nivel de instancia en el periodo de tiempo reportado.

NUM_CORES_ASIGNADOS	DESCRIPTION
4	number of CPUs for this instance

Host CPU

CPUs	Cores	Sockets	Load Average Begin	Load Average End	%User	%System	%WIO	%Idle
16	16	1	32.93	70.45	15.3	6.2	73.5	78.2

Instance CPU

%Total CPU	%Busy CPU	%DB time waiting for CPU (Resource Manager)
0.2	0.9	0.0

Ilustración 106 Host e Instancia CPU

Como se puede observar los consumos de CPU son en extremo bajos para esta base de datos, En este caso la base de datos esta con un CPU_COUNT=2 el cual está acorde según su funcionamiento.

Estadísticas de uso Memoria: Se puede observar el uso del recurso de memoria durante el periodo reportado.

Memory Statistics

	Begin	End
Host Mem (MB):	160,925.8	160,925.8
SGA use (MB):	1,984.0	1,984.0
PGA use (MB):	177.2	182.8
% Host Mem used for SGA+PGA:	1.34	1.35

Ilustración 107 Estadística memoria

Shared pool, para el caso de la BD DBSIMPC (RMAN) se observa que los usos de la SGA son idénticos entre los snapshots del reporte.

Shared Pool Statistics

	Begin	End
Memory Usage %:	65.48	65.40
% SQL with executions>1:	90.47	93.08
% Memory for SQL w/exec>1:	87.09	89.98

Ilustración 108 Estadística Shared Pool

Tamaño base de datos MINTRASD:



Ilustración 109 Tamaño DDBB MINTRASD

Actualmente la BD MINTRASD tiene parametrizada 390.909 GB a nivel de almacenamiento de los cuales 186,336 GB están en uso y se tiene libre 204,573 GB.

Tamaño de esquemas de base de datos:

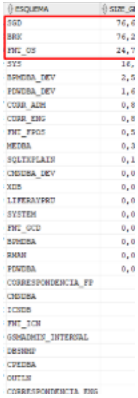


Ilustración 110 Tamaño Esquemas

Como observa en la imagen anterior se muestra el tamaño de los esquemas de mayor a menor, para este caso el esquema SGD, BRK, FNT_OS tienen el mayor consumo a nivel de almacenamiento, como tal la ocupación de dichos esquemas no es significativa.

Graficas de rendimiento de la Base de datos MINTRASD

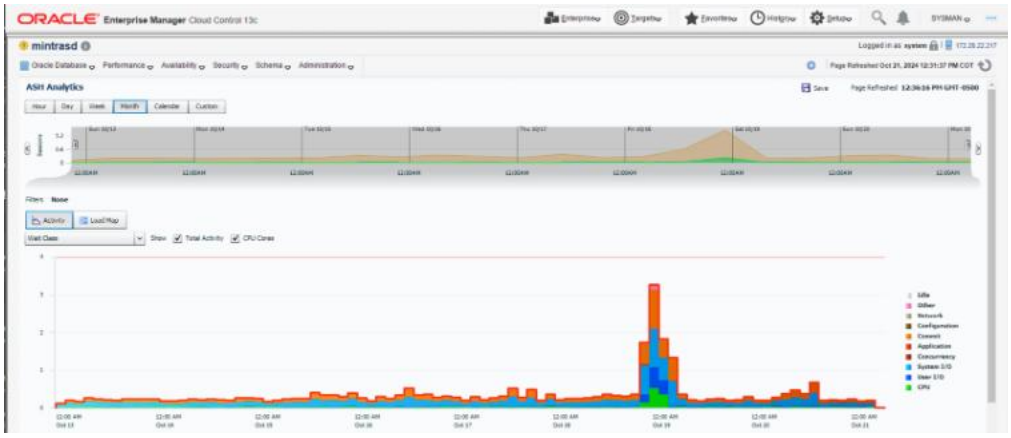


Ilustración 111 Rendimiento MINTRASD

La base de datos MINTRASD mantiene un comportamiento muy bajo, NO OBSTANTE, se puede observar para este muestreo un pico transaccional el cual fue causado por un export – import para refrescamiento de un esquema de base de datos, en general su comportamiento transaccional es bajo.

2.2 BASE DE DATOS DLIFERAY (Portal web desarrollo):

Información base de datos – Servidor:

DB Name	DB Id	Instance	Inst num	Startup Time	Release	RAC
DLIFERAY	3614794488	dliferay_2	2	10-Sep-24 22:09	12.1.0.2.0	YES

Host Name	Platform	CPUs	Cores	Sockets	Memory (GB)
mintrab89-pub	Linux x86 64-bit	16	16	1	157.15

	Snap Id	Snap Time	Sessions	Cursors/Session	Instances
Begin Snap:	45668	13-Oct-24 01:01:00	89	2.5	1
End Snap:	45872	21-Oct-24 13:00:01	109	3.0	1
Elapsed:		12,239.02 (mins)			
DB Time:		43.21 (mins)			

Ilustración 112 Información Server DDBB

Estadísticas de uso de CPU: Información referente a la carga que ha tenido la CPU a nivel de host como a nivel de instancia en el periodo de tiempo reportado.

NUM_CORES_ASIGNADOS	DESCRIPTION
4	number of CPUs for this instance

Host CPU

CPUs	Cores	Sockets	Load Average Begin	Load Average End	%User	%System	%WIO	%Idle
16	16	1	33.17	49.94	15.5	6.2	73.3	77.9

Instance CPU

%Total CPU	%Busy CPU	%DB time waiting for CPU (Resource Manager)
0.2	0.8	0.0

Ilustración 113 Host e Instancia CPU

Como se observa los consumos de CPU son en extremo bajos para esta base de datos, En este caso la base de datos esta con un CPU_COUNT=2 el cual está acorde según su funcionamiento.

Estadísticas de uso Memoria: Se puede observar el uso del recurso de memoria durante el periodo reportado.

Memory Statistics

	Begin	End
Host Mem (MB):	160,925.8	160,925.8
SGA use (MB):	4,096.0	4,096.0
PGA use (MB):	490.2	531.0
% Host Mem used for SGA+PGA:	2.85	2.88

Ilustración 114 Estadística Memoria

Shared pool, para el caso de la BD DBSIMPC (RMAN) se observa que los usos de la SGA son idénticos entre los snapshots del reporte.

Shared Pool Statistics

	Begin	End
Memory Usage %:	84.62	92.73
% SQL with executions>1:	87.97	97.19
% Memory for SQL w/exec>1:	91.26	96.62

Ilustración 115 Estadística Shared Pool

Tamaño base de datos MINTRASD:

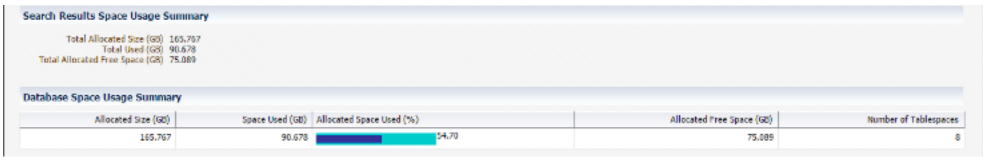


Ilustración 116 Tamaño DDBB

Actualmente la BD MINTRASD tiene parametrizada 165,767 GB a nivel de almacenamiento de los cuales 90,678 GB están en uso y se tiene libre 75,089 GB.

Tamaño de esquemas de base de datos:

ESQUEMA	SIZE_GB
SIMPCPRU	23,3
TLIFERAY	22,55
LIFERAYPRU	22,12
LIFERAYPRO	15,25
SYS	2,5
NEWIVCMT	0,74
AUDSYS	0,15
XDB	0,06
SYSTEM	0,03
WMSYS	0,01
EMPRENDIMIENTOP	0,01
MT_DEFENSA	0
OUTLN	0
DBSNMP	0
GSMADMIN_INTERNAL	0

Ilustración 117 Tamaño DDBB

Como se observa en la imagen anterior se muestra el tamaño de los esquemas de mayor a menor, para este caso los esquemas SIMPCPRU, TLIFERAY, LIFERAYPRU, LIFERAYPROS tienen el mayor consumo a nivel de almacenamiento, como tal la ocupación de dichos esquemas no es muy alta.

Graficas de rendimiento de la Base de datos DFILERAY

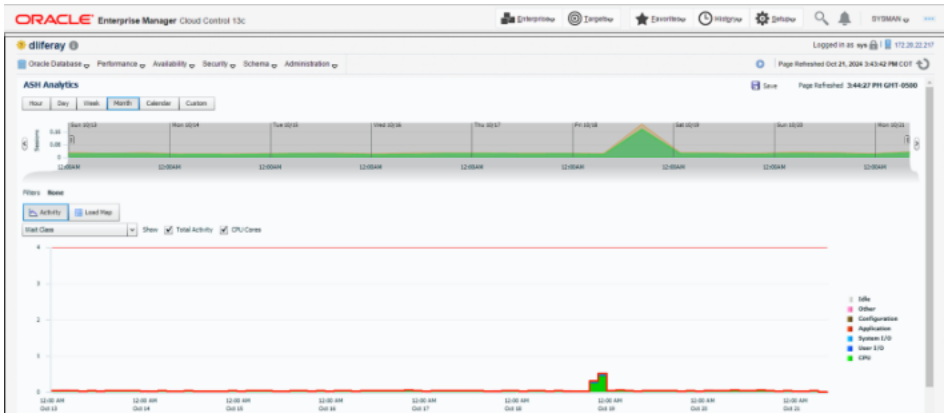


Ilustración 118 Rendimiento DDBB

La base de datos DLIFERAY mantiene un comportamiento transaccional muy bajo, NO OBSTANTE, se puede observar para este muestreo un pico transaccional el cual fue causado por un export – import para refrescamiento de un esquema de base de datos de desarrollo de delifeary para las pruebas de updates solicitado por la Ing. Maria Elena Lucumi, en general su comportamiento transaccional es bajo.

1. BASES DE DATOS VERSION 11G SERVDIOR 172.20.22.107

3.1 Base de datos DBMINTRA

Información base de datos – Servidor:

DB Name	DB Id	Instance	Inst num	Startup Time	Release	RAC
DBMINTRA	697355327	dbmintrab	1	15-Oct-24 19:10	11.2.0.1.0	NO

Host Name	Platform	CPUs	Cores	Sockets	Memory (GB)
MINTRAB32	Microsoft Windows x86 64-bit	10	10	2	32.00

	Snap Id	Snap Time	Sessions	Cursors/Session
Begin Snap:	76018	21-Oct-24 00:14:44	32	1.1
End Snap:	76033	21-Oct-24 15:00:04	27	1.1
Elapsed:		885.34 (mins)		
DB Time:		0.71 (mins)		

Ilustración 119 Información Server DDBB

Estadísticas de uso de CPU: Información referente a la carga que ha tenido la CPU a nivel de host como a nivel de instancia en el periodo de tiempo reportado.

NUM_CORES_ASIGNADOS	DESCRIPTION
10	number of CPUs for this instance

Host CPU (CPUs: 10 Cores: 10 Sockets: 2)

Load Average Begin	Load Average End	%User	%System	%WIO	%Idle
		0.2	1.1		98.8

Instance CPU

%Total CPU	%Busy CPU	%DB time waiting for CPU (Resource Manager)
0.0	1.1	0.0

Ilustración 120 Host e Instancia CPU

Como se observa, los consumos de CPU son en extremo bajos para este host y base de datos, en este caso la base de datos esta con un CPU_COUNT=10 el cual está sobredimensionado para el uso de CPU que se le está dando, por tal motivo se recomienda bajar CPU_COUNT=4

Estadísticas de uso Memoria: Se puede observar el uso del recurso de memoria durante el periodo reportado.

Memory Statistics

	Begin	End
Host Mem (MB):	32,767.5	32,767.5
SGA use (MB):	8,544.0	8,544.0
PGA use (MB):	79.0	71.8
% Host Mem used for SGA+PGA:	26.32	26.29

Ilustración 121 Estadística Memoria

Shared Pool Statistics

	Begin	End
Memory Usage %:	16.90	17.12
% SQL with executions>1:	95.47	95.71
% Memory for SQL w/exec>1:	88.11	88.72

Ilustración 122 Estadística Shared Pool

Tamaño base de datos DBMINTRA**:**

	DATABASE SIZE IN GB	USED SPACE IN GB	FREE SPACE IN GB
1	43	22	21

Ilustración 123 Tamaño DDBB

Actualmente la BD DBMINTRA tiene parametrizada 43 GB a nivel de almacenamiento de los cuales 22 GB están en uso y se tiene libre 21 GB.

Tamaño de esquemas de base de datos:

	ESQUEMA	SIZE_GB
1	LIFERAYPRU	10,87
2	SYS	3,02
3	SID3	1,65
4	SID14022023	1,64
5	APEX_040000	0,22
6	SIPGESDES	0,21
7	SIPGES	0,2
8	SIPGESNEW	0,15
9	PP	0,15
10	SIPGESPRU	0,14
11	XDB	0,13
12	GITRIV	0,12
13	SYSMAN	0,11
14	APEX_030200	0,08
15	MDSYS	0,04
16	SYSTEM	0,02
17	ORDDATA	0,01
18	RADICADOR	0
19	DBSNMP	0
20	ORDSYS	0
21	HR	0
22	COOUSR	0
23	SIG	0
24	OLAPSYS	0
25	CTXSYS	0
26	OUTLN	0
27	WMSYS	0
28	DAMI	0
29	EEVENT	0
30	SCOTT	0
31	ECS	0
32	PLANEACION_USER	0
33	EXFSYS	0

Ilustración 124 Tamaño Esquemas DDBB

Como se observa en la imagen anterior se muestra el tamaño de los esquemas de mayor a menor, para este caso el esquema LIFERAYPRU ya se encuentra alojado y la base de datos DLIFERAY – PLIFERAY por lo cual habría alguna redundancia al tenerlo en este servidor y motor de base de datos Oracle 11g, en este caso es factible validar si se puede eliminar dicho esquema.

Graficas de rendimiento de la Base de datos DBMINTRA



Ilustración 125 Rendimiento DDBB

La base de datos DBMINTRA mantiene un comportamiento transaccional muy bajo, se puede observar que solo hay en promedio de 2 a 3 sesiones, por lo cual se puede establecer que esta base de datos es solo de consulta.

3.2 Base de datos INVENTARIOS

Información base de datos – Servidor:

DB Name	DB Id	Instance	Inst num	Startup Time	Release	RAC
INVENTAR	2693810353	inventarios	1	15-Oct-24 19:10	11.2.0.1.0	NO

Host Name	Platform	CPUs	Cores	Sockets	Memory (GB)
MINTRAB32	Microsoft Windows x86 64-bit	10	10	2	32.00

	Snap Id	Snap Time	Sessions	Cursors/Session
Begin Snap:	75914	20-Oct-24 23:00:54	27	1.1
End Snap:	75931	21-Oct-24 16:00:22	26	1.2
Elapsed:		1,019.46 (mins)		
DB Time:		0.72 (mins)		

Ilustración 126 Información Server DDBB

Estadísticas de uso de CPU: Información referente a la carga que ha tenido la CPU a nivel de host como a nivel de instancia en el periodo de tiempo reportado.

NUM_CORES_ASIGNADOS	DESCRIPTION
10	number of CPUs for this instance

Host CPU (CPUs: 10 Cores: 10 Sockets: 2)

Load Average Begin	Load Average End	%User	%System	%WIO	%Idle
		0.2	1.0		98.8

Instance CPU

%Total CPU	%Busy CPU	%DB time waiting for CPU (Resource Manager)
0.0	1.0	0.0

Ilustración 127 Estadística CPU

Como se observa los consumos de CPU son en extremo bajos para este host y base de datos, en este caso la base de datos esta con un CPU_COUNT=10 el cual está sobredimensionado para el uso de CPU que se le está dando, por tal motivo se recomienda bajar CPU_COUNT=4

Estadísticas de uso Memoria: Se puede observar el uso del recurso de memoria durante el periodo reportado.

Memory Statistics

	Begin	End
Host Mem (MB):	32,767.5	32,767.5
SGA use (MB):	6,112.0	6,112.0
PGA use (MB):	71.2	70.2
% Host Mem used for SGA+PGA:	18.87	18.87

Ilustración 128 Estadística Memoria

Shared Pool Statistics

	Begin	End
Memory Usage %:	19.01	19.32
% SQL with executions>1:	90.38	97.58
% Memory for SQL w/exec>1:	79.08	92.65

Ilustración 129 Estadística Shared Pool

Tamaño base de datos INVENTARIOS**:**

DATABASE SIZE IN GB	USED SPACE IN GB	FREE SPACE IN GB
27	20	7

Actualmente la BD INVENTARIOS tiene parametrizada 27 GB a nivel de Almacenamiento de los cuales 20 GB están en uso y se tiene libre 7 GB.

Tamaño de esquemas de base de datos:

	ESQUEMA	SIZE_GB
1	SYS	3,85
2	PCT2019	0,37
3	PCT2018	0,36
4	PCT2020	0,35
5	PCT2021	0,35
6	PCT2023	0,35
7	PCT2024	0,35
8	PCT2022	0,35
9	PCT2017	0,14
10	XDB	0,13
11	PCT2016	0,13
12	DES_SSINV	0,11
13	APEX_030200	0,08
14	SYSMAN	0,08
15	MDSYS	0,04
16	SYSTEM	0,02
17	JMARTINEZ	0,02
18	ORDDATA	0,01
19	CTXSYS	0
20	OLAPSYS	0
21	ORDSYS	0
22	DBSNMP	0
23	WMSYS	0
24	SCOTT	0
25	OUTLN	0
26	EXFSYS	0

Ilustración 130 Tamaño Esquemas DDBB

Como se puede observar en la imagen anterior se muestra el tamaño de los esquemas de mayor a menor, para este caso los esquemas SYS, PCT2017 al PCT2024 son lo que tienen el mayor almacenamiento, no obstante, estos esquemas mantienen un tamaño no mayor a 400 MB excluyendo al esquema SYS que es de 3,85GB.

Graficas de rendimiento de la Base de datos INVENTARIOS

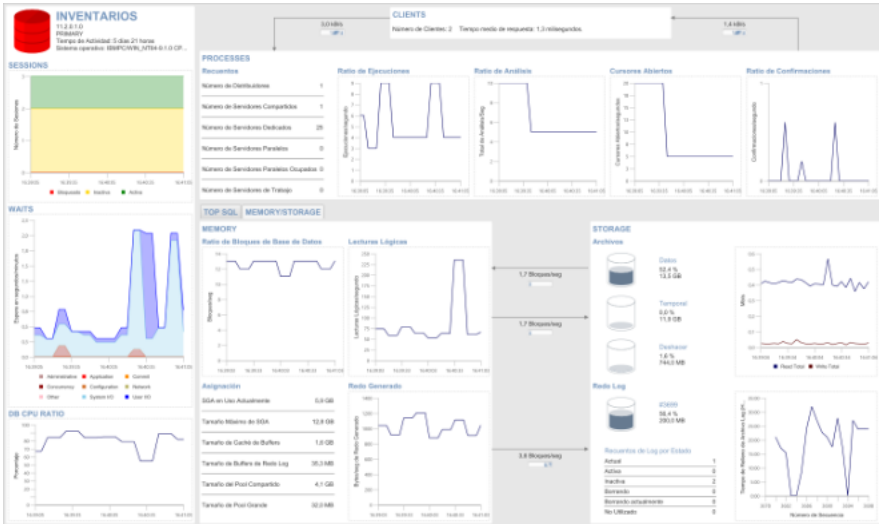


Ilustración 131 Comportamiento DDBB

La base de datos INVENTARIOS mantiene un comportamiento transaccional muy bajo, se puede observar que solo hay en promedio de 2 a 3 sesiones, por lo cual se puede establecer que esta base de datos tiene transaccionalidad por los esquemas PTC por lo cual es necesario validar si tienen una aplicación especifica que consuma estos objetos de base de datos.

ALMACENAMIENTO GENERAL SERVIDOR ODA X5-2

1. Almacenamiento General ASM:

En el siguiente apartado se muestra como esta parametrizado el almacenamiento a nivel de ASM del ODA X5-2 el cual es una preconfiguración de fabrica sobre el appliance.

	Group #	Name	Sector Size	Block Size	Alloc Unit Size	State	Type	Total MB	Free MB	Req Mirror Free MB	Usable File MB	Offline Disks	Compatibility	DB Compatibility
▶	1	DATA	512	4096	4194304	MOUNTED	HIGH	46101056	6614980	6443008	57324	2	12.2.0.1.0	12.1.0.2.0
	2	FLASH	512	4096	4194304	MOUNTED	NOR...	1526208	899004	381552	258726	0	12.2.0.1.0	12.1.0.2.0
	3	RECO	512	4096	4194304	MOUNTED	HIGH	59915128	460768	8599304	-2699512	2	12.2.0.1.0	12.1.0.2.0
	4	REDO	512	4096	4194304	MOUNTED	HIGH	763120	106024	190780	-28252	0	12.2.0.1.0	12.1.0.2.0

Ilustración 132 Almacenamiento ASM

DISKGROUP DATA:

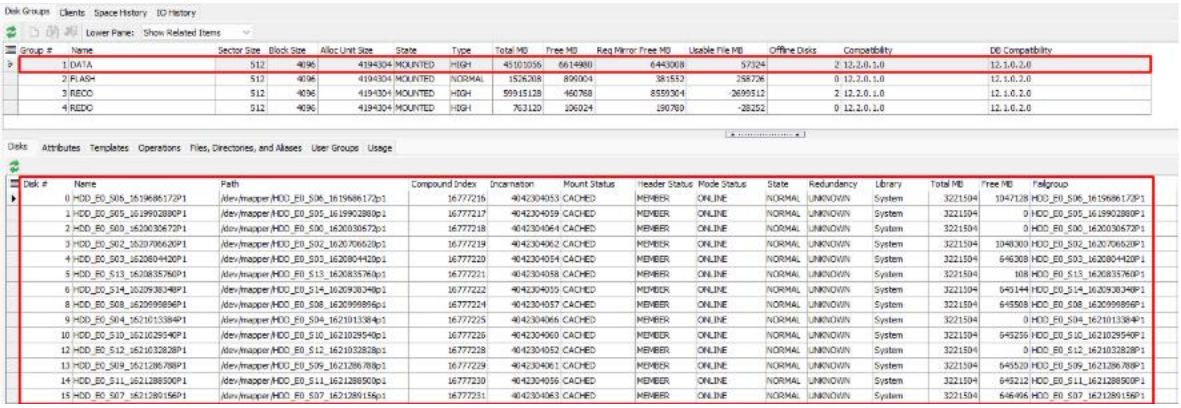


Ilustración 133 DiskGroup Data

DISKGROUP FLASH:

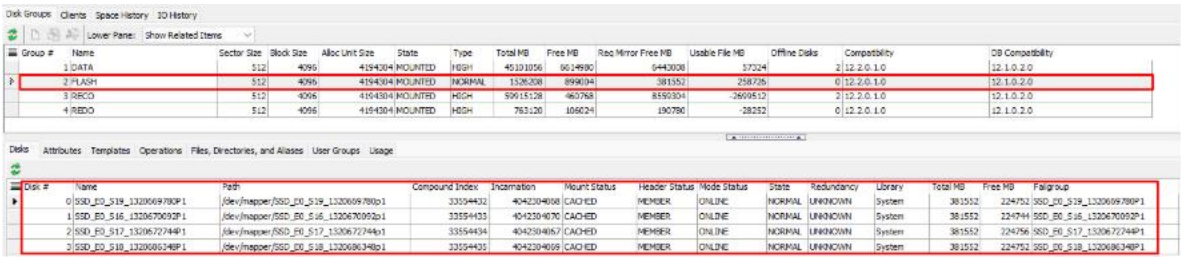


Ilustración 134 DiskGroup Flash

DISKGROUP RECO:

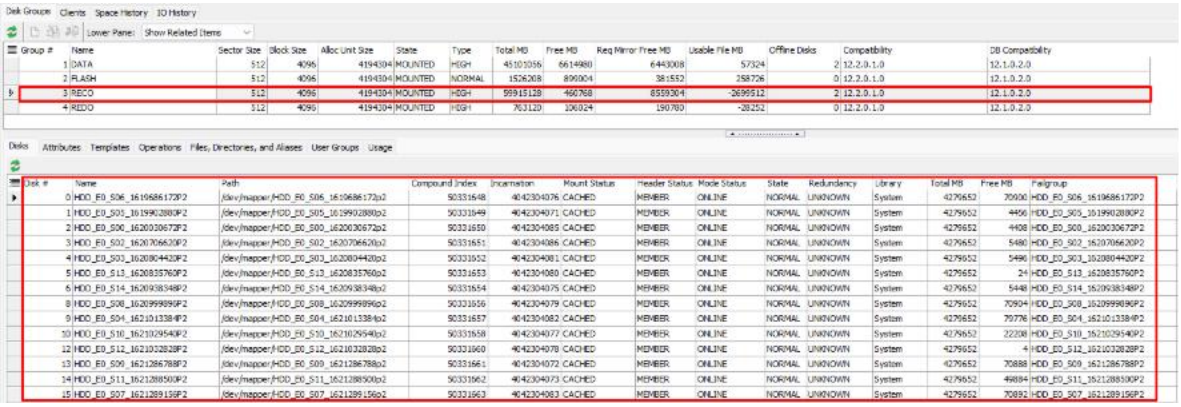


Ilustración 135 DiskGroup Reco

DISKGROUP REDO:

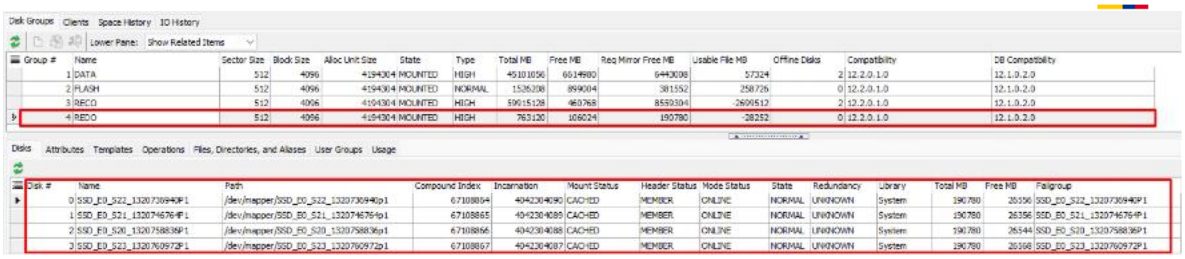


Ilustración 136 DiskGroup Redo

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 137 Licenciamiento adicional componente IBM

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 enero de 2026, los firewalls de Fortinet mantuvieron un estado óptimo en cuanto a la seguridad perimetral. Se llevó a cabo una supervisión continua de la red para garantizar que solo el tráfico autorizado tenga acceso a los recursos internos. Se implementaron políticas de seguridad sólidas para proteger contra amenazas externas, realizando ajustes según las necesidades específicas del Ministerio de Trabajo.

Se puede evidenciar que el firewall tuvo una disponibilidad del 100%, esto quiere decir que no se presentó ningún tipo de interrupción en el servicio.

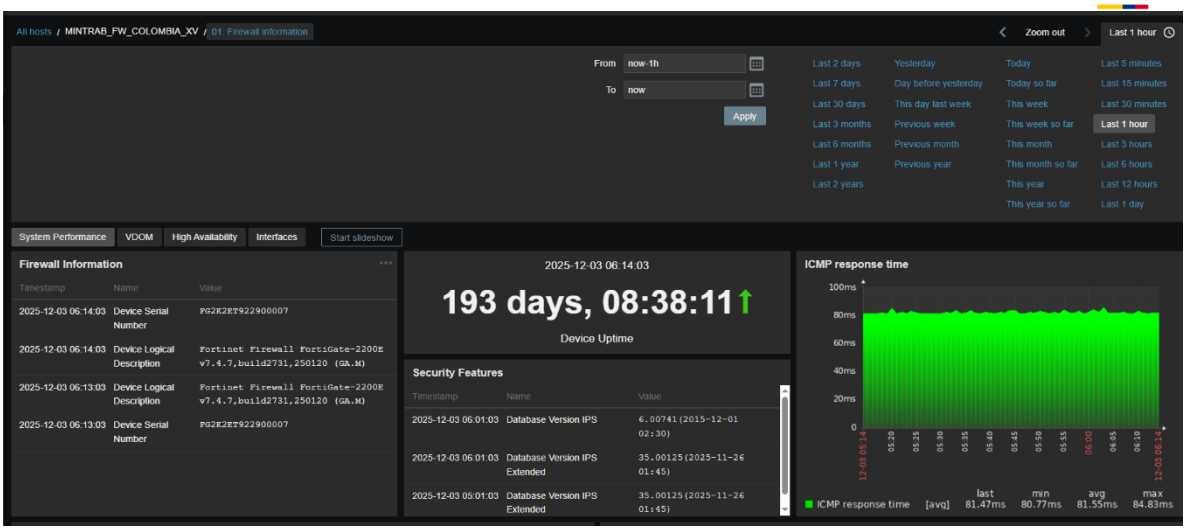


Ilustración 108 Firewall de nueva generación.

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 enero. 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 4 TB y 12 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 8–10 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 1–2 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 53 Tendencia de uso de ancho de banda

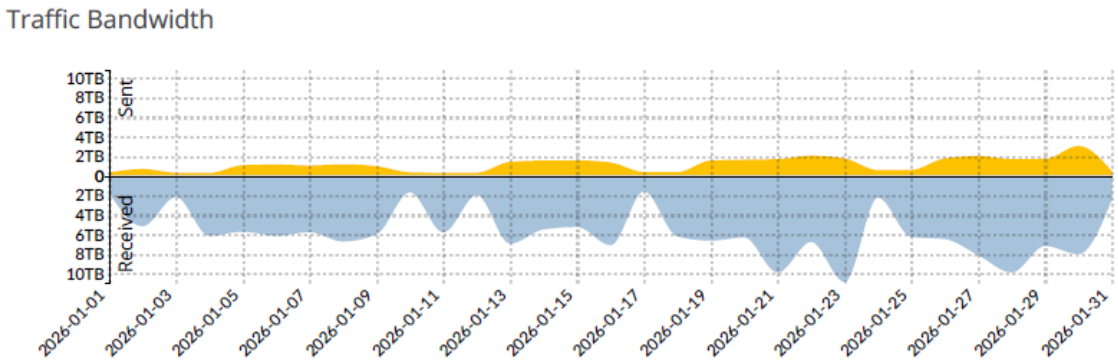


Ilustración 109 Comportamiento ancho de banda

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

N°	Usuario/IP	Total, de datos (aprox.)	Observaciones
1	172.20.22.251	**66.41 TB**	Tráfico extremadamente alto, servidor de almacenamiento, backup (MINTRABCKEXEC.mintrabajo.loc).
2	172.20.22.205	**7.95 TB**	Servidos de aplicaciones
3	172.28.28.38	**5.09 TB**	IP interna — podría corresponder a servidor de aplicaciones o gestión. Revisar patrón de uso.

4	Mduarteo	**4.11 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 54 usuarios con mayor consumo de ancho de banda

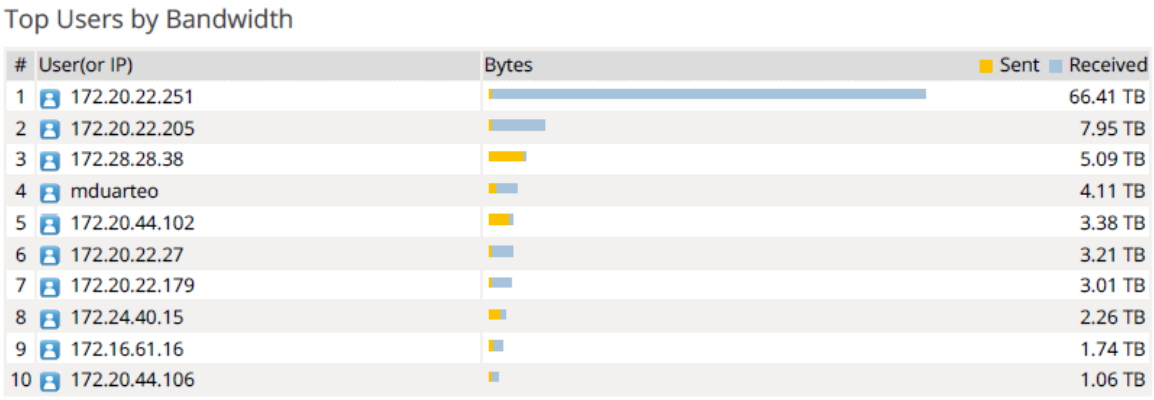


Ilustración 110 Tendencia de uso de ancho de banda

Top de usuarios por número de sesiones

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

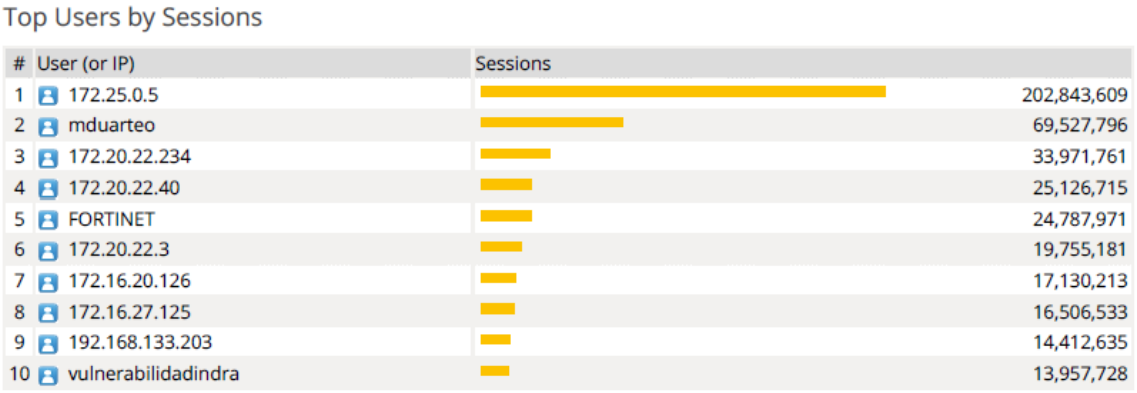


Ilustración 111 Top de usuarios por números de sesiones

Análisis Top Users by Sessions

N°	Usuario/IP	Sesiones	Observaciones
1	**172.25.0.5**	**202.843.609**	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**	**69.527.796**	Usuario con actividad muy elevada. Puede estar vinculado a gestion de alguna plataforma(Mireya Duarte Osma)
3	**172.20.22.234**	**33.971.761**	Servidor interno asociado a un controlador de dominio.
4	**FORTINET**	**24.787.971**	Tráfico legítimo del sistema de seguridad (firewall, antivirus o gestión de eventos).
5	**Resto de IPs internas (rango 172.16–172.22)**	Entre **12 y 18 millones de sesiones**	Volumen esperado para servicios de autenticación, proxy, o endpoints activos de red.

Tabla 55 Top de usuarios por sesiones

Top Applications by Bandwidth

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

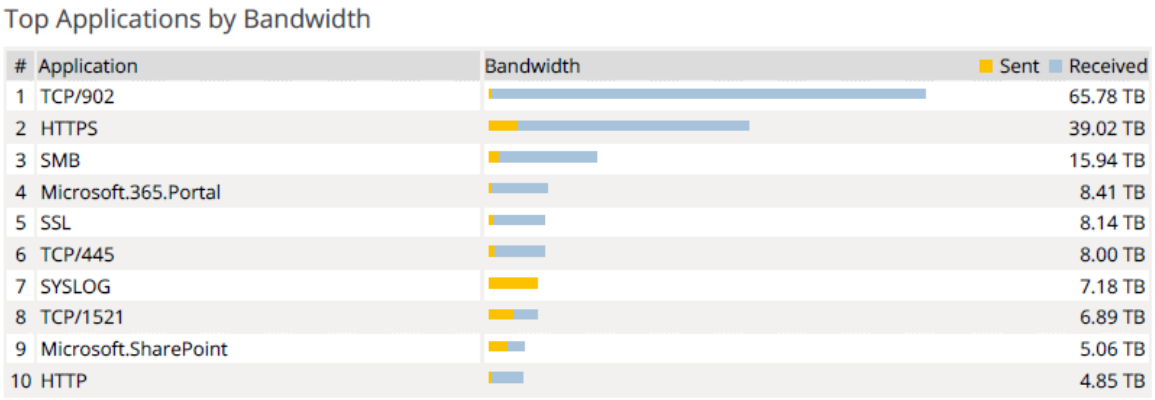


Ilustración 112 Top de aplicaciones

Aplicación	Tamaño	Descripción
1. TCP/902	65.78 TB	Puerto comúnmente usado para VMware ESXi (administración de máquinas virtuales). Indica alto volumen de sincronización o replicación de entornos virtualizados.
2. HTTPS	39.02 TB	Tráfico web cifrado — servicios cloud, correo, portales institucionales. Representa la base del tráfico corporativo seguro.
3. SMB (Server Message Block)	15.94 TB	Protocolo de compartición de archivos en red. Muestra alto uso de repositorios compartidos internos.
4. TCP/445	8.00 TB	Asociado también a SMB y autenticación Windows (Active Directory). Indica intenso intercambio de archivos y autenticaciones.
5. SYSLOG	7.18 TB	Transmisión de logs desde dispositivos hacia el FortiAnalyzer o SIEM. Tráfico esperado y saludable para monitoreo de seguridad.
6. TCP/1521	6.82 TB	Puerto usado por Oracle Database. Indica consultas o réplicas intensivas en bases de datos institucionales.
7. HTTP	4.85 TB	Tráfico no cifrado. Nivel bajo comparado con HTTPS, lo que refleja correcta adopción de canales seguros.
8. Microsoft.SharePoint	5.06 TB	Uso activo de bibliotecas documentales internas y colaboración en línea.

Tabla 56 Top de aplicaciones

Top 15 Authenticated Logins by VPN Connections

La imagen corresponde al apartado “Authenticated Logins” del informe perimetral de enero 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	2026-01-02 07:05:51	137	221:28:52
2	scelya	ssl-tunnel	2026-01-06 17:49:35	111	104:06:51
3	dfdiazd@noc_indra	ssl-tunnel	2026-01-01 14:06:40	92	498:53:24
4	200.85.231.148	ipsec	2026-01-01 00:01:25	84	742:28:07
5	RMURCIA	ssl-tunnel	2026-01-05 15:10:00	72	100:24:57
6	fgonzalez	ssl-tunnel	2026-01-01 16:44:06	65	74:37:14
7	jsanabriat	ssl-tunnel	2026-01-08 17:04:37	57	50:01:44
8	CADAZAR	ssl-tunnel	2026-01-02 11:00:28	56	24:07:30
9	ctobos	ssl-tunnel	2026-01-02 15:48:52	55	35:08:58
10	orealpe	ssl-tunnel	2026-01-05 22:29:41	54	93:40:39
11	jmeza	ssl-tunnel	2026-01-15 09:53:43	53	45:25:28
12	dacero	ssl-tunnel	2026-01-02 10:12:34	52	48:55:08
13	ablanco	ssl-tunnel	2026-01-13 07:37:56	51	91:01:35
14	omcastellanos	ssl-tunnel	2026-01-01 06:07:27	49	48:13:21
15	agente4	ssl-tunnel	2026-01-13 13:22:37	47	67:04:05

Ilustración 113 Top de Autenticación

Indicador	Descripción actualizada
Tipo de conexión	El 100 % de las sesiones se realizaron mediante SSL-Tunnel, evidenciando el uso exclusivo de la VPN segura FortiGate para el acceso remoto a la red institucional.
Usuarios más activos (por duración)	Los usuarios con mayor tiempo acumulado de conexión son: 200.85.231.148 (IPsec) (~742 h), dfdiazd@noc_indra (~498 h), contaccenter (~221 h), scelya (~104 h) y RMURCIA (~100 h). Este comportamiento es consistente con roles operativos, soporte extendido y funciones tipo SOC/NOC.
Mayor duración total	El mayor tiempo acumulado corresponde a la IP 200.85.231.148 (IPsec) con aproximadamente 742 horas, seguido de dfdiazd@noc_indra con cerca de 498 horas, lo que indica accesos persistentes y de carácter operativo, asociados a administración, monitoreo o soporte continuo.
Mayor cantidad de conexiones	Los usuarios con mayor número de conexiones registradas son: contaccenter (137 conexiones), scelya (111), dfdiazd@noc_indra (92), 200.85.231.148 (84) y RMURCIA (72). Este patrón es típico de personal con múltiples turnos o reconexiones recurrentes..
Duraciones elevadas (>200 h)	Se identifican accesos con actividad superior a 200 horas: 200.85.231.148 (IPsec), dfdiazd@noc_indra y contaccenter. Estos accesos deben estar formalmente justificados, alineados a roles críticos y documentados dentro de los procedimientos operativos autorizados.

Duraciones medias (100 h – 200 h)	Usuarios con uso estable y recurrente de la VPN: scelya, RMURCIA, orealpe, ablanco y gonzalez. Corresponden a trabajo remoto frecuente, soporte técnico y actividades operativas periódicas.
Duraciones bajas (<100 h)	Usuarios con accesos más puntuales u ocasionales: jsanabriat, CADAZAR, ctobos, jmeza, dacero, mcastellanos y agente4, lo que sugiere uso esporádico o ejecución de tareas específicas

Tabla 57 Consolidado de indicadores

Failed Login Attempts by User

Esta imagen corresponde al apartado “Failed Login Attempts” del informe perimetral de enero 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	29,282
2	administrator	ssl-web	2,387
3	User	ssl-web	1,029
4	test	ssl-web	383
5	administrador	ssl-web	334
6	cisco	ssl-web	291
7	1	ssl-web	275
8	usuario	ssl-web	262
9	scanner	ssl-web	197
10	ChinaMobile	ssl-web	171

Ilustración 114 sesiones fallidas

Análisis
Durante enero 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 enero de 2026, se generaron 100 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	*77*	0	*77*
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	77	0	*77*

File Scan - Last 4 Weeks

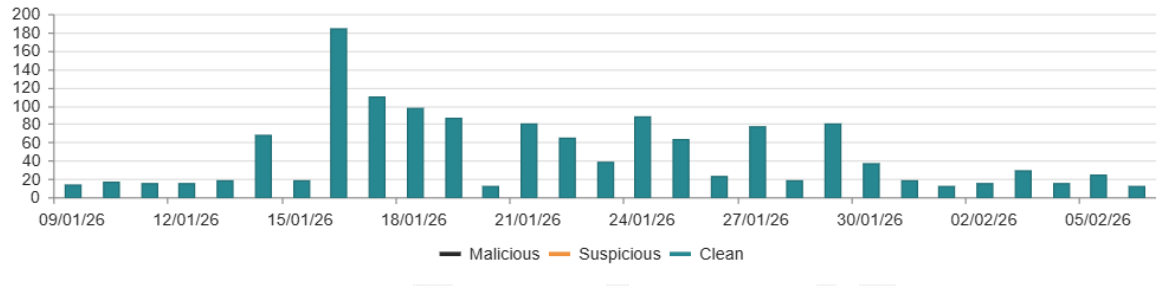


Ilustración 115 Reporte mensual enero

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

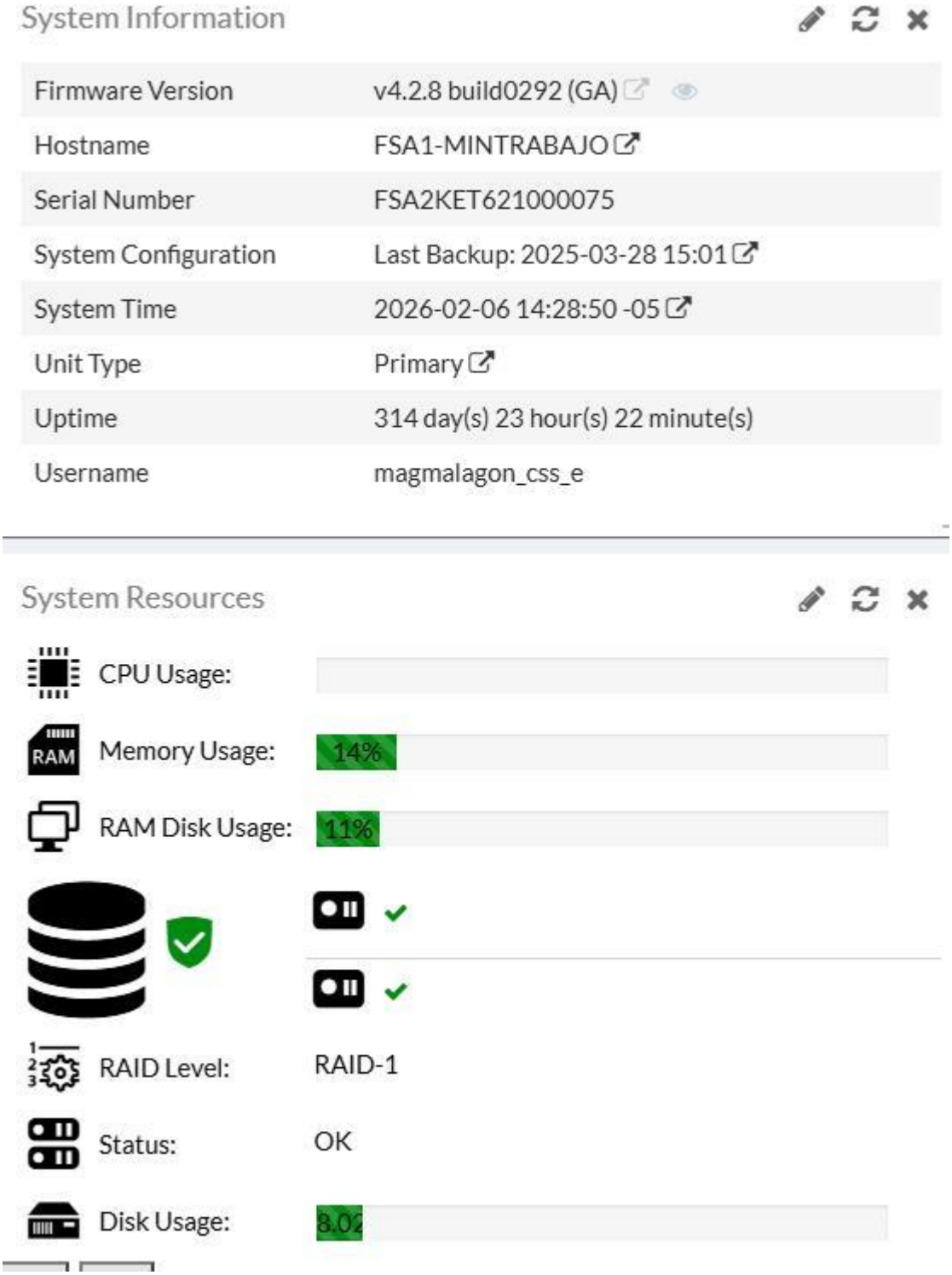


Ilustración 116 Captura de pantalla perfomance

Licencia Sandbox

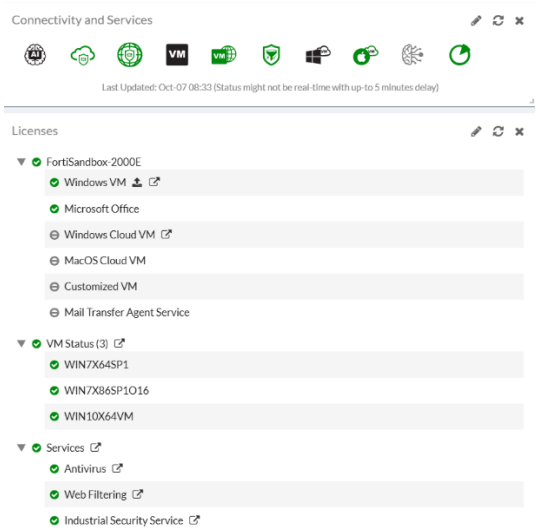


Ilustración 117 licencia sandbox

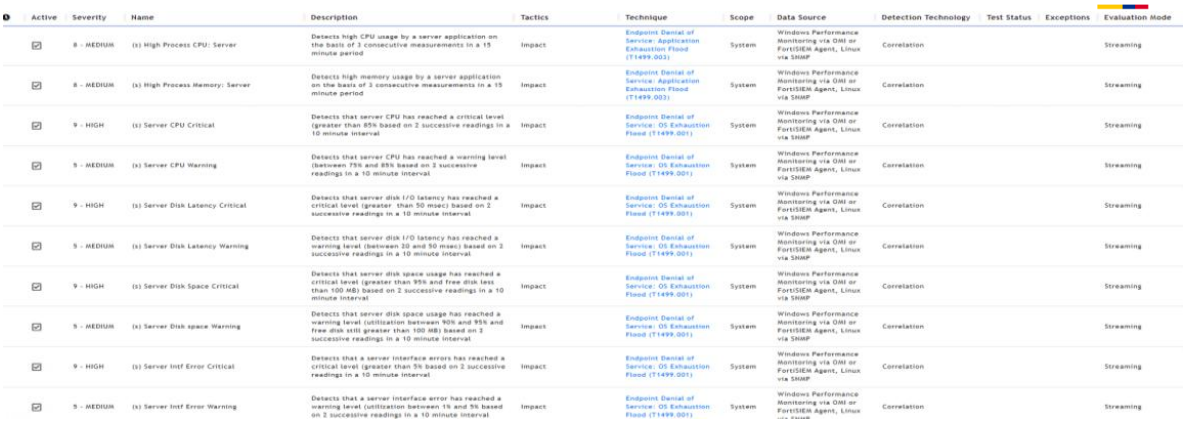
3.1.6.3 SIEM - Solución de correlación de eventos de seguridad, disponibilidad y recursos

Durante el periodo evaluado, la plataforma FortiSIEM del Ministerio del Trabajo mantuvo una supervisión continua sobre la infraestructura tecnológica, permitiendo identificar eventos de seguridad, condiciones de desempeño, incidentes de autenticación y violaciones de políticas.
El análisis confirma una postura de seguridad robusta, con capacidad para detectar de manera proactiva fallos, sobrecargas, intentos de fuerza bruta y patrones de ataque asociados a sistemas internos y externos. No se evidenciaron intrusiones exitosas.A continuación, se detallan algunos ítems particulares.

3.1.6.3.1 Casos de uso Fortisiem

Desempeño (performance)

El Sistema de Gestión de Eventos e Información de Seguridad (SIEM) implementado en el Ministerio permite la supervisión continua de la infraestructura tecnológica mediante reglas de correlación que detectan condiciones anómalas como uso elevado de CPU o memoria, latencia en discos, fallos de espacio o de memoria virtual. Estas alertas están vinculadas a técnicas específicas de seguridad como el "Endpoint Denial of Service" lo que permite activar mecanismos de respuesta ante incidentes que afectan la disponibilidad y el rendimiento de los sistemas.
A continuación, se detallan algunos ítems particulares:



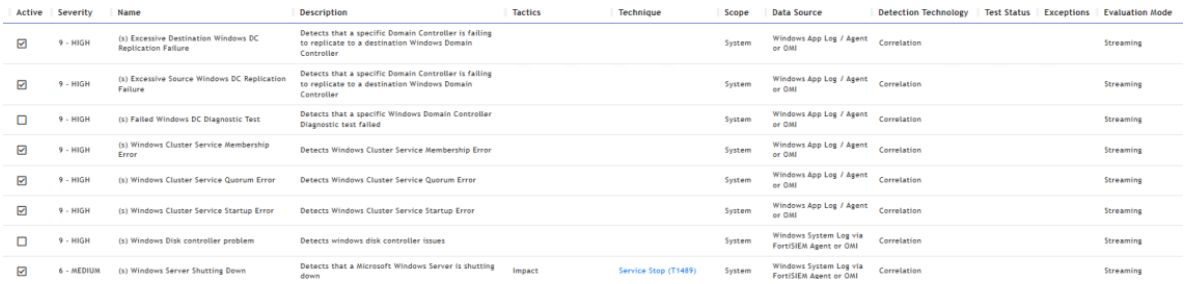
Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☑	8 - MEDIUM	(s) High Process CPU: Server	Detects high CPU usage by a server application on the basis of 3 consecutive measurements in a 15 minute period	Impact	Endpoint Denial of Service: Application Exhaustion Flood (T1499.003)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent, Linux via SNMP	Correlation			Streaming
☑	8 - MEDIUM	(s) High Process Memory: Server	Detects high memory usage by a server application on the basis of 3 consecutive measurements in a 15 minute period	Impact	Endpoint Denial of Service: Application Exhaustion Flood (T1499.003)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent, Linux via SNMP	Correlation			Streaming
☑	9 - HIGH	(s) Server CPU Critical	Detects that server CPU has reached a critical level (greater than 85% based on 2 successive readings in a 10 minute interval	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent, Linux via SNMP	Correlation			Streaming
☑	5 - MEDIUM	(s) Server CPU Warning	Detects that server CPU has reached a warning level (between 75% and 85% based on 3 successive readings in a 10 minute interval	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent, Linux via SNMP	Correlation			Streaming
☑	9 - HIGH	(s) Server Disk Latency Critical	Detects that server disk I/O latency has reached a critical level (greater than 50 msec) based on 2 successive readings in a 10 minute interval	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent, Linux via SNMP	Correlation			Streaming
☑	5 - MEDIUM	(s) Server Disk Latency Warning	Detects that server disk I/O latency has reached a warning level (between 20 and 50 msec) based on 2 successive readings in a 10 minute interval	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent, Linux via SNMP	Correlation			Streaming
☑	9 - HIGH	(s) Server Disk Space Critical	Detects that server disk space usage has reached a critical level (greater than 95% and free disk less than 100 MB) based on 2 successive readings in a 10 minute interval	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent, Linux via SNMP	Correlation			Streaming
☑	5 - MEDIUM	(s) Server Disk space Warning	Detects that server disk space usage has reached a warning level (utilization between 90% and 95% and free disk still greater than 100 MB) based on 2 successive readings in a 10 minute interval	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent, Linux via SNMP	Correlation			Streaming
☑	9 - HIGH	(s) Server Intf Error Critical	Detects that a server interface errors has reached a critical level (greater than 5% based on 2 successive readings in a 10 minute interval	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent, Linux via SNMP	Correlation			Streaming
☑	5 - MEDIUM	(s) Server Intf Error Warning	Detects that a server interface error has reached a warning level (utilization between 1% and 5% based on 2 successive readings in a 10 minute interval	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent, Linux via SNMP	Correlation			Streaming

Ilustración 118 licencia sandbox

3.1.6.3.2 Disponibilidad (Availability)

Estas alertas proporcionadas por el sistema SIEM permiten al equipo de seguridad y operaciones de TI anticipar posibles eventos de denegación de servicio (DoS) internos que no necesariamente son causados por ataques externos, sino por fallos o sobrecargas dentro de la propia infraestructura. Las detecciones abarcan condiciones críticas como:

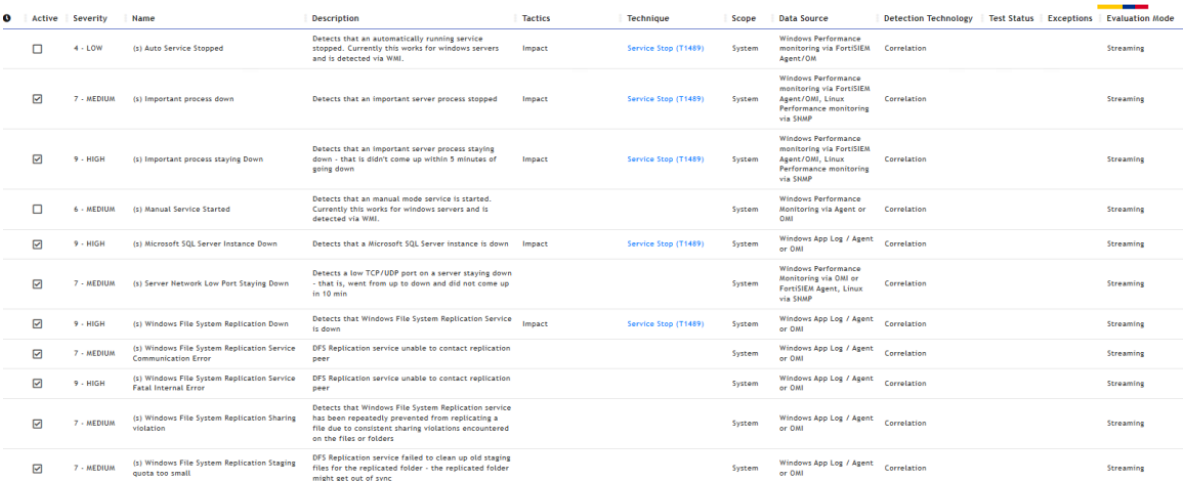
- **Uso excesivo de CPU o memoria (RAM)**, que puede indicar aplicaciones fuera de control, procesos maliciosos o configuraciones inadecuadas.
- **Latencia o errores de entrada/salida en disco**, que pueden reflejar problemas con el hardware de almacenamiento o cuellos de botella en el rendimiento de las aplicaciones



Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☑	9 - HIGH	(s) Excessive Destination Windows DC Replication Failure	Detects that a specific Domain Controller is failing to replicate to a destination Windows Domain Controller			System	Windows App Log / Agent or OMI	Correlation			Streaming
☑	9 - HIGH	(s) Excessive Source Windows DC Replication Failure	Detects that a specific Domain Controller is failing to replicate to a destination Windows Domain Controller			System	Windows App Log / Agent or OMI	Correlation			Streaming
☐	9 - HIGH	(s) Failed Windows DC Diagnostic Test	Detects that a specific Windows Domain Controller Diagnostic test failed			System	Windows App Log / Agent or OMI	Correlation			Streaming
☑	9 - HIGH	(s) Windows Cluster Service Membership Error	Detects Windows Cluster Service Membership Error			System	Windows App Log / Agent or OMI	Correlation			Streaming
☑	9 - HIGH	(s) Windows Cluster Service Quorum Error	Detects Windows Cluster Service Quorum Error			System	Windows App Log / Agent or OMI	Correlation			Streaming
☑	9 - HIGH	(s) Windows Cluster Service Startup Error	Detects Windows Cluster Service Startup Error			System	Windows App Log / Agent or OMI	Correlation			Streaming
☐	9 - HIGH	(s) Windows Disk controller problem	Detects windows disk controller issues			System	Windows System Log via FortiSIEM Agent or OMI	Correlation			Streaming
☑	6 - MEDIUM	(s) Windows Server Shutting Down	Detects that a Microsoft Windows Server is shutting down	Impact	Service Stop (T1489)	System	Windows System Log via FortiSIEM Agent or OMI	Correlation			Streaming

Ilustración 119 Detalle de latencia o errores

- Falta de espacio en disco, que puede interrumpir operaciones críticas, servicios de base de datos, o impedir la creación de archivos temporales necesarios para el funcionamiento del sistema operativo.
- Problemas en servicios de clúster o controladores de dominio, que afectan la disponibilidad de servicios distribuidos o autenticación de usuarios.



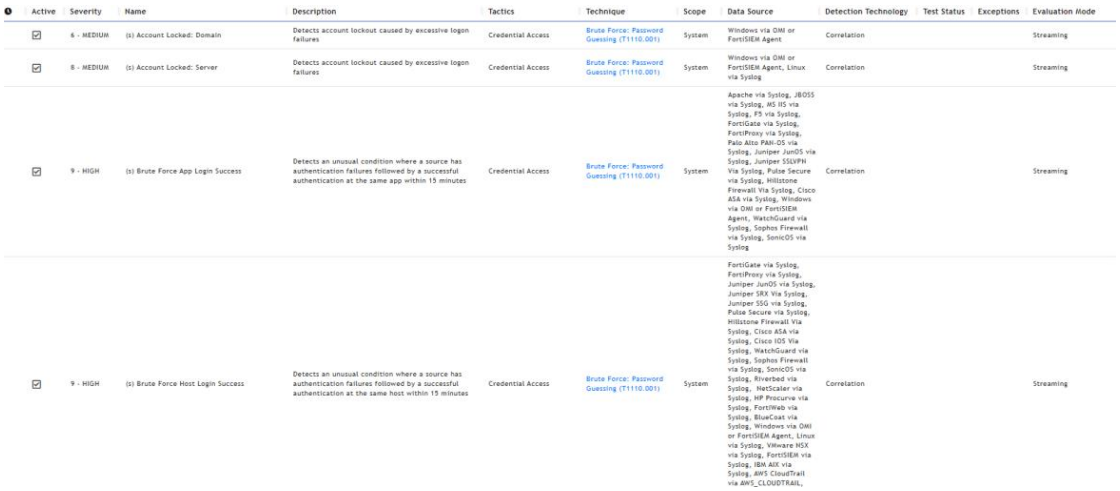
Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☐	4 - LOW	(s) Auto Service Stopped	Detects that an automatically running service stopped. Currently this works for windows servers and is detected via WMI.	Impact	Service Stop (T1489)	System	Windows Performance monitoring via FortiSIEM Agent/OMI	Correlation			Streaming
☑	7 - MEDIUM	(s) Important process down	Detects that an important server process stopped	Impact	Service Stop (T1489)	System	Windows Performance monitoring via FortiSIEM Agent/OMI, Linux Performance monitoring via SNMP	Correlation			Streaming
☑	9 - HIGH	(s) Important process staying Down	Detects that an important server process staying down - that is didn't come up within 5 minutes of going down	Impact	Service Stop (T1489)	System	Windows Performance monitoring via FortiSIEM Agent/OMI, Linux Performance monitoring via SNMP	Correlation			Streaming
☐	6 - MEDIUM	(s) Manual Service Started	Detects that an manual mode service is started. Currently this works for windows servers and is detected via WMI.			System	Windows Performance Monitoring via Agent or OMI	Correlation			Streaming
☑	9 - HIGH	(s) Microsoft SQL Server Instance Down	Detects that a Microsoft SQL Server instance is down	Impact	Service Stop (T1489)	System	Windows App Log / Agent or OMI	Correlation			Streaming
☑	7 - MEDIUM	(s) Server Network Low Port Staying Down	Detects a low TCP/UDP port on a server staying down - that is, went from up to down and did not come up in 10 min			System	Windows Performance Monitoring via OMI or FortiSIEM Agent, Linux via SNMP	Correlation			Streaming
☑	9 - HIGH	(s) Windows File System Replication Down	Detects that Windows File System Replication Service is down	Impact	Service Stop (T1489)	System	Windows App Log / Agent or OMI	Correlation			Streaming
☑	7 - MEDIUM	(s) Windows File System Replication Service Communication Error	DFS Replication service unable to contact replication peer			System	Windows App Log / Agent or OMI	Correlation			Streaming
☑	9 - HIGH	(s) Windows File System Replication Service Fatal Internal Error	DFS Replication service unable to contact replication peer			System	Windows App Log / Agent or OMI	Correlation			Streaming
☑	7 - MEDIUM	(s) Windows File System Replication Sharing violation	Detects that Windows File System Replication service has been repeatedly prevented from replicating a file due to consistent sharing violations encountered on the files or folders			System	Windows App Log / Agent or OMI	Correlation			Streaming
☑	7 - MEDIUM	(s) Windows File System Replication Staging quota too small	DFS Replication service failed to clean up old staging files for the replicated folder - the replicated folder might get out of sync			System	Windows App Log / Agent or OMI	Correlation			Streaming

Ilustración 120 detalle de problemas en servicios

La correlación de estas alertas facilita una gestión proactiva del rendimiento y la disponibilidad de los sistemas, permitiendo al equipo técnico actuar antes de que los problemas escalen a incidentes graves. Además, estas alertas aportan visibilidad en tiempo real sobre la salud operativa de los servidores y sistemas clave, favoreciendo la toma de decisiones informadas para la continuidad del negocio.

3.1.6.3.3. Seguridad (Security) Autenticación:

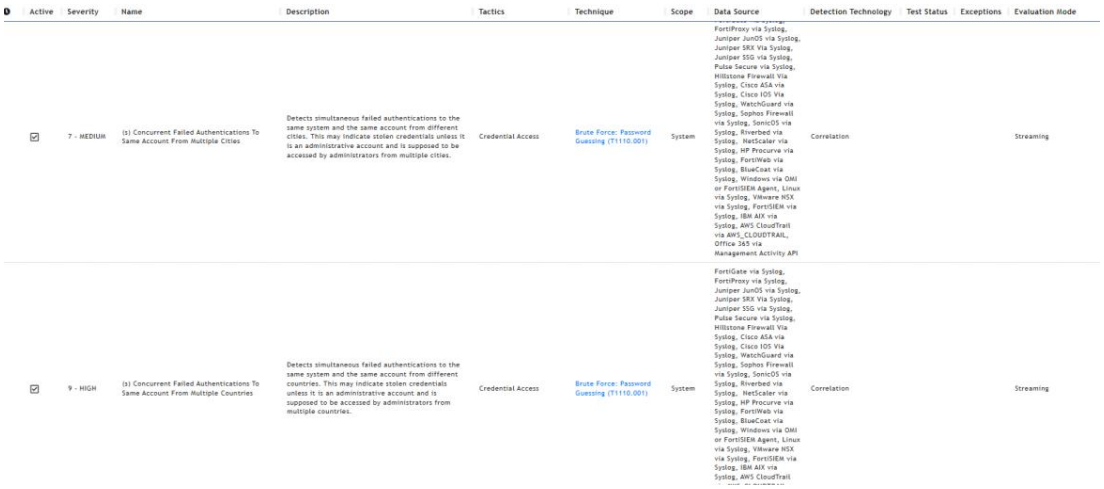
Los casos de uso de seguridad de autenticación en el FortiSIEM se centran en garantizar la integridad y la autenticidad de las credenciales de usuario en todos los dispositivos que tienen instalado el agente. Se muestran los casos Autenticación configurados para el ministerio de trabajo:



Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☑	6 - MEDIUM	(s) Account Locked: Domain	Detects account lockout caused by excessive logon failures	Credential Access	Brute Force: Password Guessing (T1110.001)	System	Windows via OMI or FortiSIEM Agent	Correlation			Streaming
☑	8 - MEDIUM	(s) Account Locked: Server	Detects account lockout caused by excessive logon failures	Credential Access	Brute Force: Password Guessing (T1110.001)	System	Windows via OMI or FortiSIEM Agent, Linux via Syslog	Correlation			Streaming
☑	9 - HIGH	(s) Brute Force App Login Success	Detects an unusual condition where a source has authentication failures followed by a successful authentication at the same app within 15 minutes	Credential Access	Brute Force: Password Guessing (T1110.001)	System	Apache via Syslog, JBOSS via Syslog, MS IIS via Syslog, F5 via Syslog, FortiGate via Syslog, FortiProxy via Syslog, Palo Alto PAN-OS via Syslog, Juniper JunOS via Syslog, Juniper SSLVPN Via Syslog, Pulse Secure via Syslog, Hillstone Firewall Via Syslog, Cisco ASA via Syslog, Windows via OMI or FortiSIEM Agent, WatchGuard via Syslog, Sophos Firewall via Syslog, SonicOS via Syslog	Correlation			Streaming
☑	9 - HIGH	(s) Brute Force Host Login Success	Detects an unusual condition where a source has authentication failures followed by a successful authentication at the same host within 15 minutes	Credential Access	Brute Force: Password Guessing (T1110.001)	System	FortiGate via Syslog, FortiProxy via Syslog, Juniper JunOS via Syslog, Juniper SRX Via Syslog, Juniper SSG via Syslog, Pulse Secure via Syslog, Hillstone Firewall Via Syslog, Cisco ASA via Syslog, Cisco IOS Via Syslog, WatchGuard via Syslog, Sophos Firewall via Syslog, SonicOS via Syslog, Riverbed via Syslog, NetScaler via Syslog, HP Procurve via Syslog, FortiWeb via Syslog, BlueCoat via Syslog, Windows via OMI or FortiSIEM Agent, Linux via Syslog, VMware NSX via Syslog, FortiSIEM via Syslog, IBM AIX via Syslog, AWS CloudTrail via AWS_CLOUDTRAIL,	Correlation			Streaming

Ilustración 121 Detalle casos de uso

Las alertas indican intentos repetitivos de autenticación fallida, lo cual es un patrón típico de ataques por fuerza bruta. Esto representa un riesgo directo a la confidencialidad e integridad de los sistemas.
También se reportan bloqueos de cuentas por intentos excesivos de inicio de sesión fallido, lo que puede interrumpir servicios críticos.



Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☑	7 - MEDIUM	(s) Concurrent Failed Authentications To Same Account From Multiple Cities	Detects simultaneous failed authentications to the same system and the same account from different cities. This may indicate stolen credentials unless it is an administrative account and is supposed to be accessed by administrators from multiple cities.	Credential Access	Brute Force: Password Guessing (T1110.001)	System	FortiProxy via Syslog, Juniper JunOS via Syslog, Juniper SRX Via Syslog, Juniper SSG via Syslog, Pulse Secure via Syslog, Hillstone Firewall Via Syslog, Cisco ASA via Syslog, Cisco IOS Via Syslog, WatchGuard via Syslog, Sophos Firewall via Syslog, SonicOS via Syslog, Riverbed via Syslog, NetScaler via Syslog, HP Procurve via Syslog, FortiWeb via Syslog, BlueCoat via Syslog, Windows via OMI or FortiSIEM Agent, Linux via Syslog, VMware NSX via Syslog, FortiSIEM via Syslog, IBM AIX via Syslog, AWS CloudTrail via AWS_CLOUDTRAIL, Office 365 via Management Activity API	Correlation			Streaming
☑	9 - HIGH	(s) Concurrent Failed Authentications To Same Account From Multiple Countries	Detects simultaneous failed authentications to the same system and the same account from different countries. This may indicate stolen credentials unless it is an administrative account and is supposed to be accessed by administrators from multiple countries.	Credential Access	Brute Force: Password Guessing (T1110.001)	System	FortiGate via Syslog, FortiProxy via Syslog, Juniper JunOS via Syslog, Juniper SRX Via Syslog, Juniper SSG via Syslog, Pulse Secure via Syslog, Hillstone Firewall Via Syslog, Cisco ASA via Syslog, Cisco IOS Via Syslog, WatchGuard via Syslog, Sophos Firewall via Syslog, SonicOS via Syslog, Riverbed via Syslog, NetScaler via Syslog, HP Procurve via Syslog, FortiWeb via Syslog, BlueCoat via Syslog, Windows via OMI or FortiSIEM Agent, Linux via Syslog, VMware NSX via Syslog, FortiSIEM via Syslog, IBM AIX via Syslog, AWS CloudTrail	Correlation			Streaming

Ilustración 122 Detalle de alertas

Acciones tomadas:

- Se analizaron inmediatamente los eventos de acceso a múltiples fallos, se crean casos de fuerza bruta en la herramienta de gestión Aranda.
- Se aplicaron límites de intentos de login, se implementaron bloqueos temporales inteligentes.
- Verificar si los accesos provienen de ubicaciones inusuales o direcciones IP sospechosas las cuales agregadas a las listas negras de mintrabajo.
- Se implementó autenticación multifactor (MFA) en todas las cuentas de mintrabajo.
- Rotación de contraseñas cada 60 días.

3.1.6.3.4. Violación de políticas (Policy violation)

Se han detectado múltiples alertas críticas y medias relacionadas con actividades potencialmente maliciosas o anómalas en sistemas Windows. Estas alertas están asociadas a prácticas de evasión de defensas, modificaciones no autorizadas, tráfico remoto y uso de software P2P (peer-to-peer), entre otras.



Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☑	9 - HIGH	(s) Multiple Windows Accounts Disabled by Administrator	Detects that multiple (more than 3) accounts were disabled by administrator in a short period of time			System	Windows Security Log via OMI or FortiSIEM Agent	Correlation			Streaming
☑	9 - HIGH	(s) Remote Desktop traffic from Internet	Detects remote desktop from the Internet, which is defined as anything outside the Internal network. Please make sure that the Internal network definition is correct to avoid false positives. Remote desktop is detected from a windows log or from a flow to the RDP port	Initial Access, Persistence, Lateral Movement, Command And Control	External Remote Services (T1133), Remote Services: Remote Desktop Protocol (T1021.001), Remote Access Software (T1219)	System	FortiGate via Syslog or Netflow, Checkpoint via Syslog or Netflow, Palo Alto via Syslog or Netflow	Correlation			Streaming
☑	7 - MEDIUM	(s) Windows Audit Policy Changed	Detects that a user changed Windows audit policy	Defense Evasion	Impair Defenses: Impair Command History Logging (T1562.003)	System	Windows Security Log via OMI or FortiSIEM Agent	Correlation			Streaming
☐	7 - MEDIUM	(s) Windows failed file access	Detects that a user failed to modify either the content or the attributes of a file or directory	Collection, Impact	Data from Local System (T1005), Data Manipulation: Stored Data Manipulation (T1565.001)	System	Windows Security log via OMI or FortiSIEM Agent	Correlation			Streaming
☑	9 - HIGH	(s) Windows Logging Service Shutdown	Detects that the windows logging service was shutdown	Defense Evasion	Impair Defenses: Disable Windows Event Logging (T1562.002)	System	Windows Security Log via OMI or FortiSIEM Agent	Correlation			Streaming
☑	7 - MEDIUM	(s) Windows Removable Media Inserts	Detects removable media inserts on Windows Servers	Collection	Data from Removable Media (T1025)	System	Windows via FortiSIEM Agent with UEBA turned on	Correlation			Streaming
☑	9 - HIGH	(s) Windows Security Log Cleared	Detects that a user cleared the windows security log	Defense Evasion	Indicator Removal on Host: Clear Windows Event Logs (T1070.001)	System	Windows Security Log via OMI or FortiSIEM Agent	Correlation			Streaming
☑	9 - HIGH	(s) Windows Security Log is Full	Detects that the windows security log buffer is full	Defense Evasion	Indicator Removal on Host: Clear Windows Event Logs (T1070.001)	System	Windows Security Log via OMI or FortiSIEM Agent	Correlation			Streaming
☐	5 - MEDIUM	(s) Windows successful file access	Detects that a user successfully modified either the content or the attributes of a file or directory	Collection, Impact	Data from Local System (T1005), Data Manipulation: Stored Data Manipulation (T1565.001)	System	Windows Security log via OMI or FortiSIEM Agent	Correlation			Streaming
☑	7 - MEDIUM	(s) Windows Torrent Client	Detects Torrent Client. Torrent is a method of file sharing over the Internet	Command And Control	Proxy: External Proxy (T1090.002)	System	Windows via FortiSIEM Agent with UEBA turned	Correlation			Streaming

Ilustración 123 Detalle de alertas

Acciones realizadas

- Se validaron actividades de usuarios con privilegios que hayan deshabilitado cuentas o modificado políticas de auditoría con los especialistas de Windows.
- Se monitoreó continuamente la integridad de los registros de eventos, aplicando controles que impidan su alteración mediante los equipos perimetrales

3.1.6.3.5. Overview incidentes

Durante enero 2025 se registraron:

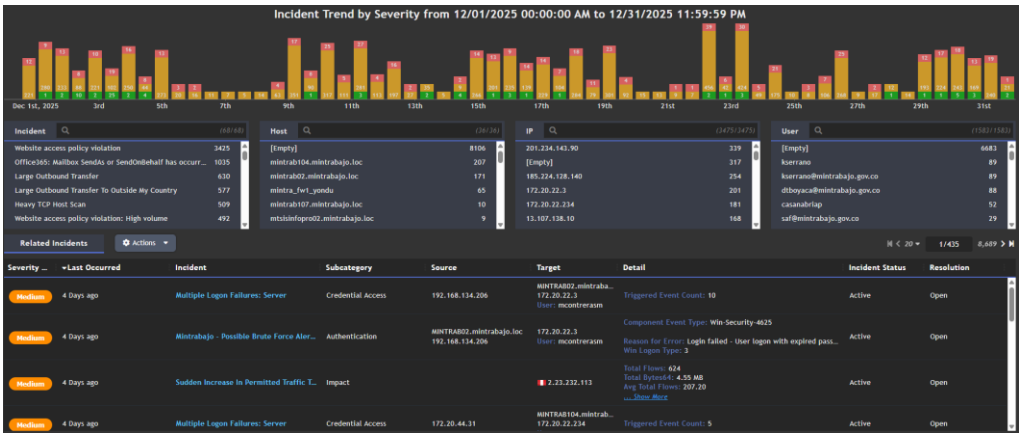


Ilustración 124 Detalle de incidentes

Análisis de incidentes

Tipo de incidente	Descripción	Volumen	Observaciones
Violaciones de política web	Accesos a categorías o sitios no permitidos por la política institucional	3.135	Requiere refuerzo de concientización y revisión de reglas de filtrado web.
Actividad Office 365 (SendOnBehalf)	Envíos de correo desde buzones compartidos o delegados	846	Actividad válida, pero altamente sensible; requiere control de permisos, auditoría y alertas específicas.
Transferencias salientes de gran volumen	Excesivo tráfico outbound detectado	588	Riesgo potencial de exfiltración o carga masiva; se recomienda análisis de usuarios, destinos y horarios.
Transferencias salientes fuera del país	Tráfico de gran volumen hacia destinos internacionales	540	Debe validarse legitimidad (cloud, backups, proveedores). Caso contrario, posible riesgo de fuga de información.
Escaneo TCP de alto volumen	Comportamiento tipo scanning desde host interno o externo	521	Indicador de actividades de pruebas de hacking
Violaciones web de alto volumen	Accesos repetitivos a contenido no permitido	492	aplicar bloqueos progresivos y control por usuario/IP.

Tabla 58 Tipos de incidentes

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 enero 2025. 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 120 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.

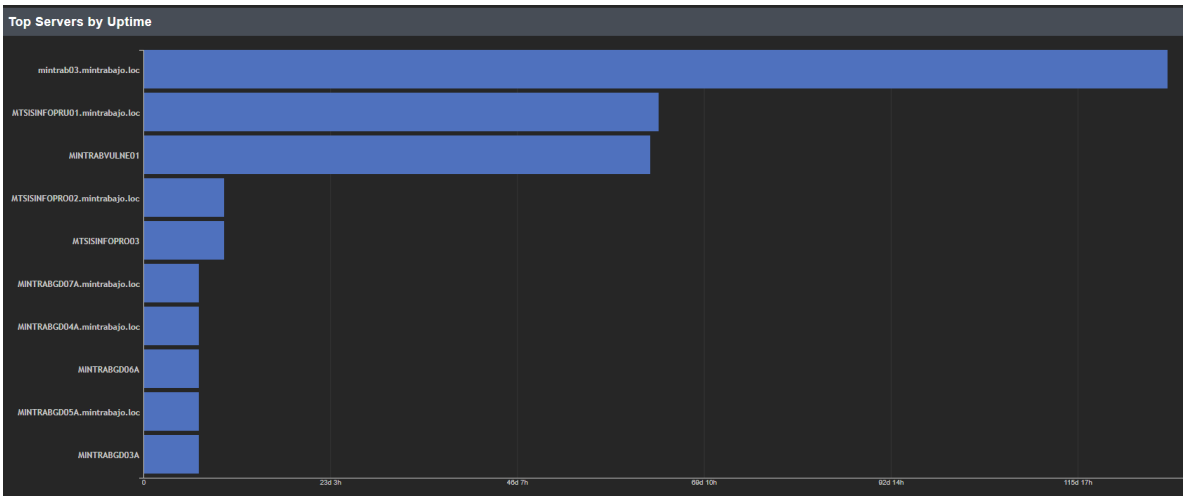


Ilustración 125 Detalle servidores

3.1.6.4.7 Top Aplicaciones por Bandwidth

Durante el último mes, el análisis del tráfico de red revela un uso intensivo de aplicaciones cifradas y servicios en la nube. El tráfico se concentra en protocolos seguros como HTTPS y SSL, lo cual indica una alta cantidad de navegación web y conexiones protegidas. También se observa un uso significativo de aplicaciones de mensajería y plataformas publicitarias, así como una fuerte participación de direcciones IP internas específicas.

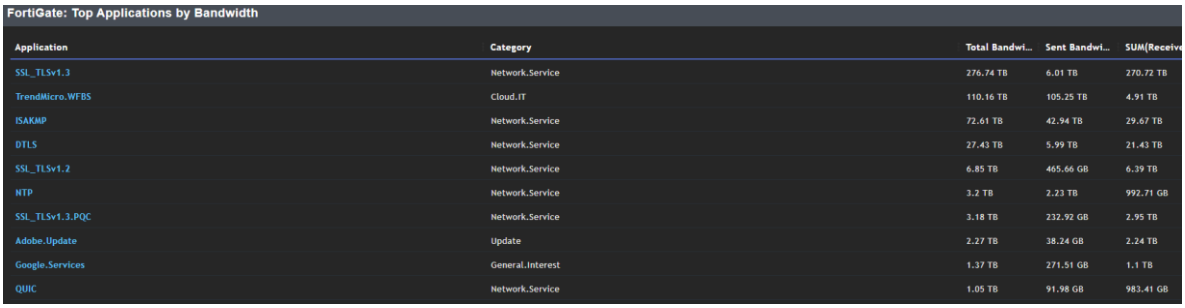
Este panel muestra que las aplicaciones que más ancho de banda consumieron fueron:

Consumo predominante:

- SSL/HTTPS: 270.72 TB
- DTLS: 21.43 TB

El tráfico revela un uso intensivo de:

- Aplicaciones cifradas.
- Servicios cloud.TrendMicro WFBS con alto volumen debido a actualizaciones.
- IPs de Google como destino principal del tráfico.



FortiGate: Top Applications by Bandwidth

Application	Category	Total Bandwi...	Sent Bandwi...	SUM(Receiv
SSL_TLSv1.3	Network.Service	276.74 TB	6.01 TB	270.72 TB
TrendMicro.WFBS	Cloud.IT	110.16 TB	105.25 TB	4.91 TB
ISAKMP	Network.Service	72.61 TB	42.94 TB	29.67 TB
DTLS	Network.Service	27.43 TB	5.99 TB	21.43 TB
SSL_TLSv1.2	Network.Service	6.85 TB	465.66 GB	6.39 TB
NTP	Network.Service	3.2 TB	2.23 TB	992.71 GB
SSL_TLSv1.3.PQC	Network.Service	3.18 TB	232.92 GB	2.95 TB
Adobe.Update	Update	2.27 TB	38.24 GB	2.24 TB
Google.Services	General.Interest	1.37 TB	271.51 GB	1.1 TB
QUIC	Network.Service	1.05 TB	91.98 GB	983.41 GB

Ilustración 126 Detalle fortigate

Esto refleja una alta dependencia de servicios cifrados para navegación web y otros tipos de comunicación segura. Otros protocolos presentes incluyen QUIC, ISAKMP, y Google Services, los cuales son comunes en aplicaciones modernas.

Conclusiones

El tráfico de red muestra un uso elevado de aplicaciones cifradas y plataformas cloud, lo que es consistente con entornos modernos, pero también requiere revisión de políticas de control de aplicaciones y uso aceptable.

Los servidores monitoreados presentan alta disponibilidad y baja latencia, indicando una infraestructura estable y sin degradaciones relevantes.

Durante el mes en curso se trabajó en el afinamiento de diversos casos de uso, incluyendo aquellos relacionados con la auditoría sobre el Directorio Activo (DA), donde se excluyeron los usuarios con permisos legítimos para realizar modificaciones sobre otras cuentas. Asimismo, se revisaron y ajustaron los procedimientos establecidos para los escalonamientos mediante la herramienta Aranda, con el fin de optimizar la gestión de los incidentes y mejorar la respuesta ante eventos de seguridad.

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

Durante el mes de enero 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.

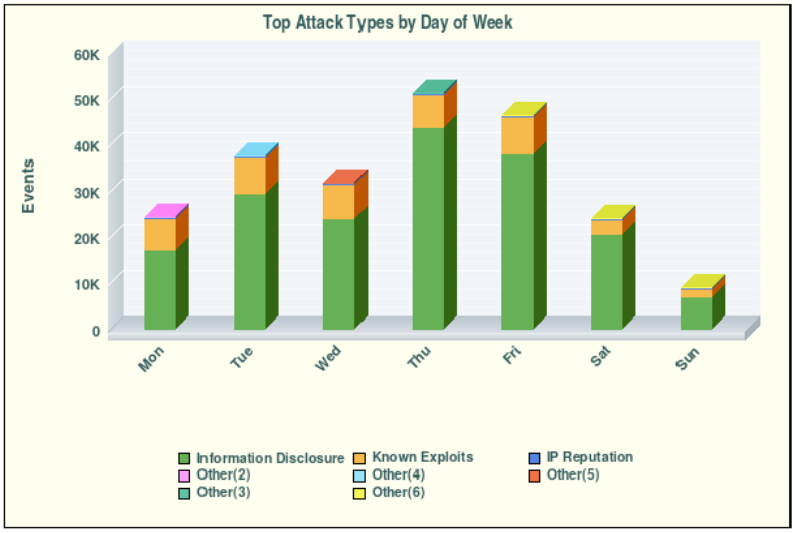


Ilustración 127 Top attack types

Análisis

Análisis	Descripción
Tipos de ataque predominantes	• El ataque más frecuente fue **Information Disclosure**, indicando intentos de reconocimiento sobre aplicaciones del Ministerio.
	• Alta presencia de **Known Exploits** como Log4Shell, Heartbleed y SACK Panic.
	• Actividad relevante de **IP Reputation**, reflejando tráfico proveniente de fuentes maliciosas.
Volumen y comportamiento temporal	• Ataques registrados **todos los días del mes**.
	• Se observaron picos de actividad en la **primera semana** y en **horarios nocturnos/fines de semana**, característicos de escaneos automatizados.
	• El entorno de amenaza es continuo y persistente.
Severidad de los ataques	• Se detectaron ataques de **severidad crítica**, principalmente asociados a vulnerabilidades explotadas globalmente (Log4j, Heartbleed).
	• La mayoría de los eventos son de severidad media y baja, pero con alto volumen acumulado.
	• El WAF bloqueó todos los intentos sin registros de compromisos exitosos.
Principales fuentes y destinos atacados	**Fuentes:** múltiples direcciones IP del extranjero, rangos con mala reputación e indicadores de botnets.
	Destinos: aplicaciones públicas del Ministerio, portales institucionales y servicios críticos expuestos a Internet.
Tipos de ataque más comunes	• Intentos de **SQL Injection**, **XSS**, **Path Traversal**, fuerza bruta y acceso no autorizado.
	• El objetivo de estos ataques es comprometer datos, manipular información o afectar la operación del servidor web.
Eficacia del WAF	• El WAF bloqueó **todos los eventos detectados**, demostrando un control robusto en primera línea.
	• No se evidencian evasiones o intrusiones exitosas.
	• Las políticas aplicadas son efectivas, aunque el volumen de ataques requiere **monitoreo continuo y ajuste preventivo**.

Tabla 59 Tipo de ataque

3.1.6.5 Solución de Anti-DDoS

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



Top Attacked SPPs

SPP	Direction	Drops	Events
PAGINA_MINTRABAJO	Outbound	82	5

Ilustración 128 Top de ataques

Análisis Detallado:

PAGINA_MINTRABAJO también muestra un número bajo de intentos salientes bloqueados (5), lo que sugiere riesgo bajo en aplicaciones web institucionales.

3.1.6.5.1 Login Fallidos

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

No. Caso	Fecha Registro	Asunto	Grupo Responsable	Categoria
RF-182336	30/01/2026 5:19	FortiSIEM Alert: TLP:RED - Mintrabajo - Malware Alert Trend Micro	SOC	Seguridad Informática
RF-177770	12/01/2026 5:43	FortiSIEM Alert: TLP:RED - Mintrabajo - Brute Force Host Windows Login Success	SOC	Seguridad Informática
RF-178061	13/01/2026 15:30	Mintrabajo - Login Attempts Using a Previously Disabled Account in Windows	SOC	Seguridad Informática

RF-178122	14/01/2026 0:46	FortiSIEM Alert: TLP:RED - Mintrabajo - Brute Force Host Windows Login Success	SOC	Seguridad Informática
RF-178740	15/01/2026 19:39	FortiSIEM Alert: TLP:RED - Mintrabajo - Brute Force Host Windows Login Success	SOC	Seguridad Informática
RF-179192	18/01/2026 20:54	FortiSIEM Alert: TLP:RED - Mintrabajo - Possible Brute Force Alert Windows	SOC	Seguridad Informática
RF-179568	20/01/2026 4:16	Mintrabajo - Office365 Phishing Attempt Detected	SOC	Seguridad Informática
RF-179966	21/01/2026 2:22	Mintrabajo - Malware Alert Trend Micro	SOC	Seguridad Informática
RF-180088	21/01/2026 10:54	Mintrabajo - Malware Alert Trend Micro	SOC	Seguridad Informática
RF-178250	14/01/2026 11:58	TLP:RED Boletín Lite // TI - Guloader como malware loader en campañas de ingeniería social dirigidas a empleados.	SOC	Agregar a listas negras
RF-178170	14/01/2026 9:22	MINTRABAJO | Navegación server segmento 43	SOC	Agregar a sitios permitidos
RF-177891	13/01/2026 10:07	MINTRABAJO | Validación Accesibilidad Puertos red 43-22	SOC	Agregar puertos
RF-178750	15/01/2026 21:39	MINTRABAJO | Navegación server segmento 43	SOC	Crear politica
RF-182582	30/01/2026 15:39	Solicitud de activación de paginas para tramites internos	SOC	Permitir acceso
RF-177084	6/01/2026 13:55	MINTRABAJO | Validación Accesibilidad Puertos red 43-22	SOC	Permitir acceso
RF-178078	13/01/2026 15:57	SOLICICITO ACCESO	SOC	Permitir acceso
RF-178482	15/01/2026 9:01	RE: MINTRABAJO | Validación Accesibilidad Puertos red 43-22	SOC	Permitir acceso
RF-179044	16/01/2026 14:21	Conexión Datacenter CALI - Bogotá	SOC	Permitir acceso
RF-180524	22/01/2026 14:25	RE: SOLICITUD ACTIVACION YOUTUBE	SOC	Permitir acceso
RF-180602	22/01/2026 16:23	Solicitud permisos navegación	SOC	Permitir acceso
RF-181387	27/01/2026 7:37	RV: ACCESO MULTIMEDIA	SOC	Permitir acceso
RF-181462	27/01/2026 9:19	RV: ACCESO MULTIMEDIA	SOC	Permitir acceso
RF-182512	30/01/2026 14:06	RV: Soporte de pago Pagare 382455 Recibidos	SOC	Revisar correo malicioso
RF-177606	9/01/2026 10:26	RV: SE ENVÍA RADICADO DE PROCESO JUDICIAL RAD-00283-OI82-GH72.	SOC	Revisar correo malicioso
RF-180257	21/01/2026 15:36	RV: OFICIO No. 01735 - COMUNICA FECHA DE AUDIENCIA - 26/01/2026	SOC	Revisar correo malicioso
RF-180680	23/01/2026 9:20	RE: Confirmación requerida de su cuenta institucional.	SOC	Revisar correo malicioso
RF-182074	29/01/2026 9:54	FortiSIEM Alert: TLP:RED - Mintrabajo - Possible Brute Force Alert Windows	SOC	Accesos por fuerza bruta
RF-182070	29/01/2026 9:52	FortiSIEM Alert: TLP:RED - Mintrabajo - Possible Brute Force Alert Windows	SOC	Accesos por fuerza bruta
RF-176633	2/01/2026 19:44	FortiSIEM Alert: TLP:RED - Mintrabajo - Possible Brute Force Alert Windows	SOC	Accesos por fuerza bruta
RF-177670	9/01/2026 13:16	FortiSIEM Alert: TLP:RED - Mintrabajo - Possible Brute Force Alert Windows	SOC	Accesos por fuerza bruta
RF-177771	12/01/2026 6:13	FortiSIEM Alert: TLP:RED - Mintrabajo - Possible Brute Force Alert Windows	SOC	Accesos por fuerza bruta
RF-177924	13/01/2026 10:37	FortiSIEM Alert: TLP:RED - Mintrabajo - Possible Brute Force Alert Windows	SOC	Accesos por fuerza bruta
RF-177933	13/01/2026 10:58	FortiSIEM Alert: TLP:RED - Mintrabajo - Possible Brute Force Alert Windows	SOC	Accesos por fuerza bruta
RF-177984	13/01/2026 13:00	FortiSIEM Alert: TLP:RED - Mintrabajo - Possible Brute Force Alert Windows	SOC	Accesos por fuerza bruta
RF-178593	15/01/2026 11:53	FortiSIEM Alert: TLP:RED - Mintrabajo - Possible Brute Force Alert Windows	SOC	Accesos por fuerza bruta
RF-178741	15/01/2026 19:44	FortiSIEM Alert: TLP:RED - Mintrabajo - Possible Brute Force Alert Windows	SOC	Accesos por fuerza bruta
RF-178746	15/01/2026 20:39	FortiSIEM Alert: TLP:RED - Mintrabajo - Brute Force Host Windows Login Success	SOC	Accesos por fuerza bruta
RF-178752	16/01/2026 6:51	FortiSIEM Alert: TLP:RED - Mintrabajo - Possible Brute Force Alert Windows	SOC	Accesos por fuerza bruta
RF-178966	16/01/2026 11:53	FortiSIEM Alert: TLP:RED - Mintrabajo - Brute Force Host Windows Login Success - Caso para el SOC bloqueo de IP y Verificación de LOGS	SOC	Accesos por fuerza bruta

RF-179164	16/01/2026 18:14	FortiSIEM Alert: TLP:RED - Mintrabajo - Possible Brute Force Alert Windows	SOC	Accesos por fuerza bruta
RF-179188	18/01/2026 5:08	FortiSIEM Alert: TLP:RED - Mintrabajo - Possible Brute Force Alert Windows	SOC	Accesos por fuerza bruta
RF-182535	30/01/2026 14:38	RV: RECORDATORIO PAGO MES DE ENERO 2026-CONTRATO 7357	SOC	Análisis de Correos
RF-182534	30/01/2026 14:37	RV: CONCILIACIÓN DE PAGO EMITIDA REF; FEV-18006 30 ENERO 2026	SOC	Análisis de Correos
RF-182516	30/01/2026 14:16	RV: FINALIZACION DE PROCESO DE OPERACION DE PAGO EMPRESARIAL | 177117825858	SOC	Análisis de Correos
RF-182414	30/01/2026 9:40	RV: CARTA DE DEMANDA IMPUESTA POR MARIO F RESTREPO P - DEMANDA IMPUESTA EL DIA 29 DE ENERO DEL 2026	SOC	Análisis de Correos
RF-176587	2/01/2026 12:33	RV: Happy New Year - ONGC Videsh Limited Sucursal Colombiana	SOC	Análisis de Correos
RF-176996	6/01/2026 8:29	RV: Su cuenta podría ser suspendida: Verificación de seguridad necesaria-	SOC	Análisis de Correos
RF-177671	9/01/2026 13:25	FortiSIEM Alert: TLP:RED - Mintrabajo - Malware Alert Trend Micro	SOC	Análisis de Correos
RF-177755	9/01/2026 20:47	Fw: Microsoft@Notificaciones.	SOC	Análisis de Correos
RF-181261	26/01/2026 15:09	RV: SE INFORMA INCIACION DE TRAMITE JUDICIAL POR DEMANDA REGISTRADA EN EL DESPACHO JUDICIAL	SOC	Análisis de Correos
RF-181561	27/01/2026 12:07	Solicitud de validación de correo sospechoso/	SOC	Análisis de Correos
RF-182637	31/01/2026 19:39	FortiSIEM Alert: TLP:RED - Mintrabajo - Malware Alert Trend Micro	SOC	Análisis de Malware

Tabla 60 Reporte de requerimientos enero

3.1.6.7 Análisis de riesgo

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

- **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:

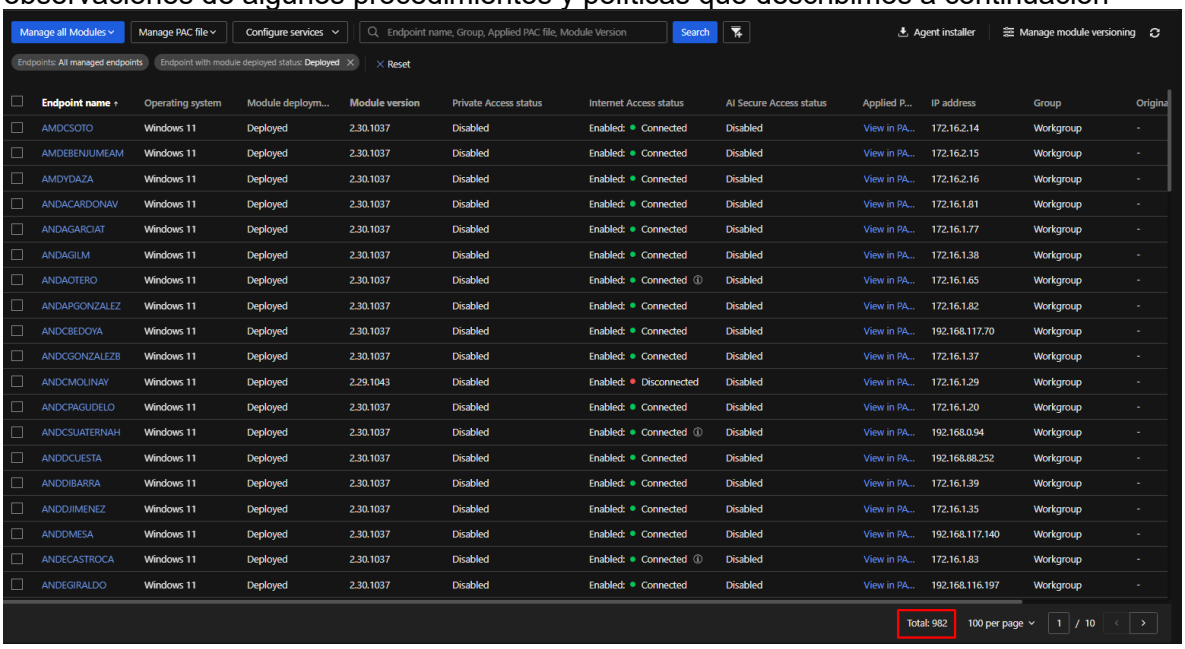
- Se están aplicando parches y actualizaciones de seguridad en la infraestructura de TI.
- Se realizó revisión periódica (semanal) de la matriz de vulnerabilidades y su priorización.
- Se realiza

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 enero 2026, se realizó la revisión, ajuste, observaciones de algunos procedimientos y políticas que describimos a continuación



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

Boletines Seguridad

19/01/2026 – MINTRABAJO
concientización en seguridad de la información (spoofing)
Riesgo: Ataques selectivos contra infraestructuras críticas.

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	100,00%	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	98,59%	90,00%
DC-10	Tiempo de solución de requerimientos asociado a los servicios de administración, soporte y monitoreo	99,81%	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 enero, no se observan caídas del canal, se tiene un consumo promedio de entrada de 27.3 Mbps y 61.48 Mbps de salida.

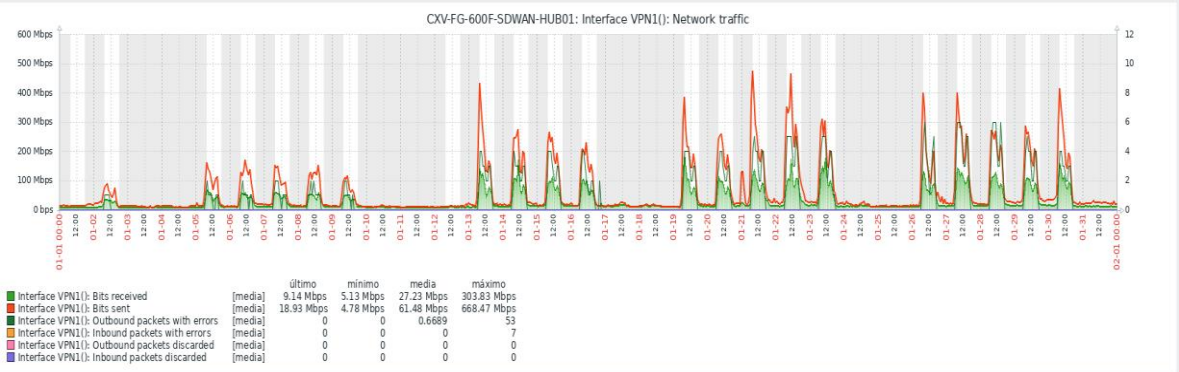


Ilustración 129 Consumo canal MPLS DC Principal

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 de 1% y de memoria de 40.7%, no se presenta problemas de procesamiento de equipo.

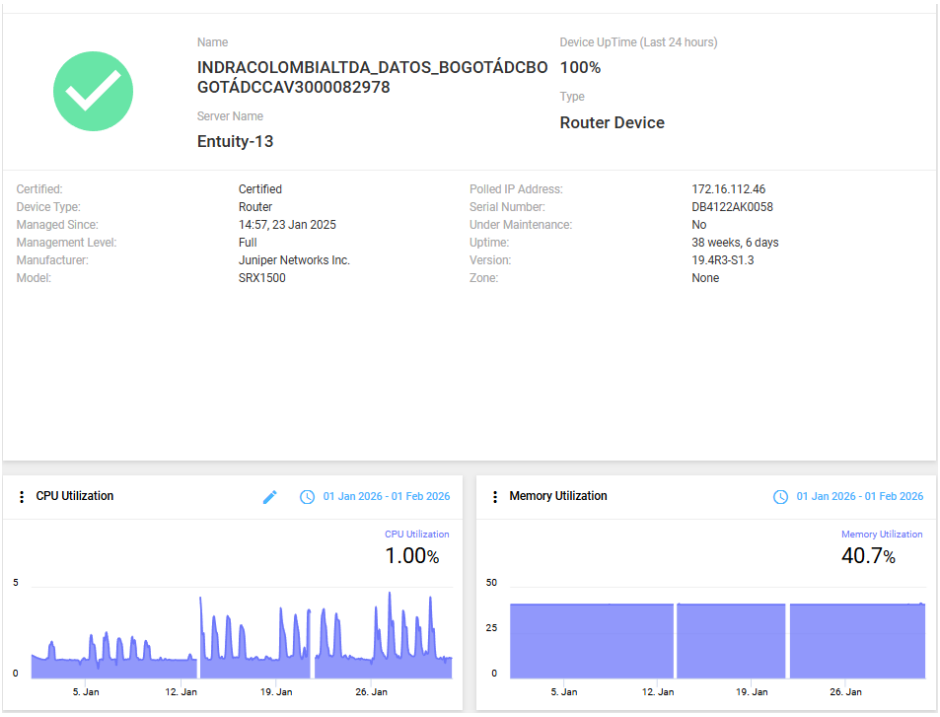


Ilustración 130 Estado Router MPLS DC Principal

3.3.1.1 Incidentes de Conectividad

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

Dirección Territorial	% de Disponibilidad	Caso Asociado
Sede Territorial Barrancaberneja	99,65	IM-181044
Sede Territorial Manizales	99,65	IM-181044
Sede Territorial Popayan	99,56	IM-176562
Sede Territorial Monteria	99,65	IM-181044
Sede Territorial Facatativa	99,65	IM-181044
Sede Territorial San Jose del Guaviare	98,90	IM-176661
Sede Territorial Santa Marta	98,13	IM-176661
Sede Territorial Pasto	94,96	IM-176905
Sede Territorial Armenia	99,65	IM-181044
Sede Territorial Pereira	99,65	IM-181044
Sede Territorial Sincelejo	99,29	IM-181044
Sede Territoria Apartado, Antioquia	99,65	IM-181044
Sede Territorial Cali	99,79	IM-181044
Sonson	96,79	IM-181044
La dorada	99,56	IM-176562
Santander de quilichao	99,56	IM-176562
Chiriguaná	98,97	IM-180646
Ubaté	99,64	IM-182063
Villeta	99,56	IM-176562
La plata	98,07	IM-182457
Pitalito	98,03	IM-180953
Puerto Gaitán	89,65	IM-180644
La virginia	99,56	IM-176562
Mariquita	91,27	IM-181407
Turbo	91,98	IM-181044
Cartago	99,56	IM-176562
Palmira	99,56	IM-176562
Sevilla	99,56	IM-176562
Tulua	99,40	IM-176562

Tabla 67 Incidentes de conectividad

3.3.1.2 Topología Actual

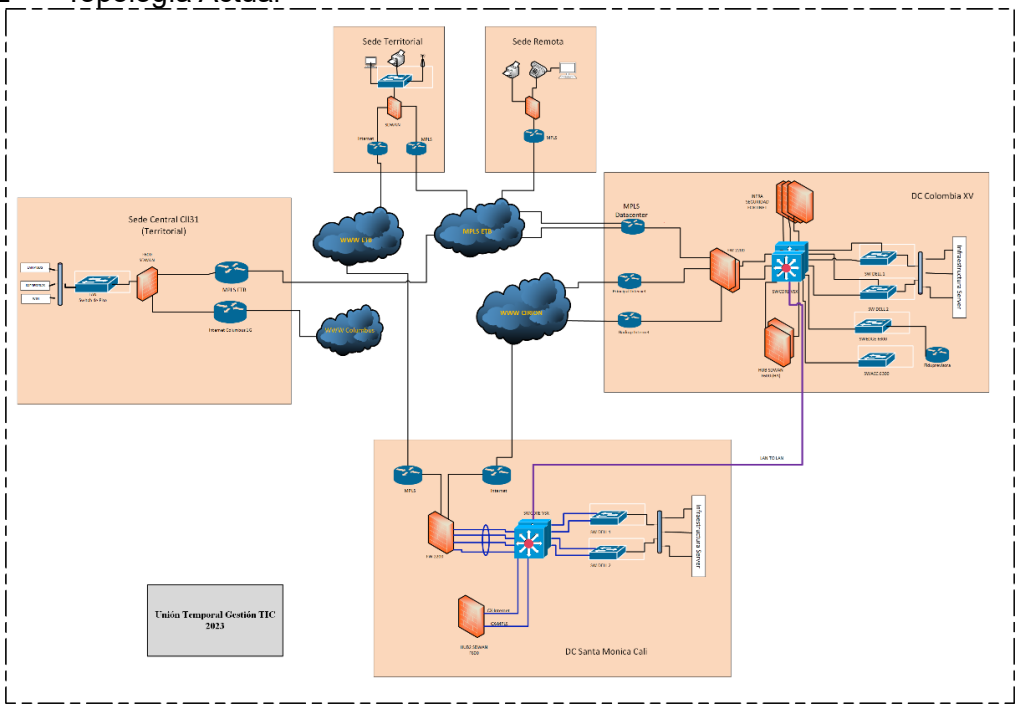


Ilustración 131 Topología actualizada

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 152 equipos registrados en esta plataforma.

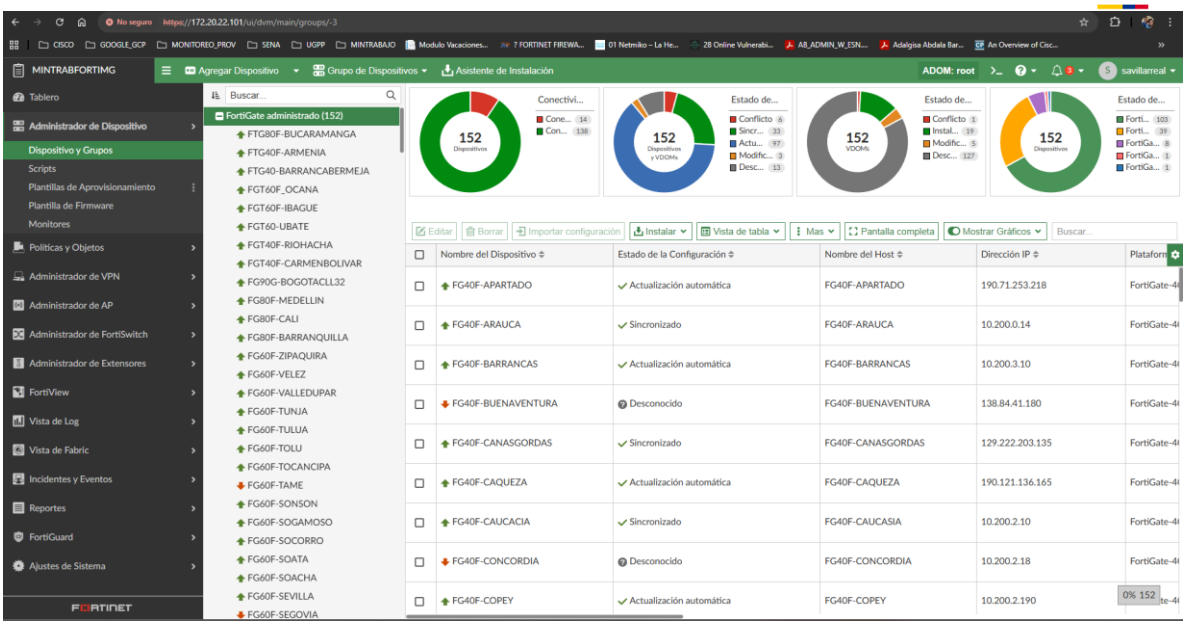


Ilustración 132 Interface Fortimanager

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 163.79 Mbps de consumo con un máximo de 1.09 Gbps, este canal es de 2GB, con el tráfico generado se observa que no presentó saturación durante el mes

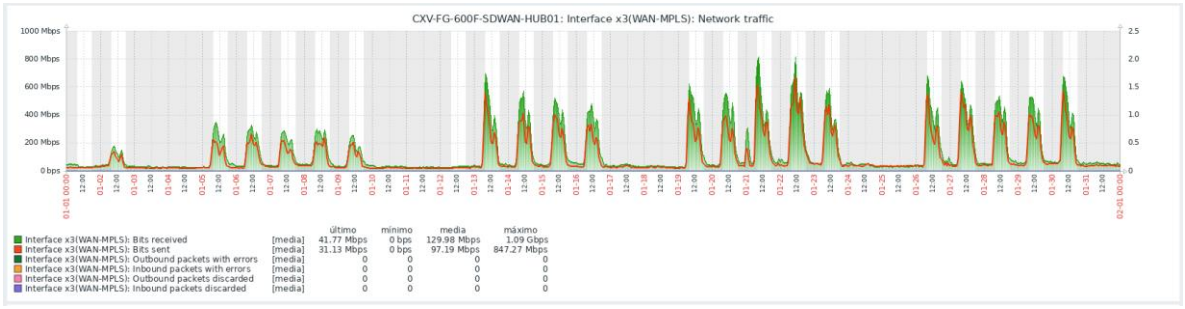


Ilustración 133 Interface MPLS HUB SDWAN

De igual forma, la interface de Internet del HUB no presenta saturación, por esta interface se establece el túnel Backup de las sedes territoriales. Se observa que se tuvo un promedio de 18.41 Mbps de consumo en el mes donde se tuvo un máximo de 450.6 Mbps. Este canal es de 1GB, con el tráfico generado en el mes, no se presentó saturación.

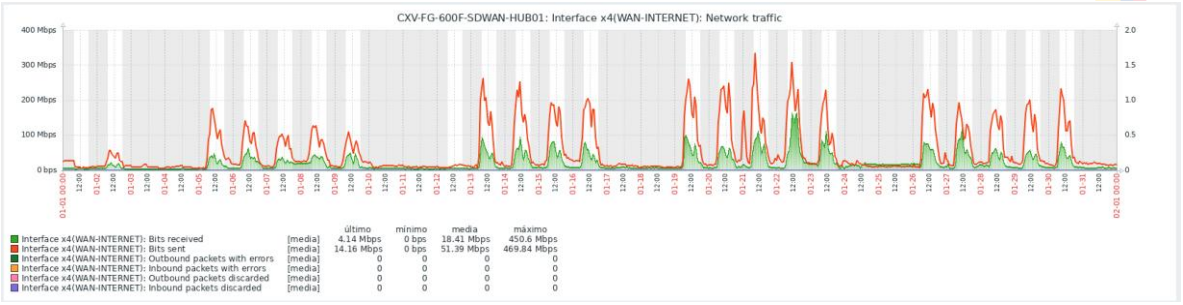


Ilustración 134 Interface Internet HUB SDWAN

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

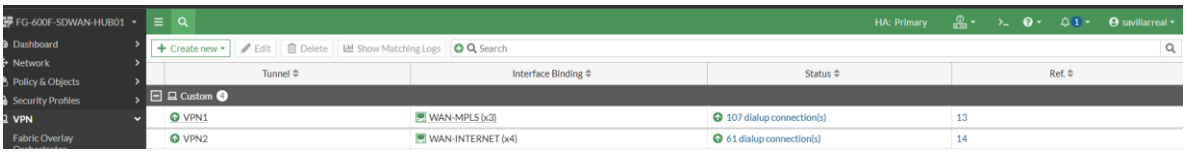


Ilustración 135 VPN SDWAN establecidas

El comportamiento del HUB SDWAN en cuanto a memoria y CPU, se observa que no ha tenido alto procesamiento, se observa un pico máximo de 22% de utilización de memoria y 6% de CPU, el equipo ha trabajado de forma estable sin presentar picos que causen algún bloqueo o algún reinicio de este.

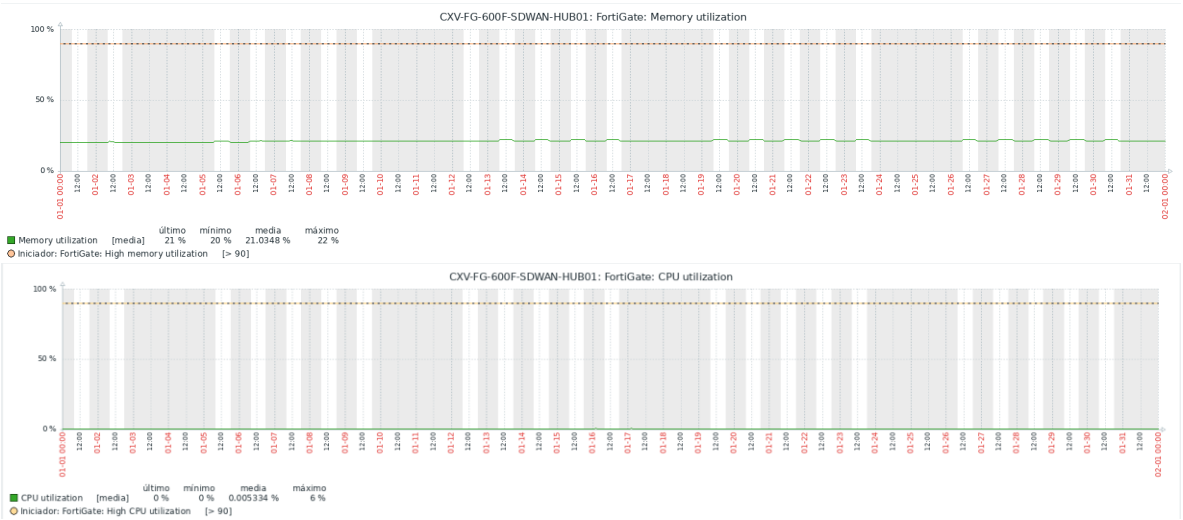


Ilustración 136 Estado HUB SDWAN Datacenter

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.

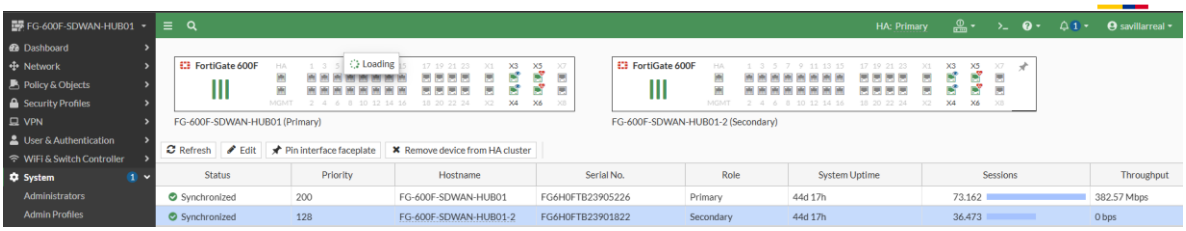


Ilustración 137 Estado HA HUB Sdwan

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 138 Recursos Fortimanager

Otras novedades del servicio:

Durante el mes de enero se realizaron las siguientes actividades:

- Se activo canal de Internet con Tigo en la sede de Ocaña, de esta forma se mejora el servicio de datos e Internet en la sede.

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 enero:

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

Dirección territorial	Población y/o ciudad de ubicación	Disponibilidad de la sede	% penalidad	Valor penalidad un enlace
ANTIOQUIA	SONSON	96,79	3%	$ 9.518
CALDAS	LA DORADA	99,56	3%	$ 9.518
CAUCA	SANTANDER DE QULICHAO	99,56	3%	$ 23.794
CESAR	CHIRIGUANA	98,97	3%	$ 9.518
CUNDINAMARCA	UBATÉ	99,64	3%	$ 9.518
CUNDINAMARCA	VILLETA	99,56	3%	$ 9.518
HUILA	LA PLATA	98,07	3%	$ 9.518
HUILA	PITALITO	98,03	3%	$ 9.518
META	PUERTO GAITÁN	89,65	10%	$ 31.725
QUINDIO	LA VIRGINIA	99,56	3%	$ 9.518
TOLIMA	MARIQUITA	91,27	10%	$ 31.725
OE APARTADO	TURBO, ANTIOQUIA	91,98	3%	$ 9.518
VALLE	CARTAGO	99,56	3%	$ 9.518
VALLE	PALMIRA	99,56	3%	$ 9.518
VALLE	SEVILLA	99,56	3%	$ 9.518
VALLE	TULUA	99,40	3%	$ 9.518
			Total	**$ 210.975**

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	Población y/o ciudad de ubicación	Disponibilidad de la sede	% penalidad	Valor penalidad doble enlace
Sede Territorial Medellin	MEDELLIN	99,44	3%	$62.774
Sede Territorial Arauca	ARAUCA	99,83	3%	$25.110
Sede Territorial Barrancaberneja	BARRANCABERMEJA	99,65	3%	$ 25.110
Sede Territorial Manizales	MANIZALEZ	99,65	3%	$37.664
Sede Territorial Popayan	POPAYAN	99,56	3%	$37.664
Sede Territorial MONTERIA	MONTERIA	99,65	3%	$50.219
Sede Territorial Facatativa	FACATATIVÁ	99,65	3%	$50.219
Sede Territorial San Jose del Guaviare	SAN JOSE DEL GUAVIARE	98,90	3%	$12.555
Sede Territorial Santa Marta	SANTA MARTA	98,13	3%	$37.664
Sede Territorial Pasto	PASTO	94,96	10%	$125.548
Sede Territorial Armenia	ARMENIA	99,65	3%	$37.664
Sede Territorial Pereira	PEREIRA	99,65	3%	$50.219

Sede Territorial Sincelejo	SINCELEJO	99,29	3%	$37.664
Sede Territoria Apartado, Antioquia	APARTADÓ, ANTIOQUIA	99,65	3%	$25.110
Sede Territorial Cali	CALI	99,79	3%	$87.884
			Total	**$703.069**

Tabla 70 Desagregado sedes con novedad con doble enlace

4 LINEA DE SERVICIOS EN SEDE

4.1.1 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**	1153	19
Equipos portátiles	**1000**	958	162
Equipos portátiles adicionales	**120**		
Total	**2292**	**2111**	**181**

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 continuó recibiendo el aval por parte del Coordinador del Grupo de Soporte Informático para la asignación de equipos de cómputo destinados a contratistas, pasantes, casos de doble asignación para funcionarios, salas de conciliación y la Contraloría.

Adicionalmente, se continua la asignación de equipos de cómputo de escritorio según el listado de funcionarios con condiciones médicas especiales entregado por el Coordinador del Grupo de Soporte Informático, no se ha logrado culminar ya que su avance depende de la disponibilidad de los usuarios para efectuar el respectivo cambio.

- **Gestión de Inventario**:

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

ASIGNACION DE EQUIPOS ENERO		
SEDE	**TIPO DE ELEMENTO**	**CANTIDAD**
Nivel Central	Portátil	22
Nivel Central	Escritorio	9
OE Apartado	Portátil	1
DT Antioquia	Portátil	5
OE Barrancabermeja	Portátil	3
TOTAL		**40**

Tabla 72 Cantidades de equipos asignados nivel nacional

DEVOLUCION DE EQUIPOS ENERO		
SEDE	**TIPO DE ELEMENTO**	**CANTIDAD**
DT Bogotá	Escritorio	4
DT Bolívar	Portátil	4
DT Bolívar	Escritorio	1
DT Boyacá	Escritorio	1
Insp. Santander de Quilichao	Escritorio	1
DT Córdoba	Portátil	1
DT Magdalena	Portátil	1
DT Meta	Portátil	2
Nivel Central	Portátil	24
Nivel Central	Escritorio	2
DT Santander	Escritorio	1
DT Tolima	Portátil	1
DT Vaupés	Escritorio	1
TOTAL		**44**

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 enero, se reportó un total de 18 casos de garantía. A continuación, se detallan los estados asociados a estos casos:

Estado de caso	Cantidad
Cerrado	10
Solucionado	1
Suspendido	7
Total	18

Tabla 74 Estado de casos de garantía.

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

ANS	Cerrado	Solucionado	Suspendido	Total
CUMPLE	10	1	5	16
NO CUMPLE			2	2
Total	10		7	18

Tabla 75 ANS casos de garantía.

Fecha de Reporte	Serial	Parte	Falla	Sede	No. Caso	Estado
19/01/2026	3CS5089	Cargador	Denuncia por Hurto a	DT Bogotá	RF-179205	Cerrado
26/01/2026	HC3BBLT8	Diadema	Garantía De Diadema	Nivel central	RF-181038	Cerrado
23/01/2026	HC3BBLWX	Diadema	Falla diadema	DT Antioquia	RF-180721	Cerrado
20/01/2026	HC3BBMN1	Diadema	Solicitud Garantía Diadema.	Nivel central	RF-179722	Cerrado
15/01/2026	HC3BBMC9	Diadema	Garantía Diadema	Nivel central	RF-178642	Cerrado
15/01/2026	HC3BBN5G	Diadema	Falla de diadema	DT Bogotá	RF-178467	Cerrado
15/01/2026	3CS5089	Cargador	HURTO DE CARGADOR	DT Bogotá	RF-178453	Cerrado
13/01/2026	HC3BBLN1	Diadema	Solicitud garantía auriculares	DT Atlántico	RF-177931	Cerrado
8/01/2026	HC3BAHHG	Diadema	Solicitud cambio diadema	Nivel central	RF-177453	Cerrado
6/01/2026	VNAA64GK	Monitor	Reporte de falla en monitor	OE Apartado	RF-176982	Cerrado
29/01/2026	HC3BBLTP	Diadema	Garantía diadema	DT Arauca	RF-182066	Solucionado
15/01/2026	PW0A3CG9	Portátil	Afectación en el puerto de carga	Insp. Puerto Gaitán	RF-178599	Suspendido
5/01/2026	PW09Z348	Portátil	GARANTIA EQUIPO PORTATIL	Nivel central	RF-176749	Suspendido
5/01/2026	PW0A0FN2	Portátil	RV: Denuncia hurto	Nivel central	RF-176659	Suspendido
22/01/2026	AVLC39SA443	Mouse	Solicitud Garantía Mouse	DT Neiva	RF-180383	Suspendido
16/01/2026	AVLC3C5A27A	Teclado	Solicitud de garantía Teclado	DT Vichada	RF-179066	Suspendido
20/01/2026	VNAA64D8	Monitor	Solicitud garantía monitor	OE Barrancabermeja	RF-179621	Suspendido
8/01/2026	VNAA627D	Monitor	Solicitud de garantía de pantalla	OE Buenaventura	RF-177492	Suspendido

Tabla 76 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

Funcionario responsable	Serial	DT	Parte afectada	Estado	Caso Aseguradora/ Lenovo
Bernardo Ardila Fernández	PW09Z34H	Valledupar	Golpes en esquinas	Aseguradora hace entrega de equipo pendiente devolución de equipo dañado	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/ Cauca	No enciende	Se deja una cpu de reposición/Aseguradora/ 09/05/2025 Pendiente reposición del equipo	PRG_2025_1766918
Lacides Manuel Morales Ortega	MJ0LS5XL	Sincelejo/ San Marcos	Se apaga y no enciende	Aseguradora 19/05/2025 pendiente reposición de equipo	PRG_2025_1921454
Jesús Manuel Martínez Franco	PW0A3BEY	Montería	Golpes en esquinas	Aseguradora hace entrega de equipo PW0A370B, Pendiente acta de asignación funcionario de vacaciones	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 pendiente devolución de equipo dañado	PRG_2025-4611910
Maria Isabel Cuenca Mendoza	PW0A3BPB	Cali Valle	no responde correctamente a comandos del teclado integrado	Se envía documentación para iniciar proceso con la aseguradora 16/12/2025	
Laura Estefanía Mendoza Quintero	PW0A3CKM	DT Quindío	Robo	Se realiza envió de portátil PW0A3BHA de contingencia	
Valeria Márquez Pereira	PW0A3AZW	Nivel central	Robo	Se realiza asignación de equipo de contingencia PW0A36XS	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 envía documentación para trámite ante aseguradora 05/01/2026-- Se realiza asignacion de equipo PW09ZT6H	

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 18 solicitudes tipificadas así:
  - Incidentes: 0 casos
  - Requerimientos: 18 casos

- Al corte de mes quedaron en estado:
  - Cerrado: 10 casos.
  - Solucionado: 1 caso
  - Suspendido: 7 casos.

- 17 casos corresponden a solicitudes de usuarios estándar y 1 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	15
Gestor de inventarios	3
Total, general	18

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	**18**
Equipo Periférico	11
Equipo Escritorio	3
Equipo Portátil	4
Total	18

Tabla 79 Solicitudes de Equipos Usuario Final – Según Grupo Responsable

4.1.2 Equipos de Escritorio

Durante el mes de enero, 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 enero 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.

- **Medición de ANS Equipo de usuario final**

A continuación, el resultado de la medición de los ANS para los equipos de usuario final:

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

Tabla 80 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.
- Se realizó gestión y seguimiento a alertas sobres canales de comunicación (MPLS e Internet) para lograr el restablecimiento del servicio por parte del proveedor de conectividad.
- Se realizaron pruebas con el soporte de Neiva sobre la red wifi y se confirmó integración de los 2 access point propiedad del ministerio con el servidor Radius para la autenticación de los usuarios.
- Se gestionó el mantenimiento de UPS en oficinas territoriales con el aliadado Apicom.
- Se instaló y configuró canal de internet con servicio Starlink en la territorial de Buenaventura.

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

- Los especialistas gestionaron un total de 21 solicitudes escaladas a través de la herramienta Aranda. Al corte del mes 16 casos quedaron en estado Cerrado, 2 casos quedaron en estado solucionado y 3 casos quedaron en estado suspendido. los casos obedecen a revisión de alertas sobre caída de servicios de conectividad, degradación y lentitud sobre los canales. 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
Sin servicio	5
Incidente Mayor	4
Equipo Conectividad internet	3
FortiGate	3
Lentitud enlace	2

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

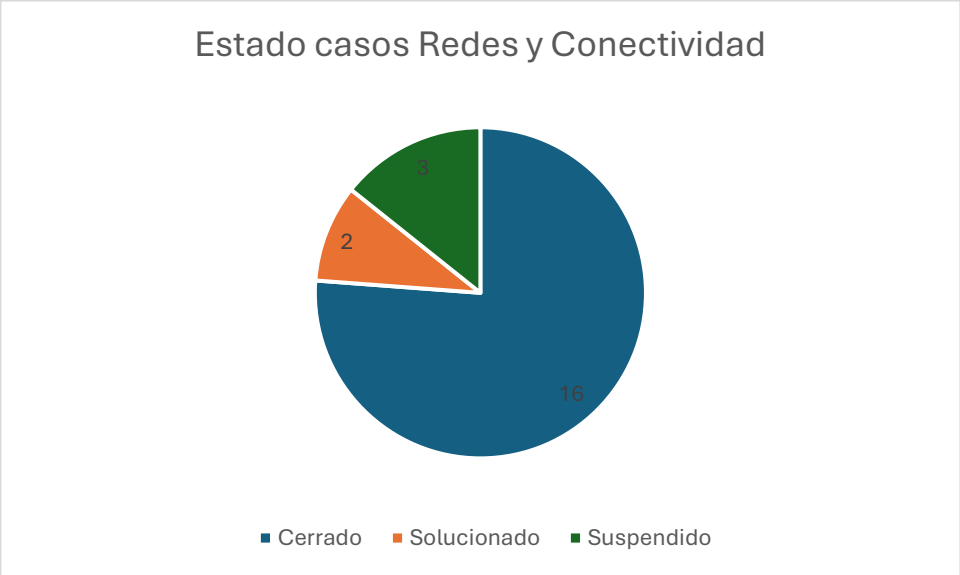


Ilustración 139 Estado de casos Redes y Conectividad

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	47
	Total	**111**

Tabla 84 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.

- **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 86 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 enero 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.
- 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-169500.



Asignación ext.
virtual_Teams_Caso_F

- **Asignación de Licencias – Extensiones**

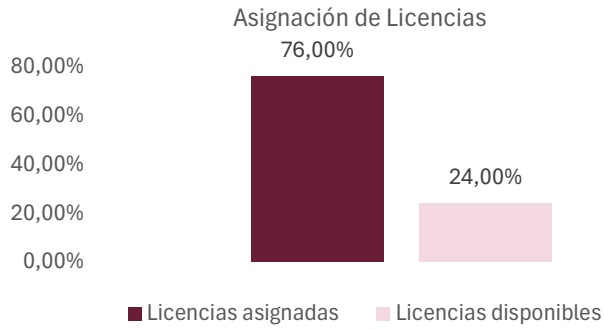


Ilustración 140 Asignación de licencias

Durante el mes en gestión, se han asignado un total de 455 extensiones a nivel nacional. Actualmente, permanecen disponibles 145 extensiones.

- **Estadísticas de Tráfico**

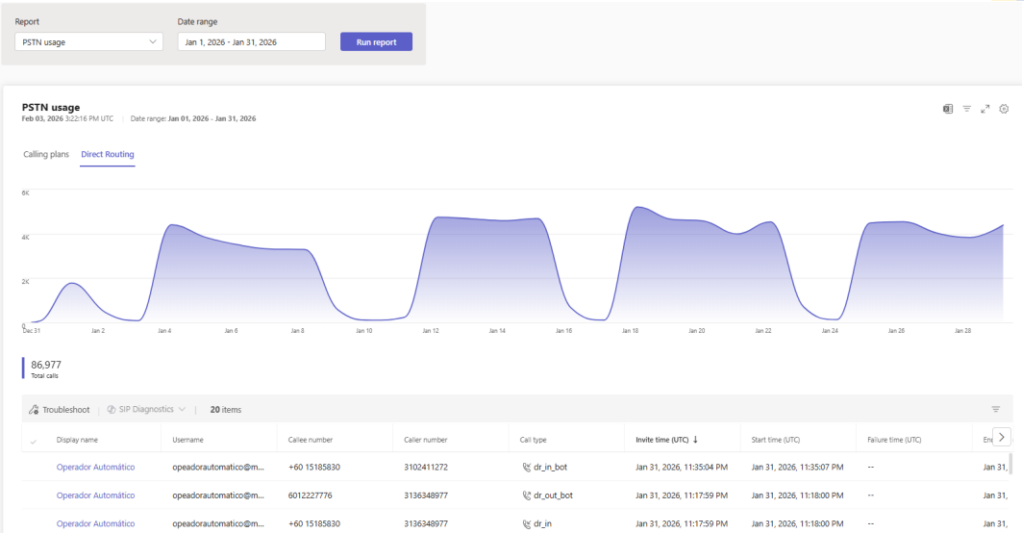


Ilustración 141 Comportamiento de tráfico

En la gráfica anterior se visualizan las tendencias de uso del servicio, en el periodo correspondiente al mes de enero de 2026, donde se atendieron un total de 86,977 llamadas.

Servicio	Minutos Disponibles	Minutos Utilizados
Locales	Ilimitados	906.36
Celular	1000	756.36
Nacional	Ilimitados	408.38
Internacional	700	6.1
Total		2077.2

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 enero de 2026, se identifica que se realizaron llamadas con una duración total de 408.38 minutos.

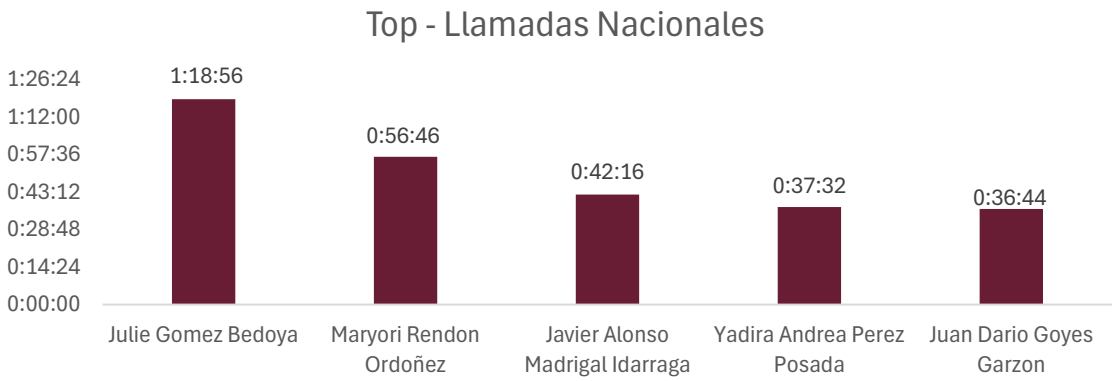


Ilustración 142 Top llamadas nacionales

N°	Usuario	Área	Tiempo llamadas
1	Julie Gomez Bedoya	Grupo Atención al Ciudadano – Valle Del Cauca	1:18:56
2	Maryori Rendon Ordoñez	Despacho Barrancabermeja	0:56:46
3	Javier Alonso Madrigal Idarraga	Grupo de Resolución de Conflictos - Antioquia	0:42:16
4	Yadira Andrea Perez Posada	Grupo de Resolución de Conflictos - Antioquia	0:37:32
5	Juan Dario Goyes Garzon	Dialogo Social - Antioquia	0:36:44

Tabla 91 Top 5 consumo de llamadas

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

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

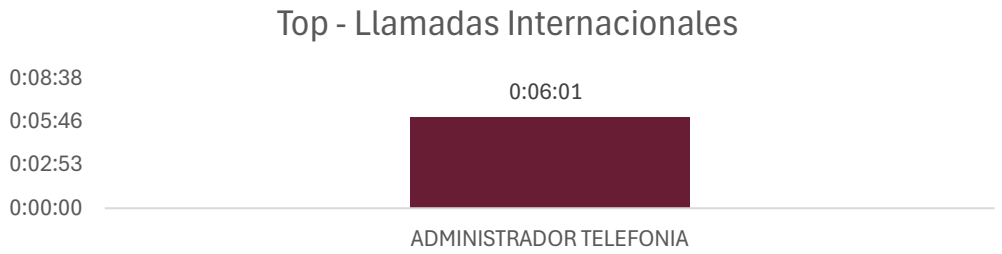


Ilustración 143 llamada internacional de prueba

Como se puede observar en el grafico anterior, se evidencia que, en el mes de enero 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	0:06:01

Tabla 92 Top 5 llamadas LDI

- **Consumo de llamadas destinos celulares**

Con respecto a las llamadas realizadas a celular en el mes de enero de 2026, se identifica que se realizaron llamadas con una duración total de 756.36 minutos (12,60 horas).

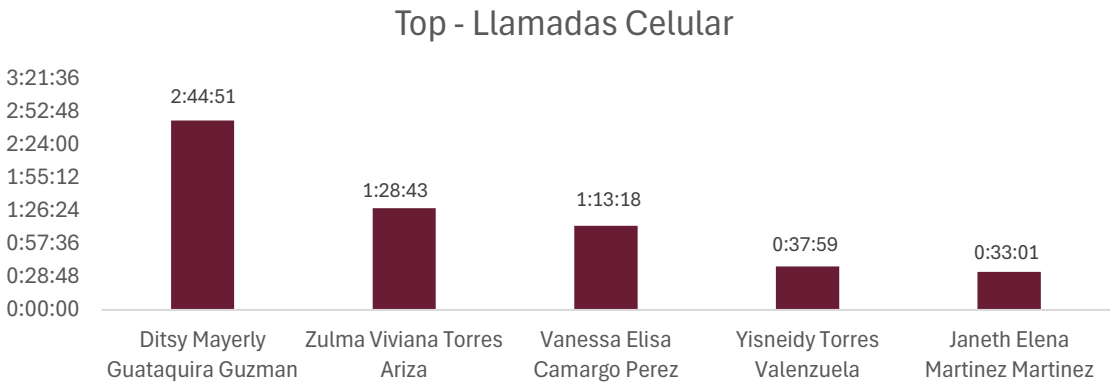


Ilustración 144 Top Celular

N°	Usuario	Área	Tiempo llamadas
1	Ditsy Mayerly Guataquira Guzman	Comunicaciones DT Bogotá	2:44:51
2	Zulma Viviana Torres Ariza	Comunicaciones DT Bogotá	1:28:43
3	Vanessa Elisa Camargo Perez	Conciliaciones DT Bolivar	1:13:18
4	Yisneidy Torres Valenzuela	Inspectora Caqueta	0:37:59
5	Janeth Elena Martinez Martinez	Subdirección Administrativa y Financiera Bogotá	0:33:01

Tabla 93 Top 5 llamadas Celular

- **Consumo de llamadas locales**

Con respecto a las llamadas realizadas a destinos locales en el mes de enero de 2026, se identifica que se realizaron llamadas con una duración total de 906.16 minutos (15,10 horas).

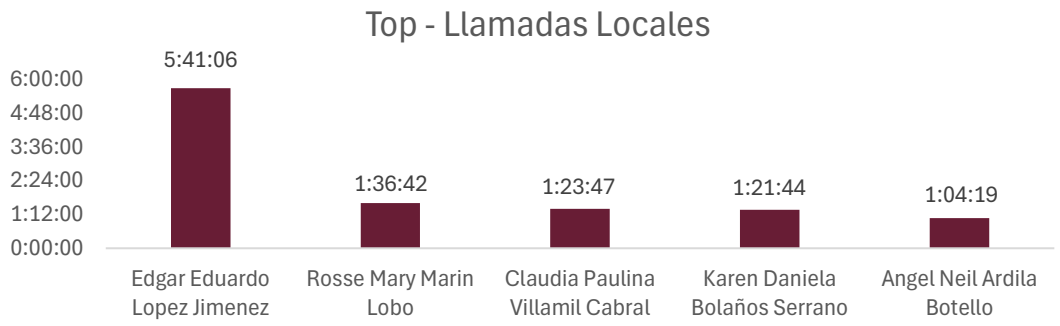


Ilustración 145 Top Local

N°	Usuario	Área	Tiempo llamadas
1	Edgar Eduardo Lopez Jimenez	Grupo RCC Bogotá	5:41:06
2	Rosse Mary Marin Lobo	Despacho Oficina Especial Barrancabermeja	1:36:42

3	Claudia Paulina Villamil Cabral	Grupo interno de trabajo de analisis y monitoreo de información Bogotá	1:23:47
4	Karen Daniela Bolaños Serrano	Grupo viceministro de empleo y pensiones Bogotá	1:21:44
5	Angel Neil Ardila Botello	Grupo De Atención al Ciudadano Bogotá	1:04:19

Tabla 94 Top 5 llamadas locales

- **Capacitaciones y divulgaciones**

En el mes de enero 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 146 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

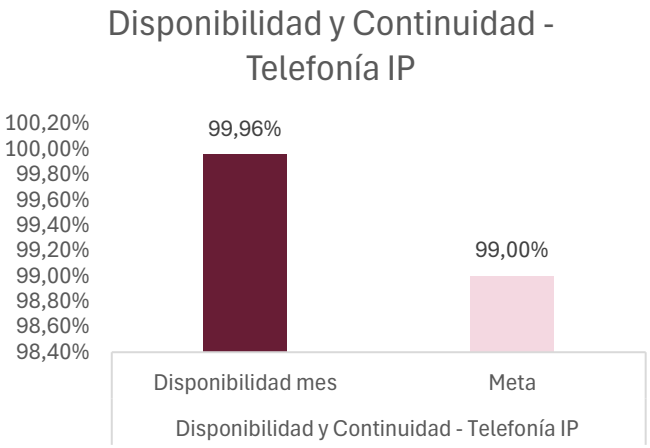


Ilustración 147 Disponibilidad y Continuidad TOIP

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

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

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

Tabla 95 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 96 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 97 Inventario de UPS – 20Kva

- **Gestión del servicio**

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

A continuación se relacionan los casos gestionados:

Ticket	Tipo de caso	Descripción	Solución / Avance	Estado
RFC-180220, RFC-178698, RFC-178201, RFC-178197, RFC-177646, RFC-177568	Cambio	Se gestionan cambios con el respectivo RFC para atención de mantenimientos preventivos de UP de territorio y revisión de tarjeta de red de UPS de Nivel Central.	Atención de mantenimientos sin novedades, en revisión tema de tarjetas de red de algunas UPS de Bogotá. Equipos operativos	Cerrados
RF-179511	Requerimiento	Solicitamos tu amable colaboración para apoyarnos con la revisión de la UPS de Pereira ya que presenta la alerta "UPS en estado Bypass"	La alarma de bypass de la UPS tuvo una duración de 1d 20h 57m. Se confirma que el personal especializado de APICOM hace la respectiva llamada y en conjunto con el personal de soporte en sitio brindan la respectiva solución a falla presentada **1. Descripción de la falla:** Se evidenció que la UPS se encontraba operando en modo BYPASS, condición que impedía el suministro regulado de energía a la carga crítica. Durante la inspección inicial se determinó que la condición fue ocasionada por un **pico eléctrico** proveniente de la red comercial, el cual generó el disparo automático de las llaves de protección internas del equipo. **2. Diagnóstico realizado:** Verificación de estado operativo de la UPS. - Revisión de alarmas y registros de eventos. - Inspección de llaves de potencia y protecciones internas. - Confirmación de que no se presentaban daños permanentes en módulos, inversor ni baterías. Se concluye que la UPS ingresó a bypass como mecanismo de protección ante la sobretensión registrada. **3. Actividades ejecutadas** - Restablecimiento de las llaves de potencia que se encontraban disparadas. - Reconfiguración de la secuencia de operación de acuerdo con el procedimiento del fabricante. - Salida controlada del modo BYPASS. - Pruebas funcionales de transferencia, carga y retorno a modo normal. **4. Resultado final**	Cerrado

			Una vez realizadas las actividades: La UPS quedó operando en modo normal (ONLINE). Se restableció el suministro regulado de energía a la carga. No se evidencian alarmas activas ni fallas adicionales. Equipo queda operativo y estable.	

Tabla 98 Casos gestionados – Energía Eléctrica Regulada UPS

- **Mantenimiento Preventivo de UPS**

Durante el período se realiza el mantenimiento preventivo de UPSs de territorio así:

- El 9/01/2026 de las UPS Ibagué, Tunja y Pereira a partir de las 4pm, se gestiona bajo el cambio RFC-177568.
- El 13/01/2026 de la UPS de Medellin a partir de las 4pm, se gestiona bajo el cambio RFC-177646.
- El 16/01/2026 de la UPS de Barrancabermeja (RFC-178698), Manizales (RFC-178201), Cartagena (RFC-178704) a partir de las 4pm.
- El 21/01/2026 de la UPS de Bucaramanga a partir de las 4pm, queda una alarma la cual el 26/01/2026 fue revisada y solventada por el aliado (asociada a la variación de voltajes en la sede).

Durante las ventanas se realiza apagado de equipos, rutina de limpieza general interna y externa de las UPS, encendido y verificación de servicios. No se presentan novedades durante la ventana.

Se consolidaron las actas de atención en el repositorio dado por la entidad para el contrato.
Ruta Repositorio MinTrabajo: Mantenimientos_Preventivos_2025

- **Novedades UPS**

- En febrero 2025 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. A espera de recibir apoyo 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 efectuó el 15/12/2025 el RFC de revisión con especialista pero no se logró solventar, se tiene escalado con fábrica Ablerex.
El 13/01/2026 personal del aliado asiste a la sede para toma de evidencias conjuntas para alimentar el caso que se tiene con el fabricante.
El 14/01/2026 se gestiona RFC-178197 para las 6pm con el propósito de hacer reconfiguración de la tarjeta de red de las UPS de Nivel Central, por parte del aliado. Como resultado no fue posible acceder a la configuración de las tarjetas de red, no obstante las UPS quedan operativas funcionando correctamente. Se validaron los pisos 18 y 17.
El 21/01/2025 bajo el RFC-180220 se desplaza especialista de UPS, para realizar acciones adicionales en búsqueda de conseguir la reconfiguración de la tarjeta de red de las UPS de Nivel Central (pisos 3, 9, 17 y 18) pero no fue posible restaurar la comunicación por red, el aliado indica que solicitaron a fábrica una tarjeta de red nueva y certificada para instalarla y verificar su funcionamiento, se solicitará un nuevo RFC para la ejecución de la ventana.

- **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 99 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 100 Inventario de impresoras para el servicio

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

- Para el mes de enero, el responsable del servicio gestionó un total de 485 solicitudes escaladas a través de Aranda. Al corte del mes, 477 casos quedaron en estado Cerrado/Solucionado, 8 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 74% 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-176475; 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.
- Se llevó a cabo la actualización de la interfaz de usuario en las impresoras Ricoh IM430F de las Direcciones Territoriales e Inspecciones a nivel nacional completando un total de 222 impresoras actualizadas, esta actividad continúa en curso para el siguiente período.
- **Mantenimientos Preventivos:** Se realiza la atención de mantenimientos preventivos de las impresoras Ricoh a nivel nacional. A corte del período se han atendido 30 Direcciones territoriales, 99 inspecciones de territorio y todo nivel central dando un total de 227 impresoras, actividad se continuará en el siguiente periodo.

En la siguiente tabla se muestra el TOP 10 de usuarios que más generaron impresiones Blanco / Negro a nivel nacional durante el período:

Nombre de la impresora	Ubicación	Nombre de Usuario	Nombre Completo	Blanco y negro
ricohpiso19a	Bogotá Sede Central	pnustes	Patricia Celestial Nustes Barrera	3.682
ricoh-bmanga-ofc205	Bucaramanga	spadilla	Sebastian Padilla Mora	3.346
ricohpiso10b	Bogotá Sede Central	asanchez	Alfonso Sanchez Carrillo	2.586
ricoh-bmanga-ofc205	Bucaramanga	dgalvan	David Ricardo Galvan Mancera	2.365
ricohpiso23b	Bogotá Sede Central	ldleal	Luz Dary Leal Cotamo	2.327
ricoh-medellin-piso1	Medellin	bcarvajal	Blanca Isabel Carvajal Perez	2.010
ricoh-bmanga-ofc205	Bucaramanga	ybeltran	Yerson Daniel Beltran Martinez	2.003
ricoh-cali-piso2-atc	Cali	gcolonia	Gustavo Adolfo Colonia Trochez	1.968
ricoh-cali-piso3	Cali	marboleda	Maria Del Carmen Arboleda Marquez	1.798
ricoh-guadalaraja-buga-insp	Guadalajara Buga	vfierro	Viviana Fierro Herrera	1.719

Tabla 101 Consumo de impresiones 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
ricoh-cali-piso3	Cali	10.126
ricoh-cali-piso4	Cali	10.084

ricoh-bmanga-ofc205	Bucaramanga	9.261
ricohpiso5a	Bogotá Sede Central	8.950
ricohpiso10b	Bogotá Sede Central	7.706
ricohpiso19a	Bogotá Sede Central	7.282
ricoh-cali-piso2-atc	Cali	7.099
ricohpiso12a	Bogotá Sede Central	7.045
ricoh-medellin-piso1	Medellin	6.744
ricoh-medellin-piso3	Medellin	6.594

Tabla 102 Top 10 de impresoras con mayor uso

Top Impresoras1.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	mserrano	Malliber Serrano Nieto	144
ricohpiso25c	Bogotá Sede Central	ymedinag	Yeisson Medina Gonzalez	130
ricohpiso25c	Bogotá Sede Central	bhernandez	Bibiana Hernandez Hernandez	9

Tabla 103 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	283	79.455	55.542	24.196	79.738	22.746	225,1
D.T. Valle del Cauca	0	38.456	26.622	11.834	38.456	11.638	112,7
D.T. Santander	0	30.121	23.030	7.091	30.121	7.499	118,5
D.T. Antioquia	0	21.521	15.408	6.113	21.521	6.425	70,5
OE	0	11.925	7.890	4.035	11.925	3.666	46,5
D.T. Tolima	0	11.559	7.328	4.231	11.559	3.556	58,3
D.T. Bogotá	0	11.455	6.878	4.577	11.455	3.354	31,4
D.T. Atlántico	0	11.345	6.256	5.089	11.345	3.500	55,6
D.T. Cundinamarca	0	11.296	6.360	4.936	11.296	2.984	110,6
D.T. Norte de Santander	0	10.116	6.996	3.120	10.116	2.948	73,1

Tabla 104 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	1405
RICOH-BMANGA-OFC205	D.T. Santander	COPY	1235
RICOH-TUNJA-PISO1	D.T. Boyaca	COPY	1136
RICOH-QUINDIO-PISO1-PPAL	D.T. Quindio	COPY	1034
RICOHPISO12A	Nivel Central	COPY	905
RICOHGAU-A	D.T. Bogotá	COPY	897
RICOH-BMANGA-OFC305	D.T. Santander	COPY	888
RICOH-CUCUTA-P2	D.T. Norte de Santander	COPY	813
RICOH-BAQ-DIR	D.T. Atlantico	COPY	741
RICOH-MEDELLIN-PISO1	D.T. Antioquia	COPY	726

Tabla 105 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
marboleda	Maria Del Carmen Arboleda Marquez	ADJUST	2455	7
ysevillana	Yuli Alexandra Sevillano Echeverri	ADJUST	3499	7
gecheverria	Gisela Yulieth Echeverria Quinto	ADJUST	1800	6
npreciado	Nora Elena Preciado Rivera	ADJUST	1900	6
oreyes	Oscar Javier Reyes Chaparro	ADJUST	2258	6
aurrea	Anderson Urrea Bautista	ADJUST	1699	5
jdiaz	Juan Manuel Diaz Rojas	ADJUST	1680	5
kvalencia	Katy Lorena Valencia Panesso	ADJUST	1500	5
pnustes	Patricia Celestial Nustes Barrera	ADJUST	7107	5
agalvist	Amalfi Galvis Torres	ADJUST	2700	4

Tabla 106 Ampliación de cuota de impresión

Asignación de saldo.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:

	nov-25		dic-25		ene-26	
	Resmas Carta	Resmas Oficio	Resmas Carta	Resmas Oficio	Resmas Carta	Resmas Oficio
Total, Resmas	432	255	536	282	93	43
Total, Cajas por Tamaño	43,2	25,5	53,6	28,2	9,3	4,3
Total, Cajas Enviadas	**68,7**		**81,8**		**13,6**	

Tabla 107 Despacho de papel a sedes del Ministerio del Trabajo

Durante el período, se despacharon a sedes del ministerio un total de 13 toners para impresora B/N IM430 y 1 unidad fusora.

4.6.1 No aplica

4.6.2 Multifuncional B/N rango medio – Cargo fijo mensual

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

Tabla 108 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 109 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 enero de 2026:

MES	DETALLE	CANTIDAD
Enero	Multifuncional blanco y negro rango medio - Clic de impresión tóner y papel carta	**365.719**
	TOTAL	**365.719**

Tabla 110 Clics de impresión de enero 2026 – Multifuncional B/N

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

Mes 2025 - 2026	Noviembre	Diciembre	Enero

Cantidad de clics consumidos	502.396	486.972	365.719

Tabla 111 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 **339.932** clics de impresión (esto incluye **4.154** de la impresora de contratos piso 8) y **25.787** de fotocopias para un total de **365.719** para este servicio.

El administrador del servicio de outsourcing de impresión remitió semanalmente vía correo electrónico al Coordinador del Grupo de Soporte Informático y demás interesados el consolidado de consumo de clics durante el período, lo anterior con el propósito de notificar el momento que se supera el umbral definido de consumo establecido para el 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 enero de 2026:

MES	DETALLE	CANTIDAD
Enero	Impresora color rango medio - Cargo fijo mensual - Clic de impresión tóner y papel carta	283
Total		283

Tabla 112 Clics de Impresión – Impresora Color

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

Mes	Noviembre 2025	Diciembre 2025	Enero 2026
Cantidad de clics consumidos	1.677	1.398	283

Tabla 113 Tendencia 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 **283** 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 114 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 enero 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.

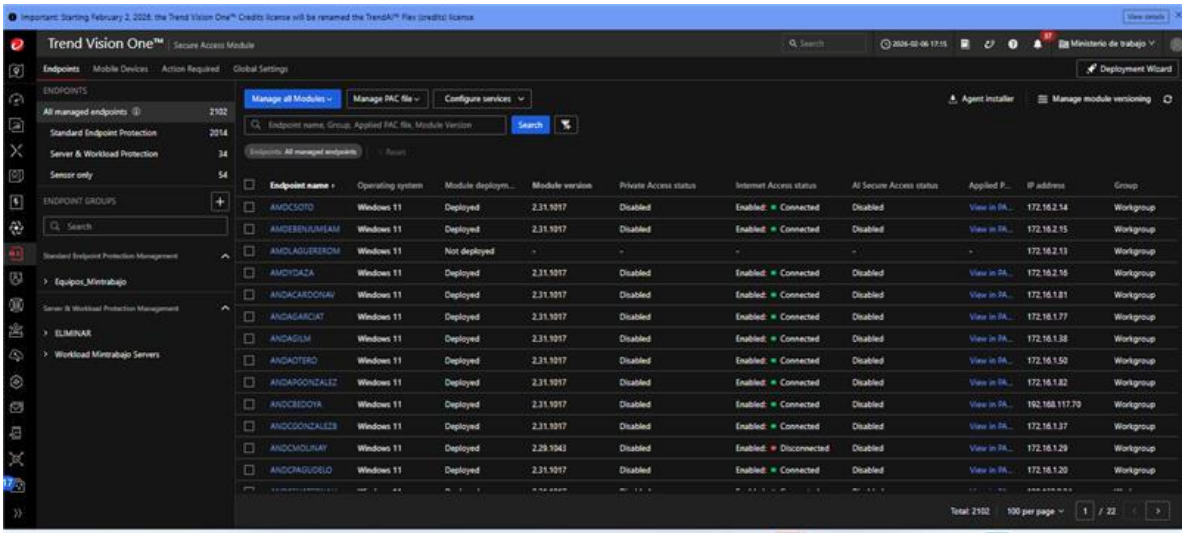


Ilustración 148 Equipos consola antivirus

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 (2102) de Mintrabajo, se cuenta con 2255 licencias, se tienen disponibles 153.

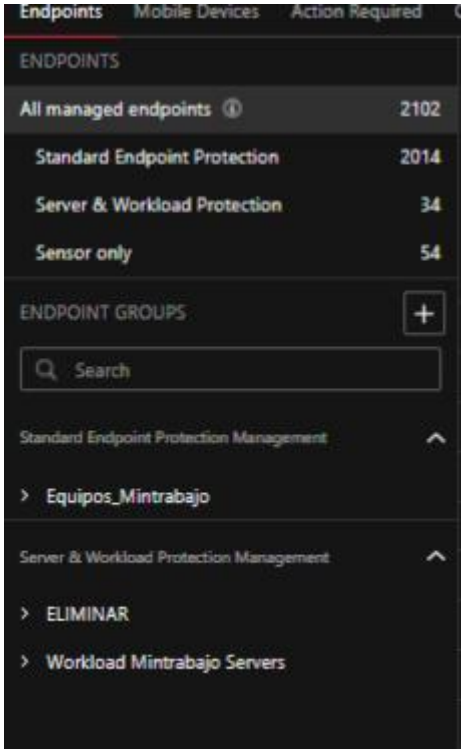


Ilustración 149 Gestión consola antivirus – equipos usuario final

4.7.3 Top 10 Virus Detectados

Durante el mes analizado, los eventos detectados por la plataforma TrendMicro se detectaron un total de 40 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:

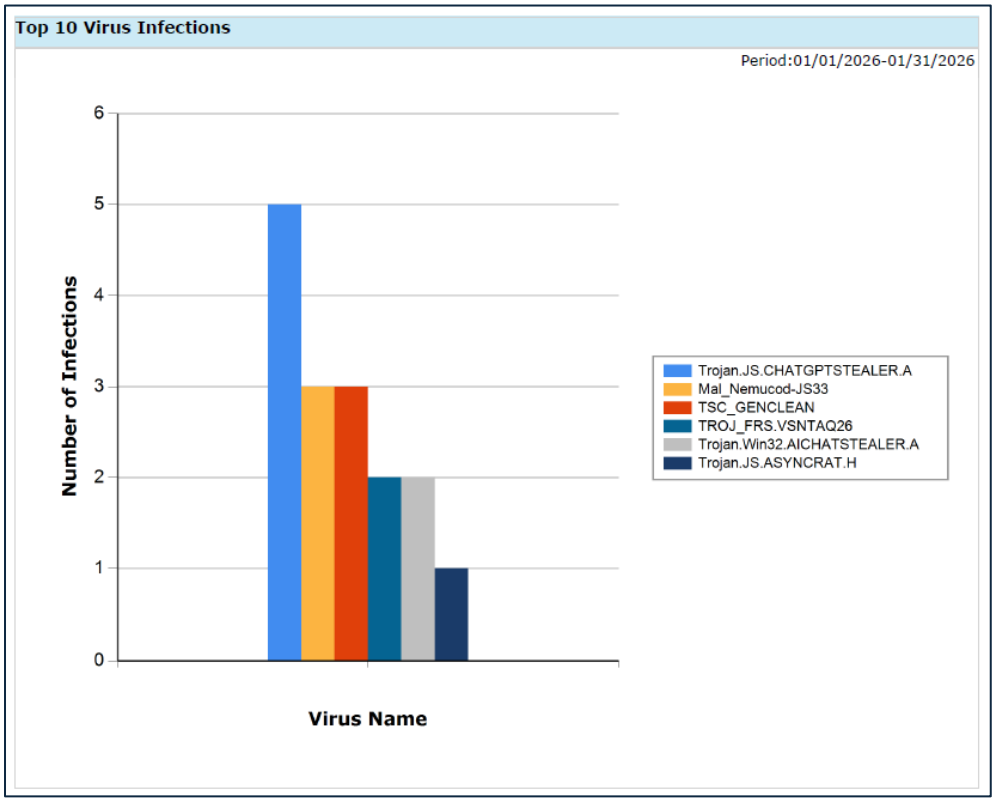


Ilustración 150 Top 10 virus detectado

Top 10 Virus Infections

Virus Name	# of Infections	Detected By
Trojan.JS.CHATGPTSTEALER.A	5	Desktop (5)
Mal_Nemucod-JS33	3	Desktop (3)
TSC_GENCLEAN	3	Desktop (3)
TROJ_FRS.VSNTAQ26	2	Desktop (2)
Trojan.Win32.AICHATSTEALER.A	2	Desktop (2)
Trojan.JS.ASYNCRAT.H	1	Desktop (1)

Ilustración 151 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.

Malware distribuido por navegación web y scripts

- **Detección:Trojan.JS.CHATGPTSTEALER**

- **Descripción. A:** Se identificó una amenaza de tipo troyano basada en JavaScript, generada con el objetivo de sustraer datos y sesiones asociadas a servicios de inteligencia artificial, tales como ChatGPT u otros utilizados a través del navegador web.

  Durante el período analizado se registraron cinco (5) eventos en el host BOLDFGARCIA, los cuales fueron controlados en su totalidad. Como acción de mitigación, se procedió a la eliminación del archivo malicioso, evitando impactos adicionales en el sistema

- **Mal_Nemucod-JS33:** Corresponde a una variante de Nemucod, un malware distribuido normalmente mediante archivos JavaScript maliciosos que descargan amenazas secundarias (como ransomware o troyanos bancarios) al ejecutarse. Su detección indica actividad sospechosa asociada a scripts que intentan conectarse a servidores externos no autorizados. Debido a su comportamiento, la herramienta tomo acciones sobre la amenaza y elimino los archivos asociados

  - BOPJVIANAD
  - GUDACAICEDO
  - BODSDIAZR

  Los elementos asociados están vinculados a un posible acceso a páginas con contenido publicitario, lo que ocasionó la carga de contenido malicioso en el caché del navegador. La solución de seguridad Trend Micro detectó y eliminó dicho contenido, protegiendo los equipos afectados. No se requieren acciones adicionales.

- **TSC_GENCLEAN:** Estas detecciones se encuentran asociadas a la tecnología de Trend Micro, la cual garantiza una limpieza coordinada y automatizada del sistema. Cuando el producto de Trend Micro identifica la presencia de malware en un equipo, se envía de manera inmediata un comando al Motor de Limpieza de Daños (Damage Cleanup Engine – DCE), encargado de ejecutar las acciones necesarias para la remediación y limpieza del sistema afectado, los archivos reportados fueron controlados en su totalidad. los eventos se reportaron en los Host que se relacionan a continuación.
  - ANDJYPEREZ
  - URPEASPRILLA
  - BOPCBUSTAMANTE

- **Trojan.Win32.AICHATSTEALER.A:** Esta amenaza corresponde a l tipo “stealer” (ladrón de información) que abusa de la popularidad de herramientas de IA (como ChatGPT y otras) para robar datos del usuario, principalmente desde el navegador. Los eventos detectados fueron controlados por la solución y se presentaron en los equipos que se relaciona a continuación.

  - ANDJYPEREZ

- **Trojan.JS.ASYNCRAT.H:** Este tipo de malware está orientado al uso del lenguaje de programación JavaScript con el objetivo de permitir a un atacante el control del equipo comprometido, el robo de información sensible y la ejecución remota de comandos. Debido a sus capacidades, representa un riesgo alto para la seguridad de los sistemas y la información. Este evento fue controlado por la solución y la acción tomada por el antivirus fue la de eliminación del archivo y se presentó en el equipo.

TOP 5 EQUIPOS

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

Product Entity/Endpoint	Cantidad	Virus/Malware
BOLDFGARCIA	5	Trojan.JS.CHATGPTSTEALER. A
URPEASPRILLA	3	TSC_GENCLEAN
ANDJYPEREZ	2	Trojan.Win32.AICHATSTEALER.A
BOPCBUSTAMANTE	2	TROJ_FRS.VSNTAQ26
BODSDIAZR	1	Mal_Nemucod-JS33

Tabla 115 Top 5 Equipos

BOLDFGARCIA

Las 5 detecciones en el equipo se deben por Trojan.JS.CHATGPTSTEALER.A identifica un tipo de archivos maliciosos los cuales son eliminados por la solución

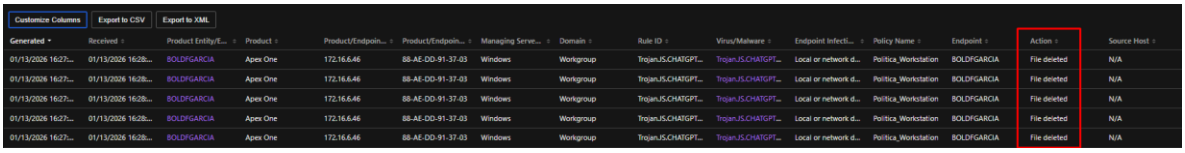


Ilustración 152 DFGARCIA

URPEASPRILLA

El día 30 de enero se reportaron 3 detecciones en el host URPEASPRILLA un archivo malicioso identificado como TSC_GENCLEAN, una variante distribuida mediante scripts JavaScript que intentan descargar malware adicional desde internet. La amenaza fue detectada en la carpeta de temporales en la ruta C:\Users\easprilla\AppData\Local\Temp\b23a9998-8df4-457c-9224-c86f67848fb1_EXPEDIENTE LEGAL INFORMADO_N°4890208424.zip.fb1\EXPEDIENTE LEGAL INFORMADO_N°4890208424.js y fue eliminado automáticamente por Trend Micro y se encontraba directamente asociada a otra detección realizada en el host reconocida como Downloader.JS.TRX.XXJSE9EFF079 TSC_GENCLEAN es reconocida como una detección genérica de Trend Micro que indica

que su motor de seguridad limpió o neutralizó automáticamente una amenaza, aunque no la clasifique con el nombre exacto de un malware específico.

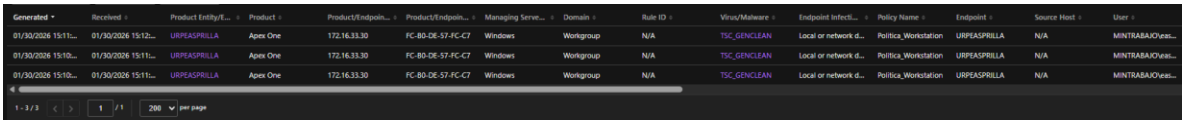


Ilustración 153 URPEASPRILLA

ANDJYPEREZ

El día 30 de enero se detectaron en el host ANDJYPEREZ dos archivos maliciosos fueron reconocidos bajo el nombre Trojan.Win32.AICHATSTEALER.A , amenaza de tipo troyano basada en JavaScript, generada con el objetivo de sustraer datos y sesiones asociadas a servicios de inteligencia artificial, estos archivos fueron controlados por la solución de manera oportuna y no fue necesario ejecutar acciones adicionales sobre el equipo.

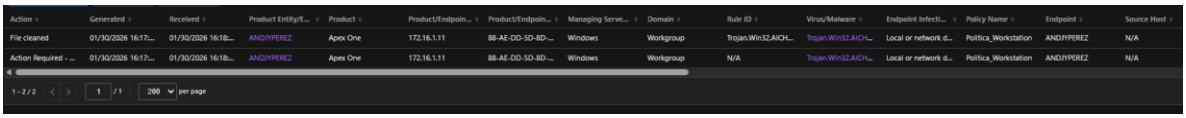


Ilustración 154 ANDJYPEREZ

BOPCBUSTAMANTE

El día 27 de enero se registraron en el host BOPCBUSTAMANTE en la ruta C:\Users\jojpatino\Downloads\ 2 detecciones de la amenaza TROJ_FRS.VSNTAQ26 los archivos infectados fueron identificados durante la ejecución del escaneo programado y reportados como Cleaned. No se hizo necesario ejecutar acciones adicionales en el equipo

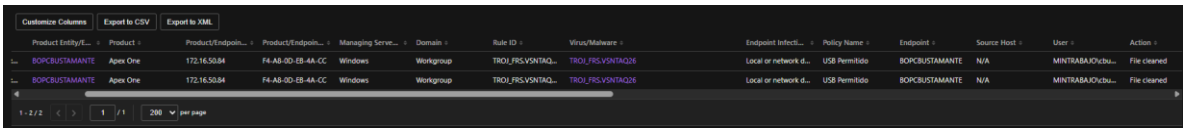


Ilustración 155 BOPCBUSTAMANTE

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.

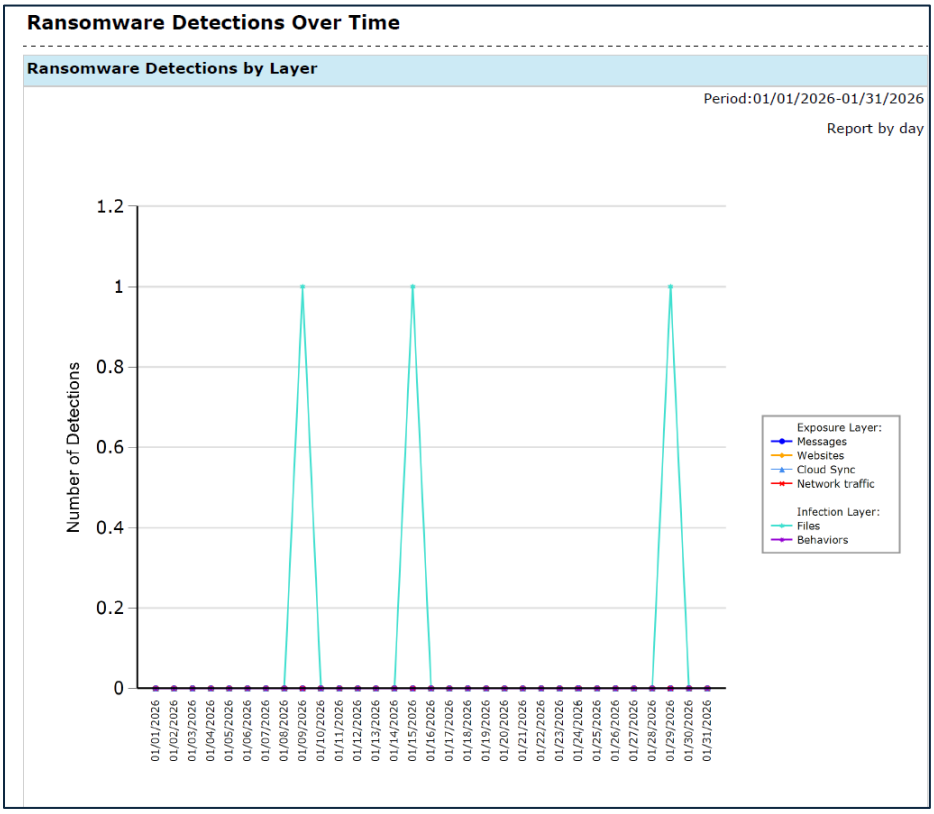


Ilustración 156 Eventos Ransomware

En el mes de enero 2026, se presentaron eventos 3 eventos escalados por detección de malware Ransomware, estas detenciones se realizaron en los hosts: GUDACAICEDO, BOPJVIANAD y 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.

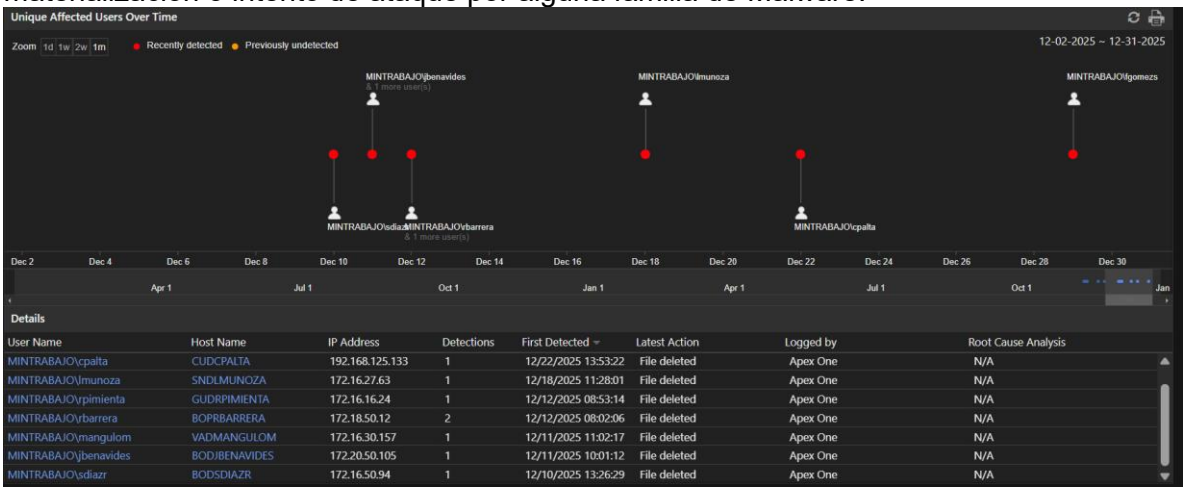


Ilustración 157 captura eventos ransonware

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

Name	Type	Channel	Units	Credit conversion	Start date	Expiration date
Trend Vision One Endpoint Security - Essentials	Paid	Trend Micro	2292	148980	2024-02-29	2026-07-31
Trend Micro Web Security Standard	Paid	Trend Micro	2172	N/A	2024-02-29	2026-07-31

Ilustración 2158. 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 enero 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 enero del 2026 se tienen registrados 322 activos TI, de los cuales, se registró un alcance sobre 312 (97%) activos.

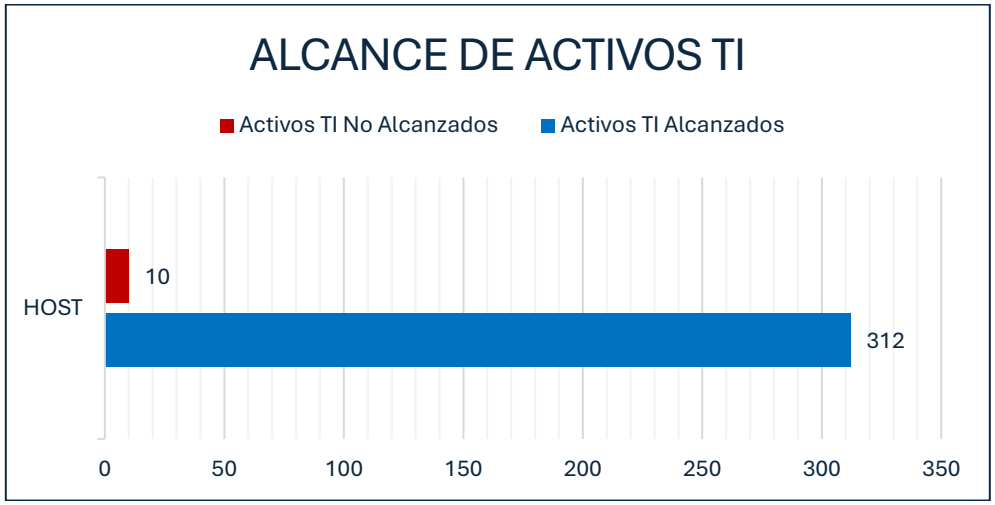


Ilustración 159 *Gestión consola Nessus*

4.7.4.2 Escaneos programados

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

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

Name	Scan Type	Schedule	Last Scanned
2026 SEMANAL I - NO AUTH	Vulnerability	Weekly on Sat at 1:00 AM	January 31 at 1:17 AM
2026 SEMANAL I - NETWORKING	Vulnerability	Weekly on Sat at 2:00 AM	January 31 at 4:06 AM
2026 SEMANAL I - WINDOWS	Vulnerability	Weekly on Sat at 8:00 PM	February 1 at 3:33 AM
2026 SEMANAL I - FORTISIEM	Vulnerability	Weekly on Sun at 6:00 PM	February 1 at 6:55 PM
2026 SEMANAL I - LINUX	Vulnerability	Weekly on Sun at 8:00 PM	February 1 at 9:36 PM

Ilustración 160 *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 enero del 2026, el activo TI con la mayor cantidad de vulnerabilidades identificadas corresponde al host (172.20.22.188), con un total de 1.727 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.

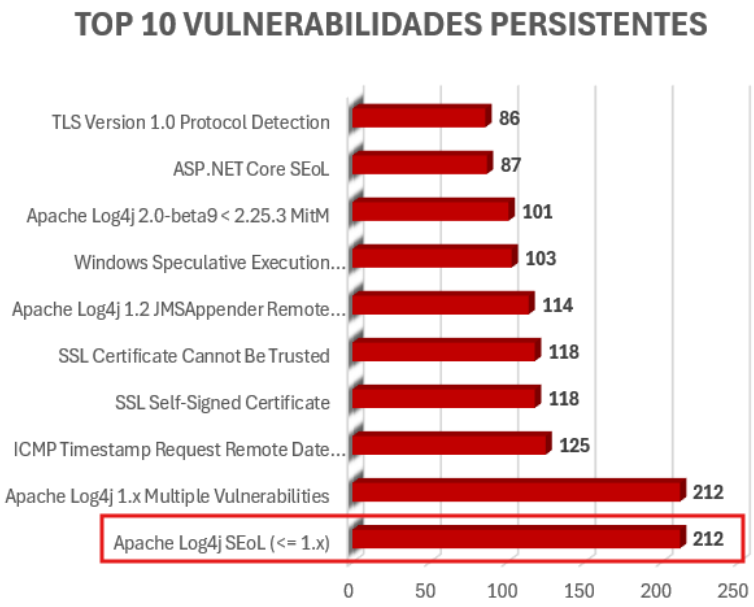


Ilustración 161 TOP 10 - Activos más explotables

Al cierre de enero del 2026, la vulnerabilidad identificada con la mayor cantidad de persistencias corresponde a (**Apache Log4j SEoL (<= 1.x)**), con un total de **212 hallazgos**, consiste en el uso de la librería Apache Log4j en versiones que actualmente son consideradas obsoletas y con una amplia cantidad de vulnerabilidades, la cual se utiliza para el registro de eventos del servicio de Apache

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 enero del 2026, se remediaron un total de 190 vulnerabilidades, de las cuales, 27 fueron de severidad crítica, 117 de severidad alta, 37 de severidad media y 9 de severidad baja. Por otro lado, con relación a indicadores semestrales, se gestionaron un total de 190 vulnerabilidades, de las cuales, 27 fueron de severidad crítica, 117 de severidad alta, 37 de severidad media y 9 de severidad baja.

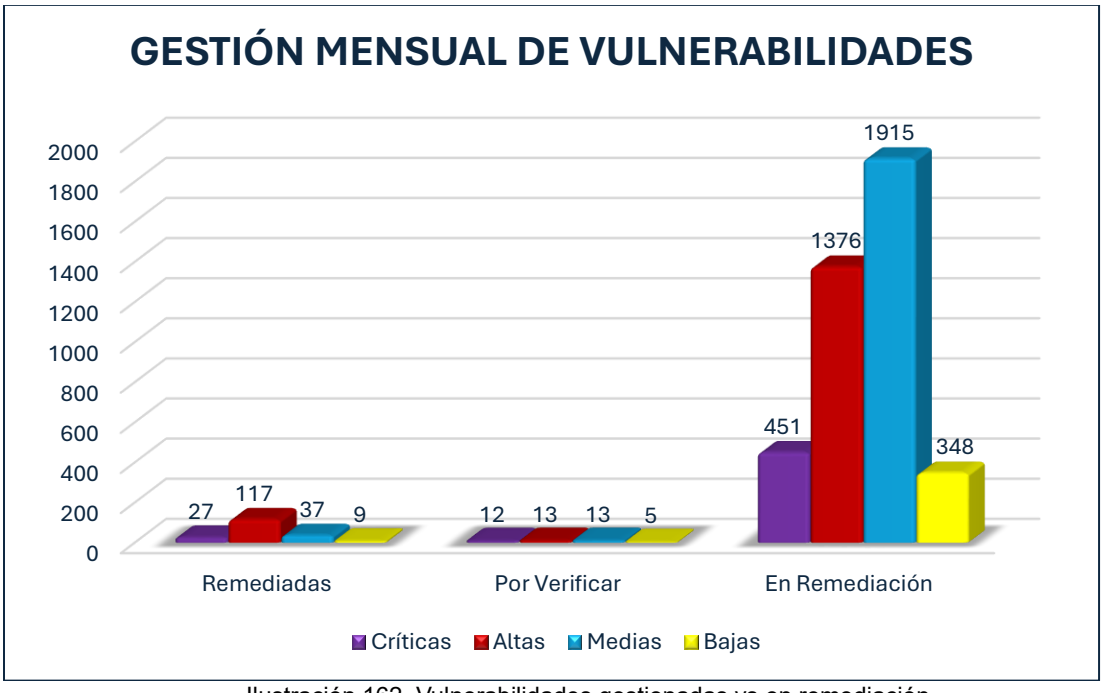


Ilustración 162 Vulnerabilidades gestionadas vs en remediación

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

Dando cumplimiento al reporte semestral de vulnerabilidades, se realizó envió a la Coordinador del Grupo de Soporte Informático, el informe de vulnerabilidades correspondiente al segundo semestre del 2025, se adjunta informe socializado.

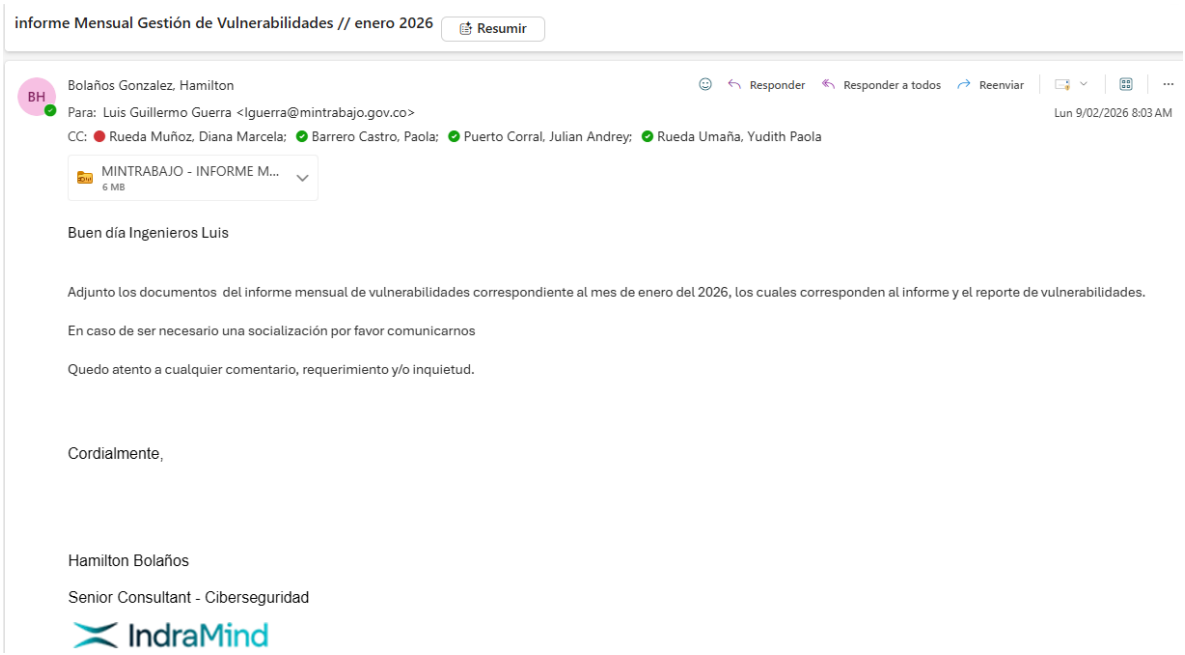


Ilustración 163 captura envío de correo gestión de vulnerabilidades

- Medición de ANS Antivirus

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

ID	Indicadores	Resultado	Meta
AV-1	Cobertura de antivirus	99,28%	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 116 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 enero 2026, se realizó la evaluación cuantitativa de la muestra de 263 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:

Items Evaluados	ENC Cometidos	Cumplimiento %
1. Tipo de caso	0	100,0%
2. Asunto	5	99,6%
3. Descripción	1	99,9%
4. Prioridad	0	100,0%
5. Categoría	0	100,0%
6. Escalamiento	0	100,0%
7. Solución	5	99,6%
8. Estado del Caso	0	100,0%
9. Justificación Estado del Caso	0	100,0%
10. Periodicidad de seguimientos	1	99,9%
11. Elemento CI	0	100,0%
12. Ortografía y redacción	16	98,8%
13. Cumplimiento de ANS	2	99,8%

Tabla 117 Errores cometidos

Se identificaron 30 errores con un porcentaje de cumplimiento consolidado de 97,72%.
De la muestra evaluada, se tiene el siguiente el top 3 de los ítems con más errores identificados:

En la evaluación del periodo, se presentaron 16 novedades de ortografía y redacción, 5 de solución y 2 cumplimiento de ANS.

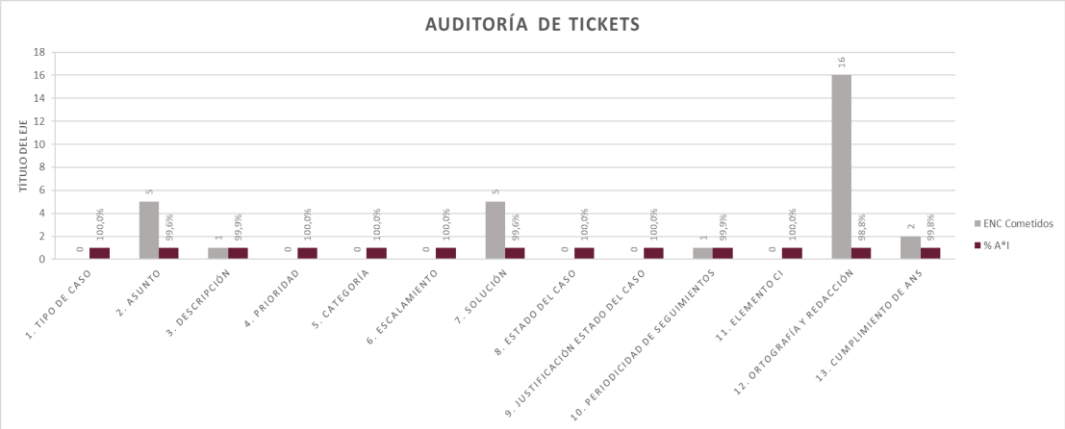


Ilustración 164 Resultados auditoria de casos

5.2 Evaluación de calidad de llamadas

En el mes de enero 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 evalúan por cada caso, los criterios definidos, obteniendo el siguiente resultado:

	PENC		
#	Practica medida	Q errores	Frec
1	Personalización de la llamada	0	100%
2	Entrega de la información necesaria y completa al usuario	0	100%
3	Agradecimiento del tiempo en línea	0	100%
4	Empatía y adaptabilidad al usuario	0	100%
5	Realización de Pre-diagnóstico o lista de chequeo correspondiente al reporte	0	100%
6	Protocolo de despedida	0	100%

	PEC		
#	Practica medida	Q errores	Frec
1	Protocolo de bienvenida y presentacion	0	100%
2	Identificación/captura de datos del usuario	0	100%
3	Comunicación del mensaje de espera	0	100%
4	Comunicación ID solicitud	0	100%
5	Confirmación de satisfacción/encuesta	0	100%

Tabla 118 Resultado de criterios y parámetros - Calidad de llamadas

5.3 Práctica de Mejora

Dar a conocer las actividades de la Práctica de Mejora Continua correspondientes al periodo del 1 al 31 de enero de 2026. Este apartado contiene información relevante sobre las acciones de mejora identificadas por los Servicios TIC durante el mes de enero de 2026.

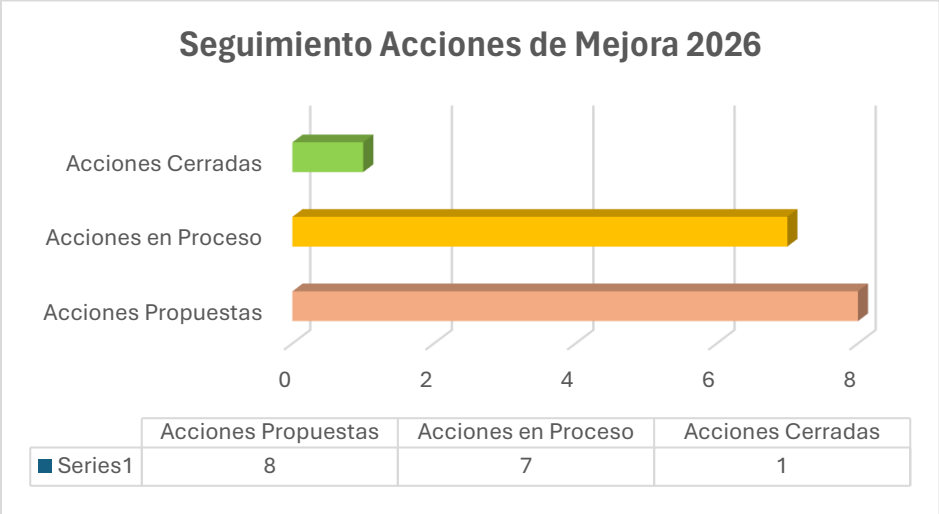


Ilustración 165 Seguimiento Práctica Mejora

En el anterior gráfico, se evidencia de las (8) acciones de mejora identificadas, (7) acciones se encuentran en proceso y (1) cerrada, lo cual se cuenta con un cumplimiento de ejecución en enero del 12,50% de los diferentes servicios TIC y Gestiones ITIL al corte del 31 de enero de 2026.

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	>= 70%	Trimestral
	AMI: Cantidad de Acciones ejecutadas en el periodo.		
	TAM: Total de Acciones planificadas para el período.		

Tabla 119 KPI Practica de Mejora

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

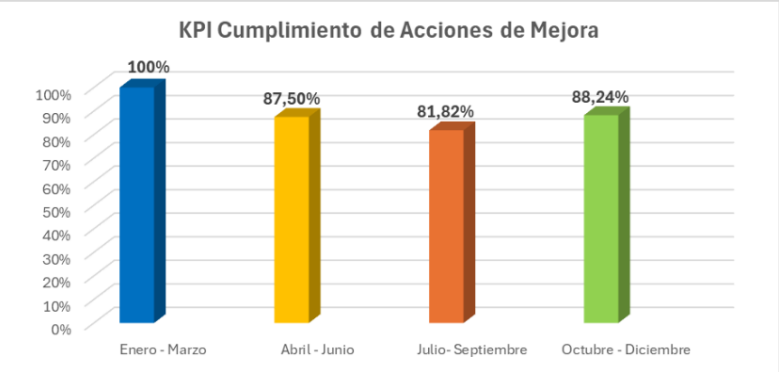


Ilustración 166 Resultado de Cumplimiento AM

Durante este mes, se realiza seguimiento de las (34) acciones de mejora, las cuales solo se encuentran pendientes (2) 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 1 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
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	Falla en el acceso y/o sincronización del correo soportemt@mintrabajo.gov.c o	NO	El correo electrónico institucional ha estado disponible

SERVICIO/ PRÁCTICA	NOMBRE	DESCRIPCIÓN	¿MATERIALIZADO?	ACCIONES PARA REALIZAR
	soportemt@mintrabajo.gov.co.			
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.
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.

SERVICIO/ PRÁCTICA	NOMBRE	DESCRIPCIÓN	¿MATERIALIZADO?	ACCIONES PARA REALIZAR
				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, administrar y operar los servicios.	NO	El personal asignado estuvo disponible durante el periodo.

SERVICIO/ PRÁCTICA	NOMBRE	DESCRIPCIÓN	¿MATERIALIZADO?	ACCIONES PARA REALIZAR
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 120 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	$1.855.427
	Subtotal	$1.855.427

Tabla 121 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	99,21%	90,00%
	Tiempo de solución de requerimientos por soporte en sitio	99,70%	90,00%
	Tiempo de respuesta de la mesa de servicio	99,72%	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	90,00%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
ANTIVIRUS	Cobertura de antivirus	99,28%	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	100,00%	90,00%
	Continuidad y disponibilidad de los servicios de directorio activo	100,00%	99,60%
	Continuidad y disponibilidad de los servicios de seguridad informática	100,00%	99,90%
	Tiempo de solución de incidentes asociado a los servicios de administración, soporte y monitoreo	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	100,00%	100,00%
Nube pública	Continuidad y disponibilidad de la nube pública	100,00%	99,90%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Outsourcing de impresión	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Telefonía IP	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Continuidad y disponibilidad de los servicios de telefonía IP	99,96%	99,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Conectividad WAN e Internet	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Continuidad y disponibilidad del servicio de WAN en sedes nacionales con un solo enlace	(*)	99,60%
	Continuidad y disponibilidad del servicio de WAN en sedes nacionales con doble enlace (principal MPLS + secundario Internet dedicado)	(*)	99,90%
	Continuidad y disponibilidad del servicio de internet en Datacenter principal	100,00%	99,95%
	Continuidad y disponibilidad del servicio de internet en Datacenter alterno	100,00%	99,70%
	Continuidad y disponibilidad del servicio de WAN en Datacenter principal	100,00%	99,95%
	Continuidad y disponibilidad del servicio de WAN en Datacenter alterno	100,00%	99,95%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 122 Medición de Acuerdos de Niveles de Servicio enero 2026

(*) 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 enero
- Detalle_llamadas_recibidas_(01.01.2026-31.01.2026)
- Datos_Mintrabajo_enero

FIN DEL DOCUMENTO