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

Diciembre de 2025

DOCUMENTO/ ARCHIVO	
Código:	**Informe Gestión - Unión Temporal Gestión TIC 2023**
Nombre Archivo:	**Informe Gestión - Unión Temporal Gestión TIC 2023 – diciembre 2025**
Fecha:	9/01/2026
Versión:	1

REGISTRO DE CAMBIOS			
Versión	**Páginas**	**Fecha Modificación**	**Motivo del cambio**
1	225	9/01/2026	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 12
Objetivo 12
Alcance 12
Definición de Siglas y Expresiones Técnicas 13
1 GERENCIA Y/O ADMINISTRACIÓN 14
2 LÍNEA DE GESTIÓN DE SERVICIOS 14
2.1. Gestión del Servicio 14
2.1.2. Prácticas ITIL 4 21
2.1.2.1. Práctica Acuerdos Niveles de Servicio (ANS) 21
2.1.2.2. Práctica Habilitación de Cambios 22
2.1.2.3. Práctica Gestión de Activos 24
2.1.2.4. Práctica Catálogo de servicios 25
2.1.2.5. Práctica de Problemas 26
2.1.2.6. Práctica de Incidentes 27
2.1.2.7. Práctica de Requerimientos 33
2.1.2.8. Práctica de Eventos 36
2.1.2.9. Práctica de Disponibilidad 50
2.1.2.10. Práctica de Implementación 53
2.2 Mesa de Servicios y Soporte en Sitio 54
3 LINEA DE SERVICIOS CENTRALES 74
3.1 Datacenter Principal 74
3.1.1 Datacenter Alterno y DRP 89
3.1.2 Procesamiento, Almacenamiento y Respaldo 94
3.1.3 Aplicaciones Especializadas 99
3.1.4 No aplica 147
3.1.5 Seguridad Informática 148
3.1.5.1 Firewalls de nueva generación 148
3.1.5.2 Sandbox – Amenazas día 0 154
3.1.5.3 SIEM - Solución de correlación de eventos de seguridad, disponibilidad y recursos 157
3.1.5.4 WAF - Servicio de tipo “Firewall de Aplicaciones Web” 163
3.1.5.5 Solución de Anti-DDoS 164
3.1.5.6 Casos atendidos de los servicios de seguridad 165
3.1.5.7 Análisis de riesgo 167
3.1.5.8 Políticas y procedimiento de seguridad 168
3.1.6 Licenciamiento 169
3.1.7 Administración, soporte y monitoreo 169
3.2 No aplica 171
3.3 Conectividad WAN, SDWAN e Internet 171
3.3.1 Canales WAN 171
3.3.1.1 Incidentes de Conectividad 172
3.3.1.2 Topología Actual 173
3.3.2 Canales SDWAN e Internet Dedicado 173
4 LINEA DE SERVICIOS EN SEDE 178
4.1 Equipos de Cómputo de usuario final 178
4.1.1 Equipos de Escritorio 182
4.1.2 Equipos Portátiles 182
4.2 Conectividad LAN y WLAN 182
4.2.1 Switch CORE Sede Principal 183
4.2.2 Switch para conexiones perimetrales (EDGE) en sede principal 183

4.2.3 Switch de acceso 24 puertos 183
4.2.4 Switch de acceso 48 puertos 184
4.2.5 Puntos de Acceso 185
4.3 Telefonía IP 186
4.3.1 Teléfono Gama Media 186
4.3.2 Teléfono Gama Baja 187
4.3.3 Troncales SIP 187
4.3.4 No Aplica 187
4.3.5 No Aplica 187
4.3.6 Módems 4G – Con plan de 50 Gbps 188
4.4 Energía Regulada UPS 193
4.4.1 UPS 10 kVA 194
4.4.2 UPS 15 kVA 194
4.4.3 UPS 20 kVA 194
4.5 No aplica 196
4.6 Outsourcing de Impresión 196
4.6.1 No aplica 201
4.6.2 Multifuncional B/N rango medio – Cargo fijo mensual 201
4.6.3 Impresora Color rango medio – Cargo fijo mensual 201
4.6.4 No aplica 201
4.6.5 Multifuncional B/N rango medio – Clic de impresión 201
4.6.6 Impresora Color rango medio – Clic de impresión 202
4.7 Antivirus 202
4.7.1 Instalaciones de antivirus en servidores 202
4.7.2 Instalación de antivirus PCs usuarios final 203
4.7.3 Top 10 Virus Detectados 204
4.7.4 Servicio de Vulnerabilidades 210
4.7.4.1 Inventario y licenciamiento 210
4.7.4.2 Escaneos programados 211
4.7.4.3 TOP 10 – Vulnerabilidades más explotables 212
4.7.4.4 Estrategia de remediación y/o mitigación 212
4.7.4.5 Resumen de mitigación efectuada 213
4.7.4.6 Prueba de Vulnerabilidades Semestre II 2025 214
5 GESTIÓN DE CALIDAD DE INFORMACIÓN 215
5.1 Evaluación calidad documental de casos 215
5.2 Evaluación de calidad de llamadas 216
5.3 Práctica de Mejora 217
6 GESTION DE RIESGOS 218
7 BOLSA DE RECURSOS 221
8 MEDICIÓN DE ACUERDOS DE NIVEL DE SERVICIO 221
9 ANEXOS 223

Índice de Tablas

Tabla 1 Atención de solicitudes por Grupo de Especialista 20
Tabla 2 Tipificación de los cambios 22
Tabla 3 Medición Indicador Porcentaje de Cambios Exitosos 23
Tabla 4 KPI Práctica Catálogo de Servicios 26
Tabla 5 Consolidado problemas identificados 27
Tabla 6 Estados Incidentes 28
Tabla 7 Top 10 Incidentes 29

Tabla 8 Incidentes Suspendidos....29
Tabla 9 Incidentes Mayores....31
Tabla 10 Medición de KPIs....31
Tabla 11 Estados de Requerimientos....33
Tabla 12 Seguimiento del Backlog Suspendidos....33
Tabla 13 Top 10 de Solicitudes....34
Tabla 14 Detalle de KIP Practica de Requerimientos....34
Tabla 15 Casos reabiertos....36
Tabla 16 KPI Práctica de Eventos....37
Tabla 17 Consolidado disponibilidad de servidores....51
Tabla 18 Consolidado disponibilidad de Directorio Activo....51
Tabla 19 Desagregado de Disponibilidad Directorio Activo....51
Tabla 20 Consolidado disponibilidad de equipos Datacenter principal....51
Tabla 21 Desagregado de Disponibilidad Datacenter Principal....51
Tabla 22 Consolidado disponibilidad de equipos Datacenter alterno....51
Tabla 23 Desagregado Disponibilidad de equipos Datacenter alterno....52
Tabla 24 Consolidado disponibilidad de equipos redes y conectividad....52
Tabla 25 Consolidado disponibilidad de equipos de seguridad....52
Tabla 26 Disponibilidad de equipos Seguridad de la Información....52
Tabla 27 Consolidado disponibilidad de equipos de telefonía....52
Tabla 28 Consolidado disponibilidad de plataforma antivirus....53
Tabla 29 Llamadas Atendida por la Mesa de Servicio....55
Tabla 30 Casos anulados por Servicio....55
Tabla 31 Casos Suspendidos por Servicio....56
Tabla 38 Casos Atendidos usuarios VIPs....60
Tabla 39 Casos Atendidos usuarios....60
Tabla 40 Medios de Ingreso de Casos....61
Tabla 41 Visitas a Sedes sin Soporte....74
Tabla 42 Medición de ANS Mesa de servicios....74
Tabla 43 Capacidades contractuales....77
Tabla 44 Capacidades contractuales....77
Tabla 45 Consumo de capacidad con servidores para desaprovisionar + ambientes de pruebas)....77
Tabla 46 Consumo de capacidad Sin servidores para desaprovisionar con ambientes de pruebas 78
Tabla 47 Consumo de capacidad Sin servidores para desaprovisionar sin ambientes de pruebas .78
Tabla 48 Consumo de capacidad Servidores Pruebas y Desarrollo....78
Tabla 49 Consumo de capacidad actual....79
Tabla 50 Servidores de pruebas Gestor Documental....87
Tabla 51 Suma Instancias....121
Tabla 52 Total Docs....122
Tabla 53 Total Radicados....122
Tabla 54 Dimensionamiento Servers IBM - Virtualización Optima....123
Tabla 55 Apps & DDBB Oracle....125
Tabla 56 Escenario de Capacidades Oracle - Estado de consumo Actual....126
Tabla 57 Escenario de Capacidades Oracle - Total de recursos empleados....126
Tabla 58 Tendencia de uso de ancho de banda....149
Tabla 59 usuarios con mayor consumo de ancho de banda....150
Tabla 60 Top de usuarios por sesiones....151
Tabla 61 Top de aplicaciones....152
Tabla 62 Consolidado de indicadores....154
Tabla 63 Tipos de incidentes....161

Tabla 64 Reporte de requerimientos diciembre 167
Tabla 65 Vulnerabilidades en la infraestructura 167
Tabla 66 Vulnerabilidades en la infraestructura 167
Tabla 67 ataques de phishing 167
Tabla 68 Licenciamiento 169
Tabla 69 Medición ANS Datacenter 170
Tabla 70 Medición ANS Nube Pública 170
Tabla 71 Incidentes de conectividad 172
Tabla 72 Medición de ANS Conectividad WAN e Internet 177
Tabla 73 Desagregado sedes con novedad un solo enlace 177
Tabla 74 Desagregado sedes con novedad con doble enlace 178
Tabla 75 Cantidades de equipos Contractual – Instalados - Almacén 178
Tabla 76 Cantidades de equipos asignados nivel nacional 179
Tabla 77 Cantidades de equipos por devolución nivel nacional 179
Tabla 78 Estado de casos de garantía. 179
Tabla 79 ANS casos de garantía. 179
Tabla 80 ANS Relación casos de garantía 180
Tabla 81 Equipos en siniestro 181
Tabla 82 Solicitudes de Equipos Usuario Final – Según Grupo Responsable 181
Tabla 83 Solicitudes de Equipos Usuario Final – Según Grupo Responsable 181
Tabla 84 Medición ANS Equipos de Usuario Final 182
Tabla 85 Top 5 de categorías en el Servicio de conectividad LAN-WLAN 183
Tabla 86 Distribución y Cantidades de switch 24 puertos 184
Tabla 87 Distribución y Cantidades de Switch 48 puertos 185
Tabla 88 Distribución de puntos de acceso 186
Tabla 89 Medición ANS LAN y WLAN 186
Tabla 90 Equipos gama media 186
Tabla 91 Sedes cerradas 187
Tabla 92 Consolidado de teléfonos gama baja 187
Tabla 93 Consolidado equipos MIFI 188
Tabla 94 Minutos, consumos 189
Tabla 95 Top 5 consumo de llamadas 190
Tabla 96 Top 5 llamadas LDI 191
Tabla 97 Top 5 llamadas Celular 191
Tabla 98 Top 5 llamadas locales 192
Tabla 99 Medición ANS Telefonía IP 193
Tabla 100 Inventario de UPS – 10kVA 194
Tabla 101 Inventario de UPS – 20Kva 195
Tabla 102 Casos gestionados – Energía Eléctrica Regulada UPS 195
Tabla 103 Medición ANS Energía Eléctrica UPS 196
Tabla 104 Inventario de impresoras para el servicio 197
Tabla 105 Consumo de impresiones por usuario - Impresoras B/N 198
Tabla 106 Top 10 de impresoras con mayor uso 198
Tabla 107 Top usuarios impresión a color 199
Tabla 108 Top oficinas 199
Tabla 109 Top 10 impresoras más usadas del servicio de fotocopiado 200
Tabla 110 Ampliación de cuota de impresión 200
Tabla 111 Despacho de papel a sedes del Ministerio del Trabajo 200
Tabla 112 Cargo mensual multifuncional rango medio 201
Tabla 113 Cargo mensual impresora color 201

Tabla 114 Clics de impresión de diciembre 2025 – Multifuncional B/N 201
Tabla 115 Tendencia de consumo de clics B/N 201
Tabla 116 Clics de Impresión de diciembre 2025 – Impresora Color 202
Tabla 117 Tendencia de consumo de clics color 202
Tabla 118 Medición ANS Outsourcing de Impresión 202
Tabla 119 Descripción de virus 204
Tabla 120 *Top 5 Equipos* 207
Tabla 121 Medición de ANS Antivirus 215
Tabla 122 Errores cometidos 216
Tabla 123 Resultado de criterios y parámetros - Calidad de llamadas 217
Tabla 124 KPI Practica de Mejora 218
Tabla 125 Gestión de riesgos 221
Tabla 126 Bolsa de Recursos 221
Tabla 127 Medición de Acuerdos de Niveles de Servicio diciembre 2025 222

Índice de Ilustraciones

Ilustración 1 Estado final de casos al corte del período 20
Ilustración 2 Socialización matriz de escalamiento 26
Ilustración 3 Efectividad de resolución de incidentes 32
Ilustración 4 Porcentaje de incidentes abiertos 32
Ilustración 5 KPI Efectividad de Resolución de Requerimientos de Servicio 35
Ilustración 6 Requerimientos de Reabiertos en el periodo 35
Ilustración 7 Top de incidentes por sedes 38
Ilustración 8 Top de incidentes por sedes 39
Ilustración 9 eventos por sedes routers 40
Ilustración 10 Top de causas por sedes switches 41
Ilustración 11 Top de eventos por sedes Access Point 42
Ilustración 12 13Top de causas por sedes Access point 42
Ilustración 14 Top de eventos por sedes Starlink 43
Ilustración 15 Top de causas por sedes Starlink 44
Ilustración 16 Top de incidentes por sedes fortigate 45
Ilustración 17 Top de causas por sedes fortigate 46
Ilustración 18 Top de eventos Windows 47
Ilustración 19 Top de servidores Windows 47
Ilustración 20 Top de causas eventos linux 48
Ilustración 21 Top de servidores linux 49
Ilustración 22 Seguimiento Pruebas de Disponibilidad 53
Ilustración 23 Seguimiento Práctica Implementación 54
Ilustración 24 Llamadas Atendidas 55
Ilustración 25 Requerimientos Solucionados por Mesa de Servicios 57
Ilustración 26 Requerimientos Solucionados por Soporte en Sitio 57
Ilustración 27 Requerimientos Solucionados por Territoriales 58
Ilustración 28 Requerimientos Solucionados por la Mesa de Servicios 58
Ilustración 29 Casos Cerrados por Soporte en Sitio 59
Ilustración 30 Casos Cerrados por Territoriales 60
Ilustración 31 *Medio de ingreso solicitudes* 61
Ilustración 32 Cumplimiento WSUS 75
Ilustración 33 Casos Win Servicio 76
Ilustración 34 Estado final de los casos Windows 77
Ilustración 35 Azure Migrate 81
Ilustración 36 RG Pruebas y prod XROAD 84

Ilustración 37 Grupos de recursos XROAD Azure 85
Ilustración 38 Stios XROAD operativos 86
Ilustración 39 Comportamiento SWCORE Datacenter Colombia XV 87
Ilustración 40 Sincronización HA de los Switch Core 88
Ilustración 41 Grafica de consumo canal Internet Datacenter 88
Ilustración 42 Captura de imagen máquinas virtuales 89
Ilustración 43 Escenario de pruebas Aplicaciones y AD 91
Ilustración 44 Extremo DC Bogotá 91
Ilustración 45 Extremo DC Cali 92
Ilustración 46 Estado canal de Internet DC Cali 92
Ilustración 47 Estado SWCORE Datacenter alterno 93
Ilustración 48 Estado HA SWCORE Datacenter alterno 93
Ilustración 49 Consumo canal MPLS DC Alterno 94
Ilustración 50 Estado Router MPLS DC Alterno 94
Ilustración 51 Casos App Servicio 101
Ilustración 52 Casos App Categoría 101
Ilustración 53 Tamaño Archivo Sindical 102
Ilustración 54 Tamaño IIS 103
Ilustración 55 Arquitectura Apps nueva 106
Ilustración 56 Distribución de sitios 106
Ilustración 57 Casos IBM Servicio 113
Ilustración 58 Casos IBM - categoría 114
Ilustración 59 Diagrama BP 116
Ilustración 60 Diagrama ODM 116
Ilustración 61 Diagrama WASND 117
Ilustración 62 Diagrama FileNet Front 117
Ilustración 63 Diagrama Datacap 118
Ilustración 64 Diagrama App Connect 118
Ilustración 65 Arquitectura Gestor Documental 119
Ilustración 66 Capacidades VM Gestor Documental 119
Ilustración 67 Licenciamiento Oracle 120
Ilustración 68 IBM Licenciamiento 121
Ilustración 69 Estado Bases de Datos 124
Ilustración 70 Información base de datos – Servidor 126
Ilustración 71 Estadísticas CPU 126
Ilustración 72 Estadísticas Memoria 127
Ilustración 73 Estadísticas Pool compartido 127
Ilustración 74 Tamaño DDBB 127
Ilustración 75 Tamaño Esquema DDBB 128
Ilustración 76 Rendimiento DDBB 128
Ilustración 77 DDBB por Server 128
Ilustración 78 Host e Instancia CPU 129
Ilustración 79 Estadísticas Memoria 129
Ilustración 80 Estadística Shared Pool 129
Ilustración 81 Tamaño DDBB DBMINTRA 129
Ilustración 82 Tamaño Esquema DDBB 130
Ilustración 83 Rendimiento DDBB MINTRASG 130
Ilustración 84 Información DDBB PLIFERAY 130
Ilustración 85 Host e Instancia CPU 131
Ilustración 86 Estadísticas Memoria 131

Ilustración 87 Estadísticas Shared Pool 131
Ilustración 88 Tamaño DDBB PLifeRay 131
Ilustración 89 Tamaño Esquemas DDBB 132
Ilustración 90 Rendimiento DDBB PlifeRay 132
Ilustración 91 Información DDBB SIGEP 132
Ilustración 92 Estadística Host e Instancia 133
Ilustración 93 Estadística Memoria 133
Ilustración 94 Estadística Shared Pool 133
Ilustración 95 Tamaño DDBB SIGEP 133
Ilustración 96 Tamaño Esquema DDBB 134
Ilustración 97 Rendimiento DDBB SIGEP 134
Ilustración 98 Información DDBB DBSIMPC 135
Ilustración 99 Estadística CPU 135
Ilustración 100 Estadística Memoria 135
Ilustración 101 Estadística Shared Pool 135
Ilustración 102 Tamaño DDBB SIMPC 136
Ilustración 103 Tamaño Esquema DDBB 136
Ilustración 104 Rendimiento DDBB 136
Ilustración 105 Información servidor DBBB 137
Ilustración 106 Host e Instancia CPU 137
Ilustración 107 Estadística memoria 137
Ilustración 108 Estadística Shared Pool 137
Ilustración 109 Tamaño DDBB MINTRASD 138
Ilustración 110 Tamaño Esquemas 138
Ilustración 111 Rendimiento MINTRASD 138
Ilustración 112 Información Server DDBB 139
Ilustración 113 Host e Instancia CPU 139
Ilustración 114 Estadística Memoria 139
Ilustración 115 Estadística Shared Pool 140
Ilustración 116 Tamaño DDBB 140
Ilustración 117 Tamaño DDBB 140
Ilustración 118 Rendimiento DDBB 141
Ilustración 119 Información Server DDBB 141
Ilustración 120 Host e Instancia CPU 142
Ilustración 121 Estadística Memoria 142
Ilustración 122 Estadística Shared Pool 142
Ilustración 123 Tamaño DDBB 142
Ilustración 124 Tamaño Esquemas DDBB 143
Ilustración 125 Rendimiento DDBB 143
Ilustración 126 Información Server DDBB 144
Ilustración 127 Estadística CPU 144
Ilustración 128 Estadística Memoria 144
Ilustración 129 Estadística Shared Pool 144
Ilustración 130 Tamaño Esquemas DDBB 145
Ilustración 131 Comportamiento DDBB 146
Ilustración 132 Almacenamiento ASM 146
Ilustración 133 DiskGroup Data 146
Ilustración 134 DiskGroup Flash 147
Ilustración 135 DiskGroup Reco 147
Ilustración 136 DiskGroup Redo 147

Ilustración 137 Licenciamiento adicional componente IBM 147
Ilustración *138* Firewall de nueva generación. 148
Ilustración 139 Comportamiento ancho de banda 149
Ilustración 140 Tendencia de uso de ancho de banda 150
Ilustración 141 Top de usuarios por números de sesiones 151
Ilustración 142 Top de aplicaciones 152
Ilustración 143 Top de Autenticación 153
Ilustración 144 sesiones fallidas 154
Ilustración 145 Reporte mensual diciembre 155
Ilustración 146 Captura de pantalla perfomance 156
Ilustración 147 licencia sandbox 156
Ilustración 148 licencia sandbox 157
Ilustración 149 Detalle de latencia o errores 158
Ilustración 150 detalle de problemas en servicios 158
Ilustración 151 Detalle casos de uso 159
Ilustración 152 Detalle de alertas 159
Ilustración 153 Detalle de alertas 160
Ilustración 154 Detalle de incidentes 161
Ilustración 155 Detalle servidores 162
Ilustración 156 Detalle fortigate 162
Ilustración 157 Top attack types 163
Ilustración 158 Tipo de ataque 164
Ilustración Top de ataques 164
Ilustración 159 Consumo canal MPLS DC Principal 171
Ilustración 160 Estado Router MPLS DC Principal 172
Ilustración 161 Topología actualizada 173
Ilustración 162 Interface Fortimanager 174
Ilustración 163 Interface MPLS HUB SDWAN 174
Ilustración 164 Interface Internet HUB SDWAN 175
Ilustración 165 VPN SDWAN establecidas 175
Ilustración 166 Estado HUB SDWAN Datacenter 176
Ilustración 167 Estado HA HUB Sdwan 176
Ilustración 168 Recursos Fortimanager 176
Ilustración 169 Estado de casos Redes y Conectividad 183
Ilustración 170 Asignación de licencias 189
Ilustración 171 Comportamiento de tráfico 189
Ilustración 172 Top llamadas nacionales 190
Ilustración 173 llamada internacional de prueba 190
Ilustración 174 Top Celular 191
Ilustración 175 Top Local 191
Ilustración 176 Requerimientos por garantía 192
Ilustración 177 Disponibilidad y Continuidad TOIP 193
Ilustración 178 Equipos consola antivirus 203
Ilustración 179 Gestión consola antivirus – equipos usuario final 203
Ilustración 180 Top 10 virus detectado 204
Ilustración 181 NAPMBOLANOS 207
Ilustración 182 GUDACAICEDO 208
Ilustración *183 BOPJSALCEDO* 208
Ilustración 184 ANDCGONZALEZB 208
Ilustración 185 BOPMMORENOS 209

Ilustración 186 Eventos Ransomware 209
Ilustración 187 captura eventos ransonware 210
Ilustración 188 *Gestión consola Nessus* 211
Ilustración 189 *Escaneos programados* 211
Ilustración 190 TOP 10 - Activos más explotables 212
Ilustración 191 Vulnerabilidades gestionadas vs en remediación 213
Ilustración 192 captura envío de correo gestión de vulnerabilidades 214
Ilustración 193 Cronograma Ethical Hacking 214
Ilustración 194 Resultados auditoria de casos 216
Ilustración 195 Seguimiento Práctica Mejora 217
Ilustración 196 Resultado de Cumplimiento AM 218

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 diciembre de 2025

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 el día 31 de diciembre de 2025 se suscribió el modificatorio No.7 *con el fin de adicionar al valor del contrato de prestación de servicios número 574-2023 la suma de DOSCIENTOS QUINCE MILLONES DE PESOS ($215.000.000) M/CTE adicionado el 29 de diciembre de 2025, expedido por el Coordinador de Presupuesto.*

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 realizó 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: parchado de seguridad, servidores de bases de datos (Archivo sindical, Cobro Coactivo, Fivicot, Moodle, Rutraport, Siriti, SISGestión, Suite Vision Empresarial – SVE, Estado Joven, Rutec, Tesorería, PILA, RUAF, SAMPL, Observatorio laboral, 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 DE

- 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 BLOQU

- Se divulga mensaje informativo del **Gestor Documental** indicando que desde el 1/12/2025 **se inhabilitó la opción de cargue de Radicados Referidos en la sección de Producción de Documentos**, esto con el fin de que las respuestas de las peticiones se realicen de acuerdo con los flujos de trabajo establecidos en el Gestor Documental.



¡INFORMACIÓN
IMPORTANTE NOVED

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. Se tiene en seguimiento hasta que se requiera retorno al lugar definitivo y organización de los equipos a cargo de la UT.

- **Santafé de Antioquia / Antioquia:** El 11/12/2025 se realiza apertura de la inspección, la UT gestiona previamente envío de los equipos de TI requeridos para la operación y el desplazamiento del recurso técnico para la conexión y configuración de equipos. Las actividades realizadas son las siguientes, se incluye acta de la visita:
  - Verificar servicio de MPLS y conectividad de la sede que quedo operativo.
  - Configuración de Fortigate FG-40F para conexión LAN.
  - Mantenimiento general, actualización y puesta en operación de la impresora.
  - Suministro de papel.
  - Actualización de inventario.
  - Se suben a monitoreo de Zabbix los equipos de conectividad e impresora



Apertura_Santafe_Antioquia.pdf

- **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, a espera de respuesta de la entidad.
- **Cañas Gordas / Antioquia:** El 15/10/2025 por temas de salud, la funcionaria Marisol Palacios fue trasladada temporalmente a trabajar en la DT Antioquia, durante diciembre 2025 la usuaria retornó a la inspección, por lo que se habilitó la sede y el monitoreo de equipos.
- **El Doncello / Caquetá:** Se deja en mantenimiento en Zabbix la sede ya que el funcionario asignado estará de permiso y vacaciones desde el 28/11/2025 y hasta el 2/02/2026, deja equipos apagados.
- Desde el 19 de diciembre y hasta el 5 de enero se deja en mantenimiento de Zabbix las sedes Cáqueza y Tibú por vacaciones de los funcionarios del ministerio.
- Durante diciembre 2025 la entidad solicita **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 inicia la gestión pertinente.

c. **Plan de trabajo documentos SIG para publicación en la SVE:** Durante el período, el equipo de procesos trabajó en la actualización la documentación de las prácticas en la plantilla de procedimiento dada por la Oficina Asesora de Planeación (OAP) para su estandarización. Se remite paquete al enlace de la OAP – Cesar Augusto Valencia con las siguientes prácticas para revisión y remisión de observaciones si aplica:

- Procedimiento Práctica Habilitación de cambios en los Servicios de Tecnologías de Información - Formato Solicitud de Cambio (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

d. **Disposición de RAEES y Residuos Electrónicos:** Durante el período del informe no se gestionó recolección de residuos por parte del proveedor SUMA Desarrollo Ambiental para el Ministerio del Trabajo.

El 19/12/2025 se da respuesta vía correo electrónico a María Camila Acosta del Ministerio del Trabajo los ajustes y evidencia solicitada relacionada con la disposición de residuos en Nivel Central, matriz de compatibilidad, hoja de seguridad de los residuos y la evidencia de los cambios realizados sobre el punto de disposición.



RE_
IMPLEMNETACIÓN DI

e. **Implementación IPV6 en Dual Stack:** Durante el período, el equipo de implementación realizó actualización del Plan de Trabajo del proyecto y del Plan de Direccionamiento según el pool asignado a la entidad.

El 26/12/2025 vía correo electrónico se remite a la entidad información relacionada con el proceso de implementación del protocolo, precisando que en el mes de noviembre finalizó la asignación del pool a nombre del ministerio por parte de LACNIC, se aclara también que la implementación es por servicios de forma controlada y de acuerdo con el plan.



RE_ Re__## 192603
##_ IPv6 EU - Ministe

f. Otras actividades

- Referente a la **Encuesta de percepción del personal de Soporte en Sitio Territorial** se envió el comunicado a los Directores Territoriales vía correo electrónico desde la cuenta de Soporte MT, al cierre del periodo solo se han recibido 16 de 30 respuestas. Se verificará con el Coordinador del Grupo de Soporte Informático apoyo para solicitar a los directores pendientes por contestar.

- 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, se solicitó sean revisadas, definidas y ajustadas.

- El 01/12/2025 se recibe indicación del Coordinador del Grupo de Soporte Informático relacionado con la solicitud de firma de paz y salvo de los contratistas la cual se realizó de manera anticipada por el calendario contractual, por tal motivo se requiere que los contratistas que tengan equipos asignados se le haga firma acta de devolución del equipo dejando la observación "se firma acta de devolución anticipada por calendario contractual el contratista se compromete hacer la devolución el día (el día que el contratista indique)". Se genera plantilla para documentar en el acta, se dan lineamientos desde la práctica de activos al equipo de MDS y SS, se replica esta información con los equipos e interesados.




Gestión de Activos _ Procedimiento Devol
RECORDATORIO_ Gestión de Activos _ P

- **Divulgaciones al equipo de trabajo:**
  - El 1/12/2025 se realiza sesión con el personal de MDS, soporte técnico de Bogotá y Territorio con el propósito de socializar un cambio sobre el Gestor Documental, la sección "Radicados Referidos" se deshabilitó en todas las pantallas del proceso ya que se debe surtir los flujos correspondientes dados por el área funcional. También se remite comunicado desde Soporte MT a todos los usuarios.

  - El 10/12/2025 la gestora de la práctica ITIL de eventos reitera con el equipo de trabajo los lineamientos para la gestión de eventos, definiciones, generación de tickets, servicios monitoreados, gestión de cambios, mantenimientos programados y temas de monitoreo.



INFORMACIÓN IMPORTANTE!!! Linea

- El 17/12/2025 el equipo de procesos realiza refuerzo con todo el equipo de trabajo de la UT asociado a las prácticas ITIL que se tienen en operación en el Ministerio del Trabajo. Incidentes, Requerimientos, Problemas, Catálogo de Servicios, Activos, Eventos, Cambios, Disponibilidad, Implementación; la charla se enfocó en reforzar las definiciones, lineamientos, ANS según el tipo de solicitud/servicio, el árbol de categorías, la matriz de escalamiento de los servicios de TI. Se comparte el material vía correo electrónico:

Capacitación
Prácticas ITIL.msg

g. Volumetría de Solicitudes Gestionadas:

En el mes de diciembre 2025 se registraron en la herramienta ITSM 5969 solicitudes asociados 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: 5185
  - Incidentes: 756
  - Cambios: 27
  - Problemas: 1
- Casos Anulados: 5 - Anulados por el personal de la MDS, se presenta la justificación en el Numeral 2.2. Mesa de Servicios y Soporte en Sitio de este documento.
- Estado final de casos a corte de diciembre 2025:



Ilustración 1 Estado final de casos al corte del período

- Gestión por parte de los grupos de especialistas:

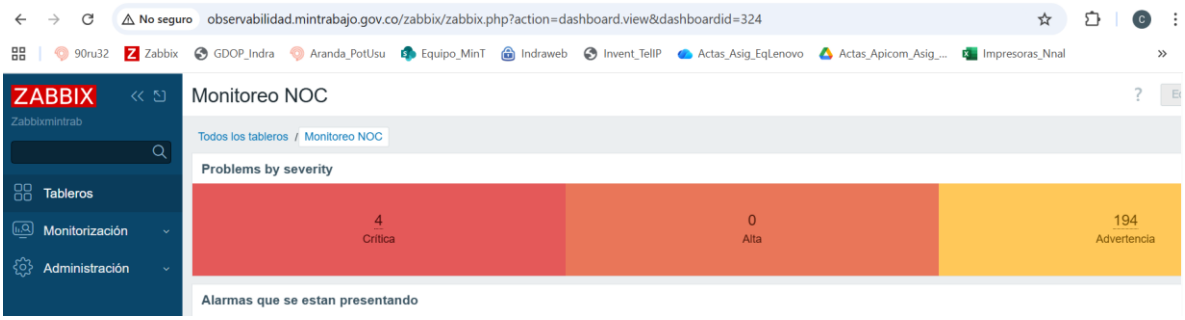
Grupo Responsable	Cantidad de casos gestionados	Porcentaje (%)
Responsable_Soporte_Territoriales	1662	27,84
Responsable_Soporte_Bogota	1401	23,47
Responsable_Mesa_De_Servicio	1071	17,94
Especialistas_IBM	519	8,69
Responsable_Soporte_Impresoras	495	8,29
NOC	466	7,81
Responsable_De_Servidores_Windows	64	1,07
Especialista_Telefonía_IP	56	0,94
SOC	52	0,87
Especialista Nube Privada	41	0,69
Especialista Base de datos	35	0,59
Especialista Herramientas de Gestion	21	0,35
Responsable Garantías Equipos	18	0,30
Gestor de Inventarios	17	0,28
Almacenamiento y Backups	14	0,23
Especialista Redes	9	0,15
Especialista Nube Publica	8	0,13
Especialista Aplicaciones .Net	7	0,12
Gestión del Servicio	7	0,12
Liferay	5	0,08
Responsable_de_Energia Electrica Regulada - UPS	1	0,02
TOTAL	**5969**	**100**

Tabla 1 Atención de solicitudes por Grupo de Especialista

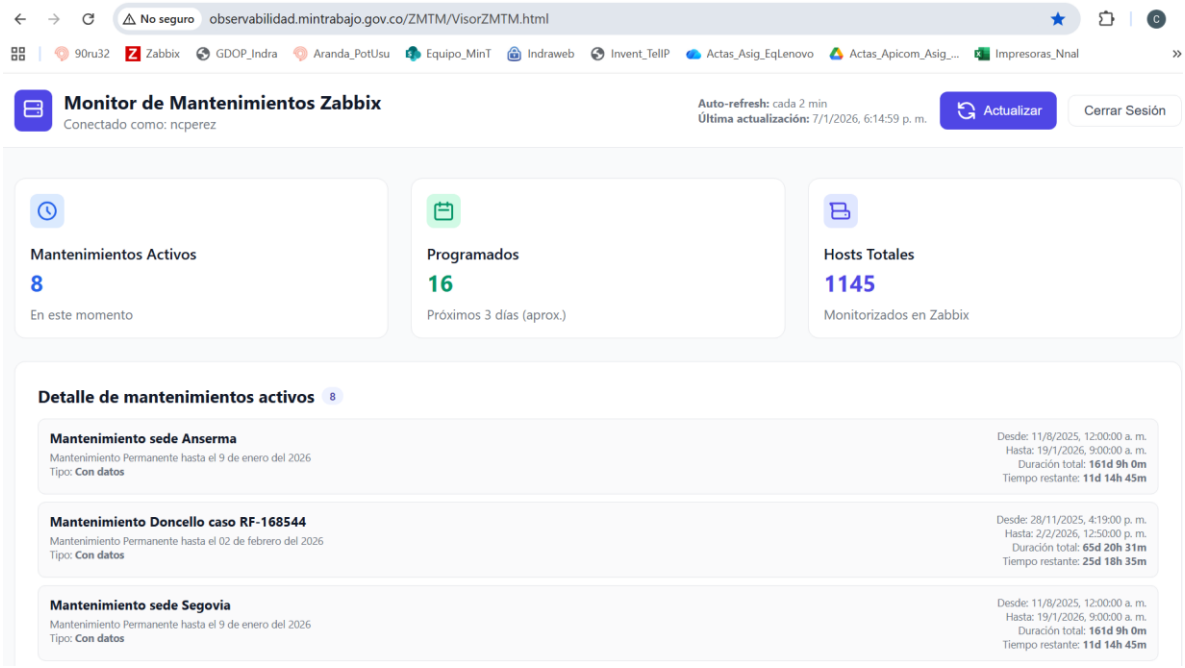
2.1.1. Herramienta de Gestión ITSM

Durante diciembre 2025 se realizaron las siguientes acciones en la herramienta de gestión Aranda y la herramienta de monitoreo Zabbix:

- Afinamiento de métricas para toma de latencia y perdida de paquetes en los hosts Internet Columbus, Router_MPLS_Scentral, BCK_MPLS_ColombiaXV, PRI_MPLS_ColombiaXV.
- Afinamiento de alertamientos basado en las métricas de perdida de paquetes y latencia.
- Se implementó nombre para la aplicación web de Zabbix para evitar exponer la IP del servidor, la url ahora es http://observabilidad.mintrabajo.gov.co/zabbix/



- Se realizó el desarrollo de la aplicación web VisorZMTM la cual permite visualizar de manera más sencilla los mantenimientos que se ejecutan y programan en Zabbix.



- Optimización de los filtros en la creación de casos a partir de correo electrónico para evitar creaciones no deseadas.
- Implementación del cambio de estado de los casos a partir de correo electrónico.
- Implementación de agregación de notas a los casos a partir de respuestas al correo electrónico enviado previamente por la herramienta.
- Afinamiento de los roles en ASMS, ADM, AQM para optimización de gestión de casos y uso de licencias de las herramientas.
- El 10/12/2025 se realiza actualización de los usuarios VIP en Aranda de acuerdo con listado recibido, estos corresponden a usuarios del piso 24 y 25.

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 diciembre de 2025, se realizó el seguimiento y control de los Acuerdos de Niveles de Servicio (ANS) parametrizados en la herramienta, en coordinación con los líderes de servicio, validando su cumplimiento conforme a lo definido contractualmente, de acuerdo con lo establecido en el Numeral 7. Medición de Acuerdos de Nivel de Servicio.

La medición mensual evidenció que los ANS se mantuvieron dentro de los niveles de cumplimiento esperados, garantizando la continuidad de los servicios. Sin embargo, se identificaron desviaciones puntuales en los indicadores de continuidad y disponibilidad del servicio de red WAN, el detalle de los valores de continuidad y disponibilidad se encuentra desagregado en el archivo "ANS Internet – MPLS". Las desviaciones corresponden a los siguientes indicadores:

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

Frente a estas desviaciones, se adelantaron acciones de análisis y seguimiento con los responsables del servicio, orientadas a identificar causas raíz identificadas por el proveedor, fortalecer el monitoreo y proponer acciones de contingencia para la prestación del servicio,

En conclusión, el desempeño general de los ANS durante diciembre de 2025 fue satisfactorio, manteniendo la estabilidad del servicio y reforzando los mecanismos de control y mejora continua.

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 diciembre de 2025. Este apartado contiene información relevante sobre actividades realizadas y novedades presentadas.

- **Tipificación de los cambios**

Durante el mes de diciembre de 2025 se gestionaron 27 casos tipificados como Cambios, clasificados en las siguientes categorías:

Servicio	No	Porcentaje
Administración de Bases de Datos	10	47,62%
Administración de servidores	9	42,86%
Aplicaciones Especializadas	5	23,81%
Energía Eléctrica Regulada - UPS	1	4,76%
Redes y Conectividad	1	4,76%
Telefonía IP	1	4,76%
Total	**27**	**100,00%**

Tabla 2 Tipificación de los cambios

- **Relación casos registrados**

A continuación, se presenta la relación de casos registrados del 1 al 31 de diciembre de 2025, en total se crearon 27 casos de los cuales se gestionaron 11 como cambios de normales, 9 cambios como de emergencia y 7 cambios como estándar



SHC_Diciembre_2025xlsx.xlsx

- **Cambios por estado**

Al corte del 31 de diciembre, veintidós (22) casos quedaron estado Cerrado y cinco (5) en 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: 26/27*100 PCE: 96,29%

Tabla 3 Medición Indicador Porcentaje de Cambios Exitosos

Durante el período evaluado 26 casos fueron exitosos y 1 fue clasificado como no exitoso, que corresponde al RFC-173897, obteniendo un PCE de 96,29%, resultado que supera la meta establecida del 80%.
En el caso del RFC-173897, se realizó la ejecución del script en la base de datos RUTEC, la cual no presentó errores técnicos durante su ejecución. No obstante, en la fase de validación posterior se evidenció que no se afectó ni actualizó ningún registro en la tabla TB_MIGRANTE_TRABAJADOR, que era el objetivo del cambio. Dado que el resultado esperado no se cumplió, el cambio fue clasificado como NO EXITOSO, de acuerdo con los criterios definidos en el proceso de Gestión de Cambios, aun cuando no se generaron impactos operativos.

En conclusión, el resultado se evidencia un proceso de cambios mayoritariamente efectivo y controlado, con una adecuada planeación y ejecución, y con mecanismos de validación que permiten identificar oportunamente desviaciones, contribuyendo a la mejora continua del proceso y a la estabilidad de los servicios.

- **Procedimiento Cierre de Año Habilitación de Cambios**

El 16 de diciembre la UT comunica a los especialistas que con motivo de los días festivos del 24 y 31 de diciembre, se realizarán los siguientes ajustes en el calendario de la práctica de Habilitación de Cambios:

- El último Comité de Evaluación de Cambios (CAB) del año se llevó a cabo el 17 de diciembre.

- Se recibieron solicitudes de Cambio (RFC) hasta el 16 de diciembre, con el fin de ejecutar los cambios a más tardar los días 19 o 20 de diciembre, en atención a los procedimientos de cierre de año.
- De manera excepcional, únicamente se atendieron cambios de emergencia, los cuales deberán contar con la debida justificación, firma y la aprobación del líder funcional correspondiente.
- Finalmente, se informa que la recepción de Solicitudes de Cambio (RFC) se retomará a partir del 2 de enero de 2026, y los Comités de Evaluación de Cambios (CAB) se reanudarán desde el 7 de enero de 2026.

2.1.2.3. Práctica Gestión de Activos

Durante diciembre de 2025, la Práctica de Gestión de Activos adelantó diversas acciones orientadas a garantizar la continuidad operativa, la disponibilidad óptima y el adecuado control del parque tecnológico de la Entidad. Todas las actividades se ejecutaron en cumplimiento de las mejores prácticas y lineamientos institucionales, con enfoque en la trazabilidad, uso eficiente de los recursos, mitigación de riesgos y soporte a la toma de decisiones.

Las principales actividades desarrolladas fueron:

- **Seguimiento a la gestión de activos**

Durante el período reportado, se llevó a cabo la ejecución del monitoreo de asignación, estado y vigencia de los activos, actualización del inventario para contar con la información actualizada y la toma de decisiones.

- **Seguimiento a Garantías y Procesos de Siniestro**

Se efectuó el seguimiento y control de los equipos en garantía y en proceso de siniestro, con el propósito de asegurar el cumplimiento de los tiempos establecidos garantizando la continuidad operativa de los recursos tecnológicos, así mismo se realizó la entrega de equipos de contingencia.

- **Gestión de Activos / Procedimiento Devolución Computadores Contratistas**

Por temas de finalización de contratos y finalización de año, la Coordinación del Grupo de Soporte Informático, solicitó indicar a los técnicos de soporte los lineamientos para la devolución de los equipos:
La firma de paz y salvo de los contratistas se realizará de manera anticipada, conforme al calendario contractual. Por tal motivo, se requiere que los técnicos de soporte en sitio gestionen la firma del Acta de Devolución del Equipo, dejando consignada la siguiente información:

- Describir el estado actual del equipo (de escritorio o portátil) y de todos sus accesorios, detallando condiciones físicas, golpes, rayones y/o cualquier otra novedad encontrada.
- Registrar el día y la hora en que se realizó la revisión del equipo.

- Indicar la fecha en la que el contratista se compromete a realizar la entrega física del equipo y demás elementos asignados.
- Informar al contratista que el equipo y sus accesorios permanecerán bajo su responsabilidad hasta el día de la entrega.
- Crear un caso por devolución de equipo, en el cual se deberá adjuntar el acta debidamente firmada y las evidencias fotográficas del estado del equipo en el momento de la firma.
    - Dicho caso deberá quedar en estado Suspendido, con el técnico de soporte en sitio como responsable, hasta que el equipo y sus accesorios sean retornados físicamente.
    - El acta permanecerá en custodia del técnico hasta la entrega física del equipo y sus accesorios.
    - Una vez realizada la devolución, el caso deberá ser escalado a la administradora de inventarios.

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 10/12/2025 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, usuarios VIP de piso 24 y 25 y la matriz de escalamiento según validaciones de primer nivel para soporte impresión e inventarios.



INFORMACIÓN
IMPORTANTE!!! Linea

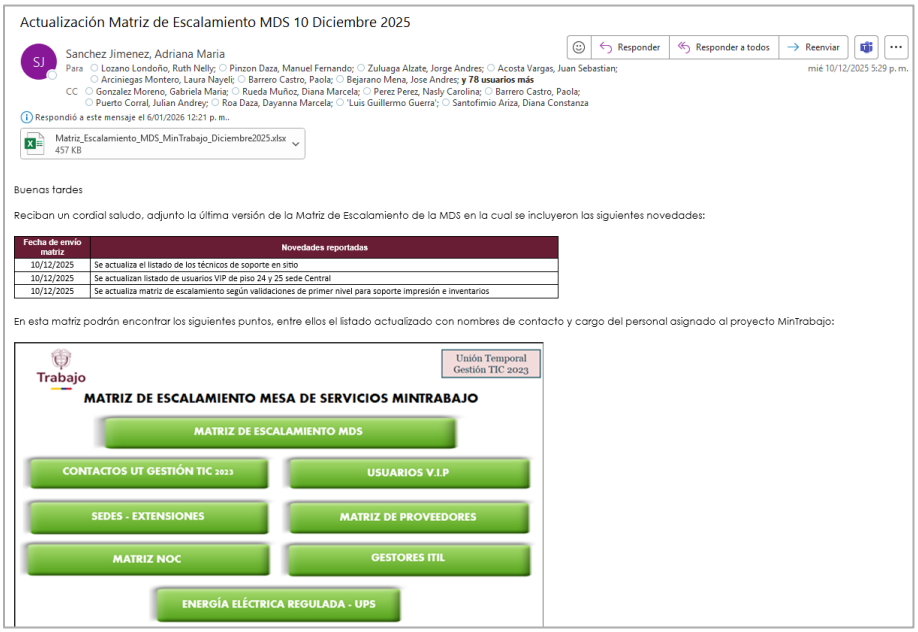


Ilustración 2 Socialización matriz de escalamiento

- 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

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 diciembre
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 4 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 diciembre 2025. 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 5 Consolidado problemas identificados

Durante el mes de diciembre se realizó seguimiento al caso 137015 asociado con el Gestor Documental.

Avances: Se finalizó la instalación y migración del componente de filenet cambiando sistema operativo 2019 al 2022, se solventa el error presentado con la máquina anterior. La nueva máquina se encuentra en monitoreo continuo para validar que todos los procesos y documentos se almacenen correctamente, así mismo para validar la integridad con los demás componentes que hacen parte del gestor documental. Se adjuntó en la herramienta de gestión documento con las evidencias de las actividades realizadas.
Con la información suministrada por los especialistas de IBM se documenta y cierra el caso con solución definitiva.

Durante el mes de diciembre se realizó apertura del caso 174025 asociado con el Gestor Documental.

Teniendo en cuenta que se presentaron incidentes recurrentes relacionados con el gestor documental los días 15 y 16 de diciembre, lo que evidenció falla al momento de radicar documentos y lentitud. Al validar con el especialista indica que se realizó una reinstalación de Filenet en un nuevo servidor según el problema asociado PM-137015, se presentó falla debido a una sobrecarga de memoria en la máquina, por lo tanto, se generó un nuevo problema PM-174025. Ya que se indicó que la afectación se debió a un bloqueo generado en Filenet, cuya causa raíz aún se encuentra en análisis. No obstante, en su momento la recuperación del servicio se logró mediante el reinicio de los servicios.
Con la información suministrada por los especialistas de IBM se documenta el caso con solución temporal.

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 diciembre 2025. Se incluye información relevante sobre los incidentes registrados, las acciones ejecutadas y las novedades ocurridas.

Durante el período del informe, se registraron 756 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	714
En proceso	8
Solucionado	17
Suspendido	17
Total general	756

Tabla 6 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	243	Incidentes generados en el servicio de redes y conectividad por afectaciones en infraestructura del proveedor.
Reportar una falla.Alarma Zabbix.Starlink	105	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.Alarma Zabbix.FortiGate	79	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.Gestor Documental.Falla radicacion	51	Novedades presentadas debido a errores generados en el radicado, extensiones de archivo erróneas, lentitud presentada con el gestor documental
Reportar una falla.Alarma Zabbix.Servidor Windows	39	Alertas generadas por actividad programada en RFC-172087, novedades en plataforma SFT, espacio al 90% en disco de servidor MINTRABGD03A, intermitencias en aplicaciones de aproximadamente 15 minutos en aplicaciones como SIRITI, con jóvenes, FTRUTEC, Tesorería y calculadora laboral
Reportar una falla.Falla impresora.No imprime	39	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.Gestor Documental.Falla Funcional	24	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.

Tipo de incidente	Total	Observación
Reportar una falla.Falla impresora.Atasco	20	Casos generados por atasco de papel en impresoras
Reportar una falla.Gestor Documental.Lentitud gestor	14	Lentitud debido al alto impacto y consumo de transacciones, en el que se evidencia bajo el análisis técnico que pasamos de 6000 a 8000 transacciones diarias, generando esto un alto consumo sobre la aplicación y base de datos, por otro lado, las conexiones simultaneas realizadas diariamente generan un consumo aun mayor en la aplicación
Reportar una falla.Equipo de computo.Falla - Error conexión a red	13	Novedades presentadas debido a contraseñas que caducan, desconexión de red Wifi, renovación de dirección IP. ETC.

Tabla 7 Top 10 Incidentes

- **Casos Suspendidos**

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

Grupo Resolutor	Noviembre	Diciembre
NOC		15
Especialistas_IBM		7
Responsable_de_Energia Electrica Regulada - UPS	6	0
Responsable_Soporte_Impresoras		2
Especialista_Telefonía_IP		1
Total general	6	25

Tabla 8 Incidentes Suspendidos

Del total de casos en backlog (suspendido y en proceso), se registra 31 tickets en gestión por parte de los grupos resolutores tales como NOC (15), especialistas IBM (7), Responsable_de_Energia Electrica Regulada – UPS (6), Responsable Impresoras (2), Telefonía IP (1). Durante el período algunos casos permanecen en estado suspendido, ya que corresponden a los procesos de evaluación y diagnóstico con el cliente, especialistas y proveedores.

- **Incidentes Mayores**

Del total de incidentes reportados, los siguientes casos fueron registrados como incidentes mayores afectando los servicios de Gestor documental (1), Intranet (1), redes y conectividad (3) los cuales se detallan a continuación:

Incidente Aranda	Estado	Fecha Registro Caso	Novedad	Causa Raíz	Acciones Realizadas para restablecer el servicio	Usuarios Afectados	Fecha/Hora inicio	Fecha/Hora Fin	Tiempo de Indisponibilidad
IM-173837	Cerrado	22/12/2025 11:35	Incidente Mayor Falla en Gestor Documental	Bloqueo de servidor BPM por desincronización del bus de BPM.	Se reiniciaron servidores AppCluster, MECluster y SUBCluster, se realizó la sincronización de nodos, se realizaron pruebas a nivel nacional, confirmando la operatividad del servicio.	General	22/12/2025 6:45	22/12/2025 7:45	1 hora de indisponibilidad
IM-174236	Cerrado	23/12/2025 14:52	Incidente Mayor Sin	La causa raíz del incidente corresponde a	Con base en el análisis técnico y la recomendación del	Usuarios de la Entodad	23/12/2025 9:40	26/12/2025 17:00	3 días

Incidente Aranda	Estado	Fecha Registro Caso	Novedad	Causa Raíz	Acciones Realizadas para restablecer el servicio	Usuarios Afectados	Fecha/Hora inicio	Fecha/Hora Fin	Tiempo de Indisponibilidad
			Acceso a la Intranet	incompatibilidades y fallas funcionales generadas tras la actualización del Portal Web de Liferay DXP versión 7.3 a la versión 7.4, las cuales impactaron el proceso de autenticación y el acceso a la Intranet. Dichas inconsistencias afectaron el comportamiento normal del servicio, impidiendo el ingreso de los usuarios sin presentar mensajes de error visibles. El análisis técnico realizado con el proveedor Liferay determinó que la versión 7.4 presentaba comportamientos no esperados en el entorno productivo, por lo cual se recomendó como acción correctiva la ejecución de un rollback a la versión estable 7.3.	soporte de Liferay, se definió como acción correctiva la ejecución de un rollback del Portal Web a la versión Liferay DXP 7.3, debido a errores presentados tras la actualización a la versión 7.4. Para la ejecución de esta actividad se radicó el RFC-174811, programado para el sábado 27 de diciembre, dentro de la ventana de mantenimiento establecida.				
IM-170536	Cerrado	9/12/2025 14:11	Incidente Mayor Lentitud en la red	saturación en el canal de internet en el Datacenter Colombia XV debido a un alto consumo de tráfico	En conjunto con el equipo de seguridad se identificaron IP origen con alto consumo que generaban saturación en el canal de CIRION, se creó una regla en el firewall de Cirion que limita el consumo por IP a un máximo de 100 Mbps. Con esta medida, se logró reducir la saturación del canal. Se realizaron pruebas de navegación, confirmando tiempos estables.	No se presentó indisponibilidad, pero si se evidencio degradación en el servicio de internet por un tiempo aproximado de 2 horas y 30 minutos.	9/12/2025 8:15	9/12/2025 10:35	No se presentó indisponibilidad, pero si se evidencio degradación en el servicio de internet por un tiempo aproximado de 2 horas y 30 minutos.
IM-174544	Cerrado	24/12/2025 15:31	Incidente Mayor Sin red zona norte	Se presentó afectaciones debido a una doble apertura en el tramo Nogales – Fundación y atenuaciones en el tramo de MC de Nogales hacia Turbaco.	Para mitigar la situación, se realizó el enrutamiento de la TG por Balsos, lo que permitió recuperar la operatividad del servicio en su totalidad.	Router_Cienaga Router_Fonseca Router_Plato Router_Fundacion RInternet_ETB_Santa_Marta	24/12/2025 4:08	24/12/2025 10:14	6 horas y 6 minutos
IM-174511	Cerrado	24/12/2025 14:11	Incidente mayor servicios Cali	se vio afectado por una falla de alto impacto que se presentó a la zona debido a una falla de la lambda 78 de Anillo Sur para el tramo Balsos	Para recuperar el servicio se hizo reinicio de la tarjeta NS4 que lleva la Lambda 78 y se recuperó la gestión y los servicios.	Router Buenaventura CAV3000077624 router armenia CAV3000077725	24/12/2025 6:22	24/12/2025 7:18	54 minutos

Incidente Aranda	Estado	Fecha Registro Caso	Novedad	Causa Raíz	Acciones Realizadas para restablecer el servicio	Usuarios Afectados	Fecha/Hora inicio	Fecha/Hora Fin	Tiempo de Indisponibilidad
				- Santa Mónica y debido a que se tuvo abierto el nodo hacia el tramo Popayán San Bernardino - Neiva El Bote se aisló el equipo OSN8800 de San Bernardino y se afectaron los servicios que llegan a Cali por la Lambda 78.		router popayan CAV3000077742 RInternet_ETB_Buenaventura ID00082677 RInternet_ETB_Cali ID00082676 RInternet_ETB_Pereira ID00082723 RInternet_ETB_Manizales ID00082706 Bugalagrande CAV3000077621			

Tabla 9 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.

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 diciembre
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= 96,4%
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= 0,0%

Tabla 10 Medición de KPIs

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

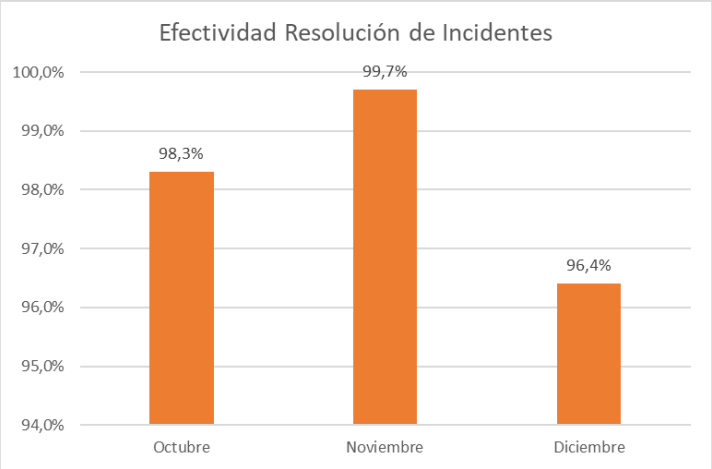


Ilustración 3 Efectividad de resolución de incidentes

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:

- Octubre: 98,2%
- Noviembre: 99,7%
- Diciembre: 96,4%

Se identificó disminución en el cálculo del KPI debido a que 2 casos presentaron afectación del ANS y 25 quedaron en proceso y en suspendido a corte del 31 de diciembre. 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.

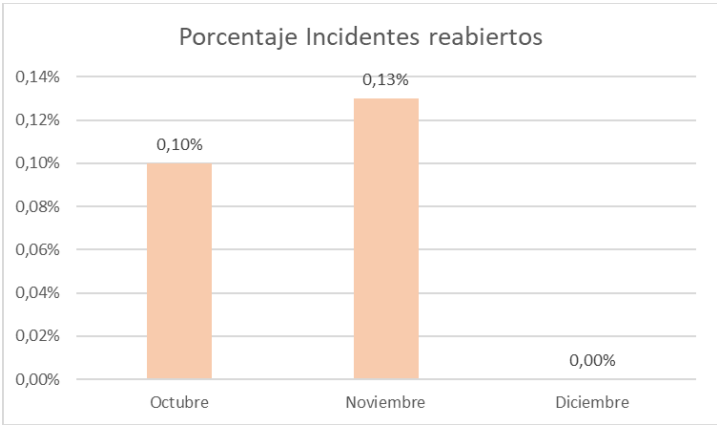


Ilustración 4 Porcentaje de incidentes abiertos

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

- Octubre: 0,10%
- Noviembre: 0.13%
- Diciembre: 0,0%

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 diciembre 2025. Este apartado contiene información relevante sobre los requerimientos generados en el periodo de medición, las actividades realizadas y novedades presentadas. En total se registraron 5185 casos tipo requerimiento quedando en los siguientes estados:

Estado	Casos
Cerrado	4917
Solucionado	218
Suspendido	25
En proceso	24
Registrado	1

Tabla 11 Estados de Requerimientos

- Durante el mes, no se presentaron casos en estado anulado.
- Realizando el seguimiento del Backlog de los casos suspendidos, en la siguiente tabla se observa el avance de atención los casos en este estado desde noviembre al periodo actual.

Grupo Responsable	Noviembre	Diciembre
Especialista Aplicaciones .Net	1	0
Especialista Herramientas de Gestión	0	0
Especialista Nube Privada	1	0
Especialista Nube Publica	0	0
Especialista Redes	2	0
Especialista_Telefonía_IP	0	0
SOC	3	1
Especialistas IBM	3	0
Responsable Garantías Equipos	9	9
Responsable_De_Servidores_Windows	1	1
Responsable_Mesa_De_Servicio	16	6
Responsable_Soporte_Bogotá	10	6
Responsable_Soporte_Impresoras	15	1
Gestor de Inventarios	2	0
Responsable_Soporte_Territoriales	14	0
Responsable_de_EER - UPS	1	0
Especialista Base de datos	1	1
Total por Periodo	**94**	**25**

Tabla 12 Seguimiento del Backlog Suspendidos

En el inicio del período, se identificaron 94 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 69 casos a través de la herramienta de Gestión Aranda de los anteriores periodos. Para el cierre del mes, se encuentran pendientes 25 casos en el mes de diciembre, los cuales se identificaron por: espera de información por parte de los usuarios finales, solicitudes de líderes funcionales o supervisor del contrato (sesiones de seguimiento y validación de aplicaciones frente a los códigos fuente o

requerimientos de desarrollo), a la espera de la terminación de tóner en los equipos de impresión, siniestros y entrega de informe técnico de las garantías de equipos.

- 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. Cargué de papel en impresora	649
Radicar una solicitud. Impresora. Instalación - configuración	467
Radicar una solicitud. Alarma Zabbix.Impresora	389
Radicar una solicitud. Impresora. Aumento de cuota	380
Radicar una solicitud. Directorio activo. Cambiar contraseña	166
Radicar una solicitud. Gestor documental. Relanzamiento	152
Radicar una solicitud. Correo Electronico.Asesoria - Consulta	138
Radicar una solicitud. Impresora. Mantenimiento preventivo	133
Radicar una solicitud. Gestor documental. Asignar Radicado TYS	99
Radicar una solicitud. Ofimatica.Soporte Aplicaciones Office 365	97

Tabla 13 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 649 tickets, instalación y configuración con 467 tickets, Alarma Zabbix Impresora con 389 tickets, y aumento de cuota con 380 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=** 5179/5185 *100
	EF: Efectividad en solución de Requerimientos.			
	RFS: Requerimientos solucionados que cumplen el ANS en el período.			**EF= 99.88%**
	RFR: Requerimientos registradas en el período.			
Porcentaje de Requerimientos Reabiertos en el Periodo	**RRP:** Porcentaje de casos Reabiertos en el periodo.	<2%	Mensual	**RRP=** 2/5135*100
	RFR: Requerimientos Reabiertos en el período.			**RRP= 0,039%**
	RFS: Requerimientos solucionadas en el período.			

Tabla 14 Detalle de KIP Practica de Requerimientos

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

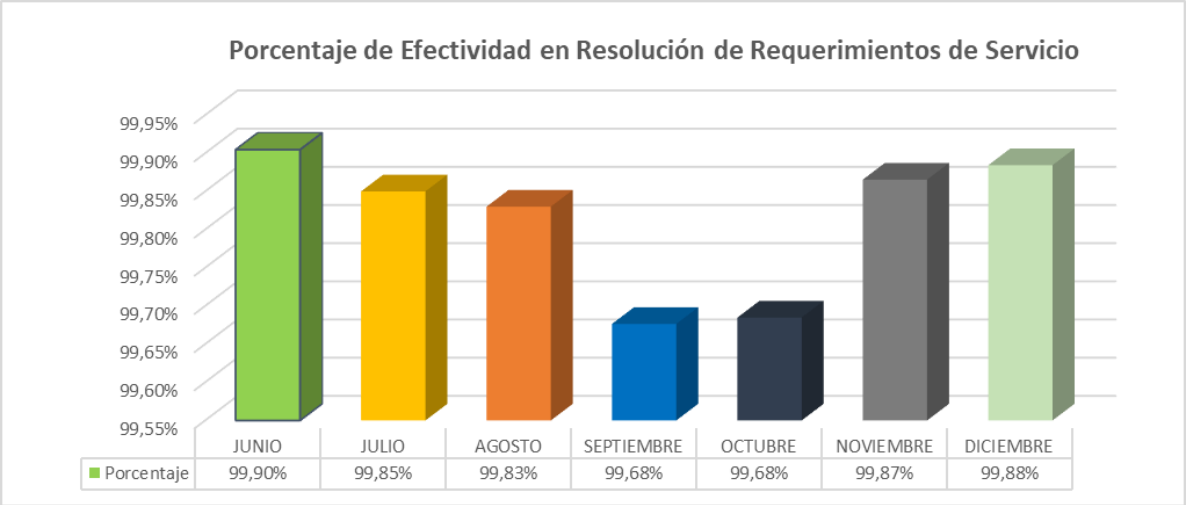


Ilustración 5 KPI Efectividad de Resolución de Requerimientos de Servicio

Durante el periodo, se evidencia el cumplimiento del 99.88% aumenta efectividad de la solución de los requerimientos a comparación de los anteriores periodos, los cuales se verifica de 5185 casos registrados en los diferentes canales oficinales de la Mesa de Servicio que fueron solucionados, 5179 casos cumplieron con los tiempos del ANS para dar una respuesta efectiva al usuario y 6 casos no cumplieron la efectividad por no realizar la actualización el estado y seguimiento continuo del caso, por lo cual se continuará las retroalimentaciones a los Servicios TIC.

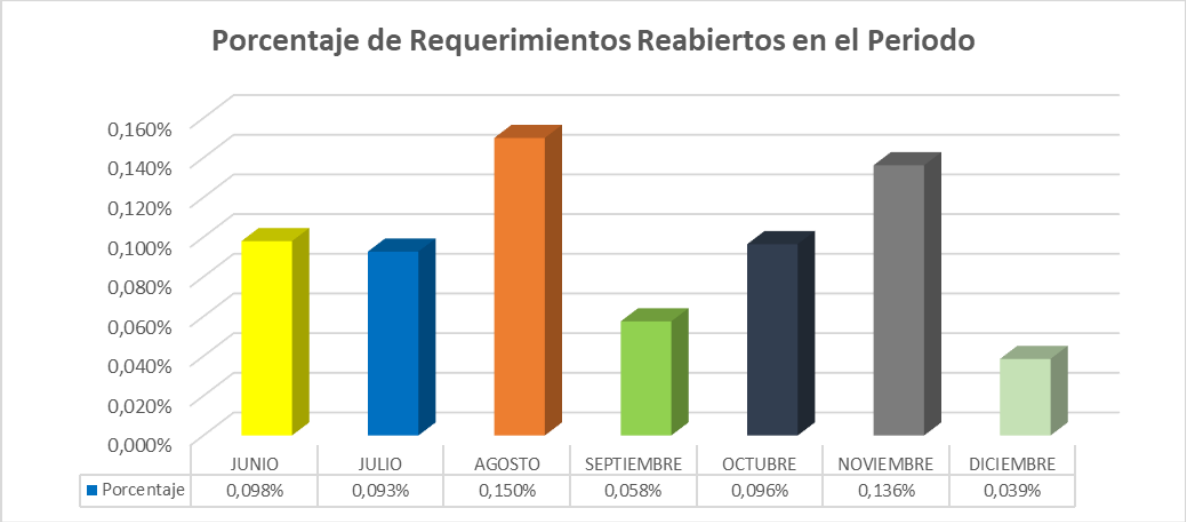


Ilustración 6 Requerimientos de Reabiertos en el periodo

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 a las retroalimentaciones y revisión del backlog desde la Práctica de requerimientos con los servicios TIC.

Para diciembre se presentaron 2 casos reabiertos y actualmente se encuentran cerrados. 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-170472	Radicar una solicitud. Gestor documental. Asignar Radicado TYS	Especialistas IBM	Se solicita por parte de la usuaria devolver una PQRS y al remitirla de nuevo sale error, por tal motivo solicita realizar esta devolución.	Se evidencia por parte de los especialistas indican esa actividad en el requerimiento, se debe hacer por parte de cada usuario de manera interna, por lo tanto, se indica en la solución y la usuaria no está de acuerdo la respuesta del especialista y reapertura el caso. Después se realiza seguimiento e indican lo siguiente: ***En atención a la información compartida en el correo adjunto, se realizó la verificación correspondiente y se evidenció que la información del traslado está errada, ya que falta incluir la persona a quien debe asignarse la actividad.*** Por lo anterior, este caso debe proceder a gestionarlo el usuario y se retroalimenta al especialista de IBM para que sea claro en la documentación de la solución y poder explicarle de manera sencilla a los funcionarios.
RF-172560	Radicar una solicitud. Navegadores. Instalación - Configuración	Responsable_Soporte_Territoriales	Usuario solicita permiso para ingreso a la plataforma de Jurados de Votación Congreso de la República 2026. https://juradoscongreso2026.registraduria.gov.co	Se indica que la solicitud se está gestionando por el área encargada con el caso RF-172883 por lo tanto, al ver esta respuesta el usuario no está de acuerdo con el cierre del caso porque se sigue presentando el error en la página que quiere ingresar. En el caso RF-172883, se brindó la respuesta y realizó el respectivo soporte y solución al caso.

Tabla 15 Casos reabiertos

2.1.2.8. Práctica de Eventos

Para el mes de diciembre, 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 834 casos escalados mediante la herramienta de gestión de los cuales 500 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.

- **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
- Se realizó la socialización de los lineamientos de la practica de eventos y monitoreo

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 diciembre
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= (483/500)*100 EF= 96,6%

Tabla 16 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 500 incidentes, lo cual evidencia una alta capacidad operativa y de respuesta ante eventos críticos.
Los Routers fueron el componente con mayor incidencia, concentrándose 244 casos (49% 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 un leve aumento en los casos reportados por Antenas Starlink, los cuales se encuentran en el segundo lugar, representando 105 (21% 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 representaron el 16% de los casos (79 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 51 (10% del total) de los incidentes, evidenciando este mes un leve aumento en comparación con el mes anterior, aunque, son considerablemente altos en comparación con los Servidores Linux con solo 4 casos, representando el 1% del total de los casos.
Los Access Points ocupan el 5to lugar con un 2% (10 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 UPS y Switches en conjunto reflejan una baja incidencia del 1% (7) 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 diciembre se gestionaron 244 incidentes relacionados con equipos de red Routers en diferentes sedes a nivel nacional, los cuales representaron el 49% de los casos.

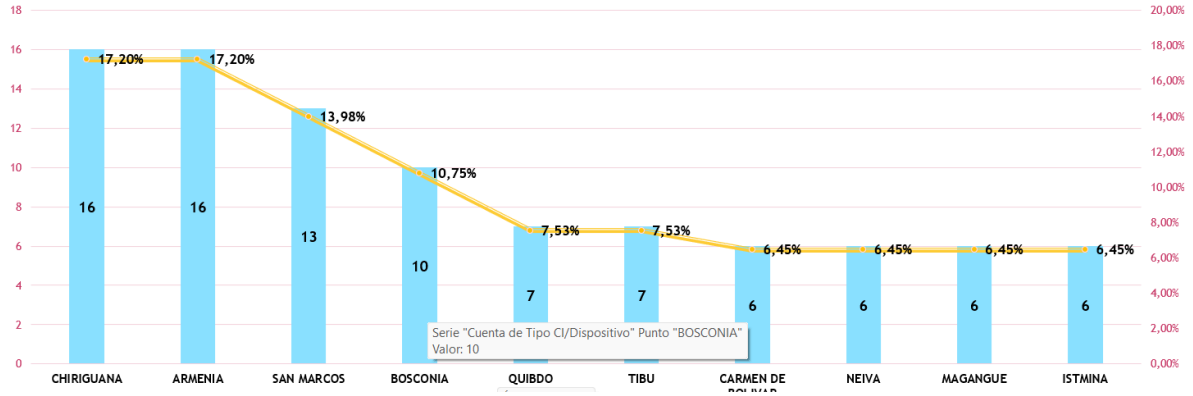


Ilustración 7 Top de incidentes por sedes

- Para este mes se evidencia que las sedes Chiriguaná y Armenia se consolidan como las sedes del TOP 10 con mayor número de incidentes, registrando 16 casos cada una, representando en conjunto el 34,4%) del total de los casos para esta categoría. La causa predominante en todos ellos 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.

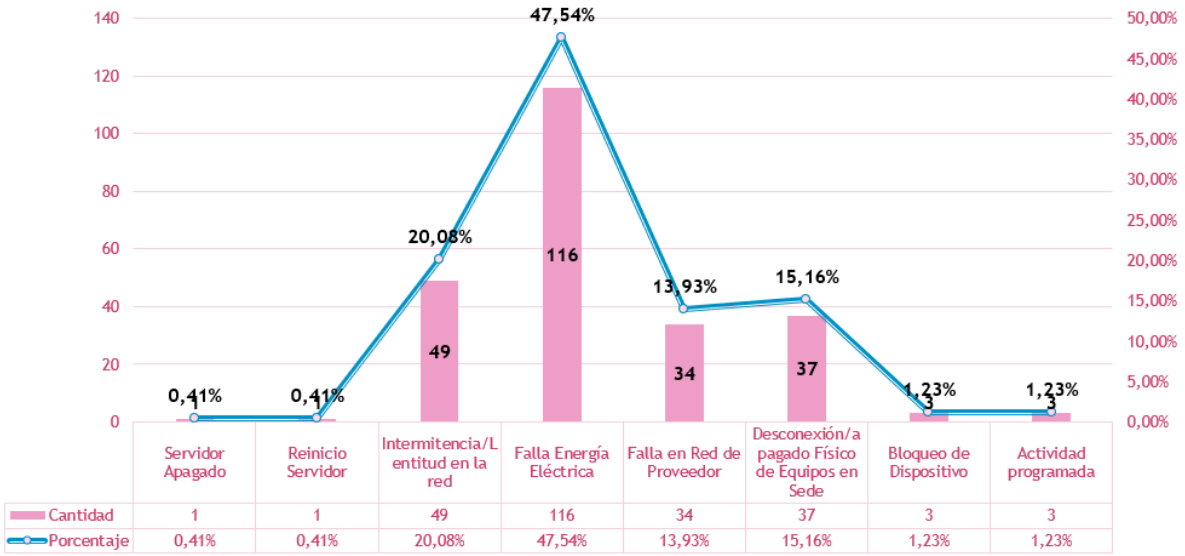
- San Marcos ocupa el segundo lugar con 13 casos (13,98%) corresponden en su mayoría (8 de los 13 casos) a fallas en Desconexión/apagado Físico de Equipos en Sede, 3 de los casos por falla de energía, 1 caso por servidor apagado y 1 caso por Intermitencia/Lentitud en la red.

- Bosconia ocupa el tercer lugar con 10 casos de los cuales 4 son por falla de energía eléctrica, 5 por Desconexión/apagado Físico de Equipos en Sede y 1 por Intermitencia/Lentitud en la red.

- Quibdó y Tibú se posicionan en el cuarto lugar del TOP 10 con 7 casos cada una. La causa principal de los incidentes en Quibdó para este mes está dividida en tres, por

un lado 3 casos por energía eléctrica, 2 casos con proveedor y 2 casos por Intermitencia/Lentitud en la red. Por otro lado, Tibú presento causa principal 3 casos por Desconexión/apagado Físico de Equipos en Sede, 2 casos por falla de energía y 2 casos por Intermitencia/Lentitud en la red.

- Las sedes de Carmen de Bolívar, Neiva, Magangué e Istmina, las cuatro con 6 casos cada una relacionada a Routers. En Carmen de Bolívar 4 de los 6 incidentes se relacionan a Falla Energía Eléctrica y los 2 restantes a falla en red de proveedor. Neiva registro 6 casos relacionados, 3 por Intermitencia/Lentitud en la red, 1 por falla en red de proveedor y 2 por falla de energía eléctrica. Magangué registro 6 casos de los cuales 3 fueron por falla de energía y 3 por el restante por falla en red de proveedor. Istmina registro 6 casos de los cuales 5 por falla de energía y el restante por Intermitencia/Lentitud en la red.



	Servidor Apagado	Reinicio Servidor	Intermitencia/Lentitud en la red	Falla Energía Eléctrica	Falla en Red de Proveedor	Desconexión/apagado Físico de Equipos en Sede	Bloqueo de Dispositivo	Actividad programada
Cantidad	1	1	49	116	34	37	3	3
Porcentaje	0,41%	0,41%	20,08%	47,54%	13,93%	15,16%	1,23%	1,23%

Ilustración 8 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 47,54% y seguido por la falla en Intermitencia/Lentitud en la red y este último con un 20,08% del total de los casos para esta categoría.

- Las fallas por energía eléctrica representan el 47,54% de los casos (116), afecta principalmente a zonas remotas o rurales como Istmina, Bosconia, Chiriguana, Armenia, entre otras, donde la red eléctrica es inestable o está sujeta a cortes constantes.

- El 20,08% (49) 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 Pasto, Neiva, Armenia y Caqueza.

- El 15,16% (37) de los casos están relacionados a desconexión apagado físico de equipos en sede, siendo Chiriguana la que registra mayor cantidad de eventos con 11, seguida de San Marcos con 7 registros, los cuales son ocasionados porque los funcionarios apagan los equipos al salir de turno con el fin de prevenir la afectación de los equipos por picos altos en el servicio de energía.

- El 13,93% (34) de los casos están relacionados a Falla en Red de Proveedor de Conectividad, siendo Armenia la sede con mayor número de eventos registrados (6) por esta causa y seguido por Florencia y Magangué cada una con 3 casos. Estos registran todos en estado cerrado por rupturas en la fibra y solucionados por personal del equipo de empalmaría en terreno.

- El 3,28% (8) de los casos es por bloqueo de dispositivo, actividad programada, servidor apagado y reinicio servidor que en conjunto suman este porcentaje. Siendo bloqueo de dispositivo y actividad programada las dos categorías con mayor numero de eventos, que sumadas en conjunto representan 6 casos (2.46%) de los eventos registrados y por último servidor apagado y reinicio servidor con 1 evento (0,41%) cada una. En varios casos, el bloqueo ocurre tras eventos eléctricos o fluctuaciones de red.

Switches

Desde el Centro de Operaciones (NOC), durante el mes de diciembre se generaron 5 casos referentes a Switches en la herramienta de monitoreo Zabbix en diferentes sedes, los cuales representan el 1% del total de los casos, donde se evidencia una baja de 5 casos en comparación con el mes pasado.

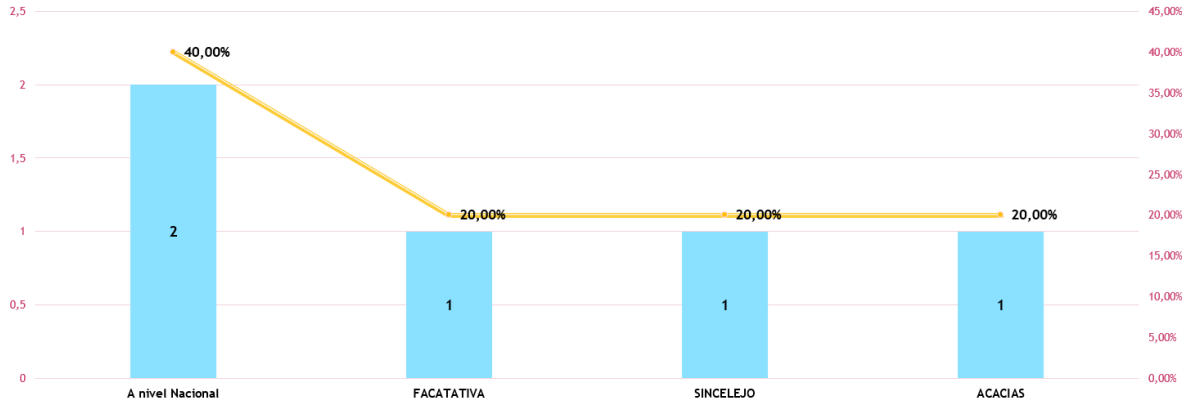


Ilustración 9 eventos por sedes routers

- Por parte del grupo NOC en el mes de diciembre, se evidencia que, de los 5 eventos registrados sobre Switches, las sedes con eventos fueron: a nivel nacional con 2 eventos (40%), Facatativá, Sincelejo y Acacias cada una con 1 evento registrado y representando el 20% de forma individual.

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

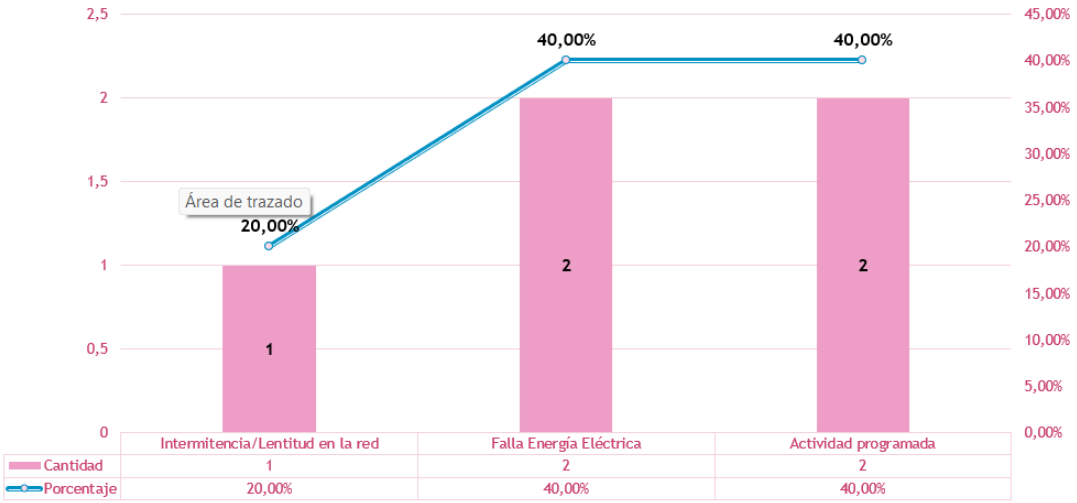


Ilustración 10 Top de causas por sedes switches

- Se listan 3 diferentes causas para la categoría de Switches registradas durante el periodo del mes de diciembre. De los 5 casos (40%) están directamente relacionados con actividad programada en la que se vieron afectadas y se registraron dos eventos a nivel nacional las cuales las 2 fueron por una actividad programada sobre el RFC171778. Las alarmas suben al finalizar la actividad.

- 2 casos (40%) se atribuyen a falla de energía eléctrica, ya que estas alarmas estuvieron activas por un lapso corto y menor a 20 minutos. Estos eventos se presentaron 1 en Sincelejo y 1 Acacias donde el servicio de energía es inestable según lo informado por el personal en sitio.

- El caso restante representa el 20% (1) del total de los casos por Intermitencia/Lentitud en la red el cual tuvo una alarma por un lapso corto de tiempo.

Access Point

Desde el Centro de Operaciones (NOC), durante el mes de diciembre se gestionaron 10 incidentes asociados a equipos de red WLAN – Access Point en distintas sedes a nivel nacional, los cuales representan el 2% 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.

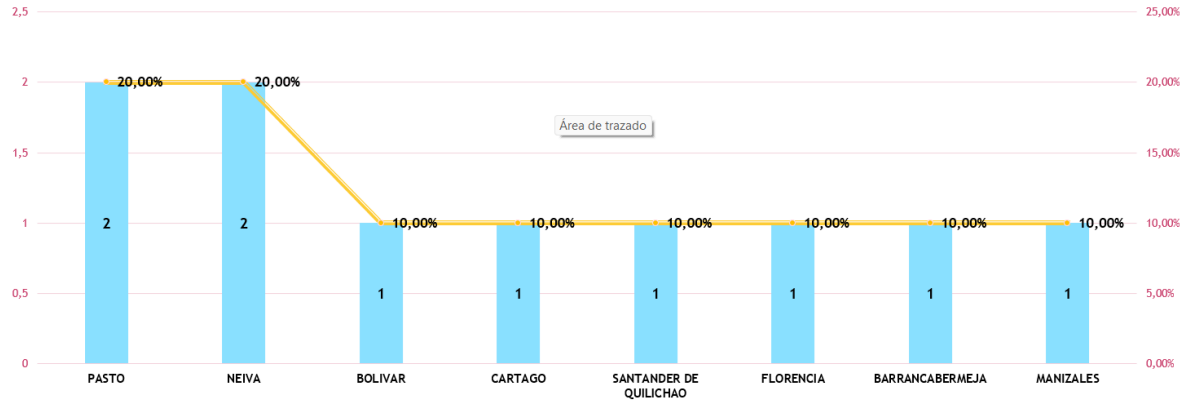


Ilustración 11 Top de eventos por sedes Access Point

- Durante el mes de diciembre se evidencia que las sedes con mayor número de eventos relacionados con Access Point es Pasto y Neiva, las dos igualando con 2 casos cada una que representa el 20,00% cada una del total de los casos, conservando el primer y segundo lugar en el TOP. Causa predominante: falla de energía eléctrica los 4 casos.

- Le sigue Bolivar, Cartago, Santander de Quilichao, Florencia, Barrancabermeja y Manizales cada una con 1 evento registrado, representando el 10.00% de forma individual, Causa: el caso de Bolívar y Manizales por bloqueo de dispositivo, Cartago y Santander de Quilichao por Intermitencia/Lentitud en la red, el caso de Florencia por falla de energía y el caso restante de Barrancabermeja por Desconexión/apagado Físico de Equipos en Sede.

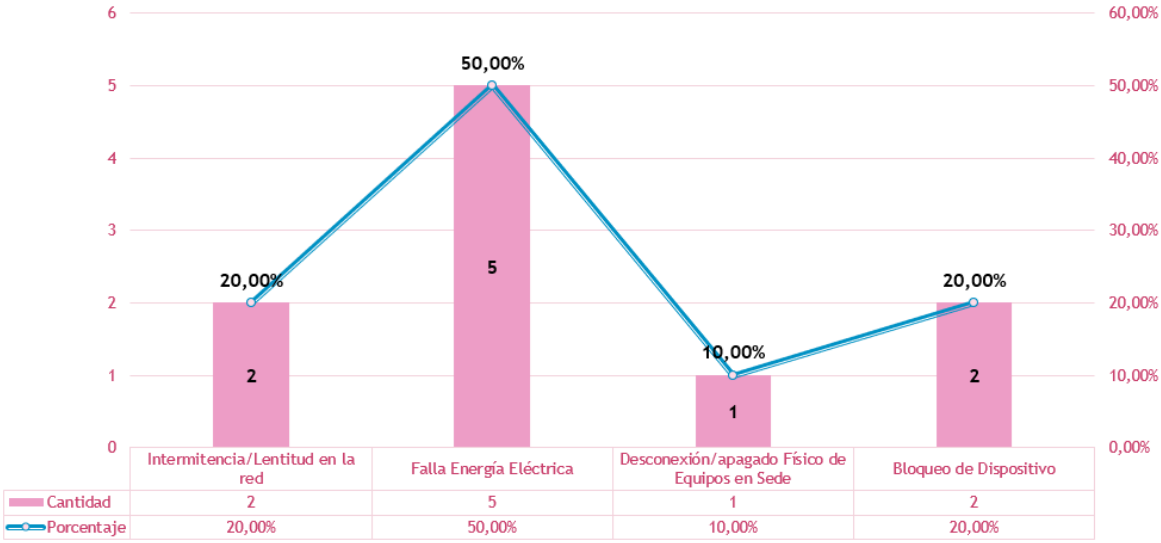


Ilustración 12 13Top de causas por sedes Access point

- Se evidencian 4 causas de fallas para el periodo del mes de diciembre con relación a los dispositivos Access Point.

- El 50% de los incidentes en APs (5 de 10) están directamente relacionados con fallas eléctricas, el 20% (2 de 10) de los incidentes por bloqueo de dispositivo, el 20% (2 de 10) por Intermitencia/Lentitud en la red y el 10% (1 de 10) por Desconexión/apagado Físico de

Equipos en Sede, lo que refuerza la necesidad crítica de implementar UPS en sedes con alta recurrencia.

- Según lo registrado de los 10 eventos generados por Access Point durante el mes de diciembre con relación a los casos suspendidos VS. Casos cerrados, se evidencian los 10 casos en estado cerrado, representando el 100% de gestión de casos para esta categoría.

Starlink

Desde el centro de operaciones NOC durante el mes de diciembre se gestionaron 105 incidentes relacionados con equipos de red Starlink en diferentes sedes a nivel nacional, los cuales representan el 21% del total de los casos.

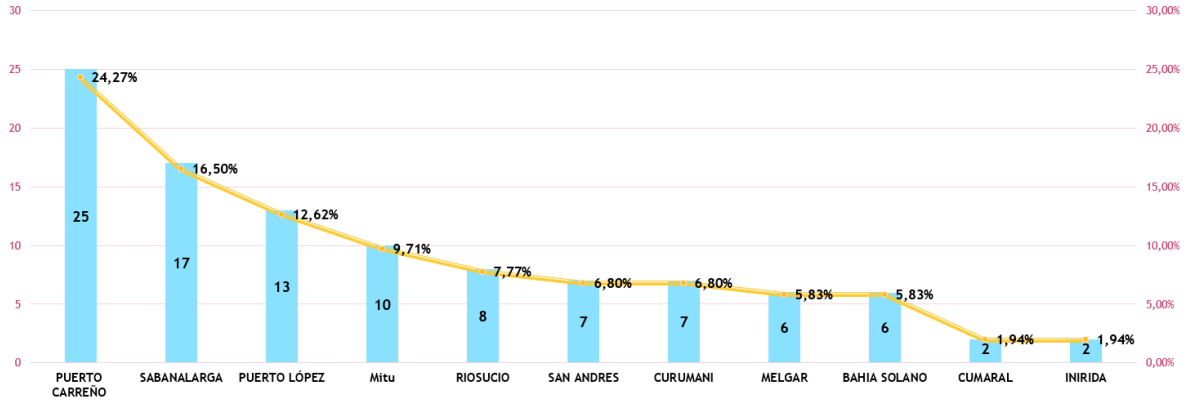


Ilustración 14 Top de eventos por sedes Starlink

- Para el mes de diciembre el TOP 10 de las sedes con mayor número de eventos generados para la categoría de Starlink fueron Puerto Carreño con 25 eventos, representando un 24,27%, la cual puntea en primer lugar. Sabanalarga con 17 eventos representando 16,50 de los casos. Puerto López con 13 evento, representando el 12,62%, Mitú con 10 eventos, representando el 9,71%, Rio Sucio con 8 eventos, representando 7,77%, San Andrés y Curumani igualan con 7 eventos cada una, representando el 6,80% de forma individual, Melgar y Bahía Solano con 6 eventos cada una, representando el 5,83% de forma individual. Por último, Cumaral e Inírida con 2 eventos cada una, representando el 1,94% de los eventos registrados individualmente.

- Las fallas Desconexión/apagado Físico de Equipos en Sede son la causa predominante con 54 casos en la mayoría de las sedes del TOP de equipos Starlink, representando el 51,43% del total de los casos para esta categoría, lo que resalta la necesidad de mejorar la infraestructura local o implementar soluciones autónomas.

- Sin embargo, en este mes Sabanalarga puntea con mayor número de eventos (15 casos) y seguido de Puerto Carreño con 14 eventos relacionados con Desconexión/apagado Físico de Equipos en Sede. Esto por temas de prevención por fluctuaciones constantes en el servicio de energía.

- Falla Energía Eléctrica es la segunda categoría con 29 eventos registrados, representando el 27,62% y por último y en tercer lugar, Intermitencia/Lentitud en la red con

22 eventos, representando el 20,95% del total de los casos, estas ocasionadas por interrupción en el servicio durante pocos minutos sin diagnostico en sitio. Por lo cual se recomienda contemplar la posibilidad de sistemas de respaldos robustos.

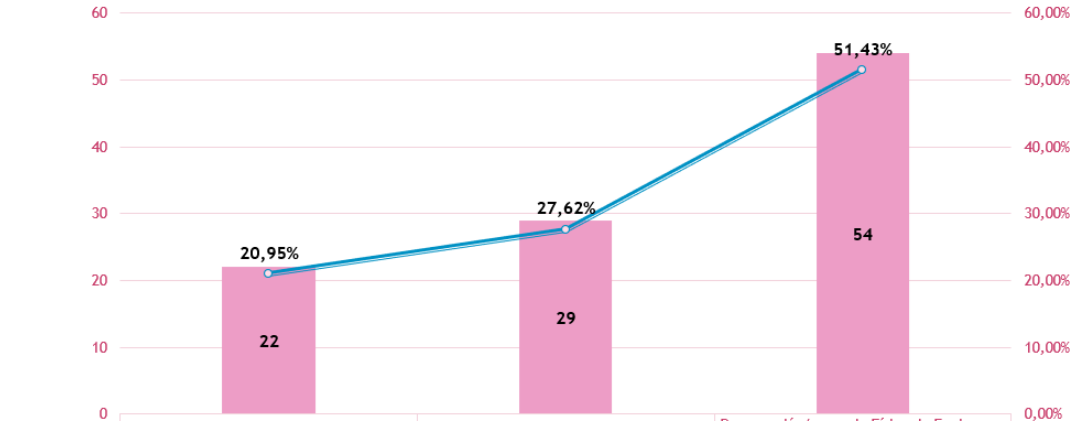


Ilustración 15 Top de causas por sedes Starlink

- Las sedes que puntean con mayor número de eventos por Desconexión/apagado Físico de Equipos en Sede son: Sabana Larga con 15 casos, Puerto Carreño con 14 casos y Puerto López con 13 casos. En estas sedes los funcionarios por falta de mecanismos de protección ante picos de energía prefieren realizar el apagado de los dispositivos.

- Las sedes con mayor número de eventos por Falla Energía Eléctrica son Mitú con 8 casos, Puerto Carreño con 6 casos, San Andrés con 5 casos. Lo que evidencia vulnerabilidad en la infraestructura energética local.

- La sede con mayor número de eventos registrados por Intermitencia/Lentitud en la red es Puerto Carreño y Bahía Solano, evidenciando una inactividad del servicio recurrente en comparación con las demás sedes durante el mes por la misma categoría.

- Durante el mes de diciembre 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 y esto causa mucha intermitencia en los puntos que manejan esta tecnología.

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.

Fortigate

Desde el centro de operaciones NOC durante el mes de diciembre se gestionaron 79 incidentes relacionados con equipos de red FortiGate en diferentes sedes a nivel nacional, los cuales representaron el 16% del total de los casos, ocupando el tercer lugar.

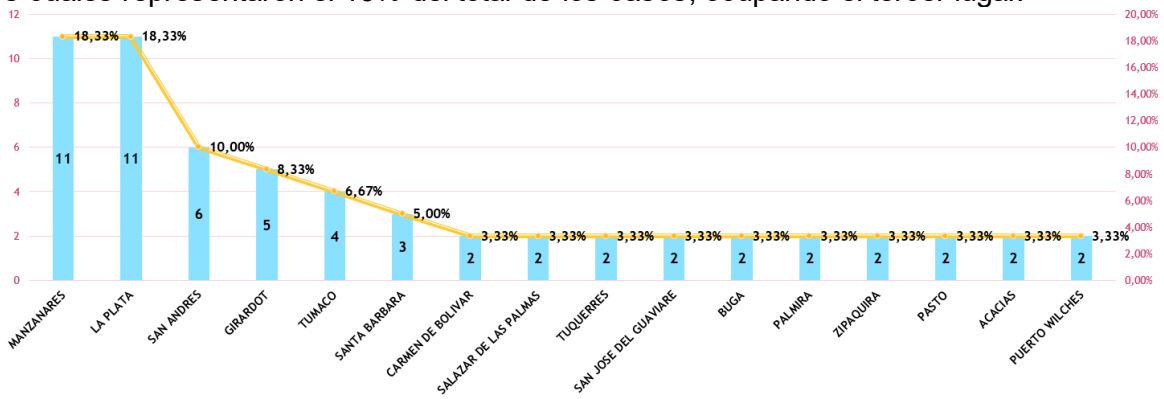


Ilustración 16 Top de incidentes por sedes fortigate

- Durante el análisis del comportamiento de la red SD-WAN en el mes de diciembre, se identificó una mayor frecuencia de afectación en las sedes de Manzanares y La Plata las cuales están ocupando el primer lugar con 18,33% (11) cada una, en tercer lugar esta San Andrés con un 10,00% (6), Girardot registra 5 casos (8,33), Tumaco registra 6,67% con 4 casos, Santa Barbara registra 3 eventos (5,00%) y el resto de sedes (Carmen de Bolívar, Salazar de las Palmas, Tuquerres, San José del Guaviare, Buga, Palmira, Zipaquirá, Pasto, Acacias y Puerto Wilches) presentan una tasa baja cada una (3,33%) de eventos registrados,

- La causa con mayor número de eventos registrados entra Manzanares y La Plata fue Desconexión/apagado Físico de Equipos en Sede con 18 casos, que afectan directamente la disponibilidad de los enlaces SD-WAN ya que los funcionarios desconectan los dispositivos de forma preventiva.

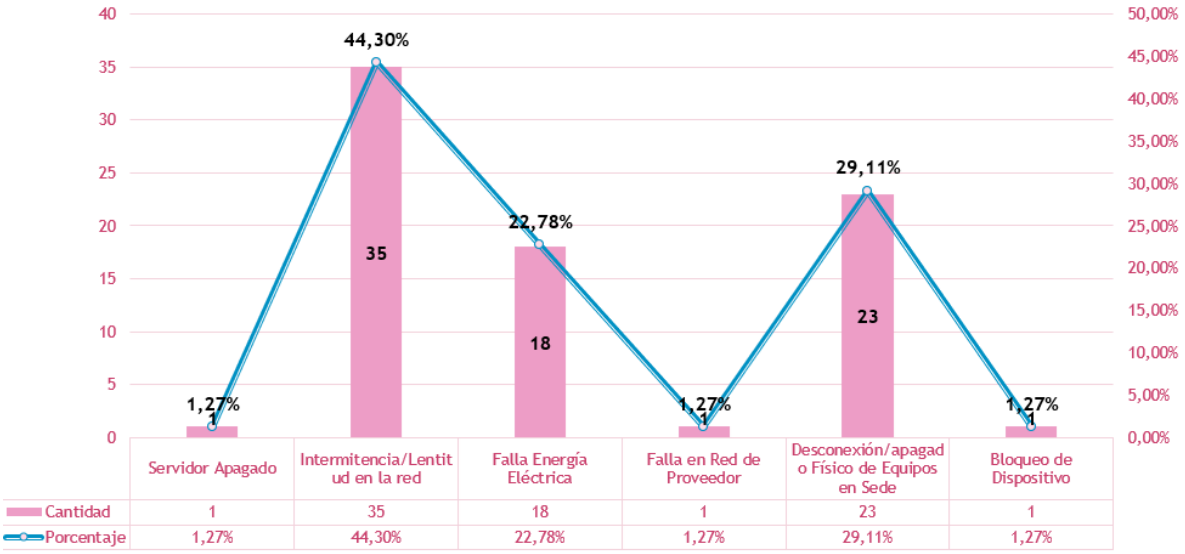


Ilustración 17 Top de causas por sedes fortigate

- Durante el mes de diciembre, los dispositivos SD-WAN presentaron una tasa alta en cuanto a la causa de Intermitencia/Lentitud en la red con 35 eventos registrados, representados con el 44,30% del total de los casos para esta categoría. Estas ocasionadas por condiciones climáticas adversas, validadas por el soporte en sitio y algunas fuera de horario hábil.

- Un 29,11% (23 casos) de las alarmas correspondieron a Desconexión/apagado Físico de Equipos en Sede 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.

- En tercer lugar, tenemos un 22,78% (18 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. Lo anterior resalta la necesidad de adaptar mecanismos de respaldo en la sede con el índice más alto de afectaciones por temas de energía, con el fin de mitigar las interrupciones en la red de datos.

- Por otro lado, el 2,54% (2 casos) de los eventos registrados y sumados en conjunto, durante el mes se atribuyeron a bloqueo de dispositivo y servidor apagado.

De los 79 casos relacionados con los dispositivos SD-WAN, 77 se encuentran a fecha de corte cerrados exitosamente, representando un 97% de resolución operativa dentro del mes por parte del centro de operaciones NOC. Mientras que el 3% (2) de los casos se encuentran en estado suspendido, 1 a espera de validaciones con soporte en sitio y 1 a espera que el proveedor brinde el RFO para proceder con el respectivo cierre.

Casos Escalados a Proveedor de Telecomunicaciones

- Durante el mes de diciembre se registraron 34 casos que fueron escalados y gestionados con proveedor ETB y TIGO de los cuales quedan 29 (85%) que registran en estado solucionado o cerrado y 5 (15%) en estado suspendido o en espera de RFO.

Servicios Centrales

Servidores Windows

Durante diciembre, el Centro de Operaciones de Red (NOC) gestionó 51 incidentes asociados a servidores Windows, equivalentes al 10% del total de casos registrados durante el mes.

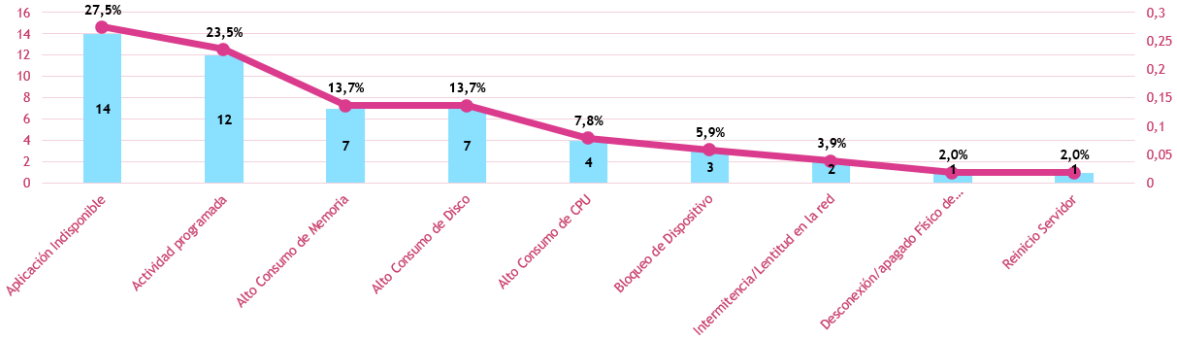


Ilustración 18 Top de eventos Windows

Se evidencia que para el mes de diciembre el mayor número de eventos se presentaron por alto consumo de las máquinas virtuales de aplicaciones de SQL Server , gestor documental, SQL productivo, aplicaciones .NET que normalmente tienen mucho tráfico, así como, actividades de parchado de máquinas relacionadas con SQL Server gestionadas a través de la práctica ITIL de habilitación de cambios con 14 eventos registrados y representando el 27,5%, seguido por actividad programada con 12 eventos registrados, representando el 23,5% y en tercer y cuarto lugar tenemos a alto consumo de memoria y alto consumo de disco cada una con 7 eventos, representando 13,7% de forma individual. Para este mes el consumo en disco y memoria bajan a tercero y cuarto lugar después de encabezar la gráfica en el mes pasado.
Otros factores como consumo de CPU, bloqueo de dispositivo, intermitencia/lentitud en la red, desconexión/apagado de equipos en sede y reinicio servidor representan una baja tasa y que sumados representan el 21,6% de los casos.

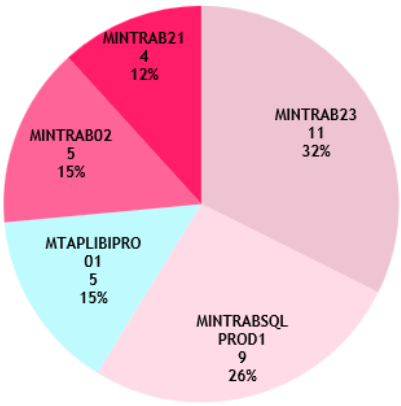


Ilustración 19 Top de servidores Windows

El servidor MINTRAB23 para este mes representan el 32% (11 casos) del total de los casos para esta categoría, se reporta que en su mayoría los casos están relacionados por alto consumo de las máquinas virtuales de aplicaciones de SQL Server como SIRITI,SFT, FTRUTEC, cobro, Tesorería, entre otras, el servidor MINTRABSQLPROD1 representa el 26% (9 casos) todos relacionados a actividad programada, Los servidores MINTRAB02 y MTAPLIBIPRO01 cada uno registra 5 eventos, representando el 15% de forma individual.
Estas VM están relacionadas a parchados realizados durante el mes de diciembre, 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 demas sonservidores de alto consumo, gestor documental, SQL productivo, aplicaciones .NET que normalmente tienen mucho trafico

Los 5 eventos del servidor MINTRAB02 están relacionados a alto consumo de memoria y los 5 casos del servidor MTAPLIBIPRO01 están relacionados a consumo de las máquinas virtuales de aplicaciones de SQL Server. El servidor MINTRAB21 registro 4 eventos y representa el 12%, de los cuales 3 esta relacionados a consumo de CPU y 1 por consumo de disco.
Se evidencia que de los 51 eventos registrados durante el mes de diciembre, quedan 50 eventos en estado cerrado y solucionado, 1 en estado suspendido y escalados al especialista a cargo. Lo cual refleja una efectiva y oportuna gestión por parte de los especialistas con los eventos reportados, reflejando un porcentaje del 98% de gestión de los casos.
Se realiza el respetivo seguimiento a los casos que se encuentra abiertos y se resuma que:

- Caso en Aranda RF-174833, está relacionado al servidor MTSGRLBDSQL por alto consumo de memoria, este caso se encuentra en suspendido y a espera de validaciones por parte del especialista. Información con corte al cierre de diciembre

Servidores Linux

Durante diciembre, el Centro de Operaciones de Red (NOC) gestionó 4 incidentes asociados a servidores Linux, equivalentes al 1% del total de casos registrados en el mes.

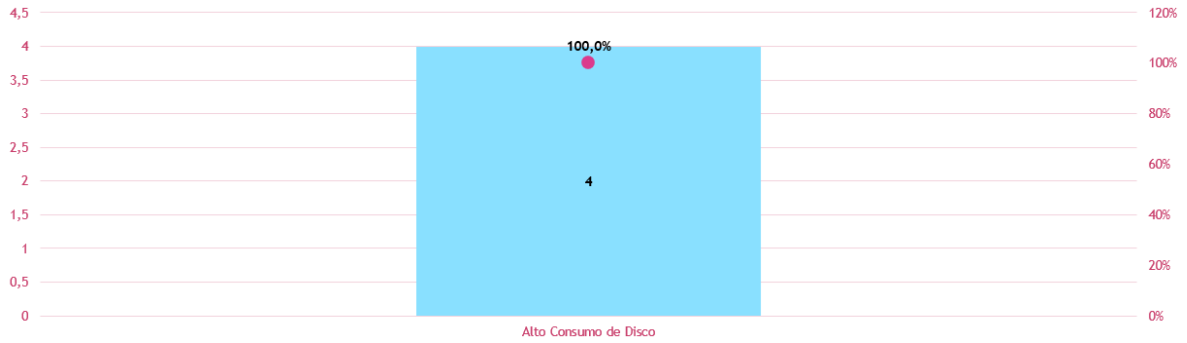


Ilustración 20 Top de causas eventos linux

La causa principal de los eventos registrados muestra que todos están asociadas a factores conocidos y potencialmente controlables. El alto consumo de disco representando un 100% ya que los 4 eventos son por esta causa.

Para este mes se observa que los 4 casos reportados tienen un solo servidor relacionado, por lo tanto, es el único servidor en la gráfica. Todos los eventos se presentaron por alto consumo de disco.

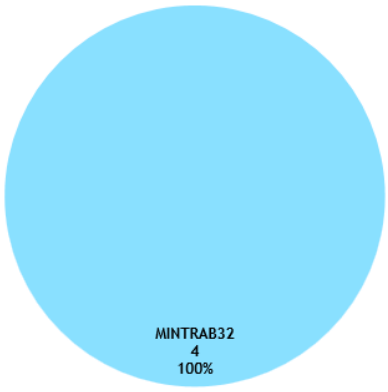
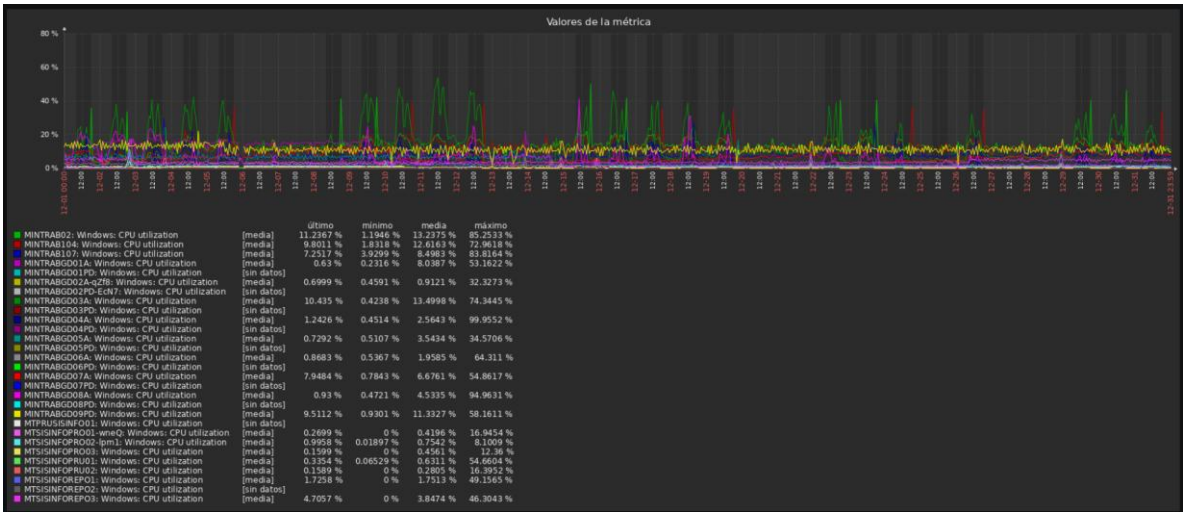


Ilustración 21 Top de servidores linux

De los 4 eventos registrados para la categoría de servidores Linux durante el mes de diciembre, los 4 registran como cerrados, representando el 100% de los casos gestionados por parte de los especialistas a cargo.

Gráficas de CPU Zabbix de todo el mes sobre servidores



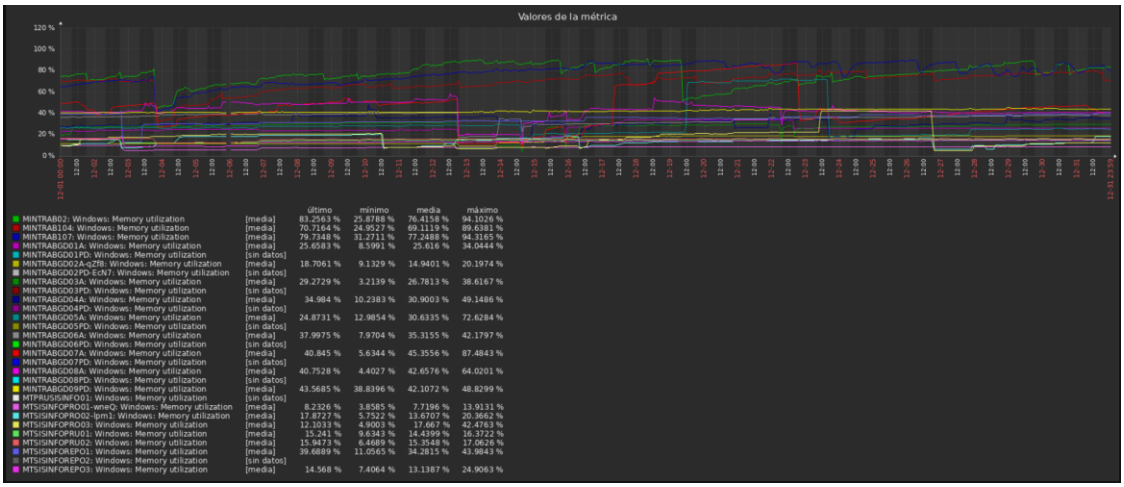
A continuación, se relaciona el TOP 5 de los servidores que por media tuvieron más utilización de recursos de CPU durante el mes.

CPU

1. MINTRABGD03A 13.4998%
2. MINTRAB02 13.2375%
3. MINTRAB104 12.6163%
4. MINTRABGD09PD 11.3327%

5. MINTRAB107 8.4983%

Gráfica de MEMORIA Zabbix de todo el mes sobre 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

1. MINTRAB107 77.2488%
2. MINTRAB02 76.4158%
3. MINTRAB104 69.1119%
4. MINTRABGD07A 45.3556%
5. MINTRABGD08A 42.6576%

Datacenter (Cali - Bogotá)

Durante el mes de diciembre se evidencia 1 evento relacionado al CXV-SWCORE1-RAT42-U44-8360, sin embargo, según la documentación suministrada por el Ing en Redes, se menciona que por ejecución de actividad sobre el RFC-171778 se realizó apagado del Switch Core1 para validar la disponibilidad del servicio bajo la operación del Switch Core2 en el proceso de sincronización de sesiones, una vez lograda la sincronización las alarmas subieron con lo cual se procedió a realizar el rollback.

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 diciembre de 2025.

Servidores

Cantidad de dispositivos	Disponibilidad consolidada
115	100%

Tabla 17 Consolidado disponibilidad de servidores

Directorio Activo

Cantidad de dispositivos	Disponibilidad consolidada
3	100,00%

Tabla 18 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 19 Desagregado de Disponibilidad Directorio Activo

Datacenter Principal

Cantidad de dispositivos	Disponibilidad consolidada
8	100,00%

Tabla 20 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-HUB02	100,00%

Tabla 21 Desagregado de Disponibilidad Datacenter Principal

Datacenter Alterno

Cantidad de dispositivos	Disponibilidad consolidada
4	100%

Tabla 22 Consolidado disponibilidad de equipos Datacenter alterno

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

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

Tabla 23 Desagregado Disponibilidad de equipos Datacenter alterno

Redes y conectividad

Cantidad de dispositivos	Disponibilidad consolidada
507	98,66%

Tabla 24 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 25 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 26 Disponibilidad de equipos Seguridad de la Información

Telefonía

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

Tabla 27 Consolidado disponibilidad de equipos de telefonía

Antivirus

Cantidad de dispositivos	Disponibilidad consolidada
1	100%

Tabla 28 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.
- El 18/12/2025 se ejecutaron las pruebas de DRP (Pruebas de recuperación ante desastres para bases de datos con Log Shipping), las cuales fueron exitosas y sin novedades por parte del equipo de infraestructura.
- Se presenta en la siguiente gráfica el seguimiento de la planeación y ejecución del calendario de pruebas de alta disponibilidad de los servicios e infraestructura, se programó realizar 33 pruebas de alta disponibilidad, de las cuales todas han sido cerradas durante el 2025 por los servicios de los servicios Conectividad, Seguridad de la Información y Telefonía IP, se encuentran ejecutadas y aprobadas en los CAB.

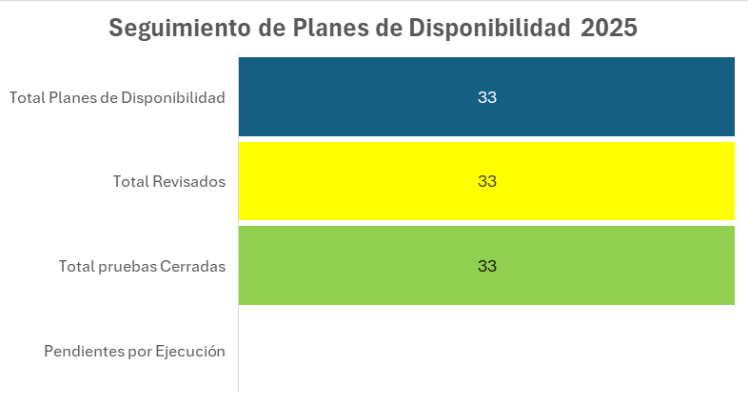


Ilustración 22 Seguimiento Pruebas de Disponibilidad

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 diciembre de 2025.

Actividades en curso:

Revisión de los RFC ejecutados durante el periodo, para los cuales (22) cambios fueron aprobados su cierre, ya que cuentan con las evidencias completas de los planes de Pruebas

Previas y Posteriores, al corte del 31/12/2025 se encuentra (5) casos abiertos (en proceso de revisión) a la espera de entrega de las evidencias por parte los especialistas.

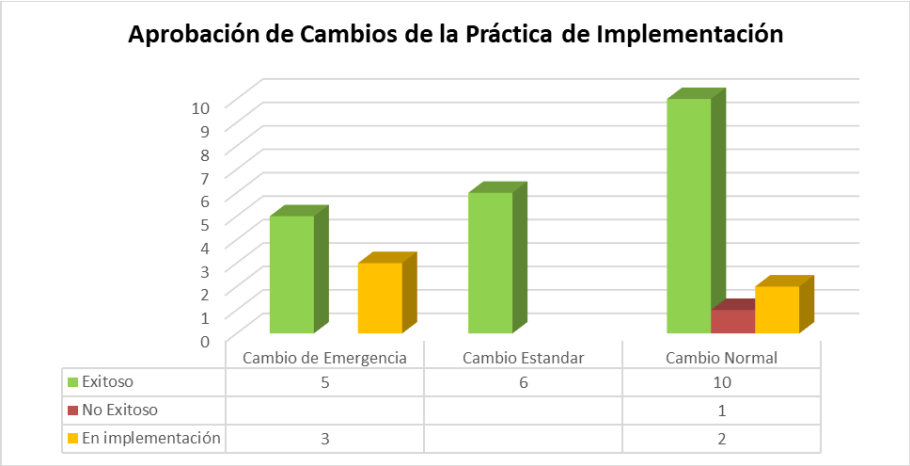


Ilustración 23 Seguimiento Práctica Implementación

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

Seguimiento%20de%20cambios%20Impler

2.2 Mesa de Servicios y Soporte en Sitio

A continuación, se presenta la gestión desarrollada durante el mes de diciembre 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 diciembre, a la MDS ingresaron 309 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	201	199	196	2	1	1
COL - Mintrabajo-Gestor-documental	61	60	60	1	1	0
COL - Mintrabajo-office365	25	25	25	0	0	0
COL - mintrabajo-Impresora	22	22	22	0	0	0
TOTAL	309	306	303	3	2	1

Tabla 29 Llamadas Atendida por la Mesa de Servicio

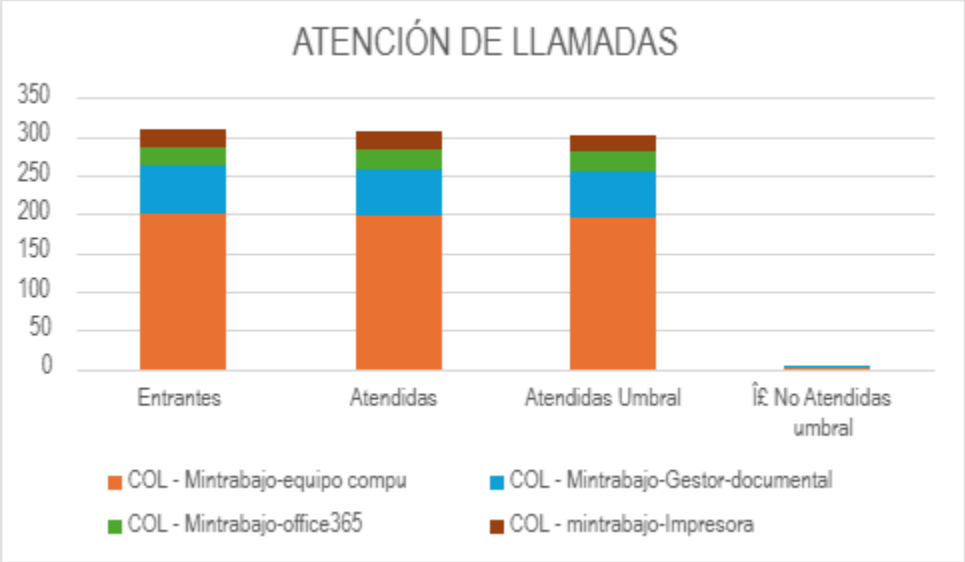


Ilustración 24 Llamadas Atendidas

El servicio más solicitado a través de la atención de llamadas es: Equipo de cómputo con 201 llamadas entrantes, se atendieron 199 solicitudes se observan: 3 llamadas no atendidas, 2 llamadas Abandonadas antes de los 20 segundos y 1 no atendida.

- **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_DICIEMBRE.xlsx pestaña *categoría.*

- **Análisis de Casos Anulados por Servicio**

Para este periodo se tiene 5 casos anulados de los siguientes servicios:

CASOS ANULADOS	TOTAL
Herramientas de Gestión	2
Seguridad informática	1
Administración de servidores	1
Aplicaciones Especializadas	1
Total general	**5**

Tabla 30 Casos anulados por Servicio

- **Herramientas de Gestión:** se tienen 2 casos de Reporte de falla de monitoreo Zabbix.
- **Seguridad Informática:** se tiene 1 caso de acceso a la fuerza.
- **Administración de Servidores:** se tiene 1 caso de Radicar un cambio.
- **Aplicaciones Especializadas:** se tiene 1 caso de radicar un problema.

En comparación del mes anterior se evidenció un aumento del 60%, que corresponde a 3 casos.

- **Análisis de Casos Suspendidos por Servicio**

Para el periodo del mes de diciembre, se dio una disminución de casos suspendidos del 51,6% que corresponde a 47 casos para un total de este mes de 44 casos de los siguientes servicios:

CASOS SUSPENDIDOS	TOTAL
Soporte Microinformática	17
Redes y Conectividad	15
Administración de servidores	4
Aplicaciones Especializadas	3
Seguridad informática	3
Total general	**42**

Tabla 31 Casos Suspendidos por Servicio

- **Soporte Microinformática:** 17 casos suspendidos debido a que se ha solicitado información complementaria a los usuarios o están pendientes por disponibilidad del usuario: Equipos de escritorio, Equipo periférico, Equipo Portátil 3 casos para cada categoría, Backup 2 casos y Asesoría – Consulta, atasco, Asignación de equipo (portátil o pc) borrado seguro, daño físico, equipo impresora con 1 caso cada categoría.

- **Redes y Conectividad:** 15 casos suspendidos debido a: Router con 8 casos, Starlink 5 casos y FortiGate 2 casos.
- **Administración de servidores**: 4 casos suspendidos por: Configuración MFA con 2 casos, Inactivar usuario y Servidor Windows 1 caso para cada categoría.
- **Aplicaciones Especializadas:** 3 casos suspendidos debido a: Asesoría-consulta, Depuración de bandeja y Relanzamiento 1 caso de cada categoría.
- **Seguridad informática:** 3 casos suspendidos: Permitir accesos, Análisis de evento y Ajuste Proxy 1 casos de 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 no quedaron incidentes en estado solucionado.

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

Requerimientos solucionados por la Mesa de Servicios: en el mes de diciembre quedaron 34 requerimientos discriminados de la siguiente manera:

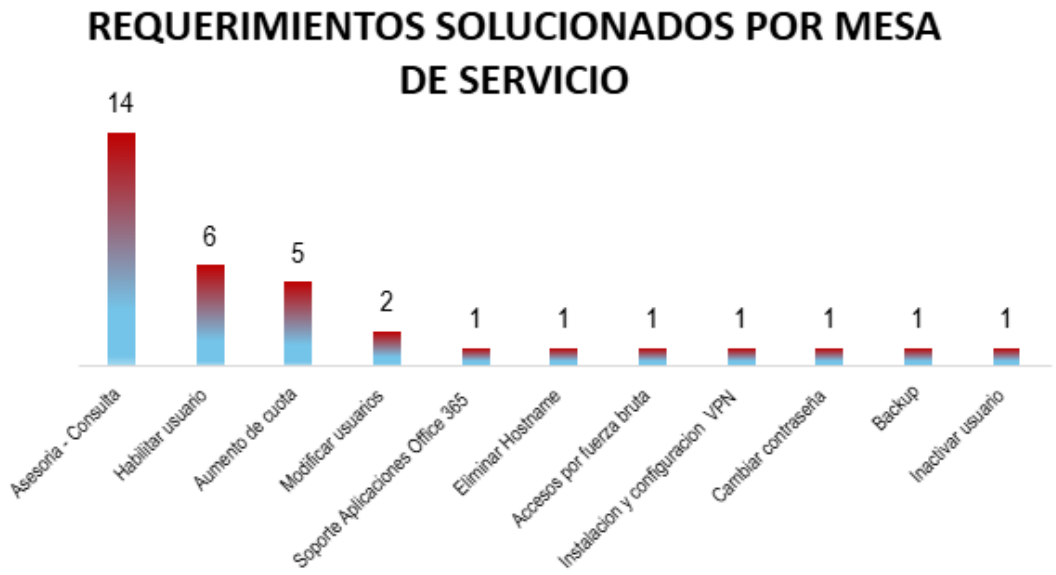


Ilustración 25 Requerimientos Solucionados por Mesa de Servicios

Requerimientos solucionados por Soporte en sitio Bogotá: en el mes de diciembre quedaron 13 requerimientos discriminados de la siguiente manera:



Ilustración 26 Requerimientos Solucionados por Soporte en Sitio

Requerimientos solucionados por Soportes Territoriales: Para el mes de diciembre quedaron 78 casos en estado solucionado de las territoriales.



Ilustración 27 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 diciembre se cerraron 1025 casos, discriminados así: Aumento de cuota con 366, Asesoría – Consulta con 262 casos, Cambiar contraseña con 145 casos, Creación de usuario 58 casos, Backup 46 casos, cambio de grupo 23 casos, Habilitar usuario 18 casos, Inactivar usuario con 15 casos, Elaborar reporte 13 e instalación y configuración VPN con 9 casos.

En comparación del mes anterior se nota un aumento de casos cerrados por la mesa de un 3% que es equivalente a 30 casos.

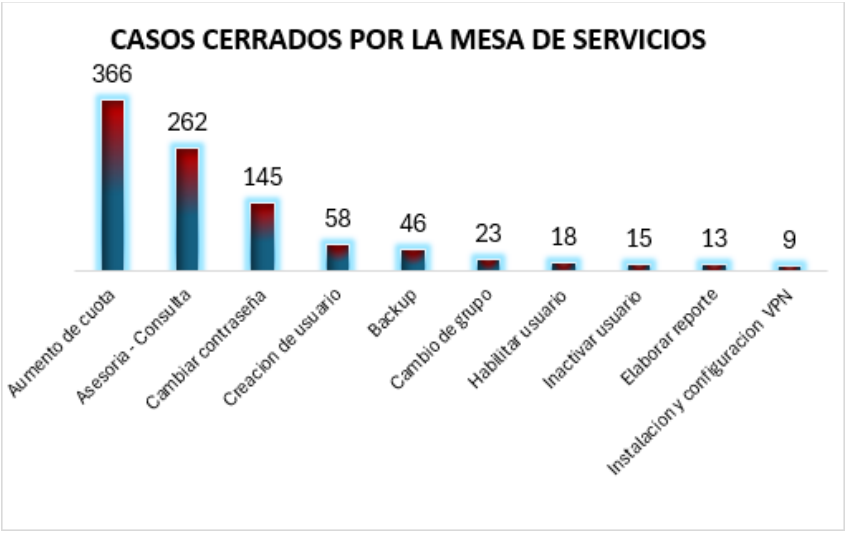


Ilustración 28 Requerimientos Solucionados por la Mesa de Servicios

Casos Cerrados por Soporte en Sitio: Se indica el top 10 de Requerimientos cerrados por soporte en sitio, para el mes de diciembre se cerraron 1343 casos discriminados así: Cargue de papel en impresora con 380 casos, Instalación - Configuración con 224 casos, Asesoría - Consulta con 154 casos, Configuración con 106 casos, Soporte Aplicaciones Office 365 con 57 casos, Préstamo 50 casos, Devolución de equipo (portátil o PC) 44 casos, Solicitud Backup 37 casos, Mantenimiento preventivo 36 casos e instalación y configuración VPN 30 casos.
169 casos en comparación con el mes anterior se tiene una disminución del 11,17% que corresponde a 169 casos.

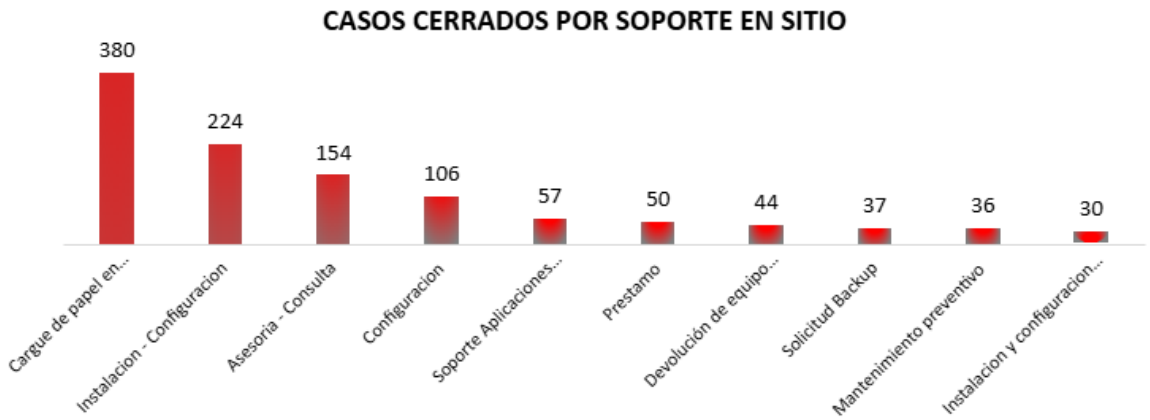


Ilustración 29 Casos Cerrados por Soporte en Sitio

Casos Cerrados por soporte en sitio Territoriales: Se indica el top 10 de Requerimientos cerrados por soporte en Territorio, para el mes de diciembre se cerraron 1542 casos discriminados así: Instalación - Configuración con 324 casos, Asesoría – Consulta con 230 casos, Cargue de papel en impresora con 211 casos, Mantenimiento preventivo con 126 casos, Configuración con 88 casos, Asesoría PDF con 71 casos, Asesoría Excel con 64 casos, Actualización BIOS con 63 casos, Copia de información y Asesoría Word 46 casos para cada categoría

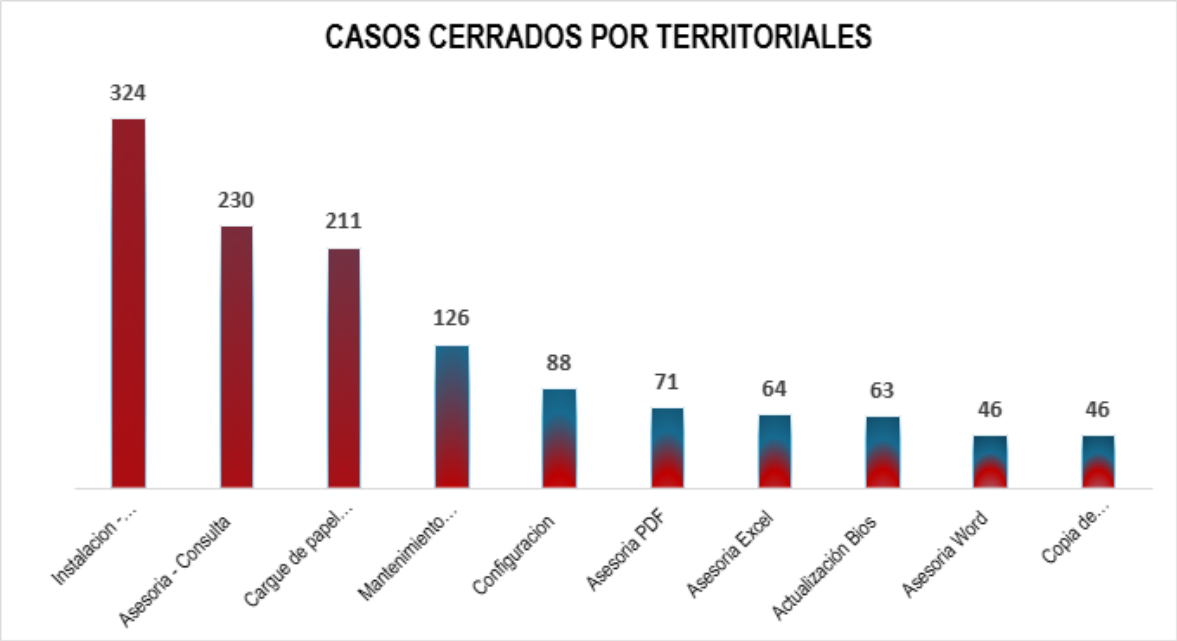


Ilustración 30 Casos Cerrados por Territoriales

- **Casos Atendidos a Usuarios VIPS**

Durante este periodo se crearon 65 solicitudes para ser atendidas por soporte en sitio, para VIPS discriminados a continuación por tipo de caso:

TIPO DE CASO_VIPS	CUMPLIMIENTO	NO_CUMPLE	TOTAL
Incidente	4	0	4
Requerimiento	61	0	61
Total general	**65**	**0**	**65**

Tabla 32 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	26	0	26
Requerimientos	1273	0	1276
Total general	**1299**	**0**	**1299**

Tabla 33 Casos Atendidos usuarios

- **Medio de Ingreso de Casos**

Durante el período ingresaron a la mesa de servicio 5758 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	2915
Correo SoporteMT	1550
Alarma Zabbix	954
Telefónico	275
Alarma Fortisiem	59
Portal Auto-Gestión	3
Case Creator Mesa de Servicios	2
Total general	**5758**

Tabla 34 Medios de Ingreso de Casos

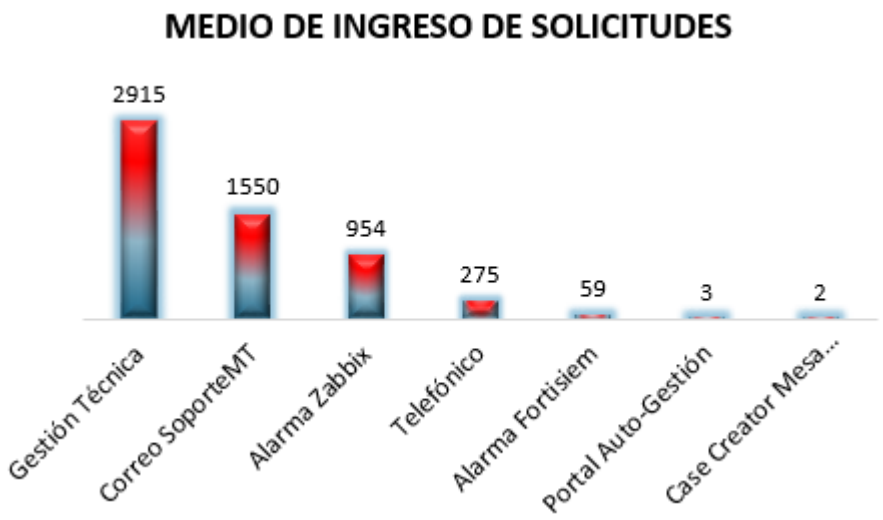


Ilustración 31 *Medio de ingreso solicitudes*

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**

Durante el mes de diciembre se continuó en espera del lineamiento para continuar con la organización, actualización del directorio activo para Nivel Central y Territoriales, esta información fue entrega a la supervisión para solicitar la inactivación de esos usuarios y liberar las licencias.

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

Se continua con el despliegue de actualización de interfaz de las impresoras Ricoh en sedes territoriales e inspecciones.

Se continúan los mantenimientos de las impresoras tanto en sede central como en las territoriales, con un avance del 20%, está actividad se continuará para el mes de enero.

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

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

Durante el mes de diciembre de 2025 los profesionales de soporte en sitio territoriales llevaron a cabo las siguientes acciones:

29 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 1662 casos, dentro de los que se destacan: Instalaciones - Configuraciones sobre aplicaciones de la línea base de software, Cargues de Papel en las impresoras de las diferentes Sedes, Asesorías – Consultas, Mantenimiento de Impresoras, Configuración de drivers, Asesorías en PDF, Asesoría Excel, Actualización de BIOS, Asesoría Word y Copia de información

Instalación de antenas Starlink requeridas por los especialistas de redes y conectividad

Se continua el proceso de mantenimiento de las impresoras que se encuentran en las inspecciones cercanas a las sedes territoriales a nivel nacional

- **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, atención de incidencias, mantenimientos y actividades masivas.

Mes	Territorial	Sede	Servicio	Descripción	Caso
Dic-25	Tolima	Espinal	Organización cableado redes y conexiones	El cableado esta mal ordenado dando una mala presentación a la oficina, se procede a ordenar tomas eléctricas y cableado mal ordenado, queda con una mejor presentación en cuanto a percepción, usuario	RF-168938

Mes	Territorial	Sede	Servicio	Descripción	Caso
				queda conforme con actividad realizada.	
Dic-25	Boyaca	Chiquinquirá	Configurar impresora con la nueva interfaz	Se configura la impresora RICOH por actualización de software de impresión.	RF-168997 RF-169003 RF-169004 RF-169005
Dic-25	Norte de Santander	Los Patios	Configurar impresora con la nueva interfaz	Se desinstala la impresora RICOH-LOSPATIOS-INS, se fuerzan políticas, se limpian archivos temporales, se reinstala la impresora, se actualiza el controlador disponible desde el servidor de impresión, se configura como predeterminada, se valida con la funcionaria el ingreso con su PIN asignado, se realizan pruebas correctamente, impresora queda operativa	RF-169874 RF-169877 RF-169879 RF-169883 RF-169889 RF-169952
Dic-25	Caqueta	Doncello	Instalar antena Starlink	Instalación de la antena starlink y comprobación de su correcto funcionamiento	RF-170392 RF-170395 RF-170397 RF-1703

Mes	Territorial	Sede	Servicio	Descripción	Caso
					98 RF-170394 RF-170400
Dic-25	Nariño	Ipiales	Revisión y mantenimiento completo de la impresora	Se realiza el mantenimiento de la la impresora RICOH así como la validaciónde la actualización de su software y la interfaz	RF-171375 RF-171104 RF-171122 RF-171110
Dic-25	Nariño	Tuquerres	Revisión y mantenimiento completo de la impresora	Se realiza el mantenimiento de la la impresora RICOH así como la validaciónde la actualización de su software y la interfaz	RF-170917 RF-171129
Dic-25	Apartadó	Turbo	Se requiere realizar la reinstalación completa de la impresora y el mantenimiento de la misma	Se realiza desplazamiento de soporte en sitio para reinstalar la impresora y comprobar el correcto funcionamiento de la misma en los equipos de cómputo.	RF-168828
Dic-25	Cordoba	Cereté	Revisión y mantenimiento completo de la impresora	Se realiza el mantenimiento de la la impresora RICOH así como la validaciónde la actualización de su software y la interfaz	RF-170721, RF-170720, RF-170719, RF-170575
Dic-25	Cordoba	Lorica	Revisión y mantenimiento completo de la impresora	apagado y aseguramiento del equipo, limpieza externa de la carcasa, apertura del	RF-172542- RF-172612

Mes	Territorial	Sede	Servicio	Descripción	Caso
				módulo interno, retiro de residuos de papel y acumulación de tóner, así como la limpieza de rodillos d	
Dic-25	Boyacá	Duitama	Revisión y mantenimiento completo de la impresora	Se realiza mantenimiento preventivo de impresora RICOH-DUITAMA. Se adjunta acta de mantenimiento y registro fotográfico del antes y después del mantenimiento.	RF-171779, RF-171781, RF-171783, RF-171784, RF-171788, RF-171792 RF-171794
Dic-25	Boyacá	Sogamoso	Revisión y mantenimiento completo de la impresora	Se realiza mantenimiento preventivo de impresora RICOH-SOGAMOSO. Se adjunta acta de mantenimiento y registro fotográfico del antes y después del mantenimiento.	RF-171779, RF-171781, RF-171783, RF-171784, RF-171788, RF-171792 RF-171794
Dic-25	Atlántico	Baranoa	Revisión y mantenimiento completo de la impresora	Se procede a realizar mantenimiento preventivo de la impresora indicada, limpieza de rodillos, cubiertas, bandejas, unidades fusora y de imagen,	RF-171825, RF-171826

Mes	Territorial	Sede	Servicio	Descripción	Caso
				limpieza de cristal y en general. Se hacen pruebas de impresión y escaner y se valida que queda operativa.	
Dic-25	Valle	Buga	Internet lento	Se deja constancia de que la falla reportada como "internet lento" en la sede de Buga corresponde realmente a una intermitencia en la plataforma Gestor Documental alojada en el Ministerio del Trabajo. El caso se cierra con la validación de que el servicio de internet funciona correctamente y con la aplicación de medidas locales de limpieza y optimización en los equipos.	RF-173054
Dic-25	Valle	Palmira	Internet presenta problemas	Tras la intervención, el servicio de internet quedó funcionando con normalidad, restableciendo la conectividad de los equipos institucionales. El caso se cierra con	IM-171998

Mes	Territorial	Sede	Servicio	Descripción	Caso
				solución efectiva y trazabilidad documentada.	
Dic-25	Cundinamarca	Tocancipá	Equipo portátil no funciona	Se informa al funcionario sobre el estado del dispositivo y se indica realizar la conexión del equipo a una fuente de energía para su carga.	RF-172815
Dic-25	Chocó	Istmina	Configurar impresora con la nueva interfaz	Se procedió a desinstalar y reinstalar correctamente la impresora en el equipo debido a la nueva actualización de la interfaz. Después de realizar las pruebas de impresión y verificación correspondientes, se confirma que la impresora queda funcionando correctamente en el equipo.	RF-173416 RF-173452 RF-173458
Dic-25	Norte de Santander	Salazar	Mantenimiento preventivo impresora	Me desplazo a la inspección de Salazar de las Palmas y realizó mantenimiento preventivo a la impresora Ricoh IM430, serial 3353PA50551, consistente en limpieza externa e interna, ajuste de rodillos y verificación	RF-173484 RF-173485 RF-173486 RF-173487 RF-173488 RF-173489 RF-173490

Mes	Territorial	Sede	Servicio	Descripción	Caso
				del fusor. Se efectuaron pruebas de impresión y el equipo quedó funcionando correctamente.	RF-1734 92 RF-1734 93 RF-1734 95 RF-1734 96
Dic-25	Bolívar	Carmen de Bolivar	Mantenimiento preventivo impresora Ricoh-Carmen-de-Bolivar	Posteriormente, se realizaron pruebas de funcionamiento después del mantenimiento, las cuales resultaron satisfactorias. Adicionalmente, se llevó a cabo la actualización de la nueva interfaz de PaperCut para impresión. La impresora queda operativa.	RF-1742 72 RF-1742 74 RF-1743 31
Dic-25	Cúcuta	Pamplona	Office 365	Se le indica a la funcionaria como realizar cambio de contraseña, cambio exitoso, enseguida se le indica en que aplicaciones debe actualizarla, confirmando envió y recepción de correo y acceso a las plataformas institucionales	RF-1747 62 RF-1747 64 RF-1747 65 RF-1747 67 RF-1747 80 RF-1747 81 RF-1747 82 RF-1747 83 RF-1747 86

Mes	Territorial	Sede	Servicio	Descripción	Caso
Dic-25	Cúcuta	Chinácota	ACTUALIZACIÓN INTERFAZ IMPRESORA.	Después de que el especialista de impresión realizo la actualización a papercut en la impresora de la inspección de Pamplona, se procede a asesorar a cada funcionario, en los procesos de imprimir, escanear y copiar, todo funciona correctamente.	RF-174673 RF-174675 RF-174677 RF-174682 RF-174689 RF-174690 RF-174692 RF-174693 RF-174756
Dic-25	Cordoba	Planeta Rica	Optimalización del S.O para mejorar el rendimiento de la maquina	Se realiza optimización del sistema operativo del equipo asignado al funcionario Jaider Luis Cogollo Llorente, con el objetivo de mejorar el rendimiento, estabilidad y tiempos de respuesta del equipo. Las actividades efectuadas incluyen verificación y control de procesos en segundo plano, deshabilitación de programas innecesarios al inicio, liberación de espacio en disco, eliminación de archivos temporales, aplicaciónde	RF-174380 RF-174375 RF-174364 RF-174363 RF-174284

Mes	Territorial	Sede	Servicio	Descripción	Caso
				actualizaciones del sistema operativo,	
Dic-25	Cundinamarca	Cáqueza	Funcionaria requiere soporte en sitio debido que manifiesta que el internet le está presentando mucha intermitencia al abrir las páginas corporativas	Se realizo visita tecnica a la inspeccion para validar la falla que manifiesta la funcionaria con el servicio de internet de los cuales se realizan las validacion con el area de comunicaciones de los cuales se evidencia que el internet en donde esta ubicada la funcionaria es de la alcaldia de los cuales tiene caidas constantes con un canal de los cuales se le informa al personal de sistemas de la alcaldia para que corrijan la falla y nuestros equipos de comunicacion queden operativos.	RF-175361
Dic-25	Tolima	Mariquita	Mantenimiento preventivo de la impresora Ricoh	Se realiza mantenimiento preventivo, Limpieza y validaciónde uso de los consumibles (Unidad fusora, unidad de imagen, rodillos arrastre de papel y rodillos de escáner), se	RF-175164 RF-175165 RF-175166 RF-175171

Mes					Territorial	Sede	Servicio	Descripción	Caso
								hace limpieza a cristales de cama plana y ADF, limpieza de bandejas de papel, limpieza interna y externa de tapas laterales, se realiza prueba de impresión, copia y escáner sin novedad	
Dic-25					Tolima	Melgar	Configuración cola de impresión	Se procede a desinstalar cola de impresión, se abren los servicio del PC, se busca el servicio de cola de impresión y se reinicia, se realiza nuevamente la instalación y se deja predetermin ada, se procede con prueba de impresión, esta funcionando sin novedad.	RF-174255 RF-174262 RF-174266 RF-174288 RF-174252
Dic-25					Meta	Puerto Gaitán	Creación de Pin de Impresión	Después de que el especialista de impresión realizo la actualización a papercut en la impresora de la inspección, se realiza pruebas con el nuevo pin de impresión con el perfil de la funcionaria con resultado exitoso	RF-175103
		Dosquebr adas	Mantenimi ento	Se realiza mantenimi			RF-171036 RF-171039		

Mes					Territorial	Sede	Servicio	Descripción	Caso
Dic-25	Pereira		preventivo de la impresora Ricoh	ento preventivo, Limpieza y validación de uso de los consumibles (Unidad fusora, unidad de imagen, rodillos arrastre de papel y rodillos de escáner), se hace limpieza a cristales de cama plana y ADF, limpieza de bandejas de papel, pruebas funcionales correctas.					
Dic-25	Pereira	Santa Rosa de cabal	Mantenimiento preventivo de la impresora Ricoh	Se realiza mantenimiento preventivo, Limpieza y validación de uso de los consumibles (Unidad fusora, unidad de imagen, rodillos arrastre de papel y rodillos de escáner), se hace limpieza a cristales de cama plana y ADF, limpieza de bandejas de papel, pruebas funcionales correctas.	RF-171044				

Mes					Territorial	Sede	Servicio	Descripción	Caso
Dic-25	Pereira	La Virginia	Mantenimiento preventivo de la impresora Ricoh	Se realiza mantenimiento preventivo, Limpieza y validación de uso de los consumibles (Unidad fusora, unidad de imagen, rodillos arrastre de papel y rodillos de escáner), se hace limpieza a cristales de cama plana y ADF, limpieza de bandejas de papel, pruebas funcionales correctas.			RF-176746 IM-176750		
Dic-25	Pereira	Cartago	Mantenimiento preventivo de la impresora Ricoh	Se realiza mantenimiento preventivo, Limpieza y validación de uso de los consumibles (Unidad fusora, unidad de imagen, rodillos arrastre de papel y rodillos de escáner), se hace limpieza a cristales de cama plana y ADF, limpieza de bandejas de papel, pruebas funcionale			RF-176747		

Mes					Territorial	Sede	Servicio	Descripción	Caso
				s correctas.					

Tabla 35 Visitas a Sedes sin Soporte

- Medición ANS Mesa de Servicios

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

Área	Nombre del Indicador	Resultado	Meta
Mesa de Servicio	Tiempo de atención de solicitudes por soporte en sitio	97,78%	95,00%
	Tiempo de solución de incidentes por soporte en sitio	98,54%	90,00%
	Tiempo de solución de requerimientos por soporte en sitio	99,90%	90,00%
	Tiempo de respuesta de la mesa de servicio	99,02	85,00%
	Abandono de llamadas	0,32%	Máximo 8,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 36 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 prestado por la Unión Temporal Gestión TIC 2023 en instalaciones del Data Center Cirion-Colombia XV, en donde está alojada la infraestructura tecnológica que soporta la operación y servicios del Ministerio del Trabajo.

3.1 Datacenter Principal

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

Se observó un comportamiento de crecimiento la asignación de licencias de Office 365 reportados a través de ARANDA, donde se realizó la atención de 100 requerimientos asociados a esta categoría del servicio de Windows, así como la creación, modificación de usuarios que reduce su reporte a 9 casos para el mes de diciembre. De la mano de asignación de licencias se atendieron 51 requerimientos, obteniendo un incremento considerable con respecto a los meses anteriores, con respecto a los casos asociados a configuración de MFA se mantiene en 10 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.

De la mano con el equipo Windows se está trabajando en una configuración para establecer de manera automática la firma de la entidad, se están validando dependencias en el directorio activo para que cada usuario del Ministerio cuente con su firma institucional de manera automática, obteniendo su información, cargo, dependencia y datos de contacto desde el directorio activo, se realizarán pruebas piloto con usuarios de sede central y se irán informando los avances respectivamente. Se solicita un nuevo logotipo con dimensiones más acordes a la firma institucional y se está a espera del envío de este para configuración dentro del Tenant.

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 el mes de diciembre y enero debido a la desvinculación de contratistas de la entidad por cierre de gestión.

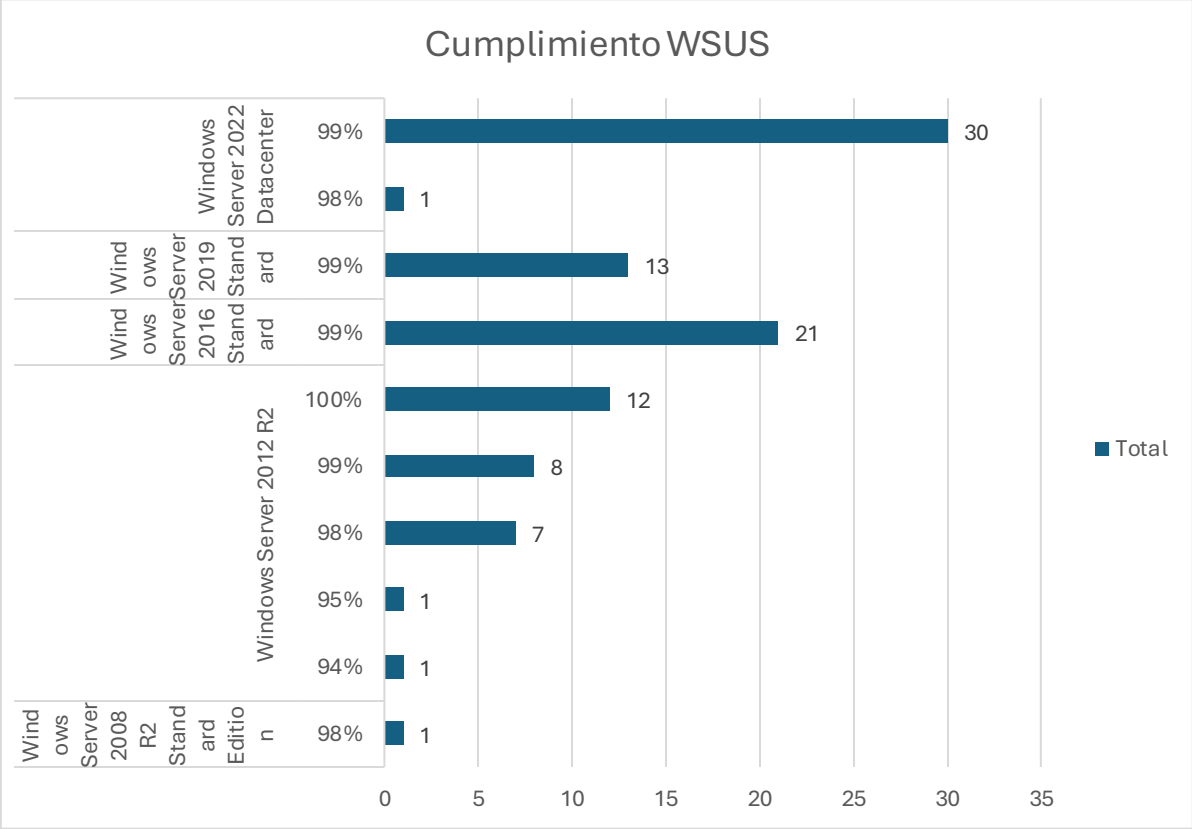


Ilustración 32 Cumplimiento WSUS

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.
Es importante que durante el mes de enero de 2026, se surtan los procesos de inactivación, reactivación o creación de usuarios de acuerdo a 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.

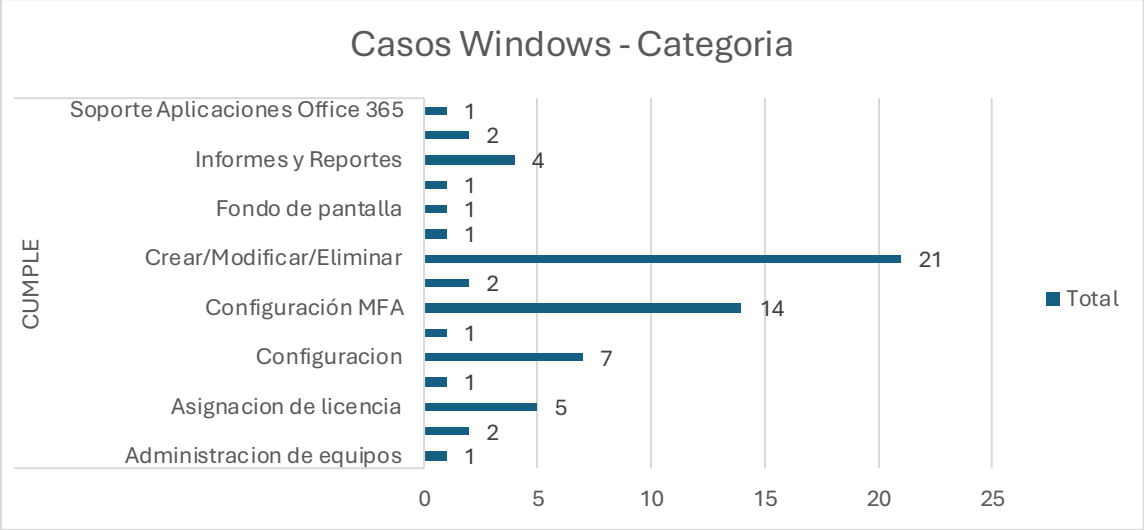


Ilustración 33 Casos Win Servicio

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.

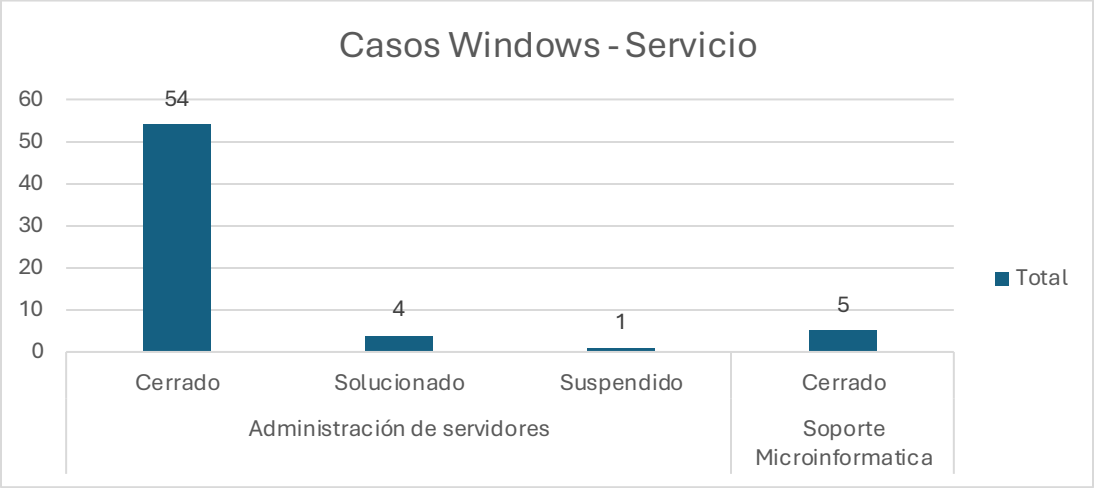


Ilustración 34 Estado final de los casos Windows

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

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

Tabla 37 Capacidades contractuales

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

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

Tabla 38 Capacidades contractuales

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

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

Tabla 39 Consumo de capacidad con servidores para desaprovisionar + ambientes de pruebas)

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

Tabla 40 Consumo de capacidad Sin servidores para desaprovisionar con ambientes de pruebas

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

Tabla 41 Consumo de capacidad Sin servidores para desaprovisionar sin ambientes de pruebas

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

Tabla 42 Consumo de capacidad Servidores Pruebas y Desarrollo

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 Asesment realizado para aplicaciones a migrar hacía Azure ya fue desaprovisionado tras autorización de la OTIC. De igual forma no se restan las capacidades de estos servidores al no estar en escenario productivo o pruebas pero dan la visual a la entidad de que no están superando su holgura de crecimiento.

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

Tabla 43 Consumo de capacidad actual

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.

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.

Así mismo, se culminó el acompañamiento en el Assesment realizado por GoToCloud para aplicaciones On Premises como lo son RUE, RUTEC y CEN, las cuales pretenden ser migradas a Azure. El Assesment ha venido avanzando en diferentes etapas, en donde se ha realizado:

- Aprovisionamiento de Appliance de Azure Migrate.
- Creación de Grupo de Recursos en el Tenant de la entidad en la Suscripción de Empleo.
- Creación de Componentes de Azure Migrate en el tenant.
- Sincronización de On Premises con Azure a través del Appliance.
- Tracking de información de las apicaciones a intervenir.
- Generación de logs exportados desde el appliance para revisión y estudio del equipo de GoToCloud.

De acuerdo con el diagnóstico realizado por el equipo GoToCloud para la migración de las aplicaciones tras la realización del Assesment. Se requiere que el equipo OTIC realice la validación y confirmación para el desaprovisionamiento del Appliance de Azure Migrate el cual fue requerido por el equipo de GoToCloud para la realización de esta actividad. Es importante esta confirmación ya que si es requerido algún tipo de log o información abstraída a través del Appliance sería ideal extraerla antes de realizar el desaprovisionamiento y la liberación de las capacidades en la Nube Privada de la entidad.

Así mismo se observan componentes que se aprovisionaron en Azure para realizar el punto de conexión a través del Appliance, por lo cual deben tenerse en cuenta de la misma forma o si de lo contrario se van a conservar:

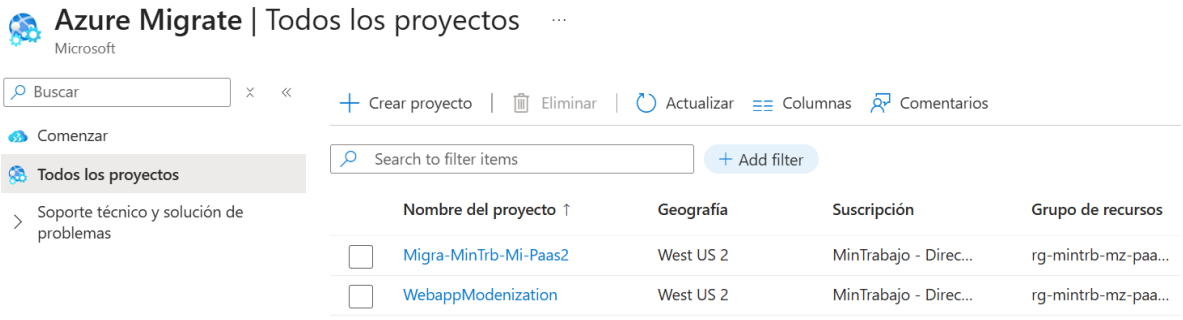


Ilustración 35 Azure Migrate

De igual forma, se culmina con el proceso de acompañamiento para migración de Apps de Nube Privada hacía Cloud, el proveedor Go to Cloud realiza envío de la propuesta y se encuentra en revisión por la Oficina de Tecnologías de la Información
Se realizaron las siguientes observaciones de los tableros de control en Power BI:

- Atenciones: la actualización desde el origen de datos 01/06/2024
- Capacitaciones y cieti: la actualización desde el origen de datos 01/05/2025
- Centros entrenamiento: la actualización desde el origen de datos 02/08/2025
- teletrabajadores: la actualización desde el origen de datos 31/12/2023.
- El campo es paz total: la actualización desde el origen de datos 30/11/2023.
- Encuestas trabajo infantil - la actualización desde el origen de datos 28/07/2025
- Equipares Rurales - la actualización desde el origen de datos 02/06/2023.
- estado joven - la actualización desde el origen de datos 08/06/2023.
- Formándonos para la paz total: la actualización desde el origen de datos 30/09/2023 al 30/11/2023.
- Fortaleciendo Sueños_Jóvenes para la Paz: la actualización desde el origen de datos no contiene fechas.
- La comunidad mi causa: la actualización desde el origen de datos 31/12/2023
- Observatorio: la actualización desde el origen de datos 25/07/2025
- RUTEC: la actualización desde el origen de datos 09/11/2023
- Subsistema de Formación para el Trabajo: la actualización desde el origen de datos 09/11/2023

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.

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. Así como el proceso de migración del ChatBot de la entidad alineado con el framework de arquitectura. Se realiza creación de la máquina virtual para el proyecto de interoperabilidad institucional en Azure, para la configuración por parte de la AND del componente de XROAD. Se está a espera de agendamiento de sesión técnica para instalación del componente de XROAD dentro de las máquinas virtuales. AND manifiesta que previamente requiere enviar un checklist a la entidad para validar que todos los prerrequisitos están acordes antes de iniciar la instalación.

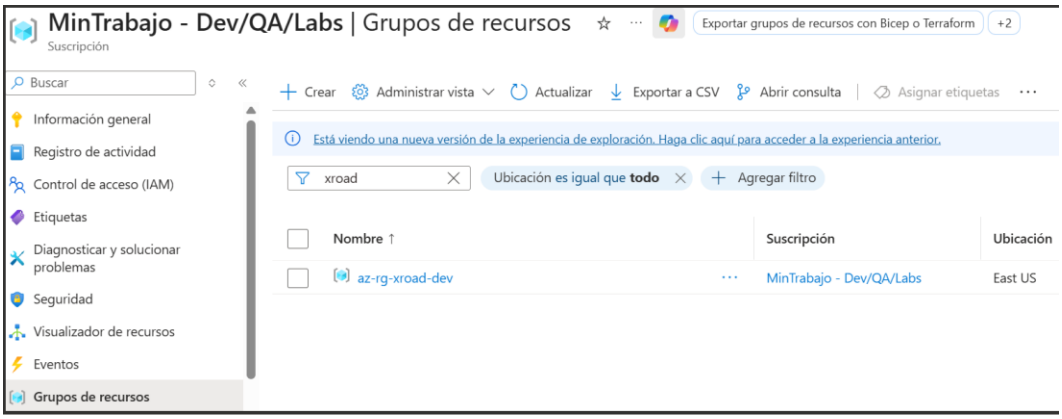
Es importante mencionar que para que el proceso de XROAD a nivel de interoperabilidad la entidad debe contar con un ambiente de pruebas de Gestor documental, ya que la AND para los procesos de pruebas que requieren para garantizar una correcta interoperabilidad requieren testear el trámite completo integrado, lo cual implica lanzar consultas hacia servicios y tablas de bases de datos del gestor documental el cual soporta la mayoría de los tramites de la entidad. Para ello es requerido validar los estados de licenciamiento de todos los componentes que permiten al gestor documental funcionar en un entorno de pruebas, tanto capa de aplicación como IBM, ya que, para aprovisionar entornos de pruebas, es requerido licenciamiento de ambos componentes y que el licenciamiento disponible tenga la capacidad de soportar el entorno a aprovisionar de acuerdo con la arquitectura planteada para la solución.

- Se ha realizado la creación de las máquinas virtuales de XROAD tanto para ambiente productivo, pre productivo y desarrollo. 15/10/2025.

    - Se realizan las configuraciones necesarias para instalar XROAD en acompañamiento del equipo de la AND. Actividad realizada el 15/12/2025.
- Se realizó el envío de las variables para la notificación de nivel 1 de lenguaje claro del trámite “Expedición del Certificado de Primer Empleo” insumo para la interoperabilidad. Actividad realizada el 15/12/2025.
- Para el aprovisionamiento de servidores virtuales asociados a la solución de gestor documental nos permitimos informar que tras las autorizaciones de IBM y Oracle a través de la jefatura de la Oficina TIC, se inició con el clonado de las VM del clúster de aplicación y el montaje del clúster de DDBB.
    - Con respecto a la máquinas virtuales de aplicación, fueron clonadas con éxito el 16/12/2025.
        - Se realizó asignación de IP privadas en un segmento aislado para evitar interferencias con el ambiente productivo debido a temas de resolución de hostname. 17/12/2025
        - Se realizó el cambio del nombre de las VM. 18/12/2025
        - Se realizó configuración para comunicación con los controladores de dominio para garantizar autenticación con Active Directory. 18/12/2025
    - Se realizó configuración del clúster de DDBB en la misma modalidad que el ambiente productivo. 12/12/2025
        - Se realiza ventana de mantenimiento de emergencia del Gestor Documental para realizar reducción de la DDBB y poder realizar una restauración más optima y con menos consumo de capacidades.
        - Se realiza restauración de la DDBB y parchado del server de Oracle que aloja la DDBB. 18-19/12/2025
    - A nivel de configuración de los servidores de aplicación como sistema de información el equipo de IBM se encuentra realizando los ajustes para visualización de servicios y conexión hacía la base de datos, se espera que la configuración culmine antes del 23/12/2025.
- El dominio ya fue creado bajo el nombre srvxroadinterop usuario dentro del dominio de la entidad, las contraseñas serán suministradas en un correo independiente a través de una DDBB de KeePass.
- Los números de radicados deben ser solicitados a las áreas funcionales o dueños de los trámites para que la AND los pueda emplear como objetos de prueba.
- A nivel de control de Firewall no hay que realizar cambios ya que los puertos 80 y 443 tienen permitido el tráfico.
- El acceso a los servidores de pruebas se realizará a través del usuario anteriormente mencionado.
- La actualización del recaptcha requiere de una ventana de mantenimiento que genera indisponibilidad del Gestor documental, por ahora se ha identificado la librería de recaptcha en el modulo de PQRSD, se está validando el código fuente del que dispone la entidad para el módulo de trámites y servicios.
- El acceso a la base de datos se realizará a través de la aplicación, en caso de requerir acceso directo a la DDBB debe realizarse en acompañamiento del DBA de la entidad.
- Los accesos de VPN serán suministrados en el correo de acceso del usuario de dominio.

- Con respecto a los ítems de la pagina Web, la ventana de actualización de versión a 7.4 de LifeRay se realizará desde el 19/12/2025 en horas de la noche hasta el 20/12/2025 lo cual permitirá culminar con la revisión de links rotos por parte del Web Master de la entidad y la implementación de acciones de mejora identificadas en el Informe remitido por la AND.

Tras la sesión sostenida con el equipo de AND y de la OTIC, nos permitimos informar que desde el equipo de Servicios Centrales/ Grupo Soporte Informático, se han realizado las actividades correspondientes para el despliegue y aprovisionamiento de este componente XROAD. A continuación, se dejarán las evidencias del aprovisionamiento respectivamente: Grupos de recursos Preproducción y producción en la suscripción de Interoperabilidad y desarrollo en suscripción de Dev:



Interoperabilidad

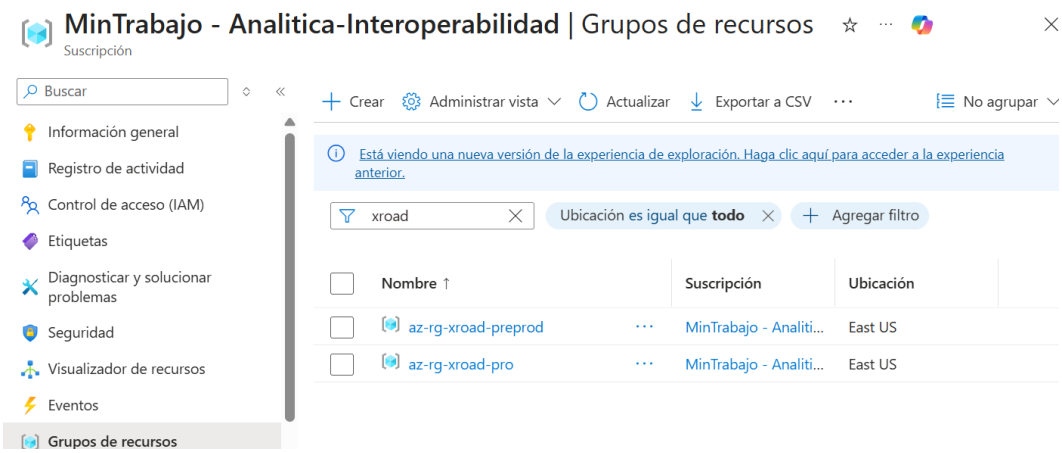


Ilustración 36 RG Pruebas y prod XROAD

Máquinas virtuales creadas, direcciones IP publicas asignadas y grupos de seguridad con las políticas y excepciones indicadas por la AND:

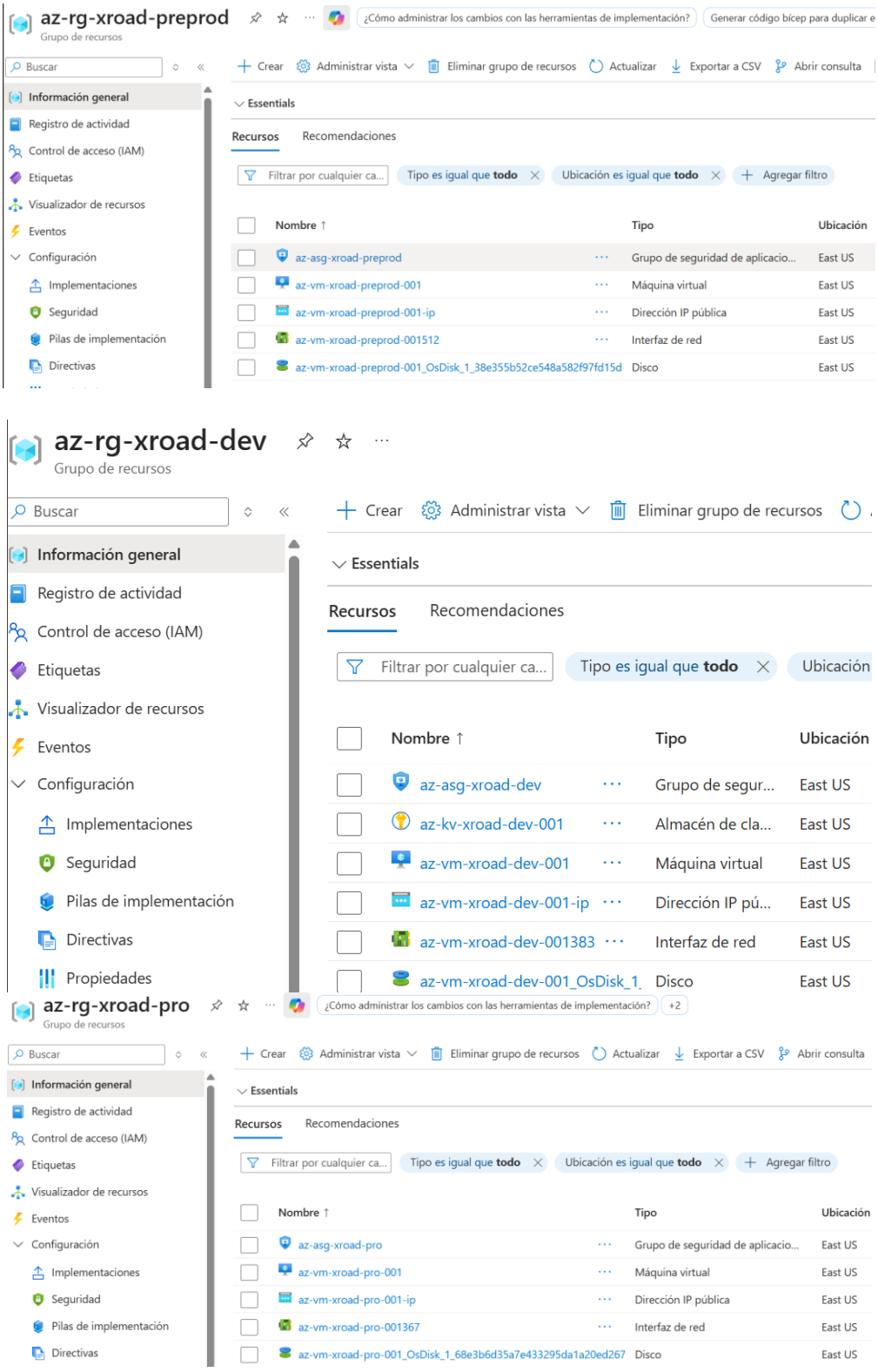


Ilustración 37 Grupos de recursos XROAD Azure

Sitios XROAD arriba:

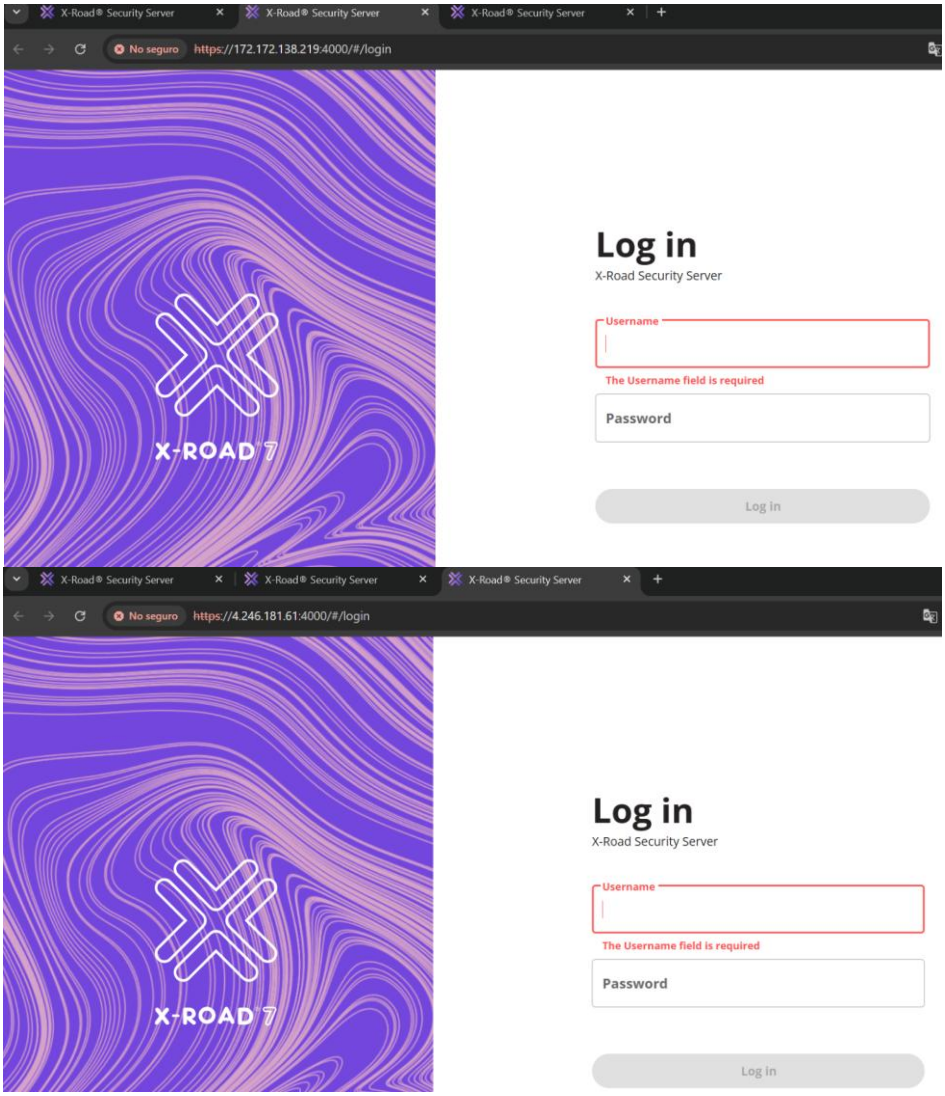


Ilustración 38 Stios XROAD operativos

URL de acceso:

- Prod: https://4.246.181.61:4000/#/login
- Dev: https://172.172.138.219:4000/#/login
- Pre-prod: https://20.185.49.46:4000/#/login

De acuerdo con lo anterior, se queda a espera del paso a seguir con respecto a la configuración desde la AND de los servicios interoperabilidad XROAD servidor central. De igual forma se remiten los servidores de pruebas a los cuales tendrían acceso el equipo AND para el proyecto de Interoperabilidad.

URL acceso DevOps: https://dev.azure.com/MinTrabajoDevOps/TramitesServicios

Servidores Aplicación Gestor Documental:
Para el acceso de las VM se debe realizar a través de Escritorio Remoto (se recomienda generar una sesión para realizarlo en acompañamiento con el equipo de trabajo y explicar en qué servidor se encuentra cada componente).

HOSTNAME	DIRECCIÓN IP
MINTRABGDPRU01	172.20.43.10
MINTRABGDPRU02	172.20.43.11
MINTRABGDPRU03	172.20.43.12
MINTRABGDPRU04	172.20.43.13
MINTRABGDPRU05	172.20.43.14
MINTRABGDPRU06	172.20.43.15
MINTRABGDPRU07	172.20.43.16
MINTRABGDPRU08	172.20.43.17

Tabla 44 Servidores de pruebas Gestor Documental

Con respecto a los servidores de pruebas del servicio RUI, por parte del área funcional, aun no se autoriza el acceso debido a que se encuentran en ejecución de set de pruebas de la nueva versión del sistema de información.
La conexión VPN se establece a través de un cliente FortiClient VPN restaurando la configuración adjunta en el presente correo. El archivo de configuración dentro del .ZIP esta nombrado VPN_Mintrabjo.conf. Para poder abrir la base de datos de KeePass se adjunta un .txt con la clave de acceso ClaveDDBB_KeePass.TXT.
Teniendo en cuenta lo anterior, las credenciales de acceso a la entidad, VPN, DevOps y VM fueron suministradas a la entidad el 24/12/2025.

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.

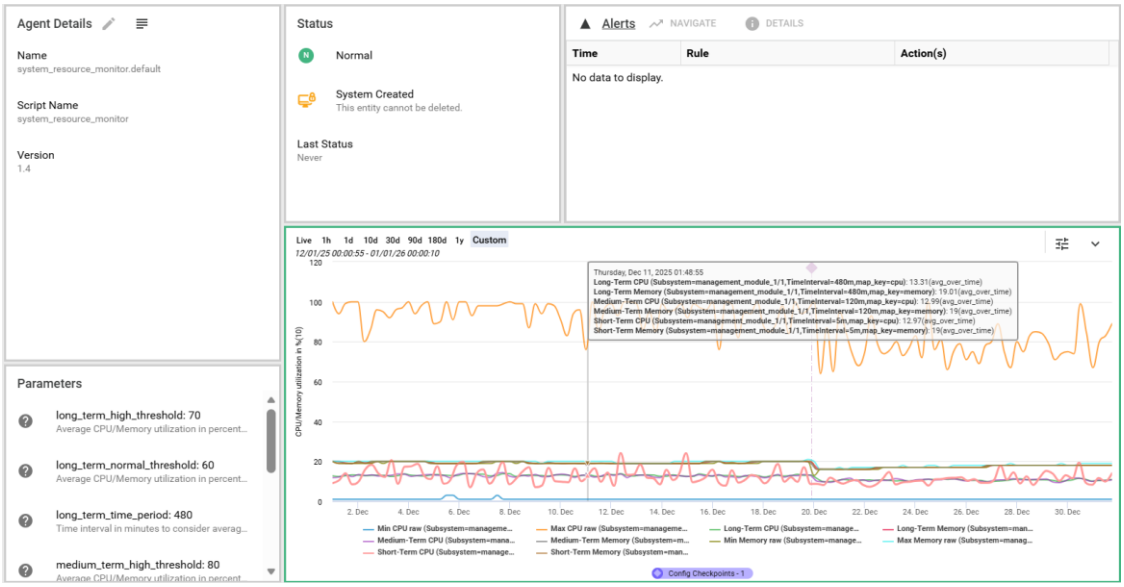


Ilustración 39 Comportamiento SWCORE Datacenter Colombia XV

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

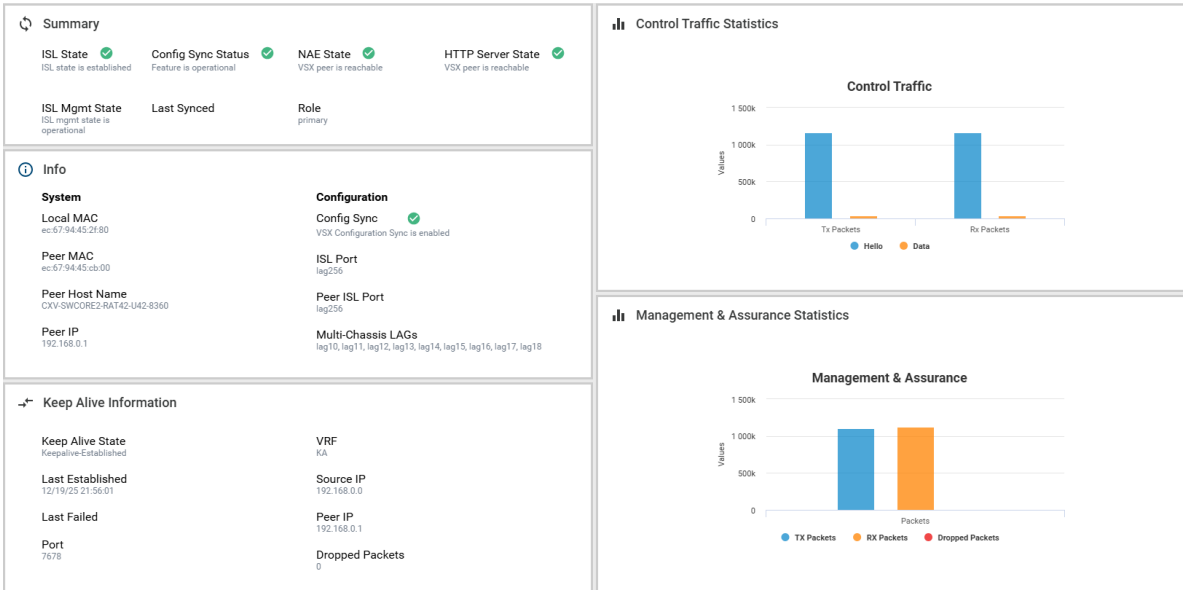


Ilustración 40 Sincronización HA de los Switch Core

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 tuvieron picos altos de consumo sin afectar el rendimiento del canal, se observa un flujo estable de tráfico, se tuvo un consumo promedio de entrada de 440 Mbps y 320 Mbps de salida. El tráfico se ha mantenido con el mismo comportamiento de consumo de los últimos meses.

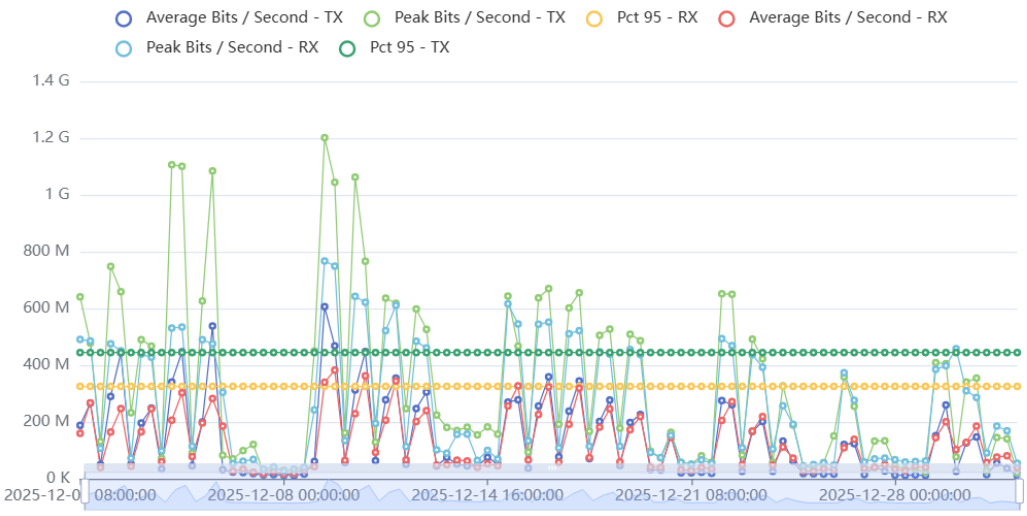


Ilustración 41 Grafica de consumo canal Internet Datacenter

Durante el mes de diciembre no se generaron incidentes sobre el canal de internet, el cual ha estado trabajando con normalidad.

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:

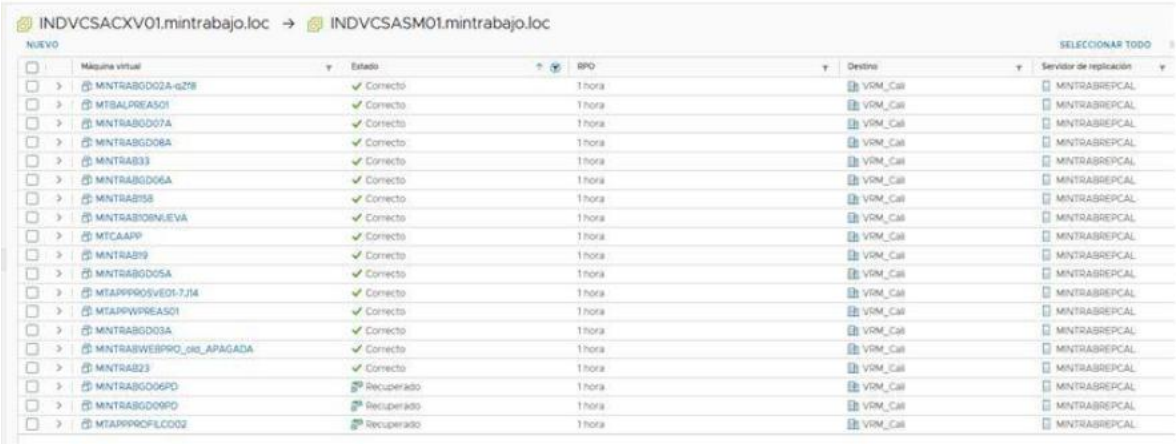


Ilustración 42 Captura de imagen máquinas virtuales

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.

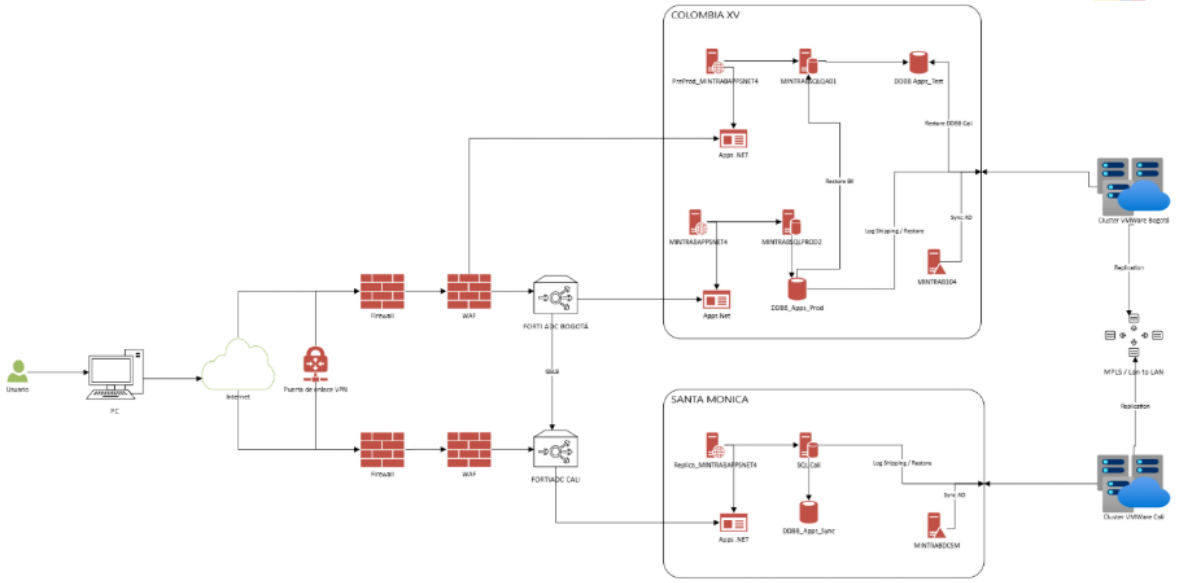


Ilustración 43 Escenario de pruebas Aplicaciones y AD

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 340 Mbps.

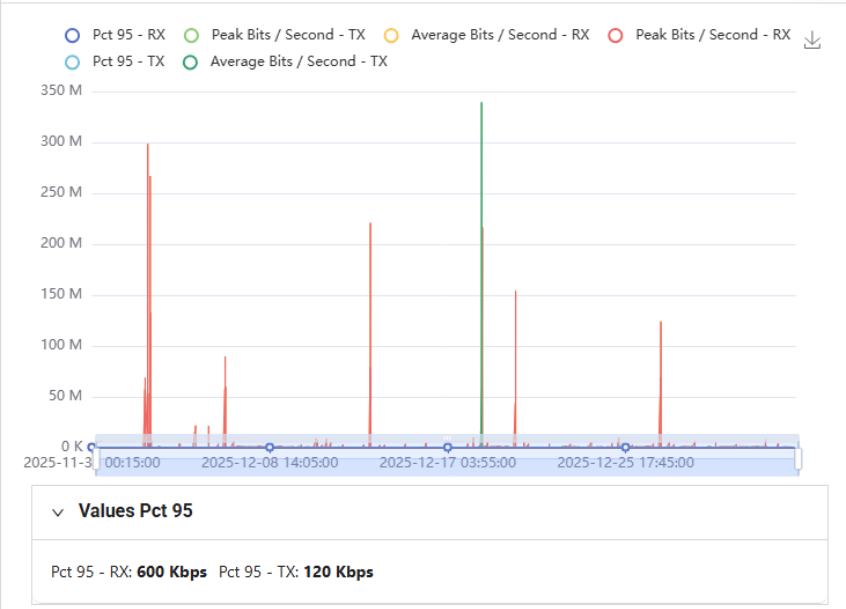


Ilustración 44 Extremo DC Bogotá

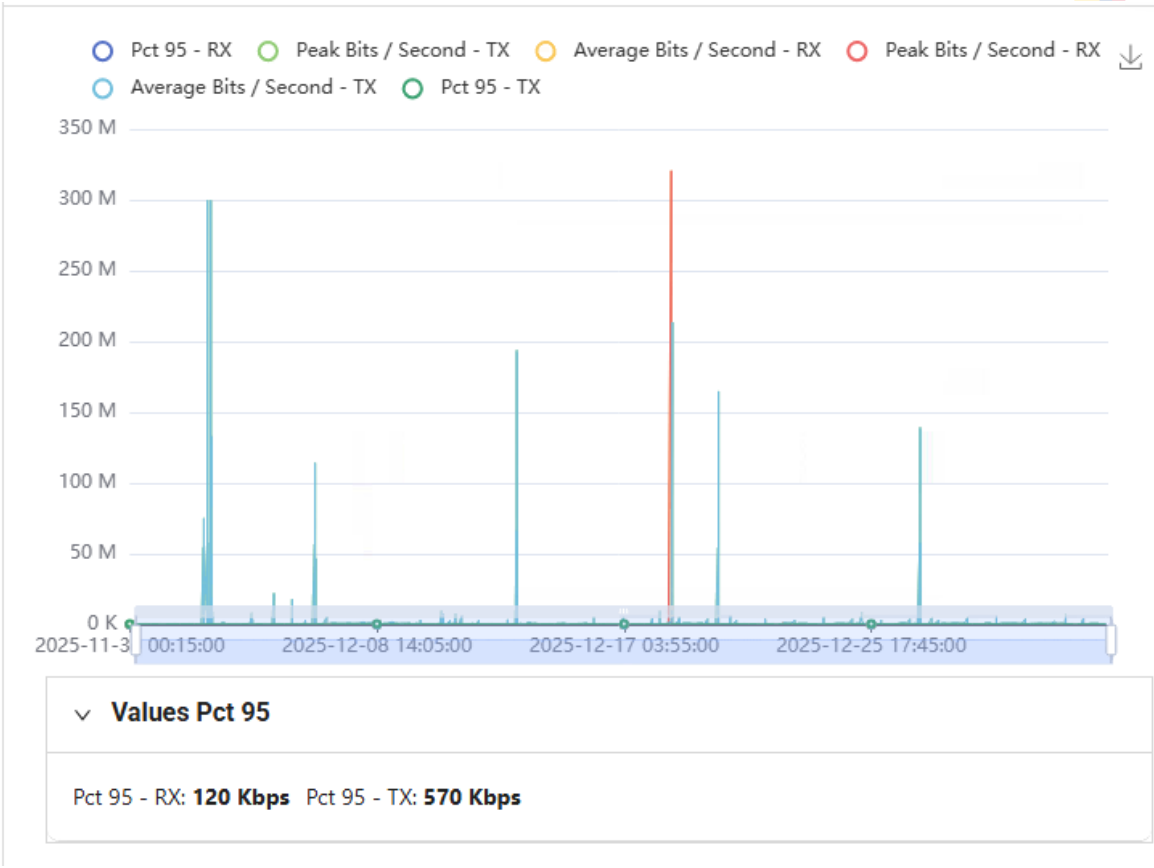


Ilustración 45 Extremo DC Cali

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 13Mbps.

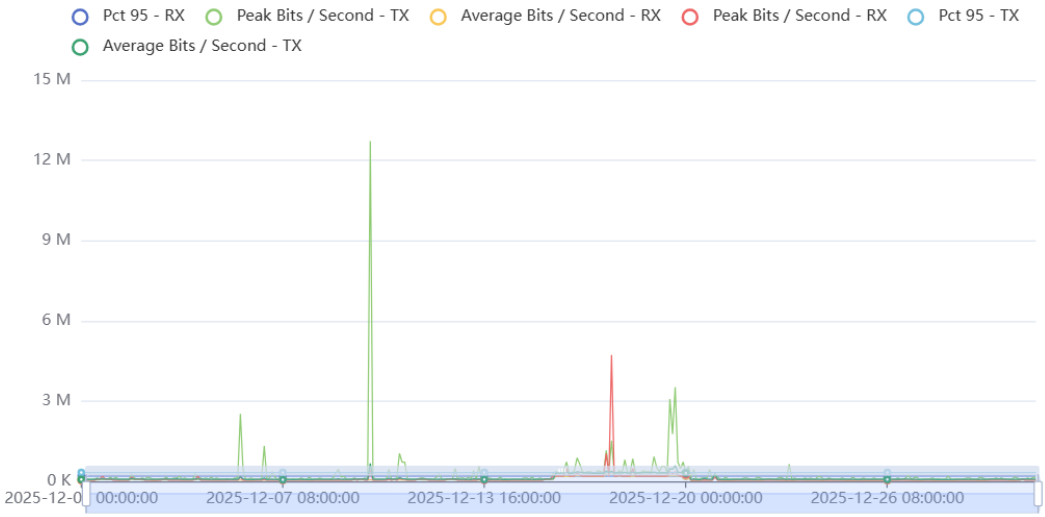


Ilustración 46 Estado canal de Internet DC Cali

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

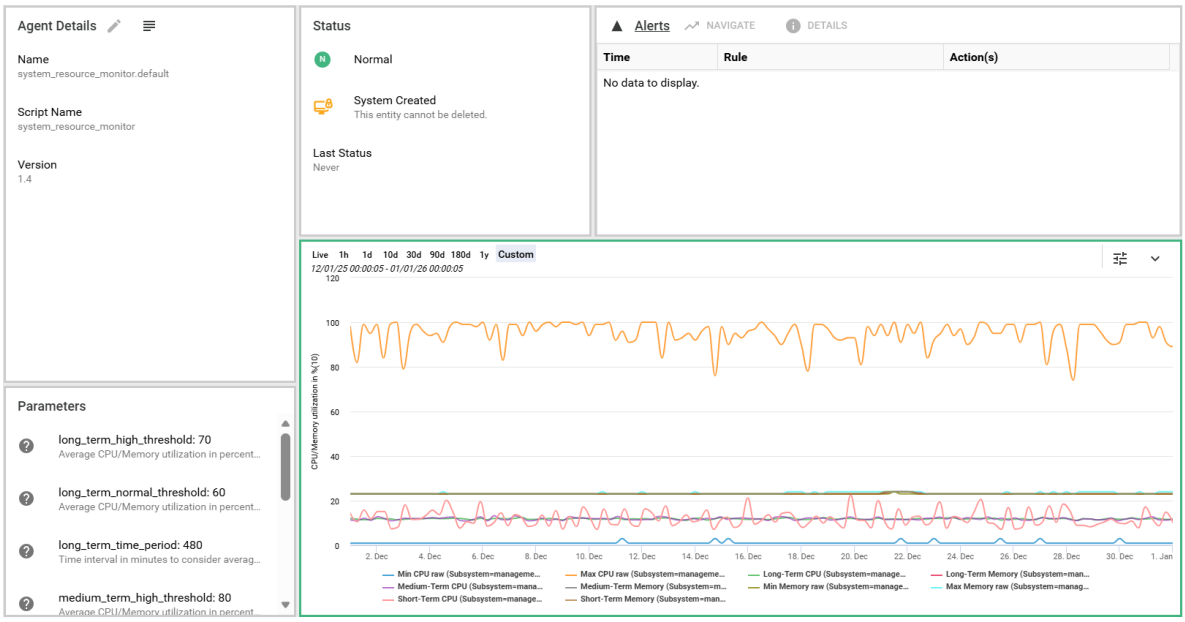


Ilustración 47 Estado SWCORE Datacenter alterno

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

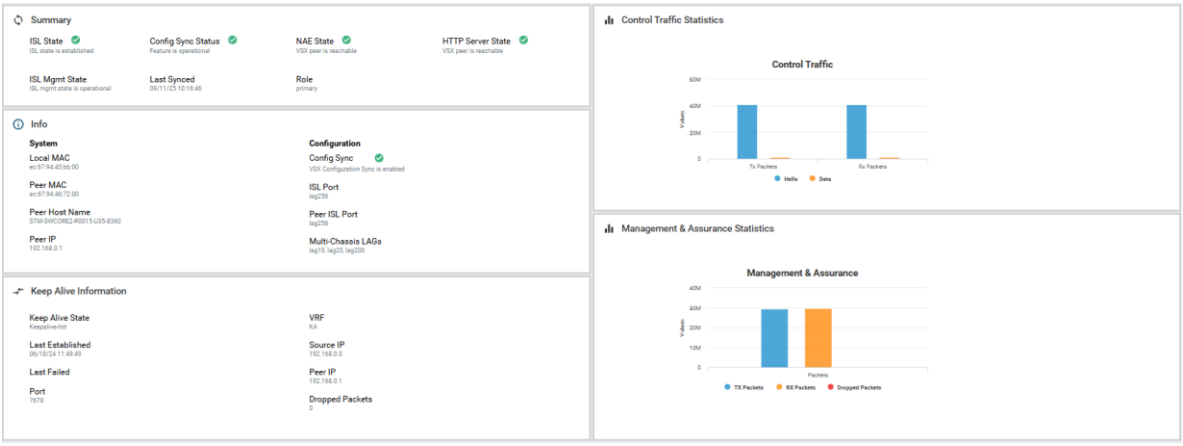


Ilustración 48 Estado HA SWCORE Datacenter alterno

Se verifica el canal MPLS de datacenter alterno, el cual se observa que se ha mantenido activo durante el mes de diciembre, 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 pico máximo de entrada de 10.92 Mbps y de salida de 8.59 Mbps.

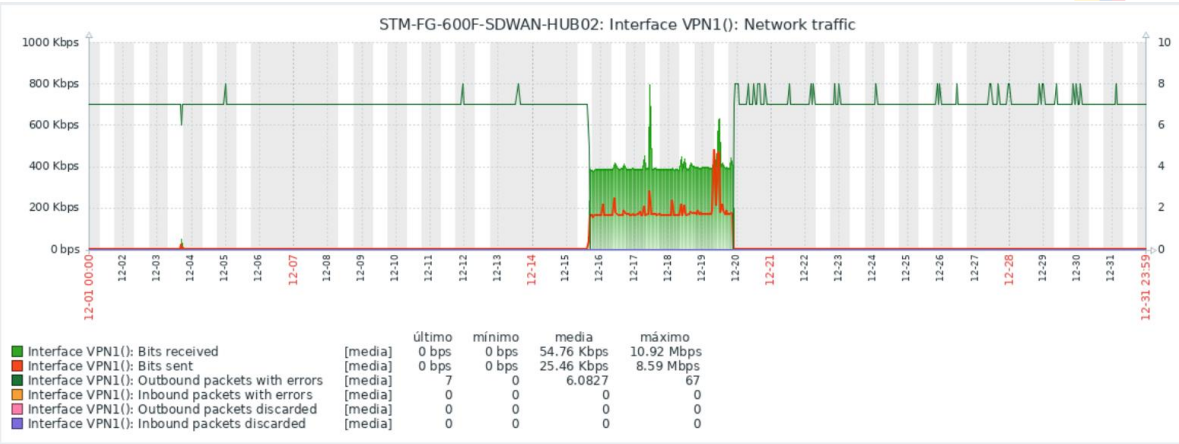


Ilustración 49 Consumo canal MPLS DC Alterno

Se verifica estado del equipo, donde se observa que presenta un uptime de 39 semanas con 1 día.

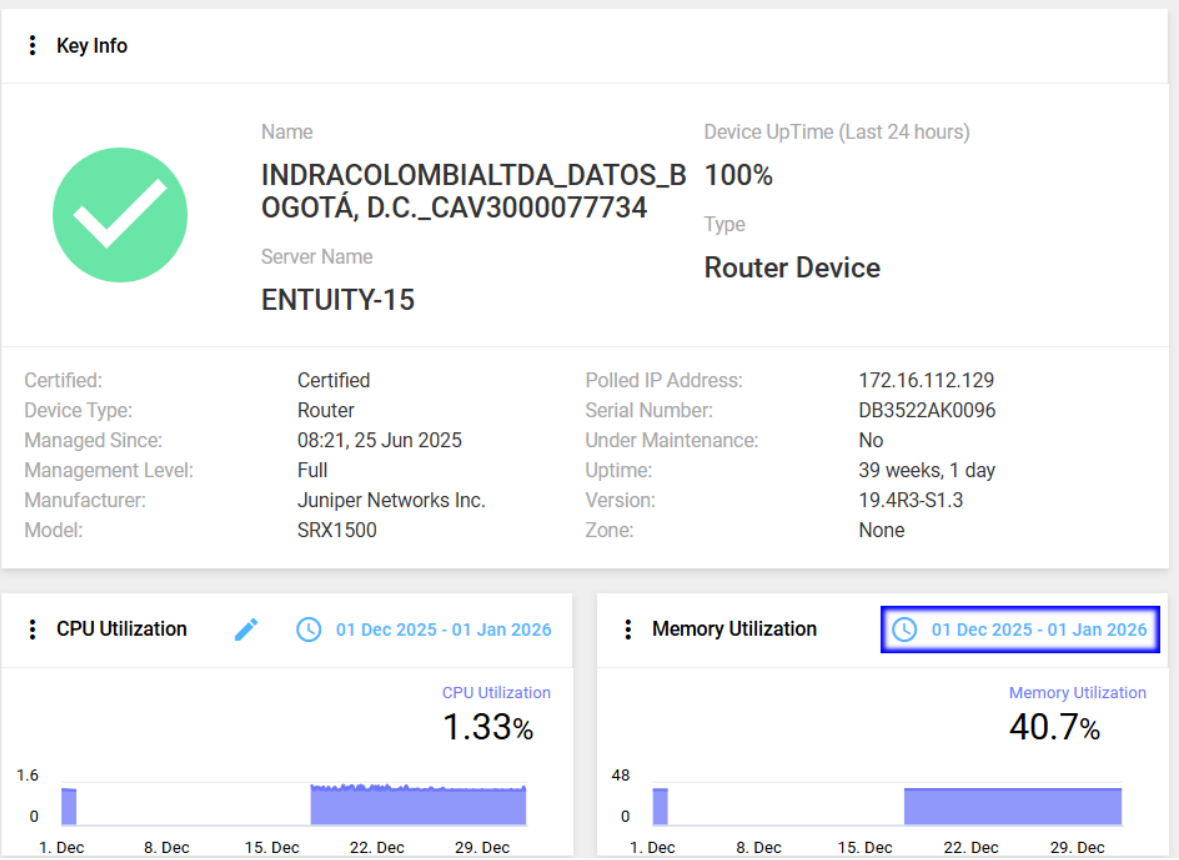


Ilustración 50 Estado Router MPLS DC Alterno

3.1.2 Procesamiento, Almacenamiento y Respaldo

- Servidores Windows e Infraestructura Virtualizada

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 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.

VM → SDTCUNDI01: Esta máquina virtual fue usado históricamente como un File Server (Servidor de archivos) para la Subdirección de IVC/Gestión Territorial. En la actualidad aloja información histórica de la entidad, pero no observamos una alta transaccionalidad hacía el servidor. Es requerido se indique si es posible dar de baja este servidor y generar una copia de seguridad o si de lo contrario es requerido migrar esta información a un File Server en uso con sistema operativo actualizado. No obstante, existe la salvedad que dentro de este servidor se aloja la base de datos de Access de CUNDISSIT por lo cual se debe validar en donde alojar este recurso o que decisión se toma con respecto al mismo.

- Se brinda acceso a los usuarios de la DT Bogotá para validación de la información que debe ser conservada en un file server actual y cual debe irse a backup respectivamente.
- La dirección de la DT aprueba el apagado de la máquina virtual tras generar un full backup y en disposición para restauración en caso de requerirse.

3.1.3 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.

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



Ilustración 51 Casos App Servicio

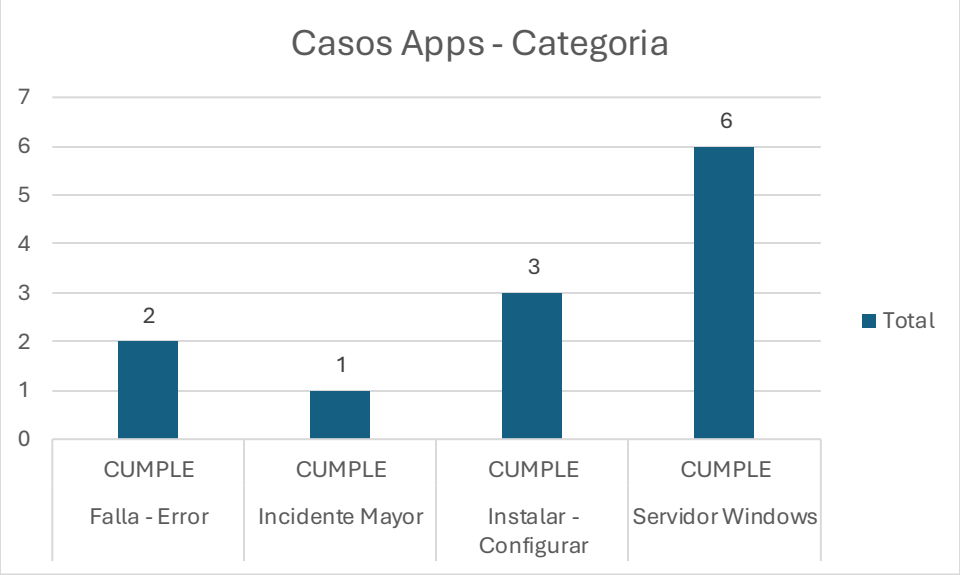


Ilustración 52 Casos App Categoría

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

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.

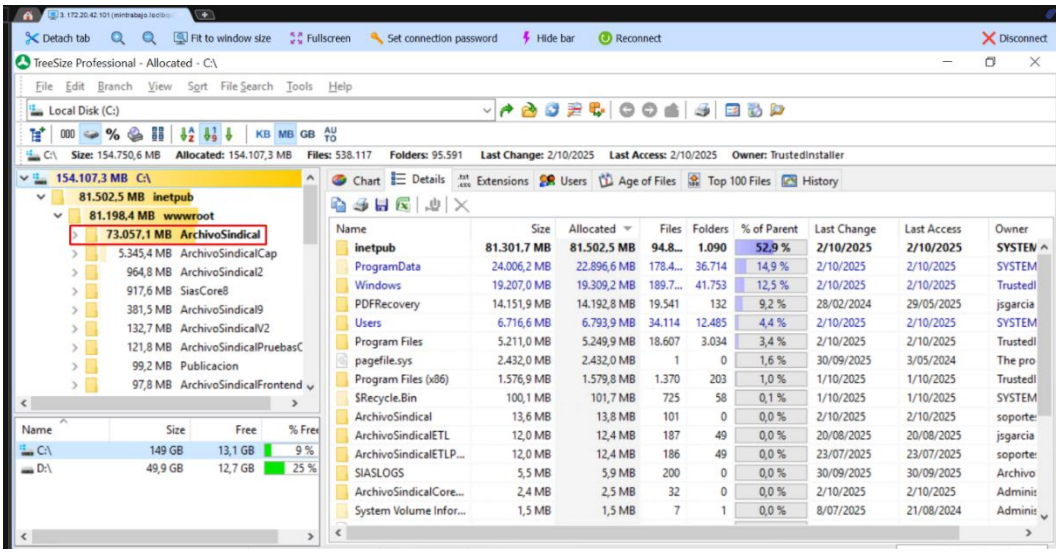


Ilustración 53 Tamaño Archivo Sindical

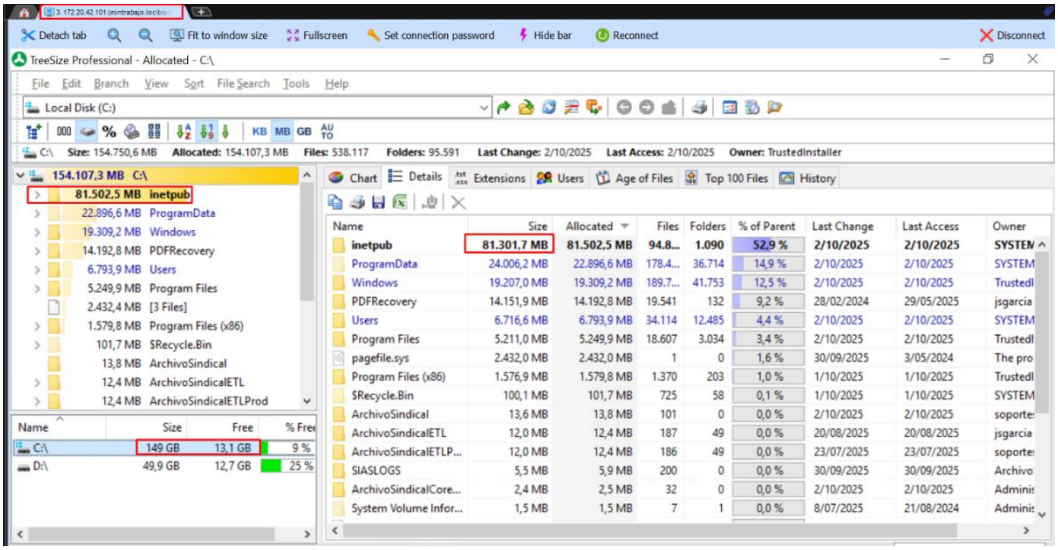


Ilustración 54 Tamaño IIS

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 através 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 sostiene 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 programa sesión para el 15 de diciembre de 2025 con el fin de socializar con las áreas funcionales la independización de aplicaciones, el impacto técnico y a nivel de seguridad de este cambio y que tengan visibilidad de la propuesta para el cambio que se espera realizar durante la vigencia del presente contrato. Tras la sesión, las áreas funcionales a través de sus lideres tomaron una posición bastante receptiva al respecto y se les socializo el nuevo escenario de aplicaciones a donde la entidad quedara productivamente.

Se socializa el estado final a nivel de arquitectura con la entidad:

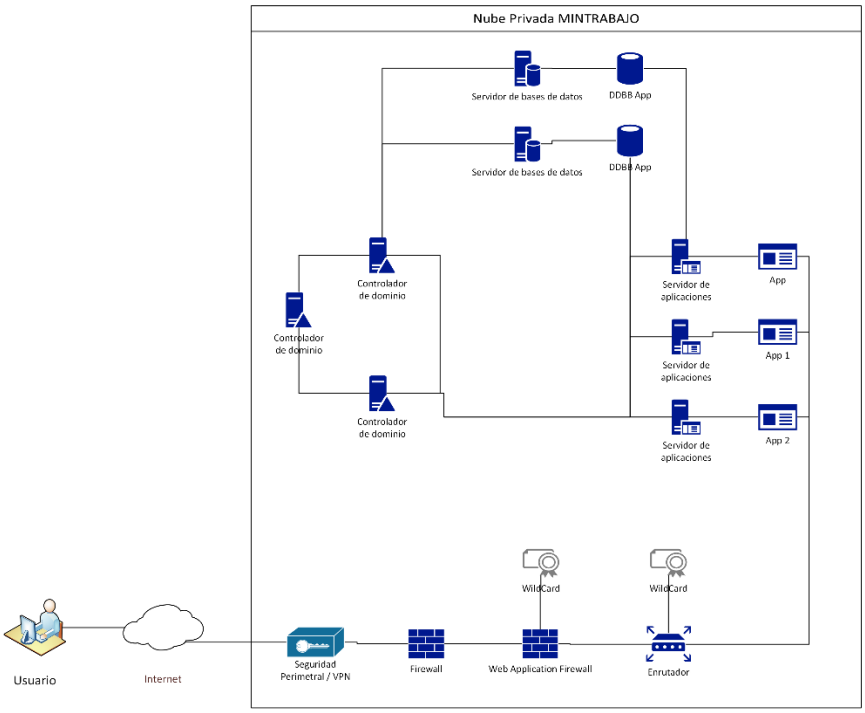


Ilustración 55 Arquitectura Apps nueva

Y la reorganización de los sitios de manera independiente:

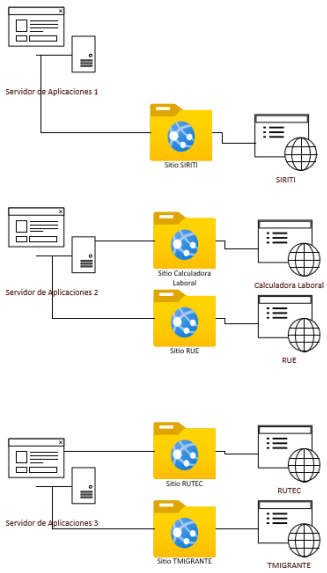


Ilustración 56 Distribución de sitios

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. o Se ejecutaron los scripts de creación de roles. o 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.

GESTOR DOCUMENTAL

A nivel de mantenimientos del gestor documental 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 primera 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.

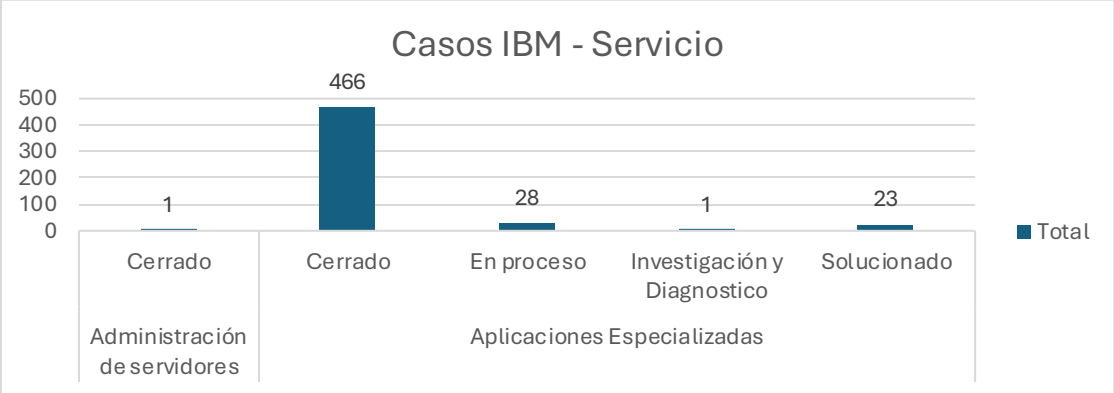


Ilustración 57 Casos *IBM Servicio*

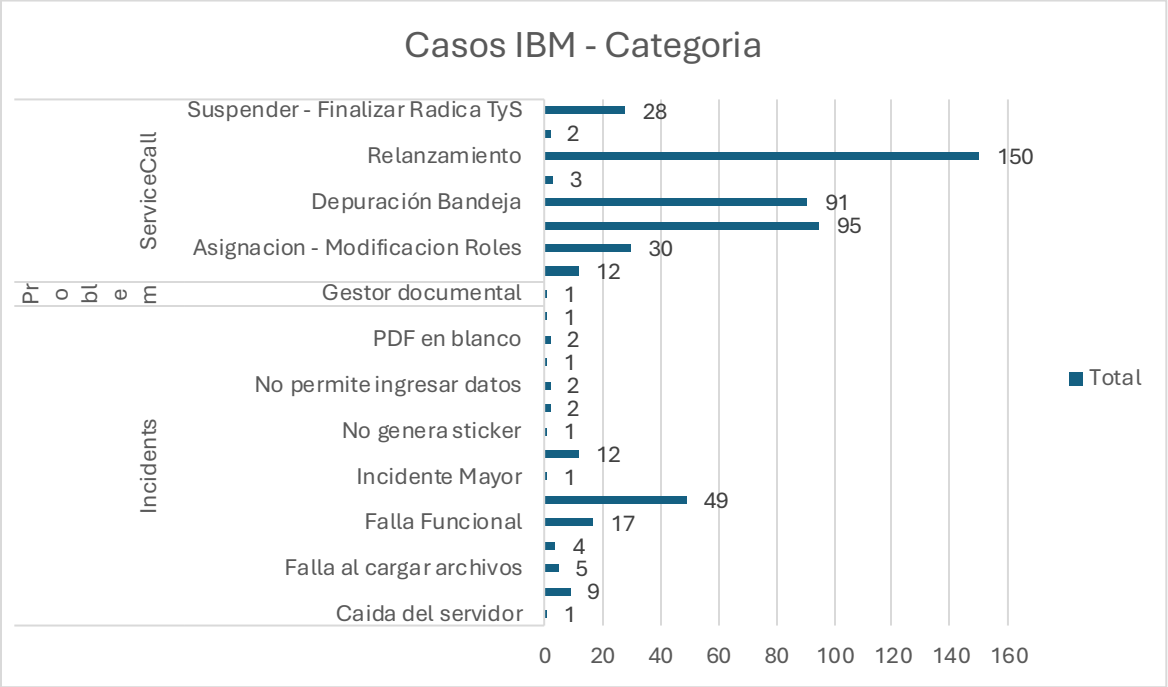


Ilustración 58 Casos IBM - categoría

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 (150 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 (95 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 (91 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 (12 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 (49 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 realiza 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 obedece 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 des habilitación tiene 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:

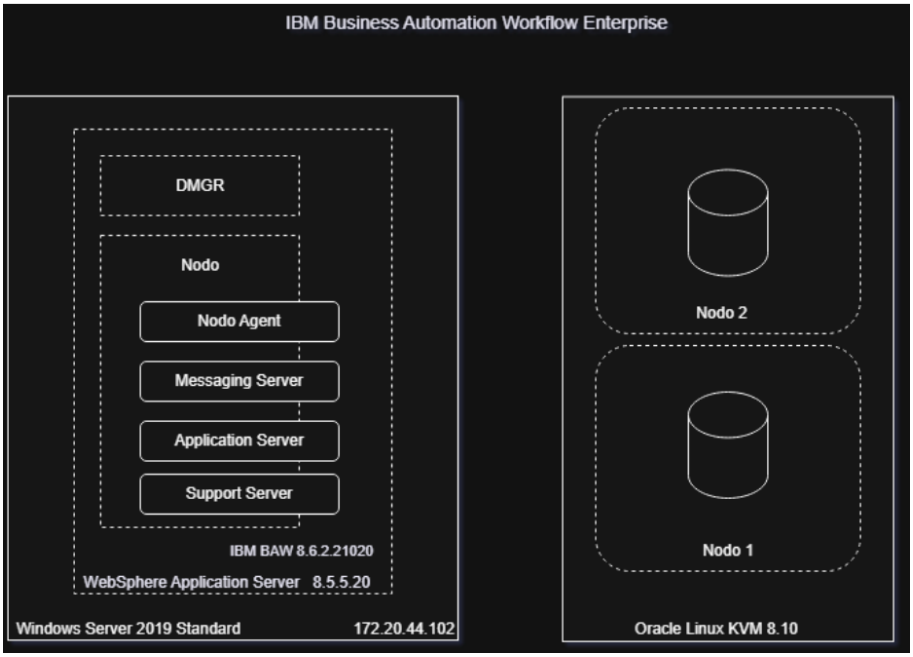


Ilustración 59 Diagrama BP

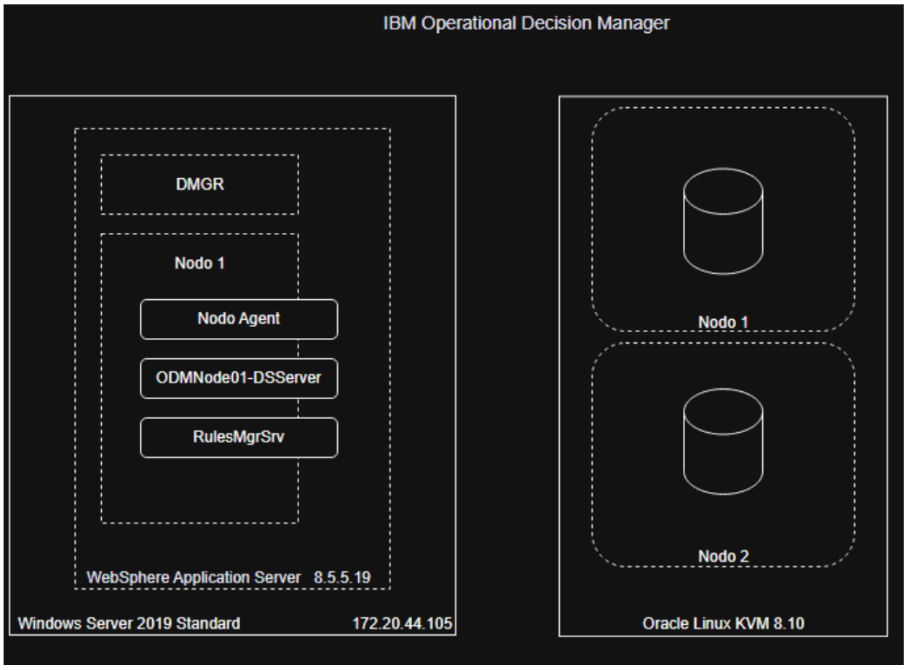


Ilustración *60* Diagrama ODM

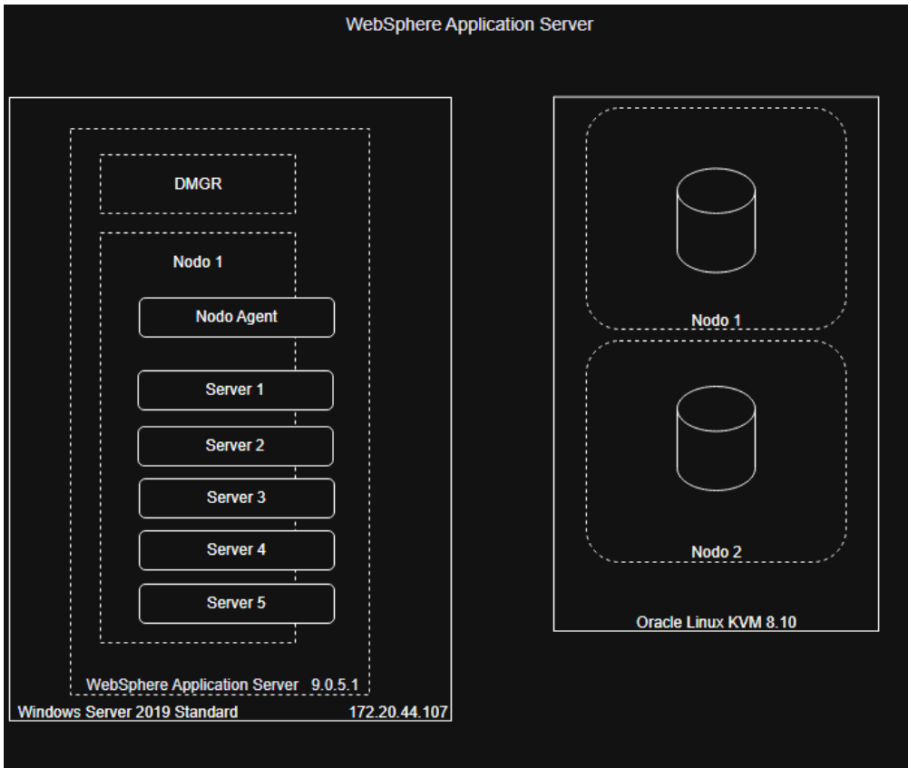


Ilustración 61 Diagrama WASND

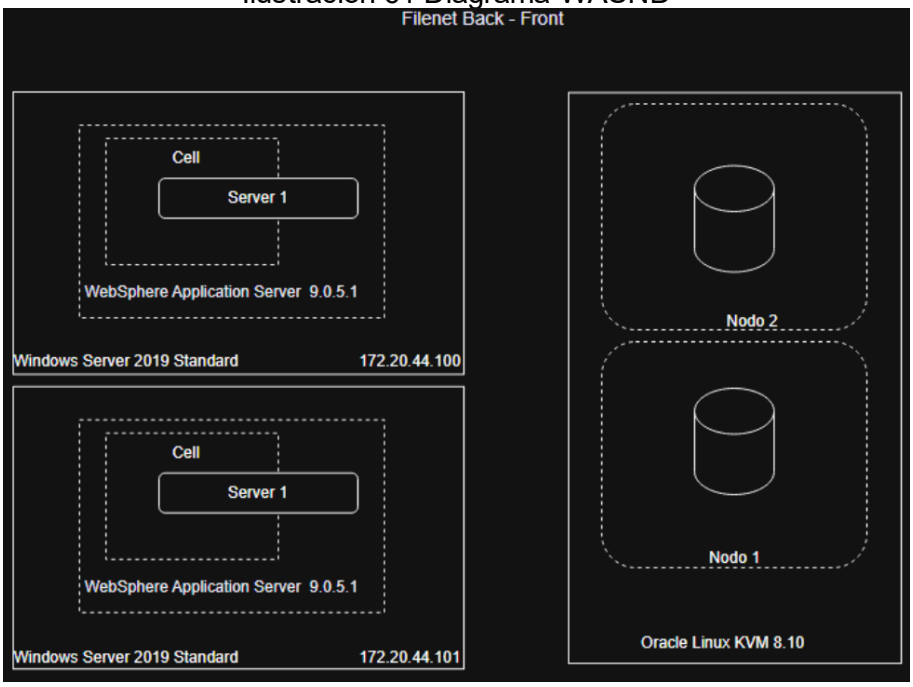


Ilustración 62 Diagrama FileNet Front

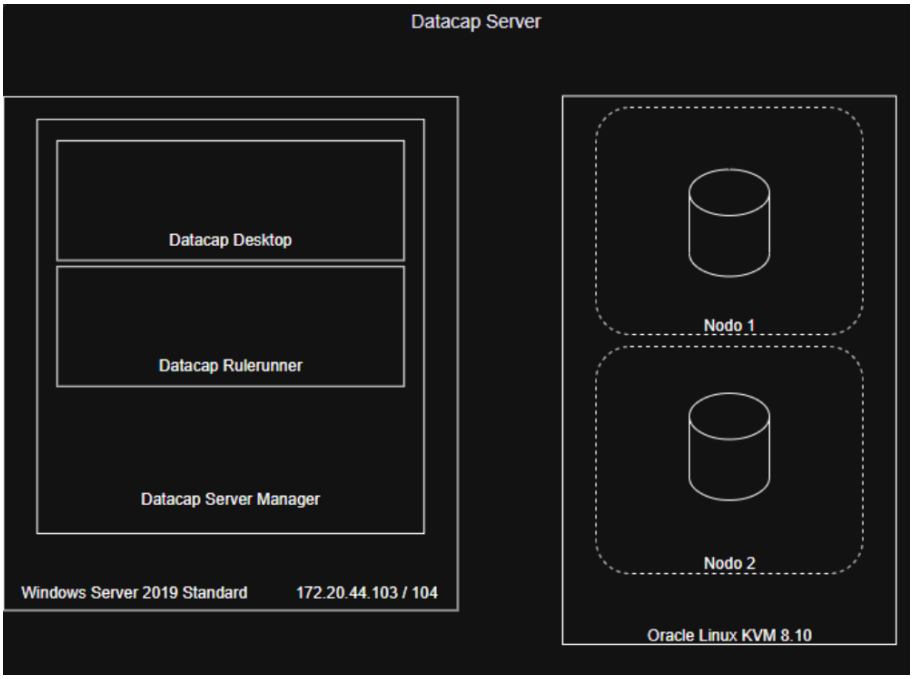


Ilustración 63 Diagrama Datacap

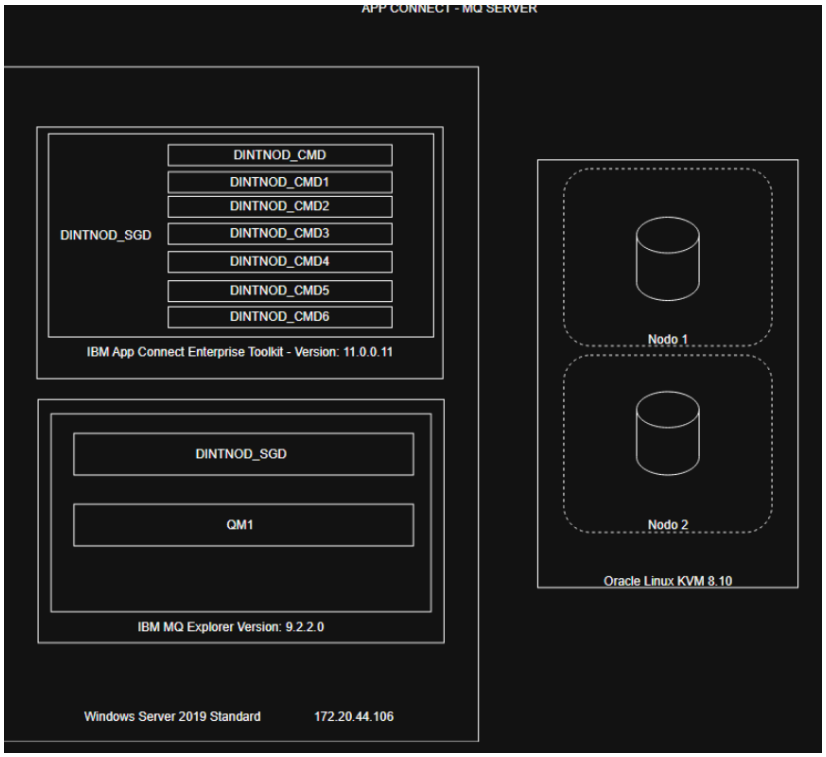


Ilustración 64 Diagrama App Connect

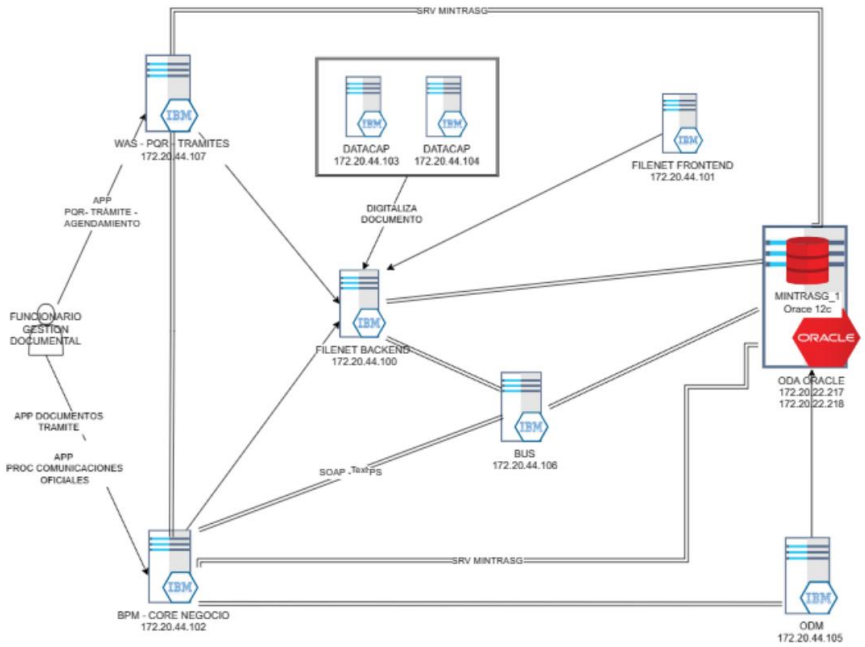


Ilustración 65 Arquitectura Gestor Documental

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 66 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 67 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 68 IBM Licenciamiento

Mes	Suma de Total Instancias
Enero 2025	111854
Febrero 2025	149070
Marzo 2025	148829
Abril 2025	135756
Mayo 2025	154121
Junio 2025	137472
Julio 2025	78502
Agosto 2025	92786
Septiembre 2025	164424
Octubre 2025	74524
Noviembre 2025	123254
Diciembre 2025	109540
Total acumulado	**1.480.132**

Tabla 45 Suma Instancias

Mes	Suma de Total Documentos
Enero 2025	149454
Febrero 2025	183729
Marzo 2025	193697
Abril 2025	180888
Mayo 2025	204354

Junio 2025	178790
Julio 2025	201882
Agosto 2025	190074
Septiembre 2025	208044
Octubre 2025	178349
Noviembre 2025	170835
Diciembre 2025	174277
Total acumulado	**2.211.873**

Tabla 46 Total Docs

Mes	Suma de Total radicados
Enero 2025	59197
Febrero 2025	70194
Marzo 2025	72317
Abril 2025	64370
Mayo 2025	73694
Junio 2025	63934
Julio 2025	79429
Agosto 2025	66811
Septiembre 2025	73473
Octubre 2025	66160
Noviembre 2025	58977
Diciembre 2025	**59671**
Total, acumulado	**808.227**

Tabla 47 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 48 Dimensionamiento Servers IBM - Virtualización Optima

- Estado de las 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.

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:

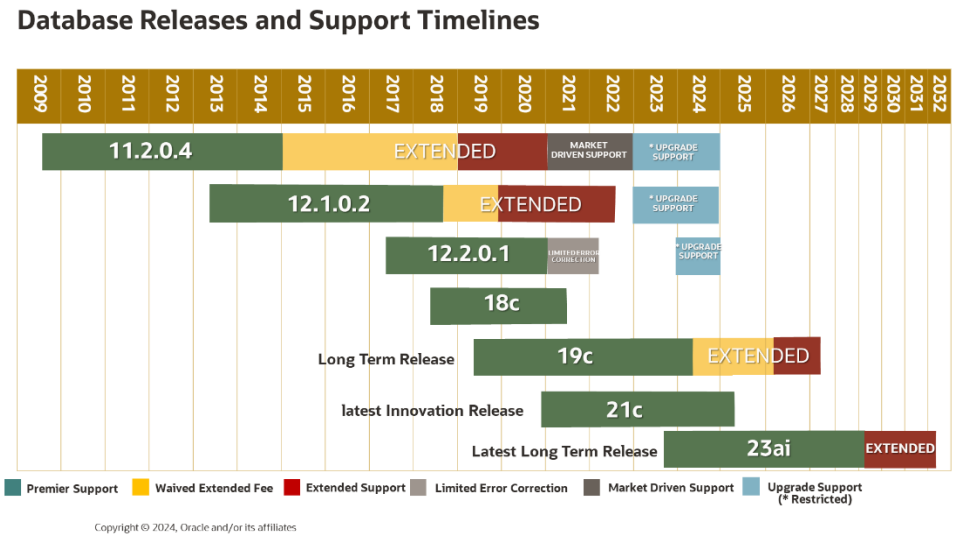


Ilustración 69 Estado Bases de Datos

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 49 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 ASIG 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	Oracle Linux	8	4	2225	1967	257

INST_NAME	IP	SERVER_NAME	AMBIENTE	Version_Motor	S.O	MEMORIA GB	CPU	STORAGE ASIG GB	STORAGE USED GB	STORAGE FREE GB
				Edition Release 12.1.0.2.0	4.9.2-6.2.0.3					
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 50 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 51 Escenario de Capacidades Oracle - Total de recursos empleados

1. TRASACCIONALIDAD BASES DE DATOS PRODUCTIVAS ODA X5-2:

1.1 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 70 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 71 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 72 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 73 Estadísticas Pool compartido

Tamaño base de datos MINSTRASG:

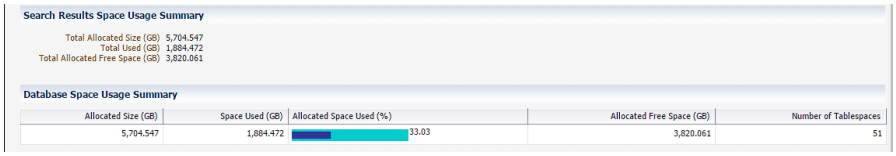


Ilustración 74 Tamaño DDBB

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
BRK	381,59
SGD	328,95
PDWDBA	195,48
AUDSYS	131,87
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 75 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

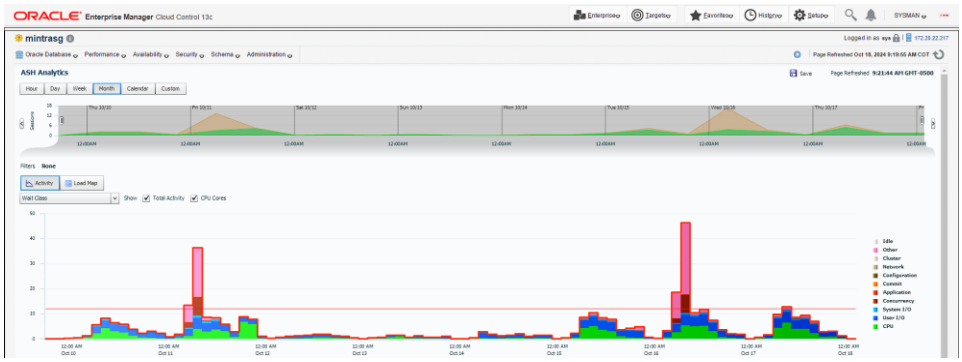


Ilustración 76 Rendimiento DDBB

1.2 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 77 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 78 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 79 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 80 Estadística Shared Pool

Tamaño base de datos DBMINTRA:

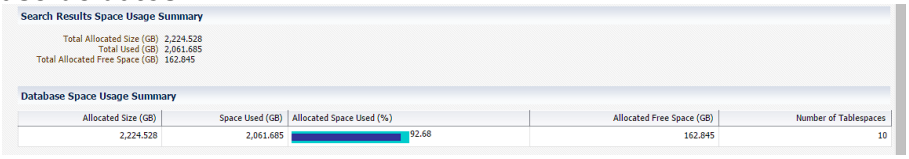


Ilustración 81 Tamaño DDBB DBMINTRA

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
IVCMT3	1936,81
NEWIVCMT	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 82 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

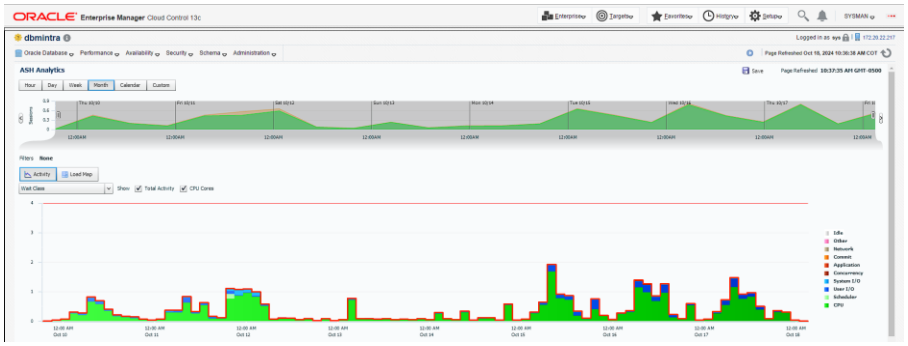


Ilustración 83 Rendimiento DDBB MINTRASG

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

1.3 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 84 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 85 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 86 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 87 Estadísticas Shared Pool

Tamaño base de datos PLIFERAY:

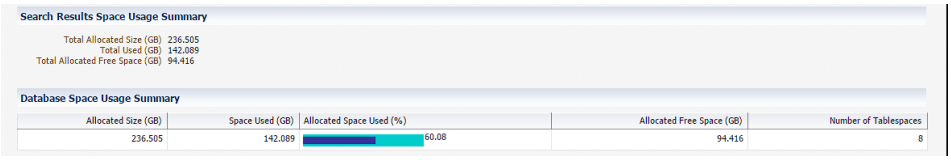


Ilustración 88 Tamaño DDBB PLifeRay

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 89 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

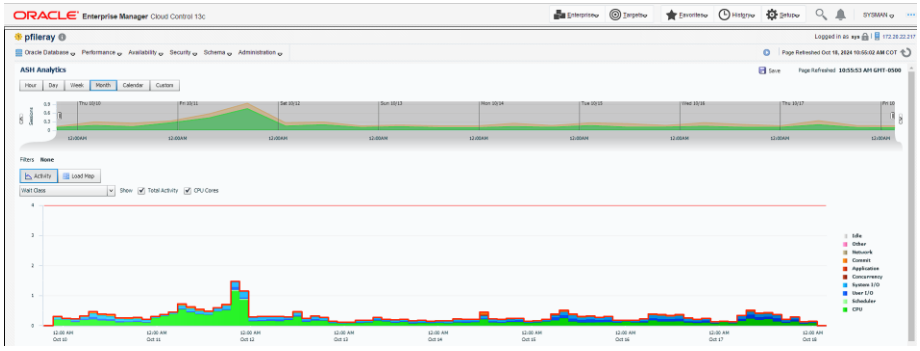


Ilustración 90 Rendimiento DDBB PlifeRay

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.

1.4 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 91 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:

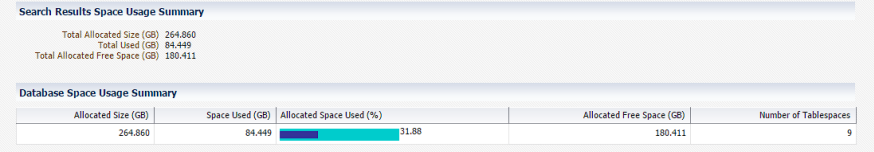


Ilustración 95 Tamaño DDBB SIGEP

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

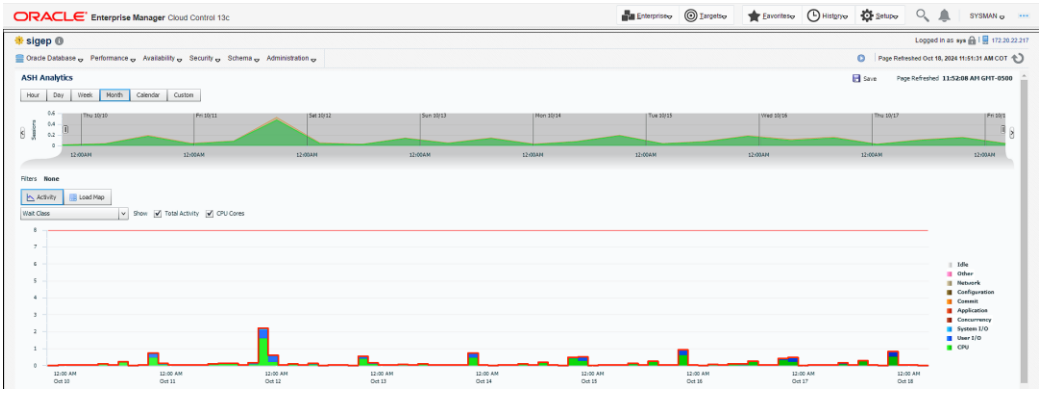


Ilustración 97 Rendimiento DDBB SIGEP

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.

1.5 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:

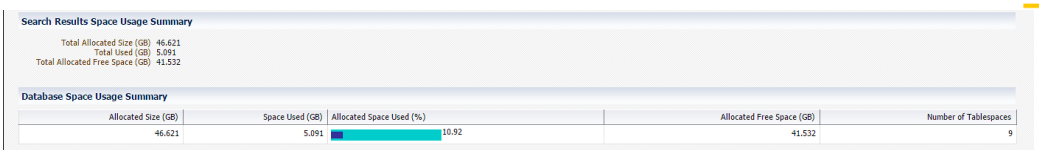


Ilustración 102 Tamaño DDBB SIMPC

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

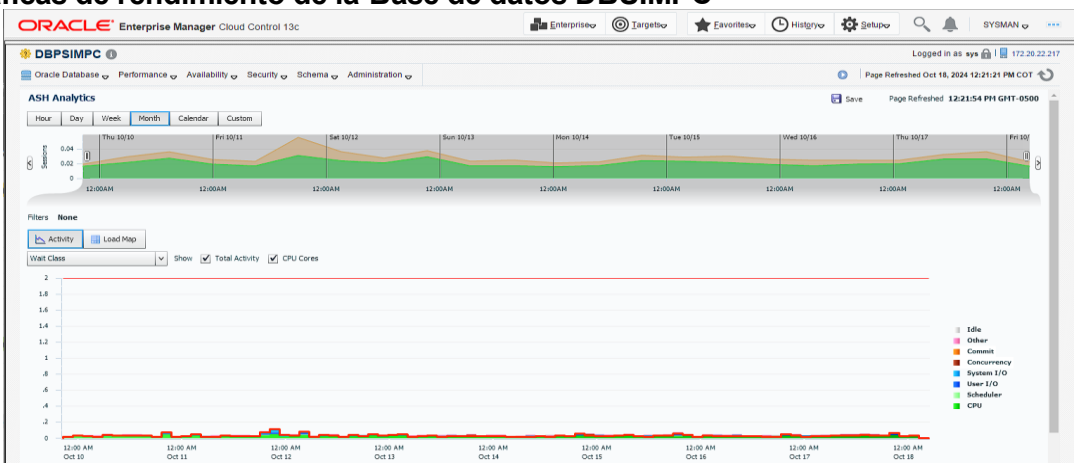


Ilustración 104 Rendimiento DDBB

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:

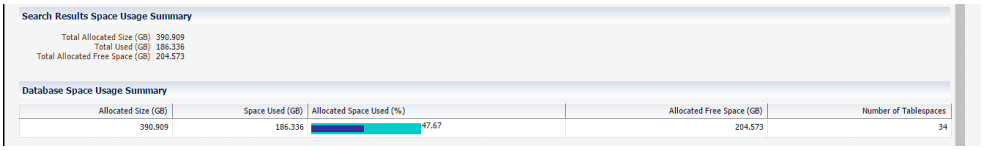
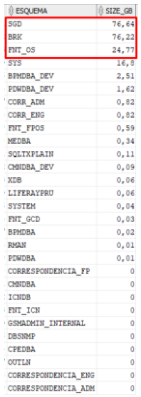


Ilustración 109 Tamaño DDBB MINTRASD

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:



ESQUEMA	SIZE_GB
SGD	76,64
BRK	76,22
FNT_OS	24,77
SYS	16,8
BPMDBA_DEV	2,51
PDWDBA_DEV	1,62
CORR_ADM	0,82
CORR_ENG	0,82
FNT_FPOS	0,59
MEDBA	0,34
SQLIXPLAIN	0,11
CMNDBA_DEV	0,09
XDB	0,06
LIFERAYPRU	0,06
SYSTEM	0,04
FNT_GCD	0,03
BPMDBA	0,02
RMAN	0,01
PDWDBA	0,01
CORRESPONDENCIA_FP	0
CMNDBA	0
ICNDB	0
FNT_ICN	0
GSMADMIN_INTERNAL	0
DBSNMP	0
CPEDBA	0
OUTLN	0
CORRESPONDENCIA_ENG	0
CORRESPONDENCIA_ADM	0

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

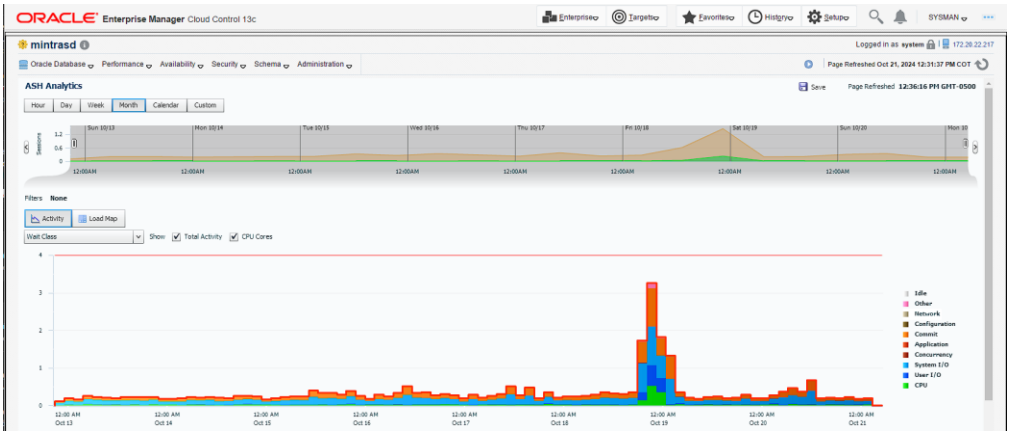


Ilustración 111 Rendimiento MINTRASD

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:

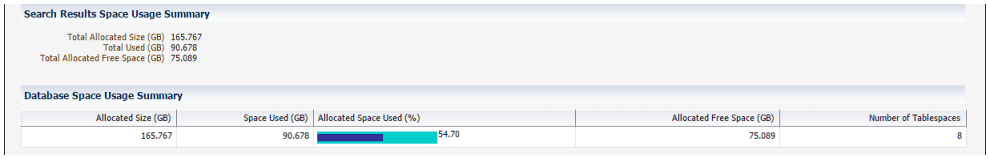


Ilustración 116 Tamaño DDBB

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	19,25
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

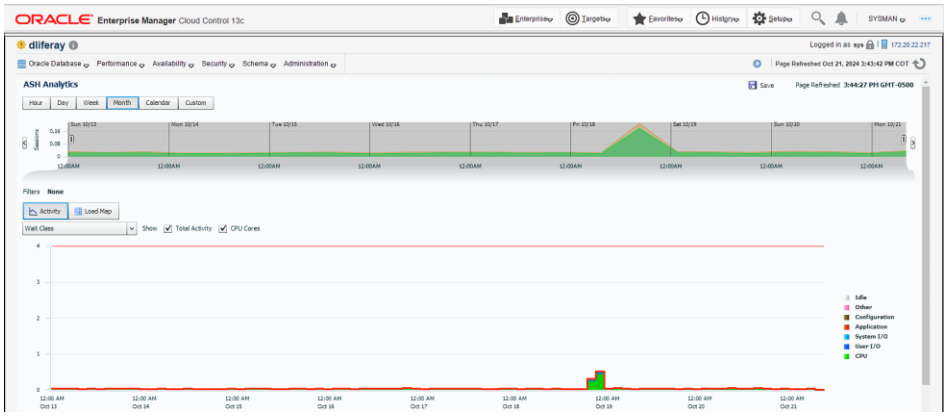


Ilustración 118 Rendimiento DDBB

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 Helena 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	DAMT	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

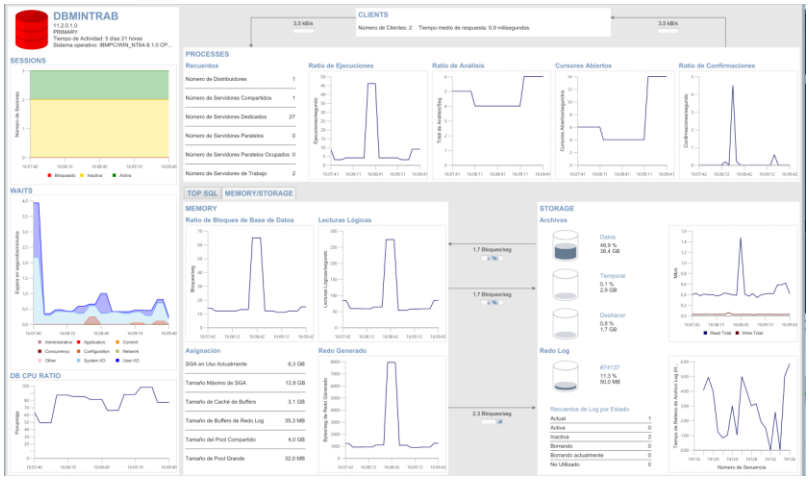


Ilustración 125 Rendimiento DDBB

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

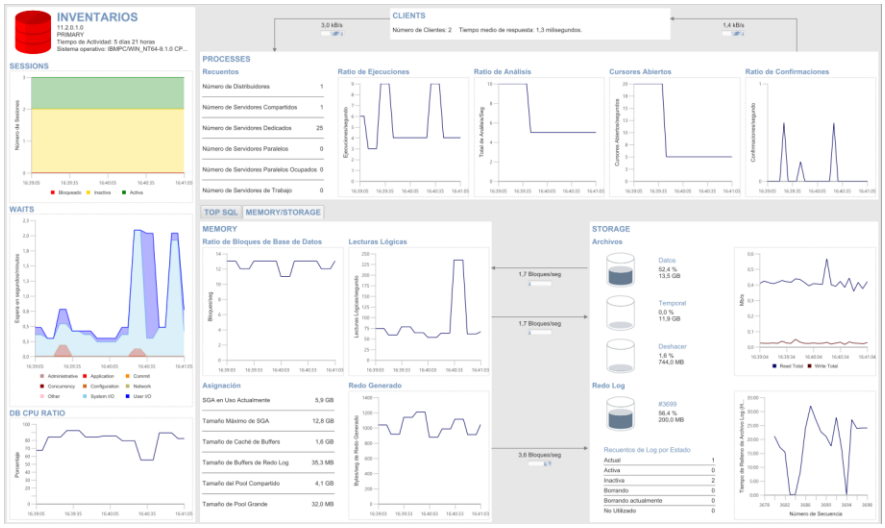


Ilustración 131 Comportamiento DDBB

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.

2. ALMACENAMIENTO GENERAL SERVIDOR ODA X5-2

4.1 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	45101056	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	8559304	-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:

Disk Groups | Clients | Space History | IO History

Lower Pane: Show Related Items

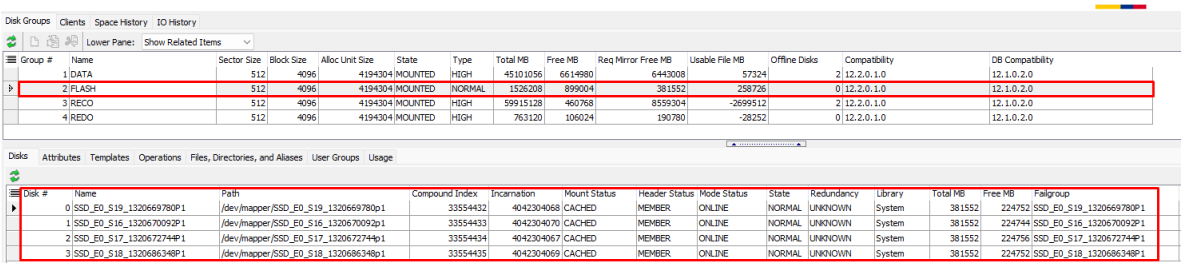
Group #	Name	Sector Size	Block Size	Alloc Unit Size	State	Type	Total MB	Free MB	Req Mirror Free MB	Usable File MB	Offline Disks	Compatibility	DB Compatibility
1	DATA	512	4096	4194304	MOUNTED	HIGH	45101056	6614980	6443008	57324	2	12.2.0.1.0	12.1.0.2.0
2	FLASH	512	4096	4194304	MOUNTED	NORMAL	1526208	899004	381552	258726	0	12.2.0.1.0	12.1.0.2.0
3	RECO	512	4096	4194304	MOUNTED	HIGH	59915128	460768	8559304	-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

Disks | Attributes | Templates | Operations | Files, Directories, and Aliases | User Groups | Usage

Disk #	Name	Path	Compound Index	Incarnation	Mount Status	Header Status	Mode Status	State	Redundancy	Library	Total MB	Free MB	Failgroup
0	HDD_E0_S06_1619686172P1	/dev/mapper/HDD_E0_S06_1619686172p1	16777216	4042304053	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	3221504	1047128	HDD_E0_S06_1619686172P1
1	HDD_E0_S05_1619902880P1	/dev/mapper/HDD_E0_S05_1619902880p1	16777217	4042304059	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	3221504	0	HDD_E0_S05_1619902880P1
2	HDD_E0_S00_1620030672P1	/dev/mapper/HDD_E0_S00_1620030672p1	16777218	4042304064	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	3221504	0	HDD_E0_S00_1620030672P1
3	HDD_E0_S02_1620706620P1	/dev/mapper/HDD_E0_S02_1620706620p1	16777219	4042304062	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	3221504	1048300	HDD_E0_S02_1620706620P1
4	HDD_E0_S03_1620804420P1	/dev/mapper/HDD_E0_S03_1620804420p1	16777220	4042304054	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	3221504	646308	HDD_E0_S03_1620804420P1
5	HDD_E0_S13_1620835760P1	/dev/mapper/HDD_E0_S13_1620835760p1	16777221	4042304058	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	3221504	108	HDD_E0_S13_1620835760P1
6	HDD_E0_S14_1620938348P1	/dev/mapper/HDD_E0_S14_1620938348p1	16777222	4042304055	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	3221504	645144	HDD_E0_S14_1620938348P1
8	HDD_E0_S08_1620999896P1	/dev/mapper/HDD_E0_S08_1620999896p1	16777224	4042304057	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	3221504	645508	HDD_E0_S08_1620999896P1
9	HDD_E0_S04_1621013384P1	/dev/mapper/HDD_E0_S04_1621013384p1	16777225	4042304066	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	3221504	0	HDD_E0_S04_1621013384P1
10	HDD_E0_S10_1621029540P1	/dev/mapper/HDD_E0_S10_1621029540p1	16777226	4042304060	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	3221504	645256	HDD_E0_S10_1621029540P1
12	HDD_E0_S12_1621032828P1	/dev/mapper/HDD_E0_S12_1621032828p1	16777228	4042304052	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	3221504	0	HDD_E0_S12_1621032828P1
13	HDD_E0_S09_1621286788P1	/dev/mapper/HDD_E0_S09_1621286788p1	16777229	4042304061	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	3221504	645520	HDD_E0_S09_1621286788P1
14	HDD_E0_S11_1621288500P1	/dev/mapper/HDD_E0_S11_1621288500p1	16777230	4042304056	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	3221504	645212	HDD_E0_S11_1621288500P1
15	HDD_E0_S07_1621289156P1	/dev/mapper/HDD_E0_S07_1621289156p1	16777231	4042304063	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	3221504	646496	HDD_E0_S07_1621289156P1

Ilustración 133 DiskGroup Data

DISKGROUP FLASH:



Disk Groups | Clients | Space History | IO History

Lower Pane: Show Related Items

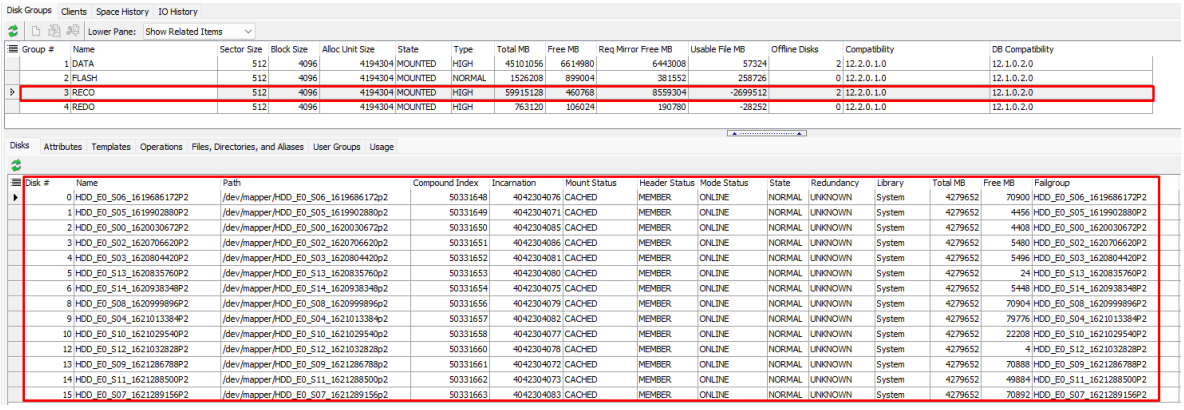
Group #	Name	Sector Size	Block Size	Alloc Unit Size	State	Type	Total MB	Free MB	Req Mirror Free MB	Usable File MB	Offline Disks	Compatibility	DB Compatibility
1	DATA	512	4096	4194304	MOUNTED	HIGH	45101056	6614980	6443008	57324	2	12.2.0.1.0	12.1.0.2.0
2	FLASH	512	4096	4194304	MOUNTED	NORMAL	1526208	899004	381552	258726	0	12.2.0.1.0	12.1.0.2.0
3	RECO	512	4096	4194304	MOUNTED	HIGH	59915128	460768	8559304	-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

Disks | Attributes | Templates | Operations | Files, Directories, and Aliases | User Groups | Usage

Disk #	Name	Path	Compound Index	Incarnation	Mount Status	Header Status	Mode Status	State	Redundancy	Library	Total MB	Free MB	Failgroup
0	SSD_E0_S19_1320669780P1	/dev/mapper/SSD_E0_S19_1320669780p1	33554432	4042304068	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	381552	224752	SSD_E0_S19_1320669780P1
1	SSD_E0_S16_1320670092P1	/dev/mapper/SSD_E0_S16_1320670092p1	33554433	4042304070	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	381552	224744	SSD_E0_S16_1320670092P1
2	SSD_E0_S17_1320672744P1	/dev/mapper/SSD_E0_S17_1320672744p1	33554434	4042304067	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	381552	224756	SSD_E0_S17_1320672744P1
3	SSD_E0_S18_1320686348P1	/dev/mapper/SSD_E0_S18_1320686348p1	33554435	4042304069	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	381552	224752	SSD_E0_S18_1320686348P1

Ilustración 134 DiskGroup Flash

DISKGROUP RECO:



Disk Groups | Clients | Space History | IO History

Lower Pane: Show Related Items

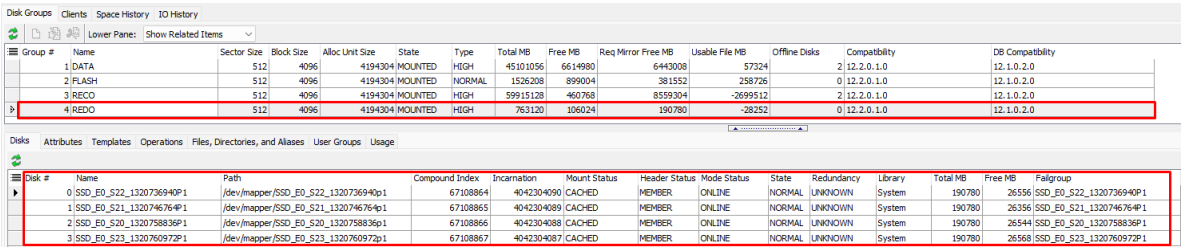
Group #	Name	Sector Size	Block Size	Alloc Unit Size	State	Type	Total MB	Free MB	Req Mirror Free MB	Usable File MB	Offline Disks	Compatibility	DB Compatibility
1	DATA	512	4096	4194304	MOUNTED	HIGH	45101056	6614980	6443008	57324	2	12.2.0.1.0	12.1.0.2.0
2	FLASH	512	4096	4194304	MOUNTED	NORMAL	1526208	899004	381552	258726	0	12.2.0.1.0	12.1.0.2.0
3	RECO	512	4096	4194304	MOUNTED	HIGH	59915128	460768	8559304	-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

Disks | Attributes | Templates | Operations | Files, Directories, and Aliases | User Groups | Usage

Disk #	Name	Path	Compound Index	Incarnation	Mount Status	Header Status	Mode Status	State	Redundancy	Library	Total MB	Free MB	Failgroup
0	HDD_E0_S06_1619686172P2	/dev/mapper/HDD_E0_S06_1619686172p2	50331648	4042304076	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	4279652	70900	HDD_E0_S06_1619686172P2
1	HDD_E0_S05_1619902880P2	/dev/mapper/HDD_E0_S05_1619902880p2	50331649	4042304071	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	4279652	4456	HDD_E0_S05_1619902880P2
2	HDD_E0_S00_1620030672P2	/dev/mapper/HDD_E0_S00_1620030672p2	50331650	4042304085	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	4279652	4408	HDD_E0_S00_1620030672P2
3	HDD_E0_S02_1620706620P2	/dev/mapper/HDD_E0_S02_1620706620p2	50331651	4042304086	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	4279652	5480	HDD_E0_S02_1620706620P2
4	HDD_E0_S03_1620804420P2	/dev/mapper/HDD_E0_S03_1620804420p2	50331652	4042304081	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	4279652	5496	HDD_E0_S03_1620804420P2
5	HDD_E0_S13_1620835760P2	/dev/mapper/HDD_E0_S13_1620835760p2	50331653	4042304080	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	4279652	24	HDD_E0_S13_1620835760P2
6	HDD_E0_S14_1620938348P2	/dev/mapper/HDD_E0_S14_1620938348p2	50331654	4042304075	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	4279652	5448	HDD_E0_S14_1620938348P2
8	HDD_E0_S08_1620999896P2	/dev/mapper/HDD_E0_S08_1620999896p2	50331656	4042304079	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	4279652	70904	HDD_E0_S08_1620999896P2
9	HDD_E0_S04_1621013384P2	/dev/mapper/HDD_E0_S04_1621013384p2	50331657	4042304082	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	4279652	79776	HDD_E0_S04_1621013384P2
10	HDD_E0_S10_1621029540P2	/dev/mapper/HDD_E0_S10_1621029540p2	50331658	4042304077	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	4279652	22208	HDD_E0_S10_1621029540P2
12	HDD_E0_S12_1621032828P2	/dev/mapper/HDD_E0_S12_1621032828p2	50331660	4042304078	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	4279652	4	HDD_E0_S12_1621032828P2
13	HDD_E0_S09_1621286788P2	/dev/mapper/HDD_E0_S09_1621286788p2	50331661	4042304072	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	4279652	70888	HDD_E0_S09_1621286788P2
14	HDD_E0_S11_1621288500P2	/dev/mapper/HDD_E0_S11_1621288500p2	50331662	4042304073	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	4279652	49884	HDD_E0_S11_1621288500P2
15	HDD_E0_S07_1621289156P2	/dev/mapper/HDD_E0_S07_1621289156p2	50331663	4042304083	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	4279652	70892	HDD_E0_S07_1621289156P2

Ilustración 135 DiskGroup Reco

DISKGROUP REDO:



Disk Groups | Clients | Space History | IO History

Lower Pane: Show Related Items

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	45101056	6614980	6443008	57324	2	12.2.0.1.0	12.1.0.2.0
2	FLASH	512	4096	4194304	MOUNTED	NORMAL	1526208	899004	381552	258726	0	12.2.0.1.0	12.1.0.2.0
3	RECO	512	4096	4194304	MOUNTED	HIGH	59915128	460768	8559304	-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

Disks | Attributes | Templates | Operations | Files, Directories, and Aliases | User Groups | Usage

Disk #	Name	Path	Compound Index	Incarnation	Mount Status	Header Status	Mode Status	State	Redundancy	Library	Total MB	Free MB	Failgroup
0	SSD_E0_S22_1320736940P1	/dev/mapper/SSD_E0_S22_1320736940p1	67108864	4042304090	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	190780	26556	SSD_E0_S22_1320736940P1
1	SSD_E0_S21_1320746764P1	/dev/mapper/SSD_E0_S21_1320746764p1	67108865	4042304089	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	190780	26356	SSD_E0_S21_1320746764P1
2	SSD_E0_S20_1320758836P1	/dev/mapper/SSD_E0_S20_1320758836p1	67108866	4042304088	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	190780	26544	SSD_E0_S20_1320758836P1
3	SSD_E0_S23_1320760972P1	/dev/mapper/SSD_E0_S23_1320760972p1	67108867	4042304087	CACHED	MEMBER	ONLINE	NORMAL	UNKNOWN	System	190780	26568	SSD_E0_S23_1320760972P1

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

3.1.4 No aplica

3.1.5 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.

3.1.5.1 Firewalls de nueva generación

Durante diciembre de 2025, 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.

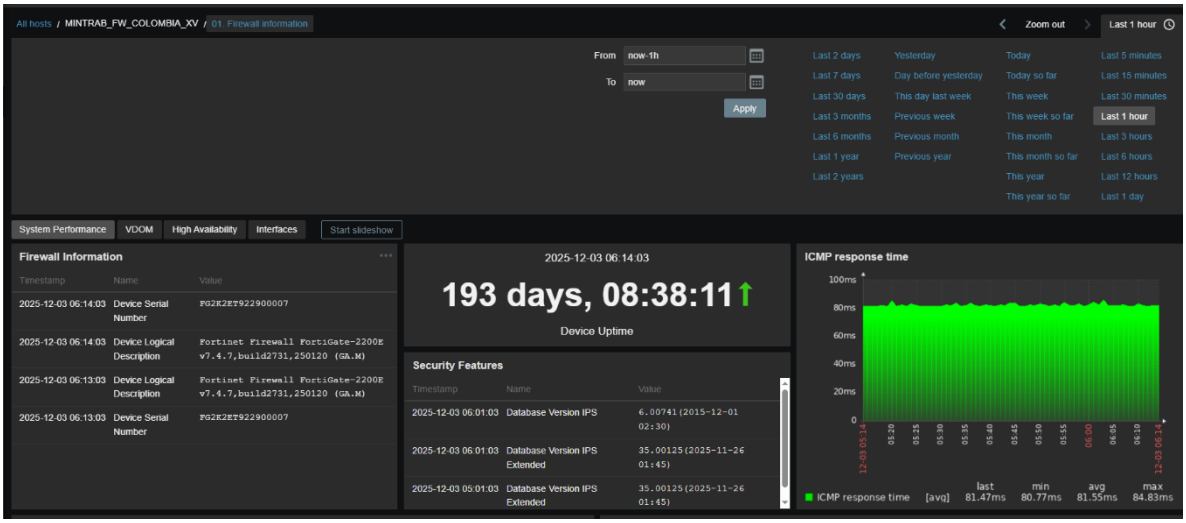


Ilustración *138* Firewall de nueva generación.

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 diciembre. 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 combinado diario (envío + recepción) oscila aproximadamente entre 3 TB y 10–12 TB, manteniéndose dentro de rangos operativos normales. El tráfico recibido predomina de forma consistente, lo que es coherente con un modelo de consumo de servicios externos y plataformas institucionales.
Tráfico recibido (azul)	Presenta variaciones periódicas con picos cercanos a 8–10 TB en días específicos. Este comportamiento es compatible con procesos de consumo de servicios en la nube, actualizaciones de plataformas gubernamentales 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 observan incrementos puntuales del tráfico recibido en fechas específicas del período, sin ruptura de tendencia. Estos picos son consistentes con ventanas operativas, procesos de actualización, sincronización o intercambio de datos con servicios como M365 y portales institucionales.
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	La curva refleja un entorno controlado, balanceado y sin signos de congestión, saturación ni actividad maliciosa. Desde una perspectiva de gestión del riesgo, el patrón observado se considera normal y aceptable, sin indicios de compromiso de la confidencialidad o integridad de la información.

Tabla 52 Tendencia de uso de ancho de banda

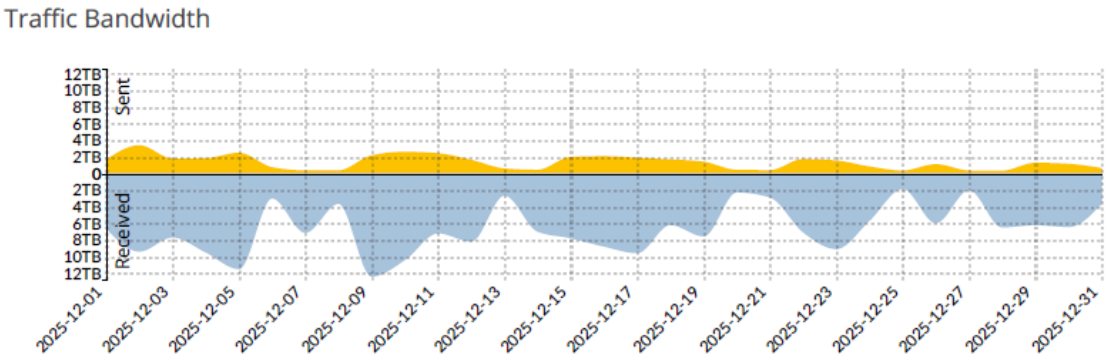


Ilustración 139 Comportamiento ancho de banda

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 diciembre. 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	**74.29 TB**	Tráfico extremadamente alto, servidor de almacenamiento, backup (MINTRABCKEXEC.mintrabajo.loc).
2	172.20.22.179	**8.93 TB**	Servidos de aplicaciones
3	172.28.28.38	**5.75 TB**	IP interna — podría corresponder a servidor de aplicaciones o gestión. Revisar patrón de uso.
4	Mduarteo	**5.08 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 53 usuarios con mayor consumo de ancho de banda

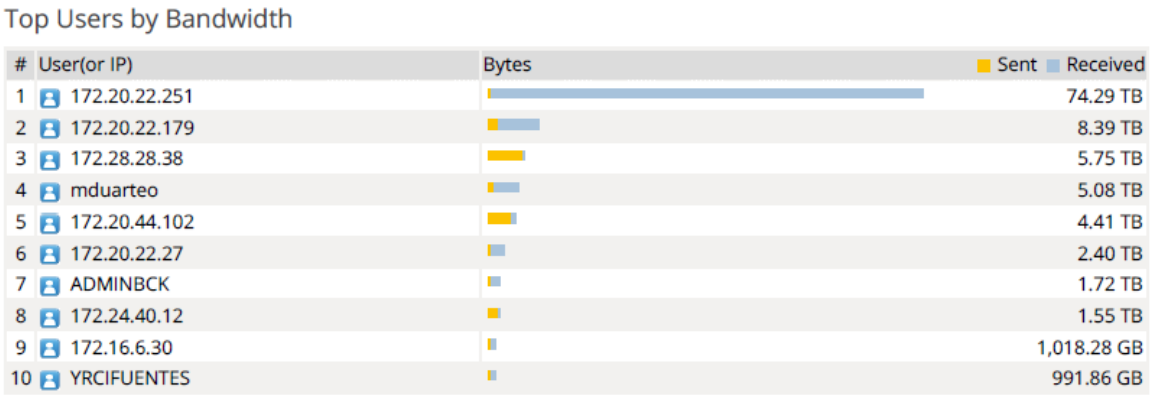


Ilustración 140 Tendencia de uso de ancho de banda

Top de usuarios por número de sesiones

La imagen corresponde al apartado "Top Users by Sessions" del informe perimetral de diciembre 2025 del Ministerio de Trabajo, donde se listan los usuarios o direcciones IP que generaron el mayor número de sesiones de red durante el periodo.

Top Users by Sessions

#	User (or IP)	Sessions
1	172.25.0.5	198,834,571
2	mduarteo	72,139,750
3	172.20.22.234	26,176,111
4	172.20.22.40	25,720,677
5	FORTINET	21,216,030
6	172.20.22.3	16,635,042
7	172.20.22.32	16,262,049
8	vulnerabilidadindra	14,821,287
9	192.168.133.203	13,152,443
10	172.20.22.228	11,767,342

Ilustración 141 Top de usuarios por números de sesiones

Análisis Top Users by Sessions

N°	Usuario/IP	Sesiones	Observaciones
1	**172.25.0.5**	**204.882.381**	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**	**81,081,991**	Usuario con actividad muy elevada. Puede estar vinculado a gestion de alguna plataforma(Mireya Duarte Osma)
3	**172.20.22.234**	**36,226,644**	Servidor interno asociado a un controlador de dominio.
4	**FORTINET**	**26,587,260**	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 54 Top de usuarios por sesiones

Top Applications by Bandwidth

La imagen corresponde al apartado “Top Applications by Bandwidth” del informe perimetral de diciembre 2025 del Ministerio de Trabajo. Este bloque muestra las aplicaciones o protocolos que más ancho de banda consumieron durante el mes, expresado en terabytes (TB), y diferenciando tráfico enviado (amarillo) y recibido (azul).

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	TCP/902			67.07 TB
2	HTTPS			40.76 TB
3	SMB			26.57 TB
4	TCP/445			13.53 TB
5	Microsoft.365.Portal			11.30 TB
6	SYSLOG			8.01 TB
7	tcp/1025			7.15 TB
8	TCP/1521			6.82 TB
9	Microsoft.SharePoint			5.92 TB
10	HTTP			5.23 TB

Ilustración 142 Top de aplicaciones

Aplicación	Tamaño	Descripción
1. TCP/902	67.07 TB	Puerto comúnmente usado para VMware ESXi (administración de máquinas virtuales). Indica alto volumen de sincronización o replicación de entornos virtualizados.
2. HTTPS	40.76 TB	Tráfico web cifrado — servicios cloud, correo, portales institucionales. Representa la base del tráfico corporativo seguro.
3. SMB (Server Message Block)	30.82 TB	Protocolo de compartición de archivos en red. Muestra alto uso de repositorios compartidos internos.
4. TCP/445	13.53 TB	Asociado también a SMB y autenticación Windows (Active Directory). Indica intenso intercambio de archivos y autenticaciones.
5. SYSLOG	8.01 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	6.45 TB	Tráfico no cifrado. Nivel bajo comparado con HTTPS, lo que refleja correcta adopción de canales seguros.
8. Microsoft.SharePoint	5.23 TB	Uso activo de bibliotecas documentales internas y colaboraciónen línea.

Tabla 55 Top de aplicaciones

Top 15 Authenticated Logins by VPN Connections

La imagen corresponde al apartado “Authenticated Logins” del informe perimetral de diciembre 2025 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	2025-12-01 07:01:21	155	219:37:21
2	cjimenez	ssl-tunnel	2025-12-01 07:04:39	119	102:25:03
3	aorozcoca	ssl-tunnel	2025-12-01 08:16:54	109	127:32:52
4	laldana	ssl-tunnel	2025-12-01 13:09:49	108	66:30:57
5	yjordan	ssl-tunnel	2025-12-01 00:06:15	89	234:33:36
6	ablanco	ssl-tunnel	2025-12-01 07:27:27	88	135:20:43
7	RMURCIA	ssl-tunnel	2025-12-01 10:20:22	87	116:04:15
8	eyreyes	ssl-tunnel	2025-12-01 08:30:05	73	189:23:37
9	fgonzalez	ssl-tunnel	2025-12-01 07:42:18	72	91:29:45
10	dfdiazd@noc_indra	ssl-tunnel	2025-12-01 06:51:37	68	457:35:35
11	bcasas	ssl-tunnel	2025-12-01 00:04:02	66	34:18:54
12	mcarrascal	ssl-tunnel	2025-12-01 19:55:40	66	83:32:36
13	jmaestre	ssl-tunnel	2025-12-01 09:54:09	65	70:49:02
14	dortizt	ssl-tunnel	2025-12-02 18:20:12	65	95:37:59
15	dporrasm	ssl-tunnel	2025-12-01 12:02:35	60	178:48:14

Ilustración 143 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: dfdiazd@noc_indra (457:35:35 h), yjordan (234:33:36 h), contaccenter (219:37:21 h), eyreyes (189:23:37 h) y dprorrasm (178:48:01 h). Este patrón es consistente con operación continua, soporte crítico y funciones tipo SOC/NOC.
Mayor duración total	El usuario dfdiazd@noc_indra presenta la mayor duración acumulada (457 horas, ~19 días), lo que indica un rol operativo permanente, asociado a monitoreo, administración o soporte 24/7.
Mayor cantidad de conexiones	Los usuarios con más reconexiones registradas son: contaccenter (155 conexiones), cjimenez (119), aorozcoca (109), laldana (108) y yjordan (89). Este comportamiento es típico de personal operativo con múltiples turnos o reconexiones diarias.
Duraciones elevadas (>200 h)	Se identifican usuarios con actividad superior a 200 horas: dfdiazd@noc_indra, yjordan y contaccenter. Estos accesos deben estar formalmente justificados y documentados dentro de los roles operativos autorizados.
Duraciones medias (100 h – 200 h)	Usuarios con uso estable y recurrente de la VPN: eyreyes (189 h), dprorrasm (178 h), ablanco (135 h), aorozcoca (127 h), RMURCIA (116 h) y cjimenez (102 h). Corresponden a trabajo remoto habitual y soporte técnico recurrente.

Duraciones bajas (<100 h)	Usuarios con accesos más puntuales u ocasionales: fgonzalez (91 h), mccarrascsl (83 h), jmaestre (70 h), laldana (66 h), bcasas (34 h). Indican uso esporádico o tareas específicas de soporte.

Tabla 56 Consolidado de indicadores

Failed Login Attempts by User

Esta imagen corresponde al apartado “Failed Login Attempts” del informe perimetral de diciembre 2025 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	18,030
2	administrator	ssl-web	1,597
3	support	ssl-web	1,016
4	User	ssl-web	807
5	test	ssl-web	746
6	scanner	ssl-web	632
7	scan	ssl-web	593
8	test1	ssl-web	593
9	Test1	ssl-web	520
10	sales	ssl-web	489

Ilustración 144 sesiones fallidas

Análisis
Durante diciembre 2025 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.

3.1.5.2 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 diciembre de 2025, 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	*56*	0	*56*
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	56	0	*56*

File Scan - Last 4 Weeks

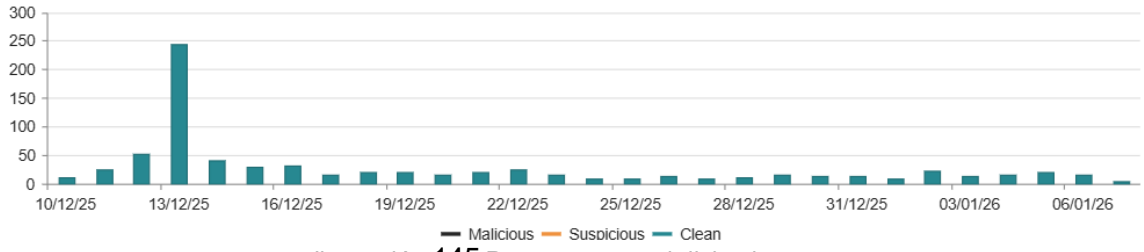


Ilustración 145 Reporte mensual diciembre

Este informe de rendimiento proporciona un análisis detallado del comportamiento y la eficiencia de FortiSandbox durante el mes de diciembre. 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 146 Captura de pantalla perfomance

Licencia Sandbox

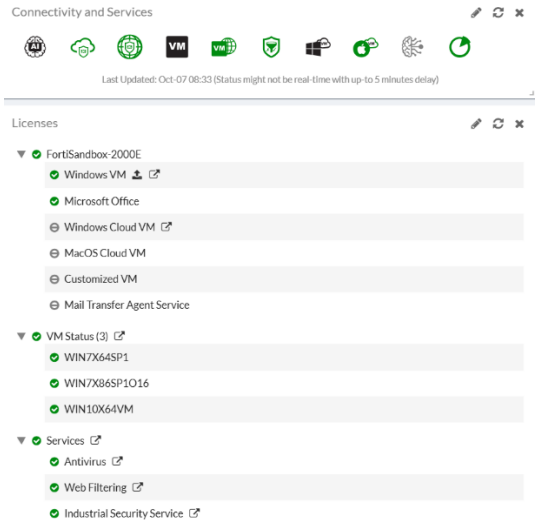


Ilustración 147 licencia sandbox

3.1.5.3 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 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 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 148 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 149 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.

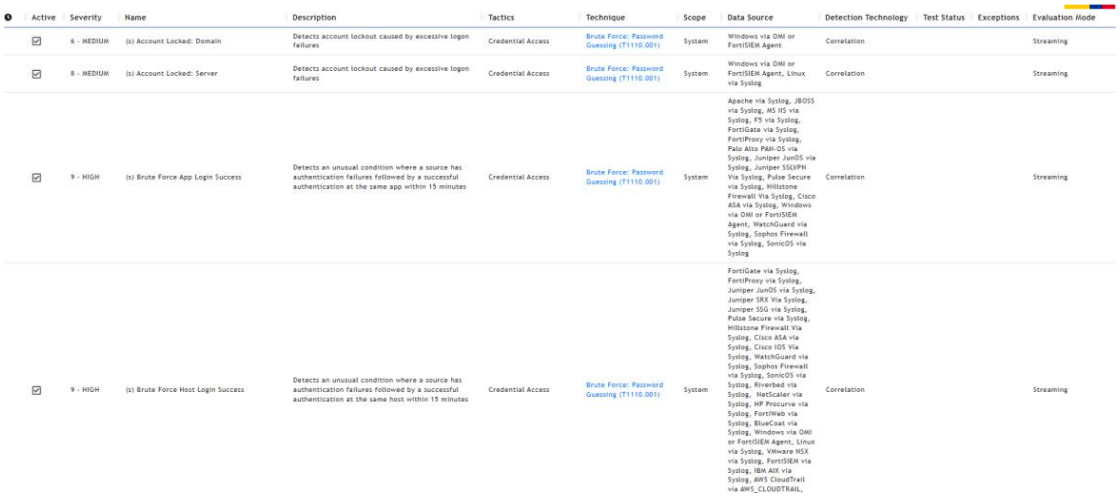
Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☐	4 - LOW	(s) Auto Service Stopped	Detects that an automatically running service stopped. Currently this works for windows servers and is detected via WMI.	Impact	Service Stop (T1489)	System	Windows Performance monitoring via FortiSIEM Agent/OM	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 150 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:

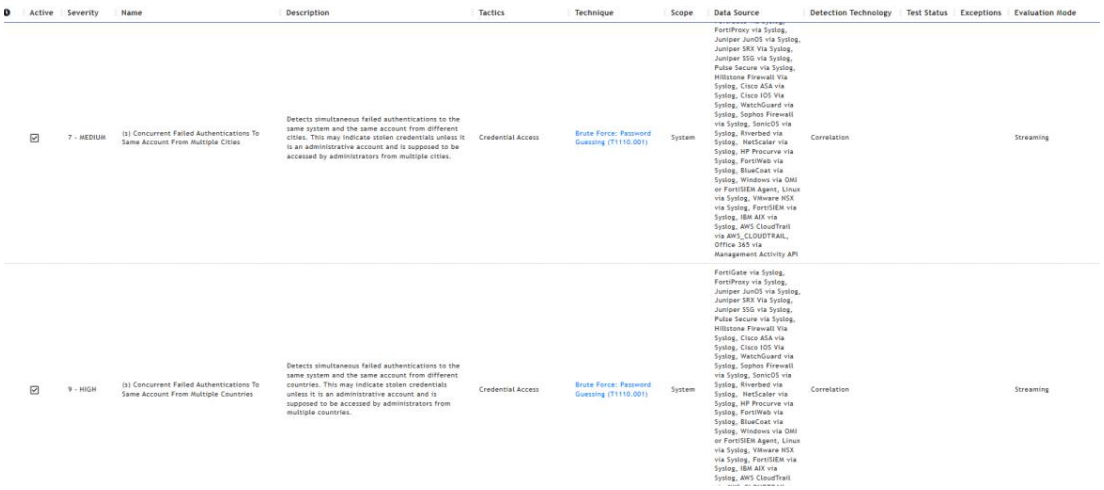
Los casos de uso de seguridad de autenticación en el FortiSIEM se centran en garantizar la integridad y la autenticidad de las credenciales de usuario en todos los dispositivos que tienen instalado el agente. Se muestran los casos Autenticación configurados para el ministerio de trabajo:



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 151 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 152 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 153 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 diciembre se registraron:

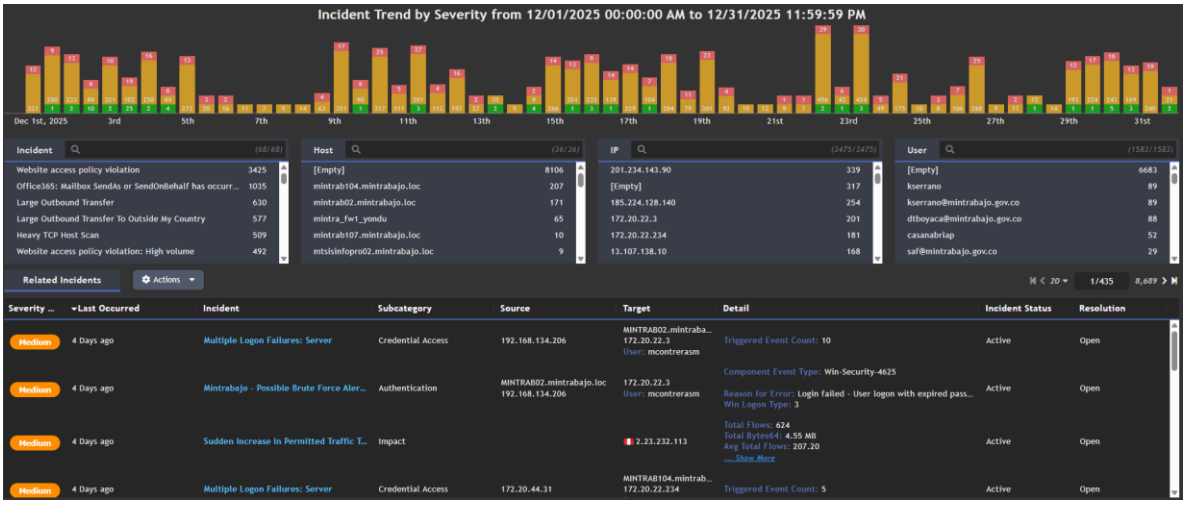


Ilustración 154 Detalle de incidentes

Análisis de incidentes

Tipo de incidente	Descripción	Volumen	Observaciones
Violaciones de política web	Accesos a categorías o sitios no permitidos por la política institucional	3.425	Incidente más frecuente. Requiere refuerzo de concientización y revisión de reglas de filtrado web.
Actividad Office 365 (SendOnBehalf)	Envíos de correo desde buzones compartidos o delegados	1.035	Actividad válida, pero altamente sensible; requiere control de permisos, auditoría y alertas específicas.
Transferencias salientes de gran volumen	Excesivo tráfico outbound detectado	630	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	577	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	509	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 57 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 diciembre. 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 92 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.

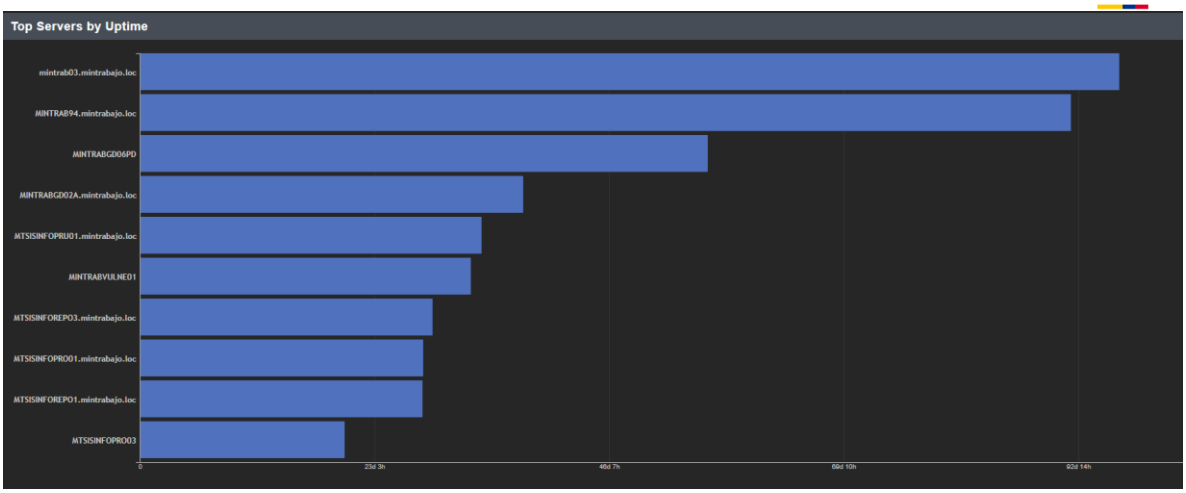


Ilustración 155 Detalle servidores

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.

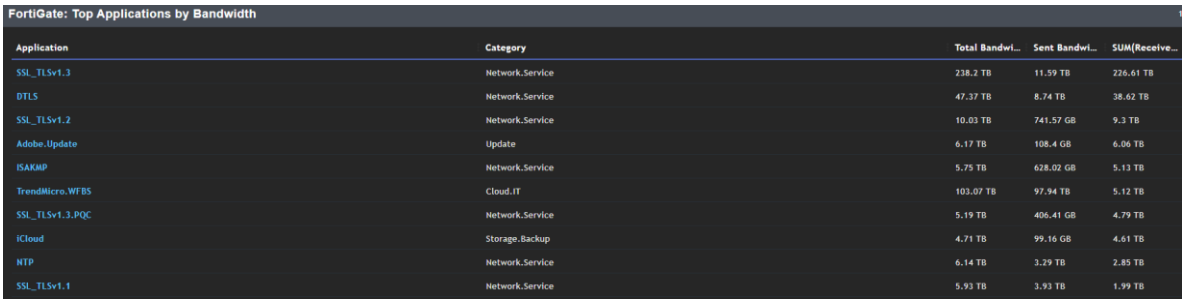
Este panel muestra que las aplicaciones que más ancho de banda consumieron fueron:

Consumo predominante:

- SSL/HTTPS: 226.61 TB
- DTLS: 53.07 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(Receive...
SSL_TLSv1.3	Network.Service	238.2 TB	11.59 TB	226.61 TB
DTLS	Network.Service	47.37 TB	8.74 TB	38.62 TB
SSL_TLSv1.2	Network.Service	10.03 TB	741.57 GB	9.3 TB
Adobe.Update	Update	6.17 TB	108.4 GB	6.06 TB
ISAKMP	Network.Service	5.75 TB	628.02 GB	5.13 TB
TrendMicro.WFBS	Cloud.IT	103.07 TB	97.94 TB	5.12 TB
SSL_TLSv1.3.PQC	Network.Service	5.19 TB	406.41 GB	4.79 TB
iCloud	Storage.Backup	4.71 TB	99.16 GB	4.61 TB
NTP	Network.Service	6.14 TB	3.29 TB	2.85 TB
SSL_TLSv1.1	Network.Service	5.93 TB	3.93 TB	1.99 TB

Ilustración 156 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.

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

Durante el mes de diciembre, 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.

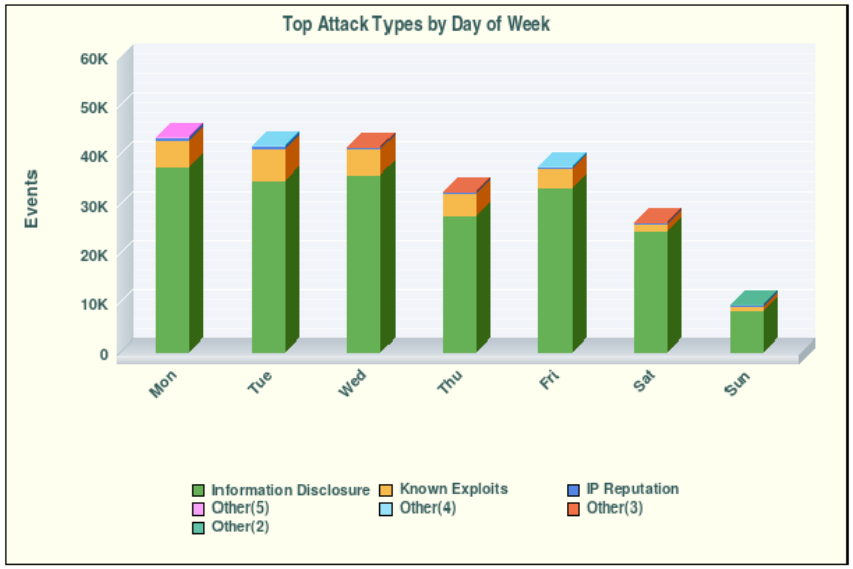


Ilustración 157 Top attack types

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**.

Ilustración 158 Tipo de ataque

3.1.5.5 Solución de Anti-DDoS

Durante el período del mes de diciembre, 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	85	6

Ilustración 159 Top de ataques

Análisis Detallado:

PAGINA_MINTRABAJO también muestra un número bajo de intentos salientes bloqueados (6), lo que sugiere riesgo bajo en aplicaciones web institucionales.

3.1.6.5.1 Login Fallidos

Durante el mes de diciembre, 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:

3.1.5.6 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:

3.1.5.6.1 Incidentes

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

3.1.5.6.2 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-172277	15/12/2025 14:22	Proceso desinstalación antivirus host BODSRIOS	SOC	Desinstalacion
RF-170675	9/12/2025 11:57	Solicitud Desbloqueo puertos USB	SOC	Habilitación Puertos USB
RF-170683	9/12/2025 12:18	Desbloqueo Puertos USB	SOC	Habilitación Puertos USB
RF-170734	9/12/2025 14:32	Solicitud Desbloqueo Puertos USB	SOC	Habilitación Puertos USB
RF-170735	9/12/2025 14:32	Solicitud DESBLOQUEO puertos USB	SOC	Habilitación Puertos USB
RF-170745	9/12/2025 14:41	Solicitud DESBLOQUEO puertos USB	SOC	Habilitación Puertos USB
RF-170747	9/12/2025 14:44	Solicitud DESBLOQUEO puertos USB	SOC	Habilitación Puertos USB
RF-171084	10/12/2025 13:54	Solicitud de habilitación de puertos del computador Funcionaria Andrea Usma Martinez Auxiliar Administrativo Grupo Atención al Ciudadano y Trámites	SOC	Habilitación Puertos USB
RF-171448	11/12/2025 11:05	DESBLOQUEO PUUERTOS USB	SOC	Habilitación Puertos USB
RF-171695	12/12/2025 6:58	Habilitar puerto USB	SOC	Habilitación Puertos USB
RF-171805	12/12/2025 11:09	Solicitud no bloqueo puertos USB Equipo Concepto Técnicos y Económicos	SOC	Habilitación Puertos USB
RF-171890	12/12/2025 14:28	RE: NECESIDAD DESBLOQUEO DE PUERTOS USB EN EQUIPOS DE LA TERRITORIAL CAQUETÁ	SOC	Habilitación Puertos USB
RF-172543	16/12/2025 11:03	Solicitud de habilitación de puertos USB para funcionaria	SOC	Habilitación Puertos USB
RF-172686	16/12/2025 15:54	SOLICITUD ACTIVACIÓN PUERTO USB WLOPEZ	SOC	Habilitación Puertos USB

RF-172858	17/12/2025 10:19	Solicitud de habilitación de puertos USB – Dirección Oficina Especial de Urabá-Apartadó	SOC	Habilitación Puertos USB
RF-172933	17/12/2025 13:52	SOLICITUD HABILITACIÓN PUERTOS EQUIPO DE COMPUT ESCRITORIO FREDDY MORALES	SOC	Habilitación Puertos USB
RF-172951	17/12/2025 14:41	Puertos UBS Secretaría General	SOC	Habilitación Puertos USB
RF-173155	18/12/2025 10:27	RV: solicitud activación puerto USB computador	SOC	Habilitación Puertos USB
RF-173272	18/12/2025 15:14	SOLICITUD PUERTOS USB-COMUNICACIONES	SOC	Habilitación Puertos USB
RF-173459	19/12/2025 11:31	RV: Solicitud de desbloqueo virtual - laboral	SOC	Habilitación Puertos USB
RF-173932	22/12/2025 9:53	Mintrabajo - Possible Brute Force Alert Windows - Evento 1139091	SOC	Seguridad Informática
RF-168905	1/12/2025 12:17	Solicitud permisos navegación	SOC	Agregar a sitios permitidos
RF-173179	18/12/2025 11:09	Solicitud de configuración y disponibilidad Firewall	SOC	Ajustar política
RF-170823	9/12/2025 17:32	Configuración Comunidad SNMPv3 Firewall F2200	SOC	Crear politica
RF-171484	11/12/2025 12:33	Solicitud enrutamiento sedes Remostas SDWAN	SOC	Permitir acceso
RF-171602	11/12/2025 15:29	RV: Desbloquear IPs para ingresar a Sitio web mintrabajo y rutec	SOC	Permitir acceso
RF-170587	9/12/2025 10:19	Solicitud Restricción Consumo Ancho de Banda IP 172.20.22.179	SOC	Restringir servicio
RF-169820	4/12/2025 9:00	Solicitud de habilitación de acceso a YouTube – Equipos DT Guajira	SOC	Asesoria - Consulta
RF-172573	16/12/2025 11:42	SOLICITUD INFORME EXCEPCIONES ACTIVACION USB	SOC	Reportes Seguridad Informática
RF-174235	23/12/2025 9:48	RE: MINTRABAJO | Validación Puertos - Comunicación Segmento 43	SOC	Ajuste de configuraciones (Crear - Eliminar)
RF-171103	10/12/2025 14:27	Correo sospechoso	SOC	Revisar correo malicioso
RF-171712	12/12/2025 8:08	RV: Curaçao: Sinta por você mesmo	SOC	Revisar correo malicioso
RF-174232	23/12/2025 9:37	RV: Sinta o ritmo do Caribe 🌴	SOC	Revisar correo malicioso
RF-170572	9/12/2025 10:03	FortiSIEM Alert: TLP:RED - Mintrabajo - Possible Brute Force Alert Windows	SOC	Accesos por fuerza bruta
RF-169431	3/12/2025 7:56	El Requerimiento No. RF-169408 se le ha solucionado	SOC	Análisis de Correos
RF-170694	9/12/2025 13:05	El Requerimiento No. RF-170663 se le ha solucionado	SOC	Análisis de Correos
RF-171869	12/12/2025 13:32	RV: Um destino, quatro formas de conhecer o Caribe 🌴 ✨	SOC	Análisis de Correos
RF-171870	12/12/2025 13:32	RV: ¡Lleve su infraestructura al siguiente nivel! 🚀 4 meses GRATIS de Colocation	SOC	Análisis de Correos
RF-172331	15/12/2025 16:06	Verificacion de correo electronico	SOC	Análisis de Correos
RF-170399	6/12/2025 9:27	FortiSIEM Alert: TLP:RED - Mintrabajo - Malware Alert Trend Micro - ANDCGONZALEZB	SOC	Análisis de Malware
RF-173338	18/12/2025 18:24	FortiSIEM Alert: TLP:RED - Mintrabajo - Office365: Suspicious File Type Uploaded	SOC	Análisis de evento
RF-173535	19/12/2025 15:16	FortiSIEM Alert: TLP:RED - Mintrabajo - Traffic to Emerging Threat IP List	SOC	Reporte de eventos
RF-173558	19/12/2025 16:04	No carga pagina especifica	SOC	Ajustes Proxy
RF-171379	11/12/2025 9:31	Eliminar equipo de la consola	SOC	Configuracion consola
RF-171767	12/12/2025 9:59	Solicitud de Licencia para desinstalar Antivirus	SOC	Configuracion consola
RF-172250	15/12/2025 13:21	Eliminación antivirus	SOC	Configuracion consola

RF-172474	16/12/2025 9:23	Solicitud de Licencia para desinstalar Antivirus	SOC	Configuracion consola
RF-175230	30/12/2025 14:32	Eliminar de la consola del antivirus	SOC	Configuracion consola
RF-173025	17/12/2025 16:11	Permiso de acceso a pagina	SOC	Crear Politicas
RF-171491	11/12/2025 13:08	RE: Solicitud enrutamiento sedes Remostas SDWAN	SOC	Ajuste de configuraciones (Crear - Eliminar)
RF-172630	16/12/2025 14:50	COLCERT AL-20251215 - 088 Alerta campaña de kits de Phishingen Colombia	SOC	Análisis de evento
RF-173945	22/12/2025 10:17	Solicitud verificación accesos a SIIF	SOC	Análisis de evento

Tabla 58 Reporte de requerimientos diciembre

3.1.5.7 Análisis de riesgo

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

- **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 59 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 60 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 61 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:

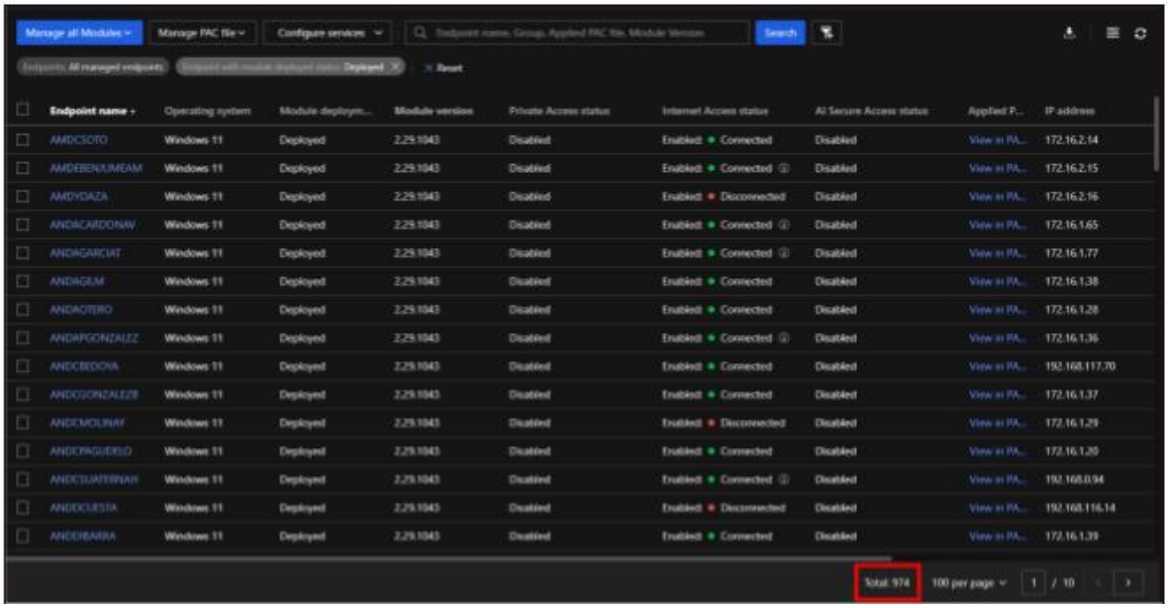
- Se están aplicando parches y actualizaciones de seguridad en la infraestructura de TI.
- Se realizó revisión periódica (semanal) de la matriz de vulnerabilidades y su priorización.
- Se realiza

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.

3.1.5.8 Políticas y procedimiento de seguridad

Dentro las activades realizadas en el mes de diciembre, 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

11/12/2025 – MINTRABAJO

Falla en Gogs permite sobreescritura de archivos y RCE (ejecución remota de código) sin autenticación
Riesgo: Ataques selectivos contra infraestructuras críticas.

9/12/2025 – MINTRABAJO
Boletín Lite // TI - JS#SMUGGLER: Campaña con iframes ocultos y JavaScript ofuscado orientada al despliegue de RATs.
Riesgo: Ataques selectivos contra infraestructuras críticas.

9/12/2025 – MINTRABAJO
Boletín Lite // TI - CastleRAT: Alerta de Backdoor sofisticado que utiliza la comunidad Steam como canal C2 encubierto para espionaje empresarial
Riesgo: Ataques selectivos contra infraestructuras críticas.

3.1.6 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 62 Licenciamiento

3.1.7 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 63 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 64 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 diciembre, no se observan caídas del canal, se tiene un consumo promedio de entrada de 31.1Mbps y 77.22 Mbps de salida.

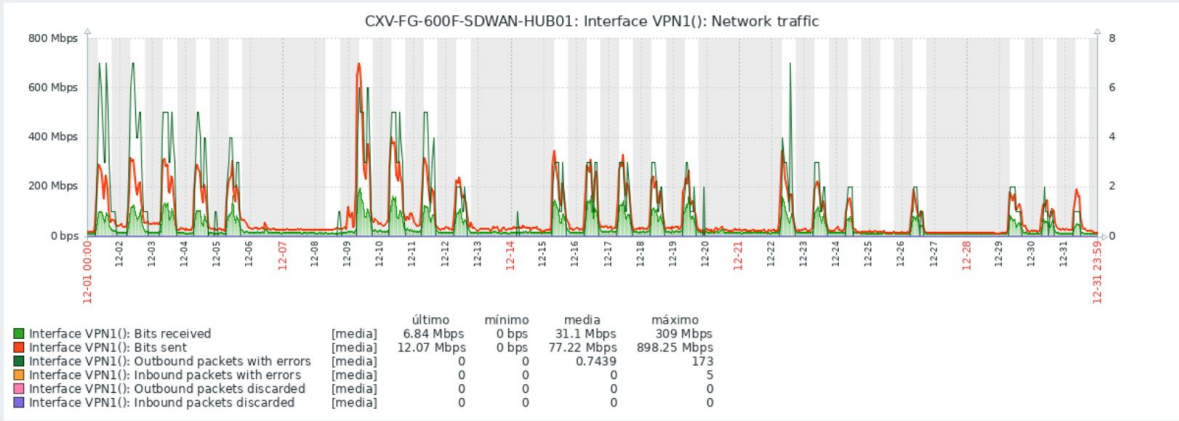


Ilustración 160 Consumo canal MPLS DC Principal

De igual forma se observa que el equipo del proveedor de servicios se encuentra operando de forma estable y no presentó reinicios.

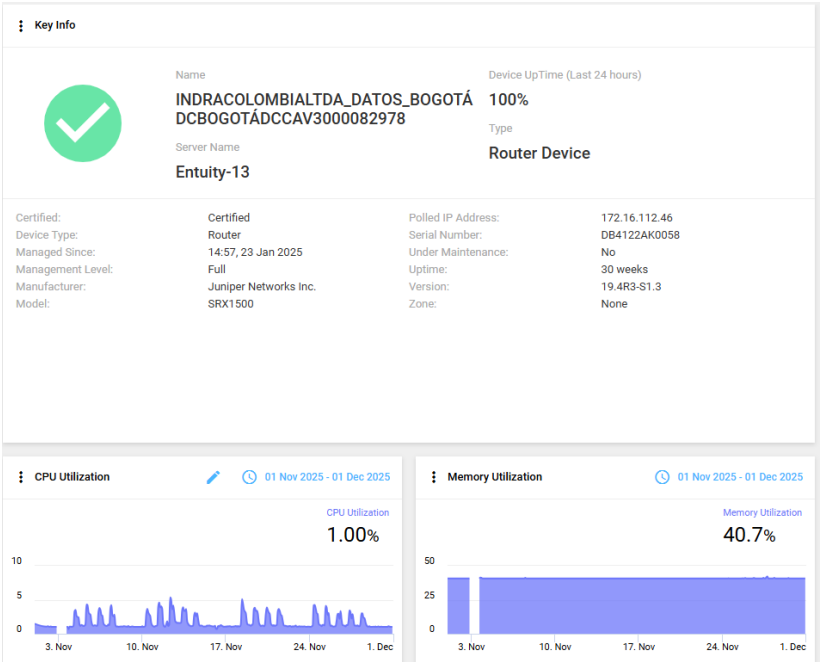


Ilustración 161 Estado Router MPLS DC Principal

3.3.1.1 Incidentes de Conectividad

Durante el mes de diciembre, 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 Arauca	98,67%	IM-170003
Sede Territorial Florencia	98,31%	IM-170437
Sede Territorial Quibdó	99,80%	IM-169935
Sede Territorial San Jose del Guaviare	99,86%	IM-168711
Sede Territorial Neiva	95,38%	IM-171859
Sede Centro Carrera 7 # 32 - 63	91,95%	IM-171450
Sede Territorial Cartagena	99,80%	IM-169933
Carmen De Bolivar	92,90%	IM-172033
Magangué	99,20%	IM-171115
Girardot	98,97%	IM-168922
Pitalito	99,14%	IM-170913
Puerto Gaitan	92,55%	IM-174620
Espinal	99,07%	IM-168850

Tabla 65 Incidentes de conectividad

3.3.1.2 Topología Actual

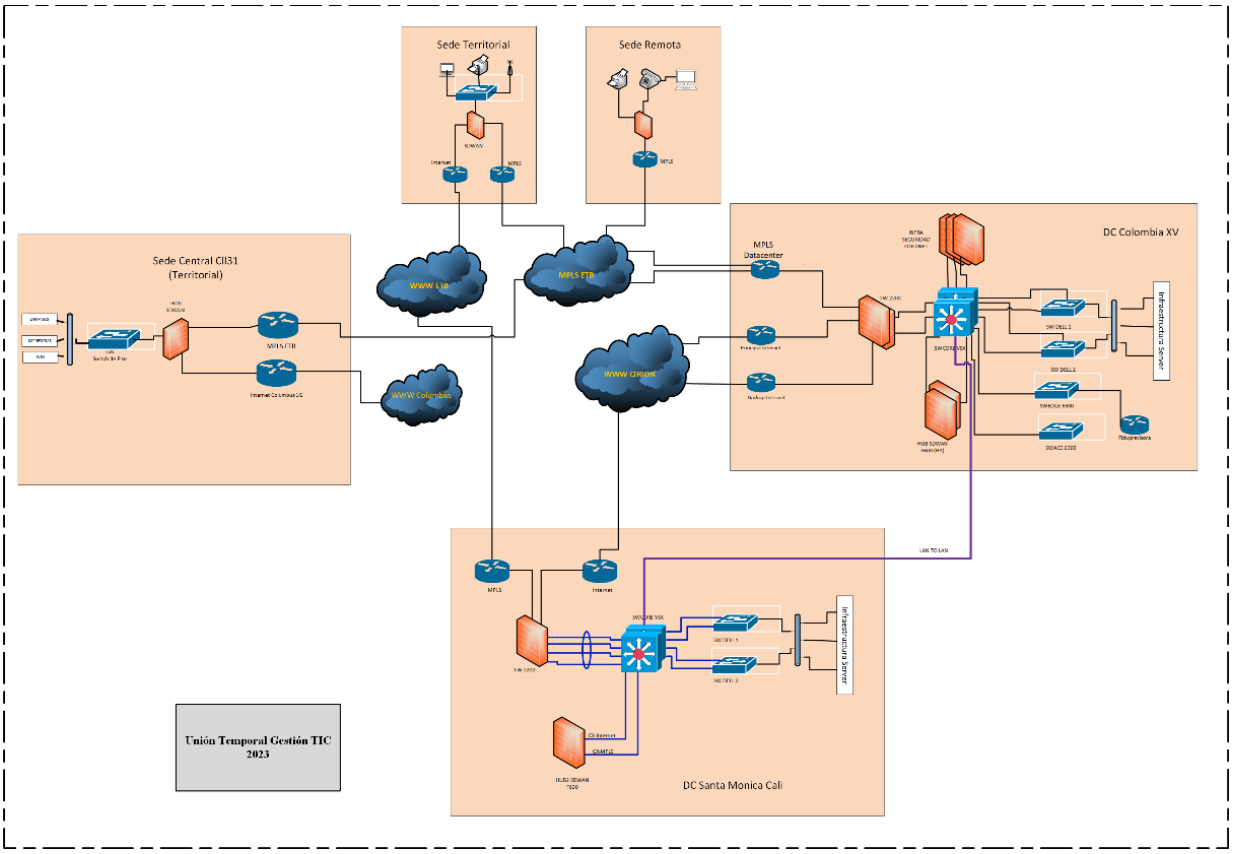


Ilustración 162 Topología actualizada

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.

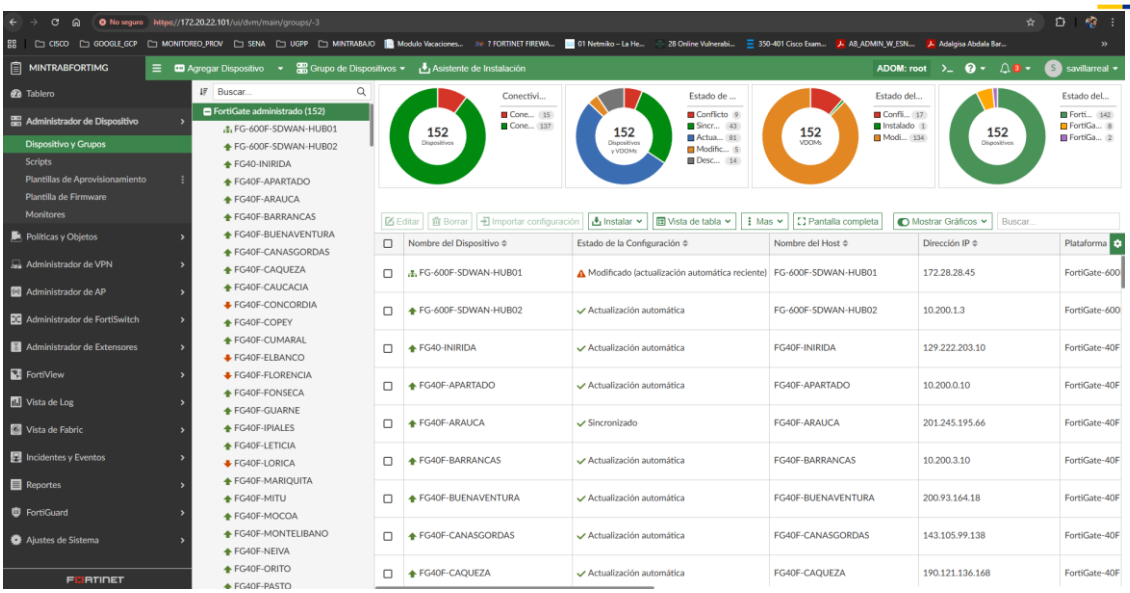


Ilustración 163 Interface Fortimanager

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 1.36 Gbps, este canal es de 2GB, con el tráfico generado se observa que no presentó saturación durante el mes

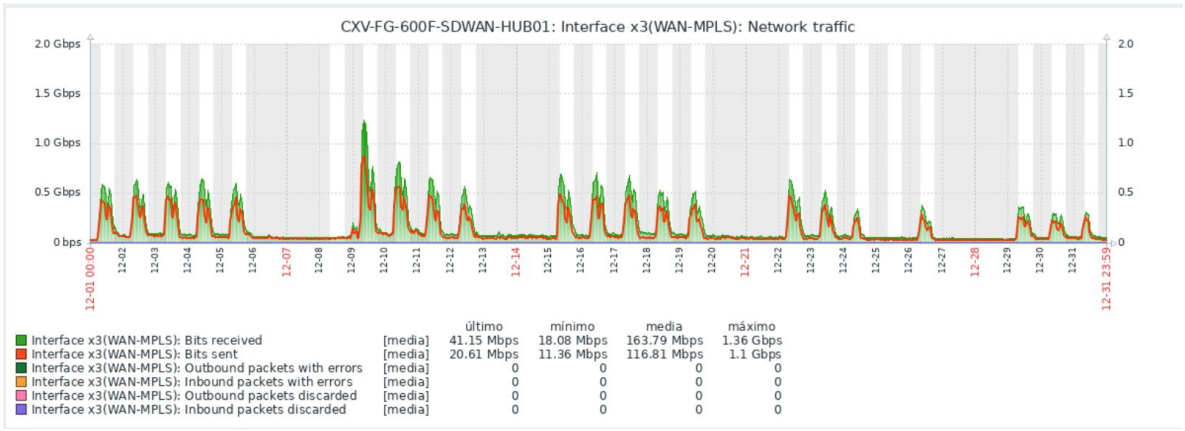


Ilustración 164 Interface MPLS HUB SDWAN

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 67.93Mbps de consumo en el mes donde se tuvo un máximo de 752.9 Mbps. Este canal es de 1GB, con el tráfico generado en el mes, no se presentó saturación.

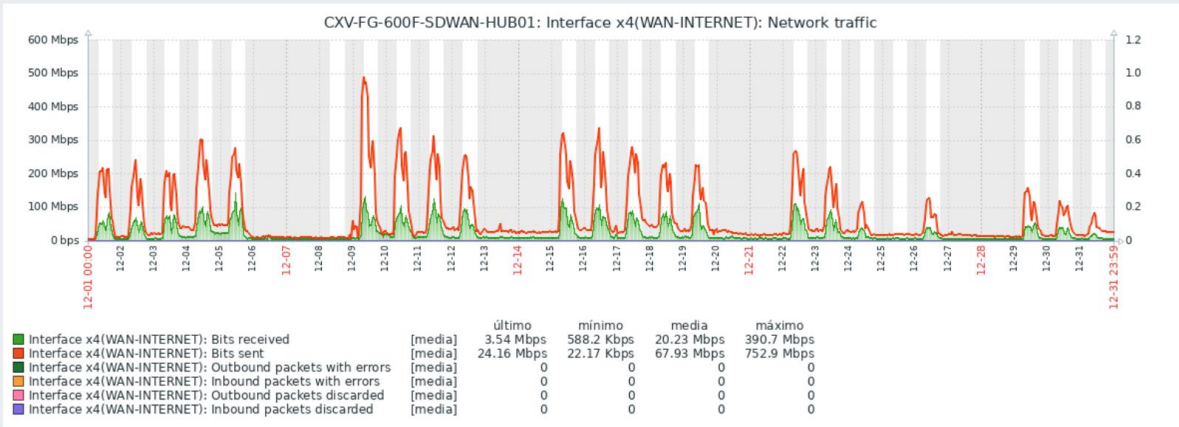


Ilustración 165 Interface Internet HUB SDWAN

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

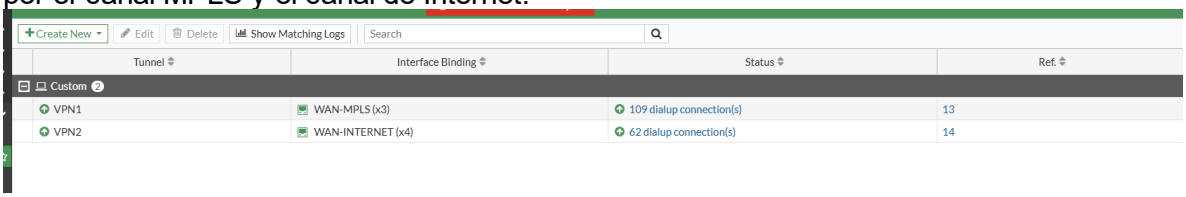
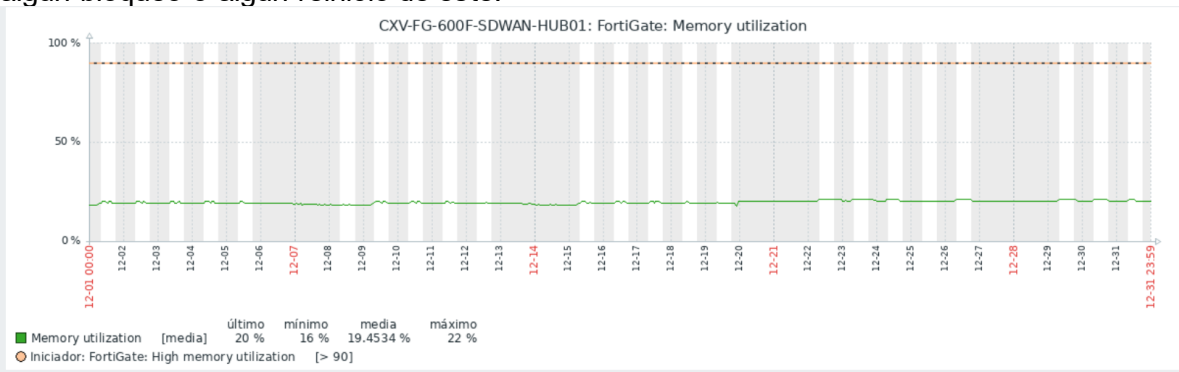


Ilustración 166 VPN SDWAN establecidas

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 8% de CPU, el equipo ha trabajado de forma estable sin presentar picos que causen algún bloqueo o algún reinicio de este.



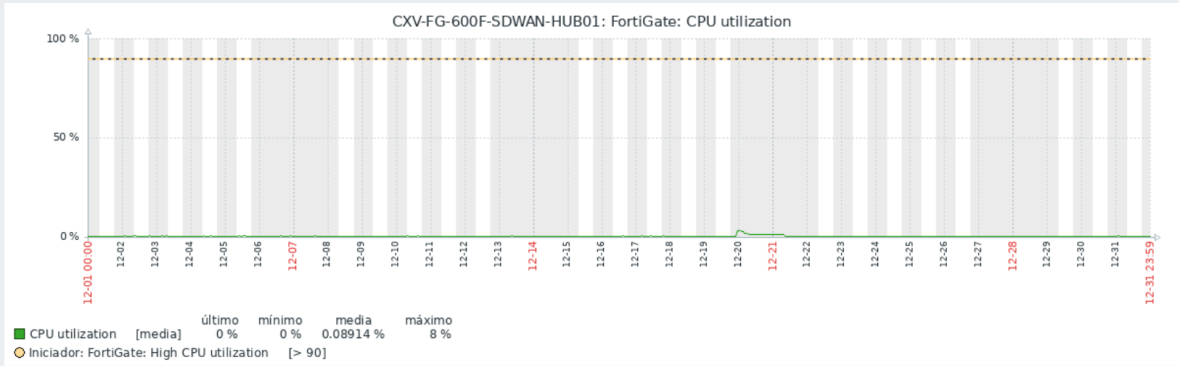


Ilustración 167 Estado HUB SDWAN Datacenter

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.

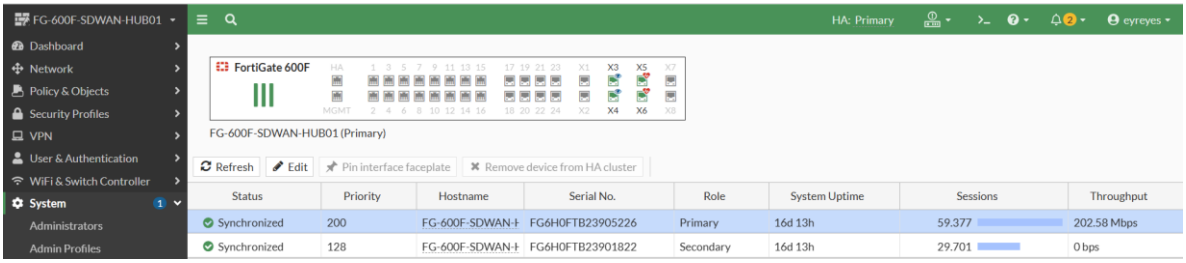


Ilustración 168 Estado HA HUB Sdwan

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

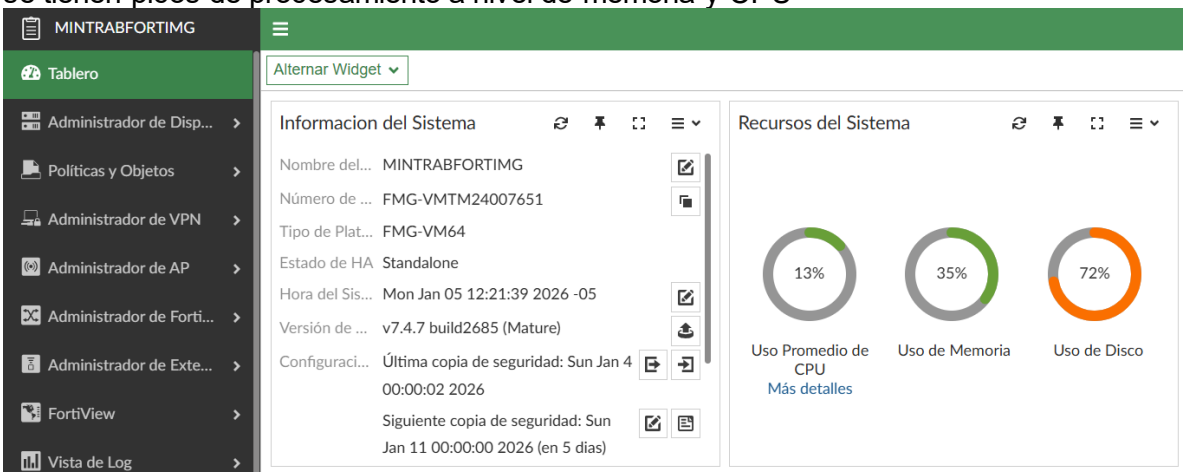


Ilustración 169 Recursos Fortimanager

Otras novedades del servicio:

Durante el mes de diciembre se realizaron las siguientes actividades:

- Se ajusto el consumo de ancho de banda en los servidores de backup de Colombia XV para evitar saturación del canal de internet.

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 66 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 Diciembre:

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

Dirección Territorial	% de Disponibilidad	Caso Asociado	% Penalidad	Valor Penalidad un enlace
Carmen De Bolivar	92,90%	IM-172033	10%	$ 30.801
Magangue	99,20%	IM-171115	3%	$ 9.240
Girardot	98,97%	IM-168922	3%	$ 9.240
Pitalito	99,14%	IM-170913	3%	$ 9.240
Puerto Gaitan	92,55%	IM-174620	10%	$ 30.801
Espinal	99,07%	IM-168850	10%	$ 30.801
Total				**$ 120.123**

Tabla 67 Desagregado sedes con novedad un solo enlace

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

Dirección Territorial	% de Disponibilidad	Caso Asociado	% Penalidad	Valor Penalidad doble enlace
Sede Territorial Arauca	98,67%	IM-170003	3%	$ 24.378
Sede Territorial Florencia	98,31%	IM-170437	3%	$ 24.378
Sede Territorial Quibdó	99,80%	IM-169935	3%	$ 36.567

Sede Territorial San Jose Del Guaviare	99,86%	IM-168711	3%	$ 12.189
Sede Territorial Neiva	95,38%	IM-171859	3%	$ 36.567
Sede Centro Carrera 7 # 32 - 63	91,95%	IM-171450	3%	$ 121.891
Sede Territorial Cartagena	99,80%	IM-169933	3%	$ 36.567
Total				**$ 292.537**

Tabla 68 Desagregado sedes con novedad con doble enlace

4 LINEA DE SERVICIOS EN SEDE

4.1 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 Almacen
Equipos de escritorio	**1172**	1145	27
Equipos portátiles	**1000**	956	164
Equipos portatiles adicionales	**120**		
Total	**2292**	**2101**	**191**

Tabla 69 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 DICIEMBRE		
SEDE	**TIPO DE ELEMENTO**	**CANTIDAD**
Nivel Central	Portátil	4
Nivel Central	Escritorio	5
DT Valle del Cauca	Portátil	2
TOTAL		**11**

Tabla 70 Cantidades de equipos asignados nivel nacional

DEVOLUCION DE EQUIPOS DICIEMBRE		
SEDE	**TIPO DE ELEMENTO**	**CANTIDAD**
DT Antioquia	Portátil	1
DT Antioquia	Escritorio	1
Nivel Central	Portátil	32
Nivel Central	Escritorio	3
DT Santander	Escritorio	1
DT Tolima	Escritorio	3
TOTAL		**41**

Tabla 71 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 diciembre, se reportó un total de 15 casos de garantía. A continuación, se detallan los estados asociados a estos casos:

Estado de caso	Cantidad
Cerrado	6
Suspendido	9
Total	15

Tabla 72 Estado de casos de garantía.

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

ANS	Cerrado	Suspendido	Total
CUMPLE	6	8	14
NO CUMPLE		1	1
Total	6	9	15

Tabla 73 ANS casos de garantía.

Fecha de Reporte	Serial	Parte	Falla	Sede	No. Caso	Estado
2/12/2025	VNAA62CV	Monitor	Garantía Monitor S-N VNAA62CV por fallas, se generan pixelada vertical en la pantalla	Cerete	RF-169247	Suspendido
3/12/2025	PW0A3BP	Portátil	Solicitud de garantía – Equipo portátil Lenovo 14 G6 ABP (Serial: PW0A3BPB)	DT Valle del Cauca	RF-169650	Suspendido
9/12/2025	HC3BBLX3	Diadema	Falla diadema - HC3BBLX3	DT Antioquia	RF-170790	Cerrado

Fecha de Reporte	Serial	Parte	Falla	Sede	No. Caso	Estado
10/12/2025	HC3BBMMB	Diadema	Falla general diadema - HC3BBMMB	B/Bermeja	RF-170984	Cerrado
11/12/2025	VNAA64AC	Monitor	Garantía Monitor S-N VNAA64AC por fallas, se generan pixelada vertical en la pantalla	DT Santander	RF-171475	Suspendido
14/12/2025	VNAA62LP	Monitor	Solicitud de garantía de pantalla ThinkVision E24-30-VNAA62LP	Sevilla	RF-172025	Suspendido
16/12/2025	HC3BBM3K	Diadema	Diadema no suena HC3BBM3K	DT Bogotá	RF-172457	Cerrado
18/12/2025	HC3BBN82	Diadema	garantía diadema “HC3BBN82 "	Nivel central	RF-173086	Cerrado
19/12/2025	PW0A3CKM	Portátil	Reporte hurto computador portátil	Quindío	RF-173397	Suspendido
19/12/2025	VNAA61ZC	Monitor	Garantía Monitor S-N VNAA61ZC por falla, se generan pixelada horizontal en la pantalla	Montería	RF-173571	Suspendido
22/12/2025	PW0A3AZW	Portátil	Funcionaria reporta Hurto de equipo PW0A3AZW	Nivel central	RF-174012	Suspendido
23/12/2025	MJ0LS5QY	Escritorio	Garantía equipo escritorio	Chiquinquirá	RF-174276	Suspendido
23/12/2025		Escritorio	Copia denuncia Penal Número de radicado # 2025122301404	DT Santander	RF-174405	Cerrado
24/12/2025	MJ0LS5CD	Escritorio	Reporte Hurto CPU MJ0LS5CD	B/Manga	RF-174468	Suspendido
26/12/2025	HC3BBMX6	Diadema	Falla audio diadema HC3BBMX6	Nivel central	RF-174681	Cerrado

Tabla 74 ANS Relación casos de garantía

- **Siniestros por daño y hurto:**

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

Funcionario responsable	Serial	DT	Parte afectada	Estado	Caso Aseguradora/ Lenovo
Muñoz Suescun Yiseth Andrea	PW0A3BE0	DT Cauca	Derrame de líquidos	Aseguradora 08/04/2025// Aseguradora realizó entrega de portátil en Bogotá con serial PW0A3BMM	PRG_2025_1221329
Pavel Santodomingo	PW0A3CDZ	Nivel Central	Derrame de líquidos	Aseguradora realizó la reposición del equipo con serial PW0A3BP1 se hace devolución de equipo dañado	PRG_2025_3256134/2025046910//2023159675
Bernardo Ardila Fernández	PW09Z34H	Valledupar	Golpes en esquinas	Aseguradora hace entrega de equipo 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

Funcionario responsable	Serial	DT	Parte afectada	Estado	Caso Aseguradora/ Lenovo
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	
Silvia Patricia Rojas Ardila	MJ0LS5CD	B/manga	Robo	Se envía documentación para trámite ante aseguradora.	

Tabla 75 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 15 solicitudes tipificadas así:
  - Incidentes: 0 casos
  - Requerimientos: 15 casos

- Al corte de mes quedaron en estado:
  - Cerrado: 6 casos.
  - Suspendido: 9 casos.

- 13 casos corresponden a solicitudes de usuarios estándar y 2 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
Total, general	15

Tabla 76 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	**15**
Equipo Periférico	8
Equipo Escritorio	4
Equipo Portátil	3
Total	15

Tabla 77 Solicitudes de Equipos Usuario Final – Según Grupo Responsable

4.1.1 Equipos de Escritorio

Durante el mes de diciembre, 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.

4.1.2 Equipos Portátiles

Durante el mes de diciembre 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	93,33%	90,00%
EUF-2	Cumplimiento en la entrega del informe	100,00%	100,00%

Tabla 78 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 realizó la configuración e instalación de Firewall Fortinet tras la apertura de la oficina de Santa Fe de Antioquia.
- Se trabajó con el SOC en la configuración de traffic shapper para limitar el consumo de ancho de banda en los servidores de tareas de backup y evitar la saturación del canal de Internet en Colombia XV.
- Se trabajó en el subnetting para la implementación del direccionamiento IPv6 en cada una de las oficinas del Ministerio.
- Se ajustaron las plantillas de SD-WAN para conmutar el tráfico hacia internet por los canales de comunicación hacia Datacenter alterno Santa Monica Cali en caso de falla de los canales de comunicación de Colombia XV.
- Se realizó cambio de ubicación de Access Point en la territorial de Manizales.

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

- Los especialistas gestionaron un total de 9 solicitudes escaladas a través de la herramienta Aranda. Al corte del mes todos los casos quedaron en estado Cerrado.

los casos obedecen a pruebas de disponibilidad Switch Core Datacenter Colombia XV, revisión y pruebas de UPS, revisión y pruebas de red en canales de internet, revisión de alerta en dispositivos de red. Los demás casos relacionados con el servicio, se gestionaron por parte del NOC, los detalles se relacionan en el apartado 2.1.2.8. Práctica de Eventos de este mismo documento.

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

Categoría	Cantidad de solicitudes
Equipo Conectividad Internet	3
Sin servicio	2
UPS	1
Switch Sede Central	1
Asesoría - Consulta	1

Tabla 79 Top 5 de categorías en el Servicio de conectividad LAN-WLAN



Ilustración 170 Estado de casos Redes y Conectividad

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

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

4.2.2 Switch para conexiones perimetrales (EDGE) en sede principal
Se encuentra operativo en Datacenter recibiendo las conexiones del canal de internet y conexiones perimetrales.

4.2.3 Switch de acceso 24 puertos
Se encuentran operativos y en monitoreo los siguientes equipos:

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

Tabla 80 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 81 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 82 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 83 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 84 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 85 Sedes cerradas

Estado	Cantidad
Operativos	327
Inspecciones cerradas	8**(*)**
Pendiente por MinTrabajo (usuario no disponible, usuario en licencia, usuarios no recibieron equipo, adecuaciones de cableado o físicas, asignación usuarios)	15
Total	**350**

Tabla 86 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 87 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 diciembre de 2025, 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. Santa Barbara.msg

- Se realizó la actualización de la infraestructura de la plataforma de telefonía a las versiones más recientes de firmware y software disponibles por parte del fabricante, con el fin de incorporar mejoras en rendimiento, nuevas funcionalidades y reforzar los niveles de seguridad del servicio. Cambio RFC – 169797.



RFC_Estandar-Telefonía IP_Diciembre.msg



Actualización_TOIP_RFC_MinTrabajo_Dicier

- Asignación de Licencias – Extensiones

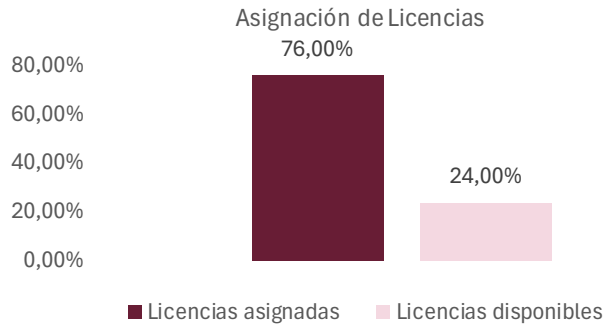


Ilustración 171 Asignación de licencias

Durante el mes en gestión, se han asignado un total de 457 extensiones a nivel nacional. Actualmente, permanecen disponibles 143 extensiones.

- Estadísticas de Tráfico

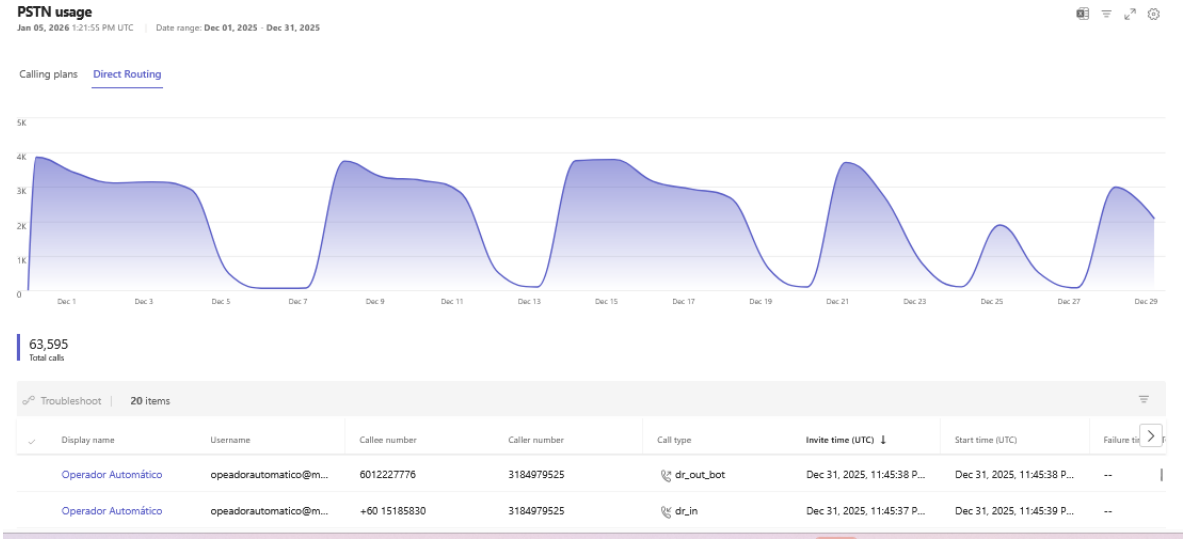


Ilustración 172 Comportamiento de tráfico

En la gráfica anterior se visualizan las tendencias de uso del servicio, en el periodo correspondiente al mes de diciembre de 2025, donde se atendieron un total de 63,595 llamadas.

Servicio	Minutos Disponibles	Minutos Utilizados
Locales	Ilimitados	730.16
Celular	1000	690.23
Nacional	Ilimitados	217.86
Internacional	700	5.12
Total		1643.37

Tabla 88 Minutos, consumos

- Consumo de llamadas LDN (Larga Distancia Nacional)

Con respecto a las llamadas realizadas a destinos larga distancia nacional en el mes de diciembre de 2025, se identifica que se realizaron llamadas con una duración total de 217.86 minutos.

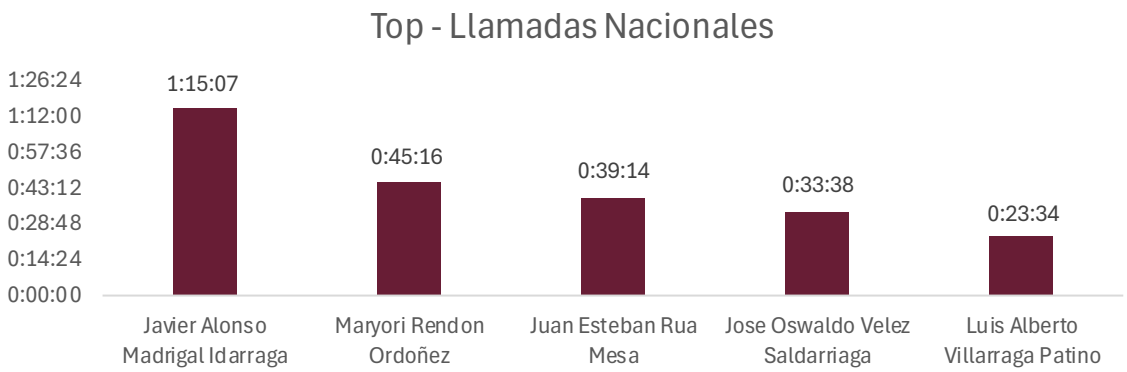


Ilustración 173 Top llamadas nacionales

N°	Usuario	Área	Tiempo llamadas
1	Javier Alonso Madrigal Idarraga	Grupo de resolución de conflictos y conciliaciones Antioquia	1:15:07
2	Maryori Rendon Ordoñez	Oficina especial Barrancabermeja	0:45:16
3	Juan Esteban Rua Mesa	Grupo de resolución de conflictos y conciliaciones Antioquia	0:39:14
4	Jose Oswaldo Velez Saldarriaga	Act DT Antioquia	0:33:38
5	Luis Alberto Villarraga Patino	Dirección de riesgos laborales Bogotá	0:23:34

Tabla 89 Top 5 consumo de llamadas

- Consumo de llamadas LDI (Larga Distancia Internacional)

Con respecto a las llamadas internacionales en el mes de diciembre de 2025, 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.

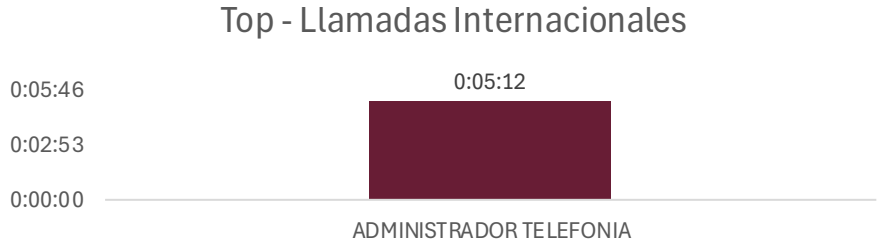


Ilustración 174 llamada internacional de prueba

Como se puede observar en el grafico anterior, se evidencia que, en el mes de diciembre de 2025 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	0:05:12

Tabla 90 Top 5 llamadas LDI

- Consumo de llamadas destinos celulares

Con respecto a las llamadas realizadas a celular en el mes de diciembre de 2025, se identifica que se realizaron llamadas con una duración total de 690.23 minutos (11,50 horas).

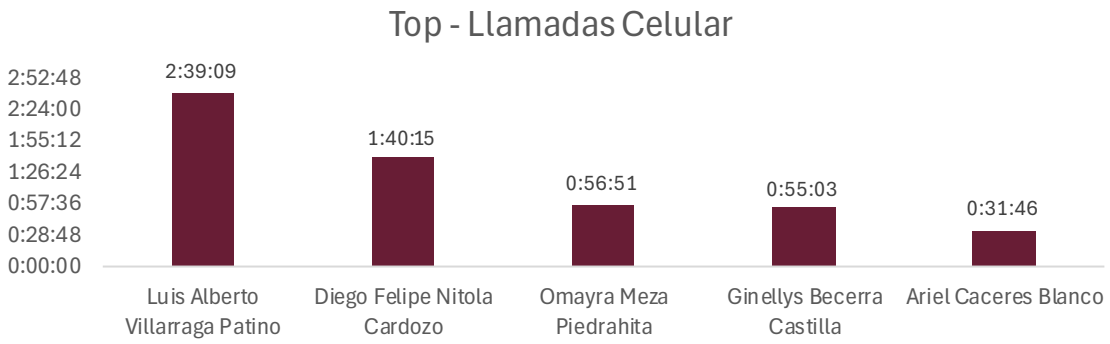


Ilustración 175 Top Celular

N°	Usuario	Área	Tiempo llamadas
1	Luis Alberto Villarraga Patino	Dirección de riesgos laborales Bogotá	2:39:09
2	Diego Felipe Nitola Cardozo	Grupo atención al ciudadano Boyacá	1:40:15
3	Omayra Meza Piedrahita	Oficina Asesora Juridica	0:56:51
4	Ginellys Becerra Castilla	Comunicaciones DT Bogotá	0:55:03
5	Ariel Caceres Blanco	Oficina Especial Barrancabermeja	0:31:46

Tabla 91 Top 5 llamadas Celular

- Consumo de llamadas locales

Con respecto a las llamadas realizadas a destinos locales en el mes de diciembre de 2025, se identifica que se realizaron llamadas con una duración total de 730.16 minutos (12,16 horas).

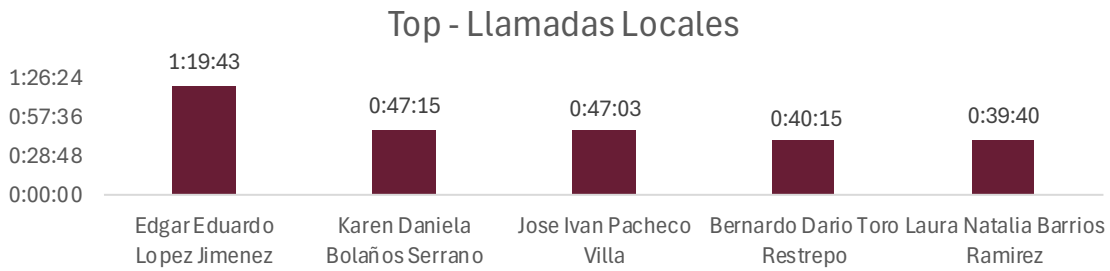


Ilustración 176 Top Local

N°	Usuario	Área	Tiempo llamadas
1	Edgar Eduardo Lopez Jimenez	Grupo RCC DT. Bogotá	1:19:43
2	Karen Daniela Bolaños Serrano	Viceministerio de empleo y pensiones Bogotá	0:47:15
3	Jose Ivan Pacheco Villa	Oficina especial Barrancabermeja	0:47:03
4	Bernardo Dario Toro Restrepo	Comunicaciones DT Bogotá	0:40:15
5	Laura Natalia Barrios Ramirez	Subdirección Administrativa y Financiera Bogotá	0:39:40

Tabla 92 Top 5 llamadas locales

- Capacitaciones y divulgaciones

En el mes de diciembre 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 177 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

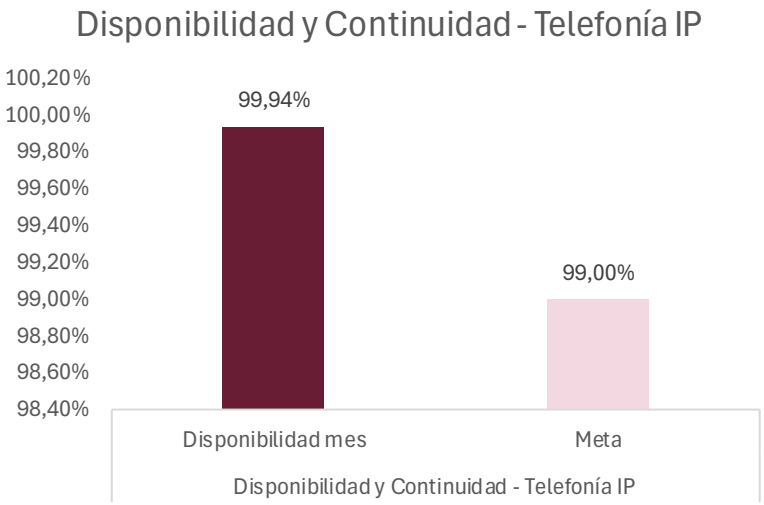


Ilustración 178 Disponibilidad y Continuidad TOIP

En el periodo correspondiente al mes de diciembre, 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	99,94%	99,00%
TIP-3	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 93 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 94 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	POBLACION Y/O CIUDAD	UBICACION 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 95 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-171161	Cambio	Se gestiona cambio con el respectivo RFC para revisión alerta tarjeta de red UPS Sede Central, la actividad está planeada para el lunes 15 de diciembre de 6 pm a 10 pm.	Se realizó reinicio sobre una de las UPS pero no surtió efecto sobre la tarjeta de red, Apicom confirma que debe crear caso con fabricante.	Cerrado
RF-172222	Requerimiento	Por favor realizar revisión de UPS en la oficina de Bucaramanga ya que la tarjeta de red no está respondiendo.	Escalada la novedad a fábrica	Suspendido
RF-172382	Requerimiento	Se ejecuta actividad de revisión de tarjeta de red de UPS, se concluye que se debe crear caso con fabricante dado que reinicio no surtió efecto sobre la tarjeta de red.	Se informa que se actualiza el cambio RFC-171161 y se cierra este caso.	Cerrado
IM-170828	Incidente	Se ha detectado un evento en el sistema de monitoreo Zabbix. A continuación, se detallan los datos del evento: Nombre del Host: UPS_Pereira IP del Host: 172.16.25.9 Tipo de Equipo: UPS Evento: UPS en estado Baterias Severidad: Disaster Fecha y Hora del Evento: 2025.12.09 17:42:50 Descripción del Problema: Valor Actual del Ítem: Baterias (5)	Buen dia, se procede a dar cierre al caso ya que se evidencia que la alarma se solventa en la herramienta y al realizar validaciones de primer nivel se ve el servicio operativo, la caída se atribuye a una falla eléctrica en la DT.	Cerrado

Tabla 96 Casos gestionados – Energía Eléctrica Regulada UPS

- **Mantenimiento Preventivo de UPS**

Durante diciembre 2025, se consolidaron las actas de atención en el repositorio dado por la entidad para el contrato, a la fecha se realizaron los mantenimientos preventivos de UPS en Nivel Central en los pisos 3, 5, 8, 9, 10, 17, 18, 19, 20, 21, 22, 23, 24, 25. Se tienen en coordinación de actividades de las UPS de Territorio.

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.

- Actualmente se está 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.

- **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 97 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 98 Inventario de impresoras para el servicio

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

- Para el mes de diciembre, el responsable del servicio gestionó un total de 474 solicitudes escaladas a través de Aranda. Al corte del mes, 471 casos quedaron en estado Cerrado/Solucionado, 3 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 65% 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-168729; 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 205 impresoras actualizadas, esta actividad continúa en curso para el siguiente período.
- El 3/12/2025 bajo el RFC-168676 se gestiona el parchado del servidor de impresión, esto con el fin de mitigar vulnerabilidades al servicio.
- **Mantenimientos Preventivos:** Se realiza la atención de mantenimientos preventivos de las impresoras Ricoh a nivel nacional. A corte del período se han atendido 21 Direcciones territoriales, 79 inspecciones de territorio y todo nivel central dando un total de 177 impresoras, actividad se continuará en el siguiente periodo.
- El 11/12/2025 se genera desde el servicio de impresión una guía técnica detallada de las acciones que se sugieren realizar desde el nivel dos (soporte técnico en sitio) para solventar el error “Atasco de original (J001)” que aparece en las impresoras Ricoh del ministerio, que va orientada a unas validaciones técnicas adicionales en el ADF previo a algún escalamiento al fabricante. Se divulga mediante correo electrónico.



Guía Técnica -
Escáner ADF en Impre

- Información relevante para el servicio de impresión, estadísticas, TOP de consumos y utilización del servicio, ampliaciones de cuotas recurrentes:

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
ricohpiso25b	Bogotá Sede Central	ysanchezc	Yesid Fernando Sanchez Colorado	8.703
ricohpiso5a	Bogotá Sede Central	cjunco	Carlos Julio Junco Arenas	4.109
ricoh-bmanga-ofc305	Bucaramanga	ybeltran	Yerson Daniel Beltran Martinez	3.486
ricoh-ibague-radicacion	Ibagué	jgonzalezcu	Jose Eugenio Gonzalez Cuella	2.624
ricohpiso23b	Bogotá Sede Central	ldleal	Luz Dary Leal Cotamo	2.305
ricohpiso23b	Bogotá Sede Central	jadiaz	Javier Diaz Marroquin	2.148
ricoh-tulua-insp	Tulua	bgarcia	Beatriz Eugenia Garcia Realpe	1.828
ricohpiso19a	Bogotá Sede Central	pnustes	Patricia Celestial Nustes Barrera	1.776
ricohpiso5a	Bogotá Sede Central	jbohorquez	Jose Hernando Bohorquez Mendoza	1.762
ricoh-cartagena-piso2	Cartagena	preyes	Pedro Mario Reyes Cassiani	1.624

Tabla 99 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
ricohpiso5a	Bogotá Sede Central	15893
ricoh-bmanga-ofc305	Bucaramanga	14658
ricohpiso23b	Bogotá Sede Central	13178
ricohpiso25b	Bogotá Sede Central	9325
ricohpiso19a	Bogotá Sede Central	9036
ricohpiso12a	Bogotá Sede Central	8295
ricohcl32-rcc	Bogotá Calle 32	8246
ricohpiso20b	Bogotá Sede Central	8100
ricohpiso21a	Bogotá Sede Central	7541
ricoh-cali-piso2-atc	Cali	7018

Tabla 100 Top 10 de impresoras con mayor uso

Top Impresoras.xlsx

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

Nombre de la impresora	Ubicación	Nombre de Usuario	Nombre Completo	Color
ricohpiso25c	Bogotá Sede Central	mserrano	Malliber Serrano Nieto	1101
ricohpiso25c	Bogotá Sede Central	ymedinag	Yeisson Medina Gonzalez	225
ricohpiso25c	Bogotá Sede Central	bhernandez	Bibiana Hernandez Hernandez	72

Tabla 101 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	1398	125979	90796	36581	127377	33108	6,2
D. T. Valle Del Cauca	0	37272	25784	11488	37272	11080	3,4
D. T. Bogota	0	36579	22762	13817	36579	10900	3,4
D. T. Santander	0	32400	24242	8158	32400	9035	3,6
D. T. Antioquia	0	22410	15472	6938	22410	6752	3,3
D. T. Atlantico	0	17300	11146	6154	17300	4925	6,5
D. T. Tolima	0	13395	8372	5023	13395	4005	3,3
D. T. Norte De Santander	0	13379	8786	4593	13379	4453	3
D. T. Cundinamarca	0	12483	6216	6267	12483	4032	3,1
D. T. Huila	0	10246	6486	3760	10246	2836	3,6

Tabla 102 Top oficinas

Oficinas.xlsx

En la siguiente tabla se muestra el TOP 10 de impresoras que más usan el servicio de fotocopiado; las cantidades corresponden a un valor consolidado de consumo desde que se inició la prestación del servicio (esta tabla refleja los totales de fotocopias, mas no periodos puntuales).

Impresora	Ubicación	Copias
ricoh-medellin-piso1	Medellín	59970
RICOH-GAU-B	Bogotá Calle 32	56640
RICOHCALLE32-RCC	Bogotá calle 32	47443
ricohpiso5b	Bogotá sede central	42881
ricoh-bmanga-ofc205	Bucaramanga	33019

ricoh-cali-piso4	Cali	32788
RICOH-BMANGA-OFC305	Bucaramanga	27094
RICOHGAU-A	Bogotá Calle 32	26607
ricohpiso9a	Bogotá sede central	22854
ricoh-monteria-piso2	Montería	22672

Tabla 103 Top 10 impresoras más usadas del servicio de fotocopiado



Copias.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
jgonzalezcu	Jose Eugenio Gonzalez Cuella	ADJUST	3460	9
ysanchezc	Yesid Fernando Sanchez Colorado	ADJUST	15351	8
bgarcia	Beatriz Eugenia Garcia Realpe	ADJUST	2100	7
lbernate	Luz Marina Bernate Barrios	ADJUST	2540	7
dgalvan	David Ricardo Galvan Mancera	ADJUST	2532	6
ybeltran	Yerson Daniel Beltran Martinez	ADJUST	4843	6
bcarvajal	Blanca Isabel Carvajal Perez	ADJUST	2000	5
bgalindo	Betzabeth Galindo Herrera	ADJUST	1500	5
egarcia	Edgar de Jesus Garcia Zapata	ADJUST	1501	5
fzorro	Fernanda Vanessa Zorro Bayona	ADJUST	2000	5

Tabla 104 Ampliación de cuota de impresión



Saldo Asignado.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:

	oct-25		nov-25		dic-25	
	Resmas Carta	Resmas Oficio	Resmas Carta	Resmas Oficio	Resmas Carta	Resmas Oficio
Total, Resmas	441	220	432	255	536	282
Total, Cajas por Tamaño	44,1	22	43,2	25,5	53,6	28,2
Total, Cajas Enviadas	**66,1**		**68,7**		**81,8**	

Tabla 105 Despacho de papel a sedes del Ministerio del Trabajo

Durante el período, se despacharon a sedes del ministerio un total de 19 toners para impresora B/N IM430F, 7 unidades de imagen y 2 unidades fusoras.

4.6.1 No aplica

4.6.2 Multifuncional B/N rango medio – Cargo fijo mensual

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

Tabla 106 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 107 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 diciembre de 2025:

MES	DETALLE	CANTIDAD
Diciembre	Multifuncional blanco y negro rango medio - Clic de impresión tóner y papel carta	**486.972**
	TOTAL	**486.972**

Tabla 108 Clics de impresión de diciembre 2025 – Multifuncional B/N

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

Mes 2025	Octubre	Noviembre	Diciembre
Cantidad de clics consumidos	553.658	502.396	486.972

Tabla 109 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 **446.352** clics de impresión (esto incluye **6.782** de la impresora de contratos piso 8) y **40.620** de fotocopias para un total de **486.972** para este servicio, superando el estimado del mes por **36.972.**

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 diciembre de 2025:

MES	DETALLE	CANTIDAD
Diciembre	Impresora color rango medio - Cargo fijo mensual - Clic de impresión tóner y papel carta	1.398
Total		1.398

Tabla 110 Clics de Impresión de diciembre 2025 – Impresora Color

A continuación, se indica la tendencia de consumo para la vigencia 2025:

Mes 2025	Octubre	Noviembre	Diciembre
Cantidad de clics consumidos	1.602	1.677	1.398

Tabla 111 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 **1.398** 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 112 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 diciembre de 2025, se aseguró la cobertura de la infraestructura de servidores con antivirus activos. Estos agentes están monitoreando continuamente los eventos de seguridad que puedan presentarse.

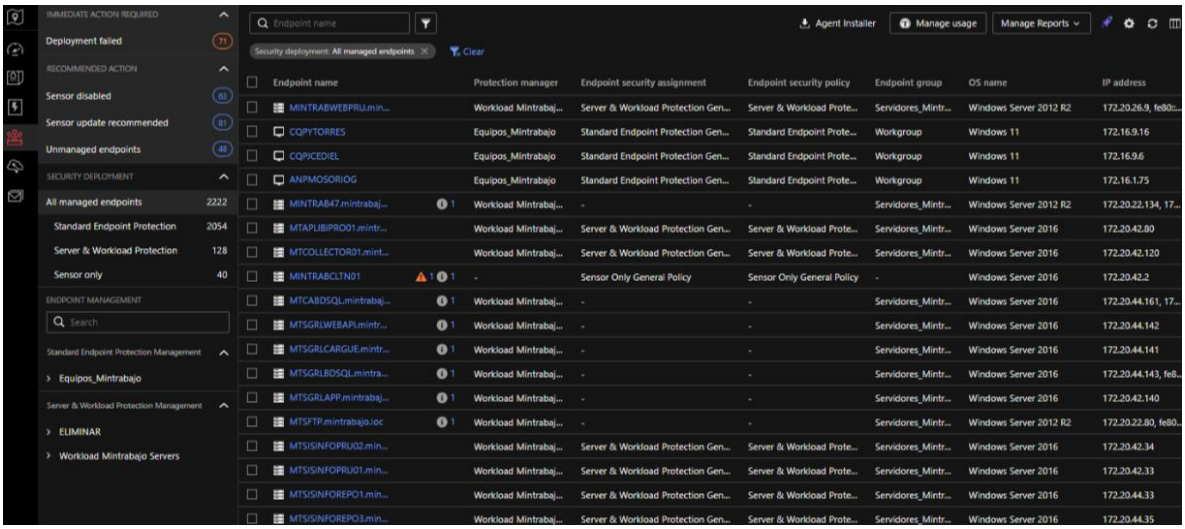


Ilustración 179 Equipos consola antivirus

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 (2222) de Mintrabajo, se cuenta con 2255 licencias, se tienen disponibles 33.

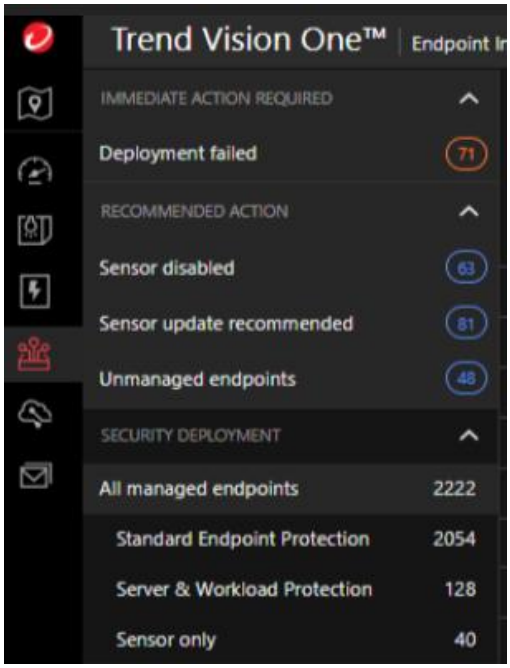


Ilustración 180 Gestión consola antivirus – equipos usuario final

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:

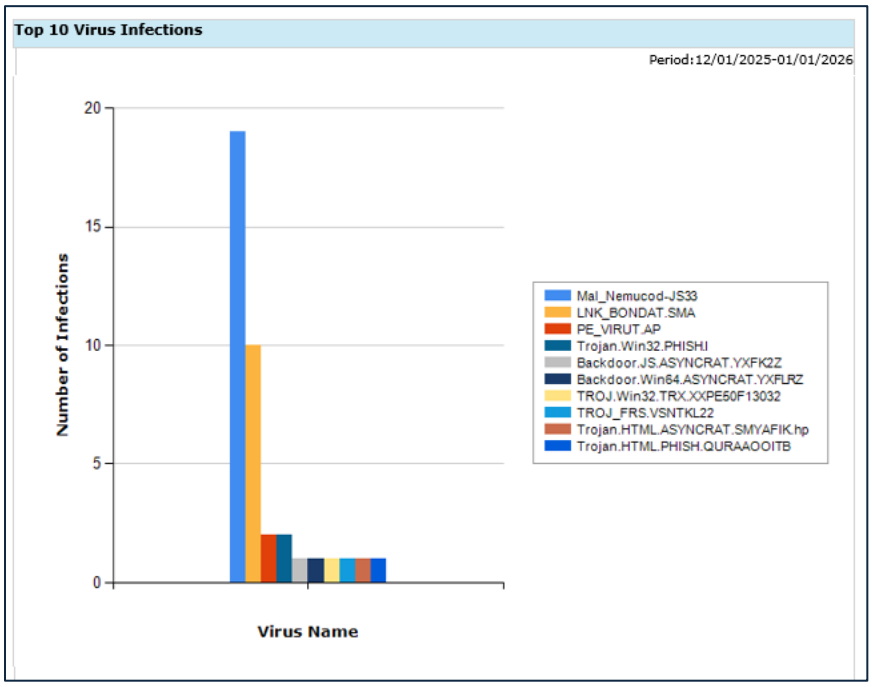


Ilustración 181 Top 10 virus detectado

Top 10 Virus Infections

Virus Name	# of Infections	Detected By
Mal_Nemucod-JS33	19	Desktop (19)
LNK_BONDAT.SMA	10	Desktop (10)
PE_VIRUT.AP	2	Desktop (2)
Trojan.Win32.PHISH.I	2	Desktop (2)
Backdoor.JS.ASYNCRAT.YXFK2Z	1	Desktop (1)
Backdoor.Win64.ASYNCRAT.YXFLRZ	1	Desktop (1)
TROJ.Win32.TRX.XXPE50F13032	1	Desktop (1)
TROJ_FRS.VSNTKL22	1	Desktop (1)
Trojan.HTML.ASYNCRAT.SMYAFIK.hp	1	Desktop (1)
Trojan.HTML.PHISH.QURAAOOITB	1	Desktop (1)

Tabla 113 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: *Mal_Nemucod-JS33*
Descripción: Variante de malware Nemucod distribuida mediante archivos JavaScript maliciosos, usualmente asociada a sitios con contenido publicitario. Este tipo de amenaza intenta descargar malware secundario desde servidores externos no autorizados.

Equipos afectados

BODSDIAZR, BODJBENAVIDES, VADMANGULOM, BOPRBARRERA, GUDACAICEDO, GUDRPIMIENTA, BOPJSALCEDO, GUDEREDONDO, SNDLMUNOZA, CUDCPALTA, BOPFGOMEZS.

Acción: Trend Micro detectó y eliminó automáticamente los archivos maliciosos almacenados en caché del navegador.

Impacto: Bajo.

Acciones adicionales: No requeridas.

Malware asociado a dispositivos USB

Detecciones:
- *LNK_BONDAT.SMA*
- *PE_VIRUT.AP*
- *TROJ_FRS.VSNTKL22*

Descripción: Amenazas introducidas mediante dispositivos USB, principalmente a través de accesos directos (LNK) o ejecutables maliciosos disfrazados de software legítimo.

Equipos afectados:
- NAPMBOLANOS
- ANDCGONZALEZB
- SNDGELIZALDE

Acción:
- Eliminación automática de archivos maliciosos.
- Limpieza de ejecutables detectados.
- En un caso puntual (*PE_VIRUT.AP*), se requirió reinicio del equipo tras la remediación.

Impacto: Bajo–medio (contenido localizado, sin propagación).
Observación: Refuerza la importancia del **control de uso de USB** y la concientización del usuario final.

Troyanos y puertas traseras (AsyncRAT y similares)

Detecciones:
- *Backdoor.JS.ASYNCRAT.YXFK2Z*
- *Backdoor.Win64.ASYNCRAT.YXFLRZ*
- *Trojan.HTML.ASYNCRAT.SMYAFIK.hp*

Descripción: Troyanos tipo **RAT (Remote Access Trojan)** que permiten control remoto, robo de información y descarga de cargas adicionales. Se presentaron principalmente como archivos JavaScript o HTML camuflados como documentos judiciales o notificaciones oficiales.

Equipos afectados
BYDEMEDINA, BYDGTELLO, BOPLGARZON.

Acción:
- Detección en escaneos en tiempo real y programados.
- Eliminación inmediata de archivos maliciosos.
- Verificación del estado del host sin hallazgos posteriores.

Impacto: Controlado. No se evidenció ejecución persistente ni compromiso del sistema.

Troyanos descargados desde correo o internet

Detecciones:
- *Trojan.Win32.PHISH.I*
- *TROJ.Win32.TRX.XXPE50F13032*
- *Trojan.HTML.PHISH.QURAAOOITB*

Descripción: Archivos maliciosos descargados mediante navegación web o correo electrónico, algunos disfrazados como notificaciones legales, actas judiciales o archivos SVG/HTML.

Equipos afectados
BOPMMORENOS, BOPMGONZALEZ, ATDLBENATE.

Acción:
- Limpieza automática por Trend Micro durante escaneos en tiempo real y programados.
- No se identificaron acciones de persistencia ni alteraciones del sistema operativo.

Impacto: Bajo.

Acciones adicionales: No requeridas.

TOP 5 EQUIPOS

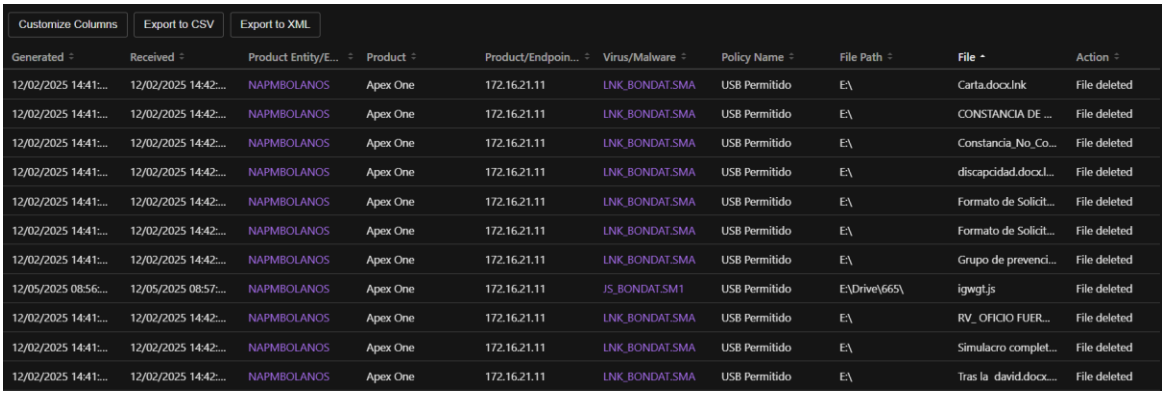
A continuación, se genera un top 5 de las amenazas durante el mes de diciembre 2025:

Product Entity/Endpoint	Cantidad	Virus/Malware
NAPMBOLANOS	11	LNK_BONDAT.SMA
GUDACAICEDO	6	Mal_Nemucod-JS33
BOPJSALCEDO	3	Mal_Nemucod-JS33
ANDCGONZALEZB	2	PE_VIRUT.AP
BOPMMORENOS	2	Trojan.Win32.PHISH.I

Tabla 114 *Top 5 Equipos*

NAPMBOLANOS

Las 11 detecciones en el equipo se deben por LNK_BONDAT.SMA identifica un tipo de archivo malicioso, probablemente un acceso directo (LNK), que apunta a un archivo dañino (como un virus o spyware) y se disfraza o forma parte de una amenaza más amplia llamada "BONDAT detecciones fueron encontradas el día 02, 05 de diciembre en el host NAPMBOLANOS se identifica conexión USB con contenido de acceso directos, los cuales fueron eliminados por Trend micro, dejando el evento como contenido y sin impacto adicional en el sistema.


Customize Columns | Export to CSV | Export to XML

Generated	Received	Product Entity/E...	Product	Product/Endpoin...	Virus/Malware	Policy Name	File Path	File	Action
12/02/2025 14:41:...	12/02/2025 14:42:...	NAPMBOLANOS	Apex One	172.16.21.11	LNK_BONDAT.SMA	USB Permitido	E:\	Carta.docx.lnk	File deleted
12/02/2025 14:41:...	12/02/2025 14:42:...	NAPMBOLANOS	Apex One	172.16.21.11	LNK_BONDAT.SMA	USB Permitido	E:\	CONSTANCIA DE ...	File deleted
12/02/2025 14:41:...	12/02/2025 14:42:...	NAPMBOLANOS	Apex One	172.16.21.11	LNK_BONDAT.SMA	USB Permitido	E:\	Constancia_No_Co...	File deleted
12/02/2025 14:41:...	12/02/2025 14:42:...	NAPMBOLANOS	Apex One	172.16.21.11	LNK_BONDAT.SMA	USB Permitido	E:\	discapcidad.docx.l...	File deleted
12/02/2025 14:41:...	12/02/2025 14:42:...	NAPMBOLANOS	Apex One	172.16.21.11	LNK_BONDAT.SMA	USB Permitido	E:\	Formato de Solicit...	File deleted
12/02/2025 14:41:...	12/02/2025 14:42:...	NAPMBOLANOS	Apex One	172.16.21.11	LNK_BONDAT.SMA	USB Permitido	E:\	Formato de Solicit...	File deleted
12/02/2025 14:41:...	12/02/2025 14:42:...	NAPMBOLANOS	Apex One	172.16.21.11	LNK_BONDAT.SMA	USB Permitido	E:\	Grupo de prevenci...	File deleted
12/05/2025 08:56:...	12/05/2025 08:57:...	NAPMBOLANOS	Apex One	172.16.21.11	JS_BONDAT.SM1	USB Permitido	E:\Drive\665\	igwgt.js	File deleted
12/02/2025 14:41:...	12/02/2025 14:42:...	NAPMBOLANOS	Apex One	172.16.21.11	LNK_BONDAT.SMA	USB Permitido	E:\	RV_ OFICIO FUER...	File deleted
12/02/2025 14:41:...	12/02/2025 14:42:...	NAPMBOLANOS	Apex One	172.16.21.11	LNK_BONDAT.SMA	USB Permitido	E:\	Simulacro complet...	File deleted
12/02/2025 14:41:...	12/02/2025 14:42:...	NAPMBOLANOS	Apex One	172.16.21.11	LNK_BONDAT.SMA	USB Permitido	E:\	Tras la david.docx....	File deleted

Ilustración 182 NAPMBOLANOS

GUDACAICEDO

Los días 12, 22, 23, 26 de diciembre se detectó en el host GUDACAICEDO un archivo malicioso identificado como Mal_Nemucod-JS33, una variante distribuida mediante scripts JavaScript que intentan descargar malware adicional desde internet. La amenaza fue detectada durante la navegación web y el archivo ubicado en la caché de Firefox fue eliminado automáticamente por Trendmicro, dejando el evento como contenido y sin

impacto adicional en el sistema. Se escala caso RF-176789 con el fin de verificación y limpieza de proceso reiterativo en el host.

Generated	Product Entity/E...	Product/Endpoin...	Virus/Malware	File Path	File	Endpoint Infecti...	Action	Result
12/12/2025 08:18:...	GUDACAICEDO	172.16.16.50	Mal_Nemucod-JS33	C:\Users\acaicedo\...	50F246D51FF191134DF1A77D168EA4062E1C5D9D	Web	File deleted	Successful
12/22/2025 16:24:...	GUDACAICEDO	172.16.16.50	Mal_Nemucod-JS33	C:\Users\acaicedo\...	50F246D51FF191134DF1A77D168EA4062E1C5D9D	Web	File deleted	Successful
12/23/2025 11:51:...	GUDACAICEDO	172.16.16.50	Mal_Nemucod-JS33	C:\Users\acaicedo\...	50F246D51FF191134DF1A77D168EA4062E1C5D9D	Web	File deleted	Successful
12/23/2025 14:11:...	GUDACAICEDO	172.16.16.50	Mal_Nemucod-JS33	C:\Users\acaicedo\...	50F246D51FF191134DF1A77D168EA4062E1C5D9D	Web	File deleted	Successful
12/23/2025 15:14:...	GUDACAICEDO	172.16.16.50	Mal_Nemucod-JS33	C:\Users\acaicedo\...	50F246D51FF191134DF1A77D168EA4062E1C5D9D	Web	File deleted	Successful
12/26/2025 09:22:...	GUDACAICEDO	172.16.16.50	Mal_Nemucod-JS33	C:\Users\acaicedo\...	50F246D51FF191134DF1A77D168EA4062E1C5D9D	Web	File deleted	Successful

Ilustración 183 GUDACAICEDO

BOPJSALCEDO

Los días 03, 29 de diciembre se detectó en el host BOPJSALCEDO un archivo malicioso identificado como Mal_Nemucod-JS33, una variante distribuida mediante scripts JavaScript que intentan descargar malware adicional desde internet. La amenaza fue detectada durante la navegación web y el archivo ubicado en la caché de Firefox fue eliminado automáticamente por Trend micro, dejando el evento como contenido y sin impacto adicional en el sistema.

Generated	Product Entity/E...	Product/Endpoin...	Virus/Malware	File Path	File	Endpoint Infecti...	Action	Result
12/29/2025 09:28:...	BOPJSALCEDO	172.16.60.5	Mal_Nemucod-JS33	C:\Users\jsalcedo\...	50F246D51FF191134DF1A77D168EA4062E1C5D9D	Web	File deleted	Successful
12/03/2025 09:53:...	BOPJSALCEDO	172.16.60.5	Mal_Nemucod-JS33	C:\Users\jsalcedo\...	50F246D51FF191134DF1A77D168EA4062E1C5D9D	Web	File deleted	Successful
12/03/2025 07:53:...	BOPJSALCEDO	172.16.60.5	Mal_Nemucod-JS33	C:\Users\jsalcedo\...	50F246D51FF191134DF1A77D168EA4062E1C5D9D	Web	File deleted	Successful

Ilustración *184 BOPJSALCEDO*

ANDCGONZALEZB

El día 05 de diciembre se registraron en el host 7.2.4ANDCGONZALEZB detecciones de virus infectado llega al sistema como un archivo arrojado por otro malware o como un archivo descargado sin que los usuarios lo sepan cuando visitan sitios maliciosos. Deshabilita el Administrador de tareas, el Editor del Registro y las Opciones de carpeta. Se identifica conexión de unidad USB la unidad E:\ ejecutable CONIME.EXE el cual por escaneo realizado por el usuario con Trend Micro procede con su limpieza y requiere de reinicio del equipo. Sin embargo, a la fecha el equipo no volvió a presentar detecciones relacionadas, por lo cual Trend Micro realizo la limpieza correspondiente.

Generated	Received	Product Entity/E...	Product/Endpoin...	Virus/Malware	Policy Name	File Path	File	Action	Result
12/05/2025 09:34:...	12/05/2025 09:36:...	ANDCGONZALEZB	172.16.1.37	PE_VIRUT.AP	USB Permitido	E:\	CONIME.EXE	File cleaned	Successful
12/05/2025 09:34:...	12/05/2025 09:36:...	ANDCGONZALEZB	172.16.1.37	PE_VIRUT.AP	USB Permitido	HKEY_USERS\S-1-...	DisallowRun	Action Required - ...	Further action req.

Ilustración 185 ANDCGONZALEZB

BOPMMORENOS

El día 03 de diciembre se registraron en el host BOPMMORENOS detecciones de un programa troyano es un malware que no puede propagarse automáticamente a otros sistemas. Los troyanos suelen descargarse de internet e instalarse por usuarios desprevenidos. Los troyanos, como su nombre indica, pueden infiltrarse en el sistema, los eventos se registraron sobre las rutas:
C:\Users\mmorenos\AppData\Local\Microsoft\Olk\EBWebView\Default\Cache\Cache_Data\
C:\Users\mmorenos\AppData\Local\Microsoft\Olk\Attachments\ooa-6088f343-006c-4b37-851d-

bbed5925e92f\60d9ce15d8da6384b1d0e9e812d28e12647819efa093a64fad4c6e1dfb9f6f92\
Archivos comprometidos: f_000dbc, 007 notificación de demanda.svg.crswap.

Los archivos fueron eliminados automáticamente por Trend micro, dejando el evento como contenido y sin impacto adicional en el sistema.

Generated	Received	Product Entity/E...	Product/Endpoin...	Virus/Malware	Policy Name	File Path	File	Action	Result
12/03/2025 10:47:...	12/03/2025 10:48:...	BOPMMORENOS	192.168.1.8	Trojan.Win32.PHIS...	Política_Workstation	C:\Users\mmoren...	f_000dbc	File cleaned	Successful
12/02/2025 15:02:...	12/02/2025 15:03:...	BOPMMORENOS	192.168.1.8	Trojan.Win32.PHIS...	Política_Workstation	C:\Users\mmoren...	007 notificación de ...	File cleaned	Successful

Ilustración 186 BOPMMORENOS

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.

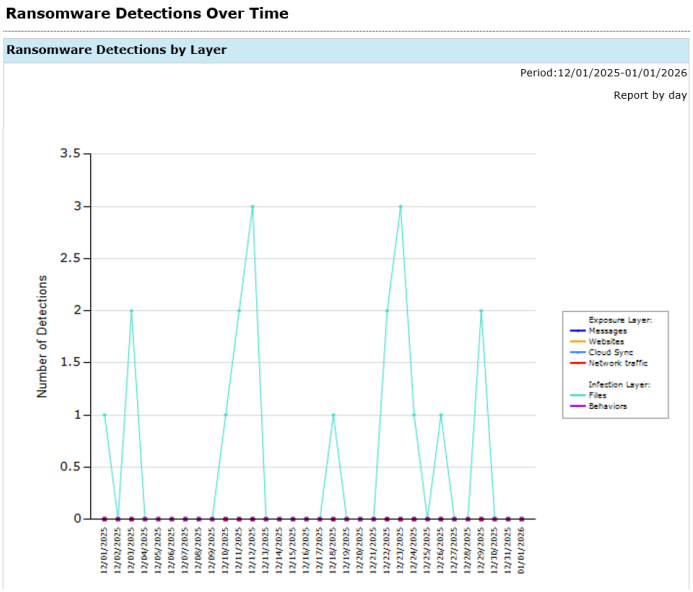


Ilustración 187 Eventos Ransomware

En el mes de diciembre 2025, se presentaron eventos 13 eventos escalados por detección de malware Ransomware, estas detenciones se realizaron en los hosts: BOPFGOMEZS, BOPJSALCEDO, GUDACAICEDO, BOPRBARRERA, CUDCPALTA, SNDLMUNOZA, GUDRPIMIENTA, VADMANGULOM, BODJBENAVIDES, BODSDIAZR, GUDEREDONDO.

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.

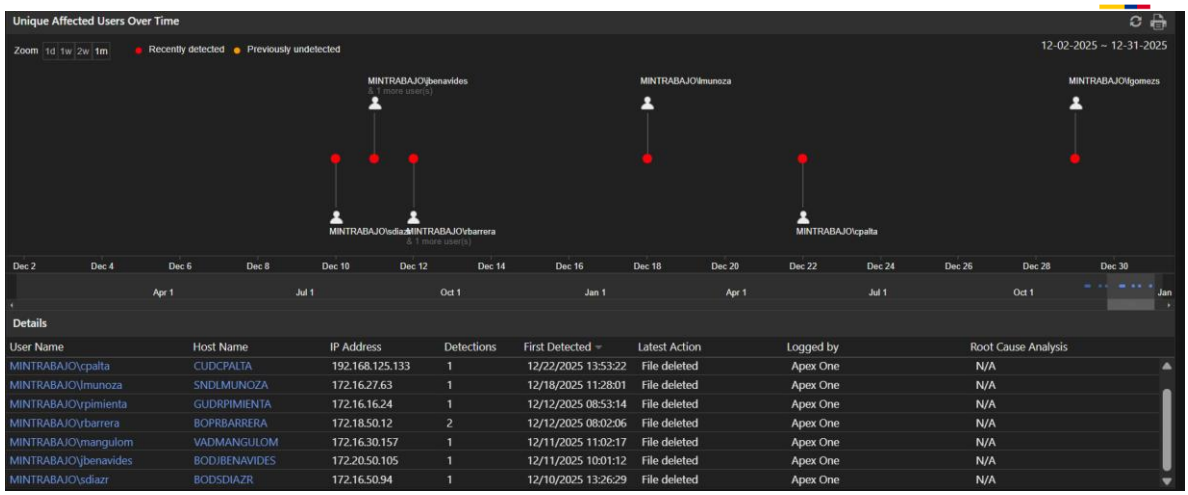


Ilustración 188 captura eventos ransonware

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 diciembre 2025 sobre la infraestructura tecnológica registrada del Ministerio de Trabajo, con el objetivo de identificar los hallazgos a nivel de vulnerabilidades que pueden alterar el nivel de exposición cibernética del negocio.

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

Se informó al Ministerio de trabajo y equipo infraestructura que se procede con la primera fase de la **Prueba de Vulnerabilidades** del **segundo semestre 2025** 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 diciembre del 2025 se tienen registrados 300 activos TI, de los cuales, se registró un alcance sobre 299 (99%) activos.

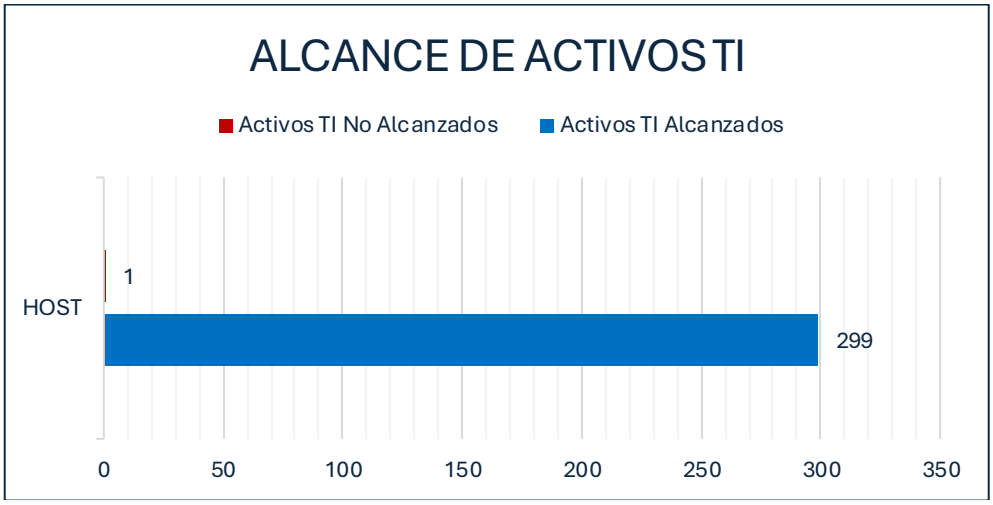


Ilustración 189 *Gestión consola Nessus*

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 ▲
2025 SEMANAL II - WINDOWS DESKTOP	Vulnerability	Weekly on Sat at 12:30 AM ✔	January 3 at 12:30 AM
2025 SEMANAL II - NETWORKING	Vulnerability	Weekly on Sat at 8:00 PM ✔	January 3 at 8:28 PM
2025 SEMANAL II - FORTISIEM	Vulnerability	Weekly on Sat at 9:00 PM ✔	January 3 at 9:43 PM
2025 SEMANAL II - VMWARE	Vulnerability	Weekly on Sat at 10:00 PM ✔	January 3 at 10:10 PM
2025 SEMANAL II - LINUX	Vulnerability	Weekly on Sat at 11:00 PM ✔	January 3 at 11:42 PM
2025 SEMANAL II - NO AUTH	Vulnerability	Weekly on Sun at 3:30 AM ✔	January 4 at 3:40 AM
2025 SEMANAL II - WINDOWS SERVER	Vulnerability	Weekly on Sun at 9:00 PM ✔	January 4 at 9:53 PM

Ilustración 190 *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 diciembre del 2025, el activo TI con la mayor cantidad de vulnerabilidades identificadas corresponde al host (172.20.42.34), con un total de 112 hallazgos, corresponde a un servidor Microsoft Windows Server 2016 Standard Build 14393 y la mayoría de las vulnerabilidades están asociadas a actualizaciones de seguridad para la librería Apache Log4j.

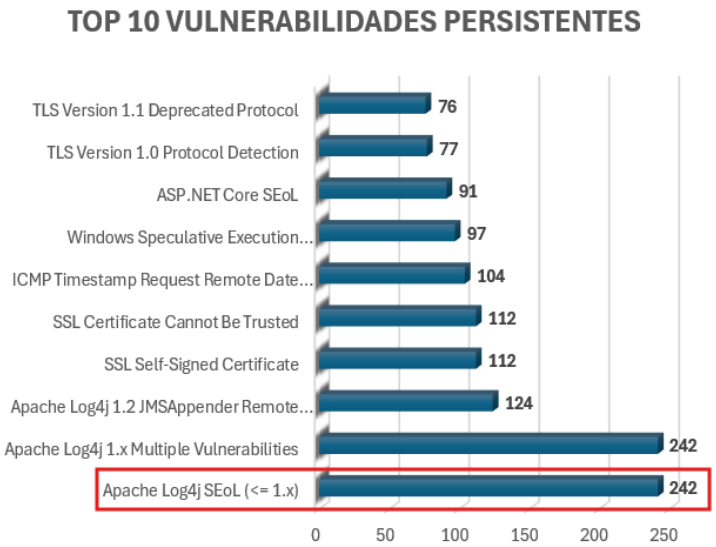


Ilustración 191 TOP 10 - Activos más explotables

Al cierre de diciembre del 2025, la vulnerabilidad identificada con la mayor cantidad de persistencias corresponde a (Apache Log4j SEoL (<= 1.x)), con un total de 242 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

Resumen de las actividades relacionas con la gestión de vulnerabilidades correspondientes al Snapshot del semestre II 2025, el cual reportó un total de 3.257 vulnerabilidades TI en las severidades:

- 692 vulnerabilidades críticas.
- 423 vulnerabilidades altas.
- 1.576 vulnerabilidades medias.
- 566 vulnerabilidades bajas.

Durante el periodo de diciembre del 2025, se remediaron un total de 40 vulnerabilidades, de las cuales, 15 fueron de severidad crítica, 3 de severidad alta, 17 de severidad media y 5 de severidad baja. Por otro lado, con relación a indicadores semestrales, se gestionaron un total de 1.443 vulnerabilidades TI, de las cuales, 305 fueron de severidad crítica, 191 de severidad alta, 600 de severidad media y 407 de severidad baja.

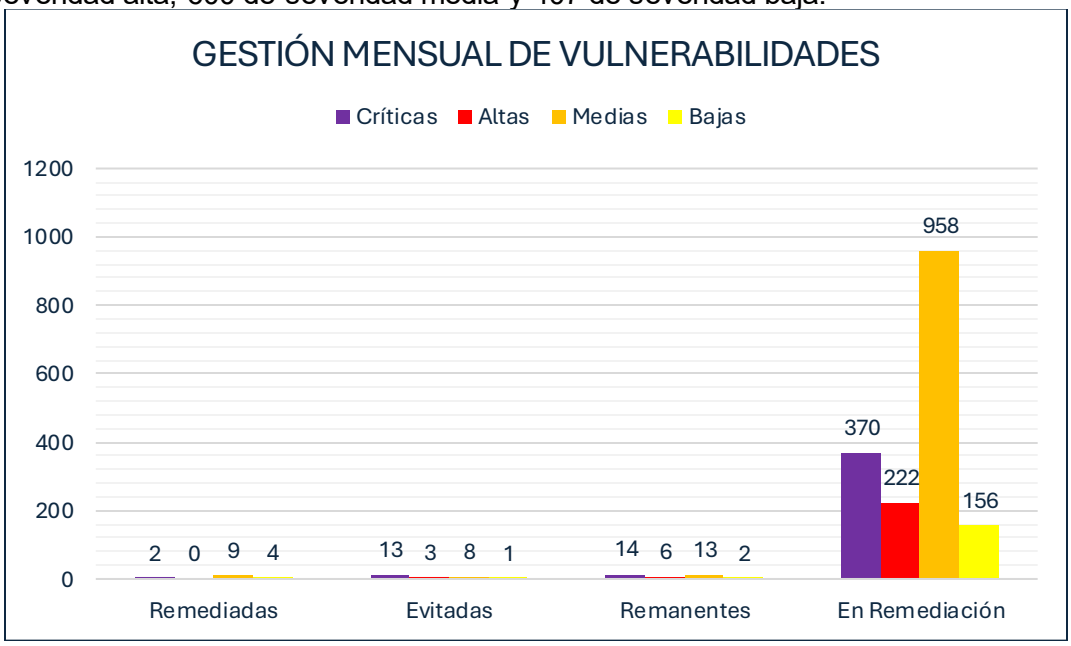


Ilustración 192 Vulnerabilidades gestionadas vs en remediación

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.

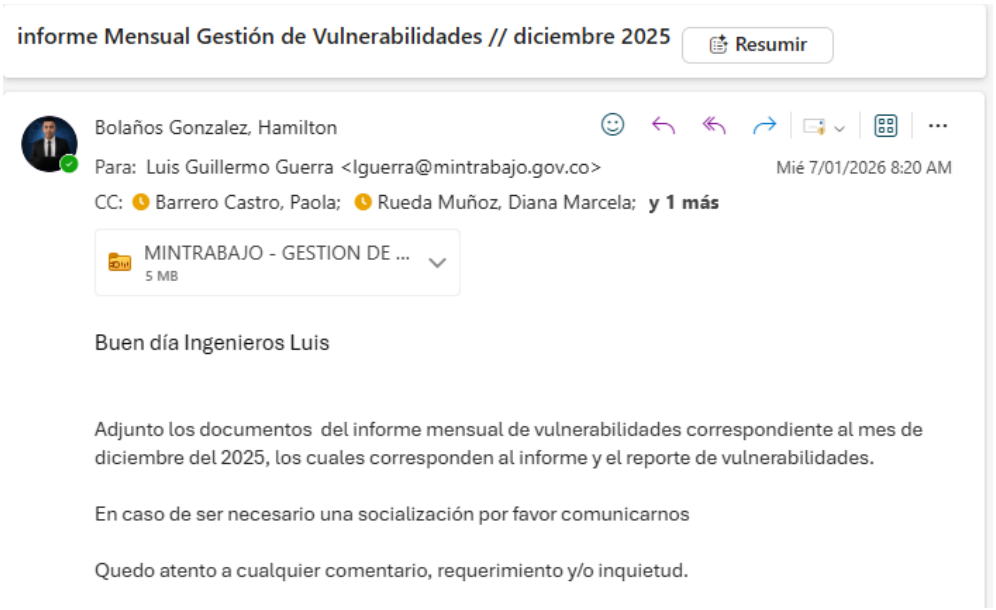


Ilustración 193 captura envío de correo gestión de vulnerabilidades

4.7.4.6 Prueba de Vulnerabilidades Semestre II 2025

Se notifica que se completan cada una de las fases de la Prueba de Vulnerabilidades del segundo semestre 2025 para el proyecto Ministerio del Trabajo, de acuerdo con el cronograma de ejecución propuesto.

FASE	RIESGO	RESPONSABLE	PROGRESO	FECHA INICIO	FECHA FIN	DÍAS
Levantamiento de información requerida	Bajo	Daniel Castillo	100%	Octubre 27, 2025	Octubre 31, 2025	5
Planeación de la prueba	Medio	Daniel Castillo	100%	Noviembre 03, 2025	Noviembre 07, 2025	5
Ejecución y diagnóstico	Alto	Daniel Castillo	100%	Noviembre 10, 2025	Noviembre 14, 2025	5
Documentación de hallazgos	Bajo	Daniel Castillo	100%	Noviembre 18, 2025	Diciembre 05, 2025	14
Presentación de Resultados	Bajo	Daniel Castillo	100%	Diciembre 09, 2025	Diciembre 12, 2025	4

Ilustración 194 Cronograma Ethical Hacking

Se registraron un total de 333 activos TI segmentados en cinco plantillas:

Networking: 178 activos TI de capa 2 y 3 mayoritariamente.
Windows: 122 activos TI Windows con capacidad de autenticación con credenciales de dominio.

- Linux: 20 activos TI Linux con capacidad de autenticación con credenciales SSH.
- No Auth: 5 activos TI sin capacidad de autenticación.
- VMware: 5 activos TI hipervisores y nodos de virtualización.
- FortiSIEM: 3 activos TI recolectores de eventos y tecnología SIEM.
- Quedo atento a cualquier comentario, requerimiento y/o inquietud.

- Medición de ANS Antivirus

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

ID	Indicadores	Resultado	Meta
AV-1	Cobertura de antivirus	97,67%	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 115 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 diciembre, se realizó la evaluación cuantitativa de la muestra de 272 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	1	99,9%
2. Asunto	1	99,9%
3. Descripción	0	100,0%
4. Prioridad	0	100,0%
5. Categoría	5	99,6%
6. Escalamiento	0	100,0%
7. Solución	9	99,3%
8. Estado del Caso	0	100,0%
9. Justificación Estado del Caso	0	100,0%
10. Periodicidad de seguimientos	0	100,0%
11. Elemento CI	0	100,0%
12. Ortografía y redacción	13	99,0%
13. Cumplimiento de ANS	1	99,9%

Tabla 116 Errores cometidos

Se identificaron 30 errores con un porcentaje de cumplimiento consolidado de 97,79%.
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 13 novedades de ortografía y redacción, 5 de categoría, 9 de solución, tipo de caso 1, Asunto 1 y cumplimiento de ANS 1

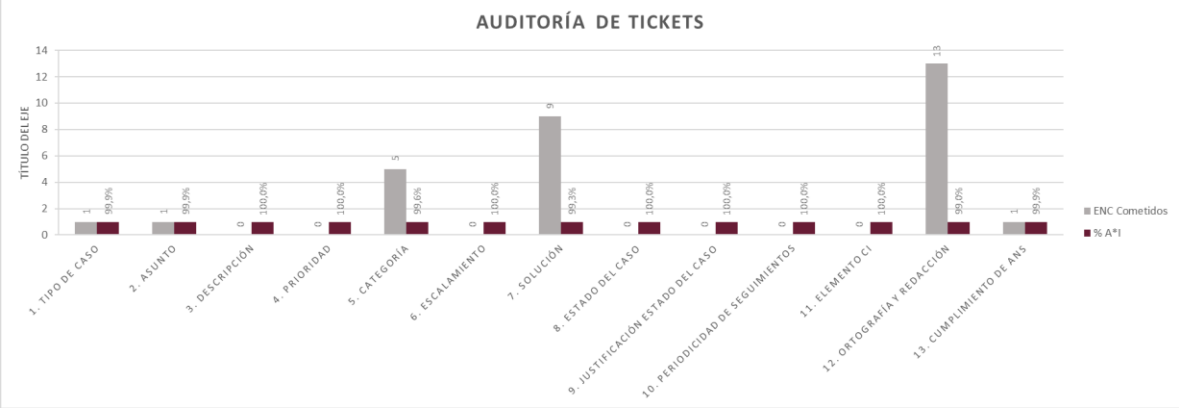


Ilustración 195 Resultados auditoria de casos

5.2 Evaluación de calidad de llamadas

En el mes de diciembre de 2025, 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 117 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 diciembre de 2025. Este apartado contiene información relevante sobre las acciones de mejora identificadas por los Servicios TIC durante el 2025.

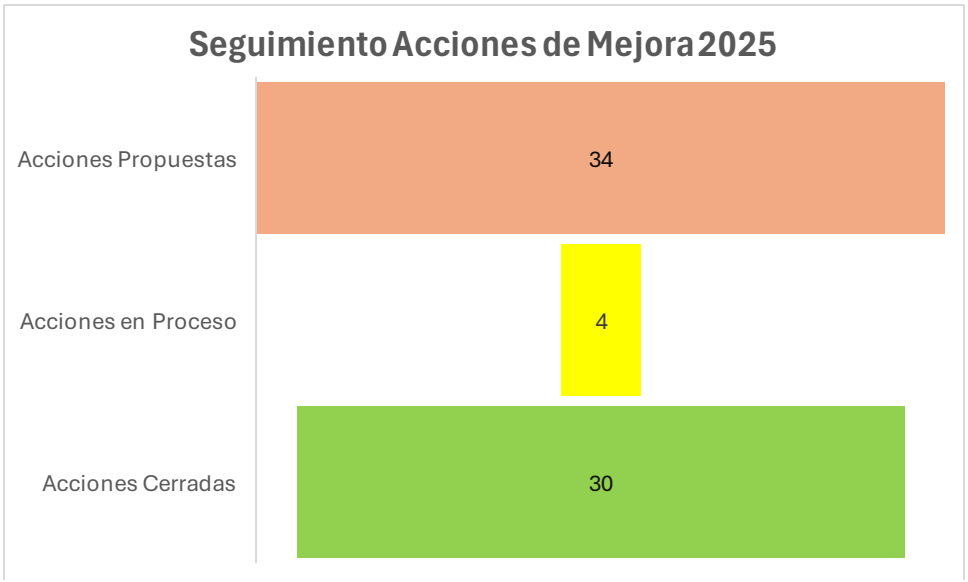


Ilustración 196 Seguimiento Práctica Mejora

En el anterior gráfico, se evidencia de las 34 acciones de mejora identificadas, 4 acciones se encuentran en proceso y cerradas 30 acciones de mejora, lo cual se cuenta con un cumplimiento de ejecución del cuarto trimestre del 88,24% de los diferentes servicios TIC y Gestiones ITIL al corte del 31 de diciembre de 2025.

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 118 KPI Practica de Mejora

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

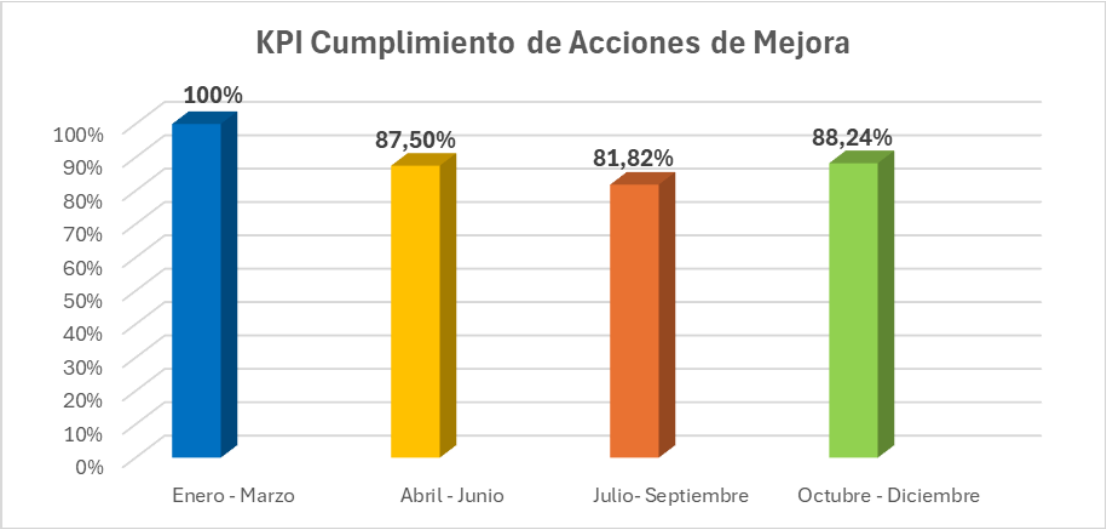


Ilustración 197 Resultado de Cumplimiento AM

Se evidencia el cumplimiento para el periodo de octubre a diciembre del 88,24% en efectividad de las 7 acciones de mejoras propuestas fueron 5 acciones ejecutadas y cerradas durante este periodo y cumplieron con las evidencias de cierre, las 2 acciones pendiente de fin de ejecución, se encuentra previstas para 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 soportemt@mintrabajo.gov.co.	Falla en el acceso y/o sincronización del correo soportemt@mintrabajo.gov.c o	NO	El correo electrónico institucional ha estado disponible
Mesa de servicios	Imposibilidad de contacto por la línea telefónica de la mesa de servicios	Falla en el ingreso de las llamadas a la mesa de servicios	NO	La línea telefónica ha estado disponible
Mesa de servicios	Desborde de solicitudes (vía correo electrónico y/o llamadas) en la Mesa de Servicios	Aumento eventual de la cantidad de solicitudes que supera la capacidad de atención de los Agentes de la Mesa de servicios	NO	No se ha presentado desborde de solicitudes
Mesa de servicios	Riesgo de seguridad de la información que comprometan la confidencialidad, integridad o disponibilidad de la información.	Posibilidad de uso indebido de la cuenta genérica del cliente, asignada para la Mesa de servicios	NO	No se ha presentado dicha situación.
Soporte en sitio	Incumplimiento de los compromisos pactados por atención de actividades urgentes - no planeadas	Solicitud de realización de actividades urgentes no planeadas que afectan la prestación del servicio de acuerdo con lo planeado	NO	No se ha presentado dicha situación.
Todas las prácticas	Deficiencias en la adopción de las prácticas de ITIL	Resistencia a la adopción de las prácticas de ITIL por las partes interesadas	NO	Se proporcionó capacitación a los involucrados
Práctica de Activos	Posibilidad de pérdida de inventario	La pérdida de inventario se produce cuando las cantidades reales del inventario son inferiores a las registradas en el módulo de gestión	NO	Se realizó seguimiento con el equipo de trabajo para revisar los compromisos de la práctica

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

SERVICIO/ PRÁCTICA	NOMBRE	DESCRIPCIÓN	¿MATERIALIZADO?	ACCIONES PARA REALIZAR
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.
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 119 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	$3.949.912
Consumo de clics adicionales		$ 1.859.648
	Subtotal	$ 5.809.560

Tabla 120 Bolsa de Recursos

8 MEDICIÓN DE ACUERDOS DE NIVEL DE SERVICIO

En cumplimiento de lo dispuesto en el Anexo Técnico Base 10102023 – definitivo, Fase de Operación que indica entre otras obligaciones del contratista las siguientes:
Iniciar la medición de ANS y seguimiento de los servicios, entendiéndose que los ANS deben ser configurados desde la fase de transición.

Efectuar la medición de los ANS mensualmente.

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

Área	Nombre Indicador	Resultado	Meta
Mesa de Servicio	Tiempo de atención de solicitudes por soporte en sitio	97,78%	95,00%
	Tiempo de solución de incidentes por soporte en sitio	98,54%	90,00%
	Tiempo de solución de requerimientos por soporte en sitio	99,90%	90,00%
	Tiempo de respuesta de la mesa de servicio	99,02	85,00%
	Abandono de llamadas	0,32%	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	93,33%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
ANTIVIRUS	Cobertura de antivirus	97,67%	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	98,59%	90,00%
	Tiempo de solución de requerimientos asociado a los servicios de administración, soporte y monitoreo	99,81%	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	99,94%	99,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Conectividad WAN e Internet	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Continuidad y disponibilidad del servicio de WAN en sedes nacionales con un solo enlace	(*)	99,60%
	Continuidad y disponibilidad del servicio de WAN en sedes nacionales con doble enlace (principal MPLS + secundario Internet dedicado)	(*)	99,90%
	Continuidad y disponibilidad del servicio de internet en Datacenter principal	100,00%	99,95%
	Continuidad y disponibilidad del servicio de internet en Datacenter alterno	100,00%	99,70%
	Continuidad y disponibilidad del servicio de WAN en Datacenter principal	100,00%	99,95%
	Continuidad y disponibilidad del servicio de WAN en Datacenter alterno	100,00%	99,95%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 121 Medición de Acuerdos de Niveles de Servicio diciembre 2025

(*) 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 diciembre
- detalle_llamadas_recibidas_(01.12.2025-31.12.2025)
- Datos_Mintrabajo_diciembre

FIN DEL DOCUMENTO