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

Junio de 2025

DOCUMENTO/ ARCHIVO	
Código:	**Informe Gestión - Unión Temporal Gestión TIC 2023**
Nombre Archivo:	**Informe Gestión - Unión Temporal Gestión TIC 2023 – Junio 2025**
Fecha:	9/07/2025
Versión:	1

REGISTRO DE CAMBIOS			
Versión	**Páginas**	**Fecha Modificación**	**Motivo del cambio**
1	225	09/07/2025	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 16
Objetivo 16
Alcance 16
Definición de Siglas y Expresiones Técnicas 16
1 GERENCIA Y/O ADMINISTRACIÓN 18
2 LÍNEA DE GESTIÓN DE SERVICIOS 18
2.1. Gestión del Servicio 18
2.1.2. Prácticas ITIL 4 22
2.1.2.1. Práctica Acuerdos Niveles de Servicio (ANS) 22
2.1.2.2. Práctica Habilitación de Cambios 22
2.1.2.3. Práctica Activos 25
2.1.2.4. Práctica Catálogo de servicios 25
2.1.2.5. Práctica de Problemas 27
2.1.2.6. Práctica de Incidentes 27
2.1.2.7. Práctica de Requerimientos ..... **¡Error! Marcador no definido.**
2.1.2.8. Práctica de Eventos 34
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 71
3.1. Datacenter 71
3.1.1. Datacenter Principal 71
3.1.2. Datacenter Alterno y DRP 93
3.1.3. Procesamiento, Almacenamiento y Respaldo 97
3.1.4. Aplicaciones Especializadas 103
3.1.5. **No aplica** 152
3.1.6. Seguridad Informática 152
3.1.6.1. Firewalls de nueva generación 153
3.1.6.2. Sandbox – Amenazas día 0 157
3.1.6.3. SIEM - Solución de correlación de eventos de seguridad, disponibilidad y recursos 160
3.1.6.4. WAF - Servicio de tipo “Firewall de Aplicaciones Web” 167
3.1.6.5. Solución de Anti-DDoS 169
3.1.7. Licenciamiento 173
3.1.8. Administración, soporte y monitoreo 174
3.2. No aplica 175
3.3. Conectividad WAN, SDWAN e Internet 175

3.3.1. Canales WAN 175
3.3.1.1. Incidentes de Conectividad 176
3.3.1.2. Topología Actual 177
3.3.2. Canales SDWAN e Internet Dedicado 177
4. LINEA DE SERVICIOS EN SEDE 182
4.1. Equipos de Cómputo de usuario final 182
4.1.1. Equipos de Escritorio 184
4.1.2. Equipos Portátiles 184
4.2. Conectividad LAN y WLAN 185
4.2.1. Switch CORE Sede Principal 187
4.2.2. Switch para conexiones perimetrales (EDGE) en sede principal 187
4.2.3. Switch de acceso 24 puertos 187
4.2.4. Switch de acceso 48 puertos 188
4.2.5. Puntos de Acceso 188
4.3. Telefonía IP 189
4.3.1. Teléfono Gama Media 190
4.3.2. Teléfono Gama Baja 190
4.3.3. Troncales SIP 191
4.3.4. No Aplica 191
4.3.5. No Aplica 191
4.3.6. Módems 4G – Con plan de 50 Gbps 191
4.4. Energía Regulada UPS 197
4.4.1. UPS 10 kVA 197
4.4.2. UPS 15 kVA 197
4.4.3. UPS 20 kVA 198
4.5. No aplica 199
4.6. Outsourcing de Impresión 199
4.6.1. No aplica 203
4.6.2. Multifuncional B/N rango medio – Cargo fijo mensual 203
4.6.3. Impresora Color rango medio – Cargo fijo mensual 203
4.6.4. No aplica 203
4.6.5. Multifuncional B/N rango medio – Clic de impresión 203
4.6.6. Impresora Color rango medio – Clic de impresión 203
4.7. Antivirus 204
4.7.1. Instalaciones de antivirus en servidores 204
4.7.2. Instalación de antivirus PCs usuarios final 205
4.7.3. Top 10 spyware 205

4.7.4. Top 10 Virus Detectados 207
4.7.5. Servicio de Vulnerabilidades 209
4.7.5.1. Inventario y licenciamiento 209
4.7.5.2. Escaneos programados 210
4.7.5.3. TOP 10 – Vulnerabilidades más explotables 211
4.7.5.4. Estrategia de remediación y/o mitigación 212
4.7.5.5. Resumen de mitigación efectuada 212
4.7.5.6. Ethical Hacking Primer semestre 2025 213
5. GESTIÓN DE CALIDAD DE INFORMACIÓN 214
5.1 Metodología calidad documental de casos 214
5.2 Evaluación calidad documental de casos 215
5.3 Metodología de calidad de llamadas 216
5.4 Evaluación de calidad de llamadas 219
6. GESTION DE RIESGOS 220
7. BOLSA DE RECURSOS 222
8. MEDICIÓN DE ACUERDOS DE NIVEL DE SERVICIO 222
9. ANEXOS 224

Índice de Tablas

Tabla 1 Atención de solicitudes por grupo de especialistas 20
Tabla 2 Disposición de residuos electrónicos y RAEEs DT Santander 20
Tabla 3 Tipificación de cambios 23
Tabla 4 Medición Indicador Porcentaje de Cambios Exitosos 23
Tabla 5 Novedad Matriz de Escalamiento 25
Tabla 6 Captura de pantalla Matriz de Escalamiento MDS 26
Tabla 7 KPI Práctica Catálogo de Servicios 27
Tabla 8 Estados Incidentes 27
Tabla 9 Top 10 Incidentes 28
Tabla 10 Casos Suspendidos 28
Tabla 11 Incidentes Mayores Registrados 29
Tabla 12 KPI Práctica de Incidentes 30
Tabla 13 Causas Reaperturas 31
Tabla 14 Estado de Solicitudes 32
Tabla 15 Seguimiento del Backlog Suspendidos 32
Tabla 16 Top 10 Jerarquía de Requerimientos 33
Tabla17 Detalle de KIP Practica de Requerimientos 33
Tabla 18 Casos reabiertos 34

Tabla 19 KPI Práctica Eventos 35
Tabla 20 Consolidado disponibilidad de servidores 50
Tabla 21 Consolidada disponibilidad de Directorio Activo 51
Tabla 22 Desagregado de Disponibilidad Directorio Activo 51
Tabla 23 Consolidado disponibilidad de equipos Datacenter principal 51
Tabla 24 Desagregado de Disponibilidad Datacenter Principal 51
Tabla 25 Consolidado disponibilidad de equipos Datacenter alterno 51
Tabla 26 Desagregado Disponibilidad de equipos Datacenter alterno 51
Tabla 27 Consolidado disponibilidad de equipos redes y conectividad 52
Tabla 28 Consolidado disponibilidad de equipos de seguridad 52
Tabla 29 Disponibilidad de equipos Seguridad de la Información 52
Tabla 30 Consolidado disponibilidad de equipos de telefonía 52
Tabla 31 Consolidado disponibilidad de plataforma antivirus 52
Tabla 32 Atención de Llamadas 54
Tabla 33 Top 10 administración de servidores 56
Tabla 34 Top 10 redes y conectividad 56
Tabla 35 Top 10 seguridad informática 57
Tabla 36 Top Telefonía IP 57
Tabla 37 Top 10 soporte aplicaciones 58
Tabla 38 Top 10 soporte microinformática 59
Tabla 39 Casos Anulados por Servicio 59
Tabla 40 Casos Suspendidos por Servicio 60
Tabla 41 Incidentes solucionados por Soporte Territoriales 61
Tabla 42 Requerimientos solucionados por Mesa de Servicios 61
Tabla 43 Requerimientos solucionados por Soporte en sitio 62
Tabla 44 Requerimientos solucionados por Soportes Territoriales 62
Tabla 45 Casos cerrados por la mesa de servicios 64
Tabla 46 Casos cerrados por soporte en sitio 65
Tabla 47 Casos cerrados por Territoriales 67
Tabla 48 Casos usuarios VIP 67
Tabla 49 Casos usuarios Regulares 67
Tabla 50 Visitas en sedes sin Soporte en Sitio 70
Tabla 51 Medición ANS Mesa de Servicios 71
Tabla 52 capacidades de acuerdo con las fichas técnicas 74
Tabla 53 Infra total + servidores de pruebas + servidores a desaprovisionar 74
Tabla 54 Infra total producción + servidores de pruebas de la entidad 74
Tabla 55 Infra total sin servidores de pruebas 74

Tabla 56 Capacidades consumidas por entornos de pruebas 74
Tabla 57 Capacidades consumidas (Sin servidores de backup) 75
Tabla 58 Migración actividades .NET 107
Tabla 59 Comportamiento casos GD 121
Tabla 60 Total Instancias 127
Tabla 61 Total Documentos 128
Tabla 62 Total radicados 128
Tabla 63 Dimensionamiento Servers IBM - Virtualización Optima 128
Tabla 65 Apps & DDBB Oracle 132
Tabla 66 Escenario de Capacidades Oracle - Estado de consumo Actual 133
Tabla 67 Escenario de Capacidades Oracle - Total de recursos empleados 133
Tabla 68 Top tráfico de aplicaciones 155
Tabla 69 eventos detectados por el SIEM 166
Tabla.70 Listado de requerimientos atendidos 171
Tabla.71 Ejecución de archivos maliciosos 171
Tabla.72 Vulnerabilidades en la infraestructura 171
Tabla.73 Ataque de Phishing dirigidos 171
Tabla 74 Licenciamiento 173
Tabla 75 Medición ANS Datacenter 174
Tabla 76 Medición ANS Nube Pública 175
Tabla 77 Novedades servicio de internet 177
Tabla 78 Medición de ANS Conectividad WAN e Internet 180
Tabla 79 Desagregado sedes con novedad un solo enlace 181
Tabla 80 Cantidades de equipos a distribuir a nivel nacional 182
Tabla 81 Cantidades de equipos asignados nivel nacional 182
Tabla 82 Cantidades de equipos por devolución nivel nacional 182
Tabla 83 Estado de casos de garantía. 183
Tabla 84 ANS casos de garantía. 183
Tabla 85 ANS Relación casos de garantía 183
Tabla 86 ANS Equipos en siniestro 184
Tabla 87 *Avance instalación de equipos* 184
Tabla 88 Solicitudes de Equipos Usuario Final – Según Grupo Responsable 185
Tabla 89 Solicitudes de Equipos Usuario Final – Según Tipificación y Categoría 185
Tabla 90 Medición ANS Equipos de Usuario Final 185
Tabla 91 Top 5 de categorías en el Servicio de conectividad LAN-WLAN 186
Tabla 92 Distribución y Cantidades de switch 24 puertos 187
Tabla 93 Distribución y Cantidades de Switch 48 puertos 188

Tabla 94 Distribución de puntos de acceso 189
Tabla 95 Medición ANS LAN y WLAN 189
Tabla 96 Equipos gama media..... 190
Tabla 97 Sedes cerradas 190
Tabla 98 Consolidado de teléfonos gama baja..... 190
Tabla 99 Consolidado equipos MIFI 191
Tabla 100 Minutos, consumos 192
Tabla 101 Top 5 llamadas LDN..... 193
Tabla 102 Top 5 llamadas LDI 194
Tabla 103 Top 5 llamadas Celular 195
Tabla 104 Top 5 llamadas locales..... 195
Tabla 105. Capacitaciones y divulgaciones 195
Tabla 106 Medición ANS Telefonía IP 197
Tabla 107 Inventario de UPS – 10kVA 197
Tabla 108 Inventario de UPS – 20Kva..... 198
Tabla 109 Medición ANS Energía Eléctrica UPS..... 198
Tabla 110 Inventario de impresoras para el servicio 199
Tabla 111 Consumo de impresiones por usuario - Impresoras B/N 200
Tabla112 Top 10 de impresoras con mayor uso..... 200
Tabla113 Top usuarios impresión a color 200
Tabla114 Top oficinas 201
Tabla 115 Top 10 impresoras más usadas del servicio de fotocopiado 201
Tabla 116 Ampliación de cuota de impresión 202
Tabla 117 Despacho de papel a sedes del Ministerio del Trabajo 202
Tabla 118 Cargo mensual multifuncional rango medio..... 203
Tabla 119 Cargo mensual impresora color 203
Tabla 120 Clics de Impresión de junio 2025 – Multifuncional B/N..... 203
Tabla 121 Tendencia de consumo de clics B/N..... 203
Tabla 122 Clics de Impresión de junio 2025 – Impresora Color 204
Tabla 123 tendencia de consumo de clics color 204
Tabla 124 Medición ANS Outsourcing de Impresión 204
Tabla 125 Top spayware..... 207
Tabla 126 Total de vulnerabilidades 211
Tabla 127 TOP 10 - Activos más explotables..... 212
Tabla 128 Ethical Hacking Primer semestre 214
Tabla 129 Medición de ANS Antivirus..... 214
Tabla 130 Criterios y parámetros calidad documental casos 215

Tabla 131 Errores cometidos 216
Tabla 132 Precisión Error NO CRÍTICO – PENC 218
Tabla 133 Criterios y parámetros calidad de llamadas 218
Tabla 134 Calificación Calidad llamadas 218
Tabla 135 Resultado de criterios y parámetros - Calidad de llamadas 219
Tabla 136 Seguimiento a riesgos 222
Tabla 137 Bolsa de Recursos 222
Tabla 138 Medición de Acuerdos de Niveles de Servicio junio 2025 223

Ilustración 1 Estado de casos en el período 19
Ilustración 2 Publicación de documentos en la SVE ..... **¡Error! Marcador no definido.**
Ilustración 3 KPI Efectividad de Resolución de Incidentes de Servicio 30
Ilustración 4 KPI Incidentes de Reabiertos en el periodo 31
Ilustración 5 KPI Efectividad de Resolución de Requerimientos de Servicio 33
Ilustración 6 KPI Requerimientos de Reabiertos en el periodo 34
Ilustración 7 Eventos por Tipo de Equipo 36
Ilustración 8 Sedes afectadas por router 36
Ilustración 9 Causas de eventos generados por router 37
Ilustración 10 Casos suspendidos VS. Casos solucionados de Router 38
Ilustración 11 Sedes Afectadas 38
Ilustración 12 Causa de eventos generados por Switch 39
Ilustración 13 Casos suspendidos VS. Casos solucionados de Switch 39
Ilustración 14 Top 10 Sedes afectadas por Access Point 40
Ilustración 15 Causa de eventos generados por AP 40
Ilustración 16 Casos suspendidos VS. Casos solucionados de AP 41
Ilustración 17 Top 10 Sedes afectadas por Starlink 41
Ilustración 18 Causas de eventos generados por Starlink 42
Ilustración 19 Casos suspendidos VS. Casos solucionados de Starlink 43
Ilustración 20 Top 10 Sedes afectadas por FortiGate 43
Ilustración 21 Causas de eventos generados por FortiGate 44
Ilustración 22 Casos suspendidos VS. Casos solucionados de FortiGate 44
Ilustración 23 Casos suspendidos VS. Solucionados 45
Ilustración 24 Causas de alarmas Servidores Windows 46
Ilustración 25 TOP 5 de servidores Windows con más alarmas 46
Ilustración 26 Casos suspendidos VS. Solucionados o cerrados Servidores Windows 47
Ilustración 27 21 Causas de alarmas Servidores Linux 47
Ilustración 28 TOP 5 de Servidores Linux con más alertas 48

Ilustración 29 Casos suspendidos VS. Solucionados o cerrados Servidores Linux 48
Ilustración 30 Seguimiento Pruebas de Disponibilidad 53
Ilustración 31 Seguimiento Práctica Implementación 53
Ilustración 32 Atención de Llamadas 54
Ilustración 33 Incidentes Solucionados por Soportes Territoriales 61
Ilustración 34 Requerimientos Solucionados por la Mesa de Servicios 61
Ilustración 35 Requerimientos Solucionados por Soporte en sitio 62
Ilustración 36 Requerimientos solucionados por Soportes Territoriales 62
Ilustración 37 Casos cerrados por la mesa de servicios 64
Ilustración 38 casos cerrados por Soporte en Sitio 66
Ilustración 39 Casos cerrados por Territoriales 67
Ilustración 40 Modo de Ingreso de Solicitudes 68
Ilustración *41* Cumplimiento WSUS 72
Ilustración 42 Estado final de los casos Windows 72
Ilustración 43 Casos por categorías Windows 73
Ilustración 44 Estado final de los casos Nube privada 73
Ilustración 45 Casos por categoría Nube privada y pública 73
Ilustración 46 Estado File Server Mintrab60 75
Ilustración 47 Bondades de la implementación del Well Architected Framework (WAF) 76
Ilustración 48 Proyección de Modelo de Suscripción 76
Ilustración 49 Modelo de Tenant bajo arquitectura 77
Ilustración 50 Suscripción de Conectividad 77
Ilustración 51 Grupo de recursos Suscripción de Conectividad 78
Ilustración 52 Sesión ejecución de cambio 79
Ilustración 53 Evidencia de Inasistencia del proveedor 79
Ilustración 54 Web App sin despliegues 80
Ilustración 55 Ejecución de Flujo 80
Ilustración 56 Errores de ejecución 81
Ilustración 57 Comportamiento SWCORE Datacenter Colombia XV 92
Ilustración 58. Grafica de consumo canal Internet Datacenter 93
Ilustración 59 Diagrama Interoperabilidad Bogotá CXV 94
Ilustración 60 VM Replicadas a través de site recovery 94
Ilustración 61 Diagrama de Replicación CXV - Santa Mónica 95
Ilustración *62* Puerto de conexión extremo Bogotá 95
Ilustración *63* Puerto de conexión extremo Cali 96
Ilustración 64 Estado SWCORE Datacenter alterno 97
Ilustración 65 Hardware solicitado ..... **¡Error! Marcador no definido.**

Ilustración 66 Componentes Moodle nuevo ..... **¡Error! Marcador no definido.**
Ilustración *67* Estado final de casos – Aplicaciones Especializadas 104
Ilustración 68 categorías Apps 104
Ilustración 69 Estado pre-ventana 111
Ilustración 70 Generación de Backups DDBB 111
Ilustración 71 Validación Tablas DDBB 112
Ilustración 72 Validación Tablas DDBB 112
Ilustración 73 Validación Tablas DDBB 112
Ilustración 74 Validación Tablas DDBB 113
Ilustración 75 Validación Tablas DDBB 113
Ilustración 76 Validación Tablas DDBB 113
Ilustración 77 validación Tablas DDBB 114
Ilustración 78 Verificación Registros 114
Ilustración 79 Verificación Registros 114
Ilustración 80 Verificación Registros tras ejecución de procesos 115
Ilustración 81 Validación de estado de tablas tras ejecución de procesos 115
Ilustración 82 Estado de instancias DDDB 115
Ilustración 83 Eliminación de instancias 116
Ilustración 84 Disminución de instancias tras ejecución de proceso 116
Ilustración 85 Estado del servidor - pre-desfragmentación 116
Ilustración 86 Ejecución desfragmentación 117
Ilustración 87 Ejecución desfragmentación 117
Ilustración 88 Ejecución desfragmentación 117
Ilustración 89 Reconstrucción de Índices 118
Ilustración 90 Validación de tamaños de tablas 118
Ilustración 91 Validación de tamaños de tablas 118
Ilustración 92 Validación de tamaños de tablas 119
Ilustración 93 Validación de tamaños de tablas 119
Ilustración 94 Validación de tamaños de tablas 119
Ilustración 95 Validación de tamaños de tablas 120
Ilustración 96 Validación de tamaños de tablas 120
Ilustración 97 Ejecución de estadísticas de validación 120
Ilustración 98 Distribución de licencias Oracle 128
Ilustración 99 Licencias ambientes 129
Ilustración 100 Casos IBM - Servicio 129
Ilustración 101 categoría DDBB 129
Ilustración 102 Casos DDBB por Servicio 130

Ilustración 103 casos DDBB 131
Ilustración *104* Estado Bases de Datos 131
Ilustración 105 Información base de datos – Servidor 133
Ilustración 106 Estadísticas CPU 133
Ilustración 107 Estadísticas Memoria 133
Ilustración 108 Estadísticas Pool compartido 134
Ilustración 109 Tamaño DDBB 134
Ilustración 110 Tamaño Esquema DDBB 134
Ilustración 111 Rendimiento DDBB 135
Ilustración 112 DDBB por Server 135
Ilustración 113 Host e Instancia CPU 135
Ilustración 114 Estadísticas Memoria 135
Ilustración 115 Estadística Shared Pool 136
Ilustración 116 Tamaño DDBB DBMINTRA 136
Ilustración 117 Tamaño Esquema DDBB 136
Ilustración 118 Rendimiento DDBB MINTRASG 136
Ilustración 119 Información DDBB PLIFERAY 137
Ilustración 120 Host e Instancia CPU 137
Ilustración 121 Estadísticas Memoria 137
Ilustración 122 Estadísticas Shared Pool 137
Ilustración 123 Tamaño DDBB PLifeRay 137
Ilustración 124 Tamaño Esquemas DDBB 138
Ilustración 125 Rendimiento DDBB PlifeRay 138
Ilustración 126 Información DDBB SIGEP 138
Ilustración 127 Estadística Host e Instancia 139
Ilustración 128 Estadística Memoria 139
Ilustración 129 Estadística Shared Pool 139
Ilustración 130 Tamaño DDBB SIGEP 139
Ilustración 131 Tamaño Esquema DDBB 140
Ilustración 132 Rendimiento DDBB SIGEP 140
Ilustración 133 Información DDBB DBSIMPC 140
Ilustración 134 Estadística CPU 141
Ilustración 135 Estadística Memoria 141
Ilustración 136 Estadística Shared Pool 141
Ilustración 137 Tamaño DDBB SIMPC 141
Ilustración 138 Tamaño Esquema DDBB 141
Ilustración 139 Rendimiento DDBB 142

Ilustración 140 Información servidor DBBB 142
Ilustración 141 Host e Instancia CPU 143
Ilustración 142 Estadística memoria 143
Ilustración 143 Estadística Shared Pool 143
Ilustración 144 Tamaño DDBB MINTRASD 143
Ilustración 145 Tamaño Esquemas 144
Ilustración 146 Rendimiento MINTRASD 144
Ilustración 147 Información Server DDBB 145
Ilustración 148 Host e Instancia CPU 145
Ilustración 149 Estadística Memoria 145
Ilustración 150 Estadística Shared Pool 145
Ilustración 151 Tamaño DDBB 145
Ilustración 152 Tamaño DDBB 146
Ilustración 153 Rendimiento DDBB 146
Ilustración 154 Información Server DDBB 147
Ilustración 155 Host e Instancia CPU 147
Ilustración 156 Estadística Memoria 147
Ilustración 157 Estadística Shared Pool 147
Ilustración 158 Tamaño DDBB 148
Ilustración 159 Tamaño Esquemas DDBB 148
Ilustración 160 Rendimiento DDBB 149
Ilustración 161 Información Server DDBB 149
Ilustración 162 Estadística CPU 149
Ilustración 163 Estadística Memoria 150
Ilustración 164 Estadística Shared Pool 150
Ilustración 165 Tamaño Esquemas DDBB 150
Ilustración 166 Comportamiento DDBB 151
Ilustración 167 Almacenamiento ASM 151
Ilustración 168 DiskGroup Data 151
Ilustración 169 DiskGroup Flash 152
Ilustración 170 DiskGroup Reco 152
Ilustración 171 DiskGroup Redo 152
Ilustración 172 Licenciamiento adicional componente IBM 152
Ilustración*173* Disponibilidad firewall 153
Ilustración*174* Comportamiento ancho de banda 154
Ilustración *175* Reporte consumo ancho de banda 154
Ilustración*176* Top de usuarios 155

Ilustración *177* Top tráfico de aplicaciones 155
Ilustración 178 Top 15 Authenticated Logins by VPN Connections 156
Ilustración *179* Failed Login Attempts by User 157
Ilustración 180 estadísticas de escaneo 158
Ilustración *181* performance 159
Ilustración *182* Licenciamiento 160
Ilustración *183* Casos de uso 161
Ilustración *184* Disponibilidad 162
Ilustración *185* Autenticación de seguridad 164
Ilustración *186* Violación de políticas 165
Ilustración *187* eventos detectados por el siem 165
Ilustración 188 Disponibilidad de servidores- Seguridad 166
Ilustración 189 Top Aplicaciones por Bandwidth 167
Ilustración 190 Top attack types 168
Ilustración 191 Top de ataques 169
Ilustración 192 Login fallidos 170
Ilustración 193 Políticas y procedimiento de seguridad 172
Ilustración 194. Grafica de consumo canal MPLS Datacenter 175
Ilustración 195j Uptime del equipo MPLS Datacenter 176
Ilustración 196. Topología actualizada 177
Ilustración 197. Interface Fortimanager 178
Ilustración 198. Interface MPLS HUB SDWAN 178
Ilustración 199 Interface Internet HUB SDWAN 179
Ilustración 200. VPN SDWAN establecidas 179
Ilustración 201. Estado HUB SDWAN Datacenter 179
Ilustración 202. Estado HA HUB Sdwan 179
Ilustración 203. Recursos Fortimanager 180
Ilustración 204 Estado de casos Redes y Conectividad 187
Ilustración *205*. Licencias y extensiones 192
Ilustración 206 Estadística de tráfico 192
Ilustración 207 Top LDN 193
Ilustración 208 Top LDI 194
Ilustración 209 Top Celular 194
Ilustración 210 Top Local 195
Ilustración *211* Requerimientos por garantía 196
Ilustración 212 Disponibilidad y Continuidad TOIP 196
Ilustración 213 Equipos consola antivirus 205

Ilustración 214 Gestión consola antivirus – equipos usuario final 205
Ilustración 215 Top 10 Spyware 206
Ilustración 216 Top 10 virus detectados 208
Ilustración 217 Top infección virus 208
Ilustración 218 Gestión consola Nessus 210
Ilustración 219 Escaneos programados 210
Ilustración 220 Vulnerabilidades gestionadas vs en remediación 213
Ilustración 221 Criterios calidad documental casos 215
Ilustración 222 Resultados auditoria de casos 216
Ilustración 223 Precisión error no Critico de llamadas 217
Ilustración 224 Precisión error Critico de llamadas 217
Ilustración 225 Resultados llamadas PENC 219
Ilustración Resultados226 llamadas PEC 219

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 junio 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 en gestión no se adelantó ningún modificatorio.

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:

El equipo de Gestores ITIL y procesos apoyaron la operación de los servicios con la elaboración, recepción de VoBo por parte de la coordinación de Grupo de Soporte Informático 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.

Se tiene en proceso de revisión y aprobación por parte de la entidad los siguientes comunicados:

- El 13 de marzo 2025 se envía a la Coordinación del Grupo de Soporte Informático la propuesta del contenido sugerido para la intranet relacionada con el Grupo de Soporte Informático. Debido al cambio de personal en el grupo, se está a la espera retomar esta iniciativa para verificar quien es el enlace con Oficina de Comunicaciones para ampliar el tema e incluir las observaciones correspondientes.



Propuesta de
información para Intra

b. Traslados y novedades de sedes:

- **Instalación de puntos de red en las Inspecciones de trabajo Acacías (Meta) y Tumaco (Nariño) luego de traslado de inmueble:** El 17/06/2025 se remite vía correo electrónico al Coordinador del Grupo de Soporte Informático los informes, actas y registro fotoIlustración de las actividades de instalación de puntos de red, realizadas por parte de la UT.



RE_ Cotizaciones
instalaciones puntos c

- **Anserma / Caldas:** Por remodelación física de la alcaldía del municipio, la sede fue trasladada temporalmente a un local cercano a cuenta del inspector mientras terminan las adecuaciones, la sede está en ese lugar desde el 8 de marzo de 2025. Se tiene en seguimiento hasta que se requiera retorno al lugar definitivo y organización de los equipos a cargo de la UT.
- **Santa Barbara / Antioquia:** E 27 de junio 2025 el inspector se retiró por pensión pero no se tiene una nueva asignación de personal para la sede. Se dejan equipos apagados pero sin confirmación por parte del ministerio para recuperación de inventario, a espera de novedades en relación con la asignación de funcionario. Se programa mantenimiento

en la herramienta de monitoreo Zabbix para que no se generen alarmas durante el tiempo de apagado de la sede.

- **San Gil / Santander:** Se realiza traslado de la sede sin previo aviso a la UT, el usuario realiza movimiento de equipos, se programa visita de personal de soporte de la UT para la conexión de equipos y habilitación de Modem provisional mientras se gestiona el traslado del canal de MPLS.

c. Volumetría de Solicitudes Gestionadas:

En el mes de junio 2025 se registraron en la herramienta ITSM 5774 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: 5244
  - Incidentes: 512
  - Cambios: 17
- Casos Anulados: 7 - 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 Junio 2025:

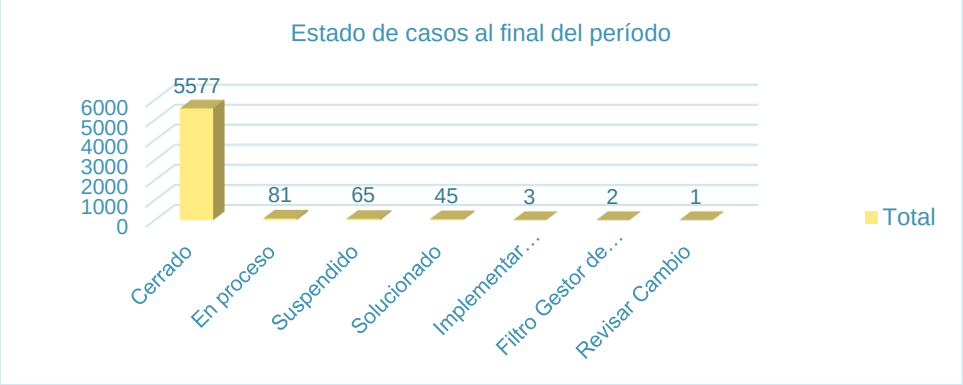


Ilustración 1 Estado de casos en el período

- Gestión por parte de los grupos de especialistas:

Grupo Responsable	Cantidad de casos gestionados	Porcentaje de casos gestionados (%)
Responsable_Soporte_Bogota	2090	36,20
Responsable_Soporte_Territoriales	1454	25,18
Responsable_Mesa_De_Servicio	642	11,12
Responsable_Soporte_Impresoras	567	9,82
Especialistas_IBM	380	6,58
NOC	214	3,71
SOC	148	2,56
Responsable_De_Servidores_Windows	83	1,44
Especialista Nube Privada	40	0,69
Especialista_Telefonía_IP	38	0,66
Especialista Herramientas de Gestion	30	0,52
Especialista Base de datos	21	0,36
Especialista Nube Publica	13	0,23

Grupo Responsable	Cantidad de casos gestionados	Porcentaje de casos gestionados (%)
Almacenamiento y Backups	13	0,23
Responsable Garantías Equipos	10	0,17
Especialista Aplicaciones .Net	8	0,14
Especialista Redes	8	0,14
Gestor de Inventarios	7	0,12
Liferay	4	0,07
Gestión del Servicio	2	0,03
Especialista Aplicaciones JAVA	1	0,02
CAB	1	0,02
TOTAL	**5774**	**100,0**

Tabla 1 Atención de solicitudes por grupo de especialistas

d. Plan de trabajo documentos SIG para publicación en la SVE

Se tiene pendiente por parte de la UT completar el entregable y definir bien las evidencias para el siguiente documento, la cual se encuentra en curso:

- Instructivo Preparación y Asignación del activo

Una vez se cuente con el VoBo de la entidad, se procederá a la entrega a la OAP del paquete completo de documentos que incluyen:

- Guía Práctica de Catálogo en los Servicios de Tecnologías de Información
- Guía Práctica de Disponibilidad en los Servicios de Tecnologías de Información
- Guía Práctica de Gestión de Activos en los Servicios de Tecnologías de Información
- Instructivo de entrega, salida, retiro, y baja de activos

e. Disposición de RAEES y Residuos Electrónicos

El 11/06/2025 se gestiona y coordina recolección de residuos por parte del proveedor SUMA Desarrollo Ambiental en la DT Santander (Bucaramanga).



RV_ Solicitud de
Salida de elementos T

Residuos	Unidades
Cartuchos y tóner de impresoras de oficina	29
Diademas - RAEE	2
Unidades de Tambor - RAEE	4
Total General	35

Tabla 2 Disposición de residuos electrónicos y RAEEs DT Santander

El 10/06/2025 el Ministerio del Trabajo recibe visita de la Secretaría Distrital de Ambiente, donde se validó la gestión de los residuos RAEE's, Cartuchos y Toners de impresión que realiza de forma permanente la UT en Nivel Central. Posterior a la visita, la secretaría remite unas observaciones que se deben ajustar:

- Rótulos o etiquetas: Las cajas o empaques donde se encuentran los Cartuchos y Toners que entran en desuso; así como, los RAEE´S debe estar debidamente rotuladas o etiquetadas.
- Documento matriz de compatibilidad de residuos generados

El 16/06/2025 se remite correo al Coordinador del Grupo de Soporte Informático con las evidencias de cumplimiento a las anteriores observaciones, las cuales fueron subsanadas por parte de la UT.



RE_ SOLICITUD DE
INFORMACIÓN Y ACT

f. Sesiones y divulgaciones con el equipo de trabajo

Se desarrollaron las siguientes sesiones o divulgación de información con el equipo de trabajo:

- Todos los días se realiza sesión vía Microsoft Teams con el personal de Soporte en Sitio de Territorio para conocer las novedades de las DT, OE e Inspecciones soportadas y gestionar en caso de que se requieran los escalamientos necesarios para asegurar la prestación de los servicios de TI.
- El 16/06/2025 se realiza divulgación por correo electrónico del listado actualizado del personal de soporte en sitio.
- El 25/06/2025 se divulga desde la práctica de requerimientos una pieza al personal de la UT para la correcta clasificación de casos en Aranda según Tipo: Incidente, Requerimiento, Cambio y Problema.



Socialización de
Clasificación de Ticket

g. Otras actividades

- El 13 de marzo se envía a la Coordinación del Grupo de Soporte Informático la propuesta de Encuesta de percepción del personal de Soporte en Sitio Territorial (en Forms) y una pieza para recordar la matriz de escalamiento por si se presentan novedades con el personal. Pendiente retoma de esta actividad con el nuevo coordinador del grupo.



Encuesta de
percepción de soporte

- Desde la Dirección del Proyecto de la UT y con todo el apoyo de los líderes de las líneas de servicios y especialistas, se dio respuesta a la entidad sobre las evidencias de cumplimiento y aclaraciones de los servicios de TI relacionadas con:
    - El 4/06/2025: Se comparte con el Ing. Mauricio Fernandez de la Oficina de TICs las topologías de redes para el ministerio.



Solicitud RF-122178
__ Topología Red Min

    - Vía correo electrónico se presentan evidencias del estado operativo de la UPS de la OE Barrancabermeja, administrada por la UT y se aclara que no se requiere ninguna acción adicional por parte de la entidad para la conexión eléctrica de esta.
    - Evidencias de cumplimiento de los servicios: Outsourcing de impresión, Equipos de usuario final, Conectividad y canales de MPLS/Internet, Data Center, Implementación de IPV6, Antivirus, Nube Pública, Póliza Todo Riesgo, Telefonía IP del Despacho del Ministro, Red WiFi Nivel Central.

- En marzo 2025 se generó y entregó informe con las novedades de las UPS propiedad del Ministerio del Trabajo, cableado eléctrico y puntos de red para presentar al Grupo de Recursos Físicos con el propósito que sean subsanadas estas novedades en pro de una buena prestación de los servicios de TI. En abril 2025 la coordinación del Grupo de Soporte

Informático solicita consolidado de los compromisos y los responsables, se genera listado y se comparten los avances a cargo de la UT. Para el período del informe, no se obtienen avances de los compromisos a cargo del ministerio.

2.1.1. Herramienta de Gestión ITSM

Durante junio 2025 se realizaron las siguientes acciones en la herramienta de Gestión Aranda:

- Se aplicaron mejoras a la integración de Aranda con las herramientas del SOC, esta mejora se realizó directamente a los filtros para que los casos puedan ser creados y categorizados de manera más eficiente.
- Con la actualización de Zabbix a la versión 7.2 se han optimizado las características de las dependencias entre los hosts a nivel de monitoreo, con esto se está logrando identificar y crear los casos directamente de los hosts que se afectan y los relacionados a modo informativo.
- En proceso de afinamiento del reporte de software no permitido generado por la herramienta, actividad en conjunto con la práctica de activos.
- **Actualización ASMS:** Se realizo la actualización de la herramienta de gestión de casos, esto con el fin de corregir bugs que se detectan en la herramienta y aplicar mejoras en sus funciones.
- **Actualización ADM**: Se realizo a actualización de la herramienta de inventarios con el fin de mejorar sus funciones de toma de inventarios.
- Acceso a funciones de control remoto: Se otorga acceso a ADM a todo el personal de soporte técnico de territoriales para que tengan acceso a la funcionalidad de toma de control remoto de los equipos de la entidad, todo esto con autorización del funcionario.
- Creación de categorías: se realizó la creación de 3 categorías para el servicio de aplicaciones especializadas del gestor documental, lo anterior con el fin de realizar clasificaciones de casos de manera más precisa.
- El 17/06/2025 se registra caso en Aranda RF-126303 para creación de usuarios de acceso a Zabbix para Luis Guillermo Guerra y Derly Milena Coconubo.
- Por solicitud del Coordinador del Grupo de Soporte Informático el 17/06/2025 se registra caso RF-126815 para acceso de Jorge Galvis a Zabbix y se realiza capacitación de acceso y visualización del tablero.

2.1.2. Prácticas ITIL 4

2.1.2.1. Práctica Acuerdos Niveles de Servicio (ANS)

Dar a conocer las actividades de la Práctica Acuerdos Niveles de Servicios correspondientes al periodo del 1 al 30 de junio de 2025. Este apartado contiene información relevante sobre actividades realizadas y novedades presentadas.

Durante el periodo, se realizó seguimiento y control a los ANS que se tienen parametrizados en la herramienta, y con cada uno de los líderes de servicio, validando su cumplimiento de acuerdo con lo definido contractualmente. Ver Numeral 7. MEDICIÓN DE ACUERDOS DE NIVEL DE SERVICIO

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

- **Tipificación de los cambios**

Durante el mes de junio de 2025 se gestionaron 17 casos tipificados como Cambios, clasificados en las siguientes categorías:

CATEGORÍAS	NÚMERO DE CASOS	PORCENTAJE (%)
Herramientas de Gestión.Aranda	1	5,88%
Seguridad informatica.Firewall de aplicaciones Web - WAF	1	5,88%
Aplicaciones Especializadas.Gestor documental	1	5,88%
Redes y Conectividad.Access point Sede Central	2	11,76%
Administración de servidores.Servidores	3	17,65%
Administración de Bases de Datos.Servidor de base de datos	9	52,94%
Total General	**17**	**100%**

Tabla 3 Tipificación de cambios

Las solicitudes fueron verificadas por el gestor de cambio y se ejecutaron de acuerdo con lo planeado.

- **Relación casos registrados**

A continuación, se presenta la relación de casos registrados del 1 al 30 de junio de 2025, en total se crearon 17 casos de los cuales se gestionaron 11 como cambios de normales, 1 cambios estándar y 5 cambio de emergencia, los cuales se describen a continuación:

SHC_Junio_2025.xlsx

- **Cambios por estado**

Al corte del 30 de junio, once (11) casos quedaron estado *Cerrado,* dos (2) casos quedaron en estado *Filtro Gestor de Cambios*, tres (3) casos quedaron en estado *Implementar Cambio*, un (1) caso quedo en estado *Revisar cambio.*

- **Medición Indicador Porcentaje de Cambios Exitosos**

Nombre	Descripción / Fórmula	Meta	Periodicidad	Resultado Junio
Porcentaje de cambios exitosos.	**PCE = (NCE/TCI)*100** Donde: **PCE:** Precisión Cambios Exitosos **NCE:** Numero de Cambios Exitosos **TCI:** Total de Cambios implementados	80%	Mensual	**PCE=8/11*100** **PCE= 72,73%**

Tabla 4 Medición Indicador Porcentaje de Cambios Exitosos

El indicador Porcentaje de Cambios Exitosos (PCE) tiene como objetivo medir la eficacia en la implementación de los cambios realizados en el entorno tecnológico, evaluando cuántos de estos se completan satisfactoriamente, es decir, sin errores, afectaciones al servicio o necesidad de retrabajo.

Durante el mes de junio, se registraron 17 cambios en total. Sin embargo, para efectos de la medición, solo se consideran los cambios que alcanzaron el estado "Cerrado" al corte del 30 de junio, ya que son los únicos que han finalizado completamente su ciclo de gestión. Bajo este criterio:

- 11 cambios se encuentran en estado Cerrado.

- 2 cambios están en estado Filtro Gestor de Cambios.
- 3 cambios permanecen en Implementar Cambio.
- 1 cambio está en estado Revisar Cambio.

De los 11 cambios cerrados, 8 fueron exitosos y 3 presentaron fallas durante o después de su implementación, razón por la cual el valor del indicador se calcula así:

PCE = (8 / 11) * 100 = 72,73%

No obstante, se deben tener en cuenta las siguientes consideraciones:

- Los cambios RFC-128515 y RFC-128621 fueron ejecutados a finales del mes de mayo. Sin embargo, debido al corto tiempo restante, no fue posible realizar la validación final ni cerrar los casos formalmente en ese mismo mes. Ambos fueron revisados y cerrados exitosamente en julio, sin presentar fallas ni afectaciones al servicio, por lo que pueden considerarse exitosos desde el punto de vista técnico y operativo.

- El cambio RFC-126831 no ha podido ejecutarse debido a que la entidad DNP no ha proporcionado la información necesaria para completar la configuración, situación que ha impedido continuar con el proceso. Por parte de la UT, todo se encuentra listo para su ejecución; sin embargo, se requiere una coordinación adicional con el funcional de la Entidad. Se tiene programada una sesión con el área funcional el 1 de julio, en la que se espera obtener la información pendiente y estimar la fecha de ejecución.

- Los cambios RFC-129146, RFC-126539 y RFC-124988 correspondientes a Eliminar desencadenador en Base de datos RUE, fueron no exitosos debido a que el área funcional no envió la eliminación de los datos en las tablas hijos solo en la tabla padre y por la llave foránea no lo permitió

Si bien no pueden incluirse en la medición del mes o por su fecha oficial de cierre, esta observación permite entender que la gestión de cambios fue efectiva en la mayoría de los casos, y que el incumplimiento del indicador responde más a una condición de tiempo en la revisión que a fallas reales en la ejecución.

Acciones ante el incumplimiento del indicador:

- Análisis de causas de los cambios fallidos, para identificar patrones comunes o fallas en el proceso.

- Revisión del procedimiento de gestión de cambios, asegurando que se cumplan todas las etapas: evaluación de riesgos, pruebas previas, validaciones, entre otros.

- Capacitación o refuerzo técnico a los responsables de ejecutar los cambios, con énfasis en la planificación y mitigación de impactos.

- Implementación de controles adicionales en la etapa de aprobación e implementación para asegurar mayor efectividad.

- Seguimiento puntual a los cambios pendientes de cierre, con el fin de garantizar su correcta ejecución y evitar fallas.

Estas acciones buscan mejorar la confiabilidad del proceso y asegurar que los cambios futuros cumplan con los estándares de calidad y disponibilidad requeridos.

2.1.2.3. Práctica Activos

Durante el mes de junio de 2025, la Práctica de Gestión de Activos llevó a cabo una serie de acciones estratégicas orientadas a asegurar la operatividad continua y la disponibilidad óptima de los servicios tecnológicos de la entidad. Estas actividades se ejecutaron conforme a los lineamientos de las mejores prácticas en gestión de activos, con el propósito de fortalecer el control, la eficiencia operativa y la trazabilidad de los recursos tecnológicos.

- **Seguimiento a la Gestión:** Se realiza quincenalmente un seguimiento sistemático a los procesos asociados a la gestión de activos, con el objetivo de mantener la información actualizada y garantizar el cumplimiento de los procedimientos establecidos.

- **Inventario de Equipos:** Durante el mes, se llevó a cabo un proceso de inventario físico y documental de los equipos tecnológicos, con el fin de mantener una trazabilidad precisa de los activos y reforzar los controles sobre su ubicación y estado.

- **Seguimiento de Casos de Garantías en la Herramienta de Gestión:** Se revisaron los casos registrados en la herramienta de gestión, priorizando su adecuada documentación y cierre oportuno. Esta tarea busca mejorar la trazabilidad de incidencias y optimizar los tiempos de respuesta ante requerimientos.

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 Matriz de Escalamiento**

Durante el período se realizó actualización de la matriz de escalamiento teniendo en cuenta las siguientes novedades, estas fueron socializadas mediante correo electrónico:

Fecha Actualización	Novedades reportadas
13/06/2025	Se realiza actualización del nuevo soporte de Cundinamarca Alberto Villa
16/06/2025	Actualización de listado de usuarios VIP en matriz y Aranda

Tabla 5 Novedad Matriz de Escalamiento

- **Refuerzo y capacitación árbol de categorías:** El 18 de junio se llevó a cabo la socialización de resultados de los casos auditados a nivel de calidad y allí se reforzó el uso adecuado del árbol de categorías en la gestión de incidentes y requerimientos. Durante la sesión se hizo énfasis en los siguientes aspectos clave:

    - Correcta categorización de los casos, según la falla reportada por los usuarios.
    - Importancia de una documentación completa tanto en la apertura como en el cierre del ticket.
    - Asignación adecuada de los casos a los distintos grupos resolutores.
    - Tipificación precisa de los incidentes para facilitar su análisis posterior.
    - Validaciones de primer nivel antes de escalar o cerrar un caso.
    - Esta actividad busca mejorar la calidad del soporte, optimizar los tiempos de resolución y reducir la cantidad de incidentes reabiertos.

- **Ajuste y Actualización Matriz de Escalamiento MDS**

Se está adelantando la actualización de la matriz de escalamiento de la mesa de servicios, con el objetivo de afinar los tipos de fallas y solicitudes, las validaciones de primer nivel que deben aplicarse y los grupos resolutores a los que se debe escalar según la situación reportada por el usuario. Se realizará la socialización a mediados de Julio.

Servicio	Categoría	Tipificación	Descripción Solicitud/Falla	Validaciones de Primer Nivel	Grupo Resolutor
Administración de Bases de Datos	Radicar una solicitud.Base de datos SQL.Restaurar base de datos	Solicitud	**SQL Server:** -Solicitud restauración BD	-Indicar Ip del servidor y Nombre de BD Origen - Indicar Ip del servidor y Nombre de BD Destino	Especialista Base de datos
Administración de Bases de Datos	Radicar una solicitud.Base de datos SQL.Crear base de datos	Solicitud	**SQL Server:** -Solicitud creación BD	-Indicar nombre de la BD - Indicar si va para un server en especifico (Si aplica) Nombre de usuario a crear - Validar e indicar si en un usuario del DA o del SQL - Validar e indicar el tipo de permisos a asignar (Lectura, escritura, control total) - Adjuntar aprobación de la supervisión del contrato - Indicar ambiente de la BD (Pruebas , pre-producción, producción) - Nombre de la APP a la que pertenece	Especialista Base de datos
Telefonía IP	Radicar una solicitud.Servicios.Asignacion de Extension	Solicitud	Solicitud para asignar una extensión	- Nombre del funcionario - Validar e indicar si el funcionario ya tenía ext asignada - Correo del funcionario	Especialista_Telefonía_IP
Telefonía IP	Radicar una solicitud.Hardphone.Asignacion	Solicitud	Asignación de teléfono físico	- Nombre del funcionario - Validar e indicar si el funcionario tiene ext asignada - Correo del funcionario - Ubicación del funcionario	Especialista_Telefonía_IP
Telefonía IP	Reportar una falla.Servicios.No ingresan llamadas	Incidente	Llamadas Ingreso de llamadas (Mudas)	-Descripicón de lo sucedido -Print de la llamada (Fecha y hora) -Extensión	Especialista_Telefonía_IP

Tabla 6 Captura de pantalla Matriz de Escalamiento MDS

- **Creación de Nuevas Categorías**

De acuerdo con la necesidad de la operación, se crearon las siguientes categorías:

- **Servicio:** Aplicaciones especializadas
  Tipo: Solicitud
  Categoría: Radicar una solicitud.Gestor documental.Relanzamiento

- **Servicio:** Administración de Servidores
  Tipo: Solicitud
  Categoría: Radicar una solicitud.Correo Electronico.Retiro de Licencia

- **Servicio**: Administración de Servidores
  Tipo: Solicitud
  Categoría: Radicar una solicitud.Buzón Compartido. Crear/Modificar/Eliminar

- **Servicio:** Administración de Servidores
  Tipo: Solicitud
  Categoría: Radicar una solicitud.Correo Electronico.Configuración MFA

- **Servicio**: Soporte Microinformática
  Categoría: Agente Aranda- Instalación-Desinstalación
  ANS: El mismo asociado a solicitudes de Soporte

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 Junio

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= (5**/5)*100 **EF= 100%**

Tabla 7 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 del 1 al 30 de junio de 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.

Por parte de las practicas ITIL, se realizó durante el mes la socialización a todo el personal del proyecto frente a la clasificación y tipo de casos.

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 comprendido entre el 1 y el 30 de junio de 2025. Se incluye información relevante sobre los incidentes registrados, las acciones ejecutadas y las novedades ocurridas.

Durante el período del informe, se registraron 512 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 detallados anteriormente:

Estado	Cantidad
Cerrado	504
En proceso	1
Solucionado	3
Suspendido	4
Total general	**512**

Tabla 8 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	131	Incidentes generados en el servicio de redes y conectividad por afectaciones en infraestructura del proveedor.
Reportar una falla.Alarma Zabbix.Starlink	64	Intermitencias presentadas por: condiciones climáticas adversas (tormentas, nubes densas), obstrucciones físicas (techos, árboles), fluctuaciones eléctricas y ajustes en la cobertura satelital en regiones específicas.
Reportar una falla.Falla impresora.No imprime	33	Incidentes generados en el servicio de impresión: desconexión de impresoras por falta de comunicación con el servidor tras cambio de contraseña, alertas por tamaño de papel incorrecto, cancelación de documentos por cupos de impresión agotados, finalización de saldos, cables de red desconectados, entre otros.
Reportar una falla.Gestor Documental.Falla Funcional	26	El 96% de los casos corresponde a errores en la aplicación del gestor documental. Se destacan reprocesos, relanzamientos y sobrecarga del sistema debido al desconocimiento de los flujos por parte de los usuarios.
Reportar una falla.Equipo de computo.Falla - Error conexión a red	26	Errores por conexión en puertos incorrectos, cambios de IP por bloqueo, patch cord desconectado, cambios de contraseña, red del proveedor con fallas, tarjeta inalámbrica inhabilitada, y problemas con controladores.
Reportar una falla.Falla impresora.Atasco	23	Novedades por atasco de papel en el mecanismo de alimentación de las bandejas de las impresoras.
Reportar una falla.Aplicaciones Office 365.Envio y recepción de correos	19	Novedades con el correo: claves incorrectas, cuentas bloqueadas o deshabilitadas, errores de sincronización, falta de espacio, límites de envío, problemas en la descarga de archivos, cierre inesperado del cliente y lentitud en el navegador.
Reportar una falla.Gestor Documental.Falla radicacion	16	Novedades debido al alto procesamiento en la plataforma lo cual no permite radicar o subir documentos o error en la parametrización de roles en los usuarios frente a la plataforma de gestor documental
Reportar una falla.Falla impresora.Zabbix	15	Incidentes generados en el servicio de impresión: desconexión de impresoras por falta de comunicación con el servidor tras cambio de contraseña, alertas por tamaño de papel incorrecto, cancelación de documentos por cupos de impresión agotados, finalización de saldos, cables de red desconectados, entre otros.
Reportar una falla.One Drive.Error sincronizacion	13	Error en sincronización por cambio de contraseña, archivos que se intentaban guardar con caracteres especiales lo cual no permite el almacenamiento del documento

Tabla 9 Top 10 Incidentes

- **Casos Suspendidos**

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

Etiquetas de fila	Abril	Mayo	Junio	Total general
NOC			11	11
Responsable_Soporte_Impresoras		2	1	3
Especialista Redes			1	1
Responsable Garantías Equipos	1			1
Total general	**1**	**2**	**13**	**16**

Tabla 10 Casos Suspendidos

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.

A corte de junio, el mes con mayor número de casos en estado suspendido, corresponde a junio, con un total de 13 casos, lo que representa el 81% del total. Este incremento está relacionado a casos asignados al equipo NOC por escalamientos al proveedor de telecomunicaciones del servicio redes y conectividad.

Al cierre del mes el grupo con mayor número de casos suspendidos es el NOC, con 11 incidentes pendientes, seguido por Soporte Impresoras, con 3 casos cada uno los cuales continúan en seguimiento.
Durante el mes se dio solución y cierre a 8 casos pendientes del mes de mayo y 1 de marzo.

- **Incidentes Mayores**

Del total de incidentes reportados, 5 casos fueron registrados como incidentes mayores afectando el servicio de redes y conectividad los cuales se detallan a continuación:

Ticket Arada	Servicio Afectado	Novedad	Acciones Realizadas durante la atención del incidente	CAUSA RAÍZ	Acciones Realizadas para restablecer el servicio	Afectación De Usuarios	Estado Aranda	FECHA INICIO	FECHA FIN	Tiempo de Indisponibilidad
IM-124192	**Internet**	Falla Internet a Nivel Nacional	Se notifica novedad a especialista de redes para revisión, se escala al proveedor.	Falla en red del proveedor	Se procede a establecer comunicación con el proveedor ETB, sin embargo, durante la llamada, todas las alarmas se disiparon, se procede a revisar el estado del servicio con el proveedor y este manifiesta que no evidencia caídas en el servicio, por lo tanto no genera caso. Se confirma que la intermitencia fue de 10 min. Se confirma correcta operación en Zabbix.	A nivel nacional	Cerrado	6/06/2025	6/06/2025	10 MIN
IM-126339	**Internet**	Falla internet zona norte	Se identifica la falla la cual es causada por temas eléctricos. Se reporta al ingeniero de redes la novedad y al proveedor de telecomunicaciones Se realiza seguimiento a la novedad hasta la solución final	caída del equipo core BANOHUNE8001, ubicado en la ciudad de Barranquilla.	se genera escalamiento con ETB para validar con N2 redes la validación del canal como de los equipos y se descubre que hubo un reinicio de los CORE que causaron la falla	Zona norte	Cerrado	14/06/2025	14/06/2025	3 HR
IM-127135	**Internet**	Incidente Mayor - Falla Masiva Nodo Central // Neiva	• Se identifica la falla • Se reporta al ingeniero de redes la novedad • Se informa a la supervisión del contrato • Se realiza seguimiento a la novedad hasta la solución final	: triple afectación de fibra en los siguientes nodos afectados: Primer enlace afectado desde Jumbo a Santa Mónica, Segundo enlace afectado de Cundinamarca a Mirolindo, Tercer enlace afectado de Cundinamarca a Chicó	Se escala novedad al proveedor quienes realizan la corrección por triple afectación de fibra en los siguientes nodos: Primer enlace afectado desde Jumbo a Santa Mónica, Segundo enlace afectado de Cundinamarca a Mirolindo, Tercer enlace afectado de Cundinamarca a Chicó. Se confirman sedes operativas	zona centro-sur país.	Cerrado	18/06/2025	18/06/2025	7 H 59 MIN 59 S
IM-127398	**Internet**	Incidente Mayor Falla Internet Zona Norte	• Se identifica la falla • Se reporta al ingeniero de redes la novedad • Se realiza seguimiento a la novedad hasta la solución final	Vandalismo – Corte de fibra	Se escala novedad al proveedor quienes realizan la corrección de fibra por aperturas en la fibra óptica en los siguientes puntos: Interface 3/0/31: apertura a 2.607 metros, cable 70723, hilo 15. Interface 4/0/13: apertura a 1.473 metros, cable 70856, hilo 10.	Zona norte	Cerrado	18/06/2025	21/06/2025	3 días
IM-129798	**Internet**	Incidente Mayor Falla Internet Zona Norte	• Se identifica la falla • Se reporta al ingeniero de redes la novedad • Se realiza seguimiento a la novedad hasta la solución final	Corte de Fibra	Se escala novedad al proveedor, se realiza seguimiento hasta confirmación de la solución, se informó a los usuarios intermitencias en el servicio	Zona norte	Suspendido	29/06/2025	En Gestión	En Gestión

Tabla 11 Incidentes Mayores Registrados

- **Otras Actividades**

  - Se realizó seguimiento a incidentes en backlog, enviando correos a los especialistas para la documentación y cierre de casos pendientes de gestión. Adicional, se realizó contacto mediante Teams solicitando celeridad en la gestión y cierre de casos.
  - Desde la gestión ITIL se realizan 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 vía Teams, con base a las novedades encontradas en cada caso.
  - Se realizó socialización a todo el personal del proyecto frente a la clasificación y tipo de casos

En el proceso de actualización de 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 Junio
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=503**/512*100 **EF= 98,2%**
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= 2**/507*100 **RRP= 0,39%**

Tabla 12 KPI Práctica de Incidentes

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

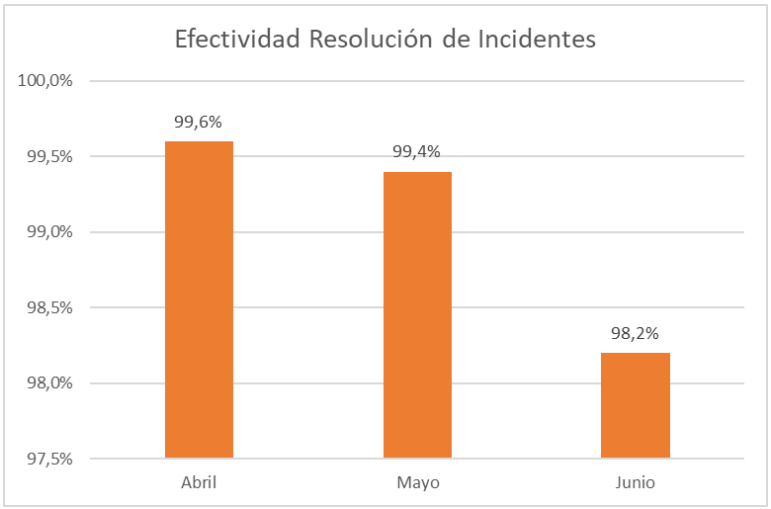


Ilustración 2 KPI Efectividad de Resolución de Incidentes de Servicio

Durante el segundo trimestre, la efectividad en la resolución de incidentes se mantuvo por encima del indicador de cumplimiento del 80%, con los siguientes resultados:

- Abril: 99,6%

- Mayo: 99,4%
- Junio: 98,2%

Aunque se evidencia una disminución en el valor del KPI 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 altamente satisfactorio. Como parte de la gestión de la práctica, se realiza feedback con el equipo haciendo énfasis en la documentación y cumplimiento de los ANS definidos por cada servicio.

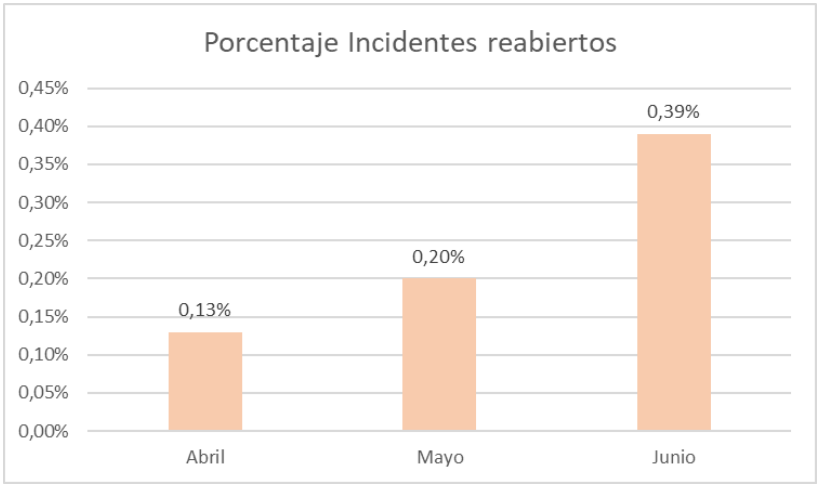


Ilustración 3 KPI Incidentes de Reabiertos en el periodo

Durante el segundo trimestre, el porcentaje de incidentes reabiertos se mantuvo muy por debajo de la meta del 2%, con un leve incremento:

- Abril: 0,13%
- Mayo: 0,20%
- Junio: 0,39%

A pesar del aumento gradual, el resultado sigue siendo favorable y refleja una adecuada gestión de incidentes. A continuación, se relaciona mayor detalle:

Caso	Descripción de la solicitud	Grupo responsable	Causa	Atención al caso
IM-122986	Solicitud eliminación de errores generados en documentos de apoyo y gestor documental dado a que funcionaria no tiene habilitada la opción	IBM	Caso reabierto por la usuaria en el que indica que el error persiste	El especialista revisó nuevamente el caso, realizó la validación técnica del radicado y confirmó que este se encuentra cerrado. Solicita verificar nuevamente la tarea asociada al radicado.
IM-128031	Proactivo Zabbix Mintrabajo - NOC - RInternet_ETB_Florencia	NOC	Caso reabierto dado a que este fue cerrado por error pues la novedad continuaba en la sede afectando el servicio de canal de internet de Florencia	Se escala la novedad al proveedor y se realiza seguimiento hasta la solución la cual se confirma el 28/06/2025, se confirmó operatividad.

Tabla 13 Causas Reaperturas

2.1.2.7. Práctica de Requerimientos

Dar a conocer las actividades de la Práctica de Requerimientos correspondientes al periodo del 1 al 30 de junio de 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 5244 casos tipo requerimiento quedando en los siguientes estados:

Estado	Cantidad
Cerrado	5061
Solucionado	42
Suspendido	61
En proceso	80
Total	**5244**

Tabla 14 Estado de Solicitudes

- Durante el mes, no se presentó algún caso 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 mayo al periodo actual.

Grupo Responsable	Mayo	Junio
Especialista Aplicaciones .Net	2	0
Especialista Aplicaciones JAVA	0	0
Especialista Herramientas de Gestión	2	2
Especialista Nube Publica	0	1
Especialista Redes	0	0
Especialista_Telefonía_IP		0
Especialistas_IBM		1
Gestor de Inventarios		0
Responsable Garantías Equipos		2
Responsable_De_Servidores_Windows	0	7
Responsable_Mesa_De_Servicio	0	6
Responsable_Soporte_Bogota	1	7
Responsable_Soporte_Impresoras	3	14
Responsable_Soporte_Territoriales	0	17
SOC	0	1
Total por Periodo	**11**	**65**

Tabla 15 Seguimiento del Backlog Suspendidos

En el inicio del período, se identificaron 11 casos suspendidos correspondientes al backlog del mes de mayo de 2025. Se realizaron seguimientos semanales de las solicitudes en estado abierto, logrando la solución de 106 casos a través de la herramienta de Gestión Aranda de los anteriores periodos. Para el cierre del mes, quedaron pendientes 65 casos de junio, los cuales se identificaron por: *espera de información por parte de los usuarios finales, Solicitudes a la Supervisión 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, entrega de actas de asignación de las garantías de equipos.*

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

Tipo de Solicitud	Cantidad
Radicar una solicitud.Impresora.Cargue de papel en impresora	605
Radicar una solicitud. Impresora. Aumento de cuota	364
Radicar una solicitud.Impresora.Cambio Toner	226
Radicar una solicitud.Impresora.Instalacion - Configuracion	220
Radicar una solicitud.Impresora.Asesoria - Consulta	213
Radicar una solicitud.Equipo de computo.Configuracion	181
Radicar una solicitud.Equipo de computo.Asesoria - Consulta	168
Radicar una solicitud.Correo Electronico.Configuracion	151
Radicar una solicitud.Correo Electronico.Asesoria - Consulta	138
Radicar una solicitud.Directorio activo.Cambiar contraseña	138

Tabla 16 Top 10 Jerarquía de Requerimientos

- 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.
- Se realizó socialización a todo el personal del proyecto frente a la clasificación y tipo de casos.

En el proceso de actualización de 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** **EF:** Efectividad en solución de Requerimientos. **RFS:** Requerimientos solucionados que cumplen el ANS en el período. **RFR:** Requerimientos registradas en el período.	80%	Mensual	**EF=** 5239/5244*100 **EF= 99.90%**
Porcentaje de Requerimientos Reabiertos en el Periodo	**RRP:** Porcentaje de casos Reabiertos en el periodo. **RFR:** Requerimientos Reabiertos en el período. **RFS:** Requerimientos solucionadas en el período.	<2%	Mensual	**RRP=** 5/5104*100 **RRP= 0.103%**

Tabla17 Detalle de KIP Practica de Requerimientos

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

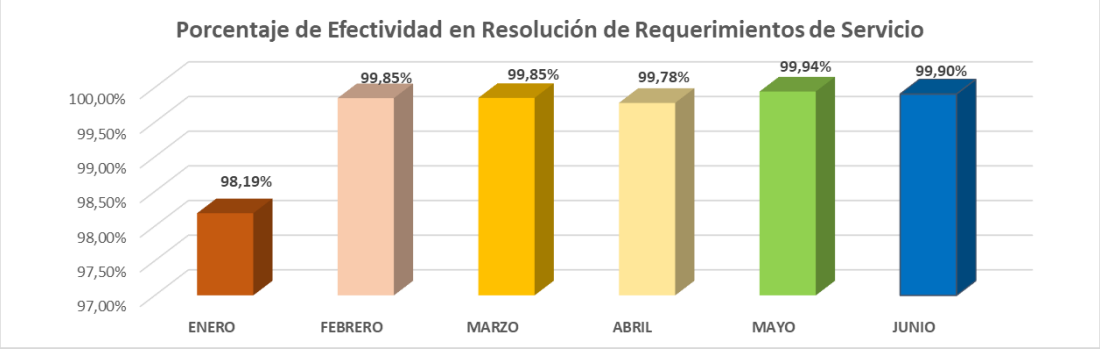


Ilustración 4 KPI Efectividad de Resolución de Requerimientos de Servicio

Durante el periodo, se evidencia el cumplimiento del 99.92% en efectividad de la solución de los requerimientos, los cuales se verifica de 5244 casos registrados en los diferentes canales oficinales

de la Mesa de Servicio que fueron solucionados, 5239 casos cumplieron con los tiempos del ANS de 16 horas hábiles para dar una respuesta efectiva al usuario y 5 casos no cumplieron la efectividad por estar a la espera de respuesta de otras áreas o proveedores o sin actualizar el seguimiento continuo por parte del Grupo especialista.

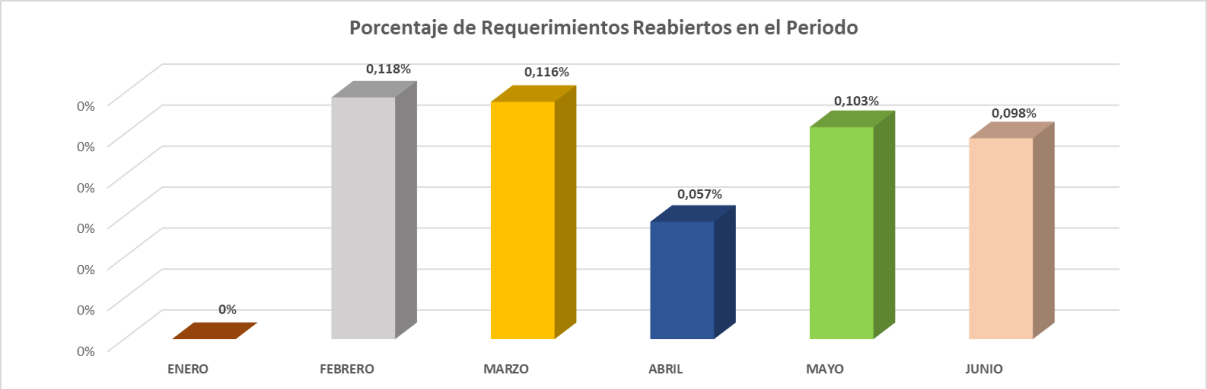


Ilustración 5 KPI Requerimientos de Reabiertos en el periodo

Durante el periodo, se realizó el seguimiento de los requerimientos reabiertos por los usuarios, se ha evidenciado durante los últimos meses una disminución de reaperturas frente al primer trimestre de 2025, lo cual para este mes se presentaron 5 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-122978	Radicar una solicitud.Gestor documental.Asignacion - Modificacion Roles	Especialistas_IBM	Se comunica Usuario solicitando una asignación de roles, la cual se realizó por el especialista y no se evidenciaba en el aplicativo de Gestor Documental, lo cual se reabrió el caso por solicitud del cliente en la MDS.	El especialista realiza la validación del radicado indicado y ya se encuentra cerrado para gestión, por favor verificar nuevamente, ya que se actualizo el listado de interlocutores para las dependencias indicadas en la solicitud.
RF-123257	Radicar una solicitud.Gestor documental.Asignacion - Modificacion Roles	Especialistas_IBM	Se comunica Usuario solicitando una asignación de roles y corrección de la DT Cesar, la cual se realizó por el especialista y no se evidenciaba en el aplicativo de Gestor Documental, lo cual se reabrió el caso por solicitud del cliente en la MDS.	El Especialista realiza la validación técnica en la aplicación y se asignan los roles al usuario indicado y se le retiran a la otra usuaria y dando por cerrada la solicitud.
RF-125072	Radicar una solicitud.Gestor documental.Asignar Radicado TYS	Especialistas_IBM	El usuario indio se está presentando inconvenientes con la planilla y se le da solución por parte del Especialista, lo cual el usuario no está de acuerdo porque la respuesta es genérica y no especifica en las fechas que se muestran en la imagen.	Se realizo la sesión en el 10/06/2025 con el usuario y se evidencio que la planilla, ya fue generada por el usuario Pérez con numero de planilla 207951 y se da por cerrado la solicitud.
RF-129285	Radicar una solicitud.Impresora.Aumento de cuota	Responsable_Soporte_Territoriales	Usuaria solicito aumento de la cuota de impresión, lo cual se valida y autoriza la Modificación, pero indica la usuaria se sigue presentando la misma novedad y no se solucionó la solicitud.	Se realiza la asignación de cuota, se realizan pruebas de impresión por parte de la funcionaria de forma correcta y se da por solucionado el caso.
RF-124817	Radicar una solicitud. Servidor de aplicaciones. Informes y Reportes	Responsable_Mesa_De_Servicio	Usuaria solicita permisos de ingreso a la carpeta compartida desde su casa en su equipo personal, por lo tanto, se le realiza el acompañamiento y se le envía la solicitud al especialista, el cual indica que la usuaria ya cuenta con acceso a la carpeta compartida de Incapacidades, pero indica que sigue presentando el mismo error desde su casa.	Por parte del agente de MDS le informa a la usuaria solo se podrá realizar acompañamiento para mapeo de la carpeta compartida por ser equipo personal en casa, ya que el equipo de la oficina no presenta inconvenientes entrar a su carpeta compartida y al evidenciar errores al momento del mapeo se le solicitan evidencias al correo Soporte MP y se abre el caso RF-126031, el cual identifican que está relacionado directamente con el funcionamiento interno de su equipo personal y se cierra el caso.

Tabla 18 Casos reabiertos

2.1.2.8. Práctica de Eventos

Para el mes de junio, 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 1176 casos escalados mediante la herramienta de gestión de los cuales 660 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**

  - ✓ Ajustes Configuración Case Creator SOC y NOC
  - ✓ Monitoreo a los enlaces WAN como parte de los procesos de gestión con el proveedor de conectividad.
  - ✓ Afinamiento de routers de las sedes
  - ✓ Creación de mantenimientos programados a sedes donde realizan apagado de equipos, actividades de cambios programados, entre otros.
  - ✓ Ajustes de campos adicionales en herramienta ITSM de automatización de bitácora NOC
  - ✓ inicio a la creación de dependencias de los hosts lo que permitirá identificar de manera eficaz el host afectado en las sedes, actualmente se están trabajando sedes territoriales e inspecciones.
  - ✓ Elaboración de listas de filtrado sobre el correo de monitoreo lo que ha permitido evitar la creación de casos cuando se reciben correos de respuestas automáticas o notificaciones enviadas por Microsoft.
  - ✓ Ajuste reglas de clasificación de casos del NOC optimizando tiempos, filtros y creación de casos sin ser asignados.

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 del estado y gestión realizada por parte de los responsables.
- ✓ Solicitud de mantenimiento de sedes en las que los funcionarios apagan los equipos y/o se ausentan de las mismas y Starlink por actualizaciones diariamente en la madrugada.
- ✓ Refuerzo para la documentación de casos según eventos gestionados
- ✓ Solicitud de Mantenimientos de acuerdo con RFC aprobados.

En el proceso de actualización de 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 Junio
Efectividad de la Gestión de eventos NOC	**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= (**649/660)*100 **EF= 98,3%**

Tabla 19 KPI Práctica Eventos

- **Informe Operación NOC**

El presente informe resume las acciones de monitoreo proactivo ejecutadas por el Centro de Operaciones de Red (NOC) sobre la infraestructura tecnológica del Ministerio de Trabajo durante el

mes de junio. La labor del equipo del NOC permitió identificar y gestionar oportunamente un total de 660 incidentes de los cuales se tiene:

Routers (37%) y Starlink (19%) concentran el 56% del total de los incidentes. Esto está asociado a factores como la estabilidad de enlaces satelitales en zonas remotas o condiciones ambientales adversas. FortiGate (16%) representa una carga significativa de eventos causados por falla en la energía comercial, intermitencias en el servicio en horario no hábil y apagado de equipos por parte de los funcionarios. Los servidores Windows y Linux, en conjunto, representan el 10% de los incidentes, los dispositivos Gateway representan el 13% de eventos reportados durante el mes para esta categoría, para los cuales la principal causa fue por apagado de equipo, seguido por intermitencia y falla de energía. Los dispositivos Switches, Access Points, Canal de Internet, UPS y seguridad informática en conjunto reflejan una baja incidencia (5%)

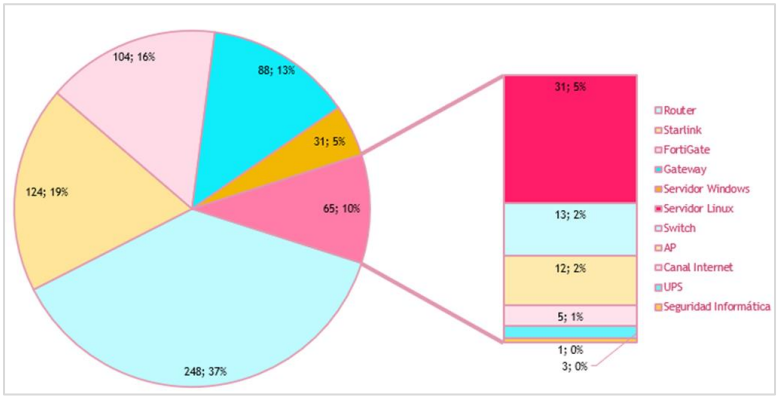


Ilustración 6 Eventos por Tipo de Equipo

Eventos por Categoría de Servicio

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

Redes y Conectividad

- **Router**

Desde el centro de operaciones NOC durante el mes de junio se gestionaron 248 incidentes relacionados con equipos de red Routers en diferentes sedes a nivel nacional, los cuales representaron el 37% de los casos en las siguientes sedes:

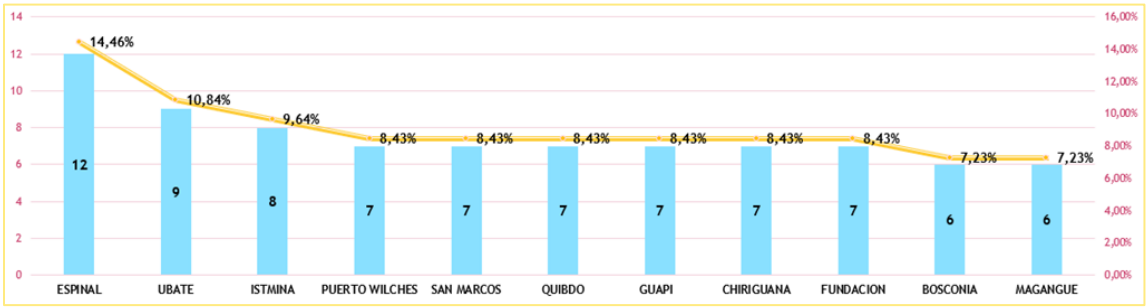


Ilustración 7 Sedes afectadas por router

- Se evidencia que la sede con mayor número de eventos en el mes de junio para la categoría de Routers es Espinal con 12 eventos registrados, los cuales representan el 14,46% del total de casos para esta categoría. Ubaté se ubica en la segunda sede con mayor número de eventos durante el mes con 9 eventos registrados, los cuales representan el 10,84% del total de los casos. Istmina se ubica en la tercera posición de las sedes con mayor número de eventos durante el mes, los cuales representan el 9,64% del total de los casos.

- Por otro lado, las sedes con menor cantidad de eventos registrados durante el mes para esta categoría se encuentran Puerto Wilches, San Marcos, Quibdó, Guapi, Chiriguana y Fundación las cuales registran 7 eventos cada una y representan en porcentaje el 8,43% individualmente. Por último, se evidencia a Bosconia y Magangué con 6 eventos registrados cada una y representan el 7,23% cada una del total de casos para esta categoría.

- A continuación, se relacionan las casusas por las que se originaron estos eventos:

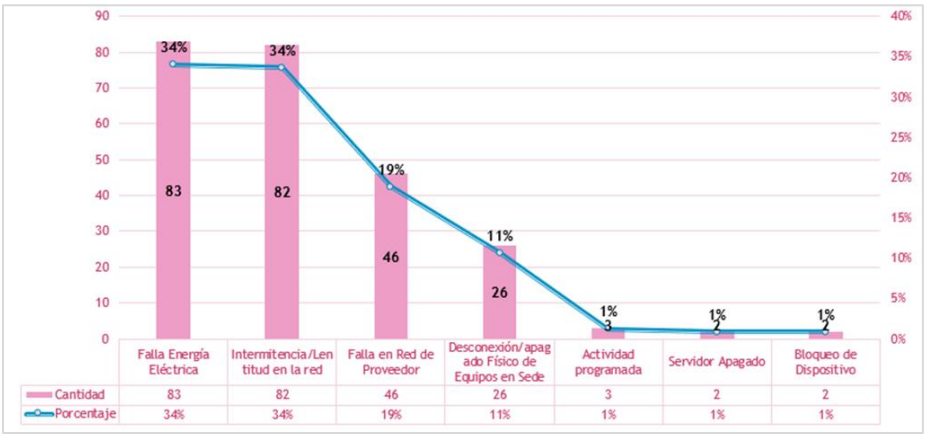


Ilustración 8 Causas de eventos generados por router

- Se identificaron siete causas distintas de incidentes asociados a la categoría de Routers: falla de energía eléctrica, intermitencia o lentitud en la red, fallas en la red del proveedor, desconexión o apagado físico de equipos en sede, actividades programadas, y bloqueo del dispositivo. Las dos causas con mayor número de eventos fueron: falla de energía eléctrica con 83 incidentes (34%) e intermitencia/lentitud en la red con 82 eventos (34%).
- La mayoría de los incidentes por intermitencia tuvieron una duración inferior a 30 minutos según registros en Zabbix. Además, gran parte ocurrieron fuera del horario laboral, lo que impidió confirmar la causa raíz debido a la ausencia de personal en sitio.
- Del total de 248 eventos generados en junio para la categoría de Routers, 244 se encuentran cerrados o solucionados, lo que representa el 98,99%. Tres eventos permanecen en estado suspendido, a la espera de avances por parte del proveedor de servicios de internet, y uno continúa en proceso, pendiente de encendido de equipos por parte del personal de la sede Santa Bárbara dado a que funcionario no se encuentra en sede.

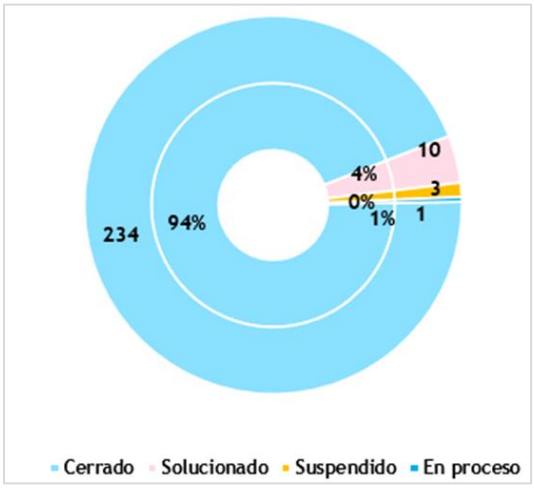


Ilustración 9 Casos suspendidos VS. Casos solucionados de Router

- **Switches**

Desde el Centro de Operaciones (NOC) identificó, durante el mes de junio se generaron 13 casos referentes a Switches en la herramienta de monitoreo Zabbix en las siguientes sedes, los cuales representan el 2% del total de los casos.

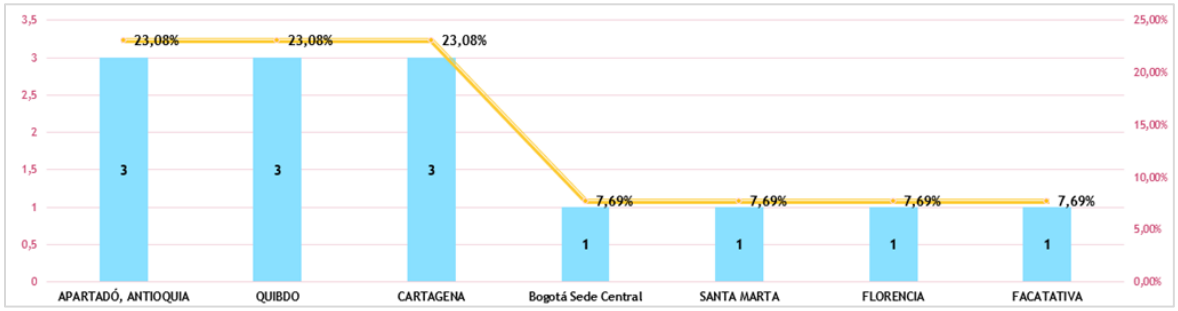


Ilustración 10 Sedes Afectadas

- Por parte del grupo NOC en el mes de junio, se evidencia que de los 13 eventos registrados sobre Switches las sedes con mayor cantidad fueron Apartado, Quibdó y Cartagena con 3 eventos registrados cada una, representando el 23,08% individualmente del total de los eventos para esta categoría. Dos de los tres eventos registrados en Apartado, fueron por apagado de equipos y el restante por falla de energía del punto. Los dos eventos registrados en Quibdó fueron por intermitencia, duraron menos de 20 minutos en Zabbix y se generaron en horario no hábil por lo que no se pudo determinar la causa real. Los tres eventos registrados en la sede de Cartagena fueron por causa de energía eléctrica en la sede.
- Por otro lado, se generaron eventos con una menor incidencia en la sede Bogotá sede central, Santa Marta, Florencia y Facatativá con 1 evento en cada una, que sumadas corresponden al 30,76% del total de los casos para esta categoría.
- Se listan 3 diferentes causas para la categoría de Switches registradas durante el periodo del mes de junio. De las 3 causas registradas, se evidencia que hay 7 por falla energía eléctrica, que representa el 54% de los casos. Por otro lado, por causa de

desconexión/apagado físico de equipos en sede e intermitencia/lentitud en la red se registraron 3 eventos por cada una, representando un 23% individualmente.

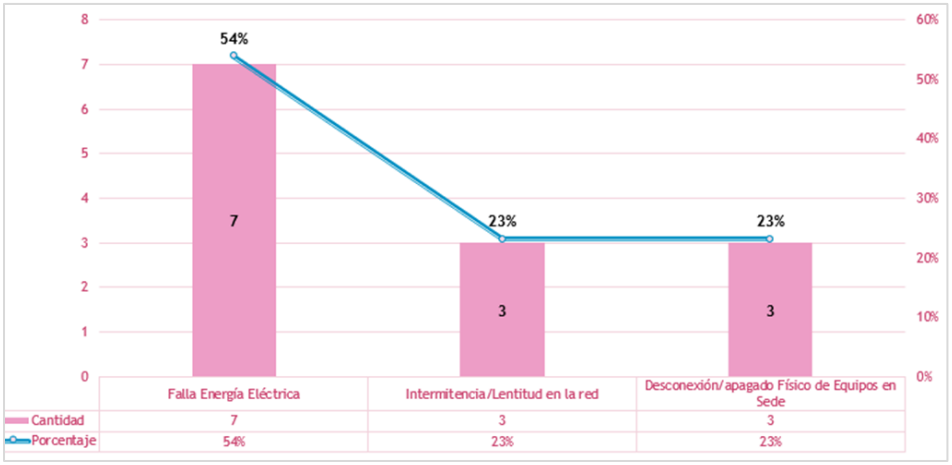


Ilustración 11 Causa de eventos generados por Switch

- De los 13 eventos registrados para la categoría de Switches en el mes de junio, los 13 registran en estado cerrado, cumpliendo de esta manera el 100% de los casos gestionados por parte del centro de operaciones NOC.

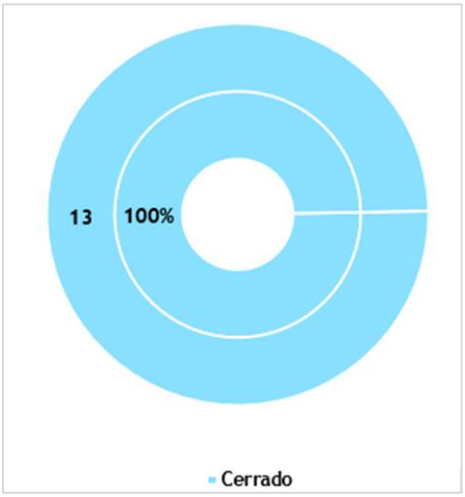


Ilustración 12 Casos suspendidos VS. Casos solucionados de Switch

- **Access Point**

Desde el Centro de Operaciones (NOC), durante el mes de junio se gestionaron 12 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.

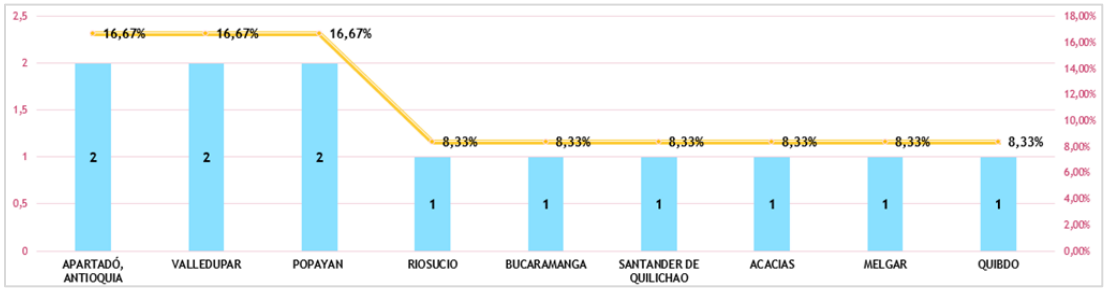


Ilustración 13 Top 10 Sedes afectadas por Access Point

Durante el mes de junio se evidencia que las sedes con mayor número de eventos relacionados con Access Point es Apartadó, Valledupar y Popayán igualando cada una con 2 casos, los cuales representan el 16,67% del total de los casos para esta categoría. De los 12 eventos registrados por Access Point, 6 corresponden a las sedes de Riosucio, Bucaramanga, Santander de Quilichao, Acacias, Melgar y Quibdó las cuales igualan cada una con 1 evento, representando el 8,33% individualmente el total de los casos para esta categoría.

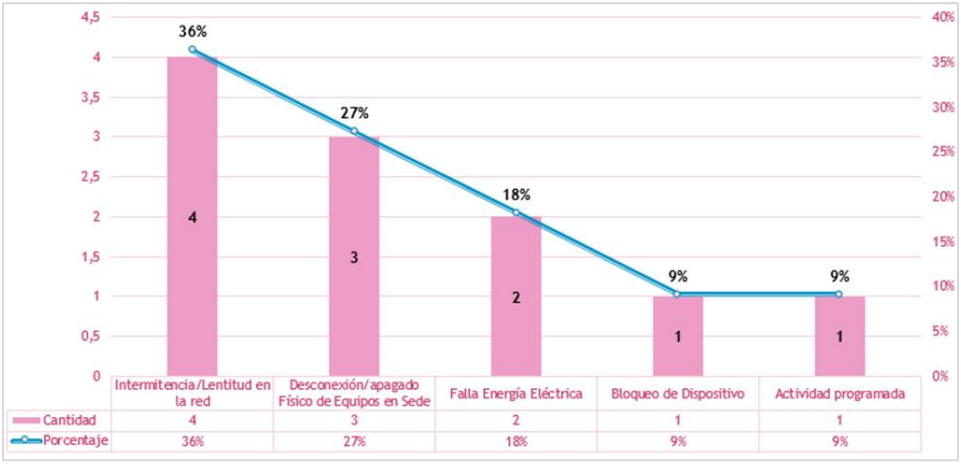


Ilustración 14 Causa de eventos generados por AP

- Se evidencian 5 causas de fallas para el periodo del mes de junio con relación a los dispositivos Access Point. La categoría de causa con más registros de eventos es intermitencia/lentitud en la red con 4 eventos, representando un 36% y seguido de la categoría de desconexión/apagado físico de equipos en sede con 3 eventos, representando el 27% del total de los casos para esta categoría. Las sedes que registraron eventos con la causa intermitencia/lentitud en la red fueron Cesar con 2 eventos, Meta con un evento y Valle con un evento, estás intermitencias fueron asociadas con novedades de los canales y no por falla del Access Point. Las sedes que registraron eventos con la causa Desconexión/apagado Físico de Equipos en Sede fueron Apartado con 2 eventos y Santander con 1 evento registrado.
- Según lo registrado de los 12 eventos generados por Access Point durante el mes de junio con relación a los casos suspendidos VS. Casos cerrados, se evidencian 11 casos en estado cerrado y 1 en estado suspendido, alcanzando un índice de cumplimiento por parte del centro de operaciones NOC del 92% de los casos. Este corresponde al AP_POPAYAN_1_ el cual fue escalado al cliente para la gestión de la certificación del punto de red.

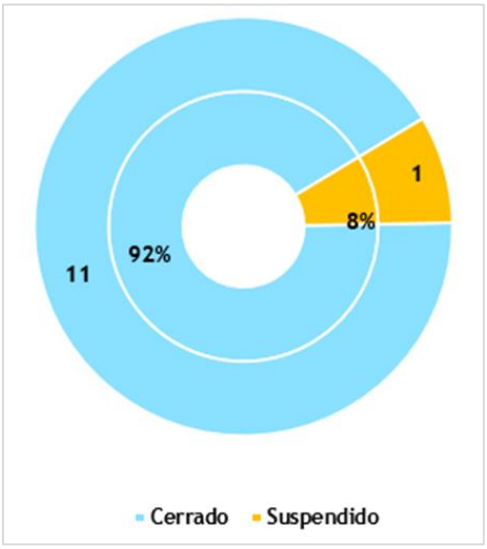


Ilustración 15 Casos suspendidos VS. Casos solucionados de AP

- **Starlink**

Desde el centro de operaciones NOC durante el mes de junio se gestionaron 124 incidentes relacionados con equipos de red Starlink en diferentes sedes a nivel nacional, los cuales representan el 19% del total de los casos.

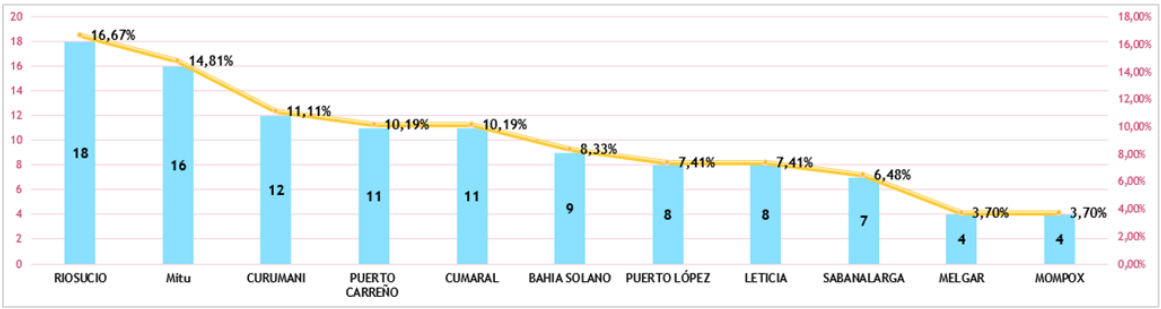


Ilustración 16 Top 10 Sedes afectadas por Starlink

- Para el mes de junio el TOP 5 de las sedes con mayor número de eventos generados para la categoría de Starlink fueron Riosucio con 18 eventos, representando el 16,67%, Mitú con 16 eventos, representando el 14,81%, Curumani con 12 eventos, representando el 11,11%, Puerto Carreño y Cumaral con igual número de eventos 11, representando 10,19% individualmente.
- Se evidencia mayor recurrencia de intermitencia del servicio de internet satelital en sede Riosucio, Mitú y Curumani, estas sedes presentan problemas de constantes fallas de energía por temas climáticos y el servicio de energía en la zona es muy inestable.

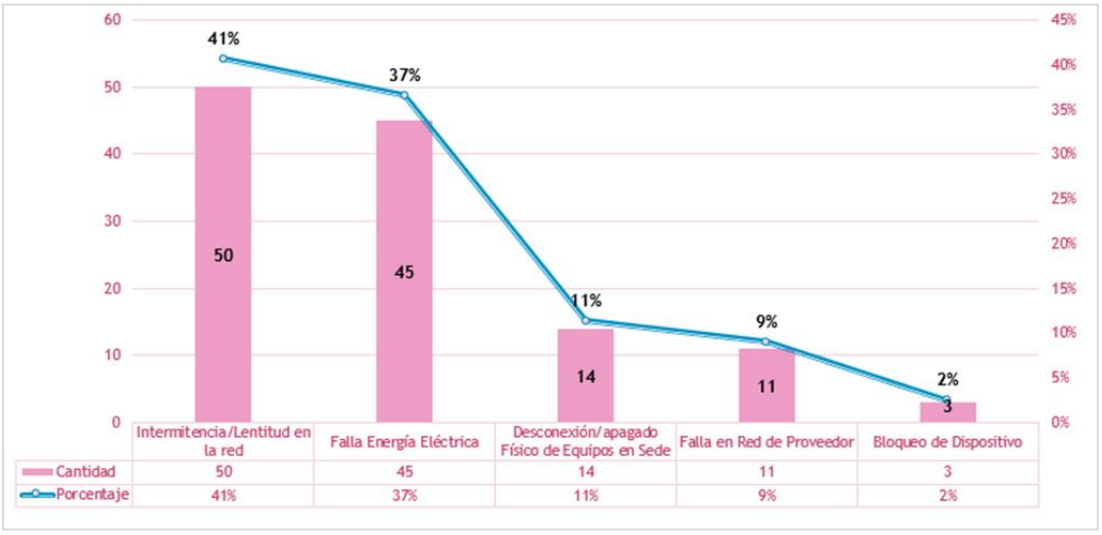


Ilustración 17 Causas de eventos generados por Starlink

- Durante junio se registraron cinco causas de incidentes en la categoría Starlink, siendo la principal intermitencia o lentitud en la red por temas climáticos o nubosidad, con 50 eventos que representan el 41% del total. Le sigue la falla de energía eléctrica con 45 eventos, equivalentes al 37%.
- Los incidentes relacionados con antenas Starlink son inicialmente validados por el equipo de soporte en sitio. Una vez realizadas las revisiones de primer nivel, se adjuntan las evidencias al ticket a través del servicio “Redes y Conectividad” y se escala al equipo de redes, quienes a su vez notifican la novedad al equipo responsable, APICOM.
- Durante el mes, se evidenció que las principales causas de falla en las ubicaciones con tecnología Starlink estuvieron asociadas a condiciones climáticas adversas y a interrupciones del suministro eléctrico, lo que generó caídas recurrentes e intermitencia en el servicio.
- En otros casos en que se presentaron alarmas con el servicio de Starlink se pudo indagar que fueron por causa de energía eléctrica con el 37%, ya que este servicio es muy inestable en dichas sedes por la ubicación geográfica en la que se encuentran.
- Según lo registrado se evidencia que los casos suspendidos VS. Casos solucionados o cerrados del total de los 124 eventos registrados para la categoría Starlink durante el mes

de junio, los 123 registran como solucionados o cerrados, alcanzando un índice de cumplimiento del 99% de casos gestionados por parte del centro de operaciones NOC.

- Queda 1 caso en estado suspendido, el cual está a la espera que el funcionario retome labores para que encienda el dispositivo, porque lo desconecto al salir de la sede.

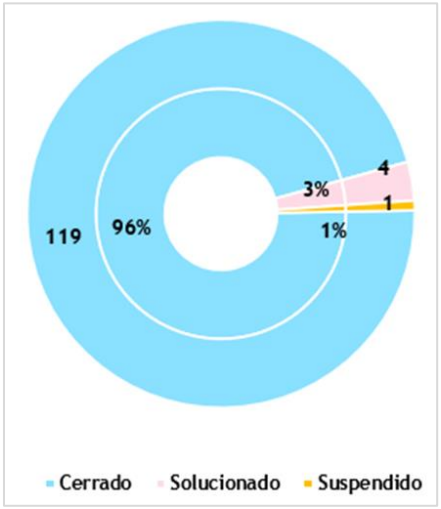


Ilustración 18 Casos suspendidos VS. Casos solucionados de Starlink

- **FortiGate**

Desde el centro de operaciones NOC durante el mes de junio se gestionaron 104 incidentes relacionados con equipos de red FortiGate en diferentes sedes a nivel nacional, los cuales representaron el 16% del total de los casos.

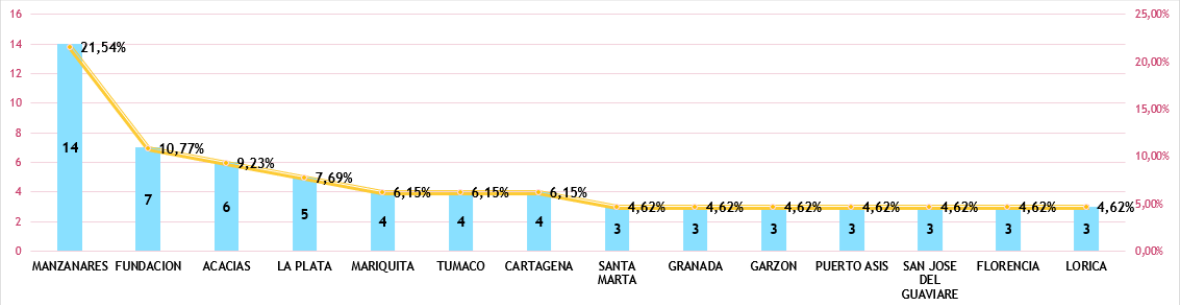


Ilustración 19 Top 10 Sedes afectadas por FortiGate

Durante el análisis del comportamiento de la red SD-WAN en el mes de junio, se identificó una mayor frecuencia de afectación en las sedes de Manzanares y Fundación. Ambas sedes presentan una alta tasa de eventos críticos asociados a la inestabilidad del servicio, atribuible principalmente a fallas recurrentes en el suministro eléctrico y a la limitada calidad de la conectividad disponible en la región,

factores que afectan directamente la disponibilidad de los enlaces SD-WAN. Se recomienda evaluar medidas de mitigación como implementación de respaldo energético (UPS o plantas electricas).

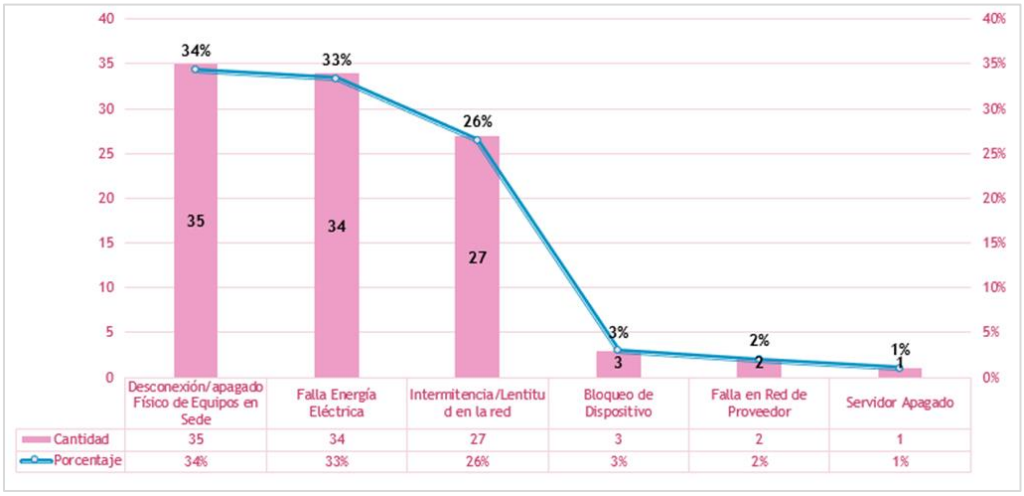


Ilustración 20 Causas de eventos generados por FortiGate

- Durante el mes de junio, los dispositivos SD-WAN presentó un volumen significativo de alarmas, siendo la principal causa la desconexión/apagado físico de equipos en sede con un 34% (35) 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 segundo lugar, el 33% (34) de los alertamientos estuvieron relacionados con fallas en el suministro eléctrico, ocasionadas por condiciones climáticas adversas y validadas por el soporte en sitio. Finalmente, un 26% (27) de las alarmas correspondieron a intermitencia/lentitud en la red estas en su mayoría en horario no hábil y atribuibles a fallas en el servicio de energía e intermitencias en el servicio de internet por temas climáticos como lluvias y tormentas eléctricas.
- De los 104 casos relacionados con los dispositivos SD-WAN, 102 se encuentran a fecha de corte cerrados o solucionados exitosamente, representando un 98% de resolución operativa dentro del mes por parte del centro de operaciones NOC.
- Los dos casos que quedan estado suspendido están a la espera de validaciones por parte del personal en sitio.

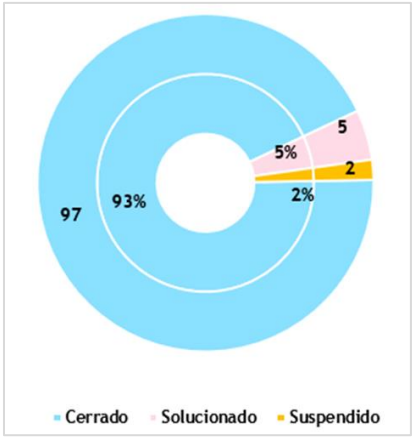


Ilustración 21 Casos suspendidos VS. Casos solucionados de FortiGate

- **Casos Escalados a Proveedor de Telecomunicaciones**

Durante el mes de junio se registraron 40 casos que fueron escalados y gestionados con proveedor de conectividad, de los cuales quedan 38 (95%) que registran en estado solucionado o cerrado y 2 (5%) en estado suspendido.

Según los eventos registrados durante el mes de junio y en relación con los 40 casos gestionados, quedan como solucionados o cerrados 38, que equivalen al 95% del total de casos escalados y gestionados con proveedor por parte del centro de operaciones NOC.

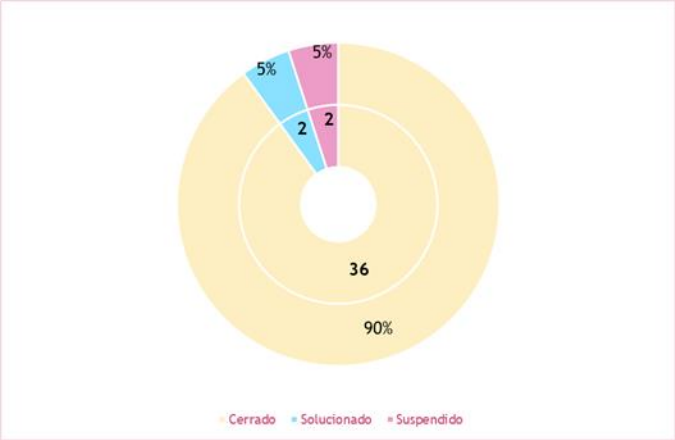


Ilustración 22 Casos suspendidos VS. Solucionados

- El caso Aranda número IM-129798 y caso ETB 24617077 abierto el 29-06-2025 por Falla Masiva en zona norte y que aun continua en validaciones por parte del proveedor de internet y el cual informa según la última validación que esta escalado y a la espera de avances por parte del proveedor de última milla.

- El caso Aranda número IM-128301 y caso ETB 24500559 abierto el 23-06-2025 por afectación critica en el Router_Bogota_Cll_32 y que aun continua en validaciones por parte del proveedor de internet y el cual informa según la última validación que esta escalado y a la espera de avances por parte del personal de correctivo de fibra.

Servicios Centrales

Servidores Windows

Durante junio, el Centro de Operaciones de Red (NOC) gestionó 31 incidentes asociados a servidores Windows, equivalentes al 5% del total de casos registrados en el mes.

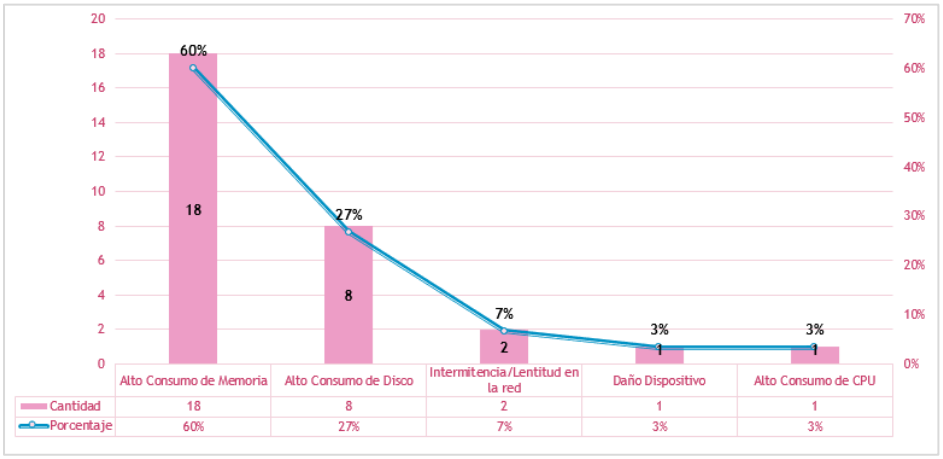


Ilustración 23 Causas de alarmas Servidores Windows

El alto consumo de memoria es el principal causante de eventos en el sistema, representando el 60% del total de eventos. Le sigue el alto consumo en disco, con un 27%. En conjunto, estos dos factores explican el 87% de los eventos registrados, lo que indica que los esfuerzos de mitigación deben centrarse prioritariamente en optimizar el rendimiento de la memoria y mejorar la gestión y mantenimiento del almacenamiento.

Otros factores, como la intermitencia, el uso elevado de CPU, tienen un impacto relativamente menor. Por lo tanto, enfocar las acciones correctivas en las causas principales permitirá lograr una reducción significativa en la ocurrencia de incidentes y un mejoramiento clave en la estabilidad operativa del sistema.

La mayoría de los eventos o recursos monitoreados están concentrados en dos servidores principales:

- MTSGRLBDSQL (32%)
- MINTRAB104 (22%)

Estos dos juntos representan el 54% del total, lo cual indica una alta carga o incidencia en estos nodos específicos. El resto de los servidores tienen una participación mucho menor.

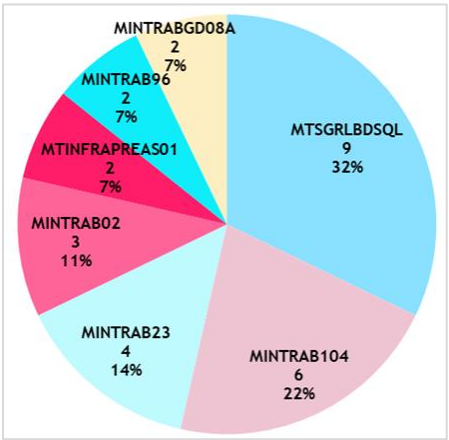


Ilustración 24 TOP 5 de servidores Windows con más alarmas

- El top 3 de los eventos o recursos monitoreados están concentrados en 3 servidores principales:

    - MTSGRLBDSQL (32%): Eventos debido al umbral de alto consumo de memoria en la ejecución de diferentes aplicaciones.
    - MINTRAB105(22%): Evento generado por ejecución de proceso FSMLogAgent
    - MINTRAB23 (14%): Alarmas generadas en aplicaciones como SIRITI y Tesorería las cuales se detuvieron por un alto consumo de recursos en el servidor

  Se evidencia que, de los 31 eventos registrados durante el mes de junio, quedan los 27 en estado cerrado y 3 casos en estado solucionado.

  A la fecha de la elaboración del informe, el ticket que aún estaba pendiente fue solucionado por los especialistas a cargo

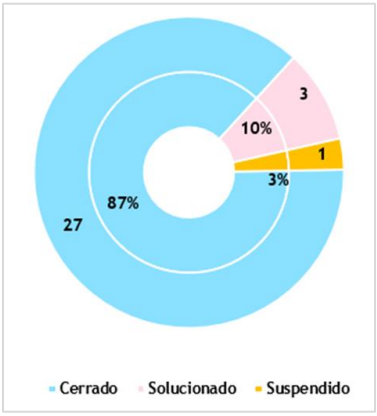


Ilustración 25 Casos suspendidos VS. Solucionados o cerrados Servidores Windows

Servidores Linux

Durante junio, el Centro de Operaciones de Red (NOC) gestionó 31 incidentes asociados a servidores Linux, equivalentes al 5% del total de casos registrados en el mes.

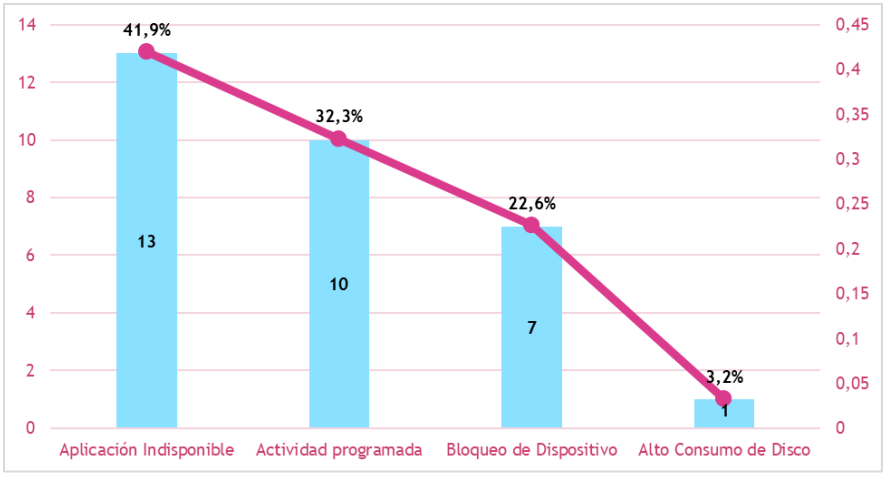


Ilustración 26 21 Causas de alarmas Servidores Linux

Aplicación indisponible es la causa principal, con 13 casos (41,9%), seguido por la actividad programada por Backup de MINTRAB158, con 10 casos (32,3%). En tercer lugar, se encuentra el bloqueo de dispositivos, responsable del 22,6% (7 casos).

Se evidencia una mayor concentración de eventos en el servidor MINTRAB158, con 29 eventos, lo que representa el 97% del total. Por otro lado, el servidor MINTRABWLSTPRO registra solo 1 evento, equivalente al 3%. La cantidad de eventos registrados sobre el servidor MINTRAB158 se deben a un Backup que la maquina ejecuta todos los días a las 5:00 am con una durabilidad de 15 minutos.

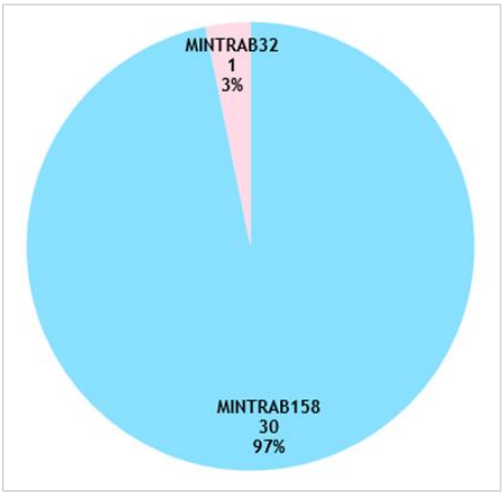


Ilustración 27 TOP 5 de Servidores Linux con más alertas

De los 31 eventos registrados para la categoría de servidores Linux durante el mes de junio, los 31 registran en estado solucionados o cerrados, representando el 100% de los casos gestionados por parte de los especialistas a cargo.

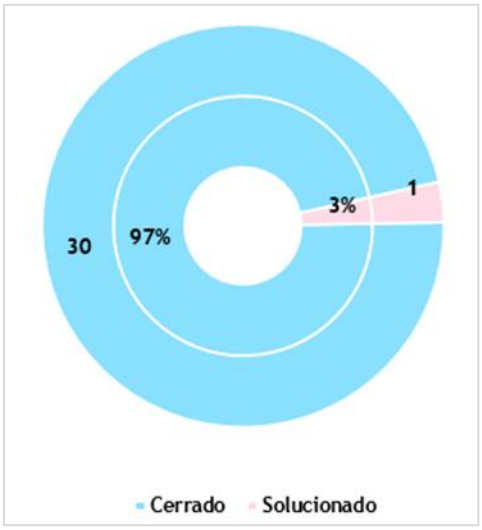
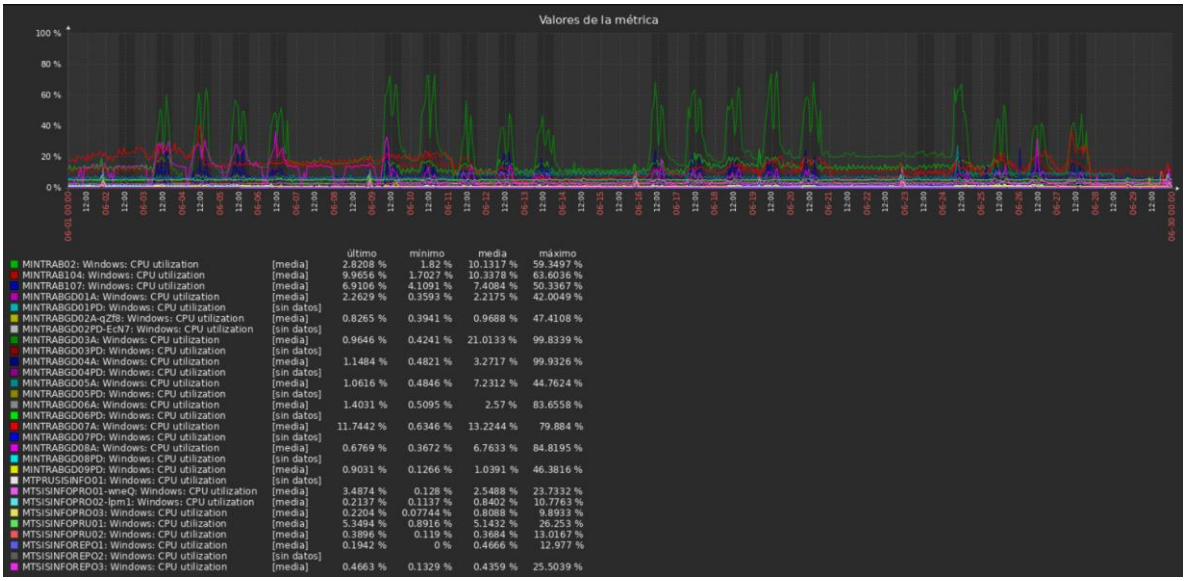


Ilustración 28 Casos suspendidos VS. Solucionados o cerrados Servidores Linux

Graficas 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 21,0133%
2. MINTRABGD07A 13.2244%
3. MINTRAB104 10.3378%
4. MINTRAB02 10.1317%
5. MINTRAB107 7,4084%

Grafica 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 80.5151%
2. MINTRAB02 77.0123%
3. MINTRAB104 76.5389%
4. MINTRABGD08A 43.7177%
5. MINTRABGD09PD 41.4452%

Durante el mes de junio, se reportó 1 incidente en el Datacenter de Bogotá; no se registraron incidentes en Cali. El evento estuvo asociado al canal de respaldo (BCK_MPLS_ColombiaXV), lo cual no generó interrupciones significativas en la continuidad del servicio gracias a la redundancia garantizada por el canal principal.

El incidente fue gestionado de manera eficiente, con tiempos de resolución dentro de los parámetros esperados. Según el informe del proveedor, la causa del evento se relacionó con problemas en las conexiones y una limpieza inadecuada de la fibra óptica. La existencia de redundancia permitió mantener la operación sin afectaciones críticas.

Resumen del motivo de la falla:

- IM-123846: Conexiones y limpieza de la fibra incorrectas.

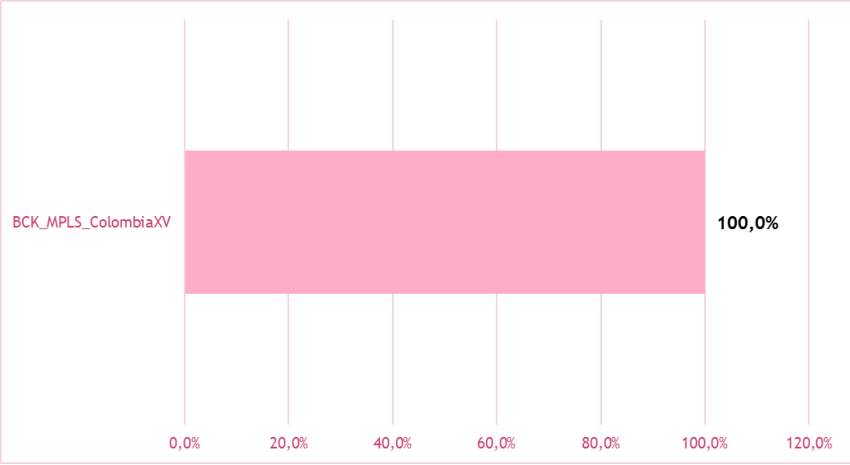


Ilustración 1 Eventos de Datacenter

2.1.2.9. Práctica de Disponibilidad

Dentro del marco de la práctica de la disponibilidad del servicio se está trabajando en los procesos y las herramientas que permitan cumplir con los objetivos de disponibilidad definidos en la práctica. A continuación, se muestra la información correspondiente a la disponibilidad de los servicios para el periodo del 1 al 30 de junio de 2025.

Servidores

Cantidad de dispositivos	Disponibilidad consolidada
129	100%

Tabla 20 Consolidado disponibilidad de servidores

No se presentó alarmas en los servidores según los en el umbral de monitoreo del periodo.

Directorio Activo

Cantidad de dispositivos	Disponibilidad consolidada
3	100,00%

Tabla 21 Consolidada disponibilidad de Directorio Activo

Los siguientes servidores, se encuentran en el Directorio Activo sin presentar indisponibilidad del servicio durante el periodo.

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

Tabla 22 Desagregado de Disponibilidad Directorio Activo

Datacenter Principal

Cantidad de dispositivos	Disponibilidad consolidada
8	100,00%

Tabla 23 Consolidado disponibilidad de equipos Datacenter principal

Los siguientes equipos se encuentran el Datacenter Principal, los cuales no presentan indisponibilidad del servicio 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 24 Desagregado de Disponibilidad Datacenter Principal

Datacenter Alterno

Cantidad de dispositivos	Disponibilidad consolidada
4	*100%*

Tabla 25 Consolidado disponibilidad de equipos Datacenter alterno

Los siguientes equipos se encuentran el Datacenter alterno, los cuales no presentan indisponibilidad del servicio 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 26 Desagregado Disponibilidad de equipos Datacenter alterno

Redes y conectividad

Cantidad de dispositivos	Disponibilidad consolidada

494	*94,81%*

Tabla 27 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 28 Consolidado disponibilidad de equipos de seguridad

Los siguientes equipos se encuentran en el Servicio de Seguridad de la Información, los cuales no presentan indisponibilidad del servicio 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 29 Disponibilidad de equipos Seguridad de la Información

Telefonía

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

Tabla 30 Consolidado disponibilidad de equipos de telefonía

Antivirus

Cantidad de dispositivos	Disponibilidad consolidada
1	100%

Tabla 31 Consolidado disponibilidad de plataforma antivirus

Actividades de la Practica de Disponibilidad:

- Seguimiento a los resultados de los cambios presentados en el CAB por partes de especialistas que afecten la disponibilidad del servicio.
- Se elaboró y revisó el plan de disponibilidad del servicio de Seguridad de las Pruebas HA del Firewall.
- Se realizó la verificación de la documentación de los resultados de las pruebas de alta de, Firmware y Firewall Colombia XV RFC-126592 y Pruebas de Conmutación Canal Internet Principal RFC-125230, Pruebas de Alta disponibilidad WLAN – Wireless Local Area Network RFC-125188.
- 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 21 pruebas de alta disponibilidad, de las cuales 13 corresponden a pruebas de disponibilidad

de los servicios Conectividad, Seguridad de la Información y Telefonía IP se encuentran ejecutadas y aprobadas en los CAB.

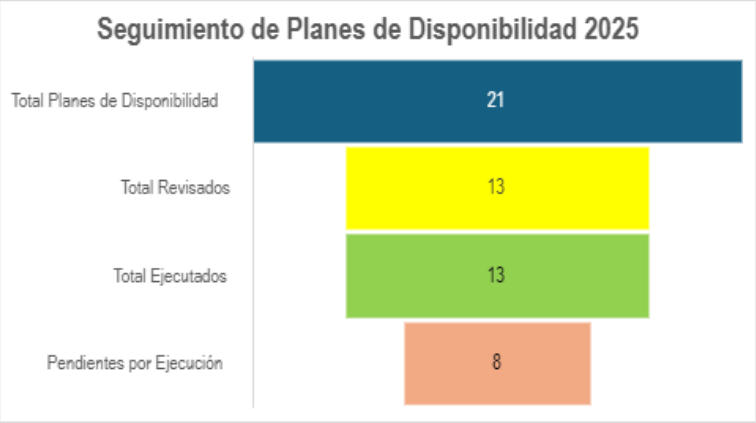


Ilustración 29 Seguimiento Pruebas de Disponibilidad

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 30 de junio de 2025.

Actividades en curso:

- Revisión de los RFC ejecutadas durante el periodo, los cuales (11) cambios se aprobó el cierre por parte de la Práctica de Implementación, ya que cuentan con las evidencias completas de los planes de Pruebas Previas y Posteriores, por lo anterior en el momento se encuentra (4) casos abiertos a la espera de entrega de las evidencias por parte los especialistas, en proceso de revisión, en implementación o por aprobación al corte del 30/06/2025.

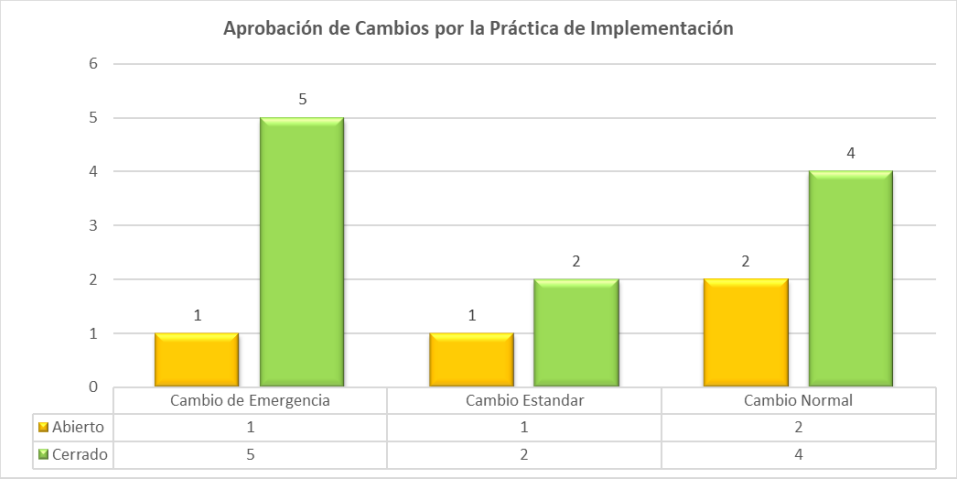


Ilustración 30 Seguimiento Práctica Implementación

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

Seguimiento de cambios Implementa

2.2. Mesa de Servicios y Soporte en Sitio

A continuación, se relaciona la gestión desarrollada en el transcurso del mes de junio, para la Mesa de Servicios y el personal de Soporte en Sitio, el cual contiene información relevante sobre la operación, hallazgos, actividades realizadas; que permiten la toma de decisiones para mejorar la calidad del servicio y la percepción de los usuarios sobre el mismo.

- **Histórico de Atención de Llamadas**

Para el periodo del mes de junio, en el Ministerio del trabajo a la MDS ingresaron 285 llamadas de usuarios finales para solicitar servicios de Soporte Tecnológico, a continuación, se discrimina la clasificación según el servicio solicitado:

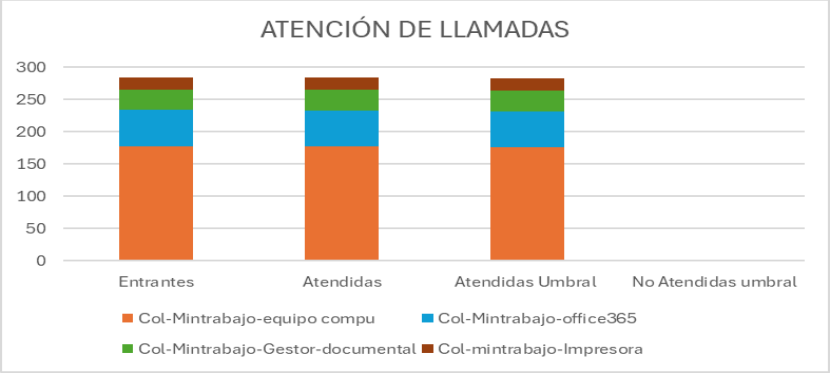


Ilustración 31 Atención de Llamadas

Servicio	Entrantes	Atendidas	Atendidas Umbral	No Atendidas umbral	Abandonadas	No Atendidas
Col-Mintrabajo-equipo compu	178	177	176	1	0	1
Col-Mintrabajo-office365	56	56	56	0	0	0
Col-Mintrabajo-Gestor-documental	32	32	32	0	0	0
Col-mintrabajo-Impresora	19	19	19	0	0	0
TOTAL	285	284	283	1	0	1

Tabla 32 Atención de Llamadas

El servicio más solicitado a través de la atención de llamadas es: *Equipo de cómputo* con 178 llamadas entrantes, se atendieron 177 solicitudes, se observa: 1 llamada no atendidas en el umbral por que fue abandonada por el funcionario antes de los 20 segundos, 1 llamada Abandonada que no le ingreso al agente y se detecta como bucle en llamada entrante, se crea el caso con fabricante Caso #2505190040009338 Numintec, dado que la falla fue del aplicativo no de la funcionabilidad de la mesa de servicio no se vería afectada el indicador.

Caso #2505190040009338:

Dentro del análisis realizado, se identificó un caso particular correspondiente a una llamada efectuada el día 7 de junio de 2025 a las 8:19:13 a. m., la cual no fue atendida inicialmente, a pesar de que el agente asignado se encontraba disponible en ese momento.

Esta llamada permaneció en la cola sin ser direccionada correctamente, lo que indica una posible anomalía en el comportamiento de la plataforma de contact center. Tras la revisión técnica, se concluye que el incidente se debe a un bug identificado en el motor de enrutamiento de llamadas, el cual afecta casos específicos de disponibilidad de agentes.

Como medida correctiva:

- Esta incidencia será mitigada en el próximo parche de la plataforma, ya programado por el equipo de desarrollo del proveedor.
- Adicionalmente, se implementó una regla de verificación en la lógica de cola que refuerza el proceso de asignación de llamadas en tiempo real, con el fin de evitar recurrencia mientras se aplica el parche definitivo.
- Se continuará haciendo seguimiento a los registros del sistema para asegurar la estabilidad operativa de la plataforma y confirmar que el comportamiento se ha corregido.

- ## Casos Registrados por Categoría de Servicio

Para este periodo se toma el top 10 de los casos más representativos de los diferentes servicios.

Top 10 de Solicitud de Administración de servidores: Los casos más representativos están asociados a la gestión de junio son las categorías: Cambio de contraseña / Creación de usuarios / Cambio de Usuarios a nivel de dominio, Servidor Windows, Asignación de licencia de Office, Inactivación de usuarios de dominio, Permisos sobre el File Server, Modificar usuarios, Asesoría - Consulta de temas asociados a Servicios de TI, Configuración y otros servicios, para un total de 451 casos, en comparación con el mes de anterio se da un aumento del 8,58% que corresponde 40 casos, donde se mantiene las mismas categorías. En la siguiente tabla se muestra el total de solicitudes para el servicio y el porcentaje correspondiente:

ADMINSTRACION DE SERVIDORES	TOTAL	PORCENTAJE (%)
Cambiar contraseña	138	30,60
Creacion de usuario	57	12,64
Cambio de grupo	45	9,98
Servidor Windows	31	6,87
Asignación de licencia	24	5,32
Inactivar usuario	21	4,66
Permisos	19	4,21
Modificar usuarios	12	2,66
Asesoria - Consulta	11	2,44
Configuración	11	2,44
Configuración MFA	11	2,44
Habilitar usuario	10	2,22
Servidor Linux	8	1,77
Asignación de permisos	5	1,11
Crear usuario	5	1,11
Informes de usuarios	5	1,11
Retiro de Licencia	4	0,89
Crear/Modificar/Eliminar	3	0,67
Aprovisionamiento	3	0,67

Informes y Reportes	3	0,67
Validar servidor	3	0,67
Restaurar información	3	0,67
Servidores	3	0,67
Crear grupos de seguridad	2	0,44
Mantenimiento preventivo	2	0,44
Crear Backups	2	0,44
Actualización de servidores	2	0,44
Administración de equipos	2	0,44
Backup	1	0,22
Desbloquear usuario	1	0,22
Tarea de copiado	1	0,22
Crear carpeta	1	0,22
Generar reporte	1	0,22
Reiniciar servidor	1	0,22
Total general	**451**	**100,00**

Tabla 33 Top 10 administración de servidores

Top 10 de Redes y Conectividad: para el mes de junio se tiene las siguientes categorías más representativos de redes y conectividad : Solicitudes asociadas a Router, Servicios de conectividad brindados por Antenas Starlink Canal Internet, Asesoría – Consulta, Revisión estado del canal, Switch, Access point (Sede Central), Equipo Conectividad internet, Falla punto de red y otros servicios, para un total de 224 casos. En comparación con el mes anterior se da una disminución del 13,17% que corresponde 34 casos, donde se mantiene las mismas categorías. En la siguiente tabla se muestra el total de solicitudes para el servicio y el porcentaje correspondiente:

REDES Y CONECTIVIDAD	TOTAL	PORCENTAJE (%)
Router	131	58,48
Starlink	64	28,57
AP	5	2,23
Canal Internet	5	2,23
Asesoria - Consulta	4	1,79
Revisión estado del canal	4	1,79
Switch	3	1,34
Access point Sede Central	2	0,89
Equipo Conectividad internet	2	0,89
Falla punto de red	1	0,45
Degradación	1	0,45
Sin servicio	1	0,45
Habilitar punto de red	1	0,45
Total general	**224**	**100,00**

Tabla 34 Top 10 redes y conectividad

Top 10 de Seguridad Informática: durante el mes de junio se tiene las siguientes categorías más representativas, de seguridad informática que corresponden a: Seguridad Informática, Permitir acceso, Análisis de Correos, Ajuste de configuraciones (Crear - Eliminar), Falla conexión VPN, Agregar a sitios permitidos, Asesoría – Consulta sobe el servicio, Análisis vulnerabilidades y Revisar correo malicioso y otros servicios para un total de 154 casos. En comparación con el mes anterior, se da una disminución del 21,42% que corresponde a 42 casos.

SEGURIDAD INFORMATICA	TOTAL	PORCENTAJE (%)
Seguridad Informática	127	82,47
Permitir acceso	5	3,25

Análisis de Correos	3	1,95
Ajuste de configuraciones (Crear - Eliminar)	2	1,30
Falla conexión VPN	2	1,30
Agregar a sitios permitidos	2	1,30
Asesoria - Consulta	2	1,30
Análisis vulnerabilidades	2	1,30
Revisar correo malicioso	2	1,30
Firewall de aplicaciones Web - WAF	1	0,65
Crear políticas	1	0,65
Autorización nuevo software	1	0,65
Configuración consola	1	0,65
Falla - error	1	0,65
Crear política	1	0,65
Restringir servicio	1	0,65
Total general	**154**	**100,00**

Tabla 35 Top 10 seguridad informática

Top 10 de Telefonía IP: Durante este periodo se gestionaron 36 casos de Telefonía IP que corresponden a: Instalación – Configuración de teléfonos, Asignación de Extensiones, novedades con Gateways de las DT, Radicar una solicitud del servicio, Configuración de red, Configuración de extensión, Asesoria – Consulta del servicio, Falla – error, Falla de red y No conecta, En comparación del mes anterior se tiene un aumento de los casos del 16,66% que corresponde a 6 casos, para un total de 36 casos.

TELEFONIA IP	TOTAL	PORCENTAJE (%)
Instalación - Configuración	10	27,78
Asignación de Extensión	7	19,44
Gateway	6	16,67
Radicar una solicitud	3	8,33
Configuración de red	3	8,33
Configuración de extensión	2	5,56
Asesoria - Consulta	2	5,56
Falla - error	1	2,78
Falla de red	1	2,78
No conecta	1	2,78
Total general	**36**	**100,00**

Tabla 36 Top Telefonía IP

Top 10 de Aplicaciones Especializadas: Para el mes de junio se tienen los casos más representativos de la gestión de aplicaciones que corresponden a las siguientes categorías: Asignar Radicado TYS, Asesoría - Consulta, Asignación - Modificación Roles, Depuración Bandeja, Relanzamiento, Falla Funcional, Falla radicación, Suspender - Finalizar Radica TyS, Instalar - Configurar, No permite Aprobar y radicar. En comparación del mes anterior se tiene una disminución de los casos del 26,173% que corresponde a 184 casos, para un total de 519 casos.

APLICACIONES ESPECIALIZADAS	TOTAL	PORCENTAJE (%)
Asignar Radicado TYS	129	24,86
Asesoria - Consulta	128	24,66
Asignación - Modificación Roles	63	12,14
Depuración Bandeja	62	11,95
Relanzamiento	33	6,36
Falla Funcional	26	5,01
Falla radicación	16	3,08
Suspender - Finalizar Radica TyS	15	2,89

Instalar - Configurar	8	1,54
No permite Aprobar y radicar	8	1,54
Solicitud depuración carpeta	5	0,96
Informes y Reportes	5	0,96
Reportar Solicitud/Falla	4	0,77
Asignación de recursos	3	0,58
Falla - Error PQRSD	3	0,58
Lentitud gestor	2	0,39
Falla al cargar archivos	1	0,19
Caída - Degradación	1	0,19
Gestor documental	1	0,19
No se encuentra radicado	1	0,19
Falla - Error ventanilla	1	0,19
Falla Error - Datacap	1	0,19
Portal Web	1	0,19
Falla error - Producir documento	1	0,19
Asesoría - Consulta	1	0,19
Total general	**519**	**100,00**

Tabla 37 Top 10 soporte aplicaciones

Top 10 de Soporte Microinformática: Los casos más representativos de la gestión de soporte microinformática que corresponden a las siguientes categorías: Asesoría - Consulta, Cargue de papel en las impresoras, Configuración, Instalación - Configuración, Aumento de cuota de impresión, Cambio Toner, Asesoria Excel, Asesoria PDF, Asesoria Word, Préstamo y otros servicios, con 109 casos que representan el 2,57%. En comparación del mes anterior se tiene una disminución en los casos del 28,57% que corresponde a 1696 casos, para un total del mes de 4239 casos.

SOPORTE MICROINFROMATICA	TOTAL	PORCENTAJE (%)
Asesoria - Consulta	889	20,97
Cargue de papel en impresora	605	14,27
Configuración	468	11,04
Instalación - Configuración	389	9,18
Aumento de cuota	364	8,59
Cambio Toner	226	5,33
Asesoria Excel	124	2,93
Asesoria PDF	122	2,88
Asesoria Word	116	2,74
Préstamo	109	2,57
Instalación y configuración VPN	100	2,36
Asesoria Consulta	65	1,53
Soporte Aplicaciones Office 365	63	1,49
Conectar a red Mintrabajo	58	1,37
Traslado - Movimiento	54	1,27
Mantenimiento preventivo	43	1,01
Asignación de equipo (portátil o PC)	33	0,78
No imprime	33	0,78
Falla - Error conexión a red	26	0,61
Solicitud Backup	25	0,59
Copia de informacion	25	0,59
Atasco	23	0,54
Reportar Solicitud/Falla	22	0,52
Instalación-Desinstalación	21	0,50
Instalacion	21	0,50
Instalación - Configuracion	20	0,47

Envio y recepción de correos	19	0,45
Solicitud instalacion	19	0,45
Falla - error	18	0,42
Zabbix	16	0,38
Devolución de equipo (portátil o PC)	16	0,38
Conectar a red Invitados	15	0,35
Borrado seguro Portátil	14	0,33
Error sincronizacion	13	0,31
Lentitud - Bloqueo	13	0,31
No enciende	12	0,28
Equipo Periférico	12	0,28
Backup	12	0,28
Préstamo Equipo (portátil o PC)	10	0,24
Configuracion de PST	8	0,19
Equipo Impresora	7	0,17
Falla Excel	7	0,17
Falla Aplicativo	6	0,14
Asesoria Power Point	6	0,14
Asesoria en ZIP	5	0,12
No escanea	5	0,12
Borrado seguro PC	4	0,09
Falla Aplicaciones Office 365	4	0,09
Falla Cargue pagina web	4	0,09
Impresión deficiente	4	0,09
Equipo Escritorio	4	0,09
Cambio de unidad de imagen	4	0,09
Error de aplicación	3	0,07
Falla Word	3	0,07
Daño Fisico	3	0,07
Solicitud de cambio	3	0,07
Equipo Portátil	2	0,05
Falla- Error	2	0,05
Falla de sistema operativo	2	0,05
Falla PDF	2	0,05
Falla General	2	0,05
Bloqueo Navegador	1	0,02
Desinstalacion	1	0,02
Falla del lector	1	0,02
Intermitencia - Lentitud	1	0,02
Falla instalacion	1	0,02
Falla aplicación	1	0,02
Total general	**4239**	**100,00**

Tabla 38 Top 10 soporte microinformática

- **Análisis de Casos Anulados por Servicio**

Para este periodo se tiene 7 casos anulados de los siguientes servicios:

CASOS ANULADOS	TOTAL
Soporte Microinformatica	3
Redes y Conectividad	3
Herramientas de Gestión	1
Total general	**7**

Tabla 39 Casos Anulados por Servicio

- **Soporte Microinformático:** se tiene 3 casos, Instalacion y configuracion VPN, Cargue de papel en impresoras.
- **Redes y Conectividad:** se tiene 3 caso por duplicidad Reportar una falla.Alarma Zabbix.Canal Internet y Radicar un cambio. servicio WLAN.Access point Sede Central.
- **Herramientas de Gestión:** se tiene 1 caso, anulado por duplicidad Monitoreo desde zabbix.

En comparación del mes anterior se evidencio una disminución del 12,5%, que corresponde a 1 caso.

- ## Análisis de Casos Suspendidos por Servicio

Para el periodo del mes de junio, se dio una disminución de casos suspendidos en 2,98% que corresponde a 2 casos para un total de este mes de 65. quedaron en estado casos de los siguientes servicios:

CASOS SUSPENDIDOS	TOTAL
Soporte Microinformatica	42
Administración de servidores	9
Aplicaciones Especializadas	9
Redes y Conectividad	2
Herramientas de Gestión	2
Seguridad informática	1
Total general	**65**

Tabla 40 Casos Suspendidos por Servicio

- **Soporte Microinformática:** 42 casos suspendidos debido a que se ha solicitado información complementaria a los usuarios o están pendientes por disponibilidad del usuario: Cambio Toner con 14 casos, Solicitud Backup, con 5 casos, Solicitud Backup, Equipo Periférico, Configuracion con 3 casos; Equipo Portátil, Mantenimiento preventivo, Equipo Escritorio con 2 casos, Instalacion – Configuracion, Prestamo, Instalacion y configuracion VPN, Devolución de equipo (portátil o PC), Falla - Error conexión a red , Backup, Instalación - Configuracion, Asesoria – Consulta, Aumento de cuota, Cambio de unidad de imagen, Daño Fisico, Asignación de equipo (portátil o PC), Equipo Impresora con 1 caso.
- **Administración de servidores: 9** casos suspendidos por: Inactivar usuario con 5 casos, Retiro de Licencia con 2 casos, Configuración y Servidor Windows con 1 caso, cada categoría.
- **Aplicaciones Especializadas: 9** casos suspendidos debido a que se ha solicitado información complementaria a los usuarios o están pendientes por disponibilidad del usuario: Asignacion - Modificacion Roles con 3 casos, Asesoria - Consulta con 2 casos, Depuración Bandeja, Instalar – Configurar, Asignacion de recursos, Asignar Radicado TYS con 1 caso cada categoria.

- **Redes y Conectividad: 2** casos suspendidos debido a: Falla en Router, Falla Canal Internet con 1 caso cada categoría.
- **Herramientas de Gestión: 2** casos suspendidos debido a: Ajustar host, Creación/Modificación/Eliminación Funcionalidades Aranda con 1 caso cada categoría.
- **Seguridad informática: 1** caso suspendido debido a: Radicar una solicitud.Firewall.Permitir acceso con 1 caso.

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

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

Incidentes solucionados por Soporte en sitio: Para este periodo no quedaron incidentes en estado solucionado.
Incidentes solucionados por Soporte Territoriales: para el mes de junio un (1) caso quedó en estado solucionado, discriminado de la siguiente manera.

SOPORTE_TERRITORIAL	TOTAL
Falla - Error conexión a red	1
Total general	**1**

Tabla 41 Incidentes solucionados por Soporte Territoriales



Ilustración 32 Incidentes Solucionados por Soportes Territoriales

Requerimientos solucionados por la Mesa de Servicios: Para el mes de junio quedaron 2 requerimientos solucionados por la mesa de servicios discriminados de la siguiente manera:

REQUERIMIENTOS SOLUCIONADOS MESA_DE_SERVICIOS	TOTAL
Asesoria - Consulta	1
Inactivar usuario	1
Total general	**2**

Tabla 42 Requerimientos solucionados por Mesa de Servicios

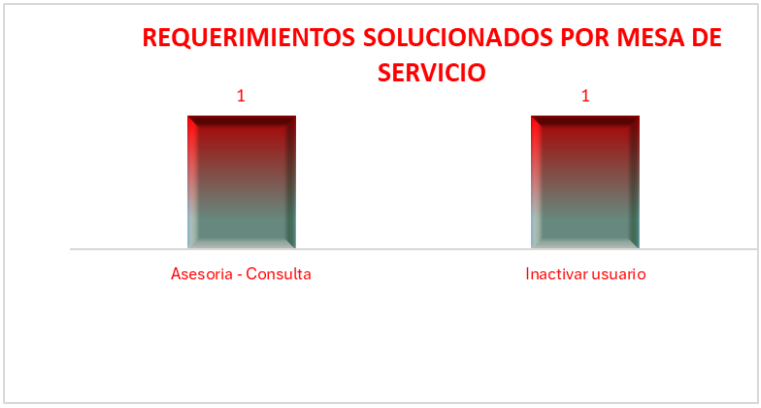


Ilustración 33 Requerimientos Solucionados por la Mesa de Servicios

Requerimientos solucionados por Soporte en sitio Bogotá: en el mes de junio quedaron 14 requerimientos discriminados de la siguiente manera:

REQUERIMIENTOS SOLUCIONADOS POR SOPORTE EN SITIO	TOTAL
Configuracion	6
Cargue de papel en impresora	5
Asesoria - Consulta	2
Instalación-Desinstalación	1

Total general	14

Tabla 43 Requerimientos solucionados por Soporte en sitio

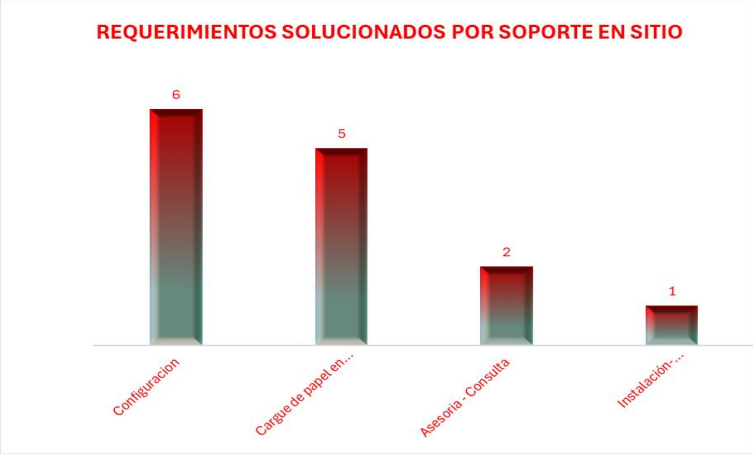


Ilustración 34 Requerimientos Solucionados por Soporte en sitio

Requerimientos solucionados por Soportes Territoriales: Para el mes de junio quedaron en estado solucionados 21 requerimientos discriminados de la siguiente manera:

REQUERIMIENTOS SOLUCIONADOS POR TERRITORIALES	TOTAL
Instalacion	20
Soporte Aplicaciones Office 365	1
Total general	**21**

Tabla 44 Requerimientos solucionados por Soportes Territoriales

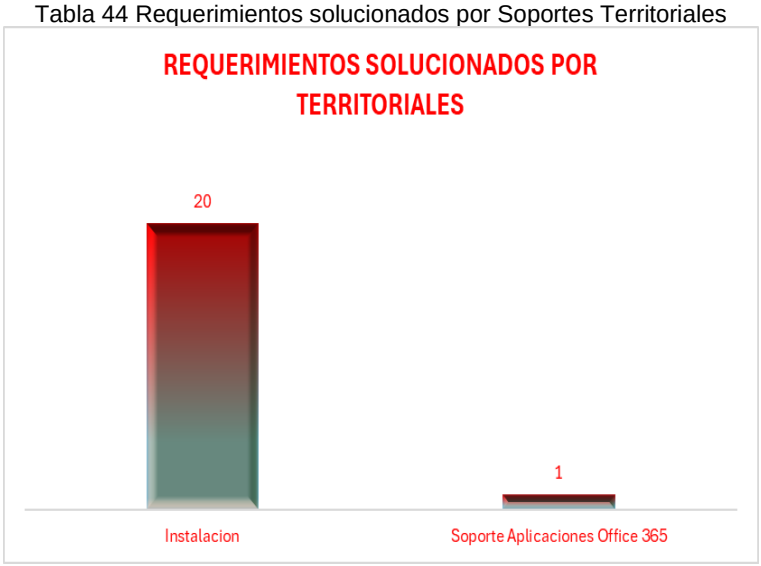


Ilustración 35 Requerimientos solucionados por Soportes Territoriales

- **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 junio se cerraron 633 casos, discriminados así: Asesoría – Consulta con 185 casos, Cambiar contraseña con 136 casos, Creación de usuario 56, Cambio de

grupo con 42 casos, Instalación y configuración VPN con 29 casos, Aumento de cuota con 21 casos, Configuracion con 19 casos, Inactivar usuario con 15 casos, Reportar Solicitud/Falla con 12 casos, Instalación y configuración VPN con 11 casos, a comparación del mes anterior se evidencia una disminución del 66,94%% que corresponden a 1282 casos.

CERRADOS POR LA MESA DE SERVICIOS	TOTAL
Asesoria - Consulta	185
Cambiar contraseña	136
Creacion de usuario	56
Cambio de grupo	42
Instalacion y configuracion VPN	29
Aumento de cuota	21
Configuracion	19
Inactivar usuario	15
Reportar Solicitud/Falla	12
Modificar usuarios	11
Asignar Radicado TYS	10
Habilitar usuario	10
Depuración Bandeja	10
Crear usuario	5
Asignacion de licencia	5
Instalacion - Configuracion	5
Informes de usuarios	4
Configuración MFA	4
Préstamo Equipo (portátil o PC)	3
Falla radicacion	3
Asignacion - Modificacion Roles	3
Relanzamiento	3
Solicitud Backup	2
Backup	2
Traslado - Movimiento	2
Instalar - Configurar	2
Configuracion de PST	2
Crear grupos de seguridad	2
Suspender - Finalizar Radica TyS	2
Permisos	2
Radicar una solicitud	2
Permitir acceso	2
Informes y Reportes	2
Falla Funcional	2
Mantenimiento preventivo	2
Caida - Degradacion	1
Solicitud de cambio	1
Administracion de equipos	1
Falla conexión VPN	1
Crear carpeta	1
Conectar a red Mintrabajo	1
Crear/Modificar/Eliminar	1
Solicitud depuracion carpeta	1
Equipo Periférico	1
Soporte Aplicaciones Office 365	1
Agregar a sitios permitidos	1
Asesoria PDF	1
Desbloquear usuario	1

Asignacion de permisos	1
Asesoria Excel	1
Asignar permisos	1
Total general	**633**

Tabla 45 Casos cerrados por la mesa de servicios

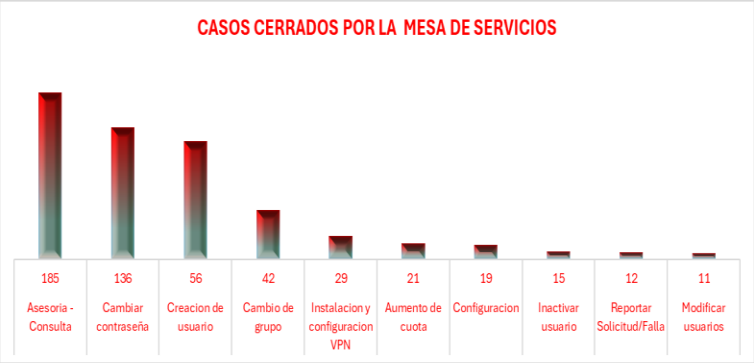


Ilustración 36 Casos cerrados por la mesa de servicios

Casos Cerrados por Soporte en Sitio: Se indica el top 10 de Requerimientos cerrados por soporte en sitio, para el mes de junio se cerraron 2069 casos discriminados así: Asesoría - Consulta con 554 casos, Cargue de papel en impresora con 374 casos, Configuración con 270 casos, Instalación - Configuración con 196 casos, Préstamo con 65 casos, Asesoria Excel con 62 casos, Conectar a red Mintrabajo, con 47 casos, Asesoria Word con 44 casos, Asesoria Consulta con 34 casos a comparación con el mes anterior se tiene una disminucion del 31,84% que corresponde a 962 casos.

CERRADOS POR SOPORTE EN SITIO	TOTAL
Asesoria - Consulta	554
Cargue de papel en impresora	374
Configuracion	270
Instalacion - Configuracion	196
Prestamo	65
Asesoria Excel	62
Instalacion y configuracion VPN	52
Conectar a red Mintrabajo	47
Asesoria Word	44
Asesoria Consulta	34
Soporte Aplicaciones Office 365	29
Asesoria PDF	25
Aumento de cuota	25
No imprime	24
Asignación de equipo (portátil o PC)	23
Traslado - Movimiento	20
Solicitud Backup	16
Conectar a red Invitados	15
Instalación-Desinstalación	15
Instalación - Configuracion	14
Cambio Toner	13
Mantenimiento preventivo	13
Borrado seguro Portátil	11
Devolución de equipo (portátil o PC)	9
Envio y recepción de correos	9
No enciende	8
Solicitud instalacion	8
Error sincronizacion	7

Falla - error	7
Falla - Error conexión a red	7
Atasco	6
Backup	5
Falla Excel	5
Lentitud - Bloqueo	5
Impresión deficiente	4
Asesoria Power Point	4
Copia de informacion	4
Falla Word	3
Reportar Solicitud/Falla	3
Falla Aplicativo	3
Cambiar contraseña	2
Borrado seguro PC	2
Préstamo Equipo (portátil o PC)	2
Equipo Impresora	2
Configuracion de PST	2
Solicitud de cambio	2
Falla Aplicaciones Office 365	2
Falla General	2
No escanea	2
Error de aplicación	1
Daño Fisico	1
Asesoria en ZIP	1
Bloqueo Navegador	1
Falla PDF	1
Habilitar punto de red	1
Falla Cargue pagina web	1
Falla aplicación	1
Desinstalacion	1
Informes y Reportes	1
Falla al cargar archivos	1
Lentitud gestor	1
Equipo Periférico	1
Total general	**2069**

Tabla 46 Casos cerrados por soporte en sitio

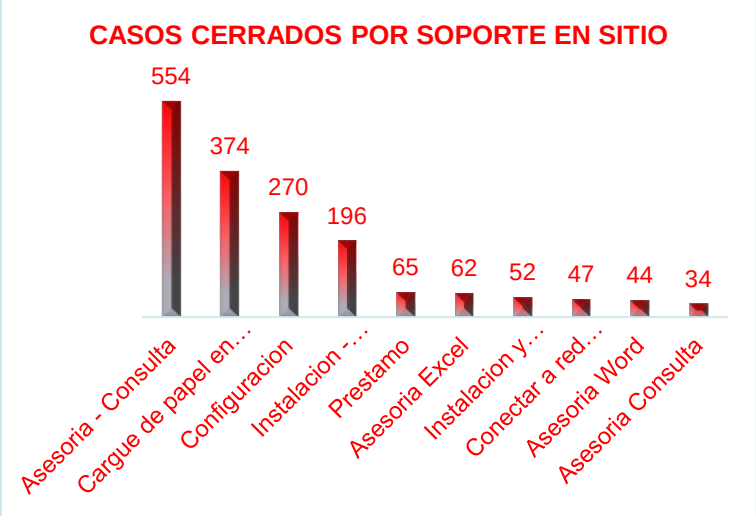


Ilustración 37 casos cerrados por Soporte en Sitio

Casos Cerrados por soporte en sitio Territoriales: Se indica el top 10 de Requerimientos cerrados por soporte en Territorio, para el mes de junio se cerraron 1418 casos discriminados así: Asesoría - Consulta con 233 casos, Cargue de papel en impresora con 192 casos, Instalacion - Configuracion con 159 casos, Configuración con 155 casos, Asesoría PDF con 96 casos, Asesoria Word con 72 casos, Asesoria Excel con 61 casos, Prestamo con 37 casos, Traslado - Movimiento con 32 casos, a comparación con el mes anterior se tiene una disminución del 46,61% que corresponde a 915 casos.

CASOS CERRADOS POR SOPORTE TERRITORIAL	TOTAL
Asesoria - Consulta	233
Cargue de papel en impresora	192
Instalacion - Configuracion	159
Configuracion	155
Asesoria PDF	96
Asesoria Word	72
Asesoria Excel	61
Prestamo	37
Cambio Toner	33
Traslado - Movimiento	32
Asesoria Consulta	31
Soporte Aplicaciones Office 365	31
Mantenimiento preventivo	27
Copia de informacion	21
Instalacion y configuracion VPN	18
Aumento de cuota	18
Atasco	17
Falla - Error conexión a red	17
Reportar Solicitud/Falla	11
Solicitud instalacion	11
Falla - error	11
Envio y recepción de correos	10
Conectar a red Mintrabajo	10
Asignación de equipo (portátil o PC)	9
No imprime	9
Lentitud - Bloqueo	8
Error sincronizacion	6
Devolución de equipo (portátil o PC)	6
Instalación - Configuracion	5
Instalación-Desinstalación	5
Zabbix	5
Préstamo Equipo (portátil o PC)	5
Asesoria en ZIP	4
Revision estado del canal	4
No enciende	4
Solicitud Backup	4
Cambio de unidad de imagen	3
Borrado seguro Portátil	3
No escanea	3
Falla Cargue pagina web	3
Falla Aplicativo	3
Error de aplicación	2
Falla- Error	2

Asesoria Power Point	2
Falla Aplicaciones Office 365	2
Falla Excel	2
Borrado seguro PC	2
Equipo Impresora	2
Falla de sistema operativo	2
Intermitencia - Lentitud	1
Instalacion	1
Falla PDF	1
Daño Fisico	1
Equipo Periférico	1
Backup	1
Equipo Conectividad internet	1
Falla instalacion	1
Instalar - Configurar	1
Falla del lector	1
Total general	**1418**

Tabla 47 Casos cerrados por Territoriales

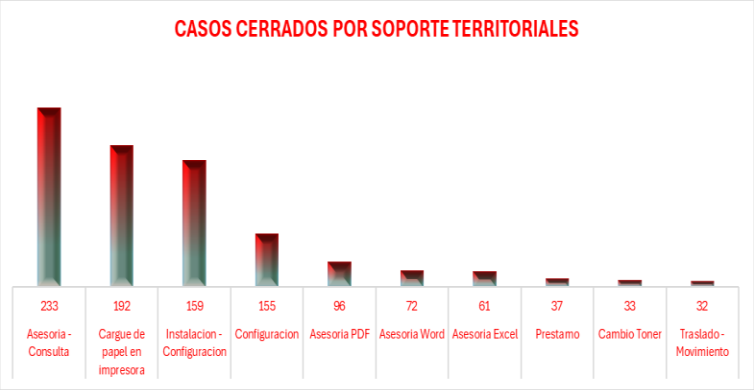


Ilustración 38 Casos cerrados por Territoriales

- **Casos Atendidos a Usuarios VIP**

Durante este periodo se crearon 2090 solicitudes para ser atendidas por soporte en sitio, de estas solicitudes se evidenciaron 109 casos creados para VIPs los cuales fueron atendidos y solucionados dentro de los ANS establecidos por la entidad, discriminados a continuación por tipo de caso:

TIPO DE CASO_VIPS	CUMPLIMIENTO	NO_CUMPLE	TOTAL
Incidents	8		8
Requerimiento	100	1	101
Total general	**108**		**109**

Tabla 48 Casos usuarios VIP

Se atendieron 1981 solicitudes para el resto de los usuarios discriminados así:

TIPO DE CASO-NO-VIPS	CUMPLIMIENTO	NO_CUMPLE	TOTAL
Incidentes	90	2	92
Requerimientos	1888	1	1889
Total general	**1978**		**1981**

Tabla 49 Casos usuarios Regulares

- **Medio de Ingreso de Casos**

Durante el período ingresaron a la mesa de servicio 5771 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:

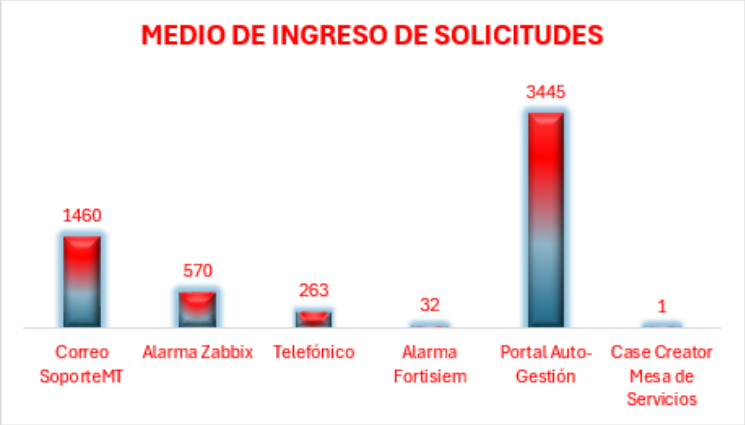


Ilustración 39 Modo de Ingreso de Solicitudes

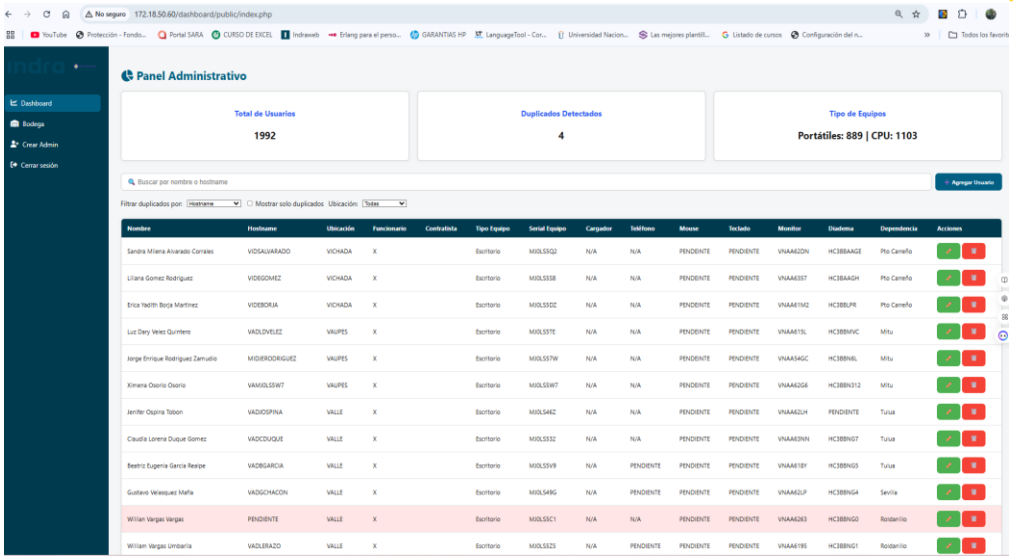
- **Novedades de la operación – Mesa de Servicios y Soporte en sitio Bogotá**

- Durante el mes de junio se continua la organización, actualización del directorio activo para sede central y Territoriales, se continúa realizando la depuración de usuarios de vigencias pasadas que ya no están en la entidad y continúan con licenciamiento activo, esta información fue entrega a la supervisión para solicitar la inactivación de esos usuarios y liberar las licencias.

- De las 30 territoriales, se cuenta con un avance del 80,00% en la actualización del directorio activo quedando pendiente para el mes de julio las siguientes territoriales:

DT Atlántico	/	Pendiente por Resolución por parte de director territorial
DT Cundinamarca	/	Pendiente por Resolución por parte de director territorial
DT Magdalena	/	Pendiente por Resolución por parte de director territorial
DT Quindío	/	Pendiente por Resolución por parte de director territorial
DT Santander	/	Pendiente por Resolución por parte de director territorial
DT Bogotá	/	Pendiente por Resolución por parte de director territorial.

- Se encuentra en diseño y construcción una página web donde se pueda ver el inventario en línea de los equipos que tiene asignados Indra al Ministerio.



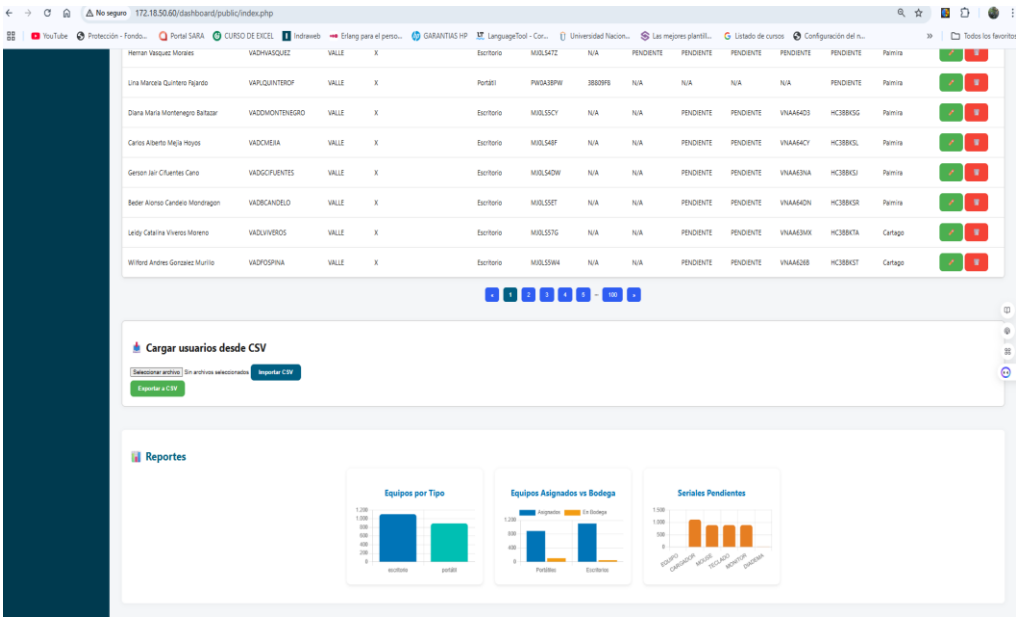


Ilustración 40 Pagina web para visualización de inventario de equipos de computo

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

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

- Visita a 9 inspecciones donde no se cuenta con personal dedicado para solucionar los casos que se requieren.

- Cierre de 1418 casos, dentro de los que se destacan: Asesorías -Consultas, Cargues de Papel, Configuraciones e Instalaciones, Asesorías en PDF, Asesorías en Excel, Asesorías en Word, Prestamos de Equipos y Cambios de Tóner

- Se realiza el arreglo del cableado de las sedes de Medellín, Pasto, Cúcuta, Quibdó, Barrancabermeja y Cartagena de acuerdo con la solicitud de los administradores de redes.

- Se realizan las validaciones y pruebas con los usuarios a nivel nacional del acceso a Youtube para que ellos puedan realizar consultas o adelantar procesos de capacitación nen esta plataforma, en horarios indicados desde sede central.

- Se presenta afectación en Vaupés debido a que desde Recursos Físicos no han aprobado la colocación de un nuevo punto de red, actualmente la impresora está conectada por USB, con el inconveniente de no permitir el monitoreo de la misma desde sede central y cualquier equipo de escritorio extra no puede navegar por Internet. Se está contemplando la compra de un switch de 8 puertos para solventar a corto plazo el inconveniente

- **Atención de servicios en Sedes Territoriales sin personal de soporte en sitio dedicado**

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

Para el período se realizaron las siguientes visitas:

Mes	Territorial	Sede	Servicio	Descripción	Caso
Junio 2025	Mariquita	Tolima	Internet y conectividad	Revisión de conectividad LAN, del estado del canal y conexiones de datos en la Inspección	RF-124229
Junio 2025	Doncello	Florencia	Impresora bloqueada	Soporte debe realizar la revisión en sitio para validar un atasco que bloquea el alimentador de originales	IM125339
Junio 2025	Baranoa	Barranquilla	Internet y conectividad	Instalación de cable UTP que presenta deficiencias de conectividad y acceso a Internet	RF-105059 y RF-105031,
Junio 2025	Sabanalarga	Barranquilla	Internet y conectividad	Verificación de las conexiones en sitio de los equipos de conectividad y verificación de navegación.	RF-125461 y RF-125463
Junio 2025	Tuquerres	Pasto	Mantenimiento semestral de la impresora	Visita del SS en la inspección para realizar el mantenimiento semestral programado	126238
Junio 2025	Ipiales	Pasto	Mantenimiento semestral de la impresora	Visita del SS en la inspección para realizar el mantenimiento semestral programado	RF-126240
Junio 2025	Ubate	Cundinamarca	Revisión de punto de red, canal y PC	Se revisa equipo de escritorio que no prendía, luego de validar, conexiones en la red estado del equipo de cómputo y validaciones del correcto funcionamiento	RF-125111
Junio 2025	Riosucio	Manizales	Mantenimiento semestral de la impresora	Visita del SS en la inspección para realizar el mantenimiento semestral programado	RF-127626
Junio 2025	Puerto López	Villavicencio	Mantenimiento semestral de la impresora	Visita del SS en la inspección para realizar el mantenimiento semestral programado	RF-129540

Tabla 50 Visitas en sedes sin Soporte en Sitio

- **Medición ANS Mesa de Servicios**

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

ID	Indicadores	Resultado	Meta
MDS 1	Tiempo de atención de solicitudes por soporte en sitio	99,65%	95,00%
MDS 2	Tiempo de solución de incidentes por soporte en sitio	99,05%	90,00%
MDS 3	Tiempo de solución de requerimientos por soporte en sitio	99,97%	90,00%
MDS 4	Tiempo de respuesta de la mesa de servicio	99,65%	85,00%
MDS 5	Abandono de llamadas	0,35%	Máximo el 8%

ID	Indicadores	Resultado	Meta
MDS 6	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 51 Medición 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

3.1.1. Datacenter Principal

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

- Depuración de usuarios
- Identificación de cuentas de servicio obsoletas.
- Creación de nuevas cuentas de servicio asociadas a una correcta gestión de estos, usuarios que ya no hacen parte del equipo de tecnología y usuarios utilizados por proveedores que no están alineadas con los estándares de seguridad y de accesibilidad de la entidad.
- Creación de cuentas de servicio a demanda de la entidad y sus servicios.
- Habilitación de privilegios sobre Shared MailBox.

Esto implica revisar regularmente la base de datos de usuarios para identificar cuentas inactivas, duplicadas o desactualizadas, y proceder con su eliminación o actualización según sea necesario. Tras atención de diferentes requerimientos asociados a este punto, se presentó un informe en donde se especifican los tiempos definidos por Microsoft, las actividades realizadas por el equipo de trabajo y las prácticas a consideración por parte de la entidad, ya que se ha identificado, que existen usuarios que comparten información desde OneDrive como repositorio único y no se percatan de descargar estos medios antes de que el usuario propietario del repositorio se desvincule de la entidad.

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.

Se ha venido realizando el despliegue de gran parte de los servidores de Windows 2012 – 2016 - 2019 – 2022 realizando instalación de los KB más recientes, mitigando la falta de instalación de actualizaciones de sistema operativo sobre los servidores de entorno de pruebas de manera adecuada. Asociada a esta actividad se postularon como cambio estándar aquellos RFC identificadas para despliegue de actualizaciones de Windows Server 2012-2016-2019-2022. Se realiza parchado del KB de Win 2012 que generaba vulnerabilidades remanentes y son mitigadas en su totalidad tras la aplicación del parche.

Se genera reporte de la totalidad de máquinas virtuales sobre cumplimiento de acuerdo con las estadísticas arrojadas por el WSUS y a nivel de cumplimiento de descarga e instalación de actualizaciones se encuentra en un 98-99% de cumplimiento, esto atado a la mitigación de

vulnerabilidades asociada a la instalación de estas actualizaciones. Es importante mencionar que el porcentaje de cumplimiento por encima del 96% es una métrica que se ha mantenido durante la gran mayoría de la ejecución del contrato.

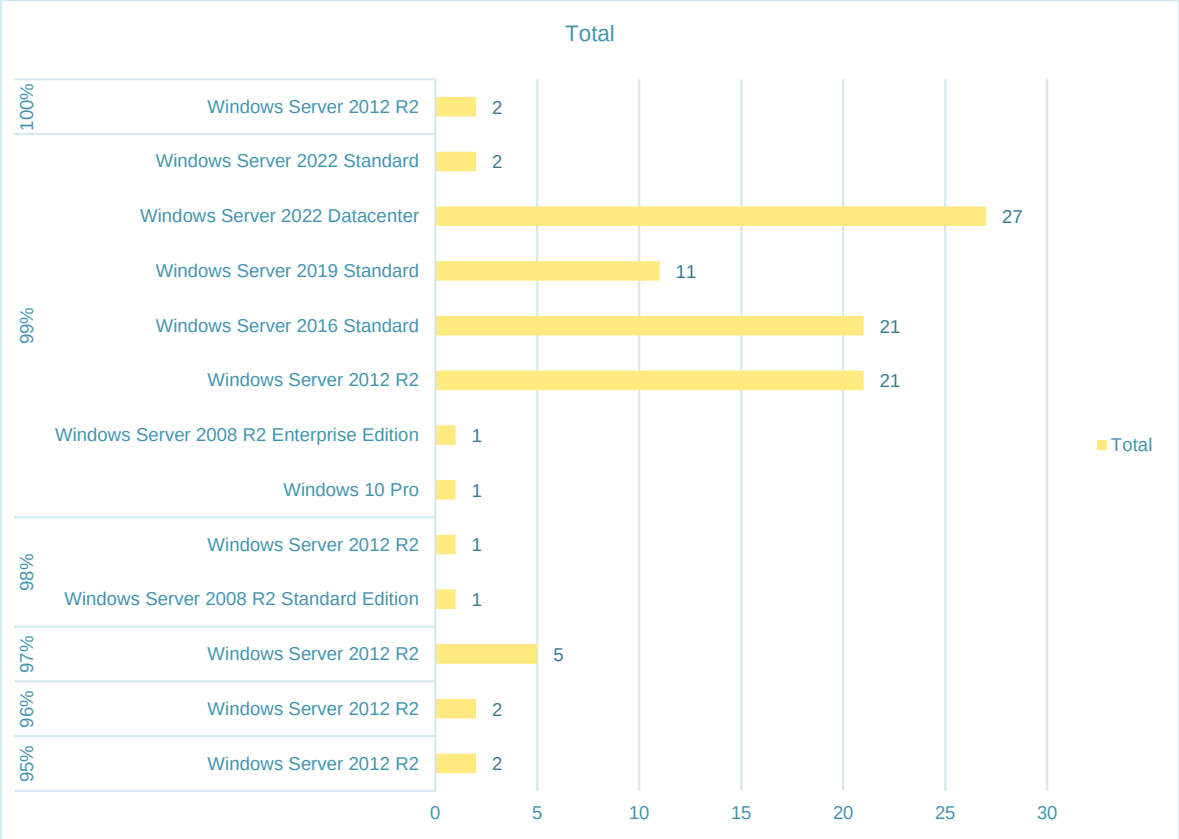


Ilustración *41* Cumplimiento WSUS

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.

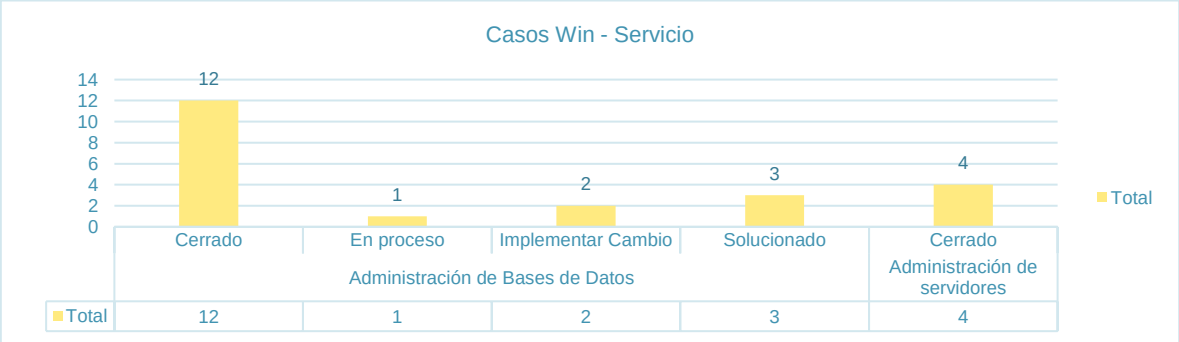


Ilustración 42 Estado final de los casos Windows

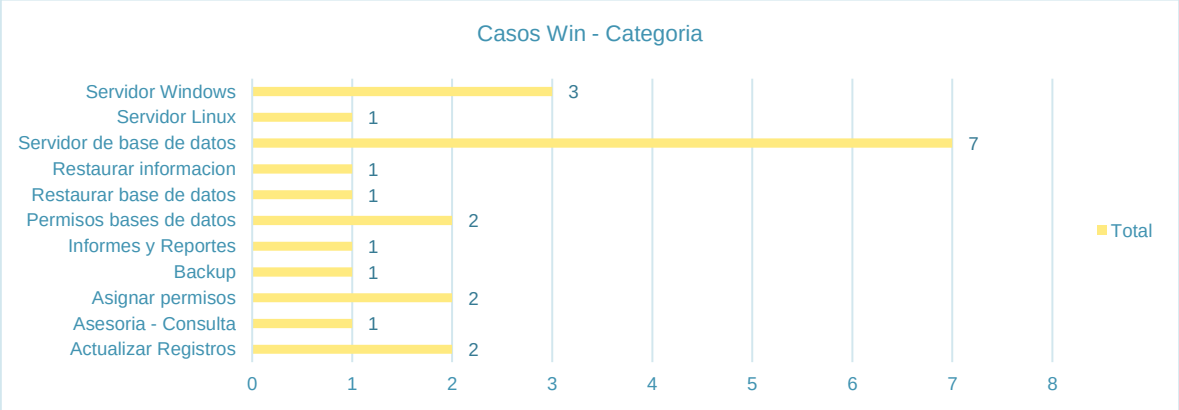


Ilustración 43 Casos por categorías Windows

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.

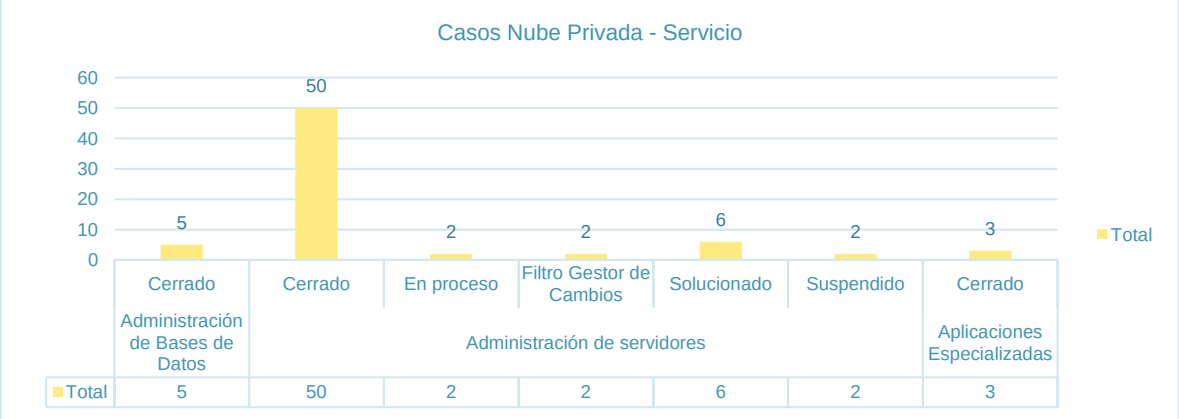


Ilustración 44 Estado final de los casos Nube privada

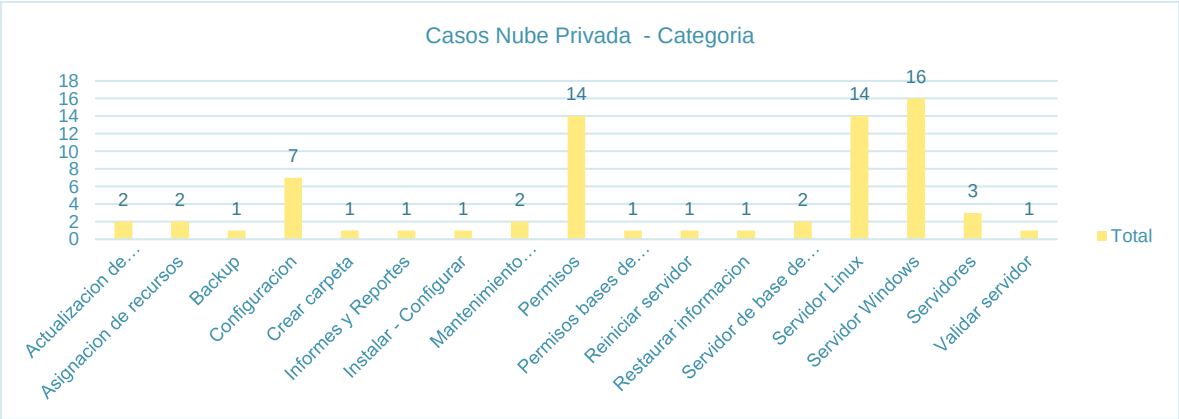


Ilustración 45 Casos por categoría Nube privada y pública

Se exponen las capacidades definidas para la nube privada de acuerdo las fichas técnicas:

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

Tabla 52 capacidades de acuerdo con las fichas técnicas

Se observa que para los siguientes ítems se presenta un diferencial de lo aprovisionado versus lo expuesto en la ficha técnica, se divide en diferentes escenarios, para que la entidad tenga claridad de cuanto consume cada entorno virtualizado de los recursos que permiten el funcionamiento de su operación.

Total MinT (Con servidores para desaprovisionar + ambientes de pruebas)	
Descripción Características	Total
vCPU	780
RAM	3 TB
Almacenamiento	146 TB
Numero de Servidores	109

Tabla 53 Infra total + servidores de pruebas + servidores a desaprovisionar

Total MinT (Sin servidores para desaprovisionar con ambientes de pruebas)	
Descripción - características	Total
vCPU	606
RAM	2.7 TB
Almacenamiento	117 TB
Numero de Servidores	88

Tabla 54 Infra total producción + servidores de pruebas de la entidad

Total MinT (Sin servidores para desaprovisionar sin ambientes de pruebas)	
Descripción - características	Total
vCPU	503
RAM	2.2 TB
Almacenamiento	102 TB
Numero de Servidores	71

Tabla 55 Infra total sin servidores de pruebas

Total MinT (Servidores Pruebas y Desarrollo)	
Descripción - características	Total
vCPU	103
RAM	441 GB
Almacenamiento	14.6 TB
Numero de Servidores	18

Tabla 56 Capacidades consumidas por entornos de pruebas

vCPU Ficha: **657** a vCPU consumida: **606**
Memoria Ficha: **2.6 TB** a Memoria consumida: **2.7 TB**
Almacenamiento Ficha: **120 TB** a Almacenamiento consumido: **117 TB**
Número de Servidores Ficha: **106** a Numero de Servidores disponibles: **88**

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 por encima de lo definido en la ficha en los ítems de vCPU y RAM, el 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.

	vCPUs	RAM - TB	Capacidad Disco
Consumos	**606**	**2.7 TB**	**117 TB**

Tabla 57 Capacidades consumidas (Sin servidores de backup)

Es importante mencionar que, en el proceso de redimensionamiento de la nube privada de la entidad, los ambientes de pruebas son los que están consumiendo las capacidades que están superando los ítems de RAM y Almacenamiento, 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 no tiene capacidad de crecimiento o ampliación de capacidades de los servicios ya aprovisionados. 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:

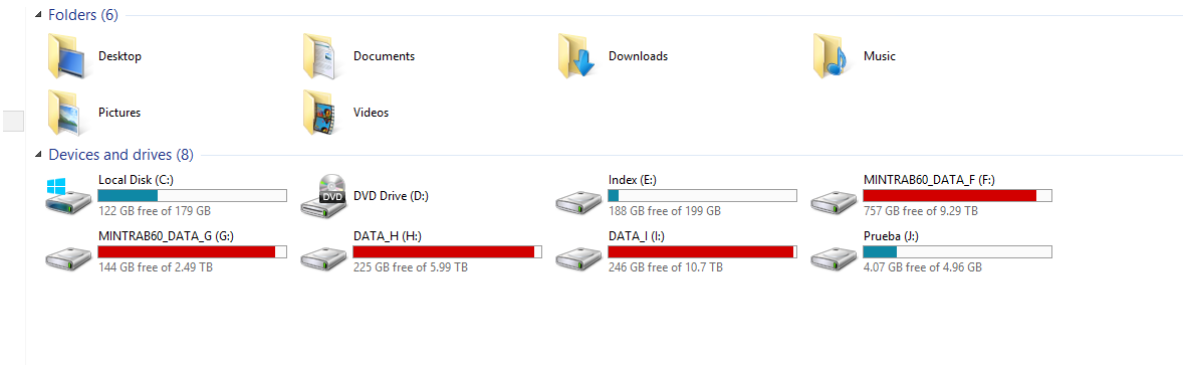


Ilustración 46 Estado File Server Mintrab60

Nube Pública

Se realizó socialización a la entidad de los escenarios de Arquitectura en Nube publica Azure y la interacción hacia los componentes que permiten el funcionamiento de tableros Power BI y componente de ciencia de datos. En este ejercicio de arquitectura, se enfatizó 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 validaron temas relacionados con el monitoreo de estos componentes a través de Azure Monitor, componentes que podrían postularse para desaprovisionamiento, estado de cada suscripción a nivel de arquitectura como de consumo de créditos, recomendaciones a nivel de cumplimiento de políticas establecidas por Azure, nombramiento de recursos y grupos de recursos, entre otras apreciaciones plasmadas en el documento de Línea base del servicio de Nube pública. Se indica la implementación de Well Architected Framework, el cual está diseñado para proveer los lineamientos de alto nivel con las mejores Prácticas para ayudar a mantener las aplicaciones confiables, seguras, con alto rendimiento, gestión del costo, y la excelencia operativa de los recursos de nube.

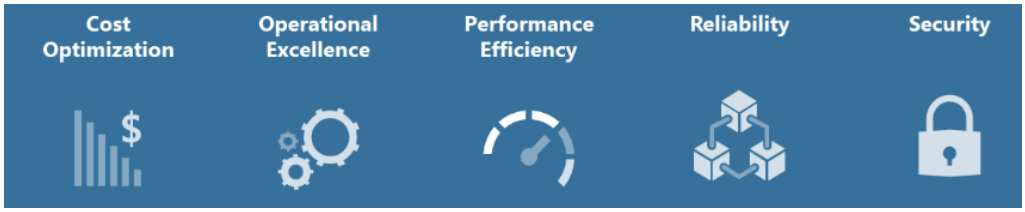


Ilustración 47 Bondades de la implementación del Well Architected Framework (WAF)

La idea de la implementación de este framework de arquitectura en nube pública permitirá llegar a un nivel de madurez y optimización de recursos en la nube publica de la entidad, permitiendo el siguiente escenario de segmentación de componentes y de suscripciones:

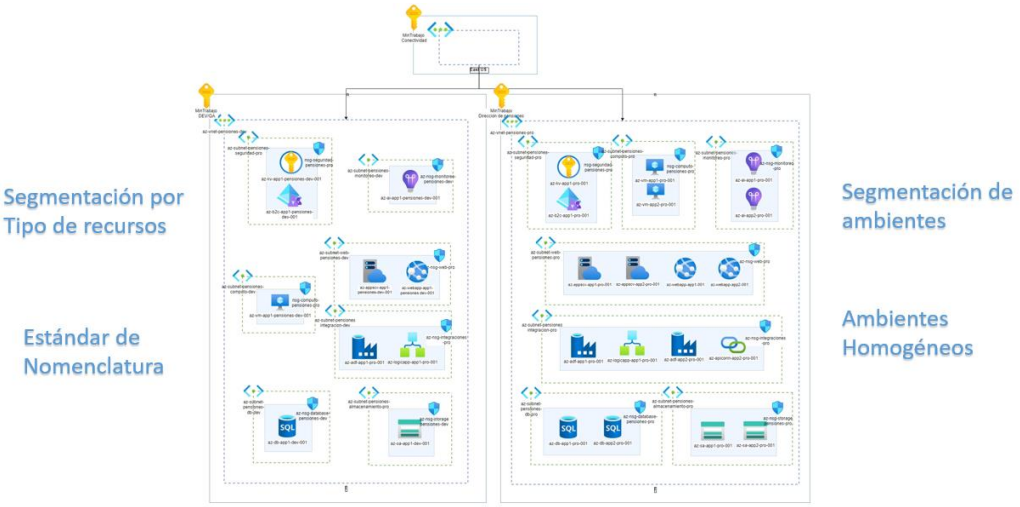


Ilustración 48 Proyección de Modelo de Suscripción

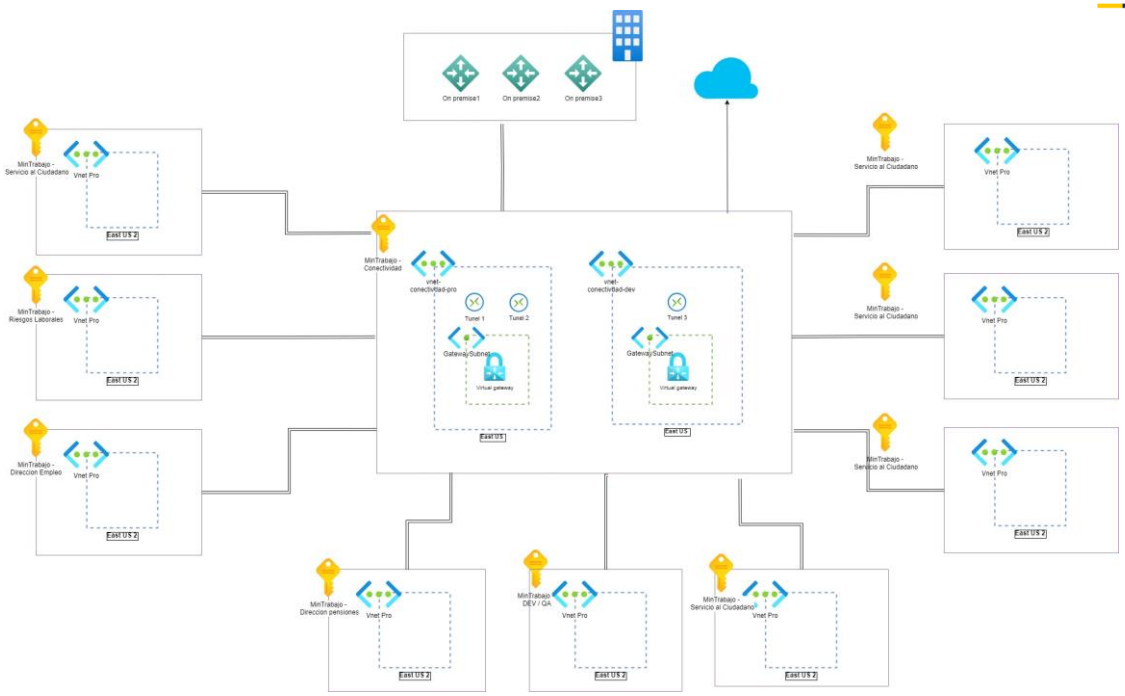


Ilustración 49 Modelo de Tenant bajo arquitectura

Tras el contexto anterior, se informa que se ha realizado la implementación de la suscripción de Conectividad y se están realizando los afinamientos para que pueda comunicarse transversalmente con las demás suscripciones del tenant de Azure de la entidad.

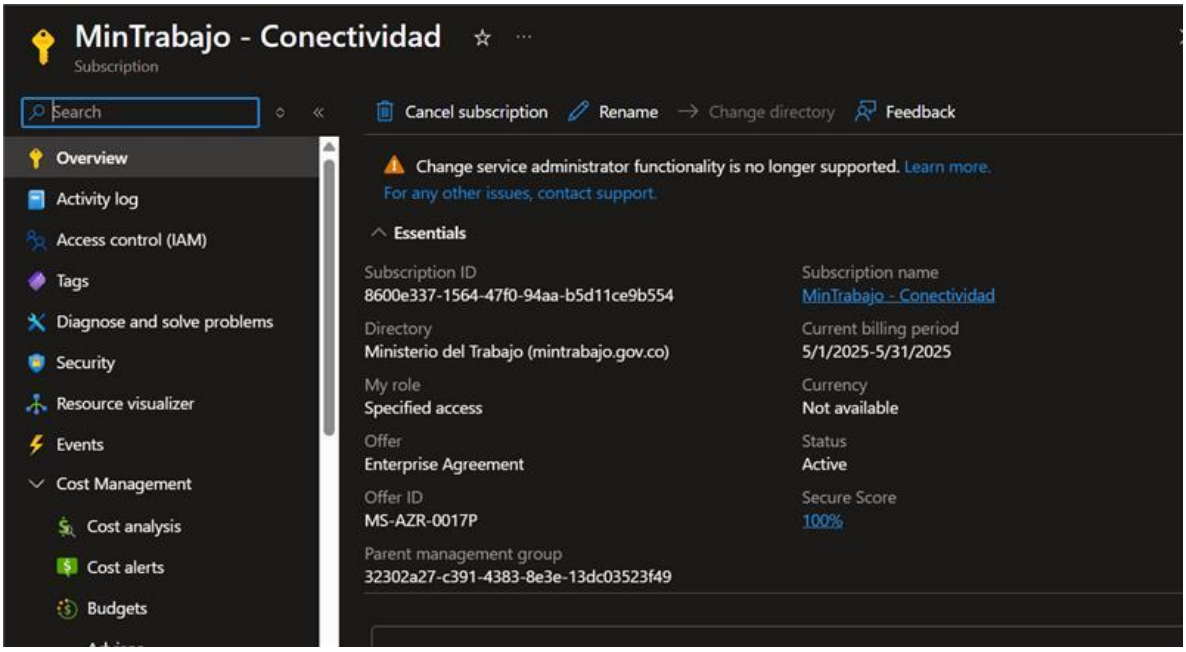


Ilustración 50 Suscripción de Conectividad

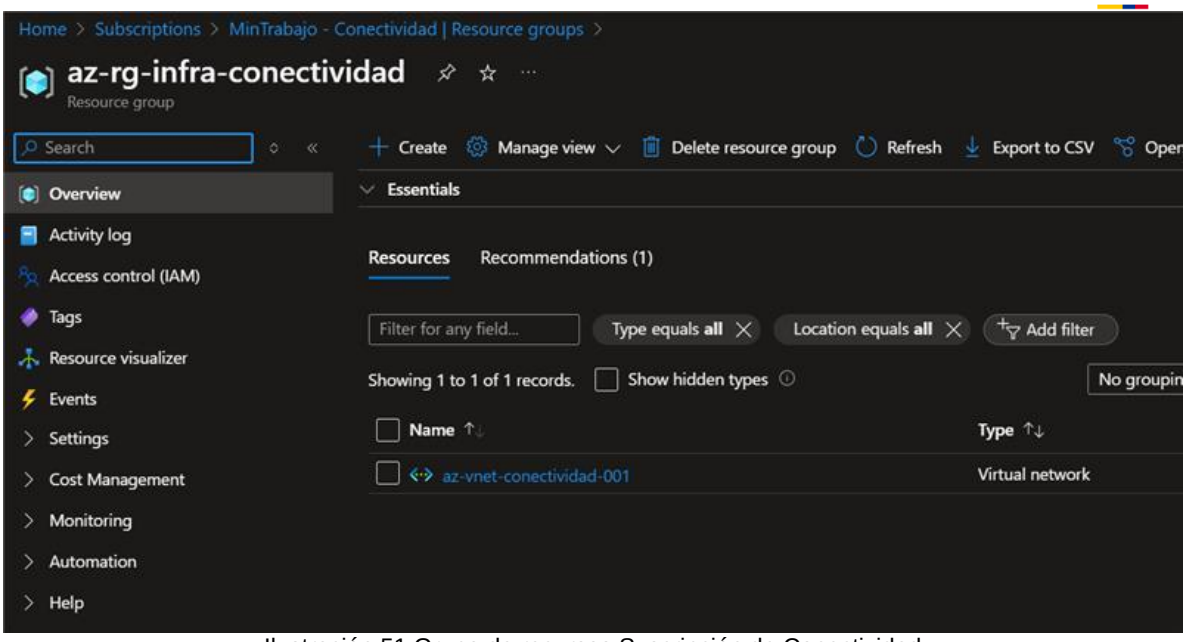


Ilustración 51 Grupo de recursos Suscripción de Conectividad

De acuerdo con lo anterior y en articulación con las necesidades expuestas por la entidad se ha realizado acompañamiento a las ventanas de mantenimiento ejecutadas por el proveedor Claro dentro del sistema de información SICIP, en donde podemos observar una reiterada ejecución del mismo control de cambios con resultados negativos para el sistema de información, en donde podemos evidenciar los siguientes ítems:

- RFC-118712 los encargados de la ejecución de despliegue de la webapp y logic app por parte del operador Global Hits no se presentan en la sesión programada desde las 6pm, de igual manera se evidencia que realizaron ejecución de la logic app en los logs e ingresando 104 registros nuevos a la base de datos de SICIP en la tabla de correspondencia, se deja evidencia de personas en la sesión y horario de finalizado por inasistencia por parte del operador.
- RFC-122127 El operador encargado Global Hits, no asistió a la sesión propuesta por ellos en el horario de 6pm a 8 pm, se deja evidencia con el funcionario que se encuentra en la sesión del incumplimiento por parte del proveedor.
- RFC-115367 No se realizó la ejecución propuesta por parte del operador, se verifican modificaciones en la logic app, se evidencia inicio de políticas el 17 de mayo, no acordes a lo planteado en el RFC - 115367. De igual manera se verifica logs y contiene las ejecuciones normales de su programación de flujo.

En mención de la ejecución del RFC-122127 se agendo una sesión de trabajo con el equipo de Claro para realizar el despliegue. La sesión fue agendada por el mismo proveedor:

URL de la sesión: URL

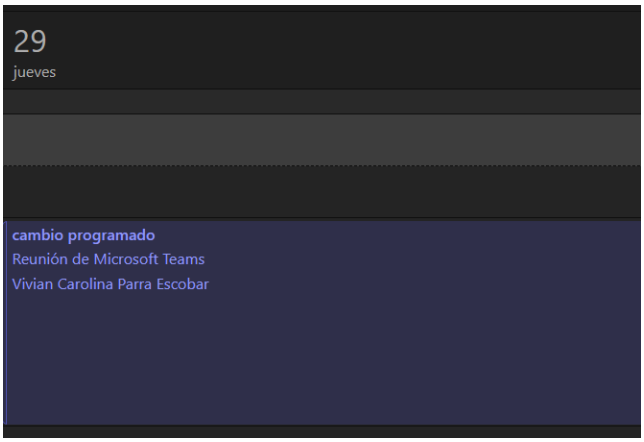


Ilustración 52 Sesión ejecución de cambio

Tras haber concretado la sesión, el equipo de trabajo de la UT/Soporte Informático se unió a la sesión, pero el equipo de Claro nunca se unió a la sesión.

Evidencia de la sesión donde asistió el equipo de Nube Publica y el área funcional, pero el equipo de Claro no se unió para realizar la ejecución del RFC:



Ilustración 53 Evidencia de Inasistencia del proveedor

Tras revisión el día 30/05/2025 observamos que la Web App no tiene despliegues:

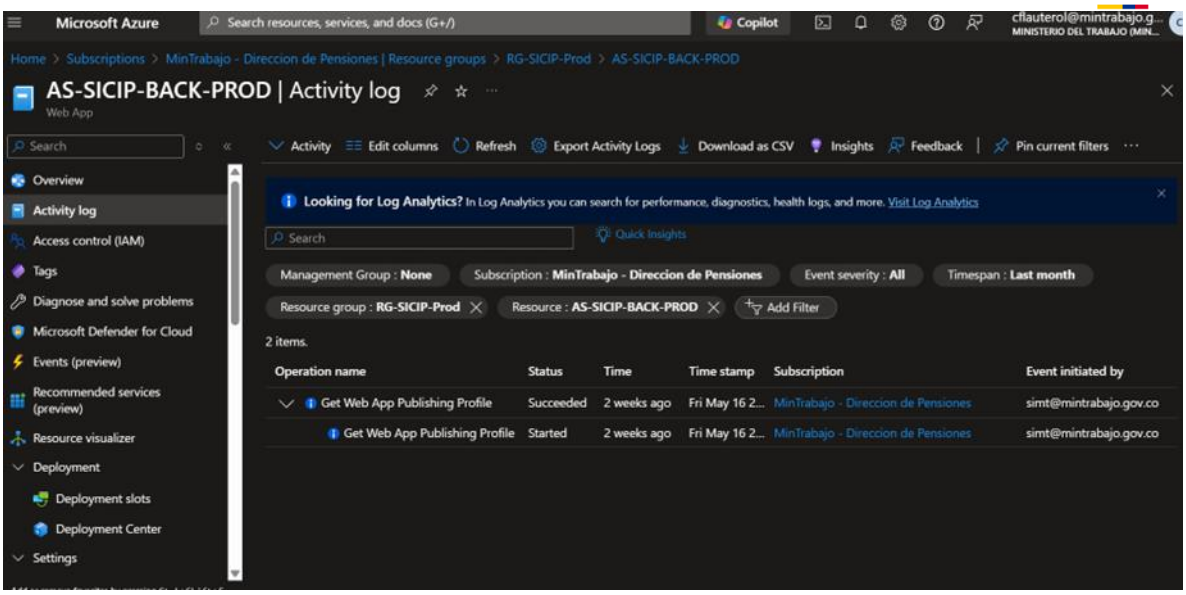


Ilustración 54 Web App sin despliegues

La Logic App tiene ejecuciones de flujo:

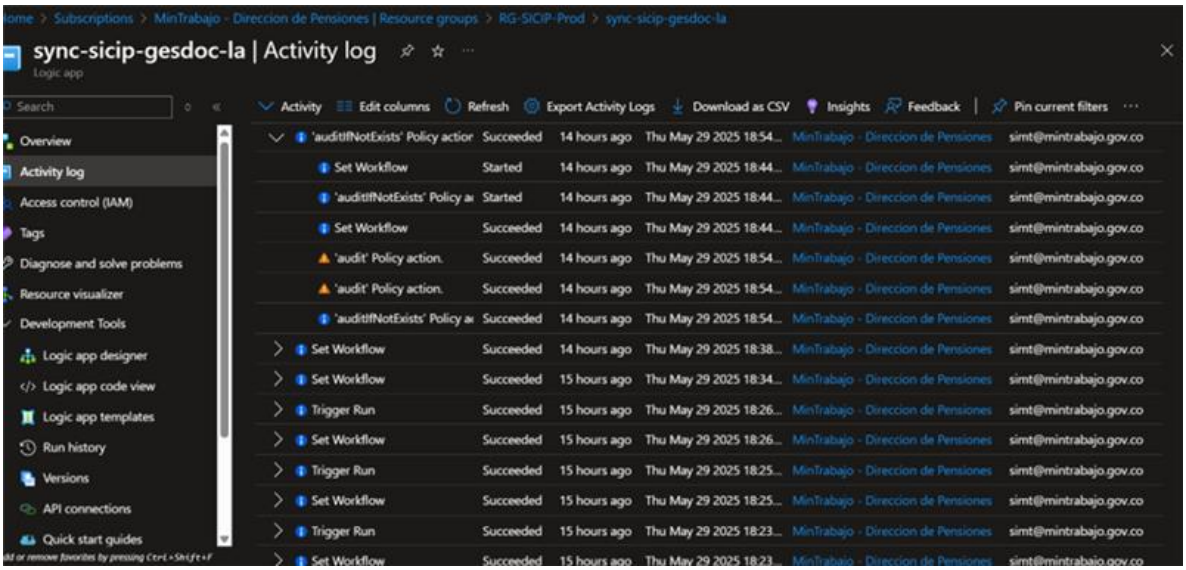


Ilustración 55 Ejecución de Flujo

El flujo continúa presentando fallas, evidencias de viernes 30/05/2025 en horas de la mañana:

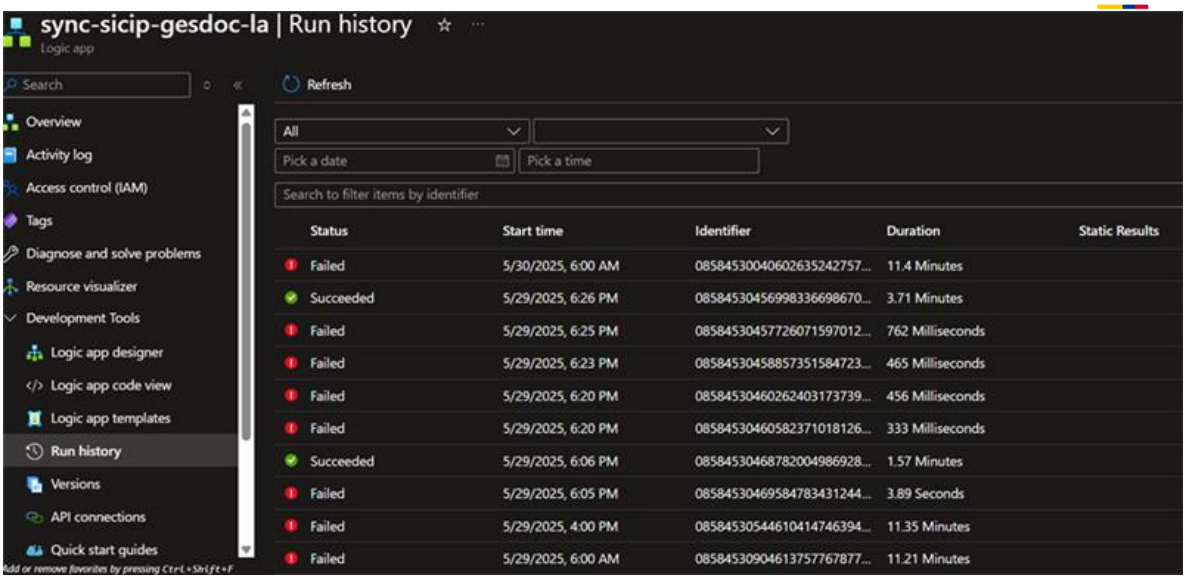


Ilustración 56 Errores de ejecución

De acuerdo con el contexto anterior se procedió a realizar el siguiente informe técnico que tuvo como objetivo documentar y evidenciar de manera estructurada los despliegues realizados por el proveedor Global Hitss en el proyecto del sistema de información SICIP, detallando los componentes involucrados en la nube de Azure, los desarrollos en código SQL y las integraciones mediante Logic Apps. Asimismo, identificar y registrar los aciertos, errores y aprendizajes derivados de estos despliegues, con el fin de fortalecer la trazabilidad técnica del proyecto y aportar insumos valiosos para la mejora continua en futuras fases de desarrollo e implementación. Así como:

- Registrar de manera detallada cada uno de los despliegues realizados por el proveedor Global Hitss en el marco del proyecto SICIP, especificando fechas, componentes intervenidos y resultados obtenidos.
- Identificar y documentar las incidencias, fallas o errores presentados durante los procesos de despliegue, así como las acciones correctivas implementadas.
- Evidenciar los despliegues exitosos, destacando las buenas prácticas técnicas aplicadas y los resultados positivos alcanzados.
- Analizar el comportamiento de los componentes desplegados en Azure, incluyendo Logic Apps, servicios SQL y otros recursos asociados, para evaluar su desempeño y estabilidad.

Generar insumos que sirvan de base para la mejora continua en la gestión de despliegues futuros, fortaleciendo la trazabilidad y calidad del sistema de información SICIP.

En el marco del proyecto SICIP, se han implementado y soportado diversos servicios tecnológicos, los cuales conforman la arquitectura funcional y operativa del sistema. Estos servicios han sido desplegados, configurados y gestionados por el proveedor Global Hitss, y forman parte de la solución integral desarrollada sobre la nube Microsoft Azure. A continuación, se detallan los principales servicios soportados:

- Azure App Services: Plataforma utilizada para el alojamiento y ejecución de aplicaciones web desarrolladas en .NET y Angular. Permite el escalado automático, integración con CI/CD y monitoreo continuo.
- Azure Logic Apps: Servicios de automatización que permiten la integración de procesos entre distintas aplicaciones y sistemas, facilitando el flujo de información mediante conectores predefinidos y reglas lógicas.

- Azure SQL Database: Motor de base de datos relacional en la nube que permite almacenar y consultar la información estructurada del sistema. Incluye funciones de alta disponibilidad, seguridad y escalabilidad.
- Bases de Datos Oracle: Sistemas de gestión de datos robustos utilizados para integrar información preexistente y permitir la interoperabilidad con sistemas legados a través de servicios API y/o conectores intermedios.
- Azure DevOps: Plataforma utilizada para la gestión del ciclo de vida del desarrollo, incluyendo control de versiones (repositorios Git), planificación de tareas (Boards), integración y entrega continua (Pipelines), y gestión de artefactos.
- API REST: Servicios web desarrollados en .NET para permitir la comunicación entre el frontend (Angular) y el backend, así como con otros sistemas externos que requieren acceso a funcionalidades o datos del sistema SICIP.
- Front-End en Angular: Interfaz web del sistema, desarrollada con Angular, que proporciona una experiencia de usuario dinámica, moderna y responsiva.
- Back-End en .NET: Servicios y lógica de negocio desarrollados en .NET Core, encargados del procesamiento de datos, validaciones y conexión con las bases de datos.
- Monitoreo y Diagnóstico en Azure: Servicios como Azure Monitor, Application Insights y Log Analytics, utilizados para supervisar el rendimiento, registrar eventos, detectar errores y tomar decisiones basadas en métricas operativas.

Para garantizar la calidad, trazabilidad y estabilidad del sistema SICIP en cada uno de sus ambientes (desarrollo, pruebas, preproducción y producción), se pretende en la entidad del Ministerio del Trabajo adopte una metodología de despliegue basada en buenas prácticas de DevOps, integrando automatización, control de versiones, pruebas y validación progresiva de los componentes.

La metodología se estructura en las siguientes fases:

1. Planificación del Despliegue
    - Definición de objetivos, alcance, componentes involucrados y responsables del despliegue.
    - Identificación de riesgos, ventanas de mantenimiento y validaciones previas.
    - Registro del despliegue en Azure DevOps (Pipeline, Release Plan, Work Items).

2. Preparación del Entorno
    - Verificación del estado del entorno de destino (infraestructura, servicios activos, disponibilidad).
    - Actualización de configuraciones específicas por entorno (variables, secretos, cadenas de conexión).
    - Validación de integraciones con sistemas externos y recursos compartidos.

3. Control de Versiones y Automatización
    - Uso de repositorios Git (Azure DevOps Repos) para gestionar el código fuente de Angular, .NET, Logic Apps y scripts SQL.
    - Construcción de artefactos mediante build pipelines automatizados.
    - Implementación de release pipelines para despliegues controlados y repetibles, con aprobación manual en ambientes sensibles.

4. Ejecución del Despliegue
    - Despliegue automatizado o semiautomatizado de componentes utilizando Azure DevOps Pipelines.
    - Aplicación de scripts SQL y configuración de Logic Apps.
    - Despliegue de servicios web en Azure App Services y actualización del frontend en Angular.

5. Pruebas Post-Despliegue
    - Verificación del correcto funcionamiento de los servicios desplegados (sanity check).
    - Ejecución de pruebas automatizadas y validaciones funcionales.
    - Validación de logs, métricas y disponibilidad de endpoints (APIs, UI, bases de datos).

6. Registro y Documentación
    - Registro de resultados en Azure DevOps (estado, logs, cambios).
    - Documentación de incidencias, errores corregidos y hallazgos.
    - Trazabilidad con historias de usuario o requerimientos funcionales.

7. Retroalimentación y Mejora Continua
    - Revisión con el equipo técnico de lecciones aprendidas y oportunidades de mejora.
    - Ajuste de procesos o pipelines para futuros despliegues.
    - Validación de cumplimiento de estándares y políticas institucionales.

Los despliegues realizados por parte del operador Global Hitss se expondrá desde el área de Soporte Informático del ministerio del trabajo, lo observado, verificado en los componentes y de acuerdo con lo informado por parte del área funcional, esto se realiza en forma cronológica desde el mes de mayo 2025.

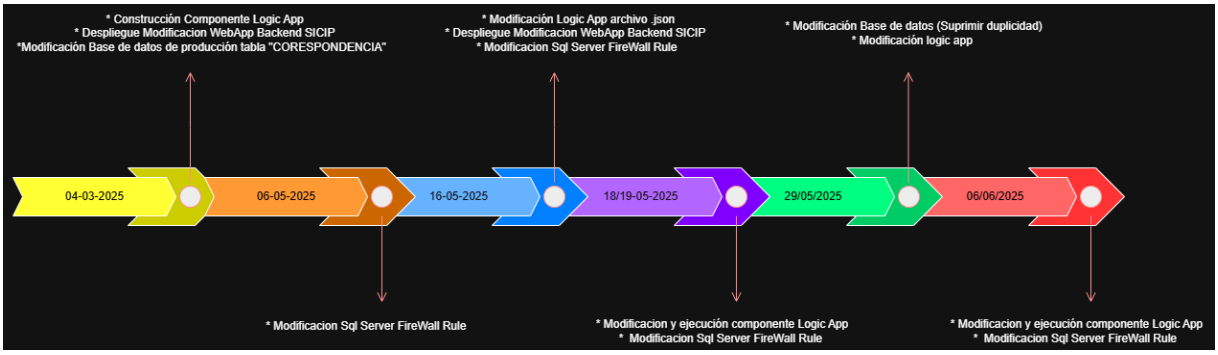


Ilustración 57 Linea_Tiempo_deploy

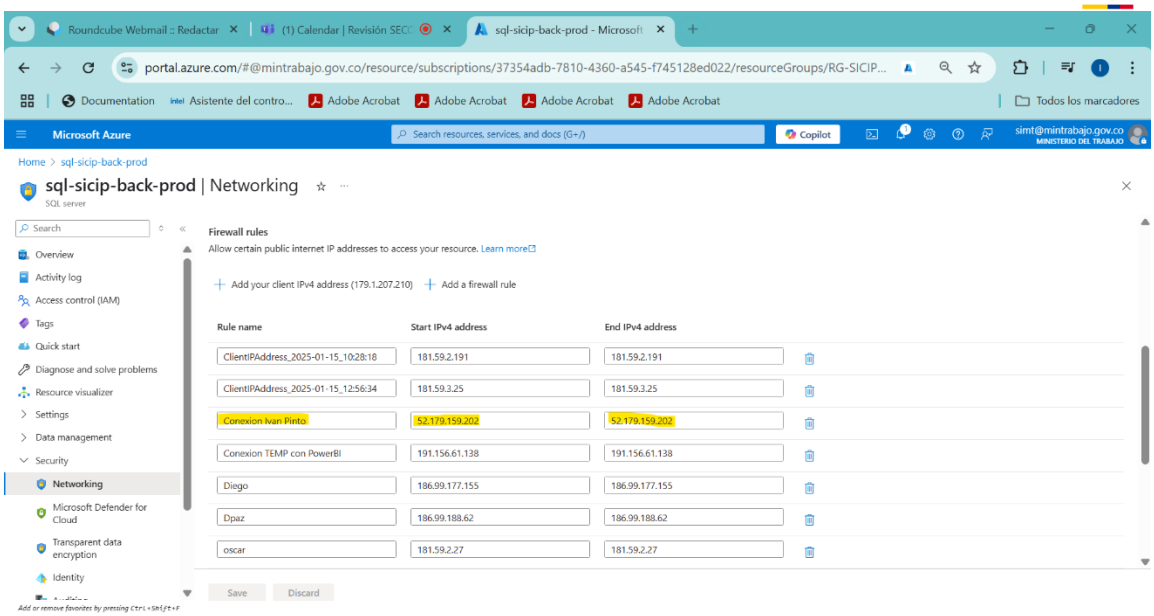


Ilustración 58 Rule FireWall

Update SQL server firewall rules	Started	2025-05-16T21:32:36.795Z	/subscriptions/37354adb-7810-4360-a545-f745128ed022/resourceGroups/RG-SICIP-Prod/providers/Microsoft.Sql/servers/sql-sicip-back-prod/firewallRules/ClientIPAddress_2025-5-16_16-
Update SQL server firewall rules	Succeeded	2025-05-16T21:32:38.154Z	/subscriptions/37354adb-7810-4360-a545-f745128ed022/resourceGroups/RG-SICIP-Prod/providers/Microsoft.Sql/servers/sql-sicip-back-prod/firewallRules/ClientIPAddress 2025-5-16 16-

Ilustración 59 Update Rule FireWall

Get Web App Publishing Profile	Started	2025-05-16T22:26:59.760Z	/subscriptions/37354adb-7810-4360-a545-f745128ed022/resourceGroups/RG-SICIP-Prod/providers/Microsoft.Web/sites/AS-SICIP-BACK-PROD
Get Web App Publishing Profile	Succeeded	2025-05-16T22:27:00.463Z	/subscriptions/37354adb-7810-4360-a545-f745128ed022/resourceGroups/RG-SICIP-Prod/providers/Microsoft.Web/sites/AS-SICIP-BACK-PROD

Ilustración 60 publishing Web App

Set Workflow	Started	2025-05-18T00:24:24.919Z	/subscriptions/37354adb-7810-4360-a545-f745128ed022/resourceGroups/RG-SICIP-Prod/providers/Microsoft.Logic/workflows/sync-sicip-gesdoc-la
'auditIfNotExists' Policy action.	Started	2025-05-18T00:24:25.825Z	/subscriptions/37354adb-7810-4360-a545-f745128ed022/resourceGroups/RG-SICIP-Prod/providers/Microsoft.Logic/workflows/sync-sicip-gesdoc-la
Set Workflow	Succeeded	2025-05-18T00:24:25.841Z	/subscriptions/37354adb-7810-4360-a545-f745128ed022/resourceGroups/RG-SICIP-Prod/providers/Microsoft.Logic/workflows/sync-sicip-gesdoc-la
Trigger Run	Started	2025-05-18T00:24:57.202Z	/subscriptions/37354adb-7810-4360-a545-f745128ed022/resourcegroups/RG-SICIP-Prod/providers/Microsoft.Logic/workflows/sync-sicip-gesdoc-la/triggers/Programacion
Trigger Run	Succeeded	2025-05-18T00:24:57.905Z	/subscriptions/37354adb-7810-4360-a545-f745128ed022/resourcegroups/RG-SICIP-Prod/providers/Microsoft.Logic/workflows/sync-sicip-gesdoc-la/triggers/Programacion

Ilustración 61Trigger Run Logic_app

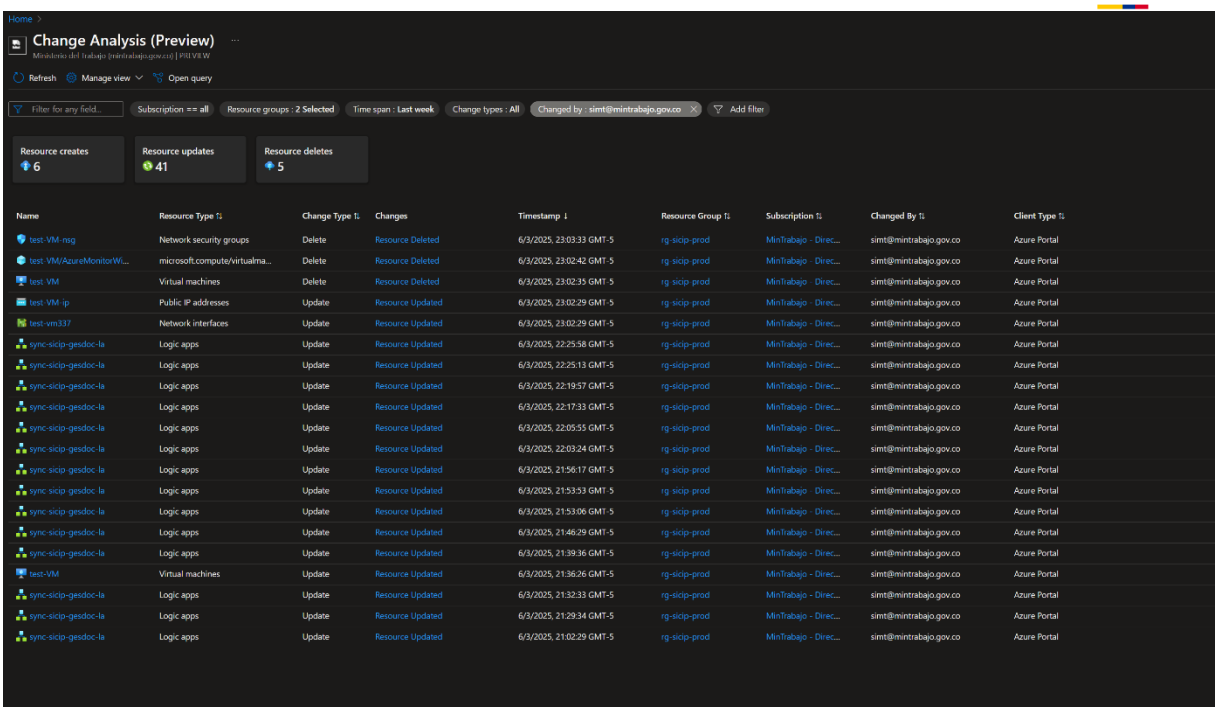


Ilustración 62 Update & delete componentes

Name	Owner	Type	Created_datetime
CORRESPONDENCIA	dbo	user table	2025-03-04 02:38:48.297

	Column_name	Type	Computed	Length	Prec	Scale	Nullable	TrimTrailingBlanks	FixedLenNullInSource	Collation
1	ID	int	no	4	10	0	no	(n/a)	(n/a)	NULL
2	VAL_ASUNTO	nvarchar	no	8000			yes	(n/a)	(n/a)	SQL_Latin1_General_CP1_CI_AS
3	FEC_RADICACION	datetime	no	8			yes	(n/a)	(n/a)	NULL
4	NRO_RADICADO	nvarchar	no	510			yes	(n/a)	(n/a)	SQL_Latin1_General_CP1_CI_AS
5	NRO_ANEXOS	int	no	4	10	0	yes	(n/a)	(n/a)	NULL
6	NRO_FOLIOS	int	no	4	10	0	yes	(n/a)	(n/a)	NULL

Identity	Seed	Increment	Not For Replication
ID	1	1	0

RowGuidCol
No rowguidcol column defined.

Data_located_on_filegroup
PRIMARY

index_name	index_description	index_keys
PK__CORRESPO__3214EC276184F668	clustered, unique, primary key	ID

constraint_type	constraint_name	delete_action	update_action	status_enabled	status_for_replication	constraint_keys
PRIMARY KEY (clustered)	PK__CORRESPO__3214EC276184F668	(n/a)	(n/a)	(n/a)	(n/a)	ID

Ilustración 63 Modificación Base de Datos productiva

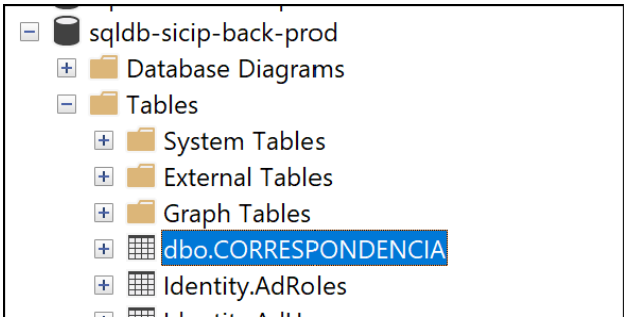


Ilustración 64 Tabla Correspondencia

Las fallas identificadas por parte del área funcional y el área de soporte informático se expondrán desde lo observado, verificado en los componentes y experiencia del usuario funcional, esto se realiza en forma cronológica desde el mes de mayo 2025 (Importante mencionar que este informe fue creado durante el mes de Junio de 2025).

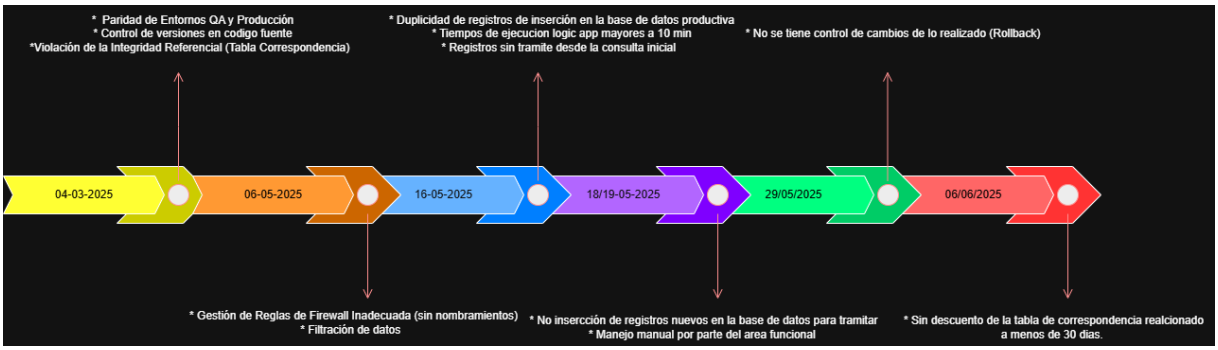


Ilustración 65 Línea del tiempo Fallas

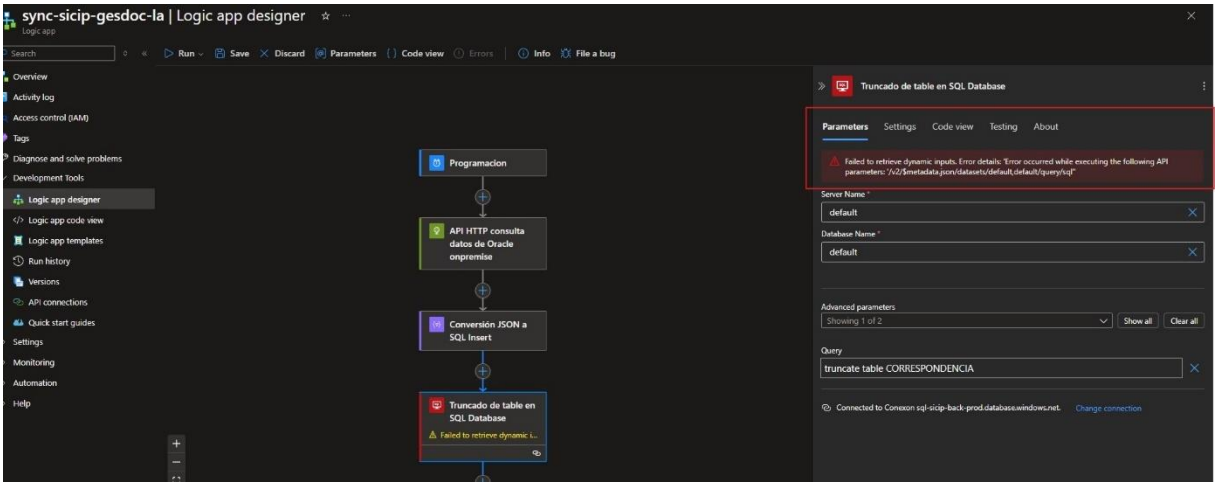


Ilustración 66 Logic App Flujo

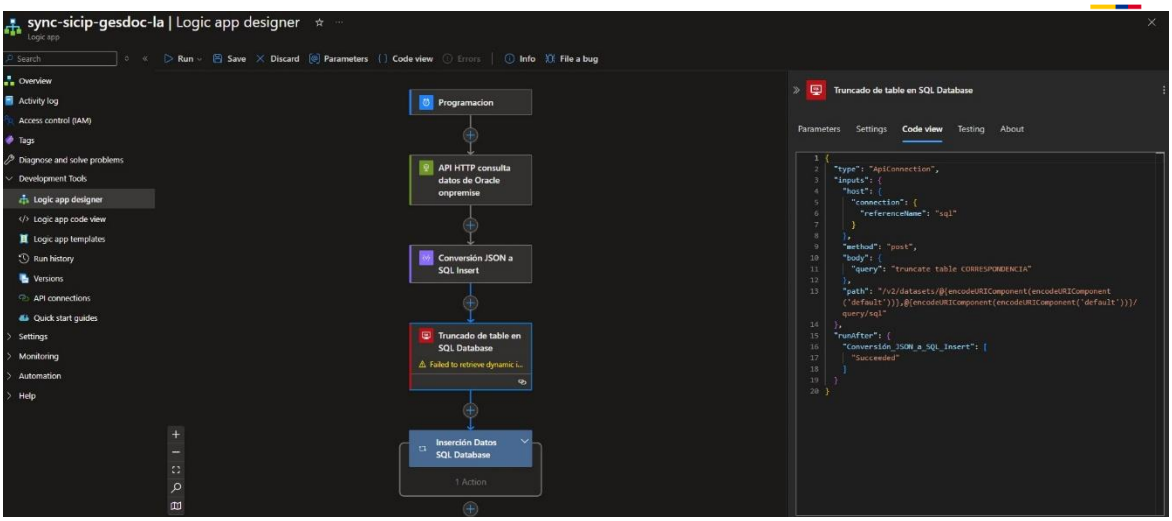


Ilustración 67 Code View Logic App

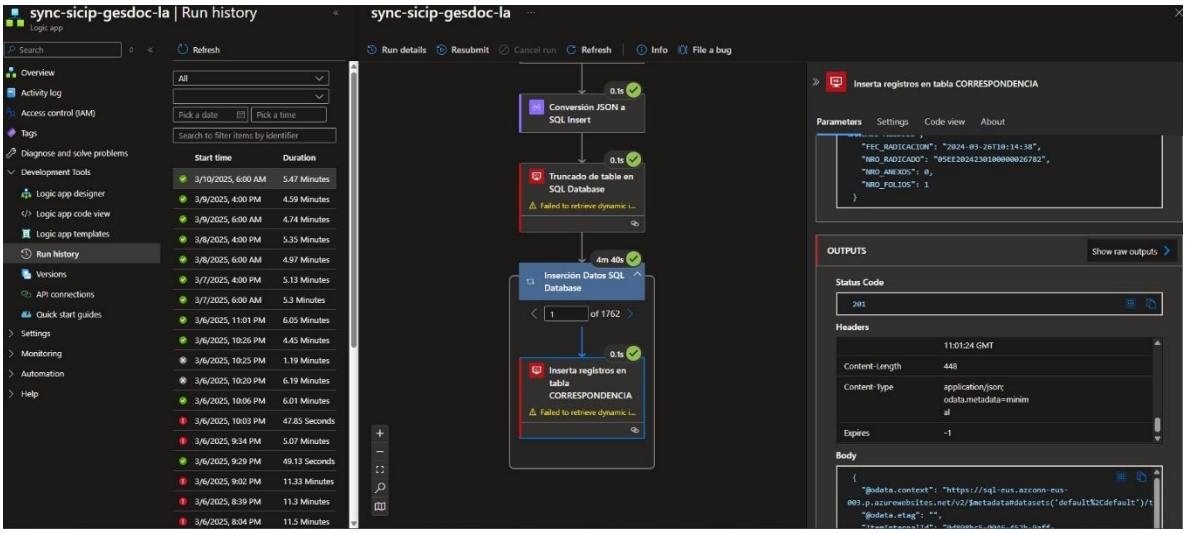


Ilustración 68 Fallas Flujo Logic App

ID	VAL_ASUNTO	FEC_RADICACION	NRO_RADICADO	NRO_ANEXOS	NRO_FOLIOS
447	CONVENIO SEGURIDAD SOCIAL - TRAMITE (COD:13...	2025-05-16 13:35:30.000	05EE2025230100000053793	0	2
1502	CONVENIO SEGURIDAD SOCIAL - TRAMITE (COD:13...	2025-05-16 13:35:30.000	05EE2025230100000053793	0	2
1833	CONVENIO SEGURIDAD SOCIAL - TRAMITE (COD:13...	2025-05-16 13:35:30.000	05EE2025230100000053793	0	2
2239	CONVENIO SEGURIDAD SOCIAL - TRAMITE (COD:13...	2025-05-16 13:35:30.000	05EE2025230100000053793	0	2
2758	CONVENIO SEGURIDAD SOCIAL - TRAMITE (COD:13...	2025-05-16 13:35:30.000	05EE2025230100000053793	0	2
2444	SOLICITUD FORMULARIO IBERO-8 LUIS ANTONIO R...	2025-05-16 12:35:55.000	11EE2025230100000053763	1	1
1909	SOLICITUD FORMULARIO IBERO-8 LUIS ANTONIO R...	2025-05-16 12:35:55.000	11EE2025230100000053763	1	1
1482	SOLICITUD FORMULARIO IBERO-8 LUIS ANTONIO R...	2025-05-16 12:35:55.000	11EE2025230100000053763	1	1
234	SOLICITUD FORMULARIO IBERO-8 LUIS ANTONIO R...	2025-05-16 12:35:55.000	11EE2025230100000053763	1	1
2786	SOLICITUD FORMULARIO IBERO-8 LUIS ANTONIO R...	2025-05-16 12:35:55.000	11EE2025230100000053763	1	1
458	LUIS ALEXANDER SOTO VELEZ PRESENTA SOLICIT...	2025-05-16 12:26:32.000	11EE2025230100000053753	0	18
1373	LUIS ALEXANDER SOTO VELEZ PRESENTA SOLICIT...	2025-05-16 12:26:32.000	11EE2025230100000053753	0	18
1746	LUIS ALEXANDER SOTO VELEZ PRESENTA SOLICIT...	2025-05-16 12:26:32.000	11EE2025230100000053753	0	18
2364	LUIS ALEXANDER SOTO VELEZ PRESENTA SOLICIT...	2025-05-16 12:26:32.000	11EE2025230100000053753	0	18
2732	LUIS ALEXANDER SOTO VELEZ PRESENTA SOLICIT...	2025-05-16 12:26:32.000	11EE2025230100000053753	0	18
2440	SOLICITUD INFORMACION SOBRE ESTADO DE RADI...	2025-05-16 12:09:11.000	11EE2025230100000053734	0	1
1955	SOLICITUD INFORMACION SOBRE ESTADO DE RADI...	2025-05-16 12:09:11.000	11EE2025230100000053734	0	1
1383	SOLICITUD INFORMACION SOBRE ESTADO DE RADI...	2025-05-16 12:09:11.000	11EE2025230100000053734	0	1
554	SOLICITUD INFORMACION SOBRE ESTADO DE RADI...	2025-05-16 12:09:11.000	11EE2025230100000053734	0	1
2819	SOLICITUD INFORMACION SOBRE ESTADO DE RADI...	2025-05-16 12:09:11.000	11EE2025230100000053734	0	1

Ilustración 69 Duplicidad de datos

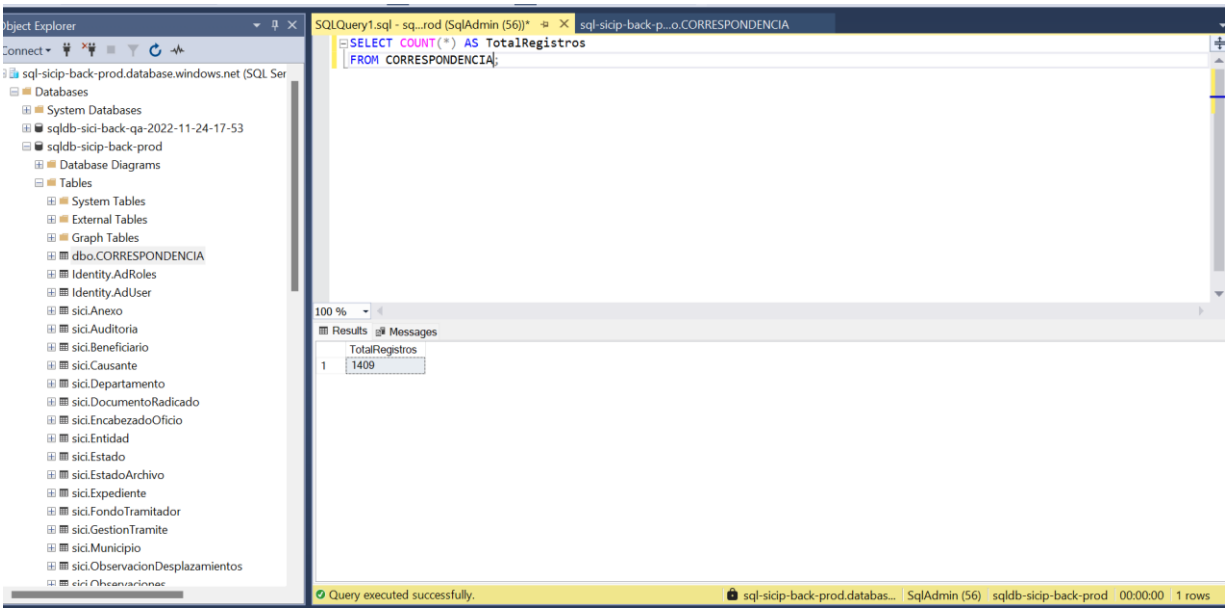


Ilustración 70 Cantidad registros

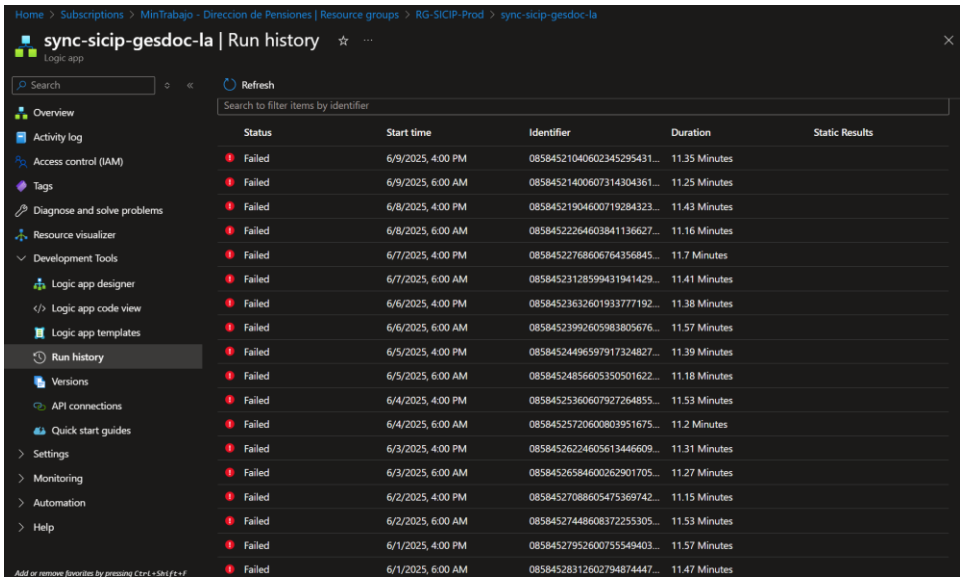


Ilustración 71 Run History

Se observa que el ambiente de pruebas está conectado directamente a la base de datos del entorno de producción, lo cual puede generar problemas en la integridad de la información misional de la entidad alojada en la base de datos, ya que las actividades de pruebas pueden generar riesgos en la pérdida o corrupción de datos, generando la posibilidad, de modificar, eliminar o sobrescribir datos reales del entorno productivo. Esto también en incumplimiento de las normativas que prohíben el uso no controlado de datos en entornos no productivos, así como la posible introducción de errores en entorno de producción.

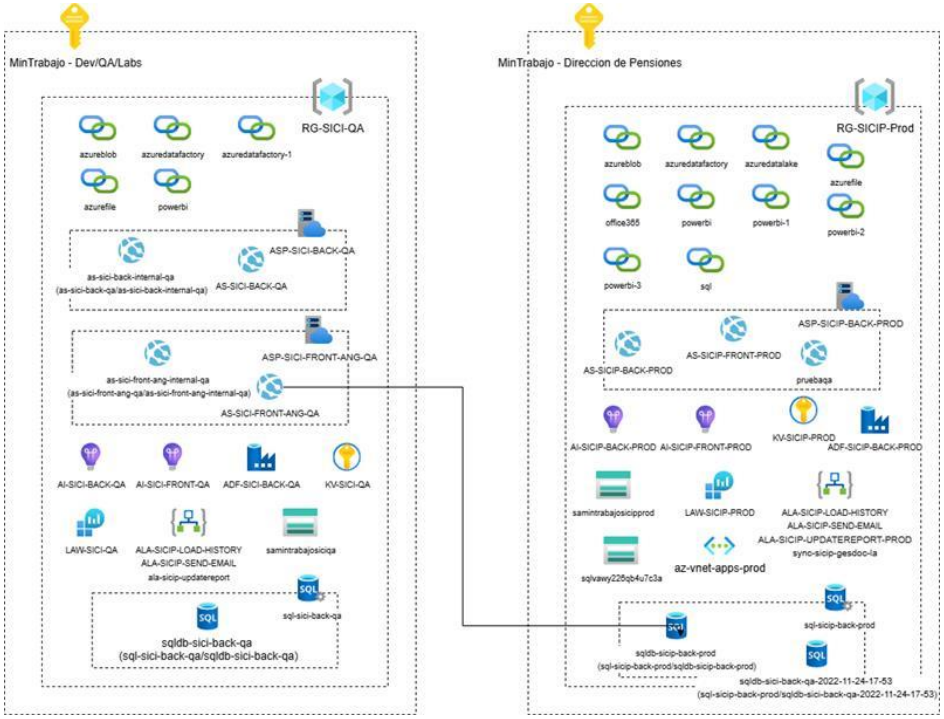


Ilustración 72 Arquitecturas componentes SICIP

Los despliegues exitosos identificados por parte del área funcional y el área de soporte informático se expondrán desde lo observado, verificado en los componentes y experiencia del usuario funcional, esto se realiza en forma cronológica desde el mes de mayo 2025 hasta el mes de junio de 2025.

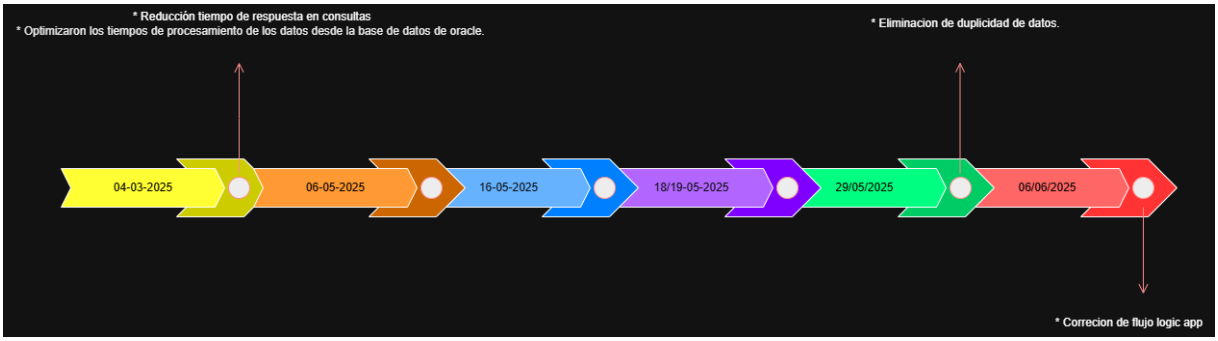


Ilustración 73 Despliegues exitosos

Es de resaltar la mejora en tiempos de respuestas en varios componentes del aplicativo a partir del primer despliegue realizado, la mejora de reducción de costos al implementar una logic app y buena práctica de consumo de datos on-premise de manera por virtual network de azure, esto mejorando tiempos de respuestas a los ciudadanos.

Tras el seguimiento a estas actividades se generan las siguientes conclusiones:

1. El no uso de una metodología estructurada de despliegue, basada en buenas prácticas DevOps y servicios nativos de Azure, no ha permitido gestionar de forma controlada y documentada los cambios en el sistema SICIP, minimizando el riesgo de fallos críticos.
2. La no automatización de procesos mediante Azure DevOps, junto con una adecuada separación de ambientes (desarrollo, pruebas, producción), no ha contribuido a una mayor trazabilidad, repetibilidad y eficiencia en las actividades de despliegue.
3. Los principales riesgos identificados durante el proceso estuvieron relacionados con fallas de configuración, integración con sistemas externos y dependencia de conocimiento centralizado en el proveedor. Estos aspectos deben ser priorizados en procesos futuros.
4. No monitoreo y diagnóstico post-despliegue, a través de herramientas como Application Insights y Azure Monitor, lo que contribuye a no detectar oportunamente errores en componentes como Logic Apps y APIs .NET.
5. Las actividades de documentación técnica y transferencia de conocimiento, aunque se han abordado parcialmente, requieren fortalecerse para garantizar sostenibilidad técnica a largo plazo dentro del equipo interno de la entidad.

Se recomienda las siguientes acciones como mejora de procesos:

1. Estandarizar el uso de pipelines CI/CD en todos los componentes del sistema, asegurando que ningún despliegue se realice de manera manual o fuera del flujo de DevOps.
2. Implementar controles de calidad en cada etapa del pipeline, incluyendo validaciones de seguridad, pruebas automatizadas y revisiones de código (code review) antes de aprobar despliegues a producción.
3. Centralizar la gestión de configuraciones y secretos utilizando Azure Key Vault y variables por entorno, evitando el uso de datos sensibles en archivos de código o configuraciones expuestas.
4. Establecer una bitácora de despliegues, actualizada por cada release, que incluya fechas, versiones, cambios aplicados, ambientes y responsables. Esto debe integrarse con Azure DevOps y mantenerse visible para los equipos de desarrollo y operación.
5. Documentar lecciones aprendidas después de cada hito de despliegue, especialmente cuando se presentan errores, para retroalimentar el proceso y prevenir recurrencias.
6. Fortalecer la formación y documentación interna, asegurando que los equipos de la entidad cuenten con manuales técnicos, diagramas de arquitectura y sesiones de capacitación sobre los componentes implementados.

6. Evaluar periódicamente los riesgos técnicos y operativos, actualizando la matriz de riesgos y ajustando las estrategias de mitigación conforme evoluciona la solución y sus dependencias.

Se hace 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.

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.

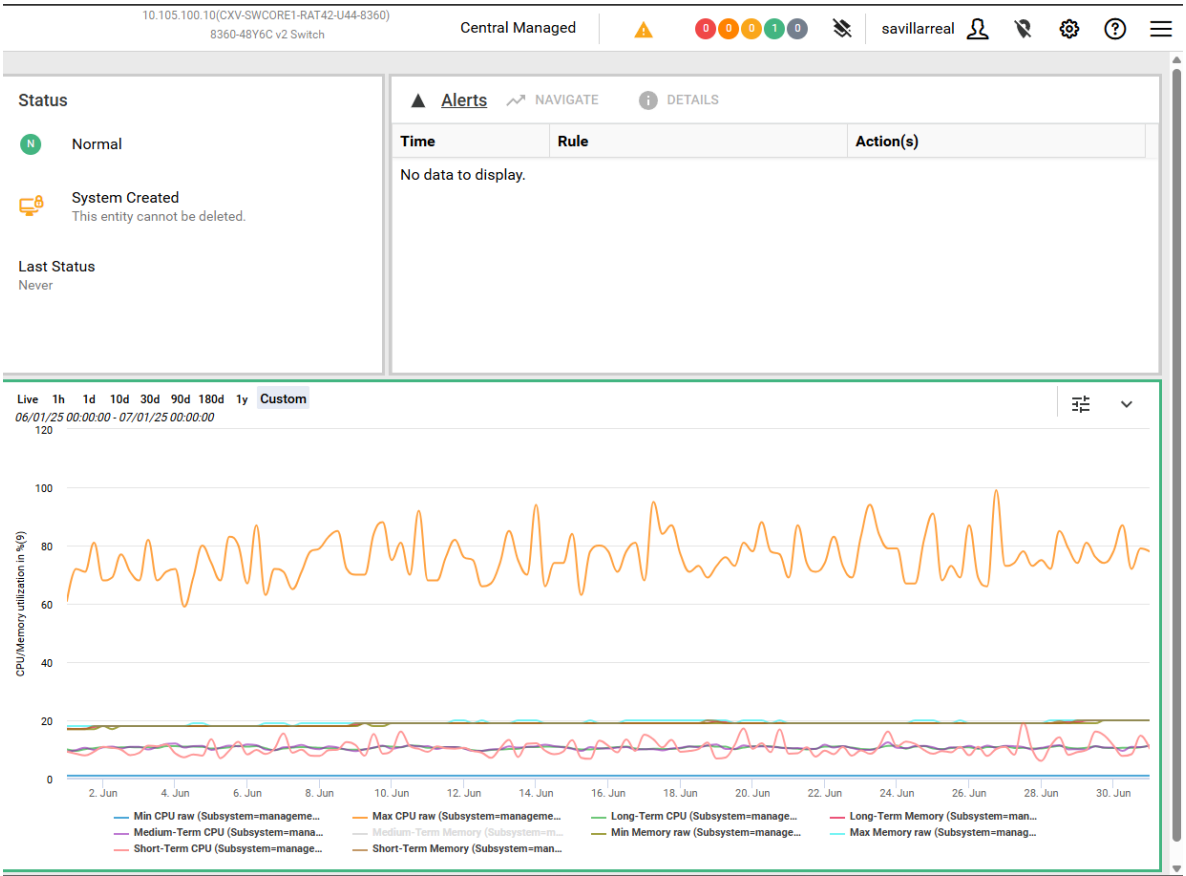


Ilustración 74 Comportamiento SWCORE Datacenter Colombia XV

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. No se observa saturación del

canal durante el mes de junio, se observa un flujo estable de tráfico, se observa que se tuvo un consumo promedio de salida de 370.44 Mbps y 491.50 Mbps de entrada

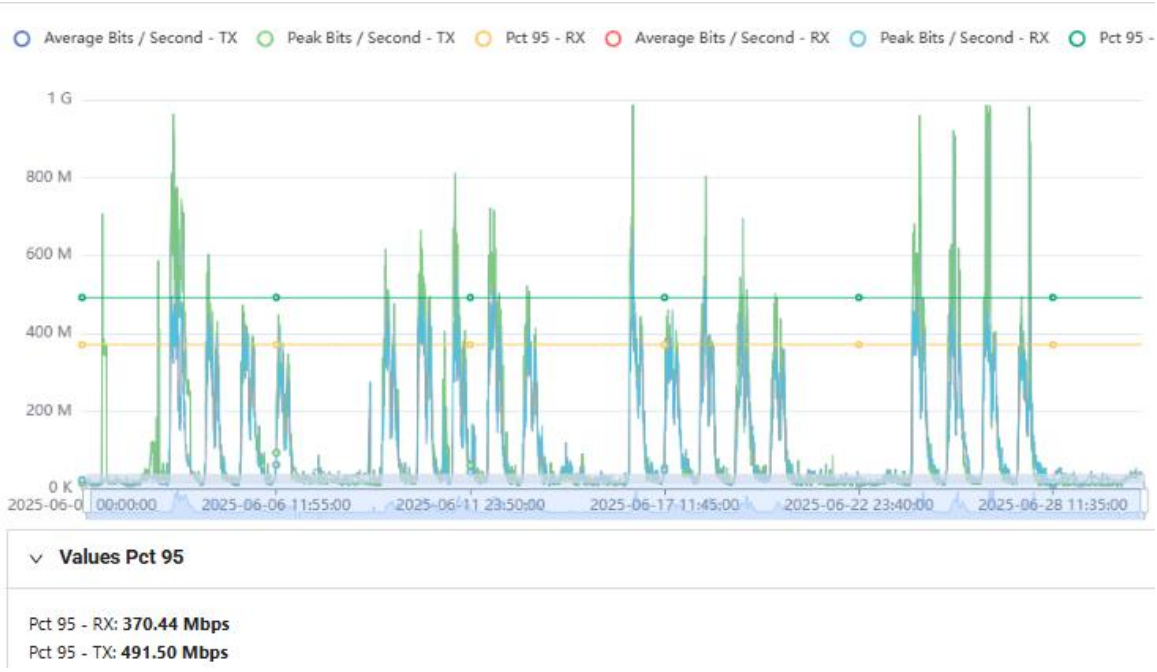


Ilustración 75. Grafica de consumo canal Internet Datacenter

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

3.1.2. Datacenter Alterno y DRP

La migración de la infraestructura se realizó con una planificación cuidadosa para minimizar el tiempo de inactividad y mitigar los riesgos. Se cuenta con la infraestructura física en sitio y el ordenamiento de los componentes tecnológicos.

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.

Durante la vigencia 2024 se realizó la identificación de servicios productivos del Ministerio del Trabajo. Esta interacción con la infraestructura tecnológica tanto física como virtualizada permitió definir diferentes frentes de servicio para replicación de esta infraestructura en el centro de datos alterno en Cirion Santa Mónica Cali. La identificación de estos servicios se ha plasmado en el siguiente diagrama de interoperabilidad del centro de datos principal.

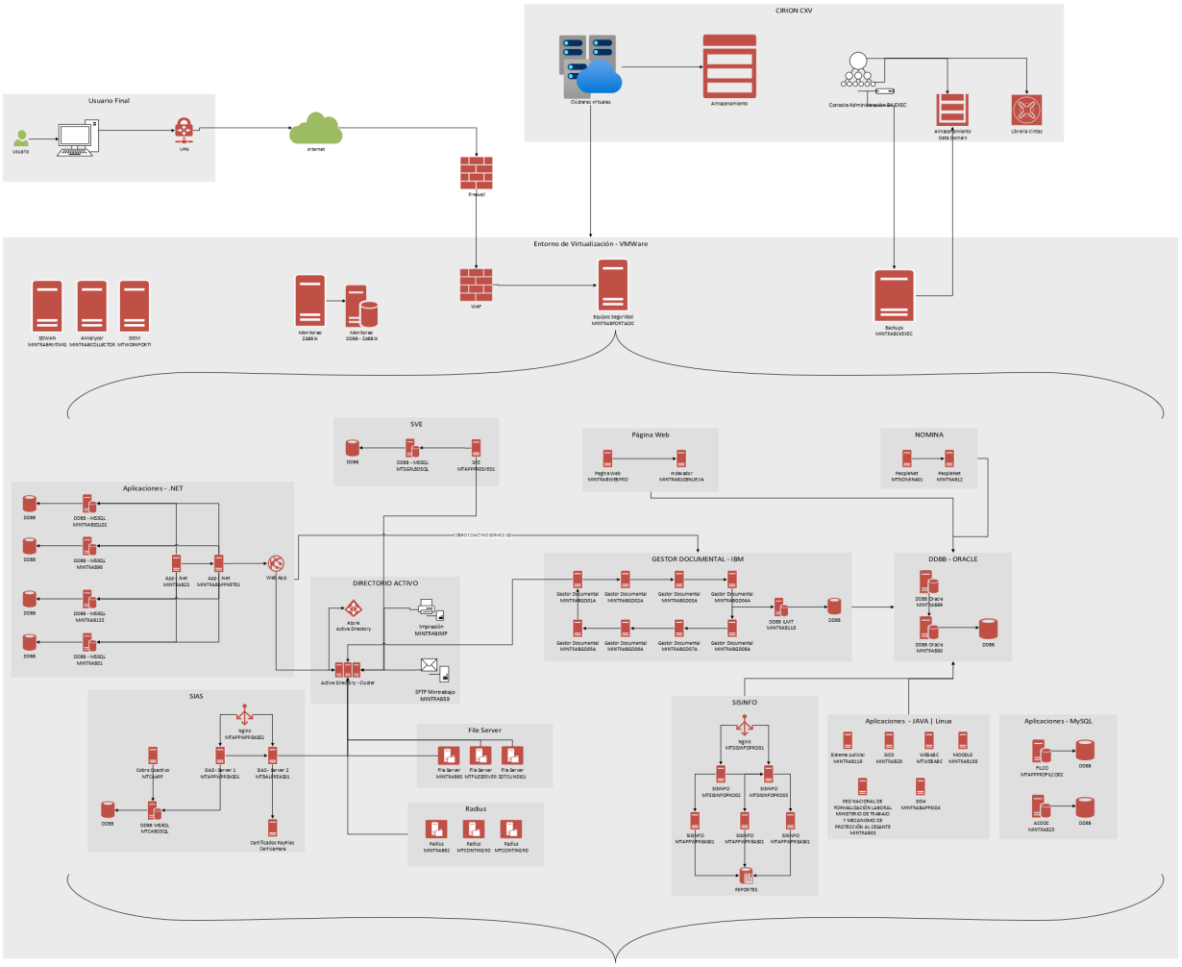
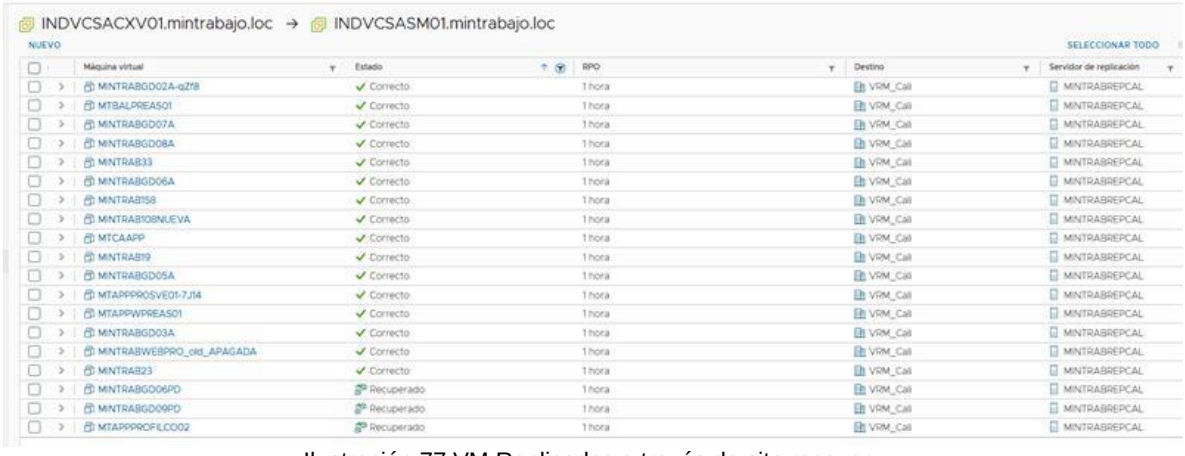


Ilustración 76 Diagrama Interoperabilidad Bogotá CXV

A nivel de las máquinas virtuales replicadas se visualizan las siguientes VM:



INDVCSACXV01.mintrabajo.loc → INDVCSASM01.mintrabajo.loc

NUEVO | SELECCIONAR TODO

Máquina virtual	Estado	RPO	Destino	Servidor de replicación
MINTRABGD02A-qZf8	Correcto	1 hora	VRM_Cali	MINTRABREPCAL
MTBALPREAS01	Correcto	1 hora	VRM_Cali	MINTRABREPCAL
MINTRABGD07A	Correcto	1 hora	VRM_Cali	MINTRABREPCAL
MINTRABGD08A	Correcto	1 hora	VRM_Cali	MINTRABREPCAL
MINTRAB33	Correcto	1 hora	VRM_Cali	MINTRABREPCAL
MINTRABGD06A	Correcto	1 hora	VRM_Cali	MINTRABREPCAL
MINTRAB158	Correcto	1 hora	VRM_Cali	MINTRABREPCAL
MINTRAB108NUEVA	Correcto	1 hora	VRM_Cali	MINTRABREPCAL
MTCAAPP	Correcto	1 hora	VRM_Cali	MINTRABREPCAL
MINTRAB119	Correcto	1 hora	VRM_Cali	MINTRABREPCAL
MINTRABGD05A	Correcto	1 hora	VRM_Cali	MINTRABREPCAL
MTAPPPROSVE01-7J14	Correcto	1 hora	VRM_Cali	MINTRABREPCAL
MTAPPWPREAS01	Correcto	1 hora	VRM_Cali	MINTRABREPCAL
MINTRABGD03A	Correcto	1 hora	VRM_Cali	MINTRABREPCAL
MINTRABWEBPRO_old_APAGADA	Correcto	1 hora	VRM_Cali	MINTRABREPCAL
MINTRAB23	Correcto	1 hora	VRM_Cali	MINTRABREPCAL
MINTRABGD06PD	Recuperado	1 hora	VRM_Cali	MINTRABREPCAL
MINTRABGD09PD	Recuperado	1 hora	VRM_Cali	MINTRABREPCAL
MTAPPPROFILCOO2	Recuperado	1 hora	VRM_Cali	MINTRABREPCAL

Ilustración 77 VM Replicadas a través de site recovery

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.

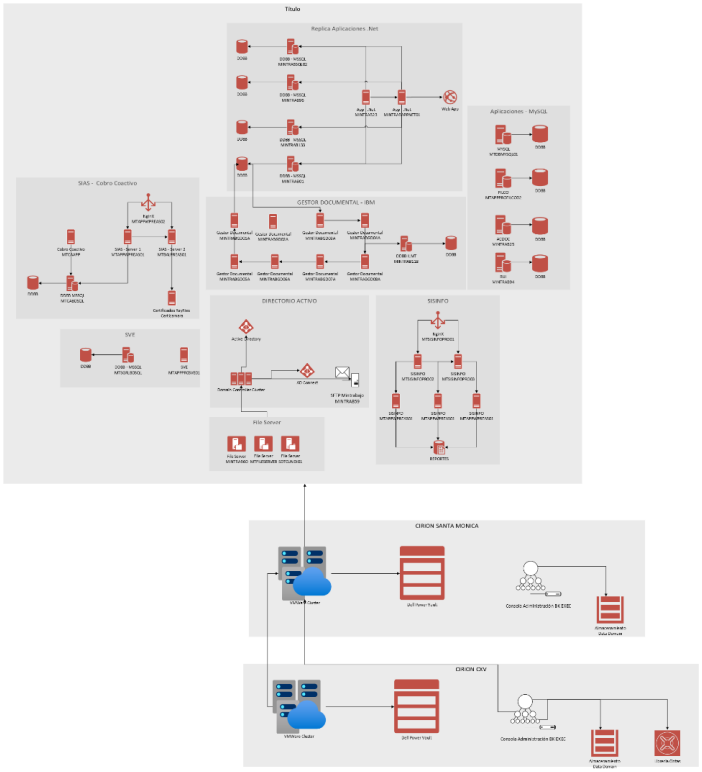


Ilustración 78 Diagrama de Replicación CXV - Santa Mónica

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 tuvo un tráfico promedio de recepción de 336.42Mbps y de transmisión de 9.76Mbps.



Ilustración *79* Puerto de conexión extremo Bogotá

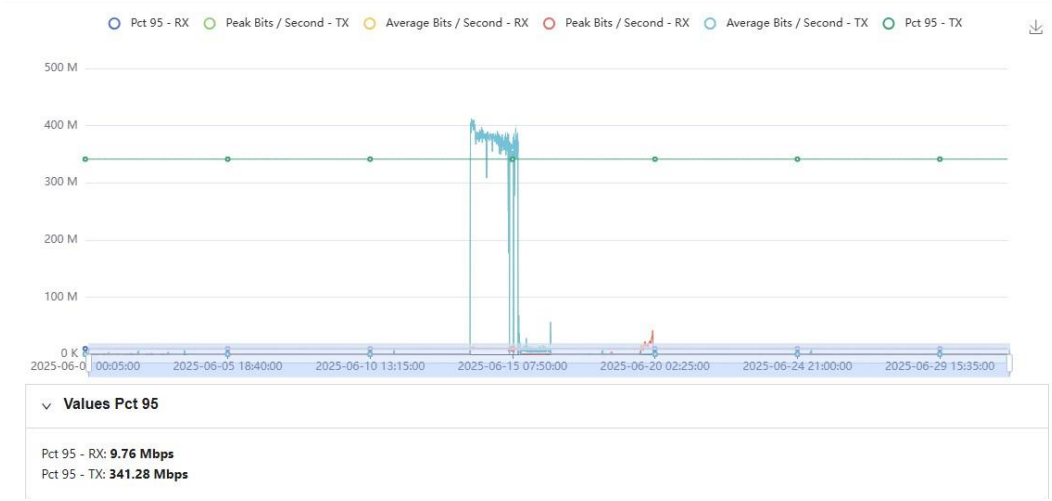


Ilustración *80* Puerto de conexión extremo Cali

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 que se tiene un consumo promedio de recepción de 240Kbps y de transmisión de 390 Kbps.

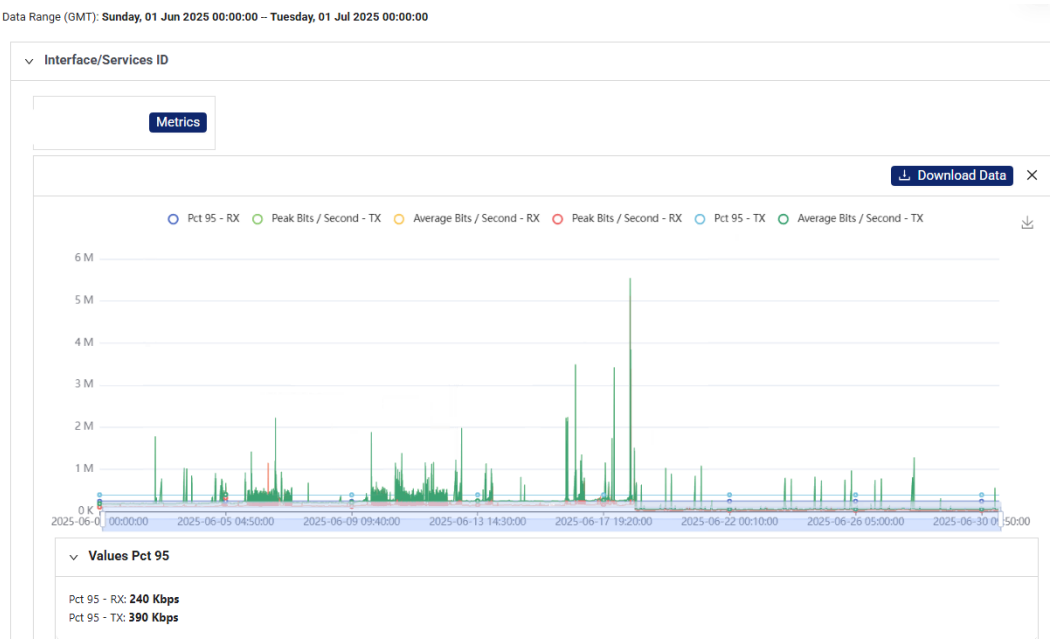


Ilustración *81* Estado canal de Internet DC Cali

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

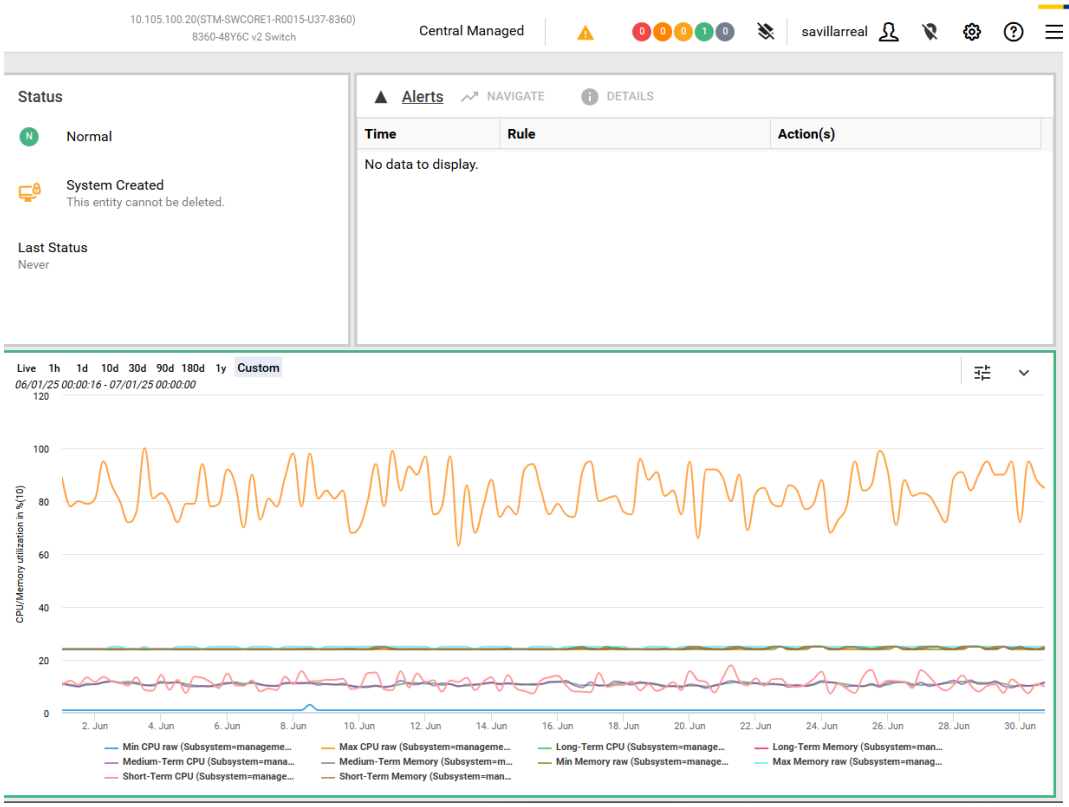


Ilustración 82 Estado SWCORE Datacenter alterno

3.1.3. 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. 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.
- 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.

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.

Con respecto al crecimiento de la aplicación Moodle se hacen las siguientes anotaciones, las características actuales del Moodle de la entidad:

Infraestructura actual
Servidor Aplicación

- vCPU: 4
- RAM: 12 GB
- Almacenamiento: 100 GB
- Sistema Operativo: Ubuntu Linux

Servidor DDBB

- vCPU: 8
- RAM: 18 GB
- Almacenamiento: 113 GB consumidos por MySQL
- Motor DDBB: MySQL
- Sistema Operativo: Windows Server
    - Importante: El server aloja la aplicación ACDOC y su DDBB – De igual forma las DDBB de Moodle y otros entornos de pruebas
- Las bases de datos de Moodle pesan:
    - Producción: 1.4 GB
    - Desarrollo y Pruebas: 2 MB cada una

Esto se escala a la Oficina TIC para validación de si cumple con los estándares mínimos definidos para desarrollo o recepción de aplicaciones en el Ministerio de Trabajo.

Tras solicitud de las áreas se realiza aprovisionamiento de servidor para Moodle nuevo con las siguientes características:

vCPU: 2
Memoria RAM: 8 GB
Almacenamiento 256 GB

El área de riesgos laborales realiza una solicitud para un ambiente de desarrollo para la construcción de una aplicación de Gestión de prevención de accidentes mayores, bajo esta premisa remite un

memorando 08SI2025310500000004084 con las especificaciones técnicas para un **AMBIENTE DE DESARROLLO**, en contestación a la solicitud se da el siguiente contexto para el aprovisionamiento de cualquier sistema de información se deben tener en cuenta los siguientes aspectos para soportar el aprovisionamiento de componentes en la nube privada de la entidad, en primera instancia, en cumplimiento de las políticas definidas por la Oficina de Tecnologías de la Información y en segunda instancia en relación a los componentes que interoperaran para que el sistema de información funcione de manera adecuada, esto teniendo en cuenta que esta tiene unas capacidades definidas y limitadas contractualmente. Para ello se requiere la siguiente información:

- Documento de Arquitectura de Solución y de Software del Sistema de Información desarrollado y/o aplicativo, alcance del sistema de información y/o aplicativo (descripción jerárquica, diagrama de módulos, descripción individual de módulos, dependencias externas, licenciamiento y certificados digitales necesarios).
- Diagrama de arquitectura e interoperabilidad y diagramas de ambientes de pruebas, desarrollo, preproducción con otros sistemas de información y/o aplicativos.
- Documento de arquitectura de la base de datos y diseño de modelo de datos.
- Manual de despliegue del sistema de información y/o aplicativo.
- Manuales técnicos y de Operación de las funcionalidades del sistema de información y/o aplicativo.

Con esta claridad se da una respuesta para cada ítem indicado por el área solicitante:

- Servidor de Base de Datos
    - Almacenamiento de 6 TB → Se requiere se envíe documento de arquitectura donde se pueda visualizar la justificación técnica para la asignación del almacenamiento, si hará uso de un servidor ya aprovisionado o si requiere de un servidor independiente para este fin. Esta en revisión y aprobación por parte de la coordinación de Soporte informático.
    - RAM 128 GB → Se requiere se envíe documento de arquitectura donde se pueda visualizar la justificación técnica para la asignación de memoria, si hará uso de un servidor ya aprovisionado o si requiere de un servidor independiente para este fin. Esto teniendo en cuenta que en la actualidad el único servidor de SQL Server que super las 100 GB de RAM soporta más de 20 bases de datos.
    - Procesador 8 Cores → Se requiere se envíe documento de arquitectura donde se pueda visualizar la justificación técnica para la asignación del almacenamiento, si hará uso de un servidor ya aprovisionado o si requiere de un servidor independiente para este fin. Se debe indicar los vCPU que se requiere asignar ya que es la métrica usada para creación de máquinas virtuales en la nube privada.
    - Windows Server 2022 → Se cuenta con licenciamiento disponible.
    - Microsoft SQL Server 2022 → Todas las licencias de este componente ya se encuentran asignadas en entornos productivos, para creación de un servidor nuevo o ampliación de uno ya existente se requeriría adquirir un licenciamiento de acuerdo con los cores de SQL en este caso se debe adquirir una licencia de 8 Cores para SQL Server 2022.

- Servidor Backend
    - Almacenamiento de 2TB → Se requiere se envíe documento de arquitectura donde se pueda visualizar la justificación técnica para la asignación del almacenamiento, si hará uso de un servidor ya aprovisionado o si requiere de un servidor independiente para este fin.
    - Memoria RAM de 256 GB → Se requiere se envíe documento de arquitectura donde se pueda visualizar la justificación técnica para la asignación del almacenamiento, si hará uso de un servidor ya aprovisionado o si requiere de un servidor independiente para este fin. Es importante mencionar que la entidad solo cuenta con 4 servidores con más de 100 GB de RAM asignadas y están asociados a

SISINFO por su carga transaccional, un servidor del gestor documental por su alto consumo de capacidades y un servidor de SQL que aloja

- Procesador de 16 cores → Se requiere se envíe documento de arquitectura donde se pueda visualizar la justificación técnica para la asignación del almacenamiento, si hará uso de un servidor ya aprovisionado o si requiere de un servidor independiente para este fin. Se debe indicar los vCPU que se requiere asignar ya que es la métrica usada para creación de máquinas virtuales en la nube privada.
- Windows Server 2022 → Se cuenta con licenciamiento disponible.

- Servidor FronEnd
  - Almacenamiento de 2TB → Se requiere se envíe documento de arquitectura donde se pueda visualizar la justificación técnica para la asignación del almacenamiento, si hará uso de un servidor ya aprovisionado o si requiere de un servidor independiente para este fin.
  - Memoria RAM de 128 GB → Se requiere se envíe documento de arquitectura donde se pueda visualizar la justificación técnica para la asignación del almacenamiento, si hará uso de un servidor ya aprovisionado o si requiere de un servidor independiente para este fin. Es importante mencionar que la entidad solo cuenta con 4 servidores con más de 100 GB de RAM asignadas y están asociados a SISINFO por su carga transaccional, un servidor del gestor documental por su alto consumo de capacidades y un servidor de SQL que aloja más de 20 bases de datos.
  - Procesador de 8 Cores → Se requiere se envíe documento de arquitectura donde se pueda visualizar la justificación técnica para la asignación del almacenamiento, si hará uso de un servidor ya aprovisionado o si requiere de un servidor independiente para este fin. Se debe indicar los vCPU que se requiere asignar ya que es la métrica usada para creación de máquinas virtuales en la nube privada.
  - Windows Server 2022 → Se cuenta con licenciamiento disponible.

En total la solución consumiría las siguientes capacidades:

- 10 TB de almacenamiento
- 512 GB de RAM
- 32 Cores

Para contrastar, toda la solución del gestor documental el sistema de información más robusto que tiene el Ministerio a nivel de capacidades, incluidos servidores de pruebas pesan alrededor de 10 TB distribuidos en más de 10 servidores y no llega a consumir 500 GB de RAM, sin contar con las capacidades asignadas para la capa de base de datos, únicamente contabilizando los servidores de aplicación, sin las bases de datos que tienen una carga mucho más elevada. Bajo esta premisa, recomendamos hacer un ejercicio de gestión de capacidades mucho más profundo y detallado, esto con el fin de asignar las capacidades estrictamente necesarias para que el sistema de información pueda funcionar de manera adecuada, con holgura de crecimiento de 15%-20% pero sin subutilizar los recursos contratados por la entidad, ya que este escenario provoca un desbalance en lo contratado por la entidad y no se aprovecharían de manera adecuada las capacidades de la Infraestructura tecnológica de la entidad. Bajo el escenario actual donde la entidad ha consumido más del 90% de sus capacidades de nube privada contratadas, se deben validar escenarios de crecimiento de la nube privada para poder atender este tipo de requerimientos de las áreas funcionales. Ala fecha se comunicó de manera formal tanto a la coordinación de Riesgos Laborales y a la Oficina de Tecnologías de la Información de la mano de la Coordinación de Soporte Informático que el escenario actual de la nube privada no permitía soportar las capacidades solicitadas para recepcionar las 6 TB de información entre Parquet y DDBB SQL Server.

3.1.4. Aplicaciones Especializadas

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

Se identificaron diversas aplicaciones que durante los procesos de afinamiento generaron indisponibilidad, pero no generaron un incremento o reporte de requerimientos de servicio e incidencias, este comportamiento permite identificar qué tipo de aplicaciones se encuentran aprovisionadas, pero sin administración funcional lo cual dentro de los procesos de re dimensionamiento de aplicaciones e infraestructura virtualizada permiten una optimización de los recursos asignados a las aplicaciones que realmente requieren capacidades superiores para un correcto funcionamiento en ambientes productivos.

Se observaron escenarios en donde 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.

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 Coordinadora 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.

De igual forma se ejecutaron diferentes controles de cambios, relacionados con sistemas de información como lo es SIRITI la cual se ha convertido en una de las aplicaciones que más controles de cambios presenta durante el mes en comparación con las demás aplicaciones en JAVA o componente .Net. Se propuso la independización del aplicativo SIRITI del servidor MINTRAB13 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.

De acuerdo con este contexto se solicita al área funcional un dimensionamiento a nivel de capacidades requeridas para realizar aprovisionamiento de un servidor de pruebas y comenzar con pruebas de funcionamiento del sistema de información en un nuevo servidor de aplicación con un sistema operativo actualizado y componentes .Net de última actualización, esto con el fin de poder garantizar una correcta migración del ambiente de producción. Actualmente el servidor de aplicación para entorno de pruebas fue aprovisionado y se está a espera de agendamiento de sesión con área funcional.

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

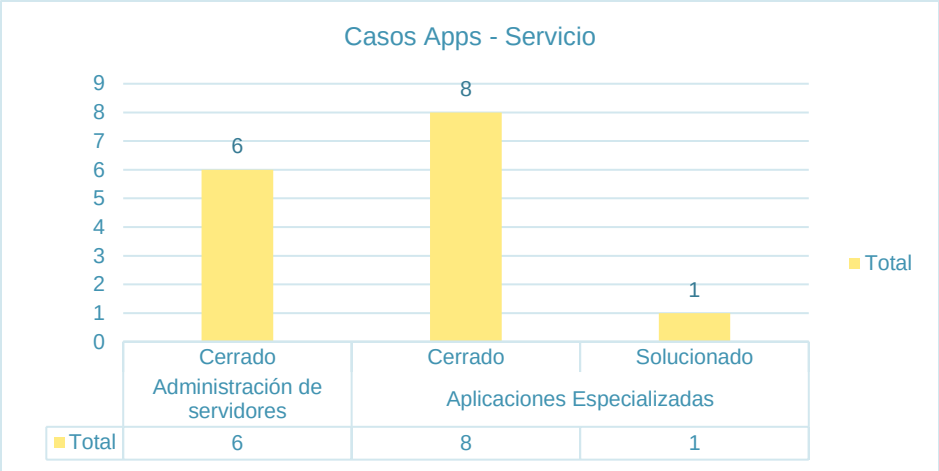


Ilustración *83* Estado final de casos – Aplicaciones Especializadas

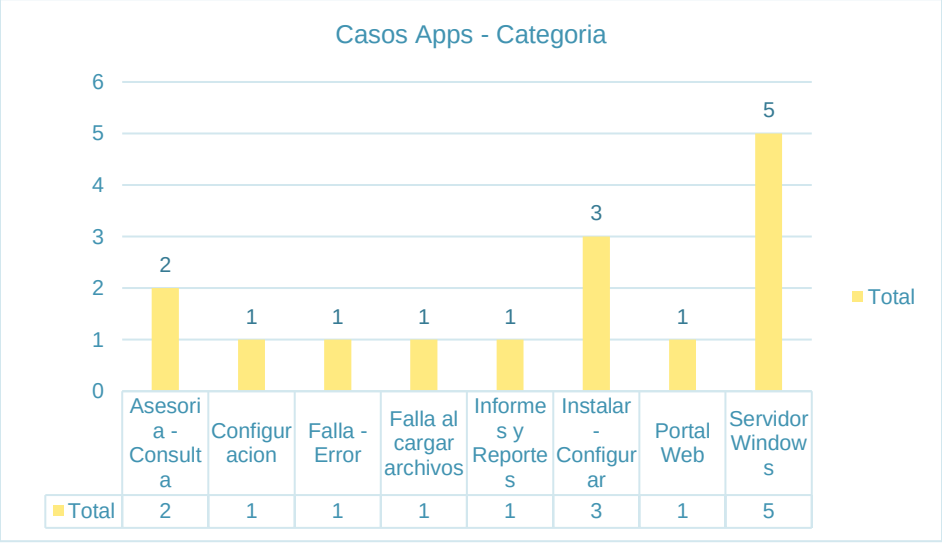


Ilustración 84 categorías Apps

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

- **Escenario SIAS**:

Se dio contexto del escenario de seguridad, las actividades realizadas de forma proactiva para prevenir que la vulneración se propagara y las acciones para poner en disponibilidad nuevamente la aplicación:

- A corto plazo se realizó la subida de servicios únicamente para la red interna del ministerio y dejando en funcionamiento únicamente uno de los servidores de FrontEnd y sin acceso desde internet a la aplicación. Actualmente la aplicación funciona de esta forma.
- A largo plazo el área IVC encargada de los desarrollos y actualizaciones a nivel de software se compromete de realizar las validaciones correspondientes para mitigar las vulnerabilidades reportadas a nivel de aplicación para que el código posea estas acciones de mejora.

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.
- Entrega de sistema de información SIAS refactorizado el cual tienen presupuestado probar y poner en producción durante el mes de Julio.

- **Escenario FILCO**:

Se dio contexto de todo el escenario de seguridad, las acciones, dependencias técnicas y las razones por las cuales se tomaron las decisiones técnicas para dar de baja el servicio y salvaguardar la información y activos tecnológicos de la entidad alojados en nube privada.

- La aplicación FILCO fue aprovisionada sin visto bueno de la Oficina de TIC, desarrollada fuera de los lineamientos definidos por la misma Oficina TIC.
    - Sitio desarrollado en WordPress, con bases de datos Postgress y componentes como DSpace para gestión de contenidos documentales.
- Tras la vulneración se tomó la decisión de dar de baja el servidor de aplicación ya que podría presentarse una propagación en servidores de la misma red virtual.
- La baja de servicios fue realizada no por una identificación de una vulnerabilidad si no por una explotación de una vulnerabilidad.

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 Pagina Web de la entidad y que es administrado actualmente por el área de Empleo.

- **Escenario RUI**:

Se dio contexto del escenario de vulnerabilidades de la aplicación y el servidor virtual, se dejó en indisponibilidad controlada esta infraestructura virtualizada mientras se realizaba validación con el equipo técnico y funcional el correcto proceder. Tras la sesión se definieron los siguientes compromisos:

- Poner en disponibilidad la aplicación únicamente dentro de la red interna del Ministerio del trabajo para que los funcionarios y contratistas de riesgos laborales pudieran acceder a la aplicación.
- Se define flujo de creación de usuarios para los intermediarios de la siguiente manera:
    - Recepción de solicitud de creación de usuario en Riesgos Laborales

- Reenvió de solicitud a la mesa de servicios por parte de riesgos laborales
- Creación de usuario en directorio activo con el perfil de VPN respectivamente
- Envío de información (usuario y contraseña) a riesgos laborales en un medio cifrado. Es importante mencionar que esta metodología siempre se ha venido trabajando para la creación de usuarios y envío de información sensible de acuerdo con la ODI Política de Gestión de Contraseñas del Ministerio del Trabajo ítems 2.5.7 y 2.5.8 indica:
  - "El administrador de cada sistema es responsable de asegurar que las contraseñas que se transmitan a través de redes públicas estén protegidas contra acceso no autorizado mientras se encuentren en tránsito, para este caso se recomienda sean cifradas."
  - "El usuario es responsable de asegurar la privacidad de las contraseñas asignadas para acceder a los sistemas de información."
  - Por ende, toda Contraseña, independientemente de su origen o su propósito, debe ser compartida en un medio seguro y cifrado para garantizar la seguridad de acceso.
- Se realiza despliegue de ambiente de contingencia de RUI, tras una serie de sesiones técnicas con riesgos laborales.
  - Se observa falta de pruebas funcionales por parte del área responsable ya que, tras dar el visto bueno de salida a producción, se observaron diversos errores que desencadenaron ajustes a nivel de código por parte del equipo técnico de riesgos laborales en producción.
- Actualmente las actividades de creación de usuario fueron suspendidas tras la implementación del ambiente de contingencia de RUI.
- Se esta a espera de avances por parte del equipo técnico de Riesgos Laborales relacionado con la implementación del nuevo RUI.

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.

Nombre App	Acceso actual	Funcionario	Observaciones
Biblioteca Virtual de Trabajo	http://app2.mintrabajo.gov.co/Biblioteca	Javier Mauricio Gomez Mantilla	
Centros de entrenamiento	http://app2.mintrabajo.gov.co/centrosentrenamiento/	Carlos Andres Matañana	
Calculadora Laboral	http://app2.mintrabajo.gov.co/CalculadoraLaboral	Ligia Carrero	
Censo Sindical	http://app2.mintrabajo.gov.co/CensoSindical	Maria Jimena Daza	
conjovenes	http://app2.mintrabajo.gov.co/conjovenes	No Se Cuenta Con Información	No se cuenta con aprobación formal para desaprovisionar por parte del área funcional
FTTrabajo	http://app2.mintrabajo.gov.co/Ftrabajo	Carlos Andres Matañana	
FTRUE	http://app2.mintrabajo.gov.co/FTRUE	Carlos Andres Matañana	

Nombre App	Acceso actual	Funcionario	Observaciones
FTTalentosEmpleo	http://app2.mintrabajo.gov.co/FTTalentosEmpleo	Carlos Andres Matañana	
Min Trabajo PRIEV	http://app2.mintrabajo.gov.co/MintrabajoPRIEV	No Se Cuenta Con Información	
SIG	http://app2.mintrabajo.gov.co/SIG	No Se Cuenta Con Información	No se cuenta con aprobación formal para desaprovisionar por parte del área funcional
SIRITI	http://app2.mintrabajo.gov.co/siriti	Magnolia Del Socorro Agudelo Velasquez - Leonor Sepulveda Carvajal	
Tmigrante	http://app2.mintrabajo.gov.co/Tmigrante	Carlos Andres Matañana	
Cobro	http://app2.mintrabajo.gov.co/cobro	Soraya Eudoxia Pino Canosa - Fabian Camilo Oviedo	
Tesoreria	http://app2.mintrabajo.gov.co/tesoreria/	Maria Patricia Mosquera Jurado - Deisy Johana Cruz	
Correspondencia (MELBA)	http://app2.mintrabajo.gov.co/Correspondencia/inicio.aspx	Diana Rocio Castiblanco Villate	Se contaba con VB de inactivación, pero por solicitud se tuvo que dar de alta nuevamente
PEPFF	http://app2.mintrabajo.gov.co/pepff	No Se Cuenta Con Información	
Auxilio - Subsidio	http://app2.mintrabajo.gov.co:444/	Jessica Tatiana Garcia Renza	
SFT	http://app2.mintrabajo.gov.co/sft/	Ligia Carrero	
SaberHacerVale	http://app2.mintrabajo.gov.co/saberhacervale/	No Se Cuenta Con Información	No se cuenta con aprobación formal para desaprovisionar por parte del área funcional y actualmente está productiva
Estado joven	http://app2.mintrabajo.gov.co/estadojoven/	Carlos Andres Matañana	
FTRUTEC	http://app2.mintrabajo.gov.co/ftrutec/	Carlos Andres Matañana	

Tabla 58 Migración actividades .NET

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.

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.

De igual forma se comunica que la información de plan de trabajo reposa en el SharePoint del contrato, dentro de la carpeta de Aplicaciones de acuerdo con lo solicitado, el plan de trabajo enmarca las actividades globales para la migración de la totalidad de las aplicaciones. Posterior a brindar esta información, se procede con el agendamiento de sesiones con cada área responsable y se programan inicio de pruebas en nuevos entornos las últimas dos semanas de febrero y la primera semana de marzo de 2025. A la fecha no se ha recibido retroalimentación de las pruebas por las áreas funcionales, es importante dejar claridad que, a nivel de infraestructura y configuración, ya se encuentran aprovisionados y listos los entornos, pero no se puede iniciar migración sin VB de la propia entidad.

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

Las aplicaciones restantes se encuentran en fase de pruebas para migración en los siguientes meses julio y agosto de 2025. A espera de envío de nueva versión de SIASla cual se desplegará en Julio de 2025 según lo informado por el área de IVC.

Migración Portal Web

- Se revisaron las conexiones desde el servidor del Portal hacia el servidor LDAP y estas respondieron de forma exitosa.
- Se realizó sesión con el Ing. Elkin Morales para revisar el servidor LDAP y probar las conexiones.
- Se revisaron los logs de servidor del portal y se encuentra que reportaba: ERROR [http-nio-443-exec-54][LDAPAuth:430] Problem accessing LDAP server java.lang.NullPointerException

Esto ocurre cuando un usuario quiere ingresar a un sitio privado como es la intranet, el portal hace la petición al servidor LDAP pero no hay acceso.

Como las conexiones configuradas desde el portal responden de forma exitosa, se procede a ejecutar el proceso de importación de usuarios desde el servidor LDAP hacia el servidor del portal. Este proceso se ejecuta en segundo plano y se reportan los usuarios que no se pueden importar porque no cumplen algún criterio de los campos que no pueden ser null para Liferay, ej: cuentas de servicio, cuentas de usuario que no tiene email, etc.
Con la ejecución del proceso se pueden ver en el log errores de cuentas que no puede importar porque no cumplen con algún criterio.

Se realizaron pruebas donde se generó un error de no cumplir con el criterio de email, así como de otros usuarios que se les solicito probar. Se le solicito al Ing. Elkin Morales que realizara el ajuste a mi cuenta desde el servidor LDAP agregándole mi correo min trabajo para probar y efectivamente una vez actualizada ya no genera error puedo ingresar, pero no tengo permisos sobre la intranet.
Realizado lo anterior se solicitó al usuario del requerimiento validar que efectivamente pueda ingresar a la intranet, se espera su respuesta.
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 7.2 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 proyecta paso a producción de las últimas versiones mencionadas en julio de 2025.

GESTOR DOCUMENTAL

A nivel de mantenimientos del gestor documental no se realizaron actividades técnicas de mantenimiento en el marco de proceso de afinamiento y optimización, esto de acuerdo con la solicitud de aplazamiento por parte de la entidad, sin embargo, se siguen plasmando como evidencia los siguientes procedimientos, ya que esta actividad no varía mensualmente y es importante dejar plasmado el procedimiento:

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.

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.

Tiempos de respuesta elevados por la concurrencia en consultas (Componente BD). A continuación, se presentan las respectivas estadísticas referentes al mes de febrero de 2025 sobre las 2 instancias de la base de datos MINTRASG en la cual se puede observar un repetido comportamiento de concurrencia sobre el objeto tabla BPMDBA.LSW_TASK.

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.

Número de instancias antes de Mantenimiento:
• Convención: • Instancias Activas: 1 • Instancias Completadas: 2 • Instancias Error: 3 • Instancias Terminadas: 4

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 no están en valores de alerta 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.

Se validó estado de servidor y base de datos operativas antes de realizar la ventana de mantenimiento. Esta actividad se realiza una vez al mes ejecutando las siguientes actividades:

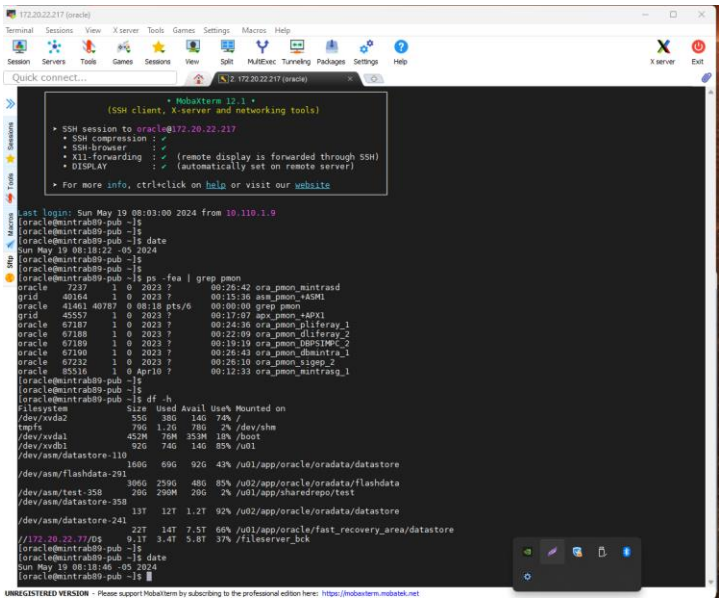


Ilustración 85 Estado pre-ventana

- **Validación de backups de base de datos.**

Antes de ejecutar el mantenimiento se deben garantizar los backups para respaldar la actividad frente a una falla en el proceso.
BACKUP FULL RMAN
BACKUP DATAPUMP (EXPDP) TABLAS INTERVENIDAS EN MANTENIMIENTO

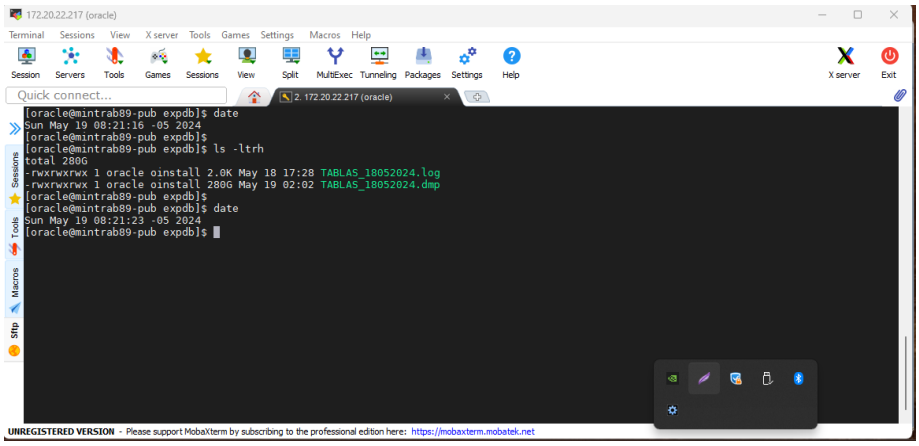


Ilustración 86 Generación de Backups DDBB

Validación tablas:

- **Tabla STORED_SYMBOL_TABLE:**

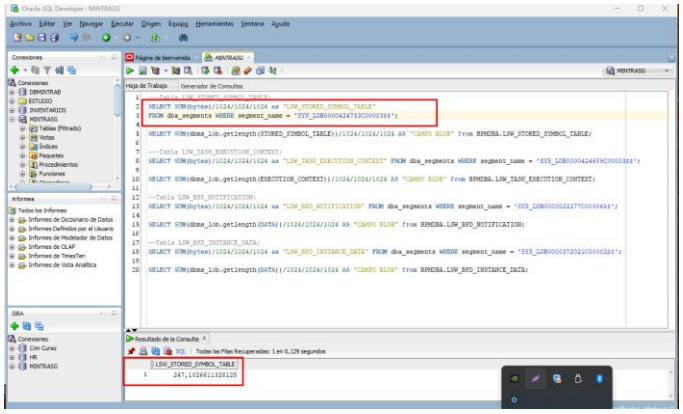


Ilustración 87 Validación Tablas DDBB

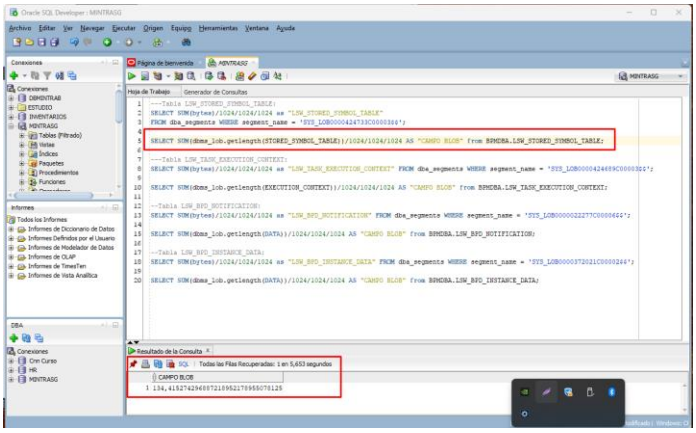


Ilustración 88 Validación Tablas DDBB

- **Tabla LSW_TASK_EXECUTION_CONTEXT:**

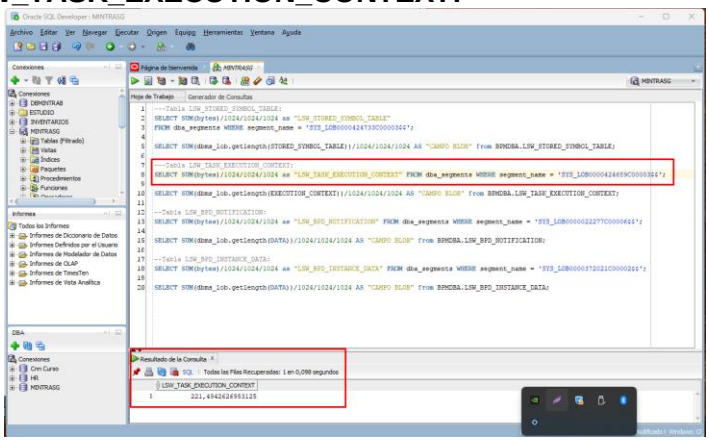


Ilustración 89 Validación Tablas DDBB

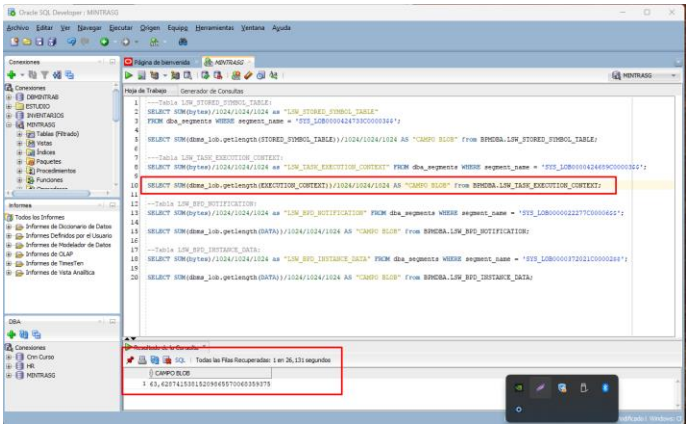


Ilustración 90 Validación Tablas DDBB

- **Tabla LSW_BPD_NOTIFICATION:**

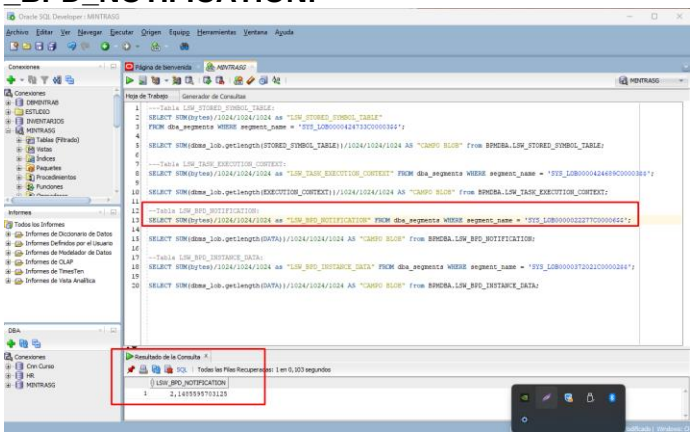


Ilustración 91 Validación Tablas DDBB

- **Tabla LSW_BPD_INSTANCE_DATA:**

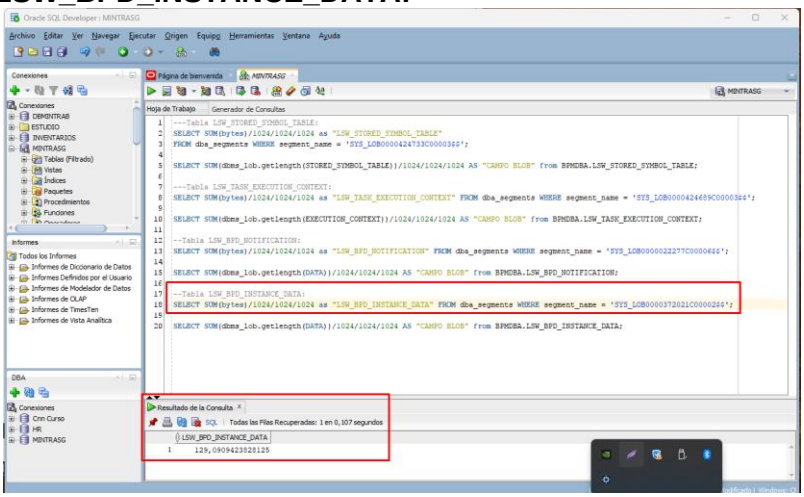


Ilustración 92 Validación Tablas DDBB

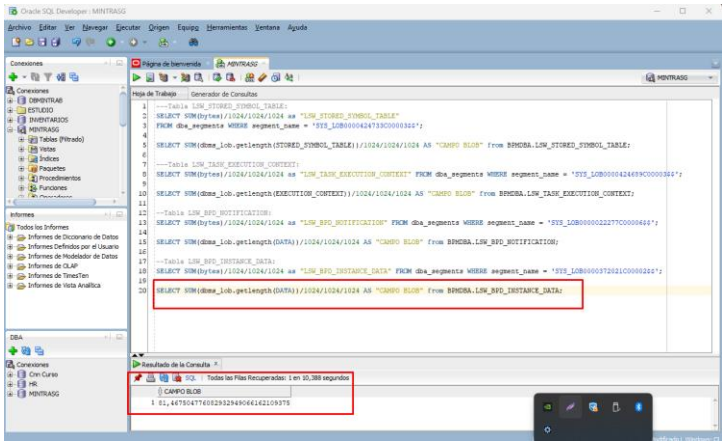


Ilustración 93 validación Tablas DDBB

- **Proceso colocar tablas en cero**

Se realiza consulta sobre las tablas BPMDBA.BPM_TASK_INDEX, BPMDBA.BPM_INSTANCE_INDEX para verificar el número de registros.

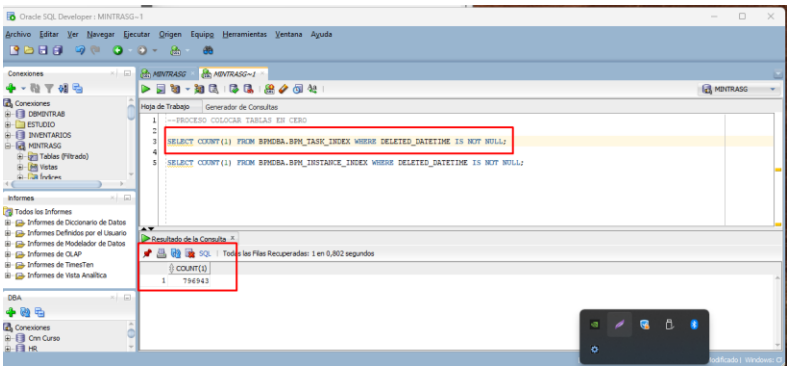


Ilustración 94 Verificación Registros

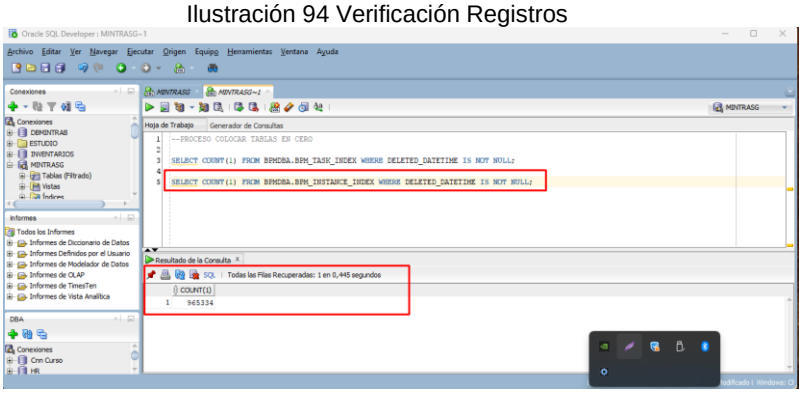


Ilustración 95 Verificación Registros

- Se ejecuta procedimiento de poner tablas en cero:
- Validación de tablas después de ejecución del proceso tablas en cero:

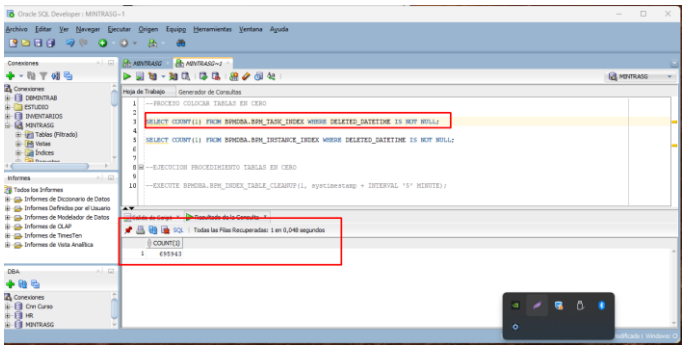


Ilustración 96 Verificación Registros tras ejecución de procesos

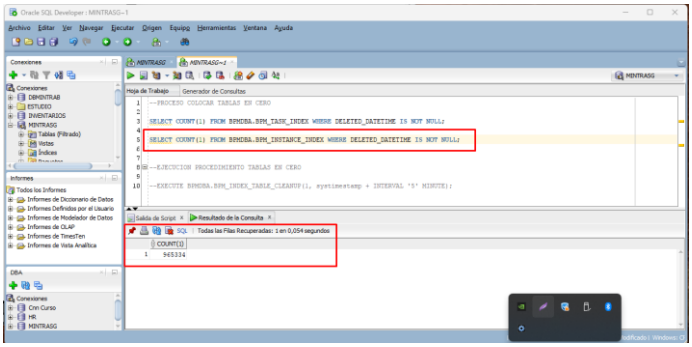


Ilustración 97 Validación de estado de tablas tras ejecución de procesos

- **Validar estatus de las instancias**

Se realizó consulta sobre la tabla BPMDBA.LSW_BPD_INSTANCE para validar cuantos registros existen con los estados 2,4 actualmente antes del mantenimiento.

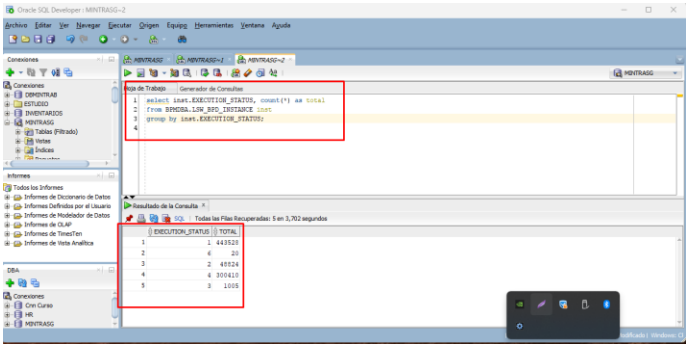


Ilustración 98 Estado de instancias DDDB

- **Eliminación de las instancias 2,4**

Se ejecutó la siguiente consulta para generar scripts para ejecutar el proceso de eliminación:

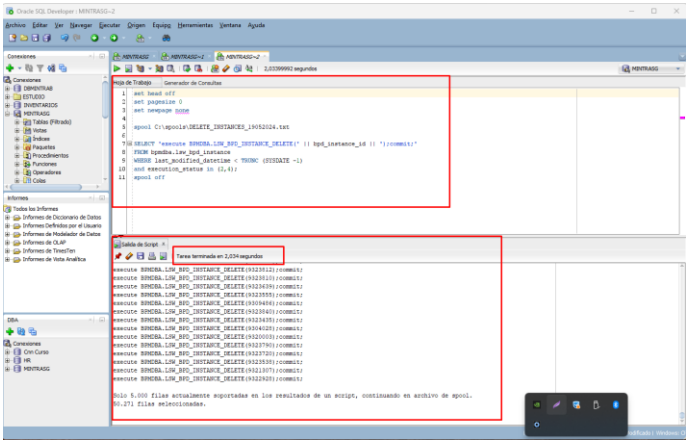


Ilustración 99 Eliminación de instancias

Se ejecutó scripts de eliminación de instancias según consulta anterior:

Validación de las instancias después de haber realizar el borrado

Se observó que para los registros 2,4 después del borrado su cantidad disminuyó en gran medida como lo muestra la imagen a continuación

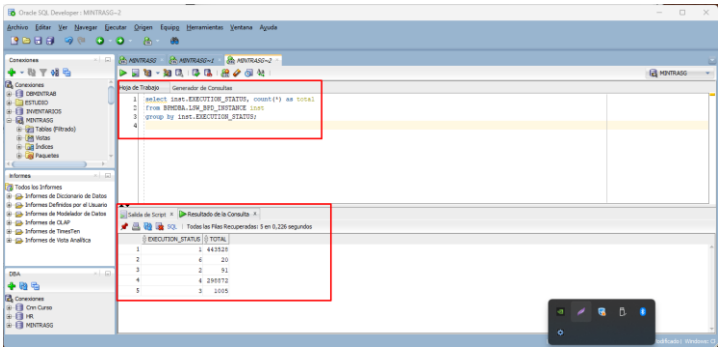


Ilustración 100 Disminución de instancias tras ejecución de proceso

Estado del servidor antes de la desfragmentación de tablas:

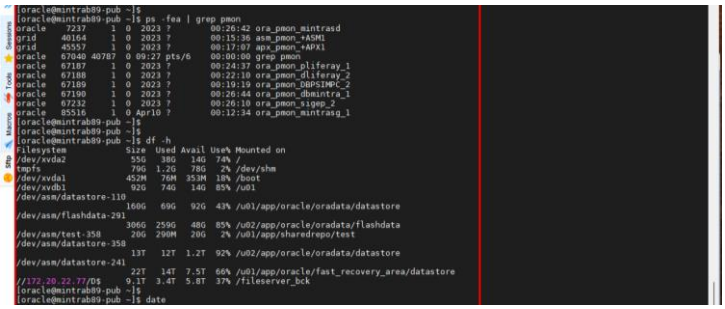


Ilustración 101 Estado del servidor - pre-desfragmentación

Proceso de desfragmentación de tablas del esquema BPMDBA:

BPMDBA.LSW_STORED_SYMBOL_TABLE
BPMDBA.LSW_TASK_EXECUTION_CONTEXT
BPMDBA.LSW_BPD_NOTIFICATION
BPMDBA.LSW_BPD_INSTANCE_DATA

Ejecución de scripts proceso de desfragmentación:

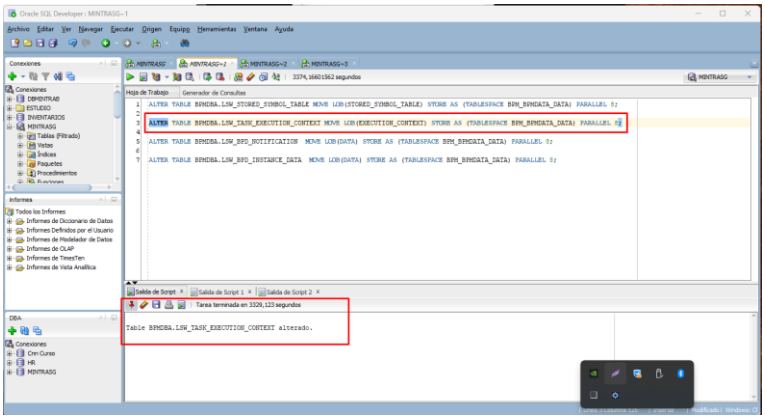


Ilustración 102 Ejecución desfragmentación

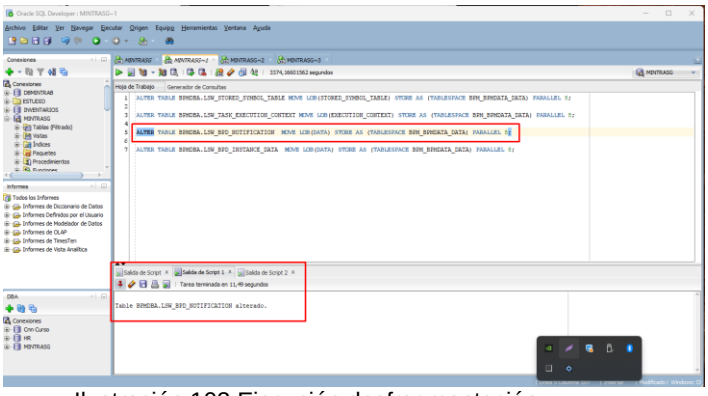


Ilustración 103 Ejecución desfragmentación

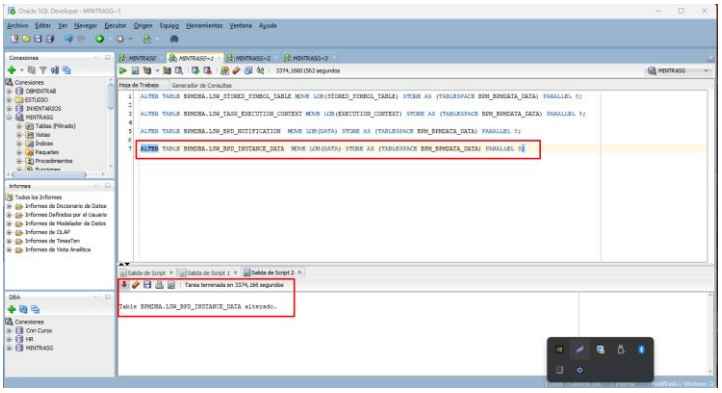


Ilustración 104 Ejecución desfragmentación

- **Reconstrucción de índices:**

Después de realizar la desfragmentación de tablas, se ejecutó el proceso para reconstruir índices, se reconstruyen los que están en estado inusable, necesarios para acelerar las consultas y mejorar el rendimiento de las operaciones de búsqueda.

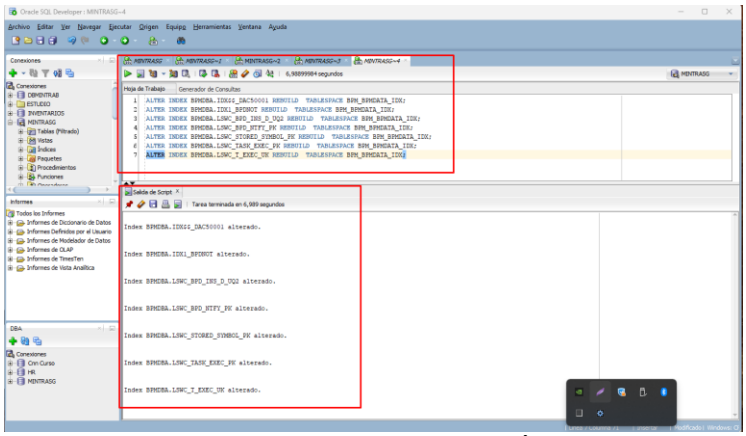


Ilustración 105 Reconstrucción de Índices

Validación de tamaños de tablas después de desfragmentación:
Tabla STORED_SYMBOL_TABLE:

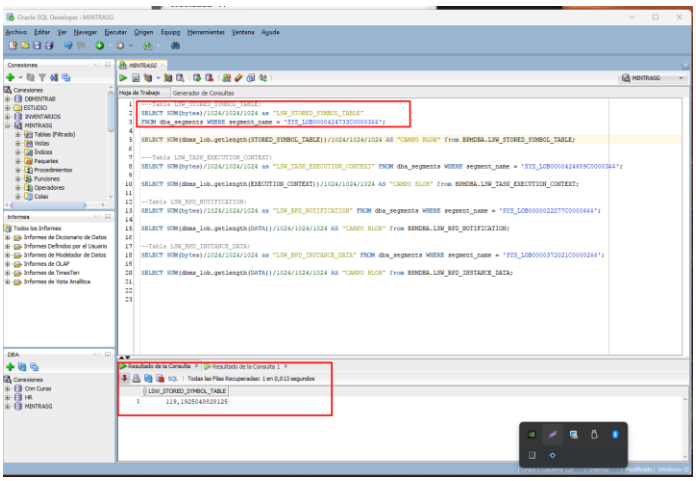


Ilustración 106 Validación de tamaños de tablas

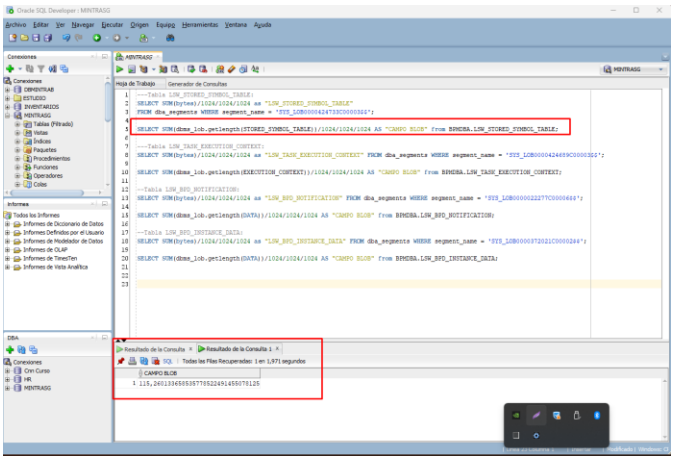


Ilustración 107 Validación de tamaños de tablas

- **Tabla LSW_TASK_EXECUTION_CONTEXT:**

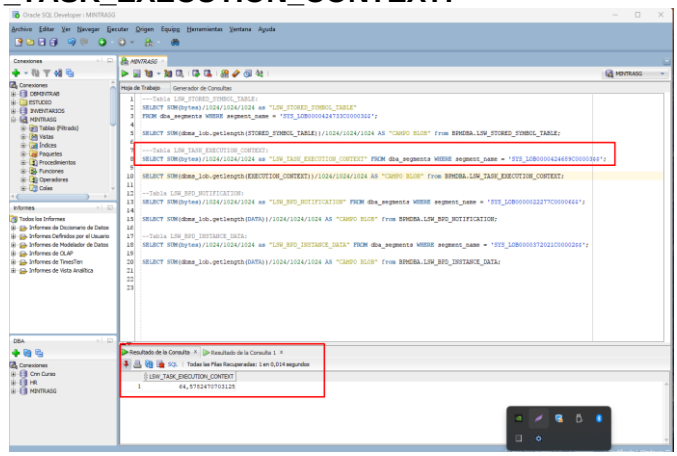


Ilustración 108 Validación de tamaños de tablas

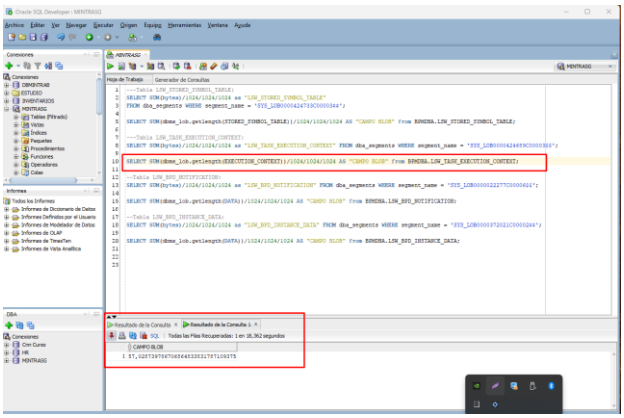


Ilustración 109 Validación de tamaños de tablas

- **Tabla LSW_BPD_NOTIFICATION:**

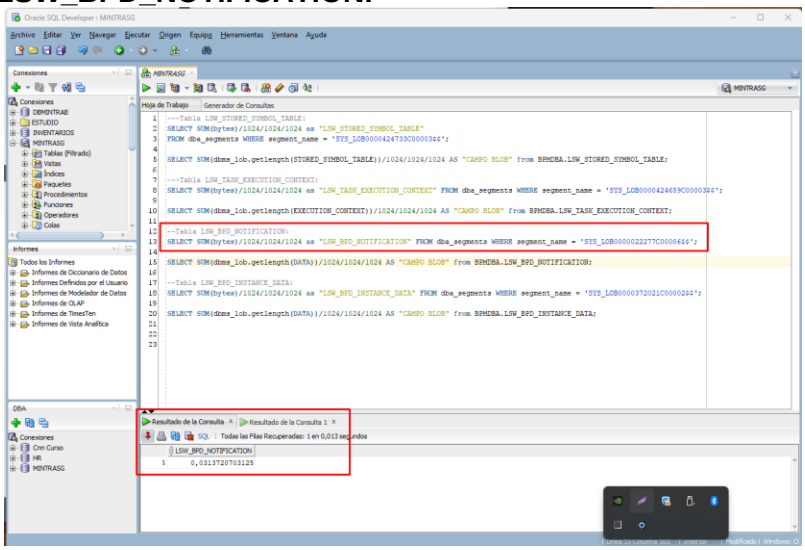


Ilustración 110 Validación de tamaños de tablas

- **Tabla LSW_BPD_INSTANCE_DATA:**

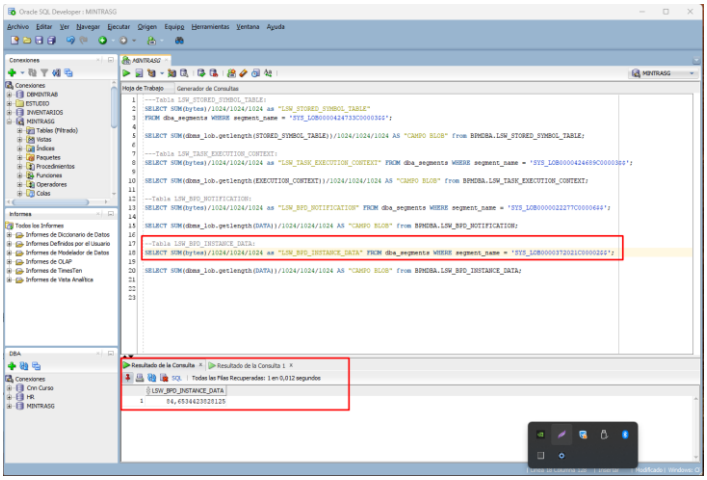


Ilustración 111 Validación de tamaños de tablas

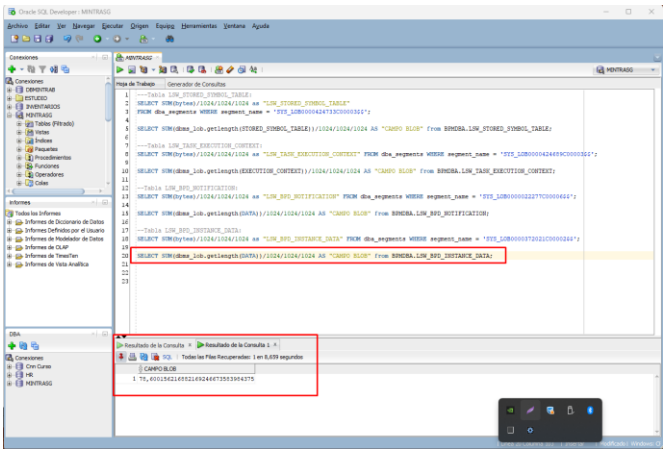


Ilustración 112 Validación de tamaños de tablas

Ejecución de estadísticas sobre las tablas antes desfragmentadas

Se procedió a ejecutar estadísticas para que el optimizador de consultas tome decisiones informadas sobre cómo ejecutar las consultas de manera más eficiente. Las estadísticas proporcionan información sobre la distribución de datos, la cardinalidad de las columnas y otros detalles que ayudan al optimizador a generar planes de ejecución más eficientes.

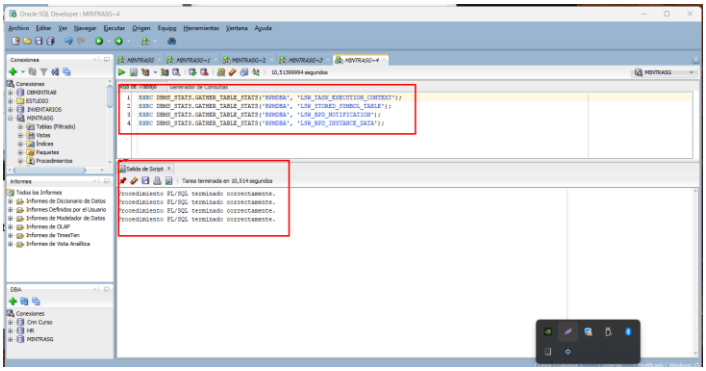


Ilustración 113 Ejecución de estadísticas de validación

Se procedió subir servicios de aplicación, donde se confirmó funcionalidad del sistema.
Se procede a ejecutar estadísticas para que el optimizador de consultas tome decisiones informadas sobre cómo ejecutar las consultas de manera más eficiente. Las estadísticas proporcionan información sobre la distribución de datos, la cardinalidad de las columnas y otros detalles que ayudan al optimizador a generar planes de ejecución más eficientes.
Se procedió a subir servicios de aplicación, donde se confirmó funcionalidad del sistema. El promedio de usuarios conectados al Gestor ha sido de 320 al mismo tiempo. Se presentan las estadísticas de los últimos meses:

De acuerdo con la información solicitada por la entidad se hace entrega de la siguiente documentación remitida en anteriores ocasiones a las anteriores supervisiones:

En el marco del fortalecimiento de los servicios digitales y la gestión eficiente de la información institucional, el Gestor Documental se ha consolidado como una herramienta clave para el soporte de los procesos operativos y administrativos. Su uso transversal en las diferentes sedes refleja la importancia de contar con una infraestructura tecnológica robusta, alineada con las necesidades crecientes de acceso, trazabilidad y seguridad documental

El objetivo principal es brindar información sobre el estado actual de la aplicación del gestor documental, abarcando aspectos como el modelo de licenciamiento, la arquitectura del sistema, la distribución de procesos y la infraestructura de servidores, con el fin de ofrecer una visión clara y detallada de su implementación y funcionamiento general.

La siguiente imagen presenta las distintas categorías definidas en la herramienta de gestión Aranda, las cuales permiten clasificar los casos de acuerdo con la naturaleza y necesidad del requerimiento reportado.

Categoría	marzo	abril	mayo	junio	Total general
Radicar una solicitud.Gestor documental.Asignar Radicado TYS	143	170	224	78	615
Radicar una solicitud.Gestor documental.Asesoria - Consulta	33	136	203	50	422
Radicar una solicitud.Gestor documental.Asignacion - Modificacion Role	121	110	105	43	379
Radicar una solicitud.Gestor documental.Depuración Bandeja	46	20	46	39	151
Reportar una falla.Gestor Documental.Falla Funcional	55	15	53	14	137
Reportar una falla.Gestor Documental.Falla radicacion	22	10	14	13	59
Radicar una solicitud.Gestor documental.Solicitud depuracion carpeta	8	18	11	4	41
Radicar una solicitud.Gestor documental.Suspender - Finalizar Radica Ty	11	12	9	8	40
Reportar una falla.Gestor Documental.No permite Aprobar y radicar	5	2	3	8	18
Reportar una falla.Gestor Documental.Falla error - Producir documento	3	5	3	1	12
Reportar una falla.Gestor Documental.Falla - Error PQRSD			9	2	11
Reportar una falla.Gestor Documental.Lentitud gestor	2	3	4		9
Reportar una falla.Gestor Documental.No genera sticker	2	1	3		6
Reportar una falla.Gestor Documental.No se encuentra radicado	4			1	5
Reportar una falla.Gestor Documental.Falla Error - Datacap		2	2	1	5
Reportar una falla.Gestor Documental.Falla - Error TYS	1	2	1		4
Reportar una falla.Gestor Documental.No permite ingresar datos	2	1	1		4
Reportar una falla.Gestor Documental.Falla al cargar archivos	2			1	3
Reportar una falla.Gestor Documental.PDF en blanco		1			1
Total general	**460**	**508**	**691**	**263**	**1922**

Tabla 59 Comportamiento casos GD

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

- Radicar una solicitud - Asignar Radicado TYS (615 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 - Asesoría/Consulta (422 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.
- Radicar una solicitud - Asignación/Modificación de Roles (379 casos) Asignación de nuevos roles debido a cambios en la dependencia del usuario final, como renuncias, traslados o reasignaciones internas dentro de la entidad.
- Radicar una solicitud - Depuración de Bandeja (151 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.
- Reportar una falla - Falla Funcional (137 casos) Fallos funcionales en la plataforma están impidiendo realizar radicaciones o cargar documentos, presentándose problemas de acceso, lentitud y desempeño del servicio. Este comportamiento se debe principalmente a una alta carga transaccional, con más de 320 usuarios concurrentes, así como a limitaciones en la conectividad de algunas sedes territoriales, especialmente al momento de cargar documentos en recursos compartidos (SharePoint, Carpetas Compartidas entre otras), lo que degrada la experiencia del usuario durante los picos de uso.

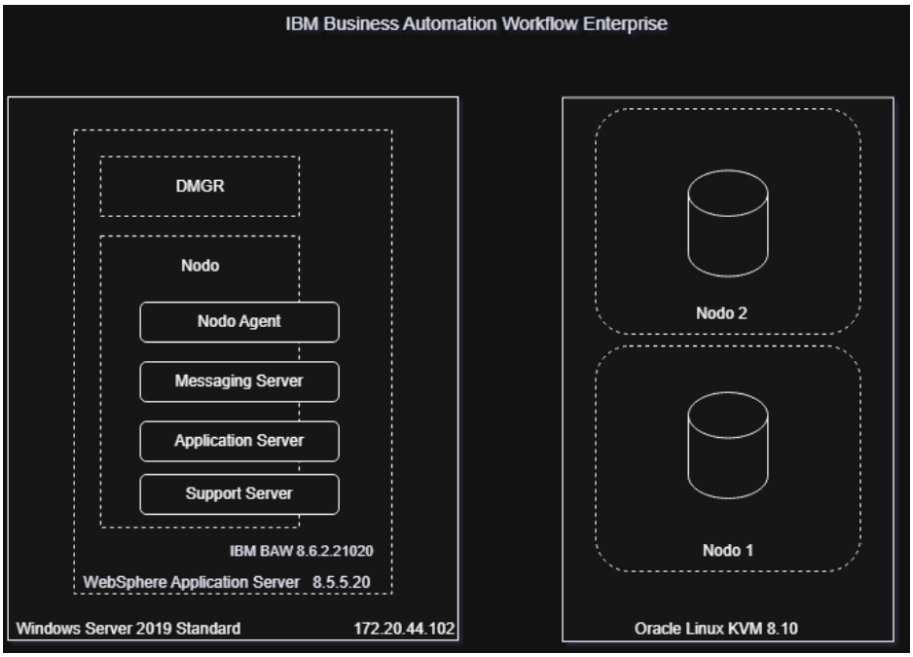


Ilustración 114 Diagrama BPM

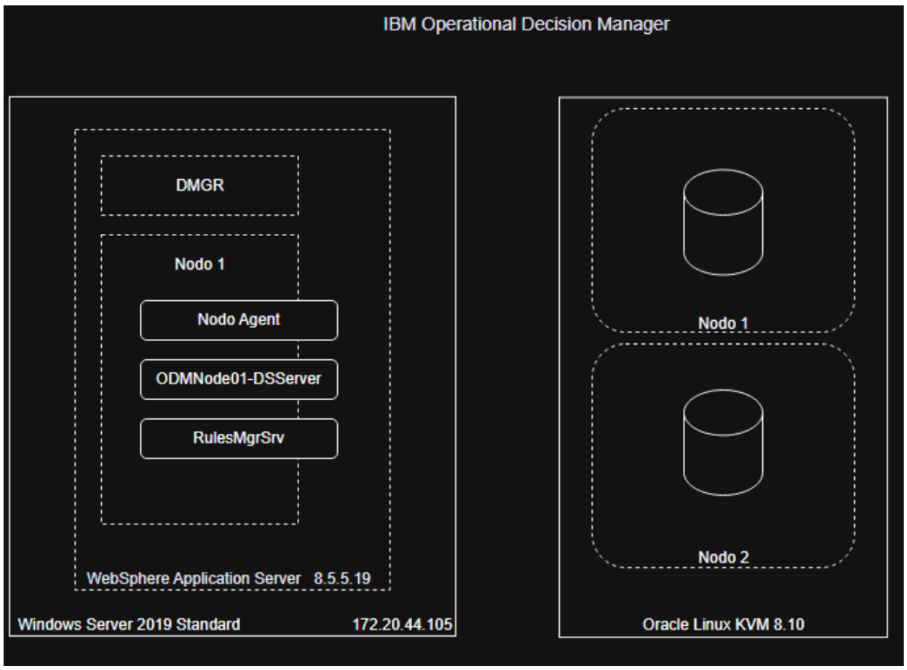


Ilustración 115 Diagrama ODM

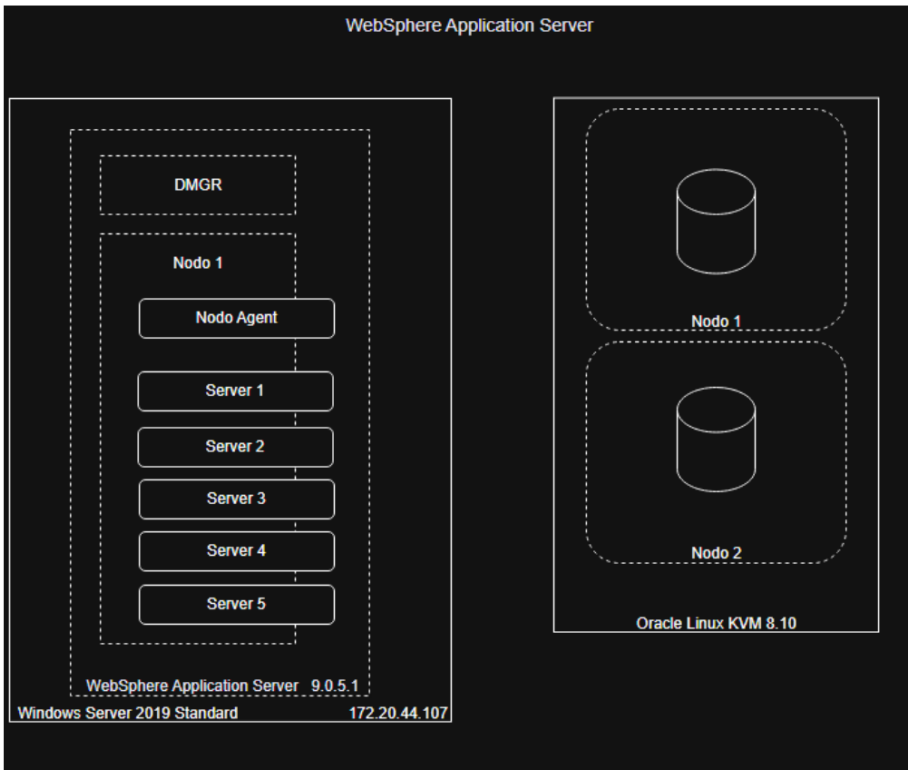


Ilustración 116 Diagrama WASND

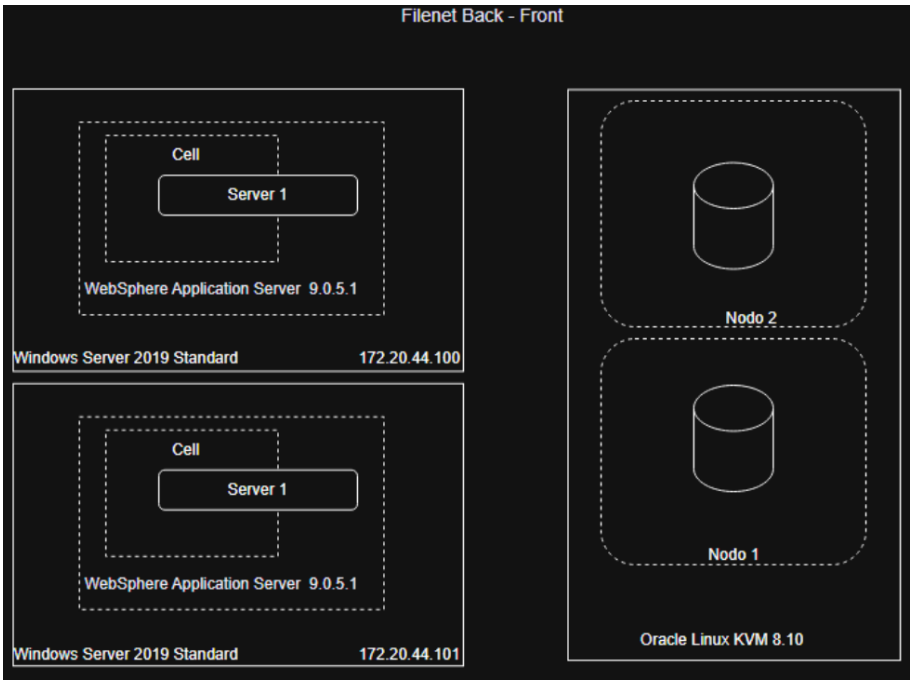


Ilustración 117 Diagrama FileNet Front

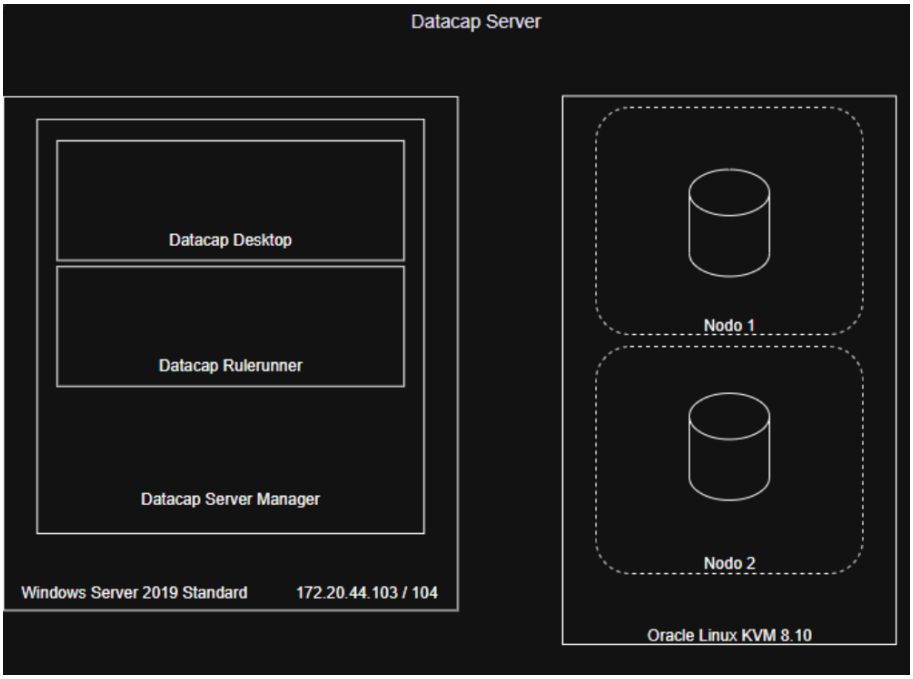


Ilustración 118 Diagrama Datacap

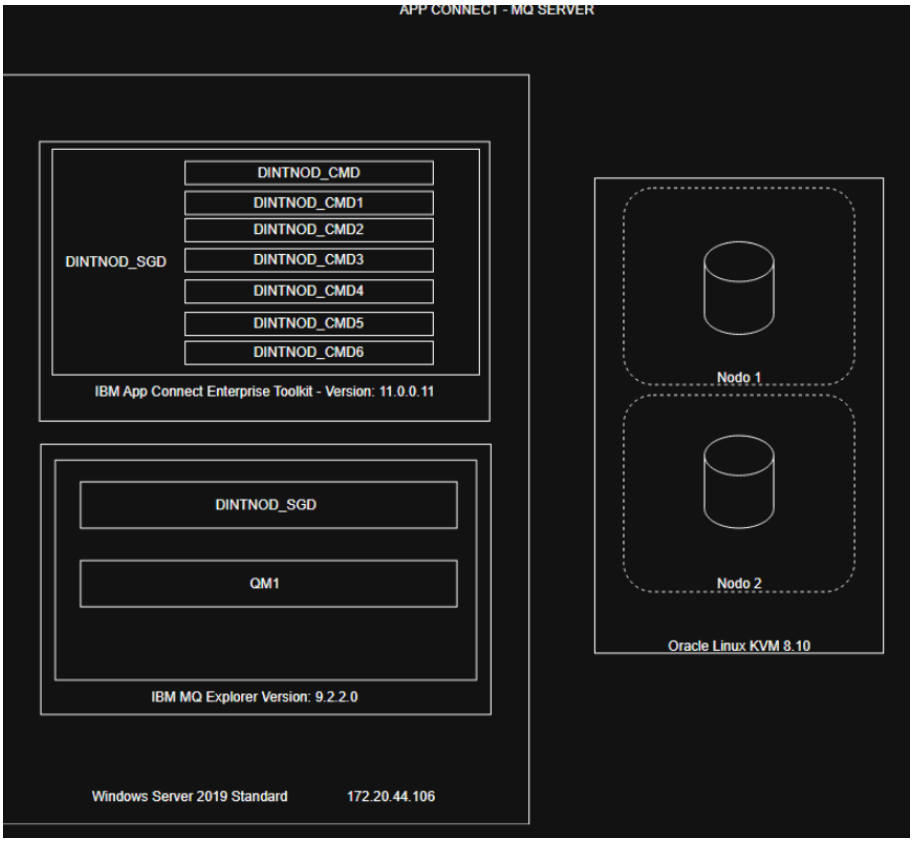


Ilustración 119 Diagrama App Connect

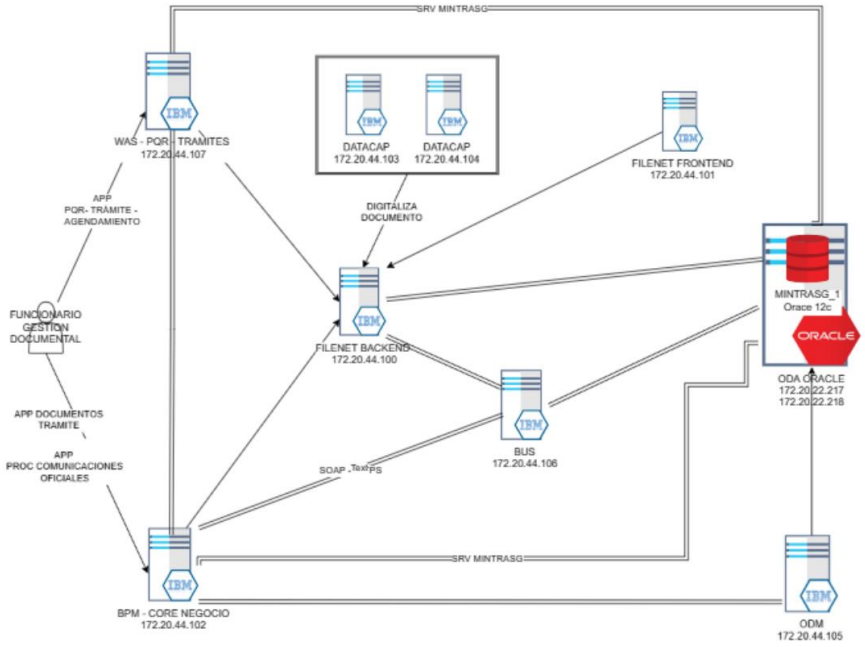


Ilustración 120 Arquitectura Gestor Documental

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 121 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 122 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 123 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
Total acumulado	**837.102**

Tabla 60 Total Instancias

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

Mayo 2025	204354
Junio 2025	178790
Total acumulado	**1.091.412**

Tabla 61 Total Documentos

Mes	Suma de Total radicados
Enero 2025	59197
Febrero 2025	70194
Marzo 2025	72317
Abril 2025	64370
Mayo 2025	73694
Junio 2025	63934
Total, acumulado	**403.706**

Tabla 62 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.

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 63 Dimensionamiento Servers IBM - Virtualización Optima

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:

BASES DE DATOS AMBIENTES PRODUCTIVOS ACTUAL								
DB_NAME	APP	INFRAESTRUCTURA	# CORES ASIGNADOS (VIRTUALES)	TOTAL CPUs NODOS	CLUSTER	ASM	LICENCIA	CANT LICENCIAS REQUERIDAS
mintrasg	Gestor documental	CLOUD PRIVADA	12	24	ACT -ACT	SI	Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	12
pliferay	Web MinTrabajo	ODA X5-2	4	4	ONE NODE		Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	2
dbmintra	SISINFO	ODA X5-2	12	12	ONE NODE		Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	6
dbsimpc	SIMPC	ODA X5-2	2	2	ONE NODE		Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	1
sigep	NOMINA	ODA X5-2	8	8	ONE NODE		Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	4
							TOTAL LICENCIAS	25

Ilustración 124 Distribución de licencias Oracle

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.

BASES DE DATOS AMBIENTES DEV - PRU ACTUALES							
dliferay		ODA X5-2	4	4	ONE NODE	Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	2
mintrasd		ODA X5-2	4	4	ONE NODE	Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	2
						TOTAL LICENCIAS	4
						TOTAL CONSOLIDADO	29

Ilustración 125 Licencias ambientes

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.

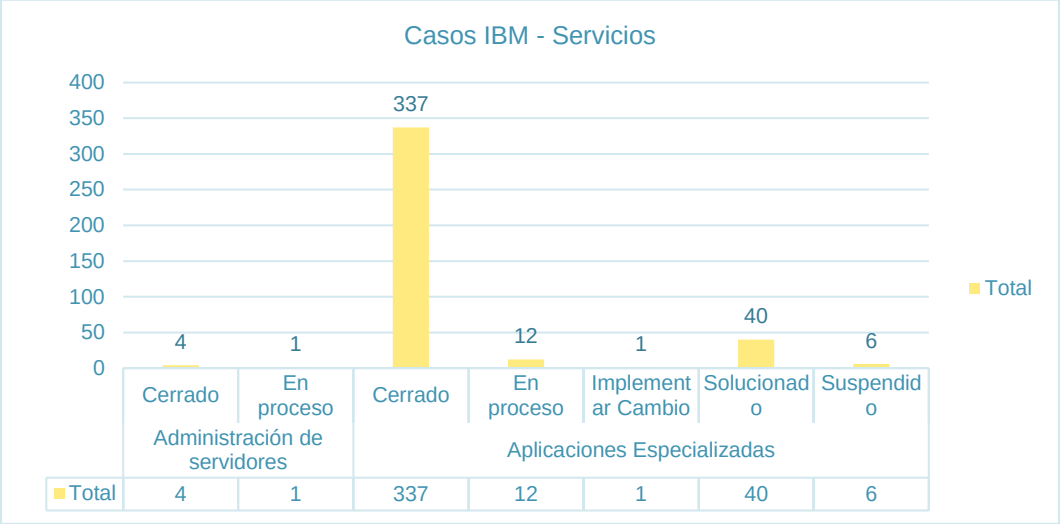


Ilustración 126 Casos IBM - Servicio

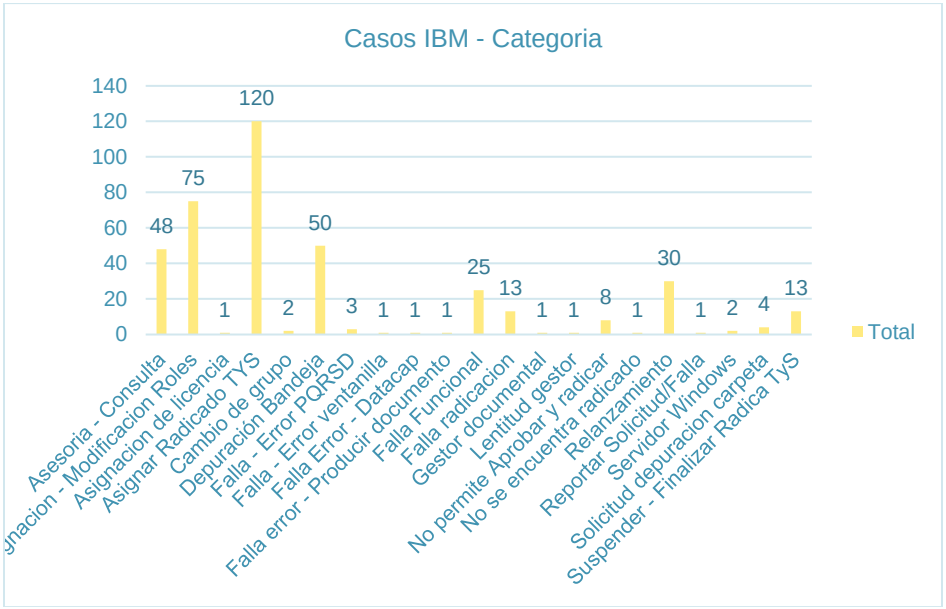


Ilustración 127 categoría DDBB

- **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. Como es de conocimiento del área funcional en el proceso de actualización para la tabla PLANILLA arrojo error, en caso de necesitar alguna modificación o realizar de nuevo el cargue por favor crear un nuevo caso.

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 Coordinadora 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.

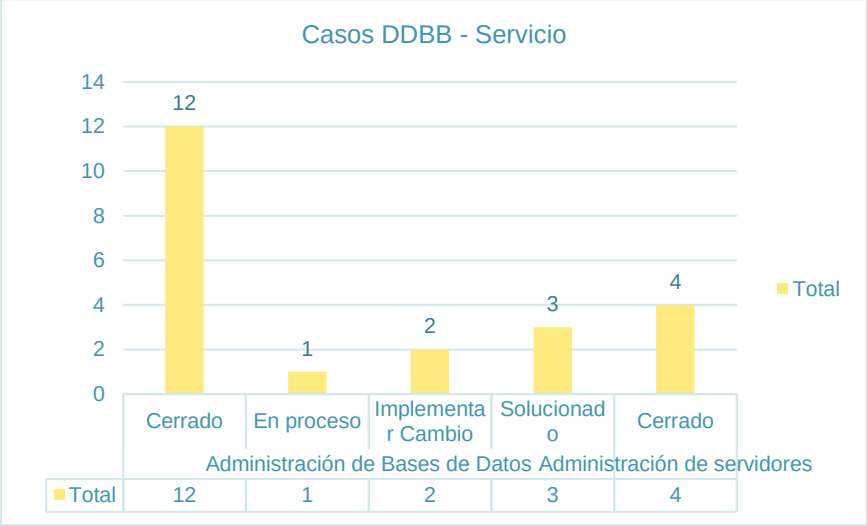


Ilustración 128 Casos DDBB por Servicio

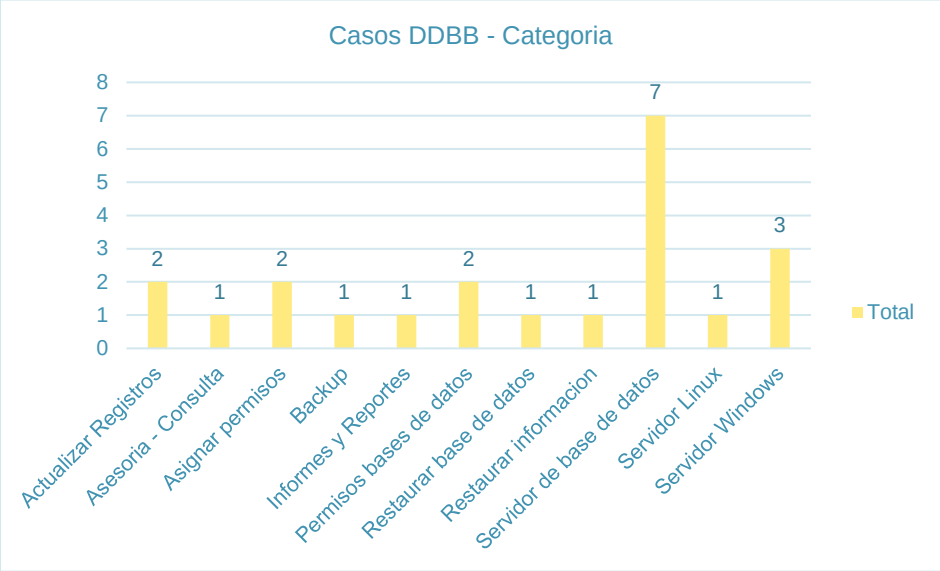


Ilustración 129 casos DDBB

- **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:

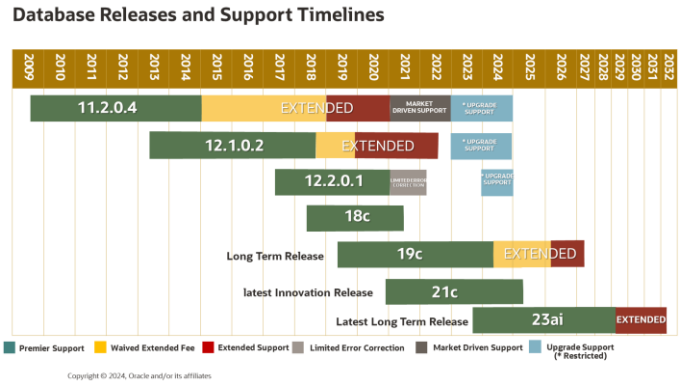


Ilustración *130* Estado Bases de Datos

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

INST_NAME	IP	SERVER_NAME	AMBIENTE	Version_Motor	S.O	MEMORIA GB	CPU	STORAGE ASIG GB	STORAGE USED GB	STORAGE FREE GB
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 65 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 66 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 131 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 132 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 133 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 134 Estadísticas Pool compartido

Tamaño base de datos MINSTRASG:

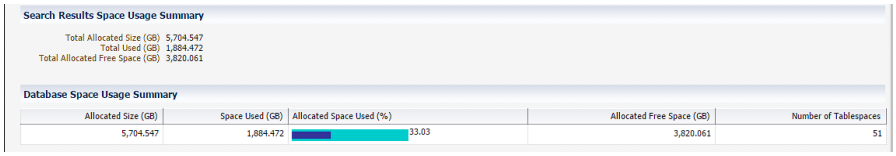


Ilustración 135 Tamaño DDBB

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 136 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

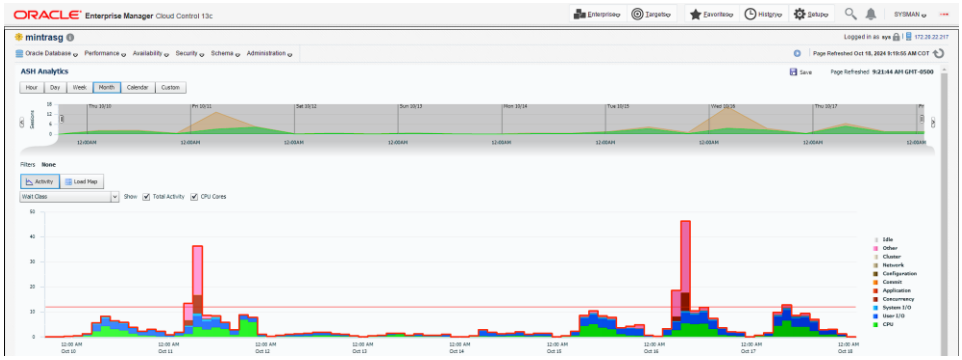


Ilustración 137 Rendimiento DDBB

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 138 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 139 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 140 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 141 Estadística Shared Pool

Tamaño base de datos DBMINTRA:

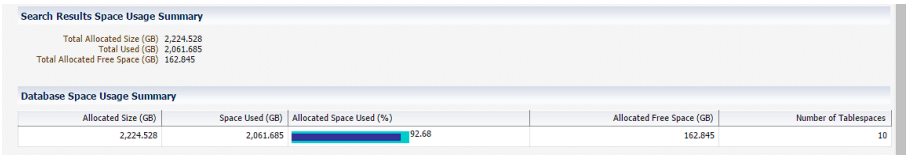


Ilustración 142 Tamaño DDBB DBMINTRA

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 143 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

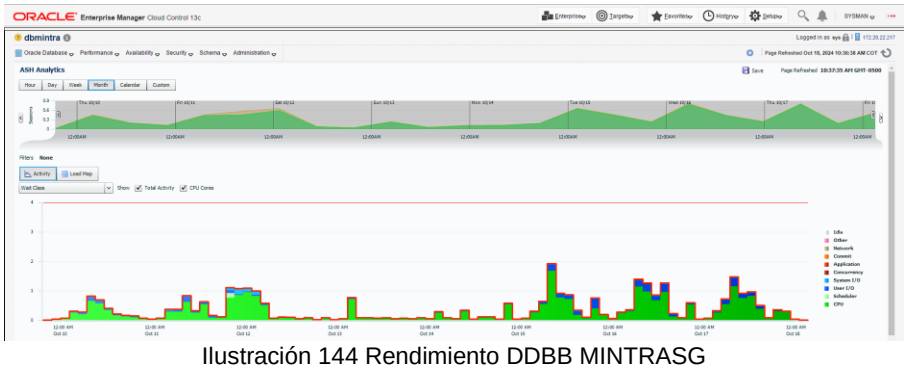


Ilustración 144 Rendimiento DDBB MINTRASG

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 145 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 146 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 147 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 148 Estadísticas Shared Pool

Tamaño base de datos PLIFERAY:

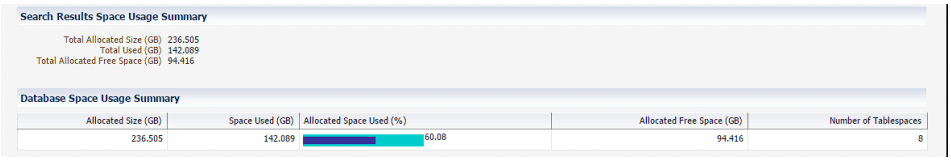


Ilustración 149 Tamaño DDBB PLifeRay

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 150 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

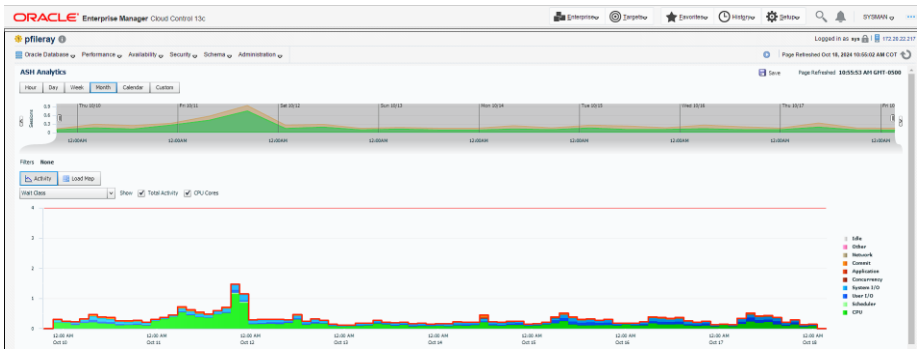


Ilustración 151 Rendimiento DDBB PlifeRay

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 152 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 153 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 154 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 155 Estadística Shared Pool

Tamaño base de datos SIGEP:

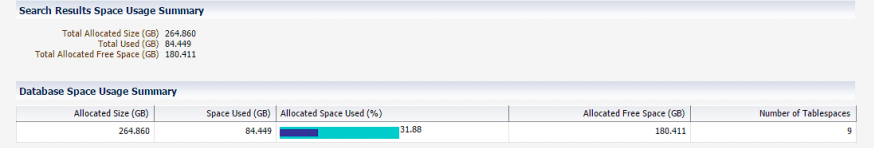


Ilustración 156 Tamaño DDBB SIGEP

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 157 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

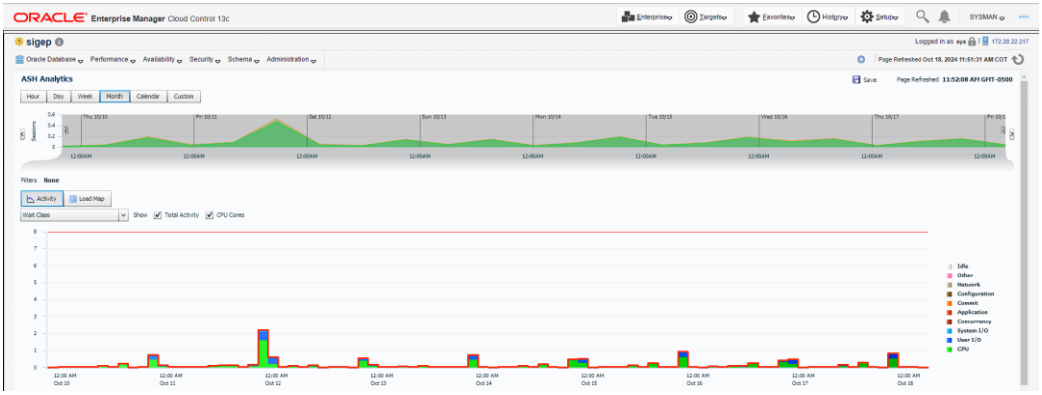


Ilustración 158 Rendimiento DDBB SIGEP

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 159 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 160 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 161 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 162 Estadística Shared Pool

Tamaño base de datos DBSIMPC:

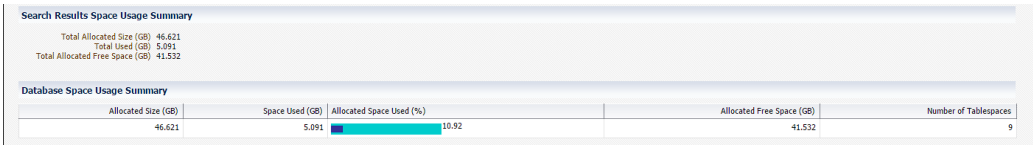


Ilustración 163 Tamaño DDBB SIMPC

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 164 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

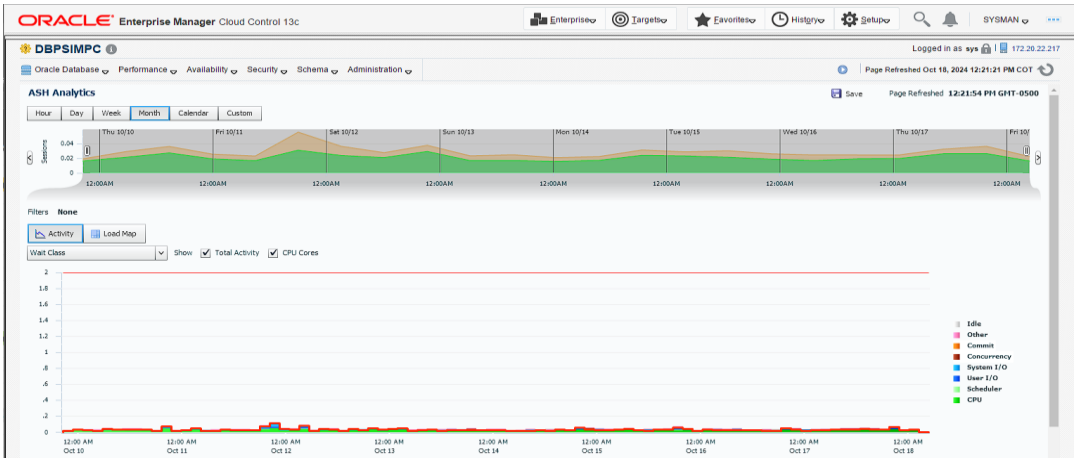


Ilustración 165 Rendimiento DDBB

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 166 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 167 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 168 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 169 Estadística Shared Pool

Tamaño base de datos MINTRASD:

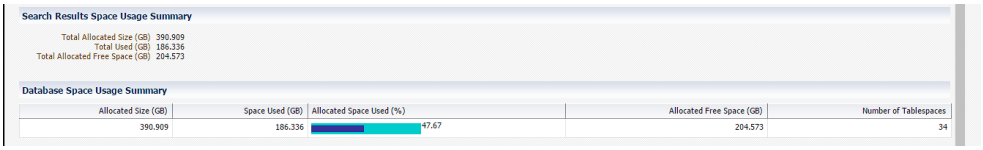


Ilustración 170 Tamaño DDBB MINTRASD

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
SQLTXPLAIN	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 171 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

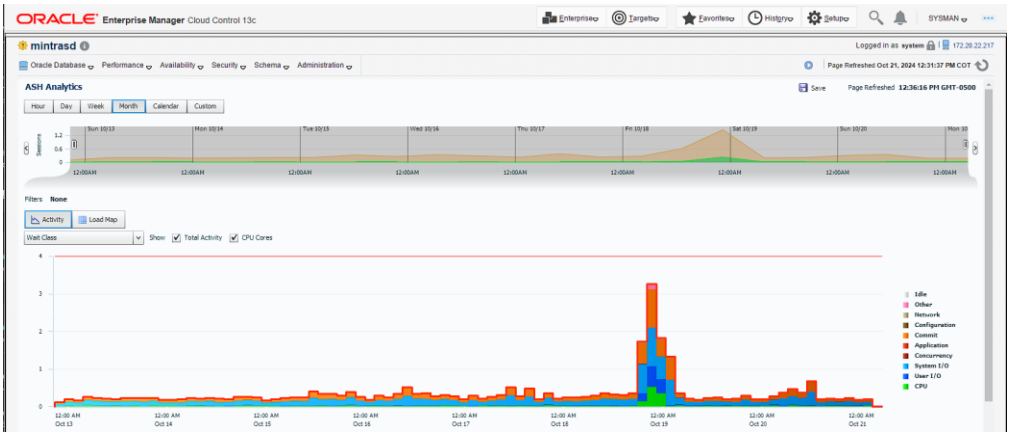


Ilustración 172 Rendimiento MINTRASD

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 173 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 174 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 175 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 176 Estadística Shared Pool

Tamaño base de datos MINTRASD:

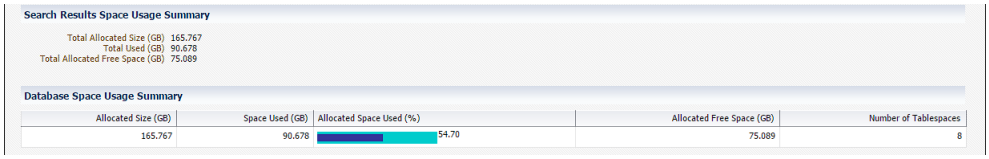


Ilustración 177 Tamaño DDBB

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 178 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

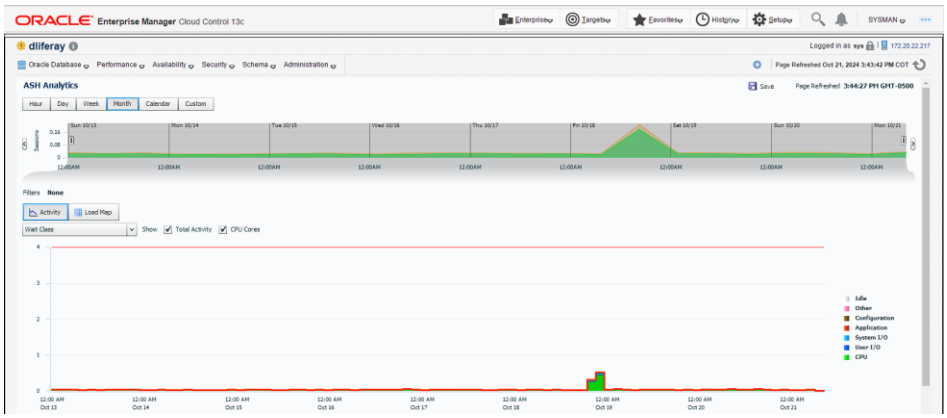


Ilustración 179 Rendimiento DDBB

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 180 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 181 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 182 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 183 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 184 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 185 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

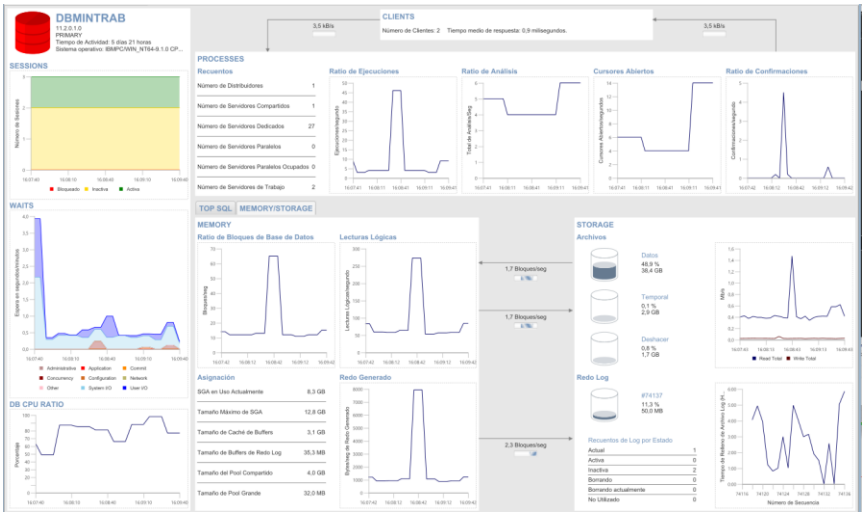


Ilustración 186 Rendimiento DDBB

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 187 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 188 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 189 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 190 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 191 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

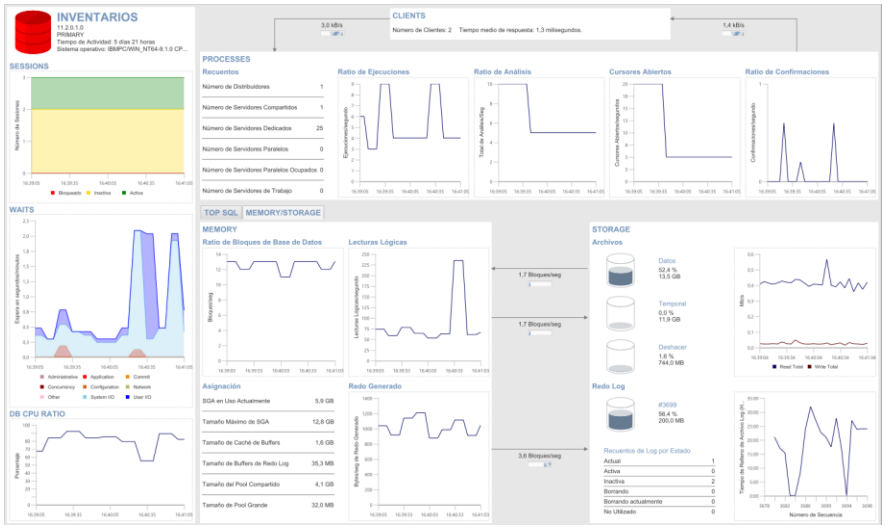


Ilustración 192 Comportamiento DDBB

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 193 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 194 DiskGroup Data

DISKGROUP FLASH:

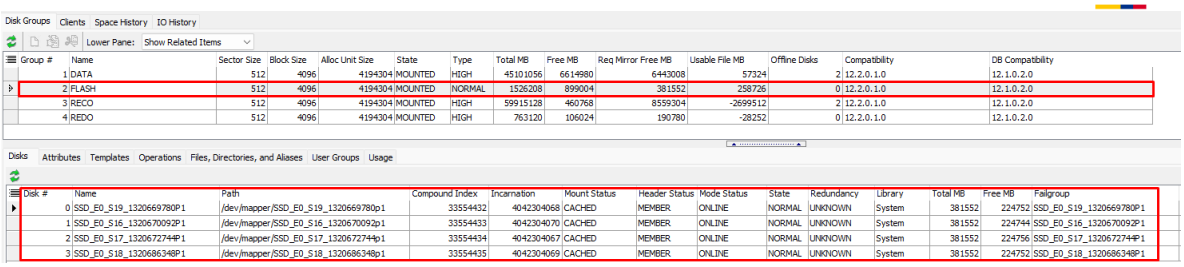


Ilustración 195 DiskGroup Flash

DISKGROUP RECO:

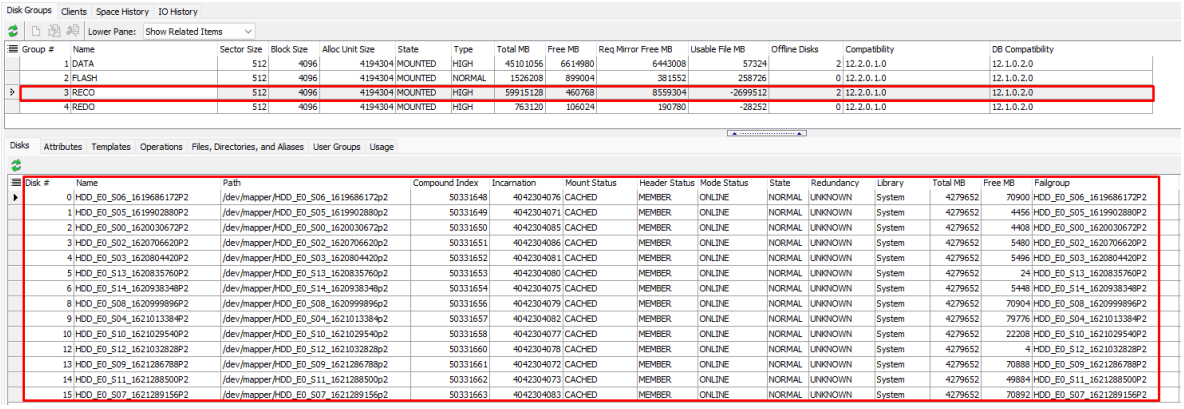


Ilustración 196 DiskGroup Reco

DISKGROUP REDO:

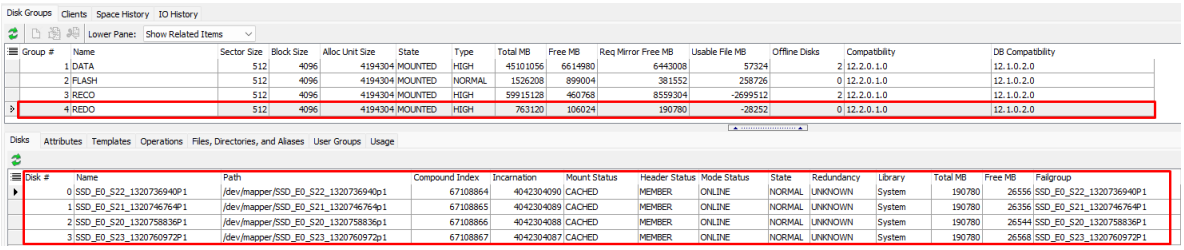


Ilustración 197 DiskGroup Redo

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 198 Licenciamiento adicional componente IBM

3.1.5. **No aplica**

3.1.6. **Seguridad Informática**

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

3.1.6.1. Firewalls de nueva generación

Durante junio de 2025, los firewalls de Fortinet han mantenido un estado óptimo en cuanto a la seguridad perimetral. Se ha llevado a cabo una supervisión continua de la red para garantizar que solo el tráfico autorizado tenga acceso a los recursos internos. Se han implementado 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

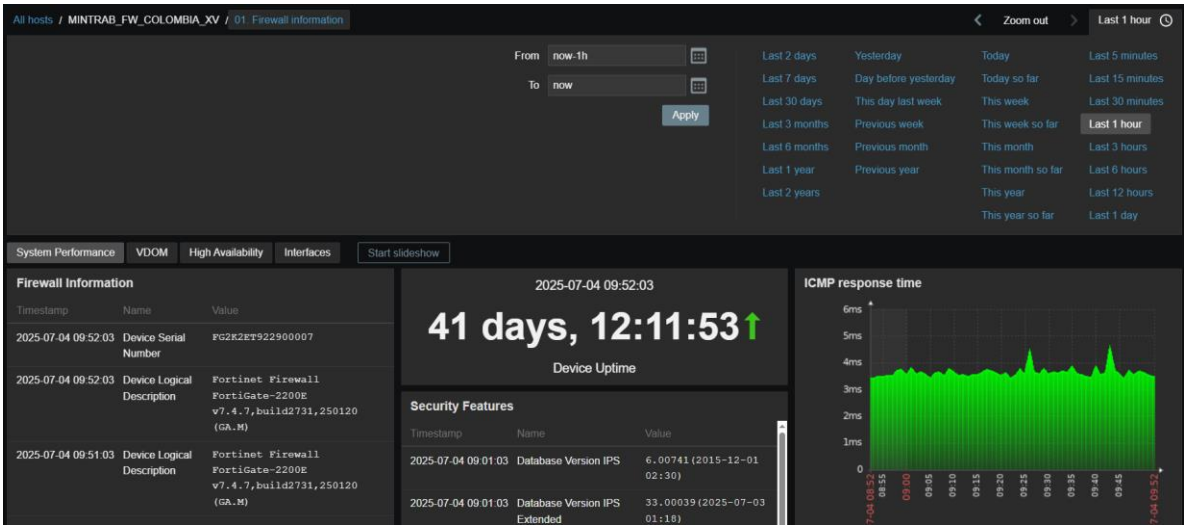


Ilustración*199* Disponibilidad firewall

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

Esta imagen presenta un resumen del uso de ancho de banda y el número de sesiones durante el período del mes de junio. 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.

Máximo Consumo: El punto más alto del consumo de ancho de banda se aproxima a los 5 TB.

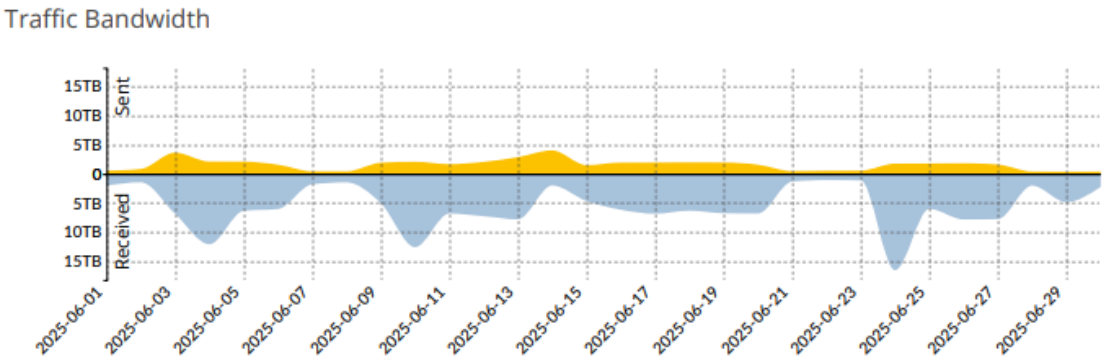


Ilustración*200* Comportamiento ancho de banda

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 junio. 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:

Top Users by Bandwidth

#	User(or IP)	Bytes	Sent	Received
1	172.20.22.251			56.55 TB
2	172.28.28.38			5.79 TB
3	mduarteo			4.87 TB
4	172.25.0.132			4.61 TB
5	172.20.44.102			4.36 TB
6	172.20.22.194			3.06 TB
7	172.20.22.179			1.97 TB
8	172.20.22.32			1.94 TB
9	172.24.40.12			1.53 TB
10	172.16.64.12			1.12 TB

Ilustración *201* Reporte consumo ancho de banda

Top de usuarios por número de sesiones

Este informe presenta un análisis de las sesiones de usuario más activas en la red, los cuales se puede identificar por su dirección IP. Centrándose en los 10 principales usuarios e IP's que han generado el mayor número de sesiones durante el período del mes de junio. A continuación, se detallan los hallazgos más relevantes:

Top Users by Sessions

#	User (or IP)	Sessions
1	172.25.0.5	370,133,008
2	mduarteo	79,296,082
3	172.20.22.234	36,840,594
4	FORTINET	26,237,859
5	172.20.22.3	20,568,914
6	172.20.22.40	19,627,633
7	172.20.22.32	16,509,515
8	172.20.22.228	10,899,265
9	172.50.0.3	6,693,257
10	172.50.0.1	6,692,932

Ilustración*202* Top de usuarios

Durante junio se observaron eventos de tráfico de red. Estos eventos se distribuyen entre una variedad de servicios y aplicaciones, con una amplia gama de volúmenes de tráfico registrados, a continuación, se observa en la imagen las aplicaciones con más tráfico consumido.

- El tráfico de red está diversificado entre una amplia gama de servicios y aplicaciones, incluyendo colaboración, servicios en la nube y actualizaciones de software.
- Las aplicaciones de colaboración empresarial, como Microsoft Sharepoint y Microsoft Windows Update, Microsoft 365, son prominentes en el entorno, lo que refleja una tendencia hacia la adopción de herramientas de trabajo remoto y comunicación en equipo.
- Los servicios de almacenamiento, como SMB, muestran una actividad consistente, destacando la importancia de las soluciones de respaldo de datos en entornos empresariales.

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	TCP/902			55.20 TB
2	HTTPS			36.52 TB
3	SMB			21.32 TB
4	TCP/445			11.10 TB
5	SYSLOG			7.59 TB
6	TCP/1521			6.55 TB
7	HTTP			6.32 TB
8	Microsoft.Portal			5.81 TB
9	TCP/31031			5.81 TB
10	Microsoft.SharePoint			3.92 TB

Ilustración *203* Top tráfico de aplicaciones

Observación	Descripción
Mayor Uso de Ancho de Aplicaciones empresarial	- Microsoft Portal 5.81 GB, indicando alta actividad colaborativa.
	- **Microsoft** SharePoint 3.92 TB, reflejando la importancia de servicios de red seguros y transferencia de archivos seguros y transferencia de archivos.

Tabla 67 Top tráfico de aplicaciones

Categoría de Aplicaciones por Ancho de banda

En junio, se registró el tráfico de red por categorías de aplicación. Este tráfico se ha categorizado en una variedad de servicios y aplicaciones para proporcionar una visión completa del uso de la red.

Principales Aplicaciones por Ancho de Tráfico:

- **Colaboración (Collaboration)**:
  Es la categoría con el mayor uso de ancho de banda, alcanzando un total de 9.30 **TB**.
- Las aplicaciones más destacadas en esta categoría son:
  - **Microsoft Portal**: 5.81 TB
  - **Microsoft SharePoint**: 3.92 TB

- **SMB (Server Message Block)** es un **protocolo de red** utilizado para compartir archivos, impresoras y otros recursos entre dispositivos en una red, principalmente en sistemas Windows. También permite la comunicación entre clientes y servidores en redes locales (LAN): 21.32 TB de uso de ancho de banda.

Top 15 Authenticated Logins by VPN Connections

Examinaremos los detalles de los inicios de sesión por conexiones VPN-SSL en el período correspondiente al mes de junio

Authenticated Logins

#	User	Type	First Used	Total Number of Connections	Total Duration Connected(HH:MM:SS)
1	contaccenter	ssl-tunnel	2025-06-03 07:01:13	185	821:18:29
2	jcalderonf	ssl-tunnel	2025-06-01 17:54:16	101	116:02:06
3	jepinzon@noc_indra	ssl-tunnel	2025-06-03 06:16:05	97	361:06:55
4	ssalinas	ssl-tunnel	2025-06-01 19:14:41	94	215:05:46
5	cjimenez	ssl-tunnel	2025-06-01 09:52:21	84	65:01:16
6	eyreyes	ssl-tunnel	2025-06-03 08:30:02	79	150:59:43
7	rmurcia	ssl-tunnel	2025-06-02 16:58:26	76	101:03:28
8	atobar	ssl-tunnel	2025-06-01 22:54:23	72	51:42:54
9	dpinzon	ssl-tunnel	2025-06-03 16:11:38	70	39:12:56
10	lanzola	ssl-tunnel	2025-06-02 19:17:01	62	87:18:50
11	ewalteros	ssl-tunnel	2025-06-01 12:56:26	62	59:55:20
12	jdduque	ssl-tunnel	2025-06-04 10:34:19	56	105:12:25
13	cabuitragoo	ssl-tunnel	2025-06-02 18:01:55	53	242:35:26
14	agente4	ssl-tunnel	2025-06-02 21:43:25	52	235:41:29
15	dfdiazd@noc_indra	ssl-tunnel	2025-06-01 00:03:44	50	256:51:17

Ilustración 204 Top 15 Authenticated Logins by VPN Connections

Usuarios con Uso Frecuente:

Usuarios como contaccenter, jcalderon, y otros comenzaron a usar la VPN temprano en el día, lo que sugiere actividades de soporte técnico o roles críticos que requieren acceso temprano.

Failed Login Attempts by User

Este informe proporciona una visión detallada de los intentos fallidos de inicio de sesión y los usuarios más activos en la VPN, ofreciendo una base sólida para tomar medidas de seguridad adicionales y garantizar la integridad de los sistemas de acceso.

Failed Login Attempts

#	User	Type	Total Number of Failed Attempts
1	admin	ssl-web	528
2	Administrator	ssl-web	458
3	scanner	ssl-web	203
4	test	ssl-web	194
5	user1	ssl-web	166
6	vpn	ssl-web	154
7	guest	ssl-web	143
8	support	ssl-web	143
9	scan	ssl-web	139
10	administrator	ssl-web	133

Ilustración *205* Failed Login Attempts by User

Intentos Fallidos Significativos:

La mayoría de los intentos fallidos están concentrados en usuarios genéricos como, "administrador", "admin", y "Administrador". Esto podría indicar intentos de fuerza bruta o scripts automáticos intentando acceder a cuentas comunes, dentro de la validación de los usuarios permitidos para acceder a la vpn no encuentran estos usuarios con los que se está tratando de acceder, por lo que este riesgo se reduce para el Ministerio de Trabajo.

3.1.6.2. Sandbox – Amenazas día 0

El servicio de Sandbox para el Ministerio del Trabajo se utiliza para crear entornos aislados y seguros donde se pueden ejecutar archivos o programas sospechosos para analizar su comportamiento. La función principal del Sandbox es detectar y analizar posibles amenazas de seguridad, como malware o software malicioso, sin comprometer la seguridad del sistema principal. Para el mes de junio de 2025, se generaron 152 eventos analizados, los cuales fueron limpiados de algún tipo de amenazas

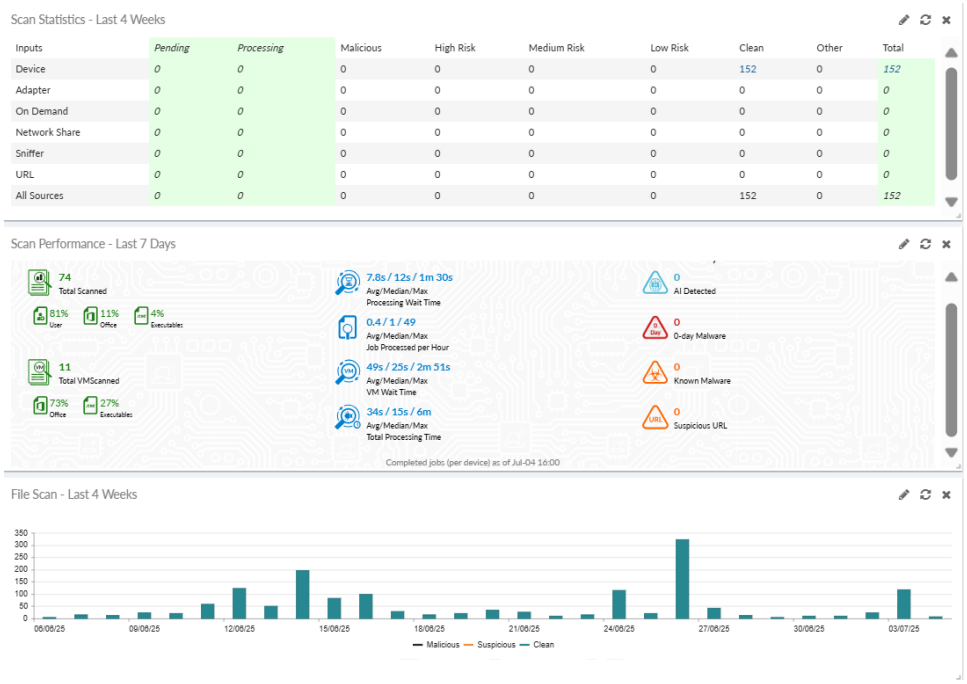


Ilustración 206 estadísticas de escaneo

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

Performance

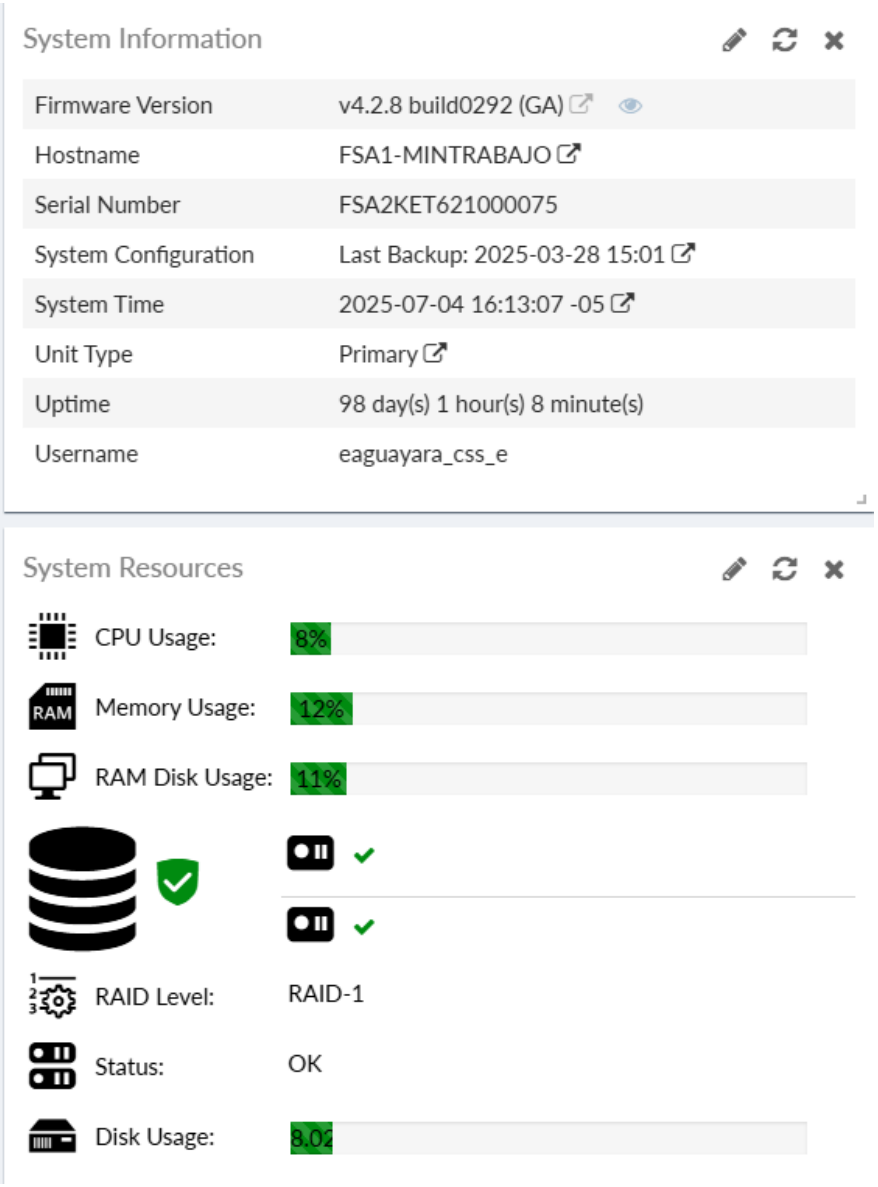


Ilustración *207* performance

Licencia Sandbox

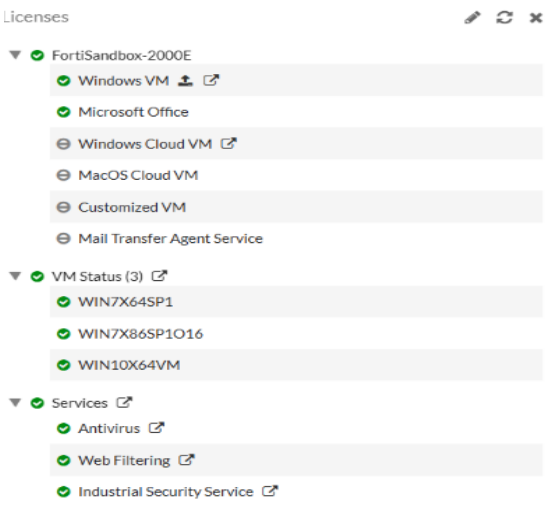


Ilustración *208* Licenciamiento

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

El sistema de Gestión de Eventos e Información de Seguridad (SIEM, por sus siglas en inglés) es una herramienta de seguridad informática implementada en el ministerio para proporcionar alertamientos en caso de generarse novedades e incidentes sobre la infraestructura.

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
☑	9 - HIGH	(s) Server Intf Util Critical	Detects that interface utilization of a network device has reached a critical level (utilization greater than 50% 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 Util Warning	Detects that interface utilization of a server has reached a warning level (utilization between 30% and 50% 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 Memory Critical	Detects that server memory 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 Memory Warning	Detects that server Memory 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 Swap Memory Critical	Detects that server swap memory has reached a critical level (free swap less than minimum swap)	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) Windows Server Health: Critical	Detects that the health of a windows server is critical and needs immediate attention based average CPU, memory, disk and interface utilization and interface errors - at least one of the measured attributes has crossed the specified HIGH threshold	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent	Correlation			Streaming
☐	5 - MEDIUM	(s) Windows Server Health: Warning	Detects that the health of a windows server need to be watched carefully based average CPU, memory, disk and interface utilization and interface errors- at least one of the measured attributes has crossed the specified LOW threshold but has not yet crossed the specified HIGH threshold	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent	Correlation			Streaming

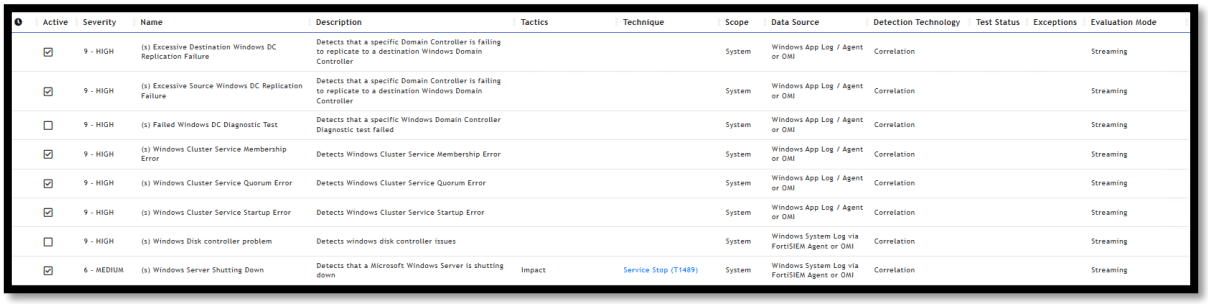
Ilustración *209* Casos de uso

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:

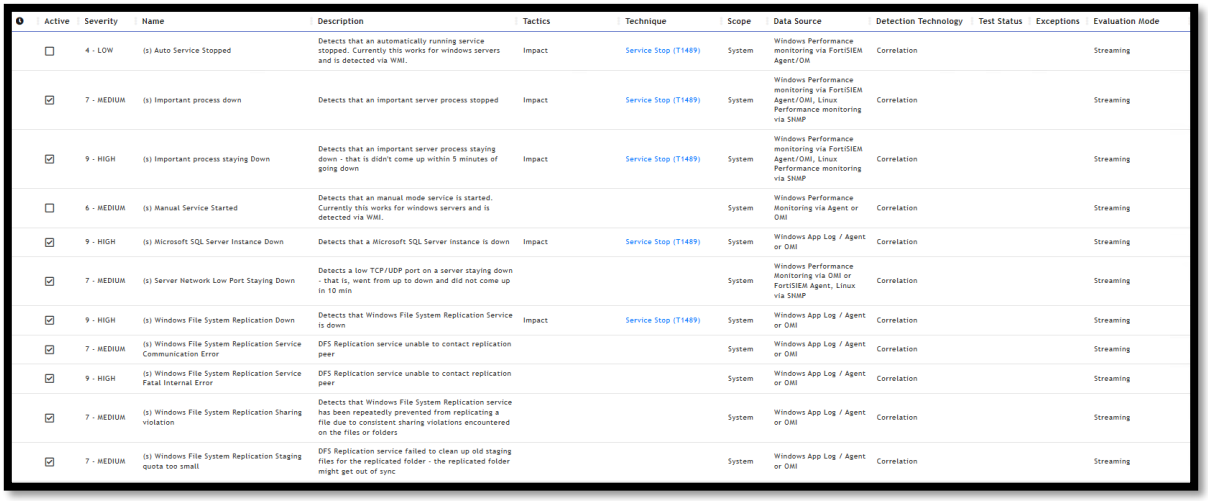
- **Uso excesivo de CPU o memoria (RAM)**, que puede indicar aplicaciones fuera de control, procesos maliciosos o configuraciones inadecuadas.
- **Latencia o errores de entrada/salida en disco**, que pueden reflejar problemas con el hardware de almacenamiento o cuellos de botella en el rendimiento de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

- **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.



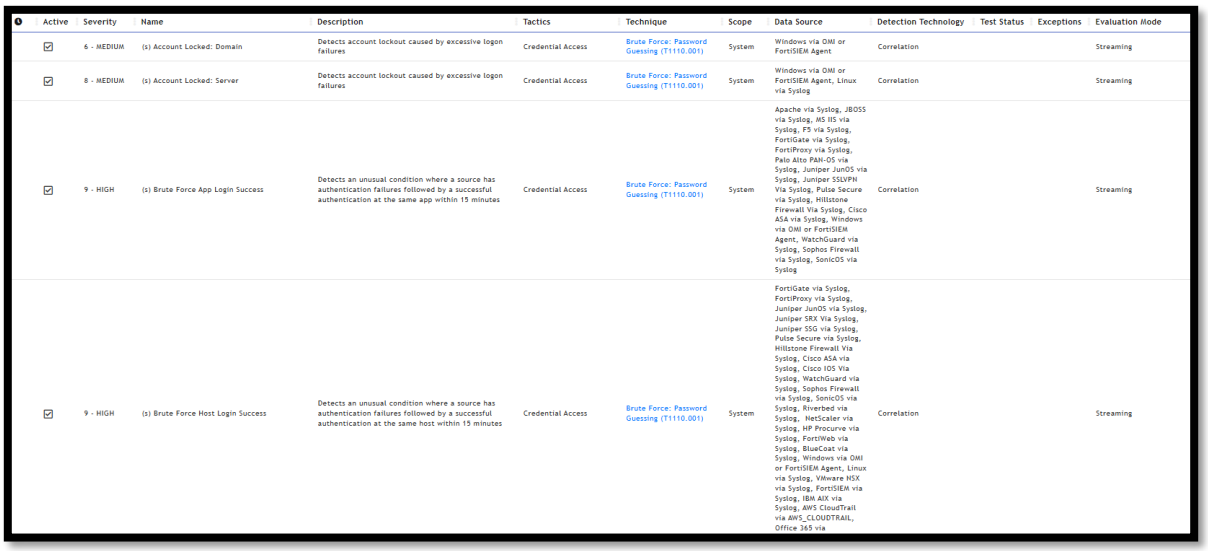
Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☐	4 - LOW	(s) Auto Service Stopped	Detects that an automatically running service stopped. Currently this works for windows servers and is detected via WMI.	Impact	Service Stop (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 *210* Disponibilidad

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:

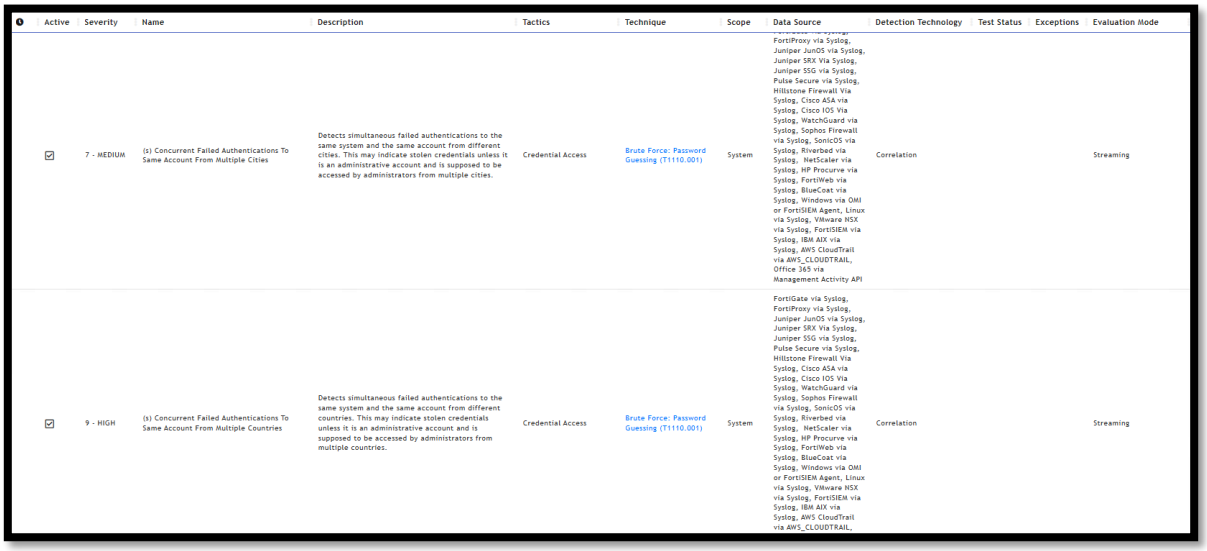
Los casos de uso de seguridad de autenticación en el FortiSIEM se centran en garantizar la integridad y la autenticidad de las credenciales de usuario en todos los dispositivos que tienen instalado el agente. Se muestran los casos Autenticación configurados para el ministerio de trabajo:



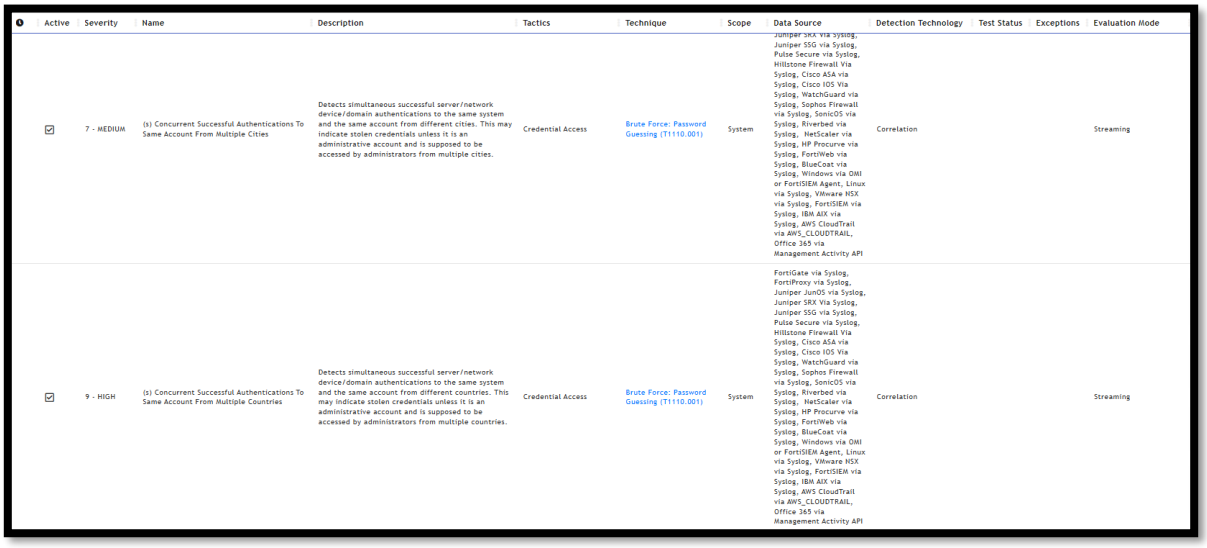
Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☑	6 - MEDIUM	(s) Account Locked: Domain	Detects account lockout caused by excessive logon failures	Credential Access	Brute Force: Password Guessing (T1110.001)	System	Windows 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 HSX via Syslog, FortiSIEM via Syslog, IBM AIX via Syslog, AWS CloudTrail via AWS_CLOUDTRAIL, Office 365 via	Correlation			Streaming

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.

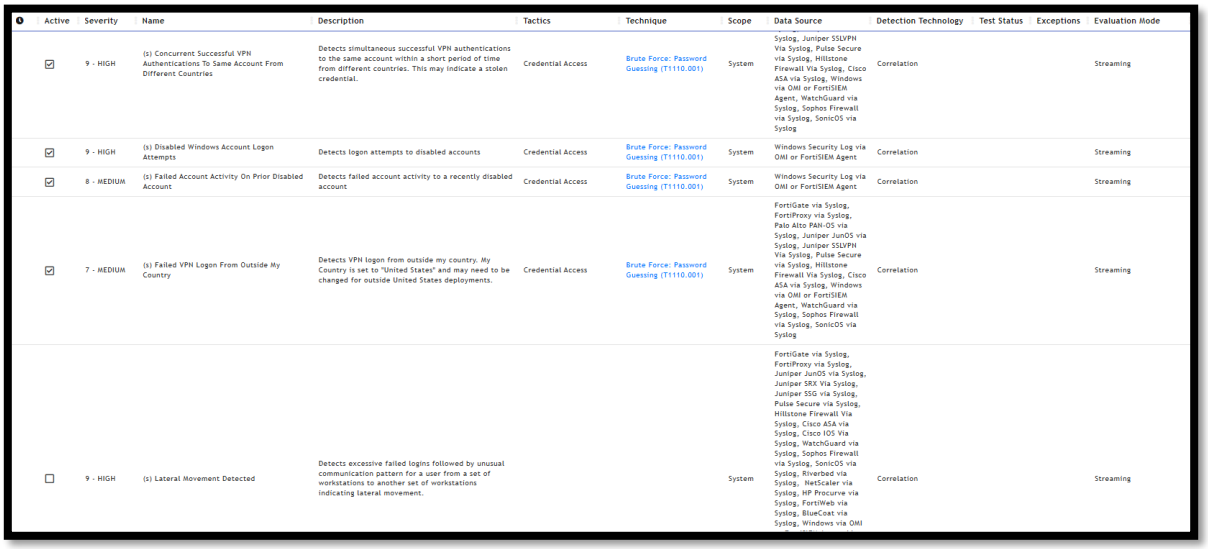
También se reportan bloqueos de cuentas por intentos excesivos de inicio de sesión fallido, lo que puede interrumpir servicios críticos.



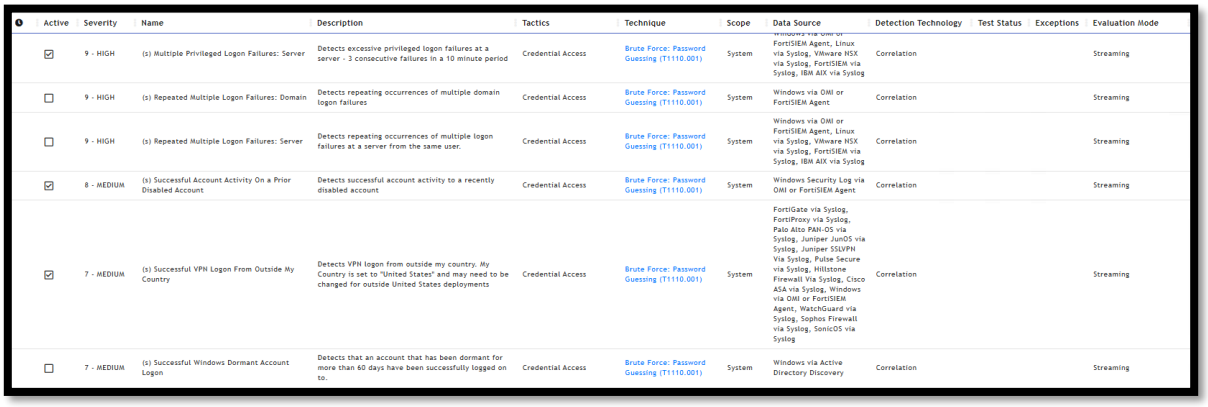
Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☑	7 - MEDIUM	(s) Concurrent Failed Authentications To Same Account From Multiple Cities	Detects simultaneous failed authentications to the same system and the same account 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 via AWS_CLOUDTRAIL,	Correlation			Streaming



Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☑	7 - MEDIUM	(s) Concurrent Successful Authentications To Same Account From Multiple Cities	Detects simultaneous successful server/network device/domain 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	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 Successful Authentications To Same Account From Multiple Countries	Detects simultaneous successful server/network device/domain 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 via AWS_CLOUDTRAIL, Office 365 via Management Activity API	Correlation			Streaming



Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☑	9 - HIGH	(s) Concurrent Successful VPN Authentications To Same Account From Different Countries	Detects simultaneous successful VPN authentications to the same account within a short period of time from different countries. This may indicate a stolen credential.	Credential Access	Brute Force: Password Guessing (T1110.001)	System	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) Disabled Windows Account Logon Attempts	Detects logon attempts to disabled accounts	Credential Access	Brute Force: Password Guessing (T1110.001)	System	Windows Security Log via OMI or FortiSIEM Agent	Correlation			Streaming
☑	8 - MEDIUM	(s) Failed Account Activity On Prior Disabled Account	Detects failed account activity to a recently disabled account	Credential Access	Brute Force: Password Guessing (T1110.001)	System	Windows Security Log via OMI or FortiSIEM Agent	Correlation			Streaming
☑	7 - MEDIUM	(s) Failed VPN Logon From Outside My Country	Detects VPN logon from outside my country. My Country is set to "United States" and may need to be changed for outside United States deployments.	Credential Access	Brute Force: Password Guessing (T1110.001)	System	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) Lateral Movement Detected	Detects excessive failed logins followed by unusual communication pattern for a user from a set of workstations to another set of workstations indicating lateral movement.			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	Correlation			Streaming



Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☑	9 - HIGH	(s) Multiple Privileged Logon Failures: Server	Detects excessive privileged logon failures at a server - 3 consecutive failures in a 10 minute period	Credential Access	Brute Force: Password Guessing (T1110.001)	System	FortiSIEM Agent, Linux via Syslog, VMware NSX via Syslog, FortiSIEM via Syslog, IBM AIX via Syslog	Correlation			Streaming
☐	9 - HIGH	(s) Repeated Multiple Logon Failures: Domain	Detects repeating occurrences of multiple domain logon failures	Credential Access	Brute Force: Password Guessing (T1110.001)	System	Windows via OMI or FortiSIEM Agent	Correlation			Streaming
☐	9 - HIGH	(s) Repeated Multiple Logon Failures: Server	Detects repeating occurrences of multiple logon failures at a server from the same user.	Credential Access	Brute Force: Password Guessing (T1110.001)	System	Windows via OMI or FortiSIEM Agent, Linux via Syslog, VMware NSX via Syslog, FortiSIEM via Syslog, IBM AIX via Syslog	Correlation			Streaming
☑	8 - MEDIUM	(s) Successful Account Activity On a Prior Disabled Account	Detects successful account activity to a recently disabled account	Credential Access	Brute Force: Password Guessing (T1110.001)	System	Windows Security Log via OMI or FortiSIEM Agent	Correlation			Streaming
☑	7 - MEDIUM	(s) Successful VPN Logon From Outside My Country	Detects VPN logon from outside my country. My Country is set to "United States" and may need to be changed for outside United States deployments	Credential Access	Brute Force: Password Guessing (T1110.001)	System	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
☐	7 - MEDIUM	(s) Successful Windows Dormant Account Logon	Detects that an account that has been dormant for more than 60 days have been successfully logged on to.	Credential Access	Brute Force: Password Guessing (T1110.001)	System	Windows via Active Directory Discovery	Correlation			Streaming

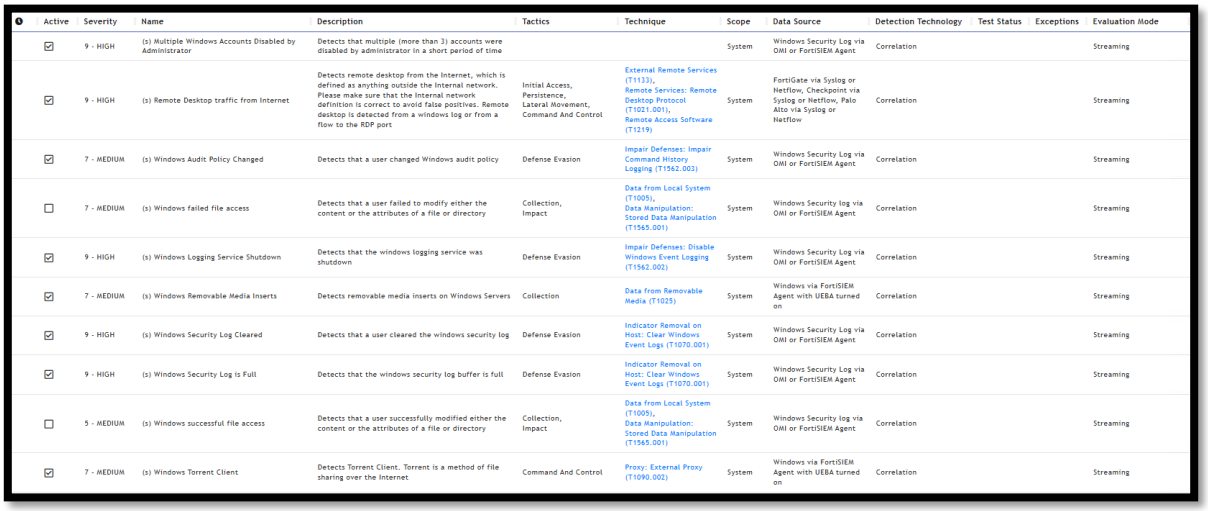
Ilustración *211* Autenticación de seguridad

Acciones tomadas:

- Se analiza inmediatamente los eventos de acceso a múltiples fallos, se crean casos de fuerza bruta en la herramienta de gestión Aranda.
- Se aplica límites de intentos de login, se implementa 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 implementa 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 on	Correlation			Streaming

Ilustración *212* Violación de políticas

Acciones realizadas:

- Se valida actividades de usuarios con privilegios que hayan deshabilitado cuentas o modificado políticas de auditoría con los especialistas de Windows.
- Se monitorear continuamente la integridad de los registros de eventos, aplicando controles que impidan su alteración mediante los equipos perimetrales.
- Se implemento controles para el uso de dispositivos USB y deshabilitar el uso de software no autorizado (ej. clientes torrent).

3.1.6.3.5. Overview incidentes

Durante el mes de junio, en el FortiSIEM se registraron eventos en la plataforma que podrían representar una amenaza para la seguridad de la red o la integridad de los sistemas monitoreados.

Se presentan algunos ejemplos de incidentes comunes por el FortiSIEM de MinTrabajo:

Prioridad	Alerta	Conteo	Descripción (Riesgo
Crítica	Domain Controller User/Group	126	Cambios no autorizados en AD (posible escalada de
	Traffic to Emerging Threat IP List	121	Comunicación con IPs maliciosas (riesgo de exfiltración o C2).
	Brute Force App/Host Login Success	20	Credenciales comprometidas (acceso no autorizado).
	Successful VPN Logon From Outside	5	Acceso VPN desde ubicaciones inusuales (posible
Media	Windows AD User Enumeration	6	Reconocimiento de usuarios (fase inicial de ataque a Kerberos o Golden Ticket).
	Office365: Suspicious File Type	2	Subida de archivos maliciosos (ej. .exe, macros) en
	Successful Activity on Disabled Account	1	Reactivación de cuenta deshabilitada (posible ataque interno).
Baja	End User DNS Queries to	9	Uso de DNS alternativos (evasión de filtros o
	A User Account Was Created	4	Creación de cuentas no autorizadas.
	Website Access Policy Violation	1	Acceso a sitios web bloqueados.

Ilustración *213* eventos detectados por el siem

Evento	Cantidad	Descripción
Permitted Traffic from Emerging Threat IP List	42	Se ha permitido tráfico desde IPs asociadas a amenazas emergentes, lo que sugiere falta de control o reglas de firewall no actualizadas.
Brute Force Host Login Success	16	Se identificaron intentos de fuerza bruta
Brute Force App Login Success	11	Accesos exitosos
Office365: Success Login Outside Colombia	9	Accesos legítimos desde ubicaciones internacionales, que pueden ser anómalos si no están autorizados.
Trend Vision One: Alert Severity 5 to 10	7	Alertas de alta criticidad en la plataforma Trend Micro (nivel 5 a 10).
Traffic to Emerging Threat IP List	5	Tráfico saliente hacia IPs maliciosas, por tal motivo fuero bloqueadas y cual puede indicar actividad de malware
Office365: Suspicious File Type Uploaded	2	Carga de archivos con extensiones riesgosas en servicios en la nube (ej: scripts, ejecutables).
Multiple Distinct IPS Events From Same Src	1	Un solo origen generó múltiples eventos detectados por el sistema de prevención de intrusos (IPS).

Tabla 68 eventos detectados por el SIEM

3.1.6.4.6 Top Disponibilidad de servidores

Esta 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 junio. 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:

- MTSISINFOPRU01: con aproximadamente 137 días de uptime.
- mintrab03 y MINTRAB94: también con tiempos cercanos a los 131 días.
- MINTRABGD06PD: con más de 125 días activos sin reinicio.

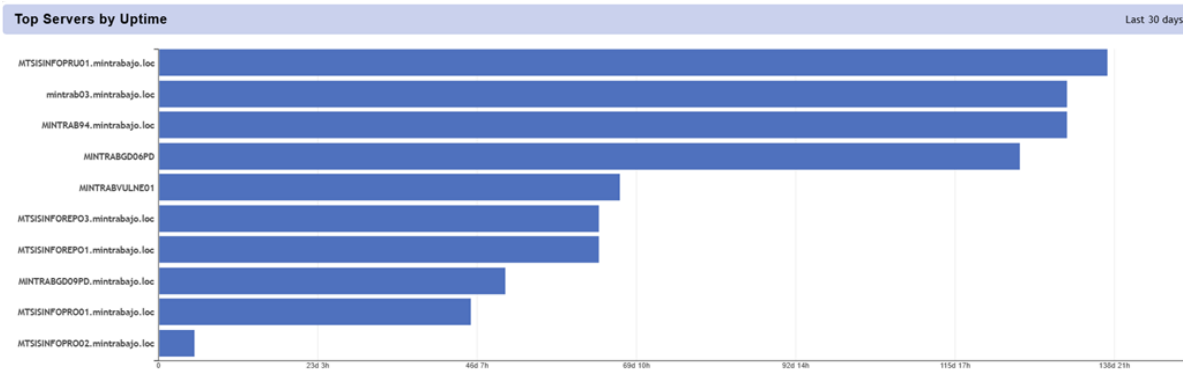


Ilustración 214 Disponibilidad de servidores- Seguridad

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:

- SSL, Network.Service: 117.85 TB
- HTTPS.BROWSER: 48.33 TB

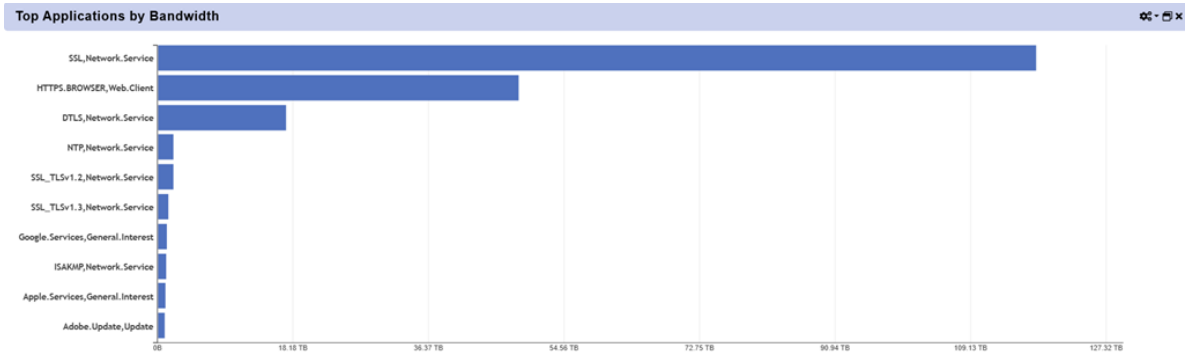


Ilustración 215 Top Aplicaciones por Bandwidth

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.

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

El Ilustración representa los tipos de ataques más comunes identificados a través del WAF por fecha en un período que abarca el mes de junio de 2025. A continuación, se presenta un análisis detallado:

- **Tipos de ataques detectados:**
- **Information Disclosure (verde):** Ataques relacionados con la divulgación no autorizada de información.
- **IP Reputation (amarillo):** Eventos relacionados con IPs identificadas con una reputación negativa.
- **Generic Attacks (azul):** Ataques genéricos no clasificados en categorías específicas.
- **Cross-Site Scripting (naranja):** Ataques que explotan vulnerabilidades XSS.

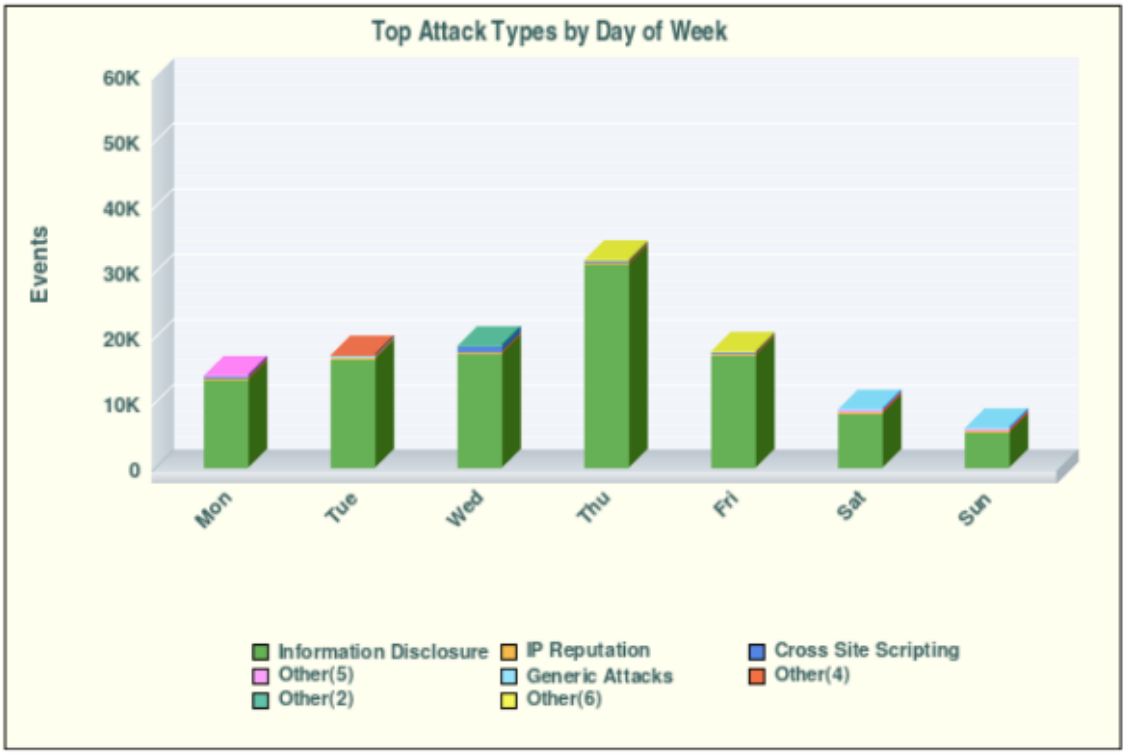


Ilustración 216 Top attack types

Information Disclosure (Divulgación de Información)

Eventos registrados: 636 (91.91% del total)

Descripción/Riesgo*:* Este tipo de incidente implica la exposición no intencional de datos sensibles, incluyendo metadatos, configuraciones de sistemas o archivos de registro.

Acciones tomadas*:* El equipo de seguridad está realizando una revisión exhaustiva de las configuraciones en servidores y aplicaciones web para identificar y corregir posibles fallos de configuración que puedan estar permitiendo estas filtraciones.

IP Reputation (Reputación de IP)

Eventos registrados: 25 (3.6% del total)

Descripción/Riesgo*:* Estos eventos corresponden a tráfico originado desde direcciones IP conocidas por su mal comportamiento, incluyendo bots, sistemas de escaneo o servidores de comando y control (C2).

Acciones tomadas: Se está implementando el bloqueo sistemático de estas IPs maliciosas mediante listas de amenazas actualizadas en nuestros firewalls perimetrales.

Cross Site Scripting (XSS)

Eventos registrados: 150 (3.72% del total)

***Descripción/Riesgo**:* Estos son intentos de inyección de scripts maliciosos en nuestras aplicaciones web, que podrían permitir a atacantes ejecutar código arbitrario en el contexto de los usuarios.

***Acciones tomadas**:* Se están implementando medidas de protección contra XSS, incluyendo la validación estricta de entradas y la implementación de políticas de seguridad de contenido.

3.1.6.5. Solución de Anti-DDoS

Durante el período del mes de junio, no se registraron eventos de ataques de denegación de servicio distribuido (DDoS) a las aplicaciones publicadas en internet por el Ministerio de Trabajo.

Top Attacked Subnets

Subnet	SPP	Direction	Drops	Events
4	Acceso_Web	Inbound	28,349	8
1	PAGINA_MINTRABAJO	Inbound	4,531	9
1	APP_MINT	Inbound	1,158	9
1	MOODLE	Inbound	56	4
1	GESTOR_DOC_MINT	Inbound	18	4
1	SVE	Inbound	4	2
1	COBRO_COACTIVO	Inbound	1	1

Ilustración 217 Top de ataques

Análisis Detallado:

Acceso_Web concentra el mayor número de paquetes bloqueados (28.349), lo que indica posible comportamiento anómalo o intento de exfiltración de datos hacia internet.

PAGINA_MINTRABAJO también muestra un número considerable de intentos salientes bloqueados, lo que sugiere riesgo en aplicaciones web institucionales.

APP_MINT y MOODLE tienen actividad considerable, probablemente debido a su naturaleza dinámica y de acceso frecuente por usuarios.

Los demás servicios muestran volúmenes más bajos, pero no deben ignorarse, especialmente si las aplicaciones manejan datos sensibles (ej. COBRO_COACTIVO, GESTOR_DOC_MINT).

3.1.6.6.2 Login Fallidos

Durante el mes de junio, se registraron varios eventos de inicio de sesión fallidos, los cuales 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:

Top Failed Logins

User	UI	Date	Time
dfcavanzo@css_e	GUI(172.30.31.6)	2025-07-04	12:30:39
admin	GUI(10.105.116.150)	2025-06-12	11:00:09
admin	GUI(10.105.116.150)	2025-06-12	11:00:07
admin	GUI(10.105.116.150)	2025-06-12	11:00:03
jlguiza@css_e	GUI(10.105.116.150)	2025-06-12	10:59:49
admin	GUI(172.30.31.2)	2025-05-23	22:22:23
dfcavanzo@css_e	GUI(172.30.31.5)	2025-05-02	12:37:57
admin	GUI(172.30.31.6)	2025-04-11	15:45:48
dfcavanzo@css_e	GUI(172.30.31.8)	2025-03-04	12:48:06
dfcavanzo@css_e	GUI(172.30.31.10)	2025-03-03	17:48:32

Ilustración 218 Login fallidos

3.1.6.6. Casos atendidos de los servicios de seguridad

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

3.1.6.6.1. Incidentes

Durante el mes de junio no se registraron incidentes atendidos dentro del servicios de seguridad informática:

3.1.6.6.2. Requerimientos

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

Caso	Fecha de registro	Asunto	Grupo responsable	Categoría
RFC-126592	16/06/2025 0:00	RFC Actualización firmware WAF Data center Colombia xv	SOC	Firewall de aplicaciones Web - WAF
RF-123669	4/06/2025 0:00	Solicitud de Enrutamiento	SOC	Ajuste de configuraciones (Crear - Eliminar)
RF-126839	17/06/2025 0:00	RE: GESTION - Solicitud autorización tráfico servidor OCI a la URL de la SVE - RF-118593	SOC	Agregar a sitios permitidos
RF-128035	20/06/2025 0:00	Solicitud de bloqueo de dominios e IP asociados a contenido no autorizado (piratería) Magistv	SOC	Crear politica
RF-129732	27/06/2025 0:00	RE: Sobre el caso RF-126839 (antes RF-118593) Sobre activación tráfico servidor OCI a la URL de la SVE	SOC	Permitir acceso
RF-123909	5/06/2025 0:00	Solicitud de instalación de software en equipo local	SOC	Permitir acceso
RF-127597	19/06/2025 0:00	Solicitud configuración perimetral	SOC	Permitir acceso
RF-128623	24/06/2025 0:00	Mintrabajo LTP:RED Campaña de distribución del infostealer Massloger: ataque sigiloso mediante VBScript	SOC	Restringir servicio

RF-126117	13/06/2025 0:00	Agregar ip 172.18.50.151 a la política de seguridad con ID 193	SOC	Autorización nuevo software
RF-123708	4/06/2025 0:00	RV: Informe de control administrativo – Radicado 11001-28-05-01688	SOC	Revisar correo malicioso
RF-125873	12/06/2025 0:00	RV: Notificación de inicio de cobro coactivo – Radicado 11001-28-05-01855	SOC	Revisar correo malicioso
RF-123629	4/06/2025 0:00	Posible correo sospechoso.	SOC	Análisis de Correos
RF-126041	13/06/2025 0:00	Revision de correo	SOC	Análisis de Correos
RF-126473	16/06/2025 0:00	favor verificar ese correo si es malicioso	SOC	Análisis de Correos
RF-127515	18/06/2025 0:00	MINTRABAJO TLP:RED Gunra realiza actividades de ransomware en Colombia	SOC	Configuracion consola
RF-123854	5/06/2025 0:00	Política de acceso a internet equipos contraloría	SOC	Crear politicas
RF-123449	4/06/2025 0:00	Aprovisionamiento de aplicaciones en el WAF	SOC	Ajuste de configuraciones (Crear - Eliminar)
RF-124146	6/06/2025 0:00	Solicitud de depuración de Hostname en plataforma Micro Trend	SOC	Falla - error
RF-124800	9/06/2025 0:00	Re: Acceso a servidores que están conectados a la VPN del DNP	SOC	Falla conexión VPN

Tabla.69 Listado de requerimientos atendidos

3.1.6.7 Análisis de riesgo

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

- **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.70 Ejecución de archivos maliciosos

- **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.71 Vulnerabilidades en la infraestructura

- **Ataques de Phishing dirigidos**

Riesgo	Impacto	Probabilidad
Intentos de phishing dirigidos a altos funcionarios, como la ministra de Trabajo, con el objetivo de robo de credenciales o entrega de malware.	Acceso no autorizado a sistemas sensibles y posible compromiso de datos confidenciales	Alta, debido al uso constante de correos electrónicos en la comunicación oficial.

Tabla.72 Ataque de Phishing dirigidos

2. Medidas de Mitigación Recomendadas

Control y restricción de archivos ejecutables:

- Se realizó plan de trabajo para Implementar restricciones de ejecución de ejecutables en servidores y estaciones de trabajo.

- Se realizó unas listas blancas de software permitido.
- Monitoreo y análisis continuo de archivos sospechosos.

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

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

3.1.6.8 Políticas y procedimiento de seguridad

Dentro las activades realizadas en el mes de junio, se realizó la revisión, ajuste, observaciones de algunos procedimientos y políticas que describimos a continuación;

- 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 969 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.

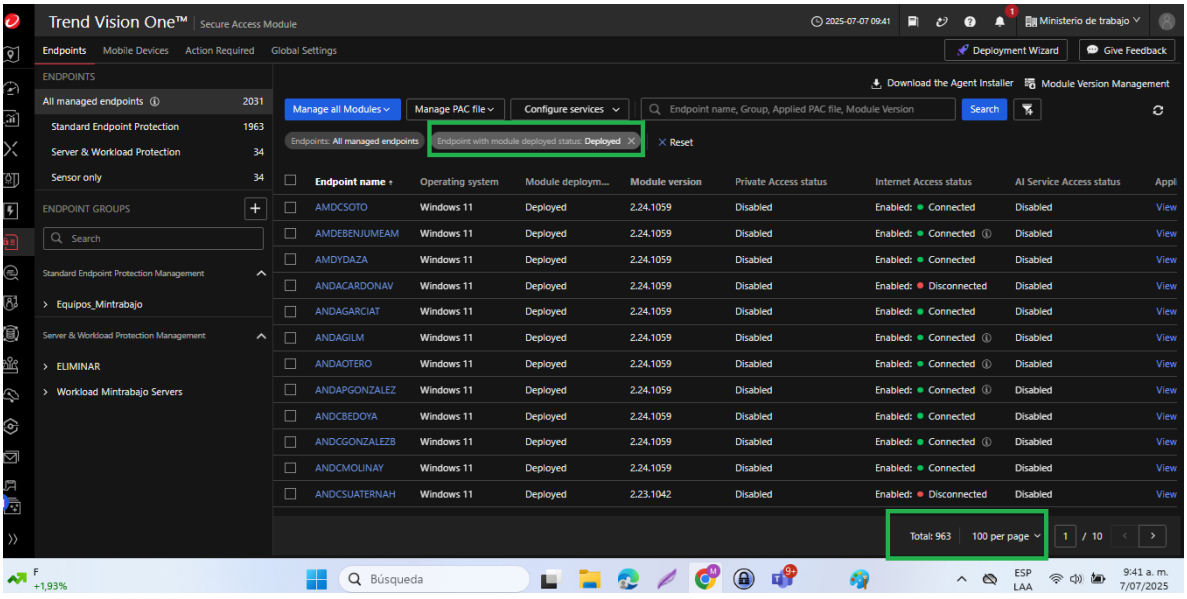


Ilustración 219 Políticas y procedimiento de seguridad

Bloqueo de IoCs Campaña de distribución del infostealer Massloger: ataque sigiloso mediante VBScript (24/06/2025)
Se implementó bloqueo de Indicadores de Compromiso (IoC) asociados a malware **Massloger** en:

- Firewall: @Usuario Genérico cybersecg2
- Trend Micro: @Bocanegra Pinzon, Saul
- Caso de seguimiento: RF-128623 en herramienta Aranda
- Hallazgo: La mayoría de IoCs ya eran detectados proactivamente por Trend Micro (evidencia adjunta)

Boletín Vulnerabilidades afectan a sistemas operativos Linux (20/06/2025)

- Se ejecutaron acciones de mitigación:
  Se valida la vulnerabilidade presentada y se logra observar que el usuario root se encuentra deshabilitado en cada uno de los servidores Linux con distribución Enterprise Linux, los Debian se encuentran en fase de migración.
- Caso de seguimiento: RF-128090 en herramienta Aranda

Solicitud de bloqueo de dominios e IP asociados a contenido no autorizado (piratería) Magistv (20/06/2025)

- Firewall: @Usuario Genérico cybersecg2
- Trend Micro: @Bocanegra Pinzon, Saul
- Caso de seguimiento: RF-128035 en herramienta Aranda
- Hallazgo: La mayoría de IoCs ya eran detectados proactivamente por Trend Micro (evidencia adjunta)

Boletín Ciberdelincuentes RED Gunra realiza actividades de ransomware en Colombia. (20/05/2025**)**

Desde el equipo de Cyber Threat Intelligence, compartimos el siguiente boletín sobre las actividades del grupo de ransomware Gunra realizadas recientemente en Colombia, contra entidades como la Superintendencia de la Economía Solidaria (@supersolidaria_), organismo público descentralizado adscrito al Ministerio de Hacienda, que supervisa las actividades financieras del sector de la economía solidaria. Además, el grupo afirma haber hackeado 45TB de datos de la Justicia Penal Militar y Policial de Colombia (@JPMP_Colombia), encargada de investigar y juzgar conductas punibles de miembros de la Fuerza Pública. Aunque no en Colombia, el grupo también ha sido vinculado a un ciberataque contra el American Hospital Dubai (@AHDubai), un centro de salud líder en Dubái, EAU.

Mitigación:
Bloquear los IoCs adjuntos en:

- *Firewall:* @Usuario Genérico cybersecg2
- *Trend Vision One:* @Bocanegra Pinzon, Saul & @Velasquez Guevara, Miller Alexander

Este boletín fue distribuido internamente el 18/06/2025 como parte de las alertas proactivas del equipo CTI.

3.1.7. Licenciamiento

A continuación, se presenta la información del licenciamiento:

Licencia	Referencia	Fecha de Vigencia	Estado
IBM (10896)	Del 01/06/2023 hasta el 31/07/2026	Vigente	**IBM (10896)**
LIFERAY	Del 01/08/2024 hasta el 31/07/2025	Vigente	**LIFERAY**

Tabla 73 Licenciamiento

3.1.8. Administración, soporte y monitoreo

- Servidores

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

- 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 realizó actualización de la base de datos indicando el nombre del especialista a quien deben reportarse las indisponibilidades y a quien deben llegar los alertamientos automáticos de la herramienta Zabbix, se da visibilidad al NOC de la misma para el escalamiento para ser asertivos en las asignaciones a los profesionales de servicios centrales para su atención.

Se ajustaron nuevos umbrales para diferentes aplicaciones y servicios a nivel de bases de datos MSSQL Server.

- Almacenamiento

Se agregan monitoreos sobre almacenamientos y datastore para establecer seguimiento de las holguras de crecimiento.

• 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	99,84%	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	100,00%	90,00%
DC-10	Tiempo de solución de requerimientos asociado a los servicios de administración, soporte y monitoreo	100,00%	90,00%
DC-11	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 74 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 75 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.

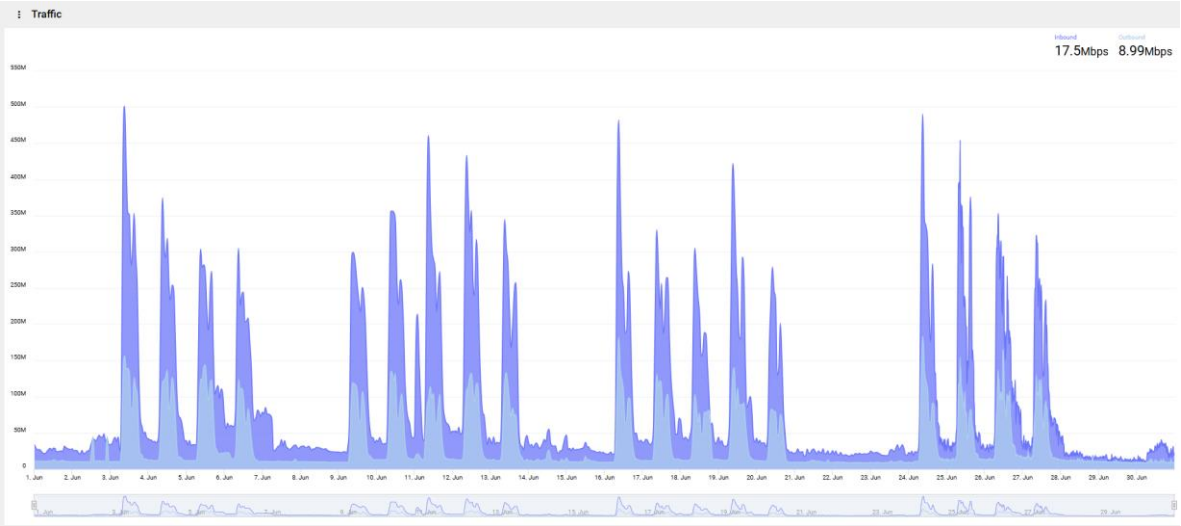


Ilustración 220. Grafica de consumo canal MPLS Datacenter

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

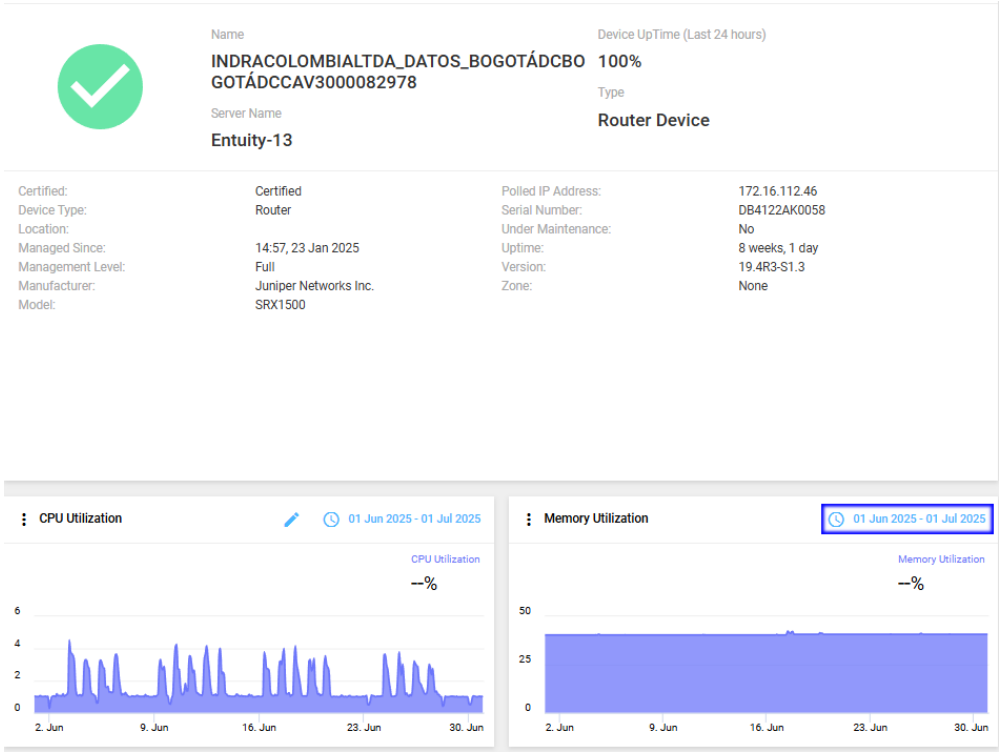


Ilustración 221 Uptime del equipo MPLS Datacenter

3.3.1.1. Incidentes de Conectividad

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

Dirección territorial	Caso Asociado	Disponibilidad
Andes	IM-127531	98,63%
Cisneros	IM-125390	67,70%
Santa Rosa	IM-126810	92,21%
Tame	IM-128867	96,59%
Baranoa	IM-127398	98,08%
Carmen De Bolívar	IM-123601	99,16%
La Dorada	IM-127135	99,50%
El Bordo Patía	IM-127398	89,27%
Santander De Quilichao	IM-127135	99,49%
Tocancipá	IM-127691	76,33%
Ubaté	IM-124125	72,50%
Villeta	IM-127135	99,50%
Granada	IM-125777	98,80%
Ipiales	IM-127135	98,89%
La Unión	IM-126715	93,81%
Los Patios	IM-127398	89,71%

Pamplona	IM-129400	97,38%
Orito	IM-127135	99,50%
Dosquebradas	IM-127135	99,50%
La Virginia	IM-127135	99,50%
Barbosa	IM-129182	43,13%
Puerto Wilches	IM-127398	89,27%
Sabana De Torres	IM-127891	99,45%
Socorro	IM-127891	99,45%
Espinal	IM-127135	99,50%
Mariquita	IM-127192	96,66%
Cartago	IM-127135	99,50%
Palmira	IM-127135	99,50%
Sevilla	IM-127135	99,50%
Tuluá	IM-127135	99,50%

Tabla 76 Novedades servicio de internet

3.3.1.2. Topología Actual

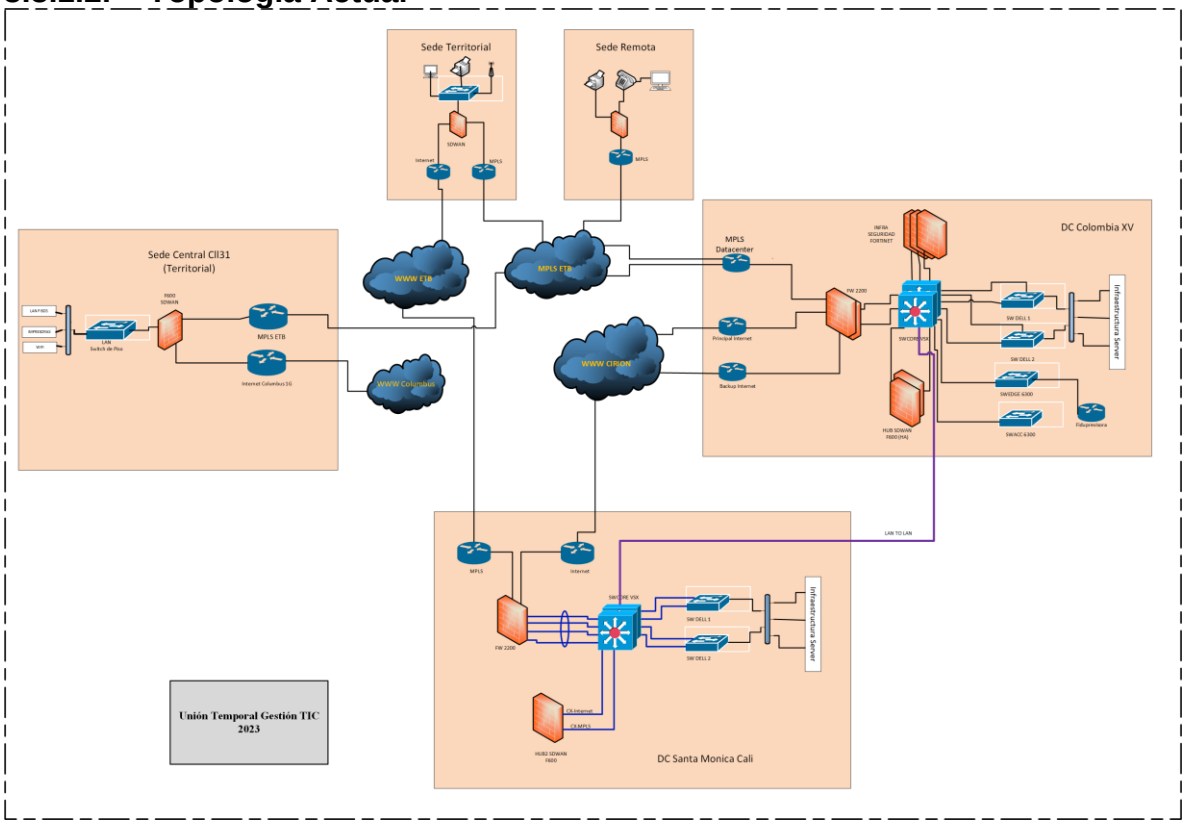


Ilustración 222. Topología actualizada

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, al igual que el estado de los túneles SDWAN establecidos contra el HUB SDWAN en Datacenter, se tienen 150 equipos registrados en esta plataforma.

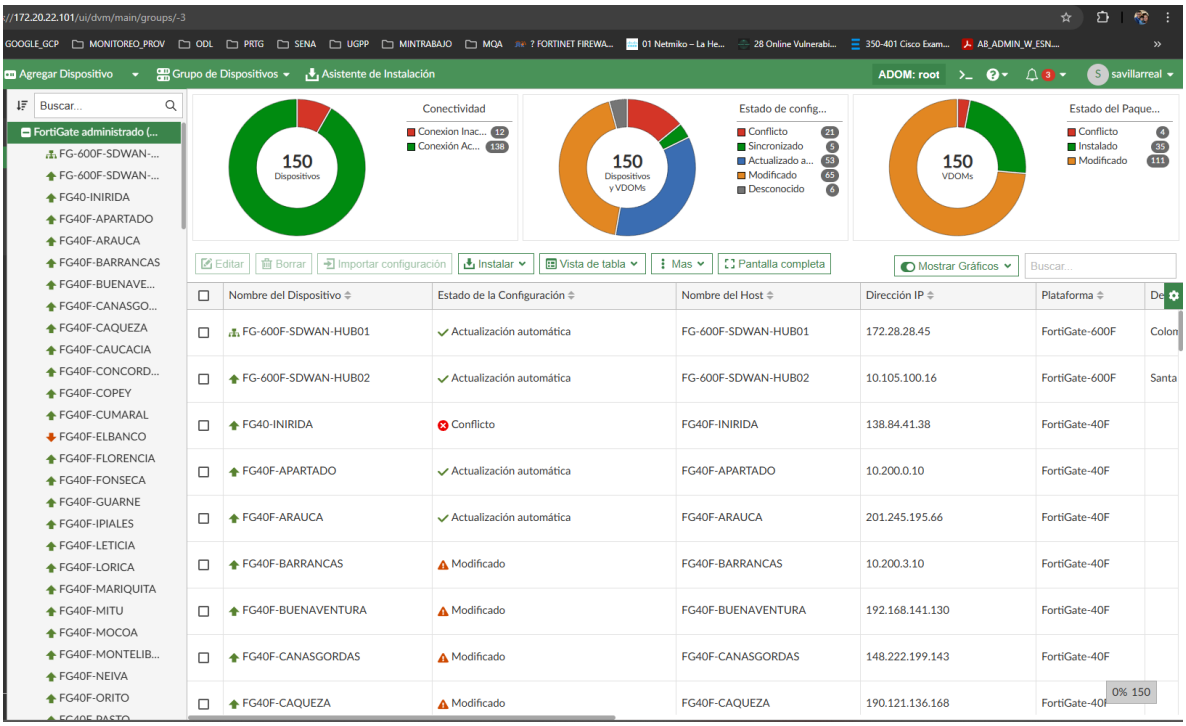


Ilustración 223. Interface Fortimanager

Desde el HUB SDWAN F600, en datacenter se observa el consumo promedio del canal MPLS, donde no se presenta saturación.

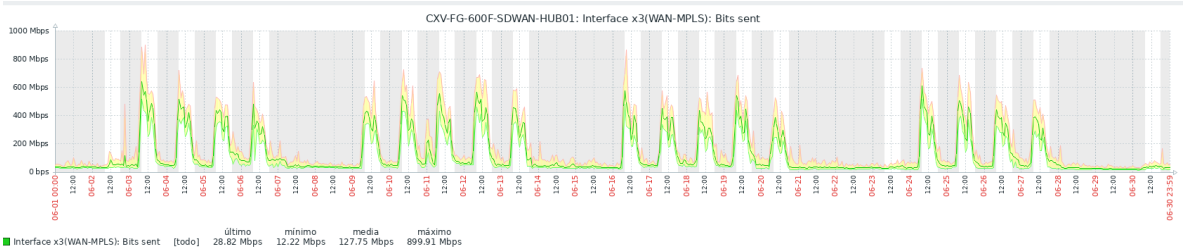


Ilustración 224. Interface MPLS HUB SDWAN

De igual forma, la interface de Internet del HUB no presenta saturación, por esta interface se establece el túnel Backup de las sedes territoriales.

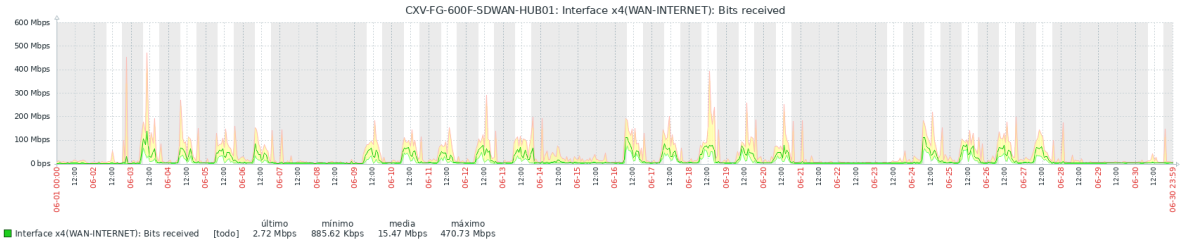


Ilustración 225 Interface Internet HUB SDWAN

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



Ilustración 226. VPN SDWAN establecidas

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

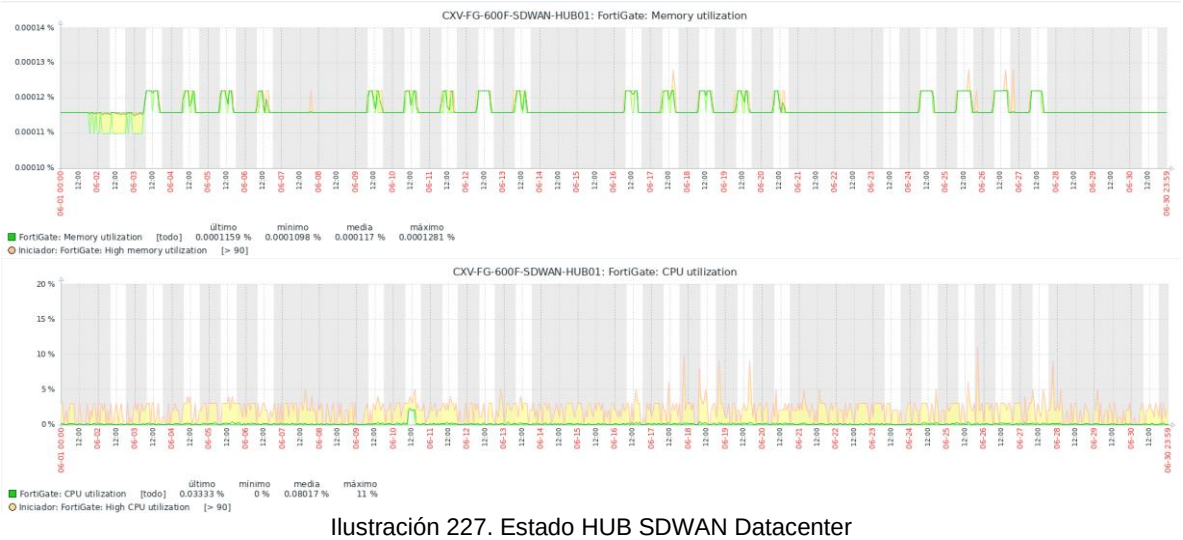


Ilustración 227. Estado HUB SDWAN Datacenter

Se verifica el estado del HA del equipo, donde se observa que se encuentra establecido y sincronizado.

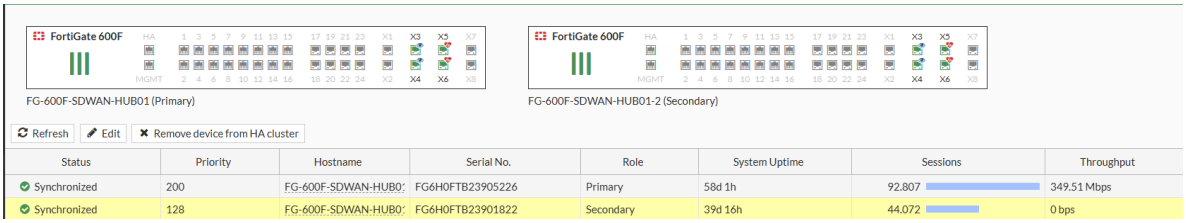


Ilustración 228. Estado HA HUB Sdwan

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

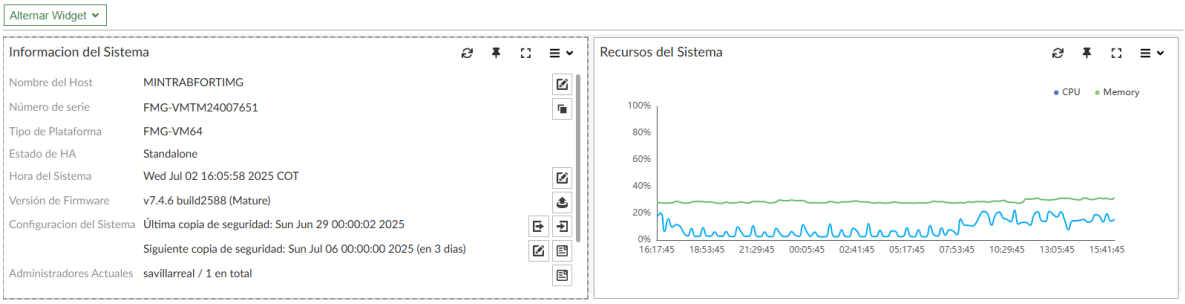


Ilustración 229. Recursos Fortimanager

- **Medición de ANS Conectividad WAN e Internet**

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

ID	Indicadores	Resultado	Meta
CWI-1	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
CWI-2	Continuidad y disponibilidad del servicio de WAN en sedes nacionales con un solo enlace	(*)	99,60%
CWI-3	Continuidad y disponibilidad del servicio de WAN en sedes nacionales con doble enlace (principal MPLS + secundario Internet dedicado)	100,00%	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 77 Medición de ANS Conectividad WAN e Internet

(*) De acuerdo con la solicitud de la Coordinadora 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 junio:

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

Dirección territorial	Caso Asociado	Disponibilidad	% Penalidad	Valor Penalidad un enlace
Andes	IM-127531	98,63%	3%	$ 9.240
Cisneros	IM-125390	67,70%	100%	$ 308.015
Santa Rosa	IM-126810	92,21%	10%	$ 30.801
Tame	IM-128867	96,59%	10%	$ 30.801
Baranoa	IM-127398	98,08%	3%	$ 9.240
Carmen De Bolívar	IM-123601	99,16%	3%	$ 9.240
La Dorada	IM-127135	99,50%	3%	$ 9.240
El Bordo Patía	IM-127398	89,27%	3%	$ 9.240
Santander De Quilichao	IM-127135	99,49%	3%	$ 23.101
Tocancipá	IM-127691	76,33%	20%	$ 61.603
Ubaté	IM-124125	72,50%	50%	$ 154.007
Villeta	IM-127135	99,50%	3%	$ 9.240

Dirección territorial	Caso Asociado	Disponibilidad	% Penalidad	Valor Penalidad un enlace
Granada	IM-125777	98,80%	3%	$ 9.240
Ipiales	IM-127135	98,89%	3%	$ 9.240
La Unión	IM-126715	93,81%	10%	$ 30.801
Los Patios	IM-127398	89,71%	10%	$ 30.801
Pamplona	IM-129400	97,38%	3%	$ 9.240
Orito	IM-127135	99,50%	3%	$ 9.240
Dosquebradas	IM-127135	99,50%	3%	$ 9.240
La Virginia	IM-127135	99,50%	3%	$ 9.240
Barbosa	IM-129182	43,13%	100%	$ 308.015
Puerto Wilches	IM-127398	89,27%	10%	$ 30.801
Sabana De Torres	IM-127891	99,45%	3%	$ 9.240
Socorro	IM-127891	99,45%	3%	$ 9.240
Espinal	IM-127135	99,50%	3%	$ 9.240
Mariquita	IM-127192	96,66%	10%	$ 30.801
Cartago	IM-127135	99,50%	3%	$ 9.240
Palmira	IM-127135	99,50%	3%	$ 9.240
Sevilla	IM-127135	99,50%	3%	$ 9.240
Tuluá	IM-127135	99,50%	3%	$ 9.240
Total				**$ 1.215.107**

Tabla 78 Desagregado sedes con novedad un solo enlace

CWI-3 Continuidad y disponibilidad del servicio de WAN en sedes nacionales con doble enlace el valor del ANS para el mes de junio de 2025 es de 100% no se presentaron novedades con los enlaces.

4. LINEA DE SERVICIOS EN SEDE

4.1. Equipos de Cómputo de usuario final

Durante el periodo del informe, la Unión Temporal (UT) atendió las solicitudes de revisión, pruebas, retiro y asignación de equipos de cómputo, y se brindó soporte a las novedades presentadas por el parque computacional Lenovo.

A continuación, se relacionan los equipos en operación durante el periodo, de acuerdo con el Anexo de Distribución de Equipos, detallado de la siguiente manera:

Ítem	Cantidad
Computador portátil (morral, guaya y diadema)	1000
Computador escritorio (monitor, CPU, teclado, mouse y diadema)	1172
Computadores portátiles adicionales (puntuables)	120
Total	**2292**

Tabla 79 Cantidades de equipos a distribuir a nivel nacional

Las actividades ejecutadas durante el periodo en relación con el servicio incluyeron:

Gestión de Inventario:

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

ASIGNACION DE EQUIPOS JUNIO		
SEDE	**TIPO DE ELEMENTO**	**CANTIDAD**
Manizales	Escritorio	2
Valledupar	Escritorio	1
Cali	Escritorio	1
Nivel central	Portátil	8
DT Bogotá	Escritorio	2
DT Bogotá	Portátil	1

Tabla 80 Cantidades de equipos asignados nivel nacional

DEVOLUCION DE EQUIPOS JUNIO		
SEDE	**TIPO DE ELEMENTO**	**CANTIDAD**
Cartagena	Portátil	1
Cúcuta	Portátil	1
Pasto	Portátil	1
Armenia	Escritorio	1
Armenia	Portátil	2
Nivel central	Portátil	14

Tabla 81 Cantidades de equipos por devolución nivel nacional

- **Consolidación de actas de entrega y devolución**: Se consolidaron las actas de entrega y devolución en formato digital, almacenándolas en el repositorio del Nivel Central.

Gestión de Garantías:

Durante el mes de junio, se reportó un total de 16 casos de garantía a corte del periodo. A continuación, se detallan los estados asociados a estos casos:

Estado de caso	Cantidad
Cerrado	9
Suspendido	7
Total	**16**

Tabla 82 Estado de casos de garantía.

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

ANS	Cerrado	Suspendido	Total
CUMPLE	9	6	15
NO CUMPLE	0	1	1
Total	9	7	16

Tabla 83 ANS casos de garantía.

Fecha de reporte	Serial	Parte	Falla	Sede	Ticket Aranda	Estado	Caso Lenovo	Observación
03/06/2025	HC3BBL5T	Diadema	Uno de los lados no se escucha	Apartado	RF-123214	Solucionado		Serial nueva diadema HC3BBL7R
03/06/2025	HC3B97NG	Diadema	Se percibe un sonido obsoleto que afecta su uso	Apartado	RF-123090	Solucionado		Serial nueva diadema HC3BBNCP
04/06/2025	VNAA64AD	Monitor	línea horizontal en la mitad de la pantalla	Montelíbano/cordoba	RF-123690	Solucionado	2025664409	Se reemplaza equipo monitor por S/N VNABD100
04/06/2025	HC3BBKV7	Diadema	Falla en sonido	Cartagena	RF-123531	Solucionado		Serial nueva diadema HC3BBM5V
06/06/2025	VNAA6287	Monitor	Informa de que la mitad de la pantalla le aparece de color Rosado intermitente	Cali	RF-124195	Solucionado	2025664434	Se reemplaza equipo monitor por S/N: VNABD0N
11/06/2025	VNAA62G3	Monitor	pantalla empezó a parpadear repentinamente	Meta/Villavicencio	RF-125605	Suspendido	2026057135	Pendiente visita Lenovo
12/06/2025	HC3BBLCD	Diadema	suenan con distorsión	Cali	RF-125987	Solucionado		Serial nueva diadema: HC3BBMVA,
16/06/2025	HC3BBM9Z	Diadema	Sonido degradado	Nivel central	RF-126418	Solucionado		Serial nueva diadema HC3BBL3X
18/06/2025	VNAA62N8	Monitor	salió una franja horizontal en el centro de la pantalla de colores verdes	Huila/ Neiva	RF-126894	Solucionado	2025852918	Se reemplaza por equipo monitor de S/N: VNABD11H
19/06/2025	VNAA62P8	Monitor	Falla en monitor con líneas horizontales y distorsionada.	Riosucio/Caldas	RF-127664	Suspendido	2025890115	Pendiente visita Lenovo
19/06/2025	AVLC3C5A2FC	Teclado	Dejo de funcionar	Boyacá/Tunja	RF-127673	Suspendido		Pendiente visita de Lenovo
20/06/2025	HC3B8DNN	Diadema	Falla en el micrófono	Sincelejo	RF-128120	Suspendido		Pendiente llegada de la diadema nueva
25/06/2025	PW09Z34K	Portátil	Equipo no reconoce el cargador	nivel central	RF-128999	Suspendido	2026003370	
25/06/2025	PW0A3BK3	Portátil	Falla en puerto de carga	Nivel central	RF-128934	Suspendido	2026050218	
27/06/2025	HC3BBL1P	Diadema	Dejo de funcionar	Cúcuta	RF-129548	Suspendido		Pendiente llegada de la diadema nueva

Tabla 84 ANS Relación casos de garantía

Siniestros:

Durante la ejecución del contrato, se han presentado diversas novedades relacionadas con los equipos de cómputo. Estas incidencias son atribuibles al uso por parte del usuario y natural. A continuación, se detalla el estado actual de cada una de ellas:

Funcionario	Equipo	DT	Parte afectada	ESTADO	Caso Aseguradora/Lenovo
Lacides Manuel Morales Ortega	MJ0LS5XL	Sincelejo/San Marcos	Se apaga y no enciende	Reportada ante la aseguradora	PRG_2025_1921454
Jesus Manuel Martinez Franco	PW0A3BEY	Monteria	Golpes en esquinas	Pendiente visita de Lenovo	2025347408

Adriana Patricia Martínez Arévalo	PW09Z369	Nivel central	Equipo no da imagen	Reportada ante aseguradora	PRG_2025_2251570
Ana Mireya Escobar Tierradentro	MJ0S5TW	Popayan/Cauca	No enciende	Reportada ante aseguradora	PRG_2025_1766918
Pavel Santodomingo	PW0A3CDZ	Nivel central	Derrame de líquidos	Pendiente visita de Lenovo	2025046910
Bernardo Ardila Fernandez	PW09Z34H	Valledupar	Golpes en esquinas	Pendiente visita de Lenovo	2024554288
Juan Baudilio Simbaqueba Vargas	PW0A3CG6	Nivel central	Falla que no se ha logrado dar solucion	Pendiente visita de Lenovo	

Tabla 85 ANS Equipos en siniestro

Instalaciones de Equipos y Entrega a Usuarios Finales:

A continuación, se presenta el parque computacional instalado en la entidad al corte del periodo del informe:

Tipo de equipo	Instalados
Portátil	887
Escritorio	1104
Total	1991

Tabla 86 *Avance instalación de equipos*

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

**Devoluciones por novedades de personal: ** En el transcurso del mes, se gestionaron devoluciones de elementos asociados a novedades de funcionarios, tales como retiros, jubilaciones, entre otros.

DEVOLUCION DE EQUIPOS JUNIO		
SEDE	TIPO DE ELEMENTO	CANTIDAD
Cartagena	Portátil	1
Cúcuta	Portátil	1
Pasto	Portátil	1
Armenia	Escritorio	1
Armenia	Portátil	2
Nivel central	Portátil	14

CANTIDAD DE EQUIPOS		
LUGAR	PORTATIL	ESCRITORIO
ALMACEN	**233**	**68**
OPERACIÓN	**887**	**1104**
TOTAL	**1120**	**1172**

4.1.1. Equipos de Escritorio

En este mes, 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 presente mes 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.

- **Gestión de solicitudes de Herramienta Aranda para el servicio**

Para el mes de junio, desde la gestión de equipos de cómputo se relacionan las solicitudes de soporte atendidas para este servicio:

- Se registraron en Aranda un total de 16 solicitudes tipificadas así:
  - Incidentes – 0 caso
  - Requerimientos de Servicio – 16 casos.

- Al corte de mes quedaron en estado:
  - Cerrado – 9 casos.
  - Solucionado – 0 casos
  - Suspendido – 7 casos.
  - En Proceso – 0 caso.

- 15 casos corresponden a solicitudes de usuarios estándar.

- 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
Responsable Garantías Equipos	10
Gestor de Inventarios	6
Total general	**16**

Tabla 87 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	**16**
Equipo Periférico	10
Equipo Escritorio	4
Equipo Portátil	2
Total general	**16**

Tabla 88 Solicitudes de Equipos Usuario Final – Según Tipificación y Categoría

- **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	99,65%	93,75%
EUF-2	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 89 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 y seguimiento a fallas presentadas en servicios de MPLS e Internet en inspecciones y territoriales para lograr el restablecimiento del servicio por parte de los ISP.
- Se realizó actualización del esquema de red de la territorial de San Jose del Guaviare con las conexiones hacia los dispositivos BDCOM y Juniper que corresponden a los canales MPLS e Internet de la oficina.
- Se realiza monitoreo constante 7x24x365 enfatizando los canales MPLS principal y backup en el datacenter Colombia XV.
- Se trabajó en la actualización del direccionamiento WAN en las territoriales.
- Se trabajó en el informe de consumos de ancho de banda en las oficinas territoriales y demás solicitudes realizadas por la entidad.

Las acciones recomendadas en capa piso se orientan a la habilitación de un Access Point adicional o reubicación de los equipos que se tienen actualmente para ampliar el rango de cobertura, trabajo que debe ser avalado por los administradores del edificio WTC y del ministerio en cuanto se requieren realizar las adecuaciones del cableado estructurado y la adquisición de licenciamiento y equipos adicionales a los dimensionados para este servicio.

Se incluye el informe entregado a la entidad con el análisis y resultados encontrados:



Mapa_Calor_WiFi_NCentral_May2025.pdf

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

- Los especialistas gestionaron un total de 8 solicitudes escaladas a través de la herramienta Aranda. Al corte del mes, los 8 casos quedaron en estado Cerrado, los casos obedecen a ejecución de cambios, revisión y pruebas de red en canales de internet, conexión de puntos de red en rack.

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

Categoría	Cantidad de solicitudes
Access point Sede Central	2
Equipo Conectividad internet	1
Canal Internet	1
Router	1
Starlink	1

Tabla 90 Top 5 de categorías en el Servicio de conectividad LAN-WLAN



Ilustración 230 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 91 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, ANTIOQUIA	1
Territorial Valle	CALI	2
OE Buenaventura	BUENAVENTURA	1
Sede Nivel Central	BOGOTA	34*
	Total	**71**

Tabla 92 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

Dirección Territorial	Población y/o ciudad de ubicación	Cantidad Access Points
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, ANTIOQUIA	2
Territorial Valle	CALI	4
OE Buenaventura	BUENAVENTURA	1
Sede Nivel Central	BOGOTA	46
	Total	**110**

Tabla 93 Distribución de puntos de acceso

Territorial Bogotá: 1 equipo restante se encuentra en Stock.
Territorial Norte de Santander - Cúcuta: El AP fue enviado e instalado en la DT Santander / Bucaramanga
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, para ser trasladado a Nivel Central para pruebas del servicio en el despacho del ministro, equipo queda en bodega de Piso 22 desde el 17/06/2025 (modelo AudioCodes C435HD - SN: CNPRK9W287).

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 94 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	BOGOTA	45*
	Total	**50**

Tabla 95 Equipos gama media

(*) Novedades en la instalación de teléfonos

Nivel Central disponibilidad de 3 teléfonos, no han proporcionado el listado de asignación de estas extensiones.

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
AMAGA	AMAGA	1	Cerrada se envió teléfono a Medellín
MONTERREY	MONTERREY	1	Cerrada
BOLIVAR	BOLIVAR	1	Cerrada
TIERRA ALTA	TIERRA ALTA	1	Cerrada
QUIMBAYA	QUIMBAYA	1	Cerrada
CALARCA	CALARCA	1	Cerrada
MAJAGUAL	MAJAGUAL	1	Cerrada
CASA DE JUSTICIA (IBAGUE)	CASA DE JUSTICIA (IBAGUÉ)	1	Cerrada
LIBANO	LÍBANO	1	Cerrada
	Total	**9(*)**	

Tabla 96 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 97 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 entregados en Nivel Central para el servicio de MIFI en la medida en que la Entidad ha informado los usuarios que los van a utilizar.

Sede	Cantidad
Asignados Sede Central	25
Pendientes definición de usuario por parte de la Coordinadora del Grupo de Soporte Informático para asignación	5
Total	30

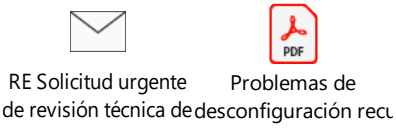
Tabla 98 Consolidado equipos MIFI

De acuerdo con la directriz recibida, los tres equipos restantes se dejarán como stock y se destinarán a una asignación emergente.

- **Gestión del servicio**

En el mes de junio de 2025, se presentan 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 lleva a cabo proceso de monitore sobre las troncales para las opciones 2 y 0 configuradas en el IVR para atención al ciudadano con el nuevo aliado BPM.
- El 12/06/2025 el especialista de telefonía informó mediante correo electrónico la novedad relacionada con la autenticación de los teléfonos del despacho del ministro, reportada el 28 de mayo de 2025, la cual fue mitigada mediante la implementación de una solución dada por fabricante. Ese mismo día se notificó formalmente a las partes involucradas, adjuntando el informe técnico con el detalle de las acciones ejecutadas.



- Capacitación para uso de servicios de TOIP en Teams a funcionarios ubicados en la territorial de Antioquia bajo requerimientos # RF-124133, RF-123636, RF-123662, RF-124263, RF-124264, RF-124395.

Capacitación
Telefonia Teams(1-2).

- **Asignación de Licencias - Extensiones**

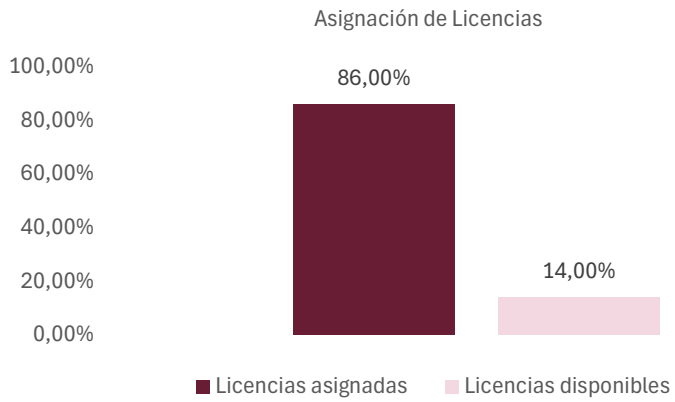


Ilustración *231*. Licencias y extensiones

Durante el mes en gestión, se han asignado un total de 1.456 extensiones a nivel nacional. Actualmente, permanecen disponibles 244 extensiones.

- **Estadísticas de Tráfico**

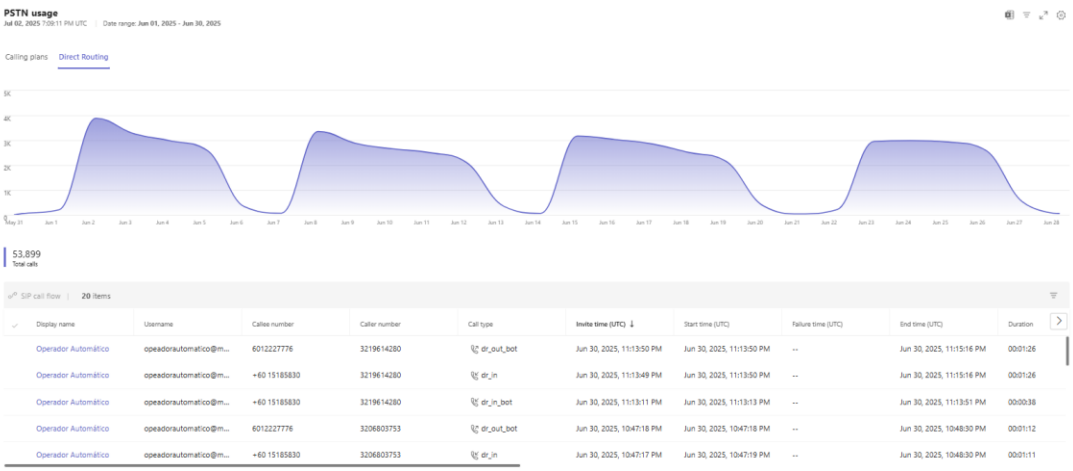


Ilustración 232 Estadística de tráfico

En la gráfica anterior se visualizan las tendencias de uso del servicio, en el periodo correspondiente al mes de junio de 2025, donde se atendieron un total de 53,899 llamadas.

Servicio	Minutos Disponibles	Minutos Utilizados
Locales	Ilimitados	791.18
Celular	1000	859.56
Nacional	Ilimitados	321.18
Internacional	700	3.45
Total		1975.37

Tabla 99 Minutos, consumos

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

Con respecto a las llamadas realizadas a destinos larga distancia nacional en el mes de junio de 2025, se identifica que se realizaron llamadas con una duración total de 321.18 minutos.

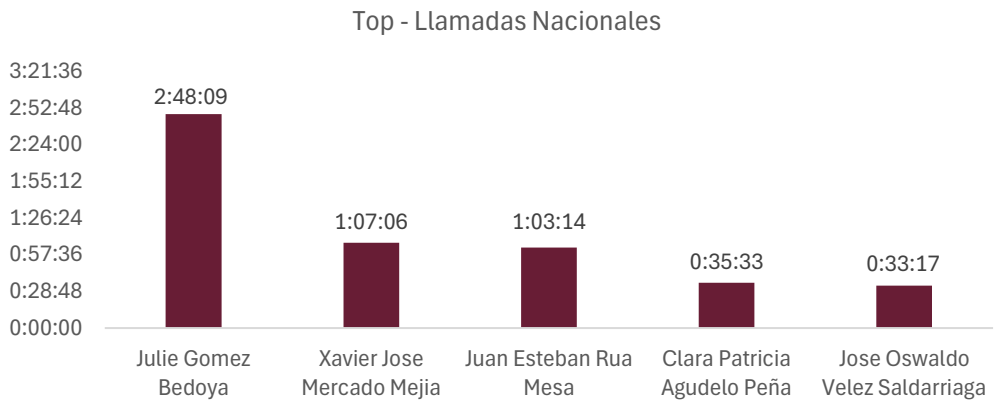


Ilustración 233 Top LDN

N°	Usuario	Área	Tiempo llamadas
1	Julie Gomez Bedoya	Grupo De Atencion Al Ciudadano Y Tramites – DT Cali	01:54:37
2	Xavier Jose Mercado Mejia	Grupo De Atencion Al Ciudadano Y Tramites	01:07:06
3	Juan Esteban Rua Mesa	PIVC Antioquia	01:03:14
4	Clara Patricia Agudelo Peña	Grupo de Comisión de Personal Antioquia	00:35:33
5	Jose Oswaldo Velez Saldarriaga	Grupo de Atencion Al Ciudadano Y Tramites	00:33:17

Tabla 100 Top 5 llamadas LDN

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

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

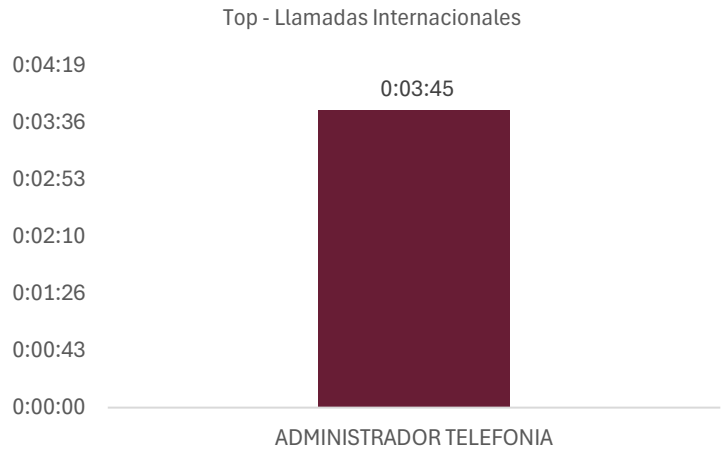


Ilustración 234 Top LDI

Como se puede observar en el grafico anterior, se evidencia que, en el mes de junio de 2025 se ha generado un consumo de llamada a destino internacional (España) por él 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 TELEFONIA	UT Gestión TIC 2023	00:03:45

Tabla 101 Top 5 llamadas LDI

- **Consumo de llamadas destinos celulares**

Con respecto a las llamadas realizadas a celular en el mes de junio de 2025, se identifica que se realizaron llamadas con una duración total de 859.56 minutos.

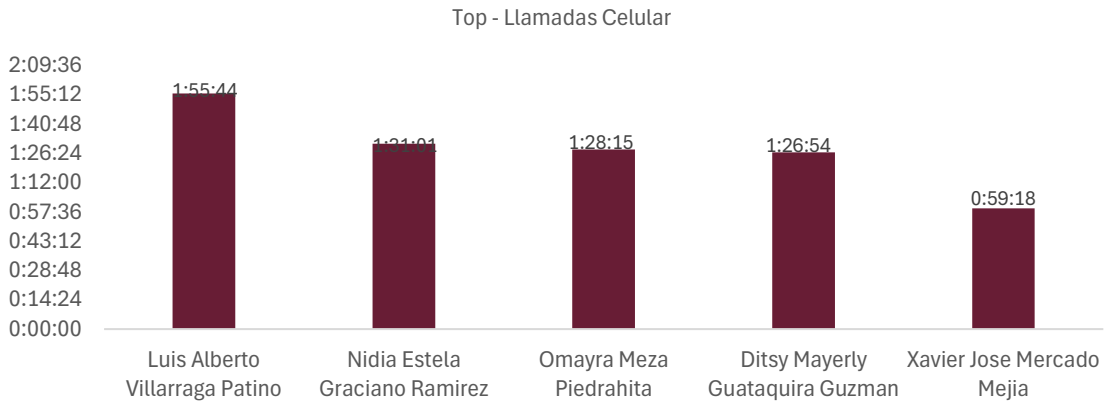


Ilustración 235 Top Celular

N°	Usuario	Área	Tiempo llamadas
1	Luis Alberto Villarraga Patino	Riesgos Laborales AMIRL – Sede Central Bogotá	01:55:44
2	Nidia Estela Graciano Ramirez	Coordinadora Grupo De Atencion Al Ciudadano Y Tramites	01:31:01

3	Omayra Meza Piedrahita	Grupo de cobro coactivo Bogotá	01:28:15
4	Ditsy Mayerly Guataquira Guzman	Acciones de Inspección GACT Bogotá	01:26:54
5	Xavier Jose Mercado Mejia	Grupo De Atencion Al Ciudadano Y Tramites	00:59:18

Tabla 102 Top 5 llamadas Celular

- **Consumo de llamadas locales**

Con respecto a las llamadas realizadas a destinos locales en el mes de junio de 2025, se identifica que se realizaron llamadas con una duración total de 791.18 minutos.

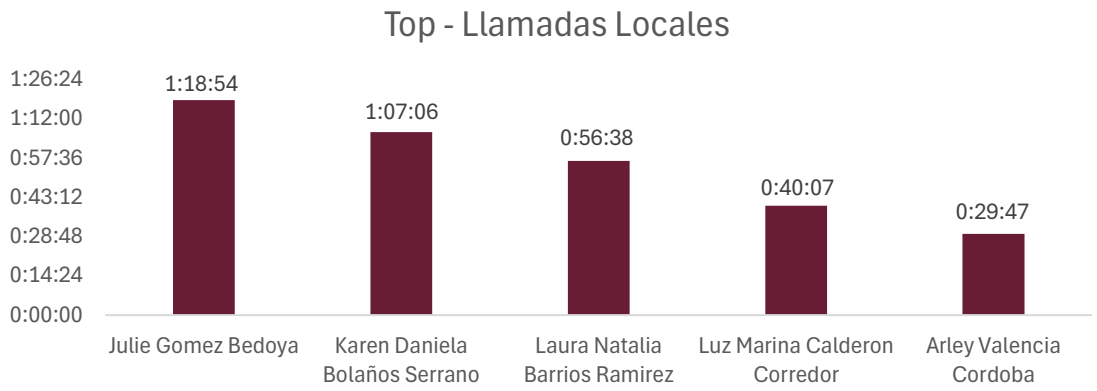


Ilustración 236 Top Local

N°	Usuario	Área	Tiempo llamadas
1	Julie Gomez Bedoya	Grupo De Atencion Al Ciudadano Y Tramites	01:18:54
2	Karen Daniela Bolaños Serrano	Despacho del viceministro de relaciones laborales	01:07:06
3	Laura Natalia Barrios Ramirez	Grupo de Subdirección Administrativa y Financiera	00:57:38
4	Luz Marina Calderon Corredor	Grupo Interno de Trabajo de Nomina e Incapacidades	00:40:07
5	Arley Valencia Cordoba	Grupo de Despacho Oficina Especial	00:29:47

Tabla 103 Top 5 llamadas locales

- **Capacitaciones y divulgaciones**

En el mes de junio se realizó proceso de capacitación y/o divulgaciones.

Item	Descripción	Fecha
1	Capacitación para uso de servicios de TOIP en Teams a funcionarios ubicados en la territorial de Antioquia bajo requerimientos # RF-124133, RF-123636, RF-123662, RF-124263, RF-124264, RF-124395.	Jun-2025

Tabla 104. Capacitaciones y divulgaciones

- **Mejores Prácticas**

Se trabajará en procesos de capacitación y divulgación del uso sobre la nueva herramienta de telefonía. Se encuentra en proceso el avance de liberación de licencias a nivel nacional, de igual

manera se continuará validando los backups de las grabaciones sobre 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

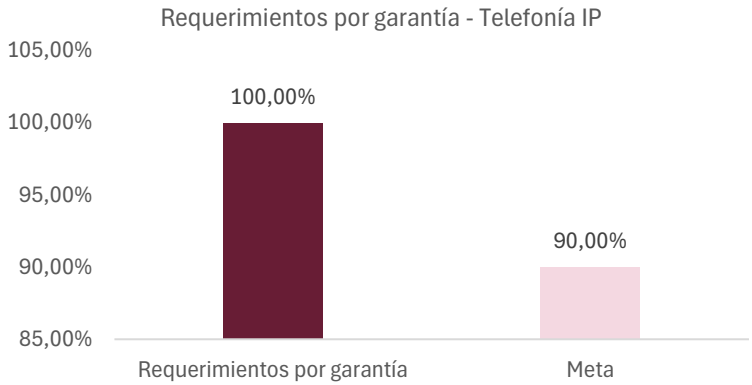


Ilustración *237* Requerimientos por garantía

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

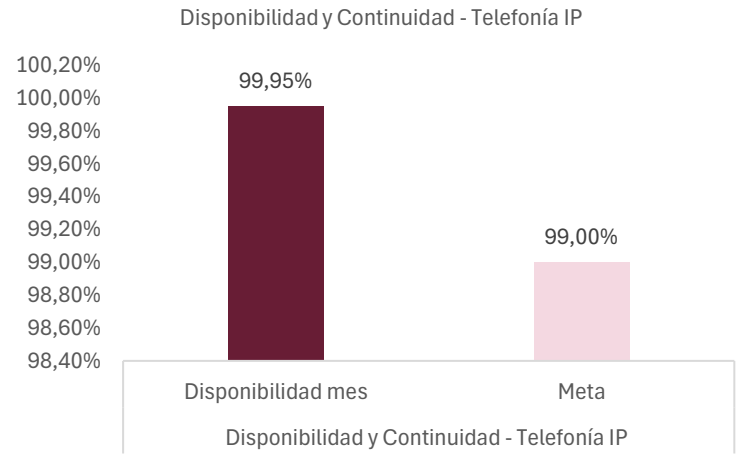


Ilustración 238 Disponibilidad y Continuidad TOIP

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

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

ID	Indicadores	Resultado	Meta
TIP-1	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
TIP-2	Continuidad y disponibilidad de los servicios de telefonía IP	99,96%	99,00%

TIP-3	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 105 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 106 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 Coordinadora del Grupo de Soporte Informático en el INFORME UT GESTION TIC 2023 - ENTREGA LINEA DE SERVICIO EER UPS

3. INFORME UT GESTION TIC 2023 - ENTREGA LINEA DE SERVICIO EER UPS.pdf

4.4.3. UPS 20 kVA

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

Tabla 107 Inventario de UPS – 20Kva

- **Gestión del servicio**

- Las UPS se encuentran operativas en cada sede de tal manera que actúen en caso de presentarse falla en el fluido eléctrico, 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.

- Se escala al ministerio en febrero 2025, novedad con la UPS en la territorial de Santander (Bucaramanga) propiedad de la entidad, 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. Al cierre de este período no se tiene ningún avance por parte de la entidad.

- Durante el período del informe no se presentaron eventos sobre los equipos de Energía Regulada UPS.

- **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 108 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 109 Inventario de impresoras para el servicio

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

- Para el mes de junio, el responsable del servicio gestionó un total de 567 solicitudes escaladas a través de Aranda. Al corte del mes, 547 casos quedaron en estado Cerrado/Solucionado, 20 en estado Suspendido (los casos suspendidos se deben a cambio de tóners a espera que se agoten y envío de consumibles).

- Se realiza el monitoreo constante de la capacidad de almacenamiento del buzón Relay Scanner para asegurar que se cuente con espacio disponible o generar la depuración correspondiente para evitar novedades en la prestación del servicio.

- Se gestiona el despacho y el 27/06/2025 se realiza la asignación de dos nuevas impresoras para la DT Santander (Bucaramanga) por solicitud del Subdirector Administrativo y Financiero y el Coordinador del Grupo de Soporte Informático. Se envía el siguiente inventario:
  IMPRESORA S/N:3354P150269
  IMPRESORA S/N:3354P150294
  BANDEJA S/N:3403P900011
  BANDEJA S/N: 3403P800620
  Guia:53082500843 COORDINADORA

- 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
ricoh-guadalaraja-buga-insp	Guadalaraja	vfierro	Viviana Fierro Herrera	4083
ricohpiso5a	Bogotá sede central	cjunco	Carlos Julio Junco Arenas	3563
ricoh-bmanga-ofc305	Bucaramanga	amateus	Andrea Johana Mateus Parra	2543
ricohpiso5b	Bogotá sede central	lforrero	Lizeth Dahiana Forero Peralta	2469
ricohpiso12a	Bogotá sede central	aquevedo	Ana Yaneth Quevedo Quintero	2088
ricoh-cali-piso2-atc	Cali	bgalindo	Betzabeth Galindo Herrera	1994
ricoh-ibague-radicacion	Ibague	mnavarrog	Maria Alejandra Navarro Garcia	1892
ricoh-cali-piso2-grcc	Cali	shurtado	Susana Hurtado Murillo	1830
ricohpiso10b	Bogotá sede central	jacero	John Mario Acero Barragan	1800
ricoh-cali-piso2-atc	Cali	mquinonesp	Mildreth Quinonez Peinado	1788

Tabla 110 Consumo de impresiones por usuario - Impresoras B/N

Clics%20junio.xlsx

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

Nombre de la impresora	Ubicación	Blanco y negro
ricoh-cali-piso4	Cali	14336
ricohcl32-rcc	Bogotá calle 32	12947
ricohpiso10b	Bogota sede central	12807
ricohpiso5a	Bogota sede central	12677
ricoh-cali-piso3	Cali	11962
ricoh-bmanga-ofc305	Bucaramanga	11891
ricohpiso12a	Bogota sede central	11444
ricoh-cali-piso2-atc	Cali	10996
ricoh-medellin-piso3	Medellin	9993
ricohpiso20b	Bogota sede central	9739

Tabla111 Top 10 de impresoras con mayor uso

Impresoras%20mas%20usadas%20junic

- 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	Doble Cara	Páginas simples	Total Páginas	Trabajos realizados	Promedio de Páginas por trabajo
ricohpiso25c	Bogotá sede central	ymedinag	Yeisson Medina Gonzalez	590	130	503	633	135	4,7
ricohpiso25c	Bogotá sede central	mserrano	Malliber Serrano Nieto	342	54	340	394	96	4,1
ricohpiso25c	Bogotá sede central	bhernandez	Bibiana Hernandez Hernandez	29	14	20	34	24	1,4

Tabla112 Top usuarios impresión a color

- 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
Centrales Dt	961	125369	93234	33096	126330	32545	3,9
D. T. Valle Del Cauca	0	56488	40128	16360	56488	15708	3,6
D. T. Bogota	0	54629	37768	16861	54629	14249	3,8
D. T. Antioquia	0	35245	25088	10157	35245	11245	3,1
D. T. Santander	0	30630	20730	9900	30630	9341	3,3

D. T. Norte De Santander	0	17109	11796	5313	17109	4773	3,6
D. T. Quindio	0	13920	9678	4242	13920	3538	3,9
D. T. Risaralda	0	12062	8708	3354	12062	3959	3
D. T. Meta	0	11709	8102	3607	11709	3392	3,5
D. T. Tolima	0	11247	7372	3875	11247	3095	3,6

Tabla113 Top oficinas

Informe%20por%20oficinas%20Junio.xls

- 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	Número de copias
ricoh-medellin-piso1	Medellín	47.754
ricohcl32-gau-b	Bogotá calle 32	43.830
ricohcl32-rcc	Bogotá calle 32	40.159
ricoh-bmanga-ofc205	Bucaramanga	27.955
ricoh-cali-piso4	Cali	25.399
ricohpiso5b	Bogotá Sede central	24.481
ricohcl32-gau-a	Bogotá calle 32	18.156
RICOH-BMANGA-OFC305	Bucaramanga	17.230
ricohpiso9a	Bogotá Sede central	16.882
ricoh-baq-dir	Barranquilla	15.175

Tabla 114 Top 10 impresoras más usadas del servicio de fotocopiado

Reporte%20copias%20junio.xlsx

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

- Se realiza la asignación de cuotas de clics de impresión de usuarios finales bajo el caso Aranda RF-130159, allí se relaciona el listado total de usuarios con el aprovisionamiento.

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

Transacciones%20junio.xlsx

Nombre de Usuario	Nombre Completo	Tipo de transacción	Cuota asignada	Número de veces que se aumento
vfierro	Viviana Fierro Herrera	ADJUST	3839	8
bgalindo	Betzabeth Galindo Herrera	ADJUST	2087	7
gparra	Gabriel Parra Trujillo	ADJUST	1657	6
jacero	John Mario Acero Barragan	ADJUST	1920	6
jguarnizo	Jorge Andres Guarnizo Molina	ADJUST	3264	6
tllanes	Tatiana Llanes Ibarguen	ADJUST	1323	6
amestre	Andrea Marcela Mestre Rozo	ADJUST	1581	5
fgalindo	Francy Galindo Pinzon	ADJUST	934	5
jlramirez	Jose Luis Ramirez Berrio	ADJUST	1072	5
lamartinez	Luz Amparo Martinez Ospina	ADJUST	1654	5

Tabla 115 Ampliación de cuota de impresión

- **Despacho de papel, tóner y unidades a nivel nacional**

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

	abr-25		may-25		jun-25	
	Resmas Carta	Resmas Oficio	Resmas Carta	Resmas Oficio	Resmas Carta	Resmas Oficio
Total Resmas	628	376	753	202	660	516
Total Cajas por Tamaño	62,8	18,2	75,3	20,2	66	51,6
Total Cajas Enviadas	**100,4**		**95,5**		**117,6**	

Tabla 116 Despacho de papel a sedes del Ministerio del Trabajo

Durante el período, se despacharon a sedes del ministerio un total de 24 tóners para impresora B/N, 0 juego de toner impresora de color.

- **Mantenimiento Preventivo de Equipos de Impresión**

La UT dentro de sus compromisos contractuales debe efectuar el mantenimiento preventivo de los equipos de impresión con una periodicidad semestral, en vista que las impresoras ya cumplieron un año de uso luego de finalizada la fase de transición y siguiendo la recomendación del fabricante Ricoh, se inicia el ciclo de mantenimiento a nivel nacional. A continuación, se presentan las actividades asociadas a esta actividad que se encuentra en curso.



Manual
Mantenimiento preve

Se da continuidad con las actividades de atención del mantenimiento preventivo, a corte del periodo se tiene un avance del 96.14% con un total de 259 impresoras intervenidas (223 de Territorio y 31 de Bogotá), faltando 5 impresoras a nivel nacional.

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 117 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 118 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 junio de 2025:

MES	DETALLE	CANTIDAD
Junio	Multifuncional blanco y negro rango medio - Clic de impresión tóner y papel carta	547.351
	TOTAL	547.351

Tabla 119 Clics de Impresión de junio 2025 – Multifuncional B/N

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

Mes 2025	Abril	Mayo	Junio
Cantidad de clics consumidos	**520.700**	**642.008**	**547.351**

Tabla 120 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 494.576 clics de impresión y 52.775 de fotocopias para un total de 547.351 para este servicio, superando el estimado del mes por 97.351

El administrador del servicio de outsourcing de impresión remitió semanalmente vía correo electrónico a la Coordinadora del Grupo de Soporte Informático 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 junio de 2025:

MES	DETALLE	CANTIDAD
Junio	Impresora color rango medio - Cargo fijo mensual - Clic de impresión tóner y papel carta	**961**
	TOTAL	**961**

Tabla 121 Clics de Impresión de junio 2025 – Impresora Color

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

Mes 2025	Abril	Mayo	Junio
Cantidad de clics consumidos	**2.818**	**2.803**	**961**

Tabla 122 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 **961** clics para este servicio.

- **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 123 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 junio 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.

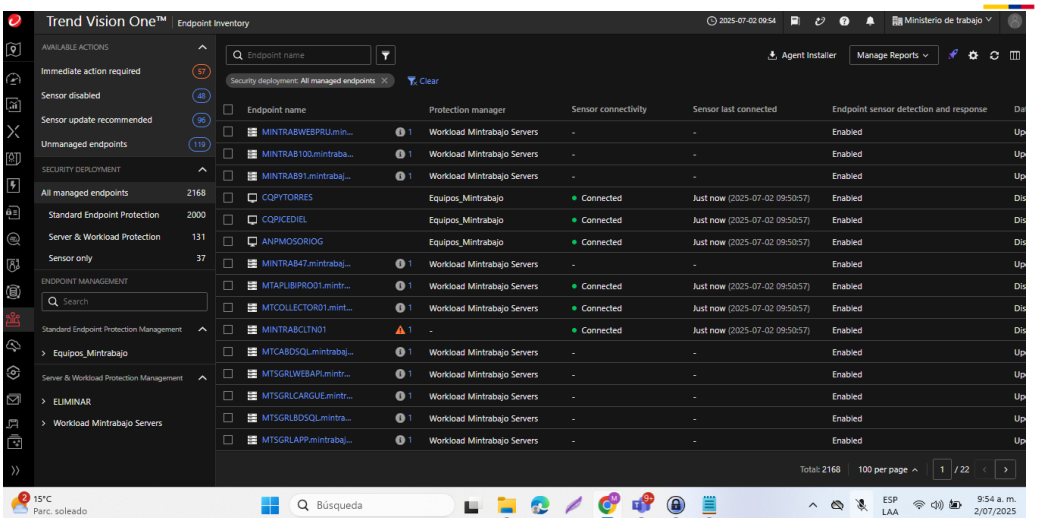


Ilustración 239 Equipos consola antivirus

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 (2050) de Mintrabajo, se cuenta con 2168 licencias, se tienen disponibles 124.

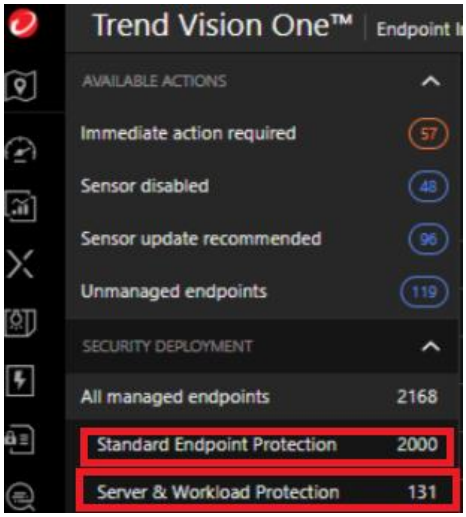


Ilustración 240 Gestión consola antivirus – equipos usuario final

4.7.3. Top 10 spyware

Uso de herramientas de crack y keygen (CRCK_KEYGEN, AutoKMS, KeyGen):

- Indica intentos de eludir licencias de software, lo cual es una práctica riesgosa y potencialmente ilegal.
- Estas herramientas suelen contener **malware oculto** o abrir puertas traseras (backdoors).

HackTools (NirSoft, PassView, PasswordSniffer):

- Son herramientas comúnmente usadas por atacantes (y a veces administradores) para recuperar contraseñas, esnifar tráfico o manipular sistemas.
- Su presencia sin autorización representa una **violación de políticas de seguridad**.

PUA (Potentially Unwanted Applications):

- Aunque no son malware por definición, sí pueden afectar el rendimiento del sistema, representar riesgos de privacidad y abrir vectores de infección.

Conclusión

La presencia de estas herramientas sugiere un posible incumplimiento de políticas de seguridad y riesgos asociados a software no autorizado. Se recomienda:

- Realizar un análisis en los equipos afectados.
- Eliminar estas herramientas y reforzar políticas de control de software.
- Implementar restricciones para evitar la instalación y ejecución de software no autorizado.
- Sensibilizar a los usuarios sobre los riesgos del uso de software no legítimo.

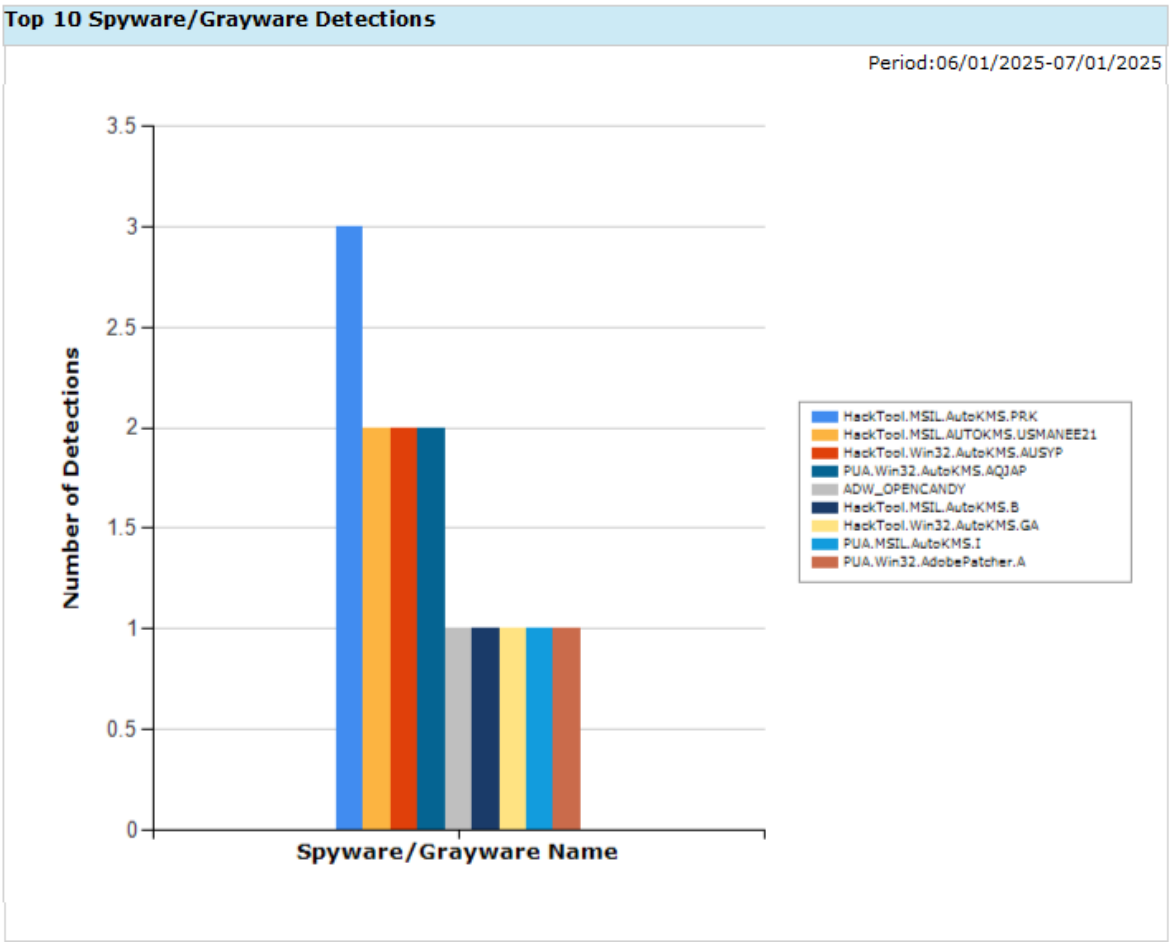


Ilustración 241 Top 10 Spyware

Top 10 Spyware/Grayware Detections		
Spyware/Grayware Nam e	# of Detections	Detected By
HackTool.MSIL.AutoKMS.PRK	3	Desktop (3)
HackTool.MSIL.AUTOKMS.USMANEE21	2	Desktop (2)
HackTool.Win32.AutoKMS.AUSYP	2	Desktop (2)
PUA.Win32.AutoKMS.AQJAP	2	Desktop (2)
ADW_OPENCANDY	1	Desktop (1)
HackTool.MSIL.AutoKMS.B	1	Desktop (1)
HackTool.Win32.AutoKMS.GA	1	Desktop (1)
PUA.MSIL.AutoKMS.I	1	Desktop (1)
PUA.Win32.AdobePatcher.A	1	Desktop (1)

Tabla 124 Top spayware

4.7.4. Top 10 Virus Detectados

Los datos reflejan la detección de múltiples amenazas de malware en equipos de escritorio.

Análisis de los Datos:

Infecciones Totales: Se registraron 135 infecciones en total.

Virus más Común:

Trojan.Win32.GRENAM.SM es el más frecuente, con 108 infecciones (80% del total).

Distribución: Todos los virus fueron detectados únicamente en Desktop (no hay infecciones en móviles/servidores).

Tipos de Malware:

- Troyanos (Trojan): 117 infecciones (86.67%).
- Gusanos (Worm): 7 infecciones (5.19%).
- Spyware (TSPY): 4 infecciones (2.96%).
- Otros (PE_MOFKSYS.A, etc.): 7 infecciones (5.19%).

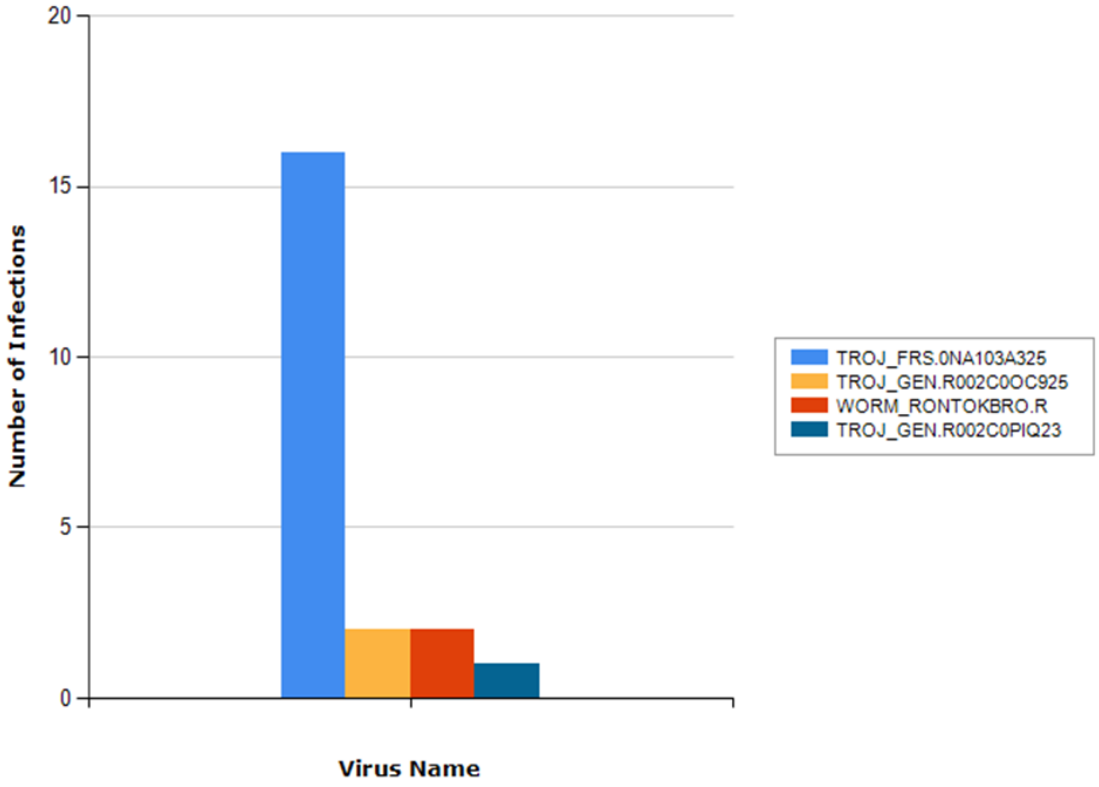


Ilustración 242 Top 10 virus detectados

Top 10 Virus Infections		
Virus Name	# of Infections	Detected By
TROJ_FRS.0NA103A325	16	Desktop (16)
TROJ_GEN.R002C0OC925	2	Desktop (2)
WORM_RONTOKBRO.R	2	Desktop (2)
TROJ_GEN.R002C0PIQ23	1	Desktop (1)

Ilustración 243 Top infección virus

TROJ_FRS.0NA103A325: Esta es la detección de Trend Micro para troyanos que exhiben acciones maliciosas como modificación de configuración del sistema, descarga y ejecución de archivos arbitrarios y robo de información. Los troyanos son una clasificación general de malware para archivos, aplicaciones o programas maliciosos que pueden incluirse en paquetes de malware o grayware.

TROJ_GEN.R002C0OC925: Esta es la detección genérica de Trend Micro para archivos con comportamiento sospechoso que pueden dañar los sistemas. Los troyanos son una clasificación general de malware para archivos, aplicaciones o programas maliciosos que se descargan comúnmente de Internet.

WORM_RONTOKBRO.R: El malware RONTOKBRO se autorreplica y, por lo tanto, se clasifica como gusano. Estos gusanos suelen propagarse entre sistemas a través de unidades extraíbles y descargadas de Internet.

TROJ_GEN.R002C0PIQ23: Esta es la detección genérica de Trend Micro para archivos con comportamiento sospechoso que pueden dañar los sistemas. Los troyanos son una clasificación general de malware para archivos, aplicaciones o programas maliciosos que se descargan comúnmente de Internet.

4.7.5. 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 junio 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 comenzará a ejecutar el plan de trabajo para el ethical hacking correspondiente al primer semestre 2025.

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.

4.7.5.1. Inventario y licenciamiento

El inventario de activos registrado en la herramienta Tenable Nessus Professional se basa en la línea base de activos del segundo semestre proporcionada por el cliente, así como en los resultados del escaneo inicial de Discovery. En total, se han registrado 286 activos de TI.

En junio, se alcanzó un registro de 278 activos de TI (97 %) de la línea base documentada en la herramienta.

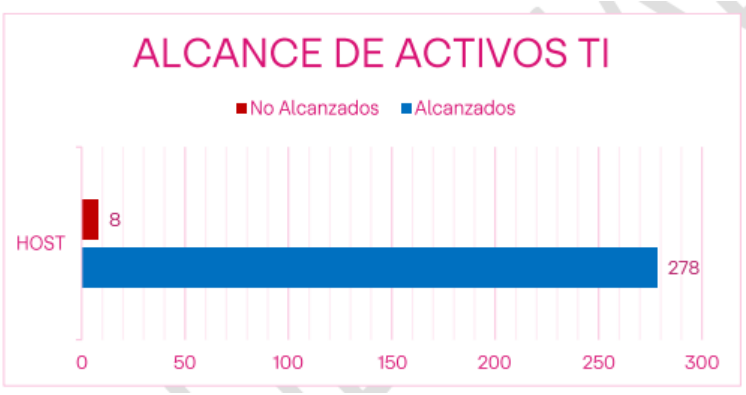


Ilustración 244 Gestión consola Nessus

4.7.5.2. 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 ▲
MINTRABAJO SEMANAL - NETWORKING	Vulnerability	Weekly on Sat at 8:00 PM	✔	June 28 at 8:29 PM
MINTRABAJO SEMANAL - FORTISIEM	Vulnerability	Weekly on Sat at 9:00 PM	✔	June 28 at 9:27 PM
MINTRABAJO SEMANALES - VMWARE	Vulnerability	Weekly on Sat at 10:00 PM	✔	June 28 at 10:11 PM
MINTRABAJO SEMANALES - LINUX	Vulnerability	Weekly on Sat at 11:00 PM	✔	June 28 at 11:43 PM
MINTRABAJO SEMANALES - WINDOWS DESKTOP	Vulnerability	Weekly on Sun at 12:30 AM	✔	June 29 at 1:10 AM
MINTRABAJO SEMANALES - NO AUTH	Vulnerability	Weekly on Sun at 3:30 AM	✔	June 29 at 3:38 AM
MINTRABAJO SEMANAL - WINDOWS SERVER	Vulnerability	Weekly on Sun at 9:00 PM	✔	June 30 at 12:30 AM

Ilustración 245 Escaneos programados

	Críticas	Altas	Medias	Bajas
MES				
Noviembre 2024	30.823	16.460	19.526	3.179
Diciembre 2024	28.604	28.530	5.316	1.836
Enero 2025	255	258	1.310	436
Febrero 2025	133	323	1.073	411
Marzo 2025	1.352	5.487	439	74
Abril 2025	182	321	3.733	1.283
Mayo 2025	187	221	1.145	556
Junio 2025	141	268	1.020	540

Tabla 125 Total de vulnerabilidades

- 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).

4.7.5.3. TOP 10 – Vulnerabilidades más explotables

A continuación, se presenta la lista con el top 10 vulnerabilidades más explotables en base a la puntuación VPR; la cual determina la facilidad de explotación de la vulnerabilidad, entre otras aproximadamente 150 variables. La puntuación VPR ayuda identificar los activos que tienen vulnerabilidades con más probabilidad de ser seleccionadas por un atacante para la ejecución de un Pentesting. La lista corresponde a:

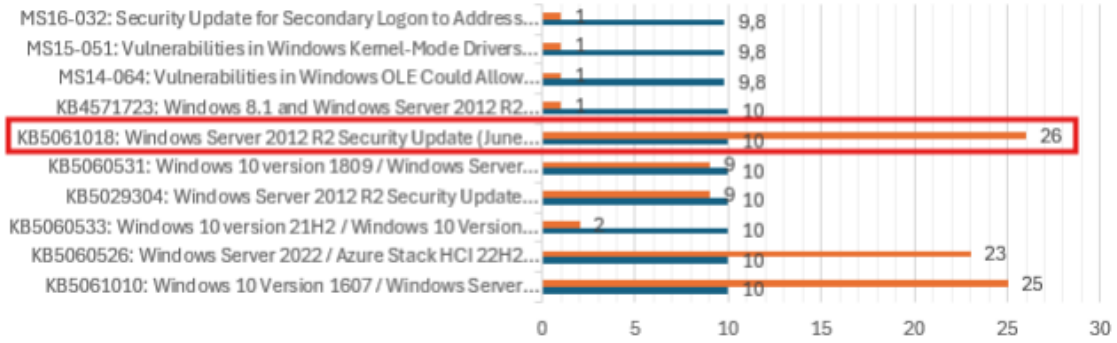


Tabla 126 TOP 10 - Activos más explotables

La vulnerabilidad "**KB5029304: Windows Server 2012 R2 Security Update "** corresponde a un boletín de seguridad para el sistema operativo Windows Server 2012 R2, publicado en agosto de 2023; abarca varias vulnerabilidades que se remedian aplicando la actualización de seguridad emitida por el fabricante.
las vulnerabilidades directamente.

4.7.5.4. 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.

4.7.5.5. Resumen de mitigación efectuada

A continuación, se contrasta un resumen de las actividades relacionas con la gestión de vulnerabilidades correspondientes al Snapshot del semestre I 2025, el cual reporta un total de 3.782 vulnerabilidades TI en las severidades:

- 42 vulnerabilidades críticas.
- 100 vulnerabilidades altas.
- 133 vulnerabilidades medias.
- 12 vulnerabilidades bajas.

Durante el periodo de junio 2025, se remediaron un total de 287 vulnerabilidades, de las cuales, 42 fueron de severidad crítica, 100 de severidad alta, 133 de severidad media y 12 de severidad baja. Por otro lado, con relación a indicadores semestrales, se han gestionado un total de 1.644 vulnerabilidades TI, de las cuales, 265 fueron de severidad crítica, 409 de severidad alta, 858 de severidad media y 112 de severidad baja.

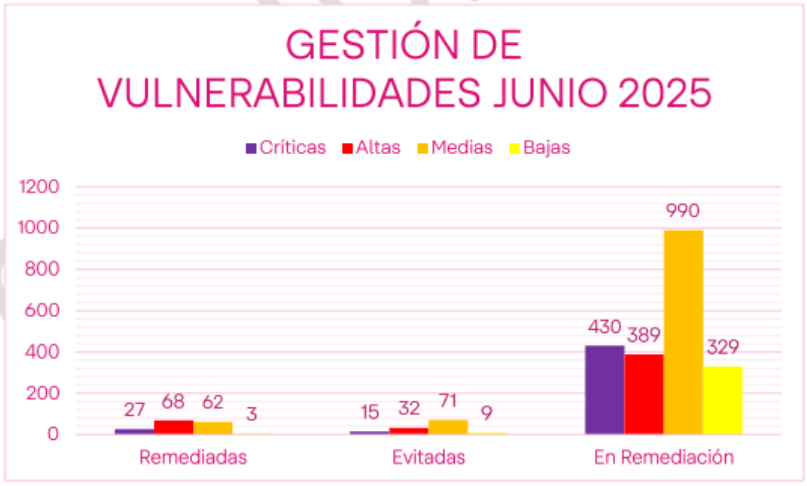


Ilustración 246 Vulnerabilidades gestionadas vs en remediación

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

Reporte
Vulnerabilidades Mi

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

MINTRABAJO -
VULNERABILIADES C

4.7.5.6. Ethical Hacking Primer semestre 2025

Durante el mes de junio, se llevó a cabo la ejecución de la actividad de **Ethical Hacking** primer semestre la cual tiene como alcance de esta prueba evaluar la seguridad del entorno de Directorio Activo "**mintrabajo.loc**". Esto incluye la evaluación de los siguientes componentes y áreas clave:

- Evaluación de la seguridad de todos los controladores de dominio dentro del domino especificado.
- Análisis de las políticas de contraseña, privilegios de usuarios y la pertenencia a grupos.
- Revisión de las políticas de grupo configuradas en el dominio.
- Evaluación de la seguridad de los servicios de autenticación, como lo es Kerberos y NTLM.

Acciones Realizadas				
Vulnerabilidad	**Cuenta/Afectado**	**Acción Tomada**	**Estado**	**Responsable**
DCSYNC (ALLEXTENDEDRIGHTS)	mintrab-data	Retirada de *Admins. del dominio* y cuenta deshabilitada.	Mitigado	Equipo de Seguridad
	servicios gestor	Retirada de *Admins. del dominio*.	Mitigado	Equipo de Seguridad
	SQL_Service01	Retirada de *Admins. del dominio*.	Mitigado	Equipo de Seguridad
	SQL_Service02	Retirada de *Admins. del dominio*.	Mitigado	Equipo de Seguridad

	SQL_Service03	Retirada de *Admins. del dominio*.	Mitigado	Equipo de Seguridad
Kerberoasting Attack	Adminbck	Cambio de contraseña pendiente.	Mitigado	Especialistas Servicios Centrales
	Admin_SQL	Cambio de contraseña pendiente.	Mitigado	Especialistas Servicios Centrales
	SQL-service1	Cambio de contraseña pendiente.	Mitigado	Especialistas Servicios Centrales
	SQL_service01	Cambio de contraseña pendiente.	Mitigado	Especialistas Servicios Centrales
	SQL_service02	Cambio de contraseña pendiente.	Mitigado	Especialistas Servicios Centrales
	consulta Servicios	Retirada de *"Password never expires"*.	Mitigado	Especialistas Servicios Centrales

Tabla 127 Ethical Hacking Primer semestre

- **Medición de ANS Antivirus**

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

ID	Indicadores	Resultado	Meta
AV-1	Cobertura de antivirus	99,39%	95,00%
AV-2	Continuidad y disponibilidad de la plataforma	100,00%	98,00%
AV-3	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 128 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 Metodología calidad documental de casos

Para llevar a cabo la evaluación de la calidad documental de los casos registrados en la herramienta de gestión, se definieron los siguientes criterios:



Ilustración 247 Criterios calidad documental casos

La evaluación se realiza de manera individual, y de esta forma se valida el cumplimiento de cada uno los criterios (SI o NO cumple), teniendo en cuenta los siguientes parámetros:

Criterios	Parámetros
Tipo de caso	Identificación adecuada de la solicitud si corresponde a un incidente o un requerimiento
Asunto	Título acorde a la solicitud del usuario (claro y congruente)
Descripción	Registro completo de la solicitud Documentación completa de la solicitud del usuario con la información necesaria para la gestión, escalamiento y solución
Prioridad	Identificación adecuada teniendo en cuenta el tipo de usuario y la naturaleza de la solicitud
Categoría	Asignación correcta de la categoría de acuerdo con el árbol de categorías
Escalamiento	Escalamiento correcto de acuerdo con el árbol de categorías
Solución	Redacción de las actividades realizadas de manera clara para fácil entendimiento del usuario. Documentación completa de las acciones adelantas para la atención del caso que incluya capturas de pantalla o documentos anexos
Estado del caso	Asignación correcta del estado del caso según la gestión realizada
Justificación estado del caso	Realiza justificación en caso de pasar a estado suspendido
Periodicidad de seguimiento	Realiza seguimiento periódico al caso
Descripción de seguimientos	Inclusión de notas de avance relacionadas con la gestión del caso.
Cumplimiento ANS	Hora de registro de la solución de la solicitud en los tiempos establecidos
Redacción y Ortografía	Se evalúa la ortografía y redacción de la documentación, además que se encuentre de acuerdo con los criterios establecidos y en coherencia con la solución.

Tabla 129 Criterios y parámetros calidad documental casos

Una vez realizada la evaluación de los criterios, se realiza individualmente la retroalimentación de los casos, teniendo en cuenta que cada ítem tiene un peso de 7.70%

5.2 Evaluación calidad documental de casos

En abril, se realizó la evaluación cuantitativa de la muestra de 290 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	100%
2. Asunto	1	100%
3. Descripción	2	99,9%
4. Prioridad	0	100%
5. Categoría	9	99,8%
6. Escalamiento	0	100%

7. Solución	2	99,9%
8. Estado del Caso	0	100%
9. Justificación Estado del Caso	0	100%
10. Periodicidad de seguimientos	1	100%
11. Descripción de seguimientos	0	100%
12. Ortografía y redacción	4	99,9%
13. Cumplimiento de ANS	1	100%

Tabla 130 Errores cometidos

Se identificaron 21 errores con un porcentaje de cumplimiento consolidado de 99,44%, lo cual se evidencia una mejora del 0,82% en la calidad de la documentación.

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 9 novedades por error en la categorización del ticket, 4 falencias en ortografía y redacción, 2 en la solución y 2 en descripción del caso.
Cómo acción de mejora, se realizó refuerzo con el equipo en sesión el cual se revisaron varios temas relacionados a la gestión y documentación de casos.
Las retroalimentaciones a los especialistas/responsables, se realizará en el mes de julio a través de sesiones para las mejoras correspondientes

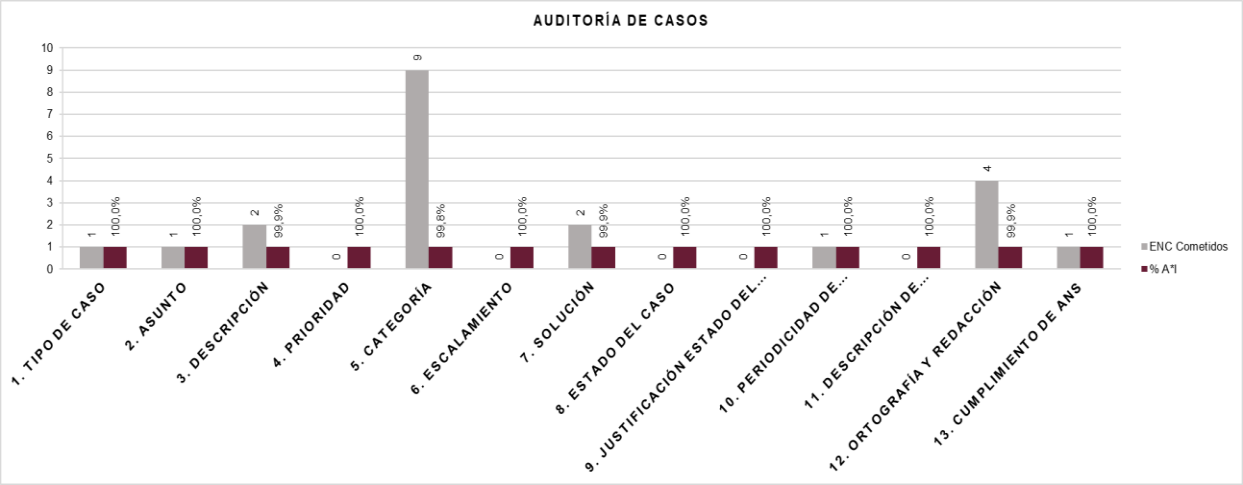


Ilustración 248 Resultados auditoria de casos

5.3 Metodología de calidad de llamadas

Para llevar a cabo la evaluación de las llamadas recibidas (datos no estructurados) por la Mesa de Servicios, de las cuales se generan los casos en la herramienta de gestión, se definieron los siguientes criterios:

PRECISIÓN ERROR NO CRÍTICO – PENC



Ilustración 249 Precisión error no Critico de llamadas

PRECISIÓN ERROR CRÍTICO – PEC

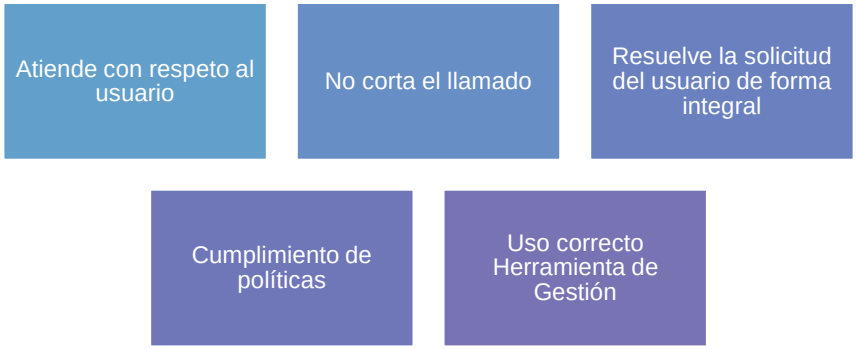


Ilustración 250 Precisión error Critico de llamadas

De los casos gestionados, se determinó como muestra las llamadas con más de 1:30 minutos, para descartar las que no reflejan la atención al usuario.

La evaluación se realiza de manera individual, y de esta forma se valida el cumplimiento de cada uno los criterios, teniendo en cuenta los siguientes parámetros:

PRECISIÓN ERROR NO CRÍTICO – PENC

Criterios	Parámetros
Bienvenida y Personalización	- Se evalúa que el agente cumpla con los protocolos de llamada al inicio da la bienvenida al usuario a la línea telefónica y se presenta correctamente. - Se evalúa si el agente está tomando los datos asignados del usuario de forma eficiente, es decir, que el usuario no tenga que repetir varias veces la misma información. - Se evalúa que el agente verifique la identidad del usuario antes de realizar cualquier procedimiento
Escucha Activa	- Se evalúa que el agente esté atento en la llamada, atendiendo y preguntando los datos necesarios, de tal forma que el usuario no tenga que repetir información antes dada.
Retroalimentación y manejo de espera	- Se evalúa que el agente comunique al usuario que lo dejará un momento en línea. - Se evalúa que el agente no deje al usuario esperando en línea por más de dos minutos. Si las actividades que debe realizar duran mayor tiempo el agente debe retomar e informar al usuario los procedimientos que está realizando. - Se evalúa que el agente comunique al usuario su agradecimiento por su espera en línea. - Se evalúa que el agente aplique el mute en la llamada cuando requiera que el usuario espere un momento.
Empatía y adaptabilidad al usuario	- Se evalúa que el agente en la llamada mantenga respeto, amabilidad y empatía con el usuario al momento de atender la solicitud. - Se evalúa si el agente mantiene un tono de voz adecuado, además si la información que suministra al usuario es clara y entendible utilizando un vocabulario adecuado.
Proceso técnico y/o lineamientos	- Se evalúa que el agente comunique eficazmente la información al usuario, para que conozca las actividades realizadas y el estado de su solicitud.

Criterios	Parámetros
	- Se evalúa si se evidencia que el asesor posee agilidad en la consulta y en el manejo de los aplicativos y procedimientos
Asegura y Despedida	- Se evalúa si el agente informa al usuario el número de ticket generado. - Se evalúa que el agente cumpla con el protocolo de despedida

Tabla 131 Precisión Error NO CRÍTICO – PENC

PRECISIÓN ERROR CRÍTICO – PEC

Criterios	Parámetros
Atiende con respeto al usuario	- Se evalúa que el agente durante la conversación es cordial con el usuario, manteniendo un adecuado tono de voz durante la conversación, no realiza acciones durante la llamada que sean irrespetuosas, groseras, insultantes
No corta el llamado	- Se evalúa que el agente atiende el llamado; no lo corta. - Se evalúa que el agente no deja al usuario en línea hasta que corta. - Se evalúa que el agente no insista a que usuario cuelgue llamada.
Resuelve la solicitud del usuario de forma integral	- Se evalúa que el agente realiza el procedimiento que corresponde de acuerdo con la necesidad del usuario, utilizando las herramientas disponibles para realizarlo y lo documenta en el ticket. - Se evalúa que el agente entrega solución al usuario teniendo en cuenta los procedimientos vigentes de la mesa
Cumplimiento de políticas	- Se evalúa que el agente no descalifica a la compañía y/o a sus pares - Se evalúa que el agente cuida la confidencialidad - Se evalúa que el agente escala requerimiento cuando lo amerita
Uso correcto Herramienta de Gestión	- Se evalúa que el agente realiza el ingreso del ticket en la herramienta de gestión - Se evalúa que el agente Ingresa correcta y completamente la información en la herramienta de gestión

Tabla 132 Criterios y parámetros calidad de llamadas

Una vez realizada la evaluación de los criterios, se realiza individualmente la de los casos, de acuerdo con los siguientes pesos porcentuales para cada criterio:

PRECISIÓN ERROR NO CRÍTICO - PENC		
1. Bienvenida y Personalización (10%)		
2. Escucha Activa (10%)		
3. Retroalimentación y manejo de espera (15%)	No deja al usuario en silencio sin previo aviso (5%)	
	Solicitar y agradecer los tiempos de espera (5%)	
	Realiza acompañamiento al usuario (5%)	
4. Empatía y adaptabilidad al usuario (20%)	Lenguaje (5%)	
	Seguridad y confianza (5%)	
	Se adapta al usuario y a la situación presentada (5%)	
	Mantiene una sonrisa telefónica (5%)	
5. Proceso técnico y/o lineamientos (35%)		
6. Asegura y Despedida (10%)	Asegura la atención (5%)	
	Utilizando guion de despedida establecido (5%)	
	RESULTADO PENC	**0%**
PRECISIÓN ERROR CRÍTICO - PEC		
1. Atiende con respeto al usuario		
2. No corta el llamado		
3. Resuelve la solicitud del usuario de forma integral		
1. Cumplimiento de políticas		
2. Uso correcto Herramienta de Gestión		
	RESULTADO PEC	**0%**

Tabla 133 Calificación Calidad llamadas

5.4 Evaluación de calidad de llamadas

En el mes de junio 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:

PRECISIÓN ERROR NO CRÍTICO - PENC	Junio 2025	%
Escucha Activa	1	94%
Retroalimentación y manejo de esperas	2	96%
Empatía y adaptabilidad al usuario	0	100%
Asegura y Despedida	1	98%
Bienvenida y Personalización	0	100%
Soporte Primer Nivel	0	100%

PRECISIÓN ERROR CRÍTICO – PEC	Junio 2025	%
Uso correcto Herramienta de Gestión	3	81%
No corta el llamado	0	100%
Resuelve el requerimiento del usuario de forma integral	0	100%
Cumplimiento de políticas	0	100%
Atiende con respeto al usuario	0	100%

Tabla 134 Resultado de criterios y parámetros - Calidad de llamadas

Una vez realizada la revisión individual de las llamadas, se realiza el siguiente análisis frente a los resultados de las 16 llamadas evaluadas de las cuales se evidencia las siguientes afectaciones en el resultado global por categoría:

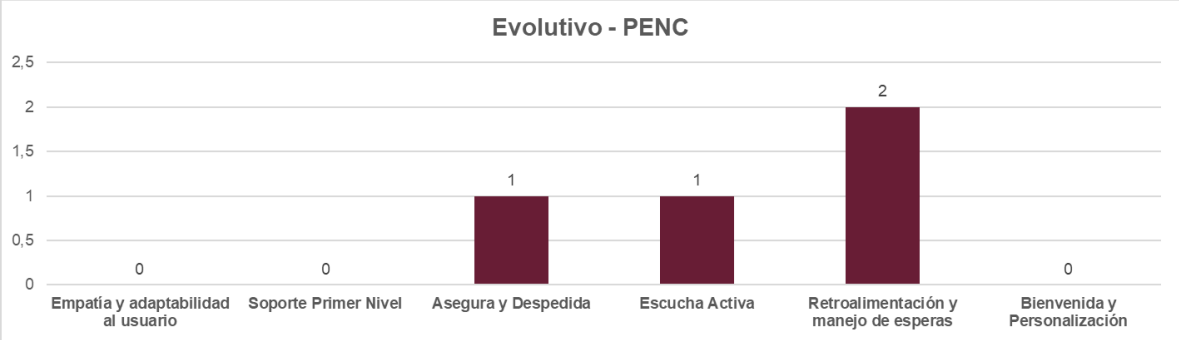


Ilustración 251Resultados llamadas PENC

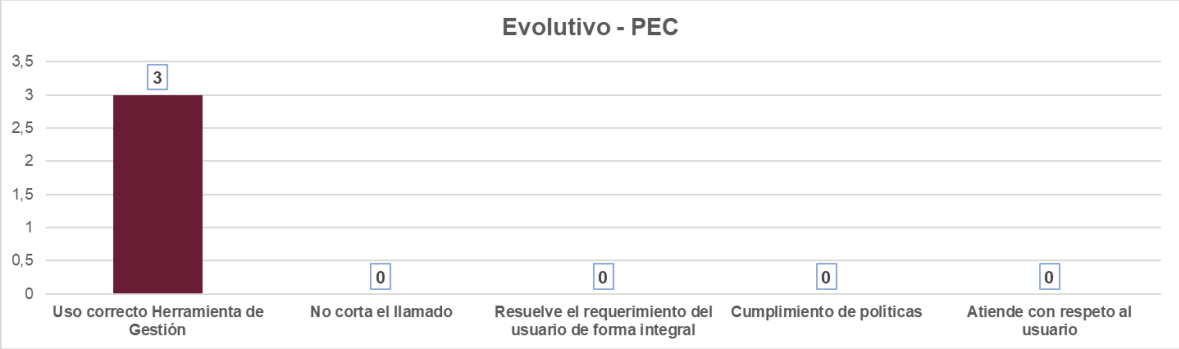


Ilustración Resultados 252 llamadas PEC

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 de acceso a la Herramienta de monitoreo (Zabbix)	Falla de acceso a la herramienta de monitoreo	NO	La herramienta de gestión ha estado disponible
Mesa de servicios	Problemas de funcionalidad en la cuenta de soportemt@mintrabajo.gov.co.	Falla en el acceso y/o sincronización del correo soportemt@mintrabajo.gov.co	NO	El correo electrónico institucional ha estado disponible
Mesa de servicios	Imposibilidad de contacto por la línea telefónica de la mesa de servicios	Falla en el ingreso de las llamadas a la mesa de servicios	NO	La línea telefónica ha estado disponible
Mesa de servicios	Desborde de solicitudes (vía correo electrónico y/o llamadas) en la Mesa de Servicios	Aumento eventual de la cantidad de solicitudes que supera la capacidad de atención de los Agentes de la Mesa de servicios	NO	No se ha presentado desborde de solicitudes
Mesa de servicios	Riesgo de seguridad de la información que comprometan la confidencialidad, integridad o disponibilidad de la información.	Posibilidad de uso indebido de la cuenta genérica del cliente, asignada para la Mesa de servicios	NO	No se ha presentado dicha situación.
Soporte en sitio	Incumplimiento de los compromisos pactados por atención de actividades urgentes - no planeadas	Solicitud de realización de actividades urgentes no planeadas que afectan la prestación del servicio de acuerdo con lo planeado	NO	No se ha presentado dicha situación.
Todas las prácticas	Deficiencias en la adopción de las prácticas de ITIL	Resistencia a la adopción de las prácticas de ITIL por las partes interesadas	NO	Se proporcionó capacitación a los involucrados
Práctica de Activos	Posibilidad de pérdida de inventario	La pérdida de inventario se produce cuando las cantidades reales del inventario son	NO	Se realizó seguimiento quincenal con el equipo de trabajo para revisar los compromisos de la práctica

SERVICIO/ PRÁCTICA	NOMBRE	DESCRIPCIÓN	¿MATERIALIZADO?	ACCIONES PARA REALIZAR
		inferiores a las registradas en el módulo de gestión		
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
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

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.
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 135 Seguimiento a 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
Clics adicionales blanco y negro	97351	$13.629.140
	Subtotal	$17.579.052

Tabla 136 Bolsa de Recursos

8. MEDICIÓN DE ACUERDOS DE NIVEL DE SERVICIO

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

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

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

Se incluye información actualizada del reporte de ANS

Área	Nombre Indicador	Resultado	Meta
Mesa de Servicio	Tiempo de atención de solicitudes por soporte en sitio	99,65%	95,00%
	Tiempo de solución de incidentes por soporte en sitio	99,05%	90,00%
	Tiempo de solución de requerimientos por soporte en sitio	99,97%	90,00%
	Tiempo de respuesta de la mesa de servicio	99,65%	85,00%
	Abandono de llamadas	0,35%	Máximo 8,00%

Área	Nombre Indicador	Resultado	Meta
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Equipos de usuario final	Tiempo de solución de requerimientos de garantía	93,75%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
ANTIVIRUS	Cobertura de antivirus	99,39%	95,00%
	Continuidad y disponibilidad de la plataforma	100,00%	98,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
LAN y WLAN	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Energía Regulada	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Datacenter	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Continuidad y disponibilidad del datacenter principal	100,00%	99.95%
	Continuidad y disponibilidad del datacenter alterno	100,00%	99,60%
	Continuidad y disponibilidad de la plataforma de procesamiento, almacenamiento y respaldo	100,00%	99,70%
	Tiempo de solución de incidentes asociado a los servicios de aplicaciones especializadas	100,00%	90,00%
	Tiempo de solución de requerimientos asociado a los servicios de aplicaciones especializadas	100,00%	90,00%
	Continuidad y disponibilidad de los servicios de directorio activo	100,00%	99,60%
	Continuidad y disponibilidad de los servicios de seguridad informática	100,00%	99,90%
	Tiempo de solución de incidentes asociado a los servicios de administración, soporte y monitoreo	100,00%	90,00%
	Tiempo de solución de requerimientos asociado a los servicios de administración, soporte y monitoreo	98,50%	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	99,95%	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)	100.00%	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 137 Medición de Acuerdos de Niveles de Servicio junio 2025

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

Dando cumplimiento a lo establecido en el Anexo Técnico Base 10102023 – definitivo, capítulo Fase de Operación, se realizó la medición de los ANS y esta actividad será tenida en cuenta para efectos de los afinamientos y ajustes a que haya lugar en la operación de los servicios.

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 Coordinadora del Grupo de Soporte Informático dentro del tiempo comprometido.

9. ANEXOS

- Certificación_backup_servidores
- Consumo de cuotas junio
- detalle_llamadas_recibidas_(01.06.2025-30.06.2025)
- Datos_Mintrabajo_junio

FIN DEL DOCUMENTO