Trabajo

Informe de Gestión Mensual Contrato 574 de 2023

Servicios Tecnológicos Informáticos para el Ministerio del Trabajo a Nivel Nacional

Unión Temporal
Gestión TIC 2023

Agosto de 2025

DOCUMENTO/ ARCHIVO	
Código:	**Informe Gestión - Unión Temporal Gestión TIC 2023**
Nombre Archivo:	**Informe Gestión - Unión Temporal Gestión TIC 2023 – Agosto 2025**
Fecha:	8/09/2025
Versión:	1

REGISTRO DE CAMBIOS			
Versión	**Páginas**	**Fecha Modificación**	**Motivo del cambio**
1	219	08/09/2025	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 11
Objetivo 11
Alcance 11
Definición de Siglas y Expresiones Técnicas 11
1 GERENCIA Y/O ADMINISTRACIÓN 13
2 LÍNEA DE GESTIÓN DE SERVICIOS 13
2.1. Gestión del Servicio 13
2.1.2. Prácticas ITIL 4 17
2.1.2.1. Práctica Acuerdos Niveles de Servicio (ANS) 17
2.1.2.2. Práctica Habilitación de Cambios 17
2.1.2.3. Práctica Gestión de Activos 18
2.1.2.4. Práctica Catálogo de servicios 19
2.1.2.5. Práctica de Problemas 20
2.1.2.6. Práctica de Incidentes 21
2.1.2.7. Práctica de Requerimientos 27
2.1.2.8. Práctica de Eventos 30
2.1.2.9. Práctica de Disponibilidad 45
2.1.2.10. Práctica de Implementación 47
2.2. Mesa de Servicios y Soporte en Sitio 48
3. LINEA DE SERVICIOS CENTRALES 68
3.1. Datacenter 68
3.1.1. Datacenter Principal 68
3.1.2. Datacenter Alterno y DRP 81
3.1.3. Procesamiento, Almacenamiento y Respaldo 87
3.1.4. Aplicaciones Especializadas 91
3.1.5. **No aplica** 145
3.1.6. Seguridad Informática 146
3.1.6.1. Firewalls de nueva generación 146
3.1.6.2. Sandbox – Amenazas día 0 150
3.1.6.3. SIEM - Solución de correlación de eventos de seguridad, disponibilidad y recursos 152
3.1.6.4. WAF - Servicio de tipo "Firewall de Aplicaciones Web" 159
3.1.6.5. Solución de Anti-DDoS 161
3.1.7. Licenciamiento 165
3.1.8. Administración, soporte y monitoreo 166
3.2. No aplica 167
3.3. Conectividad WAN, SDWAN e Internet 167
3.3.1. Canales WAN 167
3.3.1.1. Incidentes de Conectividad 168
3.3.1.2. Topología Actual 169
3.3.2. Canales SDWAN e Internet Dedicado 169
4. LINEA DE SERVICIOS EN SEDE 173
4.1. Equipos de Cómputo de usuario final 173
4.1.1. Equipos de Escritorio 176
4.1.2. Equipos Portátiles 176
4.2. Conectividad LAN y WLAN 177
4.2.1. Switch CORE Sede Principal 178
4.2.2. Switch para conexiones perimetrales (EDGE) en sede principal 178
4.2.3. Switch de acceso 24 puertos 178
4.2.4. Switch de acceso 48 puertos 179
4.2.5. Puntos de Acceso 179

4.3. Telefonía IP 181
4.3.1. Teléfono Gama Media 181
4.3.2. Teléfono Gama Baja 181
4.3.3. Troncales SIP 182
4.3.4. No Aplica 182
4.3.5. No Aplica 182
4.3.6. Módems 4G – Con plan de 50 Gbps 182
4.4. Energía Regulada UPS 188
4.4.1. UPS 10 kVA 188
4.4.2. UPS 15 kVA 189
4.4.3. UPS 20 kVA 189
4.5. No aplica 190
4.6. Outsourcing de Impresión 191
4.6.1. No aplica 194
4.6.2. Multifuncional B/N rango medio – Cargo fijo mensual 194
4.6.3. Impresora Color rango medio – Cargo fijo mensual 194
4.6.4. No aplica 194
4.6.5. Multifuncional B/N rango medio – Clic de impresión 194
4.6.6. Impresora Color rango medio – Clic de impresión 195
4.7. Antivirus 195
4.7.1. Instalaciones de antivirus en servidores 195
4.7.2. Instalación de antivirus PCs usuarios final 196
4.7.3. Top 10 spyware 197
4.7.4. Top 10 Virus Detectados 199
4.7.5. Servicio de Vulnerabilidades 200
4.7.5.1. Inventario y licenciamiento 201
4.7.5.2. Escaneos programados 201
4.7.5.3. TOP 10 – Vulnerabilidades más explotables 203
4.7.5.4. Estrategia de remediación y/o mitigación 203
4.7.5.5. Resumen de mitigación efectuada 204
4.7.5.6. Ethical Hacking Segundo semestre 2025 205
5. GESTIÓN DE CALIDAD DE INFORMACIÓN 206
5.1 Metodología calidad documental de casos 206
5.2 Evaluación calidad documental de casos 207
5.3 Metodología de calidad de llamadas 208
5.4 Evaluación de calidad de llamadas 210
5.5 Práctica de Mejora 211
6. GESTION DE RIESGOS 212
7. BOLSA DE RECURSOS 214
8. MEDICIÓN DE ACUERDOS DE NIVEL DE SERVICIO 214
9. ANEXOS 216

Índice de Tablas

Tabla 1 Atención de solicitudes por grupo de especialistas 15
Tabla 3 Tipificación de cambios 17
Tabla 4 Medición Indicador Porcentaje de Cambios Exitosos 18
Tabla 7 KPI Práctica Catálogo de Servicios 19
Tabla 8 Consolidado de casos creados 20
Tabla 9 Detalle problema 133831 20
Tabla 10 Detalle problema 137015 21
Tabla 11 Estados Incidentes 22
Tabla 12 Top 10 Incidentes 22
Tabla 13 Casos Suspendidos 23

Tabla 14 Incidentes Mayores Registrados 24
Tabla 15 KPI Práctica de Incidentes 25
Tabla 16 Causas Reaperturas 26
Tabla 17 Estado de Solicitudes....27
Tabla 18 Seguimiento del Backlog Suspendidos....27
Tabla 19 Top 10 Jerarquía de Requerimientos 28
Tabla20 Detalle de KIP Practica de Requerimientos....28
Tabla 21 Casos reabiertos....30
Tabla 22 KPI Práctica Eventos....31
Tabla 23 Consolidado disponibilidad de servidores....45
Tabla 24 Consolidada disponibilidad de Directorio Activo 45
Tabla 25 Desagregado de Disponibilidad Directorio Activo 45
Tabla 26 Consolidado disponibilidad de equipos Datacenter principal 45
Tabla 27 Desagregado de Disponibilidad Datacenter Principal 45
Tabla 28 Consolidado disponibilidad de equipos Datacenter alterno....46
Tabla 29 Desagregado Disponibilidad de equipos Datacenter alterno....46
Tabla 30 Consolidado disponibilidad de equipos redes y conectividad....46
Tabla 31 Consolidado disponibilidad de equipos de seguridad 46
Tabla 32 Disponibilidad de equipos Seguridad de la Información....46
Tabla 33 Consolidado disponibilidad de equipos de telefonía 46
Tabla 34 Consolidado disponibilidad de plataforma antivirus 46
Tabla 35 Atención de Llamadas....49
Tabla 36 Top 10 administración de servidores....50
Tabla 37 Top 10 redes y conectividad....51
Tabla 38 Top 10 seguridad informática....51
Tabla 39 Top Telefonía IP....52
Tabla 40 Top 10 soporte aplicaciones....53
Tabla 41 Top 10 soporte microinformática 54
Tabla 42 Casos Anulados por Servicio....55
Tabla 43 Casos Suspendidos por Servicio....55
Tabla 41 Casos Suspendidos por Servicio....56
Tabla 46 Requerimientos solucionados por Mesa de Servicios....57
Tabla 47 Requerimientos solucionados por Soporte en sitio 57
Tabla 49 Casos cerrados por la mesa de servicios 59
Tabla 50 Casos cerrados por soporte en sitio 60
Tabla 46 Casos cerrados por soporte en sitio 63
Tabla 51 Casos usuarios VIP....65
Tabla 52 Casos usuarios Regulares 65
Tabla 53 Visitas en sedes sin Soporte en Sitio....67
Tabla 54 Medición ANS Mesa de Servicios....68
Tabla 55 capacidades de acuerdo con las fichas técnicas 72
Tabla 56 Infra total + servidores de pruebas + servidores a desaprovisionar 72
Tabla 57 Infra total producción + servidores de pruebas de la entidad 73
Tabla 58 Infra total sin servidores de pruebas....73
Tabla 59 Capacidades consumidas por entornos de pruebas 73
Tabla 60 Capacidades consumidas (Sin servidores de backup)....73
Tabla 61 Migración actividades .NET....96
Tabla 62 Cronograma Implementación SISGESTIÓN....98
Tabla 63 Comportamiento casos GD 115
Tabla 64 Total Instancias....121
Tabla 65 Total Documentos....121
Tabla 66 Total radicados....122
Tabla 67 Dimensionamiento Servers IBM - Virtualización Optima....122
Tabla 68 Apps & DDBB Oracle 126
Tabla 69 Escenario de Capacidades Oracle - Estado de consumo Actual 126
Tabla 70 Escenario de Capacidades Oracle - Total de recursos empleados....127
Tabla 71 Top tráfico de aplicaciones....148
Tabla 72 eventos detectados por el SIEM....158
Tabla 73 Listado de requerimientos atendidos....163
Tabla.74 Ejecución de archivos maliciosos....163
Tabla.75 Vulnerabilidades en la infraestructura....163
Tabla.76 Ataque de Phishing dirigidos....164
Tabla 77 Licenciamiento....166
Tabla 78 Medición ANS Datacenter 167
Tabla 79 Medición ANS Nube Pública....167
Tabla 80 Novedades servicio de internet 168

Tabla 81 Medición de ANS Conectividad WAN e Internet 172
Tabla 82 Desagregado sedes con novedad un solo enlace....172
Tabla 83 Desagregado sedes con novedad con doble enlace....172
Tabla 84 Cantidades de equipos a distribuir a nivel nacional 173
Tabla 85 Cantidades de equipos asignados nivel nacional 173
Tabla 86 Cantidades de equipos por devolución nivel nacional....173
Tabla 87 Estado de casos de garantía. 174
Tabla 88 ANS casos de garantía....174
Tabla 89 ANS Relación casos de garantía....174
Tabla 90 Equipos en siniestro....175
Tabla 91 *Avance instalación de equipos* 175
Tabla 92 Solicitudes de Equipos Usuario Final – Según Grupo Responsable 176
Tabla 93 Solicitudes de Equipos Usuario Final – Según Tipificación y Categoría....176
Tabla 94 Medición ANS Equipos de Usuario Final 177
Tabla 95 Top 5 de categorías en el Servicio de conectividad LAN-WLAN....177
Tabla 96 Distribución y Cantidades de switch 24 puertos....178
Tabla 97 Distribución y Cantidades de Switch 48 puertos 179
Tabla 98 Distribución de puntos de acceso....180
Tabla 99 Medición ANS LAN y WLAN....180
Tabla 100 Equipos gama media....181
Tabla 101 Sedes cerradas 181
Tabla 102 Consolidado de teléfonos gama baja....181
Tabla 103 Consolidado equipos MIFI....182
Tabla 104 Minutos, consumos 184
Tabla 105 Top 5 llamadas LDN....185
Tabla 106 Top 5 llamadas LDI 185
Tabla 107 Top 5 llamadas Celular....186
Tabla 108 Top 5 llamadas locales....186
Tabla 109. Capacitaciones y divulgaciones....187
Tabla 110 Medición ANS Telefonía IP 188
Tabla 111 Inventario de UPS – 10kVA....189
Tabla 112 Inventario de UPS – 20Kva 189
Tabla 113 Medición ANS Energía Eléctrica UPS....190
Tabla 114 Inventario de impresoras para el servicio 191
Tabla 115 Consumo de impresiones por usuario - Impresoras B/N....192
Tabla 116 Top 10 de impresoras con mayor uso....192
Tabla117 Top usuarios impresión a color....192
Tabla118 Top oficinas....193
Tabla 119 Top 10 impresoras más usadas del servicio de fotocopiado 193
Tabla 120 Ampliación de cuota de impresión....193
Tabla 121 Despacho de papel a sedes del Ministerio del Trabajo....194
Tabla 122 Cargo mensual multifuncional rango medio....194
Tabla 123 Cargo mensual impresora color....194
Tabla 124 Clics de impresión de agosto 2025 – Multifuncional B/N....194
Tabla 125 Tendencia de consumo de clics B/N....194
Tabla 126 Clics de Impresión de agosto 2025 – Impresora Color....195
Tabla 127 tendencia de consumo de clics color 195
Tabla 128 Medición ANS Outsourcing de Impresión 195
Tabla 129 Top spayware....198
Tabla 130 Total de vulnerabilidades....202
Tabla 131 TOP 10 - Activos más explotables....203
Tabla 132 Ethical Hacking Segundo semestre 205
Tabla 133 Medición de ANS Antivirus 205
Tabla 134 Criterios y parámetros calidad documental casos....206
Tabla 135 Errores cometidos 207
Tabla 136 Precisión Error NO CRÍTICO – PENC 209
Tabla 137 Criterios y parámetros calidad de llamadas 209
Tabla 138 Calificación Calidad llamadas....209
Tabla 139 Resultado de criterios y parámetros - Calidad de llamadas 210
Tabla 140 Seguimiento de Acciones de Mejora 211
Tabla 141 KPI Practica de Mejora....211
Tabla 142 Seguimiento a riesgos....214
Tabla 143 Bolsa de Recursos 214
Tabla 144 Medición de Acuerdos de Niveles de Servicio agosto 2025....216

Índice de Ilustraciones

Ilustración 1 Estado de casos en el período 14
Ilustración 2 KPI Efectividad de Resolución de Incidentes de Servicio 25
Ilustración 3 KPI Incidentes de Reabiertos en el periodo 26
Ilustración 4 KPI Efectividad de Resolución de Requerimientos de Servicio 28
Ilustración 5 KPI Requerimientos de Reabiertos en el periodo 29
Ilustración 6 Eventos por Tipo de Equipo 32
Ilustración 7 Sedes afectadas por router 32
Ilustración 8 Causas de eventos generados por router 33
Ilustración 9 Casos suspendidos VS. Casos solucionados de Router 34
Ilustración 10 Sedes Afectadas 34
lustración 11 Causa de eventos generados por Switch 35
Ilustración 12 Casos suspendidos VS. Casos solucionados de Switch 35
Ilustración 13 Top 10 Sedes afectadas por Access Point 36
Ilustración 14 Causa de eventos generados por AP 36
Ilustración 15 Casos suspendidos VS. Casos solucionados de AP 37
Ilustración 16 Top 10 Sedes afectadas por Starlink 37
Ilustración 17 Causas de eventos generados por Starlink 38
Ilustración 18 Casos suspendidos VS. Casos solucionados de Starlink 39
Ilustración 19 Top 10 Sedes afectadas por FortiGate 39
Ilustración 20 Causas de eventos generados por FortiGate 40
Ilustración 21 Casos suspendidos VS. Casos solucionados de FortiGate 40
Ilustración 22 Seguimiento Pruebas de Disponibilidad 47
Ilustración 23 Seguimiento Práctica Implementación 48
Ilustración 24 Requerimientos Solucionados por la Mesa de Servicios 57
Ilustración 25 Requerimientos Solucionados por Soporte en sitio 57
Ilustración 26 Casos cerrados por la mesa de servicios 59
Ilustración 27 casos cerrados por Soporte en Sitio 61
Ilustración 28 casos cerrados soporte territoriales 63
Ilustración 29 Modo de Ingreso de Solicitudes 65
Ilustración 30 Cumplimiento WSUS 69
Ilustración 31 Estado final de los casos Windows 70
Ilustración 32 Casos por categorías Windows 70
Ilustración 33 Estado final de los casos Nube privada 71
Ilustración 34 Casos por categoría Nube privada y pública 72
Ilustración 35 Estado File Server Mintrab60 74
Ilustración 36 Proyección de Modelo de Suscripción 75
Ilustración 37 Modelo de Tenant bajo arquitectura 75
Ilustración 38 Comportamiento SWCORE Datacenter Colombia XV 80
Ilustración 39 Grafica de consumo canal Internet Datacenter 81
Ilustración 40 Diagrama Interoperabilidad Bogotá CXV 82
Ilustración 41 VM Replicadas a través de site recovery 82
Ilustración 42 Diagrama de Replicación CXV - Santa Mónica 83
Ilustración *43* LANTOLAN extremo Bogotá 84
Ilustración *44* LANTOLAN extremo Cali 84
Ilustración *45* Estado canal de Internet DC Cali 85
Ilustración 46 Estado SWCORE Datacenter alterno 85
Ilustración 47 Estado canal MPLS DC Alterno 86
Ilustración 48 Estado interface de conexión equipo MPLS DC Alterno 86
Ilustración 49 Estado equipo MPLS DC Alterno 87
Ilustración *50* Estado final de casos – Aplicaciones Especializadas 92
Ilustración 51 categorías Apps 93
Ilustración 52 Arquitectura de la Aplicación Sugerida por la UT 98
Ilustración 53 Error 1 CC 102
Ilustración 54 Error 2 CC 102
Ilustración 55 Estado pre-ventana 105
Ilustración 56 Generación de Backups DDBB 105
Ilustración 57 Validación Tablas DDBB 106
Ilustración 58 Validación Tablas DDBB 106
Ilustración 59 Validación Tablas DDBB 106
Ilustración 60 Validación Tablas DDBB 107
Ilustración 61 Validación Tablas DDBB 107
Ilustración 62 Validación Tablas DDBB 107
Ilustración 63 validación Tablas DDBB 108

Ilustración 64 Verificación Registros 108
Ilustración 65 Verificación Registros 108
Ilustración 66 Verificación Registros tras ejecución de procesos....109
Ilustración 67 Validación de estado de tablas tras ejecución de procesos....109
Ilustración 68 Estado de instancias DDDB 109
Ilustración 69 Eliminación de instancias....110
Ilustración 70 Disminución de instancias tras ejecución de proceso....110
Ilustración 71 Estado del servidor - pre-desfragmentación....110
Ilustración 72 Ejecución desfragmentación 111
Ilustración 73 Ejecución desfragmentación 111
Ilustración 74 Ejecución desfragmentación 111
Ilustración 75 Reconstrucción de Índices 112
Ilustración 76 Validación de tamaños de tablas....112
Ilustración 77 Validación de tamaños de tablas....112
Ilustración 78 Validación de tamaños de tablas....113
Ilustración 79 Validación de tamaños de tablas....113
Ilustración 80 Validación de tamaños de tablas....113
Ilustración 81 Validación de tamaños de tablas....114
Ilustración 82 Validación de tamaños de tablas....114
Ilustración 83 Ejecución de estadísticas de validación 114
Ilustración 84 Diagrama BPM....116
Ilustración 85 Diagrama ODM....117
Ilustración 86 Diagrama WASND 117
Ilustración 87 Diagrama FileNet Front....118
Ilustración 88 Diagrama Datacap 118
Ilustración 89 Diagrama App Connect....119
Ilustración 90 Arquitectura Gestor Documental 119
Ilustración 91 Capacidades VM Gestor Documental 120
Ilustración 92 Licenciamiento Oracle....120
Ilustración 93 IBM Licenciamiento....121
Ilustración 94 Distribución de licencias Oracle 122
Ilustración 95 Licencias ambientes....122
Ilustración 96 Casos IBM - Servicio....123
Ilustración 97 categoría DDBB 123
Ilustración 98 Casos DDBB por Servicio 124
Ilustración 99 casos DDBB 125
Ilustración *100* Estado Bases de Datos....125
Ilustración 101 Información base de datos – Servidor....127
Ilustración 102 Estadísticas CPU 127
Ilustración 103 Estadísticas Memoria....127
Ilustración 104 Estadísticas Pool compartido 127
Ilustración 105 Tamaño DDBB....128
Ilustración 106 Tamaño Esquema DDBB 128
Ilustración 107 Rendimiento DDBB 128
Ilustración 108 DDBB por Server 129
Ilustración 109 Host e Instancia CPU....129
Ilustración 110 Estadísticas Memoria....129
Ilustración 111 Estadística Shared Pool....129
Ilustración 112 Tamaño DDBB DBMINTRA 129
Ilustración 113 Tamaño Esquema DDBB 130
Ilustración 114 Rendimiento DDBB MINTRASG 130
Ilustración 115 Información DDBB PLIFERAY 130
Ilustración 116 Host e Instancia CPU....131
Ilustración 117 Estadísticas Memoria....131
Ilustración 118 Estadísticas Shared Pool 131
Ilustración 119 Tamaño DDBB PLifeRay....131
Ilustración 120 Tamaño Esquemas DDBB 131
Ilustración 121 Rendimiento DDBB PlifeRay....132
Ilustración 122 Información DDBB SIGEP....132
Ilustración 123 Estadística Host e Instancia 132
Ilustración 124 Estadística Memoria....133
Ilustración 125 Estadística Shared Pool....133
Ilustración 126 Tamaño DDBB SIGEP 133
Ilustración 127 Tamaño Esquema DDBB 133
Ilustración 128 Rendimiento DDBB SIGEP 134
Ilustración 129 Información DDBB DBSIMPC 134

Ilustración 130 Estadística CPU 134
Ilustración 131 Estadística Memoria 135
Ilustración 132 Estadística Shared Pool 135
Ilustración 133 Tamaño DDBB SIMPC 135
Ilustración 134 Tamaño Esquema DDBB 135
Ilustración 135 Rendimiento DDBB 136
Ilustración 136 Información servidor DBBB 136
Ilustración 137 Host e Instancia CPU 136
Ilustración 138 Estadística memoria 137
Ilustración 139 Estadística Shared Pool 137
Ilustración 140 Tamaño DDBB MINTRASD 137
Ilustración 141 Tamaño Esquemas 137
Ilustración 142 Rendimiento MINTRASD 138
Ilustración 143 Información Server DDBB 138
Ilustración 144 Host e Instancia CPU 138
Ilustración 145 Estadística Memoria 139
Ilustración 146 Estadística Shared Pool 139
Ilustración 147 Tamaño DDBB 139
Ilustración 148 Tamaño DDBB 139
Ilustración 149 Rendimiento DDBB 140
Ilustración 150 Información Server DDBB 140
Ilustración 151 Host e Instancia CPU 140
Ilustración 152 Estadística Memoria 141
Ilustración 153 Estadística Shared Pool 141
Ilustración 154 Tamaño DDBB 141
Ilustración 155 Tamaño Esquemas DDBB 141
Ilustración 156 Rendimiento DDBB 142
Ilustración 157 Información Server DDBB 142
Ilustración 158 Estadística CPU 143
Ilustración 159 Estadística Memoria 143
Ilustración 160 Estadística Shared Pool 143
Ilustración 161 Tamaño Esquemas DDBB 143
Ilustración 162 Comportamiento DDBB 144
Ilustración 163 Almacenamiento ASM 144
Ilustración 164 DiskGroup Data 144
Ilustración 165 DiskGroup Flash 145
Ilustración 166 DiskGroup Reco 145
Ilustración 167 DiskGroup Redo 145
Ilustración 168 Licenciamiento adicional componente IBM 145
Ilustración*169* Disponibilidad firewall 146
Ilustración*170* Comportamiento ancho de banda 147
Ilustración *171* Reporte consumo ancho de banda 147
Ilustración*172* Top de usuarios 148
Ilustración *173* Top tráfico de aplicaciones 148
Ilustración 174 Top 15 Authenticated Logins by VPN Connections 149
Ilustración *175* Failed Login Attempts by User 150
Ilustración 176 estadísticas de escaneo 151
Ilustración *177* performance 151
Ilustración *178* Licenciamiento 152
Ilustración *179* Casos de uso 153
Ilustración *180* Disponibilidad 154
Ilustración *181* Autenticación de seguridad 156
Ilustración *182* Violación de políticas 157
Ilustración *183* eventos detectados por el siem 157
Ilustración 184 Disponibilidad de servidores- Seguridad 158
Ilustración 185 Top Aplicaciones por Bandwidth 159
Ilustración 186 Top attack types 160
Ilustración 187 Top de ataques 161
Ilustración 188 Login fallidos 162
Ilustración 189 Políticas y procedimiento de seguridad 165
Ilustración 190. Grafica de consumo canal MPLS Datacenter 167
Ilustración 191 Uptime del equipo MPLS Datacenter 168
Ilustración 192. Topología actualizada 169
Ilustración 193. Interface Fortimanager 170
Ilustración 194. Interface MPLS HUB SDWAN 170
Ilustración 195 Interface Internet HUB SDWAN 170

Ilustración 196. VPN SDWAN establecidas....171
Ilustración 197. Estado HUB SDWAN Datacenter....171
Ilustración 198. Estado HA HUB Sdwan....171
Ilustración 199. Recursos Fortimanager....171
Ilustración 200 Estado de casos Redes y Conectividad....178
Ilustración *201*. Licencias y extensiones....183
Ilustración 202 Estadística de tráfico....184
Ilustración 203 Top LDN....184
Ilustración 204 Top LDI....185
Ilustración 205 Top Celular....186
Ilustración 206 Top Local....186
Ilustración *207* Requerimientos por garantía....187
Ilustración 208 Disponibilidad y Continuidad TOIP....188
Ilustración 209 Equipos consola antivirus....196
Ilustración 210 Gestión consola antivirus – equipos usuario final....197
Ilustración 211 Top 10 Spyware....198
Ilustración 212 Top 10 virus detectados....199
Ilustración 213 Top infección virus....200
Ilustración 214 Gestión consola Nessus....201
Ilustración 215 Escaneos programados....202
Ilustración 216 Vulnerabilidades gestionadas vs en remediación....204
Ilustración 217 Criterios calidad documental casos....206
Ilustración 218 Resultados auditoria de casos....207
Ilustración 219 Precisión error no Critico de llamadas....208
Ilustración 220 Precisión error Critico de llamadas....208
Ilustración 221 Resultados llamadas PENC....210
Ilustración 222 Resultados llamadas PEC....210
Ilustración 223 Seguimiento Práctica Mejora....211
Ilustración 224 Resultado de Cumplimiento AM....212

Introducción

Objetivo

El presente documento tiene como objetivo dar a conocer a la entidad el informe mensual sobre los servicios y componentes de TI que soportan la infraestructura tecnológica en el Ministerio del Trabajo, de acuerdo con las obligaciones contractuales establecidas en el contrato No. 574 de 2023 suscrito con la ***Unión Temporal Gestión TIC 2023***.

El informe presenta los resultados y el análisis de la gestión de los servicios para el periodo en evaluación que corresponde al mes de agosto de 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: Servidores de Bases de Datos (Apps Archivo Sindical, Cobro Coactivo, MIPPAM, Moodle, Siriti, SISGestión, Visitas, Collector, SVE, Centros de entrenamiento, PRIEV, entre otras).
- Aspectos claves para **creación de contraseñas seguras** de acceso a la red, los sistemas de información y aplicaciones; así mismo, se informa que no se deben almacenar contraseñas en navegadores de equipos de cómputo por seguridad de la información y para evitar el bloqueo de usuarios en el dominio por políticas internas.
- **Canales de atención** disponibles para comunicarse con la **Mesa de Servicios** del Grupo de Soporte Informático.
- El 14/08/2025 se brinda apoyo a la Oficina TICs en la publicación de un fondo de pantalla que hace parte de la ejecución del plan de sensibilización y comunicación en seguridad de la información relacionado con la **Política de uso del servicio de acceso a internet del MinTrabajo**.
- Aclaración de emisión del **proceso de devolución de bienes y elementos tecnológicos asignados**, VoBo y Paz y Salvo por parte de la persona encargada del Grupo de Soporte informático.

Temas en curso:

- Se presentó al Coordinador del Grupo de Soporte Informático piezas propuestas actualizadas para la divulgación de los lineamientos de OneDrive para que los usuarios finales sincronicen la información institucional; para ello se creó un fondo de pantalla, y una pieza de comunicación con el instructivo para ser divulgada a través de Soporte MT solicitamos revisión y aprobación para dar inicio a la publicación recurrente. Se recibe el VoBo correspondiente y se distribuirán de forma periódica a través del buzón de Soporte MT y el fondo de pantalla.

b. Traslados y novedades de sedes:

- **Anserma / Caldas:** Por remodelación física de la alcaldía del municipio, la sede fue trasladada temporalmente el 8/03/2025 a un local cercano a cuenta del inspector mientras terminan las adecuaciones. Se tiene en seguimiento hasta que se requiera retorno al lugar definitivo y organización de los equipos a cargo de la UT.
- **Santa Barbara / Antioquia:** El 27/06/2025 el inspector se retiró por pensión, pero no se tiene una nueva asignación de personal para la sede. Equipos es sede se encuentran apagados, a espera de novedades en relación con la asignación de funcionario.

- **Barrancas / Guajira:** El 27/08/2025 la sede se encuentra apagada por arreglos locativos que culminan según información el 9/09/2025.

c. Volumetría de Solicitudes Gestionadas:

En el mes de agosto 2025 se registraron en la herramienta ITSM 6922 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: 5899
  - Incidentes: 1000
  - Cambios: 23
  - Problemas: 0
- Casos Anulados: 8 - 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 Agosto 2025:

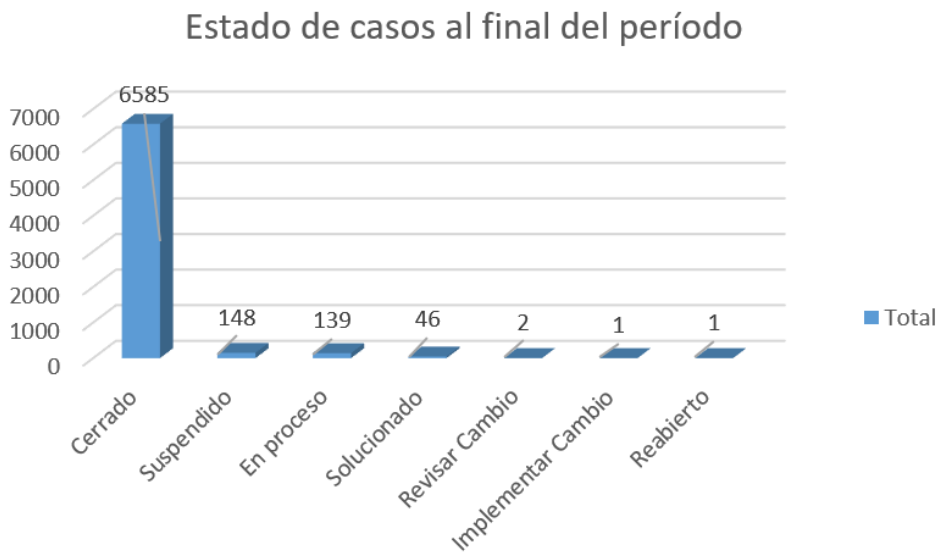


Ilustración 1 Estado de casos en el período

- Gestión por parte de los grupos de especialistas:

Grupo Responsable	Cantidad de casos gestionados	Porcentaje de casos gestionados (%)
Responsable_Soporte_Bogota	2044	29,53
Responsable_Soporte_Territoriales	1814	26,21
Responsable_Mesa_De_Servicio	669	9,66
Especialistas_IBM	660	9,53
Responsable_Soporte_Impresoras	644	9,30
NOC	632	9,13
Responsable_De_Servidores_Windows	129	1,86
Especialista Nube Privada	71	1,03
Especialista_Telefonía_IP	60	0,87
SOC	50	0,72
Especialista Base de datos	28	0,40
Especialista Herramientas de Gestion	24	0,35

Responsable Garantías Equipos	21	0,30
Especialista Nube Publica	17	0,25
Especialista Redes	14	0,20
Especialista Aplicaciones .Net	14	0,20
Gestor de Inventarios	11	0,16
Liferay	10	0,14
Almacenamiento y Backups	7	0,10
Gestión del Servicio	3	0,04
TOTAL	**6922**	**100,00**

Tabla 1 Atención de solicitudes por grupo de especialistas

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

En proceso de recibir el VoBo de la coordinación del Grupo de Soporte Informático al segundo paquete de documentos para publicación en la SVE, para que posteriormente se realice 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
- Instructivo Preparación y Asignación del activo

El correo fue enviado el 14/08/2025, se tiene en seguimiento.

e. Disposición de RAEES y Residuos Electrónicos

Durante el período del informe no se gestionaron recolección de residuos por parte del proveedor SUMA Desarrollo Ambiental.

f. Implementación IPV6

El 14 de agosto 2025 se concreta la firma del acuerdo de servicio entre LACNIC y el Ministerio del Trabajo; los documentos firmados fueron enviados en físico a Uruguay a través de la transportadora 4-72 bajo número de guía UP000061353CO. En seguimiento por parte de la UT para la firma correspondiente.

g. 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 28/08/2025 se remite vía correo electrónico al equipo de trabajo de la UT indicando que a partir del 1/09/2025 se hace obligatorio el registro del CI en todos los casos y se da una Aclaración sobre la selección de CI (Elemento de Configuración) en Aranda durante la gestión de casos.

h. Otras actividades

- Se continuó el proceso de recolección de activos propiedad del anterior operador de servicios tecnológicos en las diferentes sedes del Ministerio del Trabajo. Durante el periodo se gestionan los permisos de acceso y autorización de salida, se aclara que esta actividad continuará para el siguiente período: Delcop: 2 sedes, EyS: 1 sede.

- El 6/08/2025 vía correo electrónico se da respuesta a Maria Camila Acosta con información del cuatrimestre que contiene las evidencias de manejo ambiental y gestión de residuos tecnológicos y suministro de resmas de papel. Los documentos entregados fueron:

  Instructivo Recolección y Disposición de Residuos Especiales
  Reporte de la cantidad de residuos tecnológicos en el cuadro de control de abril a Julio 2025 y Matriz de compatibilidad de residuos en el mismo archivo, archivo con nombre: PRG-MNF-0808-F2-E1-Seguimiento Abril-Julio2025.xlsx
  Certificados de disposición final expedidos por SUMA (Desarrollo Ambiental) durante abril a julio 2025:
  - *Certificado Valle del Cauca*
  - *Certificado Territorial Bucaramanga*
  - *Certificado Disposición-Tratamiento Territorial Antioquia*

  Certificado de Manifiesto de la última recolección de sede Central del 17/07/2025.
  Despachos por resmas de papel a Nivel Nacional
  Control de recarga de resmas en impresoras - Territoriales, Oficinas Especiales e Inspecciones Municipales
  Control de recarga sede Nivel Central, edificio WTC
  Consumo_Papel_Bogota
  Archivo Clics impresoras abril -julio por sedes.

- El 8/08/2025 se envía correo al Coordinador del Grupo de Soporte Informático solicitando revisión y VoBo de la Encuesta de percepción del personal de soporte en sitio territorial, con el propósito de retomar la medición de la percepción del cliente e implementar las acciones de mejora correspondientes. A espera de respuesta.
- El 13/08/2025 se reitera por correo electrónico la novedad de la DT Caldas donde se requieren puntos de red en el piso 7, se requiere de cableado y canaleta desde cuarto técnico donde se encuentra los switches de acceso, ya se ha informado a la territorial que este requerimiento se debe tramitar con recursos físicos. Se tenía una solución temporal de conexión por MiFi pero el usuario presenta problemas de conectividad por la ubicación del archivo.
- El 26/08/2025 se comparte a la Oficina de TICs la Información de Disponibilidad de los equipos de DataCenter del primer semestre 2015. Lo anterior a solicitud de ellos para crear indicador de disponibilidad de infraestructura.
- Se tiene en proceso de delegación al personal de MDS la actividad para realizar la búsqueda y exportación de información de una cuenta de usuario en eDiscovery, lo anterior con el propósito que sea atendida y resuelta en primer y segundo nivel sin necesidad de realizar un escalamiento a especialistas de Windows. Para este proceso, se realizó un instructivo detallado con el paso a paso de las actividades a desarrollar y una sesión de transferencia de información al personal de la mesa que intervendrán en estos casos. Se tiene en proceso de afinamiento los flujos de trabajo según los escenarios posibles.
- El 21/07/2025 se reporta vía correo electrónico al Coordinador del Grupo de Soporte Informático la novedad de la UPS de la OE Apartadó (propiedad del ministerio), ya que el personal de soporte en sitio reitera que se vienen presentando eventos sobre el equipo, el apoyo que brinda actualmente nuestro técnico es generar el reinicio correspondiente, pero en ocasiones algunos usuarios de la sede no comprenden que se encuentra fuera de nuestro alcance su reparación y atención.
  A espera de recibir poyo para que la dependencia responsable de este equipo pueda emitir una respuesta formal a la directora de la OE con el propósito de oficializar las acciones que se desarrollarían para esta UPS.

2.1.1. Herramienta de Gestión ITSM

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

- El 5/08/2025 se ejecuta RFC para la actualización de ADM a la versión 9.23.0.
- Se realizó la depuración de la base de datos de zabbix dejando que esta únicamente almacene los datos de los último 6 meses, esto con el fin de optimizar el uso del almacenamiento.

- Se optimizó las solicitudes de ping que realiza zabbix a los hosts para evitar que estos saturen la base de datos y ocupen más espacio del necesario.
- Afinamiento de mediciones de uso de banda ancha para SDWAN para las Direcciones Territoriales en Zabbix.
- Mejora en los mantenimientos creando un formulario que ha permitido aumentar la velocidad con la que estos se crean, ahora se pueden realizar mantenimientos de manera masiva reduciendo tiempos de operación.
- Modificación del flujo de estados para las categorías de CMDB, creando nuevas categorías para lo CI de tipo audiovisuales.

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 31 de agosto 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 31 de agosto de 2025. Este apartado contiene información relevante sobre actividades realizadas y novedades presentadas.

- **Tipificación de los cambios**

Durante el mes de agosto de 2025 se gestionaron 23 casos tipificados como Cambios, clasificados en las siguientes categorías:

CATEGORÍAS	NÚMERO DE CASOS	PORCENTAJE (%)
Administración de servidores.Servidores	9	39,13%
Administración de Bases de Datos.Servidor de base de datos	7	30,43%
Herramientas de Gestión.Aranda	4	17,39%
Herramientas de Gestión.Zabbix	1	4,35%
Telefonía IP.Infraestructura de telefonía	1	4,35%
Aplicaciones Especializadas.Gestor Documental	1	4,35%
Total General	**23**	**100%**

Tabla 2 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 31 de agosto de 2025, en total se crearon 23 casos de los cuales se gestionaron 4 como cambios de normales, 6 cambios estándar y 13 cambios de emergencia, los cuales se describen a continuación:

SHC_Agosto_2025.xlsx

- **Cambios por estado**

Al corte del 31 de agosto, veintidós (22) casos quedaron estado *Cerrado* y un (1) caso quedo en Revisar Cambio.

- **Medición Indicador Porcentaje de Cambios Exitosos**

Nombre	Descripción / Fórmula	Meta	Periodicidad	Resultado Agosto
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=22/23*100** **PCE= 95,65%**

Tabla 3 Medición Indicador Porcentaje de Cambios Exitosos

En el mes se implementaron **23 cambios**, de los cuales **22 fueron exitosos** y 1 presentó inconvenientes, debido a que uno de los scripts arrojo error. Se notificó del error al usuario para que realice los ajustes correspondientes y realice una nueva solicitud de ejecución con el respectivo RFC.

El valor obtenido (**95,65%**) supera la meta establecida del **80%**, lo que evidencia un adecuado control en la planeación, aprobación y ejecución de los cambios.

Este resultado refleja que:

- La mayoría de los cambios fueron implementados de manera correcta, minimizando el impacto en los servicios.
- Los procedimientos de gestión de cambios han sido efectivos, garantizando la continuidad operativa.
- La desviación (un solo cambio no exitoso) está dentro de lo aceptable y no compromete el cumplimiento del objetivo.

2.1.2.3. Práctica Gestión de Activos

Durante agosto de 2025, la Práctica de Gestión de Activos ejecutó diversas acciones estratégicas orientadas a garantizar la continuidad operativa y la disponibilidad óptima de los servicios tecnológicos de la Entidad. Todas las actividades se desarrollaron bajo lineamientos de mejores prácticas en gestión de activos, con el fin de fortalecer el control, la eficiencia operativa y la trazabilidad de los recursos tecnológicos.

- **Seguimiento a la gestión de garantías:** Se realizó monitoreo y control sobre las garantías de los activos tecnológicos que presentaron fallas o requerimientos técnicos dentro de su periodo de cobertura. Esta gestión tuvo como objetivo asegurar el cumplimiento de las condiciones contractuales con fabricantes y proveedores, así como garantizar la atención oportuna de los incidentes reportados.
- **Gestión de software permitido y no permitido:** Se realiza seguimiento del software instalado en los equipos de la Entidad, estas actividades abarcaron la verificación del nivel de actualización del parque computacional y el seguimiento a la instalación de aplicaciones no autorizadas. Dichas acciones son determinantes para mantener la seguridad, la legalidad y el buen funcionamiento de la infraestructura tecnológica.
- **Gestión del inventario de activos tecnológicos:** A la fecha de corte del periodo, el inventario registrado en Aranda asciende a **3.526 activos**, incluyendo: portátiles, servidores, equipos de escritorio, aplicaciones, monitores, impresoras, UPS, teléfonos, NUC, switches, access point, diademas, dispositivos Fortinet y Mi-Fi.

Respecto al periodo anterior, se evidenció un incremento significativo en el inventario de equipos físicos, derivado del alistamiento y configuración de nuevos dispositivos asignados a contratistas y practicantes. Actualmente, la Entidad cuenta con:

- 937 portátiles en operación a nivel nacional.
- 183 portátiles en almacén.
- 1.145 equipos de escritorio en operación.
- 27 equipos de escritorio en almacén.

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:

- **Refuerzo y capacitación árbol de categorías:** El 15 de agosto 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 de acuerdo con los hallazgos encontrados en la revisión de casos. 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.

- **Creación de Nuevas Categorías**

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

Creación Categoría Actualización BIOS
Creación Categoría Eliminar Hostname

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 Agosto
Porcentaje de cumplimiento de la actualización del Catálogo	**CPS=(TCG/TCE) *100** **CPS:** Cumplimiento en la prestación de los servicios **TCE:** Total de casos escalados (Recibidos) (Modificación, Agregar o Desactivar el servicio). **TCG:** Total de casos gestionados (Solucionados) (Modificación, Agregar o Desactivar el silencio).	90%	Mensual	**CPS= (2/2)***100 **EF= 100%**

Tabla 4 KPI Práctica Catálogo de Servicios

En conjunto con la práctica de ANS se está revisando el catálogo de servicios con el fin de realizar los ajustes necesarios a nivel de categorización, servicios, grupos resolutores y ANS.

2.1.2.5. Práctica de Problemas

Dar a conocer las actividades de la Práctica de Problemas correspondientes al periodo del 1 al 31 de agosto 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.

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

CI afectado	# casos creados	Estado de los casos
Controlador de dominio	1	Solución definitiva - cierre
Módulo de radicación - Gestor documental	3 2 1 1	Error conocido Solución Temporal Solución definitiva Investigación y diagnóstico
MINTRABGD01A - Gestor documental	1	Investigación y Diagnóstico
Office 365	1	Error conocido
Página web	1	Solución definitiva - cierre
servicio de relay en el ISS	1	Solución Temporal
SISINFO	1	Solución Temporal
Telefonía	1	Solución definitiva - cierre
UPS Manizales	1	Solución Temporal
Total	13	

Tabla 5 Consolidado de casos creados

Durante el mes de agosto se realizó seguimiento a dos casos tipo problema asociado con el Gestor Documental.

ID Problema	Servicio TI/ Gestion ITIL Afectado	Problema identificado	Líder Técnico o Funcional del servicio	Causa Raiz	Solución	# Casos Relacionados	Estado Aranda
133831	Gestor documental	se está presentando una novedad recurrente con el gestor documental. Esta situación se debe a una alta transaccionalidad en las instancias y un procesamiento elevado, lo que genera lentitud significativa y en ocasiones la caída del aplicativo. Como medida de mitigación, los especialistas proceden al reinicio de los servicios; sin embargo, se han evidenciado intermitencias con durabilidad de aproximadamente 7 minutos.	Jimmer Molina	Las áreas funcionales de la entidad no permitieron la realización del mantenimiento ya que generaba indisponibilidad de la aplicación y también se realizaba la inactivación de los radicados pendientes por gestionar, falta de conocimiento por parte de los funcionales de las limitaciones de la infraestructura actual de la plataforma	Realización del cambio para bajar servicios de aplicación gestor documental, para proceder con las tareas de mantenimiento de tablas de la aplicación gestor documental, desfragmentación, reconstrucción de índices, ejecución de estadísticas en base de datos MINSTRASG, y mantenimiento servidores de aplicación.	131900, 131908, 131910, 131914, 131934, 131940, 131941, 131948, 131949, 131911	Solución Definitiva

Tabla 6 Detalle problema 133831

Se realizó actualización a la cross connection y se ejecutó el mantenimiento mensual del sistema gestor documental el cual fue satisfactorio, a la fecha no se han presentado nuevos incidentes relacionados con la misma situación del problema identificado. Se procede al cierre del caso con solución definitiva.

ID Problema	Servicio TI/ Gestion ITIL Afectado	Problema identificado	Líder Técnico o Funcional del servicio	Causa raíz	Solución	# Casos Relacionados	Estado Aranda
137015	Gestor documental MINTRABGD 01A	Desde la práctica de Incidentes se postula problema con la siguiente información: De acuerdo con lo conversado y con los incidentes registrados el pasado martes 22 de julio,	Brayan Quintero	Al realizar la migración de servidores físicos a servidores virtuales se presentan conflictos lo que ocasiona inconvenientes con	1. Creación de registro en Active Directory Sites 2. Deshabilitar agente de fortiSIEM para validar	IM-136737, IM-136745 IM-136013,	Investigación y diagnóstico

		relacionados con la caída del Gestor Documental en dos ocasiones, situación ocasionada por el bloqueo del servidor MINTRABGD01A, informo que el día de hoy se presentó nuevamente la misma novedad, afectando de nuevo la disponibilidad del servicio. Hasta el momento no se ha identificado la causa raíz del inconveniente. Como solución temporal, los especialistas acceden al servidor a través del administrador de VM y realizan un reinicio controlado de la máquina, lo que permite restablecer los servicios.		el sistema operativo sin aparente causa raíz. Inconvenientes para la obtención de los medios de instalación en el portal del fabricante.	monitoreo y comportamiento 3.Realizar monitoreo del comportamiento del servidor 4.Definir plan de acción de acuerdo con los resultados del monitoreo del comportamiento 5.Una vez se presente el evento nuevamente se propone: Desplegar un script antes de proceder con el reinicio del equipo para levantar los servicios y lograr recolectar los datos de la falla (con el propósito de realizar un análisis detallado) Aprovisionamiento de nuevo servidor Culminar la configuración del nuevo servidor (instalación, pruebas, RFCs)	IM-135998, IM-135999, IM-136004, IM-136007, IM-136008, IM-136009, IM-136010, IM-136011, IM-136018, IM-136072, IM-136073, IM-136080, IM-136081, IM-136082, IM-136083, IM-136084, IM-136085, IM-136095	

Tabla 7 Detalle problema 137015

Avances: Se realizó mesa de trabajo con los especialistas IBM para seguimiento a las acciones propuestas, se definió contar con el plan de trabajo para la configuración del servidor aprovisionado para el 22 de agosto de 2025.

Se realizó reasignación del caso a los especialistas IBM teniendo en cuenta que las próximas actividades para dar solución al caso están a cargo de dichos especialistas.
Se realizó mesa de trabajo con los especialistas IBM para revisar el plan de trabajo para la configuración del servidor aprovisionado, se definió un plan preliminar de actividades. Se adjuntó documento en la herramienta de gestión y se programó reunión de seguimiento para el 5 de septiembre de 2025.

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

Durante el período del informe, se registraron 1000 incidentes, este volumen incluye:

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

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

Estado	Cantidad
Cerrado	884

Estado	Cantidad
Solucionado	36
Suspendido	51
En proceso	28
Reabierto	1
Total general	**1000**

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	371	Incidentes presentados en el servicio de redes y conectividad debido a afectaciones en la infraestructura del proveedor, fallas eléctricas en algunas sedes y desconexión o apagado físico de equipos en sitio
Reportar una falla.Alarma Zabbix.FortiGate	137	Incidentes presentados en el servicio de redes y conectividad debido a afectaciones en la infraestructura del proveedor, fallas eléctricas en algunas sedes y desconexión o apagado físico de equipos en sitio
Reportar una falla.Alarma Zabbix.Starlink	60	Relacionado a incidente mayor 136949 en el que se presentó una falla global en el sistema Starlink, adicional, 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.Gestor Documental.Falla Funcional	49	Novedades debido al alto procesamiento en la plataforma lo cual genera lentitud, 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.Atasco	41	Novedades por atasco de papel en el mecanismo de alimentación de las bandejas de las impresoras.
Reportar una falla.Gestor Documental.Falla radicacion	39	Novedades debido al alto procesamiento en la plataforma lo cual genera lentitud, 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.Alarma Zabbix.AP	34	Incidentes presentados en el servicio de redes y conectividad debido a afectaciones en la infraestructura del proveedor, fallas eléctricas en algunas sedes y desconexión o apagado físico de equipos en sitio
Reportar una falla.Falla impresora.No imprime	24	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, envío de documentos para imprimir estando estos bloqueados, entre otros.
Reportar una falla.Alarma Zabbix.Servidor Windows	22	En el top de los servidores con mayor afectación está: MTSGRLBDSQL (20): se observa proceso de SQL con alto consumo en recurso de memoria RAM, el cual es normal por su rol. MINTRAB104: Se realiza revisión de consumo de memoria reportado en servidor MINTRAB104, se procede a restablecer servicio y sesiones que estaban con consumo alto, de esta manera queda superada la alerta.
Reportar una falla.Equipo de computo.Falla - Error conexión a red	21	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.

Tabla 9 Top 10 Incidentes

- **Casos Suspendidos**

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

Grupo Resolutor	Julio	Agosto
Almacenamiento y Backups		2
Especialista Aplicaciones .Net		1
Especialista Nube Privada		2
Especialista Redes		1
Especialistas_IBM		24
NOC		47
Responsable Garantías Equipos		1
Responsable_Soporte_Impresoras	1	1
Responsable_Soporte_Territoriales		1
Total general		**80**

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 agosto, el mes con mayor número de casos en estado suspendido, corresponde a agosto, con un total de 80 casos, lo que representa el 98% del total. Este incremento está relacionado a casos asignados al equipo NOC por escalamientos al proveedor de telecomunicaciones del servicio redes y conectividad debido a incidentes mayores que se presentaron en la zona sur occidente del país el pasado 30 de agosto y al equipo Especialistas IBM debido a backlog represado por novedades en servidor debido al alto consumo

- **Incidentes Mayores**

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

Ticket Arada	SERVICIO AFECTADO	NOVEDAD	CAUSA RAÍZ	Acciones Realizadas para restablecer el servicio	ESTADO ARANDA	FECHA INICIO	FECHA FIN	Tiempo de Indisponibilidad
IM-139397	**Scanner**	No llegan los Scanner	Bloqueo del buzón ralay por parte de Microsoft	Durante el análisis de la novedad presentada con el servicio de escáner, se identificó que un Job del área de Bases de Datos falló, lo que generó el envío masivo de notificaciones al buzón de la cuenta DBA a través del Relay. En total, se enviaron 19.680 correos entre el sábado y el domingo, superando el límite de 10.000 correos permitidos por Microsoft en un periodo de 24 horas. Esto ocasionó el bloqueo automático del buzón por parte de la plataforma. De acuerdo con las políticas de Microsoft, la cuenta será habilitada automáticamente 24 horas después, es decir, a las 09:00 a. m. del 5 de agosto de 2025. Como medida de mitigación, se procedió a independizar el servicio de escáner, el cual se configuró manualmente siendo en las impresoras a nivel nacional. Hasta el momento, culminando con e 90% de las impresoras. Adicionalmente, desde el área de Bases de Datos se inhabilitaron los Jobs	Cerrado	4/08/2025	4/08/2025	8H 10 Min

				implicados y se implementaron acciones correctivas para evitar que este tipo de incidentes se repita. Se confirmo operatividad en las sedes afectadas.				
IM-141545	**Portal Web**	Caída página del ministerio	proceso de vulnerabilidad para todos los portales incluido el portal web MinTrabajo, este proceso scanner de seguridad (o prueba de vulnerabilidades) envía URLs malformadas (ej.: bxss.me). l portal intenta tratarlas como “ámbito de búsqueda” y lanza la IllegalArgumentException, generando muchos errores y crecimiento del log que afectan el rendimiento del servidor (alto uso de memoria y disco).	Se realizo proceso de reinicio de servicio Liferay para los eventos en los cuales el servidor llevaba por fuera más de 1 hora. Se revisaron los logs del día 12 y 13 de agosto se detecto un crecimiento exagerado del tamaño de los logs, normalmente llegan a pesar 20000 Kb y el del 12 de agosto llego a 1670000 Kb y el del 13 de agosto en la mañana ya pesaba 400000 Kb. Se encontraron muchos errores de este tipo: 2025-08-13 15:13:44.513 ERROR [https-jsse-nio-443-exec-72][render_portlet_jsp:122] null java.lang.IllegalArgumentException: The string //xfs.bxss.me?gov.co does not correspond to a valid search scope Se solicitó apoyo soporte a Liferay sobre el tema y ellos me informaron que validara con el equipo de seguridad si se estaba realizando scanner de seguridad (o prueba de vulnerabilidades) por eso solicite al equipo WAF la revisión y en sesión con ellos me informaron que desde el día 12 después de las 6 pm. Iniciaron este proceso, por lo tanto, esta era la causa del problema en el portal. Una vez encontrada la causa se debe esperar a que termine el proceso de vulnerabilidades, el cual termino el día 13 en las horas de la noche, durante este tiempo se realizó monitoreo del servidor del portal y solo se reinició hasta las 10 pm. Cuando ya había finalizado el escaneo de vulnerabilidades.	Cerrado	13/08/2025	13/08/2025	Intermitencias de 10 a 15 minutos aproximadamente
IM-145947	**Internet**	Incidente Mayor Sin internet Zona Norte	falla del transceiver por daño en tarjeta de memoria	ETB genera un cambio de emergencia para la tarjeta averiada, se realiza el cambio y se resuelve la falla de alto impacto en el nodo afectado y las sedes que fueron impactadas por lo mismo realizan pruebas en la sede y confirman operatividad	Cerrado	30/08/2025	30/08/2025	1 H 15 min
IM-145897	**Internet**	Incidente Mayor Sin internet Zona Norte	Falla del transceiver por daño en tarjeta de memoria	ETB genera un cambio de emergencia para la tarjeta averiada, se realiza el cambio y se resuelve la falla de alto impacto en el nodo afectado y las sedes que fueron impactadas por lo mismo realizan pruebas en la sede y confirman operatividad	Cerrado	30/08/2025	30/08/2025	3h 18 min

Tabla 11 Incidentes Mayores Registrados

- **Otras Actividades**

  - Se realizó seguimiento a incidentes en backlog, 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, con base a las novedades encontradas en cada caso.

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 agosto
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=984**/1000*100 **EF= 98,4%**
Porcentaje de Incidentes Reabiertos en el Periodo	**RRP:** Porcentaje de casos Reabiertos en el periodo. **IFS:** Incidentes solucionadas en el período. **IFR:** Incidentes Reabiertos en el período.	<2%	Mensual	**RRP= 6**/920*100 **RRP= 0,65%**

Tabla 12 KPI Práctica de Incidentes

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

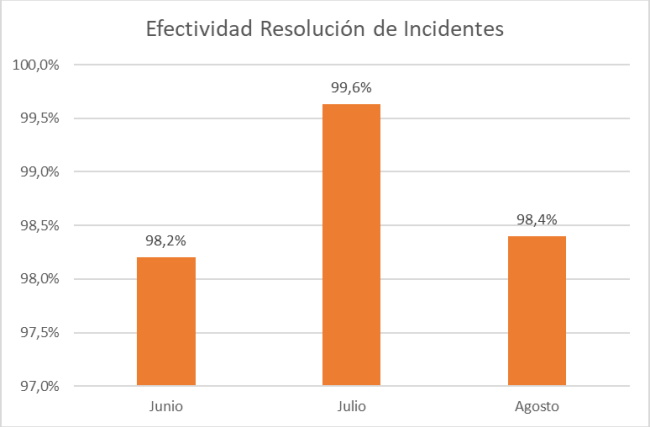


Ilustración 2 KPI Efectividad de Resolución de Incidentes de Servicio

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:

- Junio: 98,2%
- Julio: 99,6%
- Agosto: 98.4%

Se evidencia disminución en el valor del KPI debido a la afectación del ANS en 6 casos, es importante mencionar que el cálculo mensual depende de la cantidad de incidentes reportados en la herramienta de gestión durante cada mes, el desempeño sigue siendo satisfactorio. Como parte de la gestión de la práctica, se realiza retroalimentación con el equipo haciendo énfasis en la documentación y cumplimiento de los ANS definidos por cada servicio. Adicional, se está trabajando en la revisión y ajuste de ANS definidos en el catálogo de servicios.

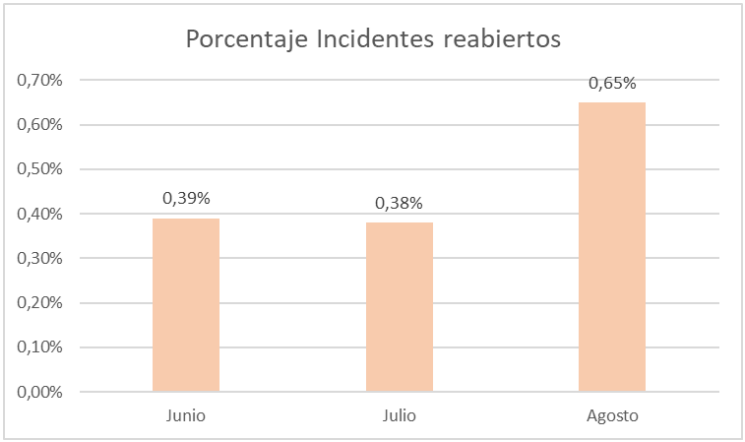


Ilustración 3 KPI Incidentes de Reabiertos en el periodo

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

- Junio: 0,39%
- Julio: 0,38%
- Agosto: 0.65%

A pesar de la disminución, el resultado sigue siendo favorable y refleja una adecuada gestión de incidentes, sin embargo, se visualiza un aumento en la reapertura de casos. A continuación, se relaciona mayor detalle:

Caso	Descripción de la solicitud	Grupo responsable	Causa	Atención al caso
IM-139117	Falla en Gestor Documental al redireccionar radicados	Especialistas_IBM	Usuaria reabre caso indicando que no le han ayudado con la solución de la falla	Se realiza sesión con la Usuaria y se le explica la forma de asignación, funcionalidad de la Búsqueda de radicados, funcionalidad de dependencias y ejecución de esta.
IM-139323	Proactivo Zabbix Mintrabajo Router Santa Marta	NOC	Se verifica caso y se identifica que corresponde a una alarma, se evidenció que el analista de turno del soporte NOC cerró el caso por equivocación escogiendo como razón "solución no aprobada por el cliente"	Se realiza feedback a todos los analistas del NOC
IM-139593	Falla en Gestor Documental al redireccionar radicados	Especialistas_IBM	Usuaria reabre caso indicando que no le han ayudado con la solución de la falla	Se realiza sesión con la Usuaria y se le explica la forma de asignación, funcionalidad de la Búsqueda de radicados, funcionalidad de dependencias y ejecución de esta.
IM-143934	Proactivo Zabbix Mintrabajo Router Riosucio Caldas	NOC	Se verifica caso y se identifica que corresponde a una alarma, se evidenció que el analista de turno del soporte NOC cerró el caso por equivocación escogiendo como razón "solución no aprobada por el cliente"	Se realiza feedback a todos los analistas del NOC
IM-143935	Proactivo Zabbix Mintrabajo Router Riosucio Caldas	NOC	Se verifica caso y se identifica que corresponde a una alarma, se evidenció que el analista de turno del soporte NOC cerró el caso por equivocación escogiendo como razón "solución no aprobada por el cliente"	Se realiza feedback a todos los analistas del NOC
IM-144054	Proactivo Zabbix Mintrabajo Router Riosucio Espinal	NOC	Se verifica caso y se identifica que corresponde a una alarma, se evidenció que el analista de turno del soporte NOC cerró el caso por equivocación escogiendo como razón "solución no aprobada por el cliente"	Se realiza feedback a todos los analistas del NOC

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 31 de agosto 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 5899 casos tipo requerimiento quedando en los siguientes estados:

Estado	Cantidad
Cerrado	5681
Solucionado	10
Suspendido	97
En proceso	111
Total	**5899**

Tabla 14 Estado de Solicitudes

- Durante el mes, se presentaron 5 casos en estado anulado, los cuales corresponden a novedades en la herramienta de Gestión Aranda.
- 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 julio al periodo actual

Grupo Responsable	Julio	Agosto
Especialista Aplicaciones .Net	1	1
Especialista Herramientas de Gestión	1	1
Especialista Nube Privada	1	2
Especialista Nube Publica	3	2
Especialista Redes	1	1
Especialista_Telefonía_IP	0	1
SOC	2	2
Especialistas_IBM	6	7
Responsable Garantías Equipos	10	7
Responsable_De_Servidores_Windows	3	4
Responsable_Mesa_De_Servicio	8	20
Responsable_Soporte_Bogota	9	10
Responsable_Soporte_Impresoras	13	24
Responsable_Soporte_Territoriales	8	15
Total por Periodo	**66**	**97**

Tabla 15 Seguimiento del Backlog Suspendidos

En el inicio del período, se identificaron 66 casos suspendidos correspondientes al backlog del mes de julio de 2025. Se realizaron seguimientos semanales de las solicitudes en estado abierto, logrando la solución de 20 casos a través de la herramienta de Gestión Aranda de los anteriores periodos. Para el cierre del mes, quedaron pendientes 97 casos de agosto, 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 informe técnico de las garantías de equipos.*

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

Tipo de Solicitud	Cantidad
Radicar una solicitud. Impresora. Cargué de papel en impresora	728
Radicar una solicitud. Impresora. Cambio Tóner	498
Radicar una solicitud. Equipo de cómputo. Actualización Bios	362
Radicar una solicitud. Equipo de cómputo. Configuración	269
Radicar una solicitud. Impresora.Instalacion - Configuración	235

Radicar una solicitud.Gestor documental. Relanzamiento	221
Radicar una solicitud. Impresora. Aumento de cuota	217
Radicar una solicitud.Directorio activo. Cambiar contraseña	170
Radicar una solicitud.Gestor documental.Asesoria - Consulta	135
Radicar una solicitud.Gestor documental.Asignar Radicado TYS	112

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.

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=** 5889/5899*100 **EF= 99.83%**
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= 9**/5691*100 **RRP= 0,15%**

Tabla 17 Detalle de KIP Practica de Requerimientos

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

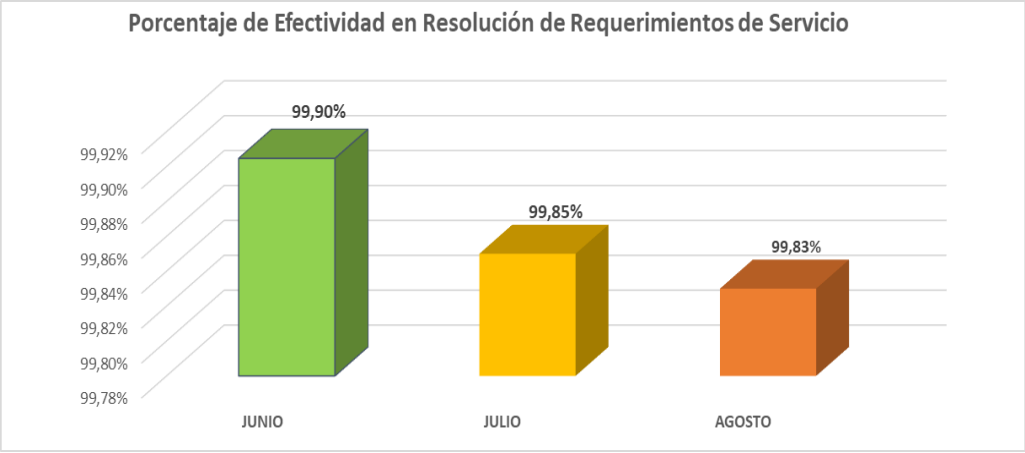


Ilustración 4 KPI Efectividad de Resolución de Requerimientos de Servicio

Durante el periodo, se evidencia el cumplimiento del 99.83% en efectividad de la solución de los requerimientos, los cuales se verifica de 5899 casos registrados en los diferentes canales oficinales de la Mesa de Servicio que fueron solucionados, 5889 casos cumplieron con los tiempos del ANS para dar una respuesta efectiva al usuario y 10 casos no cumplieron la efectividad por no realizar la actualización el estado y seguimiento continuo del caso, por lo cual se continuará las retroalimentaciones a los Servicios TIC.

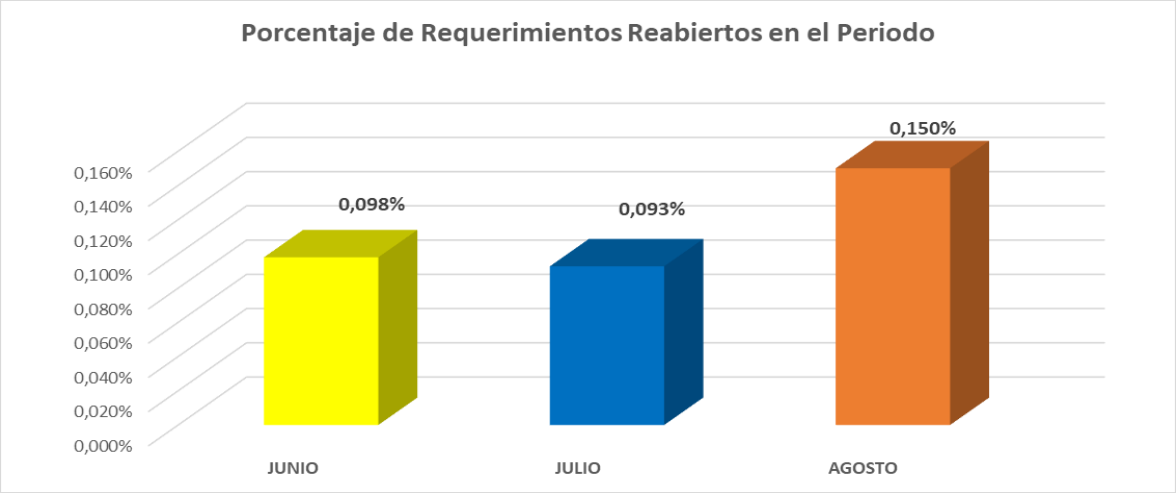


Ilustración 5 KPI Requerimientos de Reabiertos en el periodo

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 9 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-139342	Falla en el DATACAP	Responsable_Mesa_De_Servicio	Usuaria indica que se está presentando falla en el aplicativo de Datacap desde el 01/08/2025 y se comunicó a la mesa de servicio, lo cual se le informo sobre el caso relacionado que está manejando el inconveniente.	El Agente de Mesa de Servicio procede a revisar el reabierto y documenta es un caso informativo y le relaciona el IM-139213 con el que se está trabajando la falla del aplicativo y se cierra el caso.
RF-139224	Solicitud desbloqueo de usuario	Responsable_Mesa_De_Servicio	Usuaria se comunica indicando que no puede acceder al equipo, ya que le genera mensaje: "La cuenta a la que hace referencia se encuentra bloqueada y no se puede utilizar" y el soporte realizado no fue efectivo, ya que durante la llamada con MDS se desbloqueó, pero volvió a presentar el problema y no se resolvió de fondo, por lo que de manera constante el computador se bloquea debiendo radicar de manera reiterada la solicitud. Tengo una semana con el presente inconveniente sin solución de fondo. Relaciono los reportes: RF-138370 RF-138655 RF-137938 RF-138370 RF-138238 RF-138055 RF-137996 RF-137989 RF-137782 RF-137610 RF-137607 RF-137374 RF-136982	Desde MDS se procedió a realizar nuevamente con el desbloqueo de la cuenta en Directorio Activo. 1. El técnico de Soporte en sitio en la sede configuró el equipo de la funcionaria, según las indicaciones del especialista. 2. El técnico de Soporte en sitio en la sede ha realizado seguimiento continuo desde el 01/08/2025 a la fecha, el cual se ha evidencia que el equipo no se ha vuelto a bloquear y no se ha presentado más reportes de novedad por parte del usuario. 3. Se indica a la usuaria por parte de la Mesa de Servicios, que las posibles causas de bloqueo pueden ser debido a contraseñas guardadas en navegador, en el equipo, correos, celulares u otros computadores en los cuales se ingresara al usuario, por contraseñas inseguras o falta de una correcta suspensión del equipo de cómputo cuando no se está utilizando. 4. Se evidencia desde el 01/08/2025 no se ha vuelto presentar bloqueos y se procede al cierre del caso.
RF-143590	RV: RUTEC	SOC	La usuaria no puede acceder a RUTEC desde ningún dispositivo (de la compañía o personal). Algunos miembros del equipo desde Colombia trataron de acceder desde el ordenador de la empresa y tampoco pudieron, pero desde los dispositivos personales si pudieron. Consultamos con el equipo de tecnología de la empresa y nos indicaron que no registran ningún bloqueo con la página de RUTEC por lo que nos recomendaron consultar con ustedes: existe un impedimento	Desde la MDS se evidencia que el caso esta reabierto por la usuaria y que no corresponde la respuesta por lo tanto lo vuelve a escalar y el Especialista SOC realiza una actualización a la respuesta del caso y se procede al cierre.

			para acceder a la página de RUTEC desde el extranjero o equipos corporativo por lo tanto se escala al servicio del SOC y se procede a dar la respuesta, pero al verificar el usuario no estado acorde su solicitud y reabre el caso.	
RF-139622	Gestor documental	Especialistas_IBM	El funcionario informa que tiene fallas con gestor documental, tiene radicados de otras correspondencias, el agente de MDS le indica que se está trabajando su caso otro IM y maneja como informativo, pero al cierre no está de acuerdo y se reabre el caso	Se envía el caso al especialista de IBM para validar el inconveniente y no satisfacción de la usuaria, por lo tanto, realiza sesión con la Usuaria y se le explica la forma de asignación, funcionalidad de la Búsqueda de radicados, funcionalidad de dependencias y ejecución de esta.
RF-139123	Gestor Documental Radicado Duplicado01EE2025726800100010774-01EE2025756800100070774	Especialistas_IBM	El usuario presenta un radicado duplicado en el Gestor documental de dos direcciones territoriales y no está de acuerdo con la validación del especialista.	Se le brinda asesoría al usuario indicándole con base en la información proporcionada, se realizó la validación técnica en la aplicación y se verificó la trazabilidad del radicado indicado, el cual se encuentra debidamente asignado. Adicional se valida y los números finales son iguales pero los subrayados son diferentes, por tal razón no es el mismo número de radicado. Por favor verificar nuevamente en el Gestor Documental y se procede al cierre del caso.
RF-140916	Solicitud eliminación de item que no tienen número de radicado	Especialistas_IBM	El usuario solicita eliminación de un radicado que visualiza en la bandeja del Gestor documental y no le pertenece, por lo tanto, el Especialista le indica que es un tema informativo y todos los perfiles en ese grupo lo pueden ver, pero el usuario no está de acuerdo con la respuesta del caso.	De acuerdo con la información revisada, se le aclara al usuario que las actividades en cuestión no están asignadas de forma individual, sino a varios usuarios, por lo que cualquiera de ellos puede gestionarlas. Solicitamos que nos suministren la información correspondiente para proceder con el retiro de los radicados, considerando que no todas las actividades del gestor documental son responsabilidad directa de quien las visualiza, sino únicamente aquellas que correspondan a su dependencia y funciones asignadas.
RF-141718	Cuota de impresión	Responsable_Soporte_Territoriales	El funcionario informa que no puede imprimir y solicita revisen su impresora, al momento por parte de la MDS se evidencia el caso para aumento de cuota, pero le asignan el saldo y todavía presenta falla al imprimir.	Se realizo por parte del Administrador de Impresión el respectivo saldo, ya que no contaba con cuota de impresión el usuario, pero presentaba adicional una Falla para imprimir en la configuración con el equipo por lo tanto al momento de reabrir el caso, se envía un Técnico de Soporte en Sitio para configurar y se soluciona el caso.
RF-141783	Inspecciones Sena enviado correctamente a bmontano@mintrabajo.gov.co	Responsable_Soporte_Territoriales	Usuaria se comunica a solicitar permisos para ingreso a una URL, la cual está bloqueada, por lo tanto, se realizó él envió del formato de Seguridad perimetral.	Se evidencia que, al momento de documentar la solución de la solicitud, por error del Soporte Técnico al solucionar, documento erradamente y procedió a reabrir el caso y después se solucionó sin inconvenientes.
RF-140297	Reporte de fallos críticos en Moodle – Acceso a administración y gestión de cursos	Especialista Aplicaciones .Net	El usuario presenta fallos críticos con Moodle, por lo tanto, el especialista revisa el caso y documenta el error presentado.	Se evidencia que, al momento de documentar, se cerró sin alguna evidencia y el especialista lo reabrió el caso, adjunto lo pendiente y cierra el caso. Por lo tanto, se procede a realizar Retroalimentación de lo sucedido.

Tabla 18 Casos reabiertos

2.1.2.8. Práctica de Eventos

Para el mes de agosto, 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 802 casos escalados mediante la herramienta de gestión de los cuales 550 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**

  - ✓ Implementación monitoreo consumo de banda ancha para los SDWAN permitiendo saber el porcentaje de ocupación.
  - ✓ Creación de mantenimientos programados a sedes donde realizan apagado de equipos, actividades de cambios programados, entre otros.

- ✓ 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.
- ✓ Cambios en nombres e IP de Host.
- ✓ Inhabilitación de monitoreo para equipos apagados desde infraestructura.
- ✓ Configuración de nuevos hosts para monitoreo.
- ✓ Monitoreo de servicios SQL por medio de agente zabbix 2
- ✓ Automatización de envió de bitácora NOC.
- ✓ Automatización de creación de mantenimientos, por medio de esta se mejoraron los tiempos de creación de loa mantenimientos, haciéndolos más precisos y evitando errores.

Actividades realizadas desde la Gestión de Eventos:

- ✓ Se realizó seguimiento a casos en backlog
- ✓ Se realizó seguimiento de alarmas diarias en Zabbix y se envía reporte diario con apoyo del equipo NOC
- ✓ Solicitud de mantenimiento de sedes en las que los funcionarios apagan los equipos y/o se ausentan de las mismas 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.
- ✓ Implementación de formato para la automatización de mantenimientos

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 agosto
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= (**520/550)*100 **EF= 95%**

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 agosto. Se gestionaron un total de 550 incidentes con las siguientes características:
Los Routers fueron el componente con mayor incidencia durante el mes, concentrando 267 casos (49% del total). Esta situación está relacionada principalmente con la inestabilidad de la red eléctrica en zonas remotas y con condiciones ambientales adversas.

En segundo lugar, los dispositivos FortiGate registraron 89 incidentes (16%), ocasionados por fallas en la energía comercial, apagado de equipos por parte de los funcionarios e intermitencias presentadas fuera del horario hábil. Cabe resaltar que, en estos últimos casos, no fue posible determinar la causa raíz.

Por su parte, las antenas Starlink ocuparon el tercer lugar con 60 casos (11%), evidenciando un incremento frente a meses anteriores. Los incidentes reportados se relacionan principalmente con

problemas eléctricos en las sedes y con intervenciones humanas derivadas del apagado de los equipos.
En cuarto lugar, los servidores Windows representaron 56 incidentes (10%), manteniendo un volumen de casos considerablemente alto frente a los servidores Linux, que solo registraron 4 casos (1%).
Finalmente, los Switches, Access Points, Canal de Internet y UPS en conjunto representaron una baja incidencia del 6% (30 casos), lo que refleja el impacto positivo de la implementación de dependencias en Zabbix.

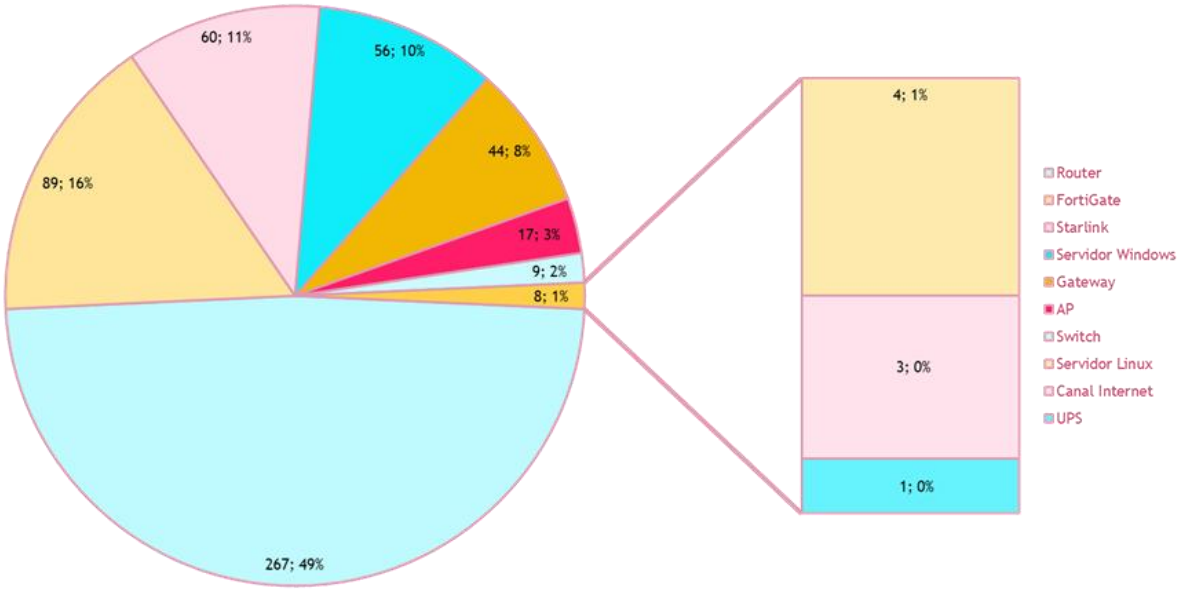


Ilustración 6 Eventos por Tipo de Equipo

Eventos por Categoría de Servicio

A continuación, se presenta un desglose por categoría de las incidencias gestionadas durante el mes de agosto 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.

Redes y Conectividad

- **Router**

Desde el centro de operaciones NOC durante el mes de agosto se gestionaron 267 incidentes relacionados con equipos de red Routers en diferentes sedes a nivel nacional, los cuales representaron el 49% de los casos.

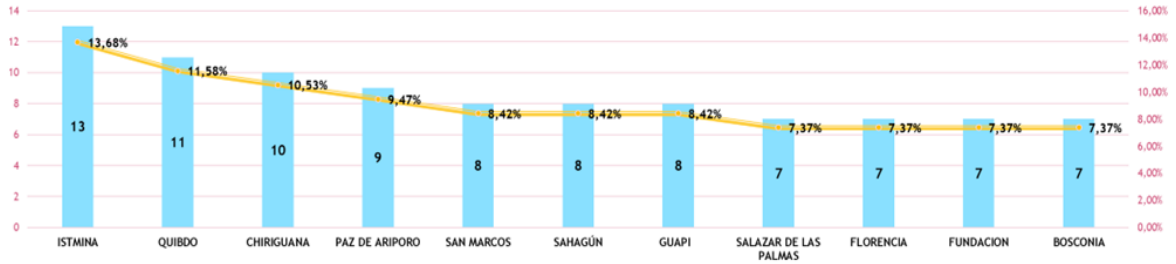


Ilustración 7 Sedes afectadas por router

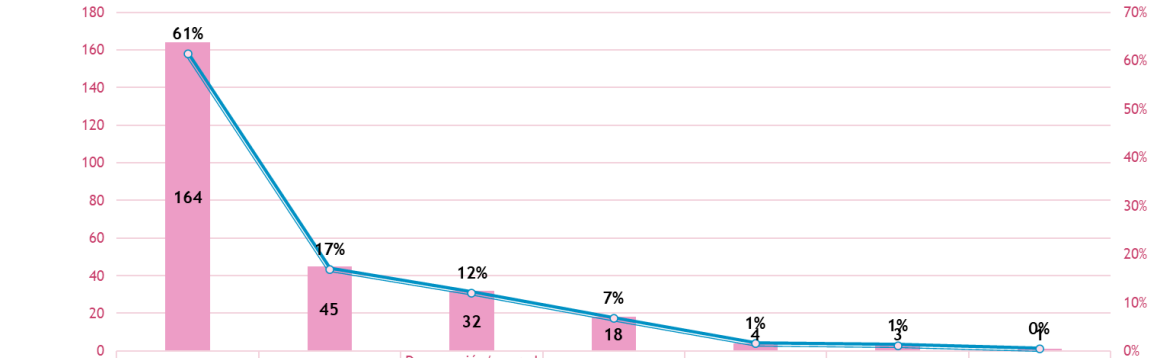
En el mes de agosto, la sede con mayor número de eventos en la categoría de Routers fue Istmina, con 13 incidentes registrados, lo que representa el 13,68% del total. De estos, 9 casos estuvieron asociados a fallas eléctricas en la zona. En segundo lugar, se ubicó la sede de Quibdó, con 10 incidentes (11,58%), manteniéndose entre las sedes con mayor recurrencia de eventos. En este caso, 7 incidentes se debieron a fallas eléctricas.

El tercer lugar lo ocupó Chiriguaná, que ascendió este mes en el ranking con 10 incidentes (10,53%). De ellos, 6 se relacionaron con el apagado manual de los equipos en la sede y 3 con fallas eléctricas en la zona.

En las posiciones siguientes se encuentran sedes como Paz de Ariporo, Sahagún, Salazar, Florencia y Bosconia, que ingresan al top 10 principalmente debido a constantes fallas eléctricas. En estos casos, al igual que en Quibdó, es importante evaluar la implementación de sistemas de respaldo eléctrico robustos.

Por otro lado, sedes como San Marcos, Fundación y Bosconia también se incluyen en el top 10 debido a la desconexión o apagado de equipos al finalizar la jornada laboral por parte de los funcionarios, lo que genera indisponibilidad en el servicio.

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



	Falla Energía Eléctrica	Intermitencia/Lentitud en la red	Desconexión/apagado Físico de Equipos en Sede	Falla en Red de Proveedor	Bloqueo de Dispositivo	Actividad programada	Falla en Red de Proveedor
Cantidad	164	45	32	18	4	3	1
Porcentaje	61%	17%	12%	7%	1%	1%	0%

Ilustración 8 Causas de eventos generados por router

- Se listan 8 diferentes causas de incidentes para Routers: Falla energía eléctrica, intermitencia/lentitud en la red, desconexión/apagado físico de equipos en sede, falla en red de proveedor, actividad programada, servidor apagado y bloqueo de dispositivo.

- Entre las causas con mayor número de eventos tenemos, Falla energía eléctrica la cual puntea con 162 eventos registrados durante el mes para la categoría de Routers, la cual representa el 61%, seguida por intermitencia/lentitud en la red con 45 eventos, representados en un 17%.

- La mayor parte de los eventos por intermitencia registraron un valor inferior a los 30 minutos de duración en Zabbix. También una gran parte se presentaron en horario no hábil, por lo que en dichos casos no se pudo determinar la causa real de las interrupciones ya que no había personal en sitio.

Se evidencia que del total de eventos generados (267) para la categoría de Routers durante el mes de agosto registran entre cerrados y solucionados 257, los cuales representan el 97% de los casos y 9 en estado suspendido, los cuales están pendientes por avances de parte del proveedor de

servicios de internet o pendiente por encendido de equipos y 1 reabierto que está pendiente por descartes de primer nivel en horario hábil.

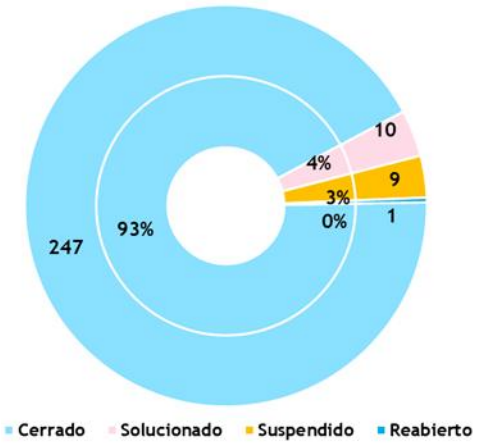


Ilustración 9 Casos suspendidos VS. Casos solucionados de Router

- **Switches**

Desde el Centro de Operaciones (NOC), durante el mes de agosto se generaron 9 casos referentes a Switches en la herramienta de monitoreo Zabbix en diferentes sedes, los cuales representan el 2% del total de los casos, disminuyendo así un 2% en comparación con el mes anterior.

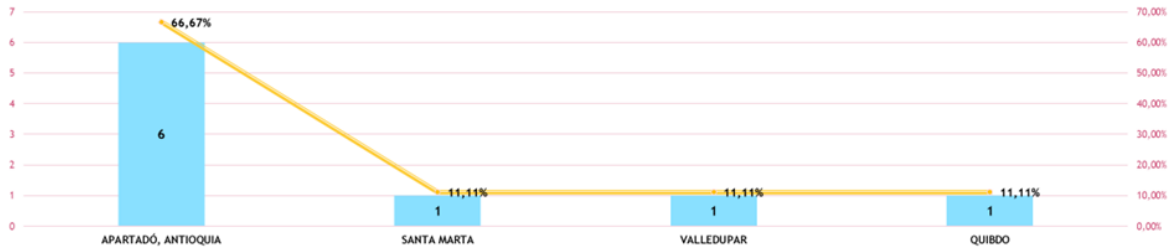
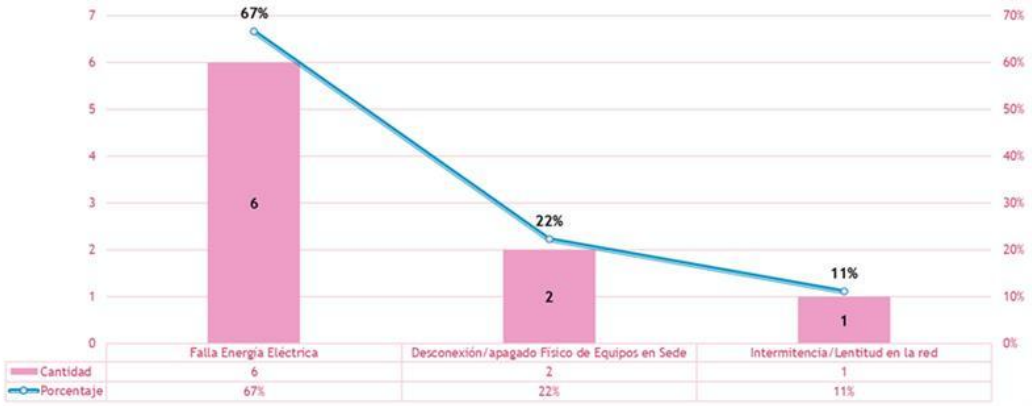


Ilustración 10 Sedes Afectadas

Por parte del grupo NOC en el mes de agosto, se evidencia que de los 9 eventos registrados sobre Switches las sedes con mayor cantidad fueron Apartado, Antioquia con 6 casos y las demás sedes

solo con 1 caso, 4 de los 6 eventos registrados en Apartado, Antioquia por falla de energía del punto y los demás por apagado de equipos.

Las demás sedes presentan mayormente fallas eléctricas y una intermitencia.



lustración 11 Causa de eventos generados por Switch

Se listan 3 diferentes causas para la categoría de Switches registradas durante el periodo del mes de agosto.
De las 3 causas registradas, se evidencia que hay 6 por falla energía eléctrica, que representa el 67% de los casos. Por otro lado, por causa de desconexión/apagado físico de equipos en sede encontramos 2 casos, representando un 22%, en cuanto a intermitencia/lentitud en la red se registraron 1 eventos representando un 11%.

De los 9 eventos registrados para la categoría de Switches en el mes de agosto, los 9 registran en estado cerrado o solucionado, cumpliendo de esta manera el 100% de los casos gestionados por parte del centro de operaciones NOC.

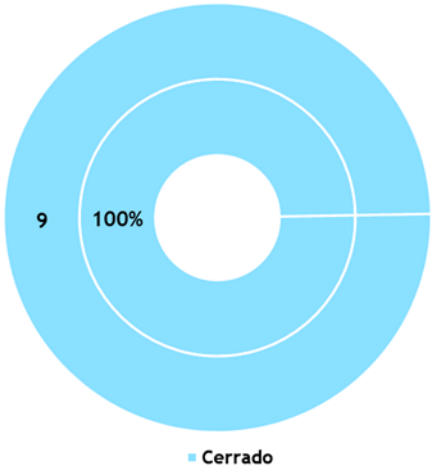


Ilustración 12 Casos suspendidos VS. Casos solucionados de Switch

- **Access Point**

Desde el Centro de Operaciones (NOC), durante el mes de agosto se gestionaron 17 incidentes asociados a equipos de red WLAN – Access Point en distintas sedes a nivel nacional, los cuales representan el 3% del total de casos reportados, aumentando un 1% para este mes. Estos eventos fueron abordados dentro de los niveles de servicio establecidos, sin afectación crítica a la operación general de la red.

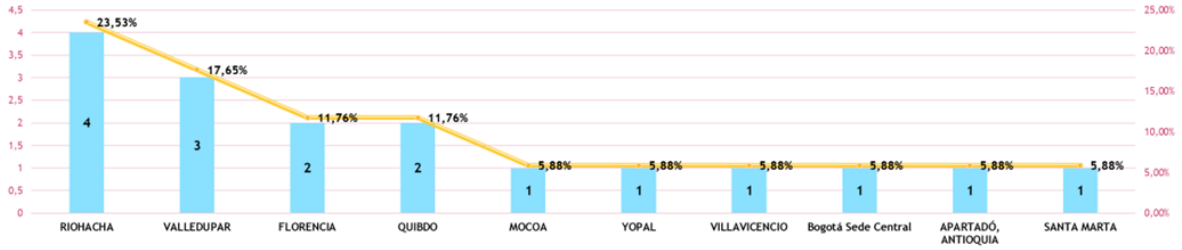


Ilustración 13 Top 10 Sedes afectadas por Access Point

Durante el mes de agosto se evidencia que la sede con mayor número de eventos relacionados con Access Point es Riohacha, con 4 casos que representan el 23% del total de los casos, seguidos de Valledupar quien se mantiene en su posición en los últimos meses, Florencia, la cual registra en el top 10 debido a fallas eléctricas este mes y Quibdó, quien también se mantiene en el top.

Para las sedes de Buenaventura, Villavicencio, Magangué, Bogotá Sede Central las cuales igualan cada una con 1 evento, representando el 8,33% individualmente el total de los casos para esta categoría.

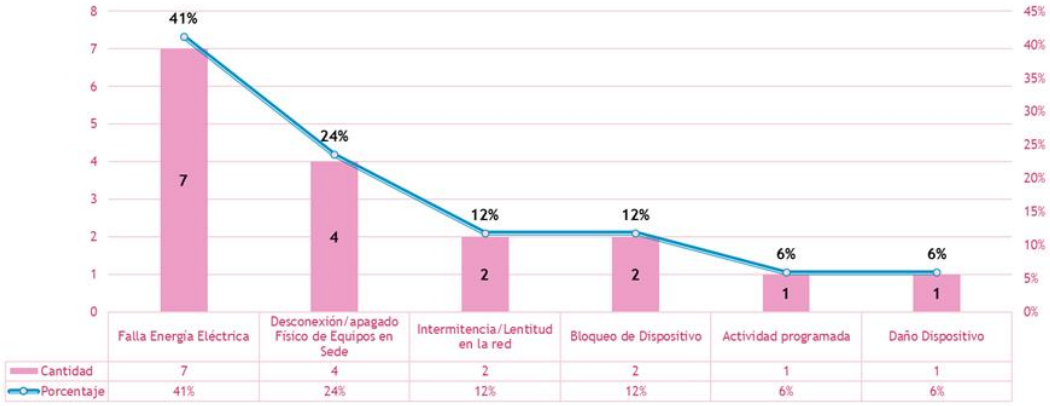


Ilustración 14 Causa de eventos generados por AP

Se evidencian 6 causas de fallas para el periodo del mes de agosto con relación a los dispositivos Access Point.

La causa de energía eléctrica sigue punteando como en otros dispositivos como Routers o FortiGate, con un 41% para AP, seguido de desconexión o apagado de equipos por funcionarios o analistas. Se evidencia una mejoría en la cantidad de casos reportados mes a mes.

Según lo registrado de los 17 eventos generados por Access Point durante el mes de agosto con relación a los casos suspendidos VS. Casos cerrados, se evidencian 17 casos en estado cerrado, es decir el 100% de los casos fueron gestionados, documentados y cerrados.

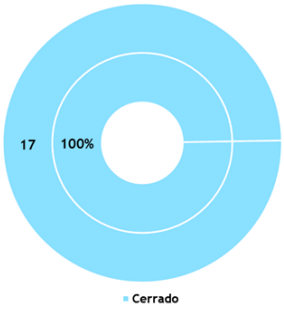


Ilustración 15 Casos suspendidos VS. Casos solucionados de AP

- **Starlink**

Desde el centro de operaciones NOC durante el mes de agosto se gestionaron 60 incidentes relacionados con equipos de red Starlink en diferentes sedes a nivel nacional, los cuales representan el 11% del total de los casos, evidenciándose que para este mes se aumentó un 3% la cantidad de casos.

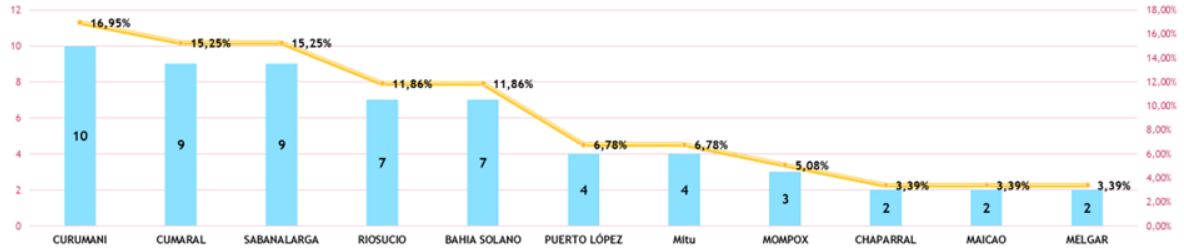


Ilustración 16 Top 10 Sedes afectadas por Starlink

Para el mes de agosto el TOP 5 de las sedes con mayor número de eventos generados para la categoría de Starlink fueron Curumani con 10 eventos, representando un 16%, aunque se mantiene en el primer lugar, se evidencia una disminución de casos, Cumaral con 9 eventos, representando el 15%, sede que también se mantiene en el TOP, Sabanalarga con 9 eventos, representando el 15%, sede que también se mantiene en el TOP, Riosucio y Bahía Solano subiendo en el top con 7 (11%) cada una.

Sin embargo, a pesar de que Curumani se mantiene, se evidencia que esta sede presenta constantes fallas eléctricas, Riosucio Choco, Mitú y Mompox también reporta con múltiples fallas eléctricas. A

diferencia de las sedes anteriores mencionadas, Cumaral, Bahía Solano tiene un número importante de casos asociados a fallas con el proveedor.

Por otro lado, tenemos sedes como Sabana Larga y Puerto López que reportan en el TOP por apagado de equipos. Evidenciando estabilidad en el servicio de las sedes.

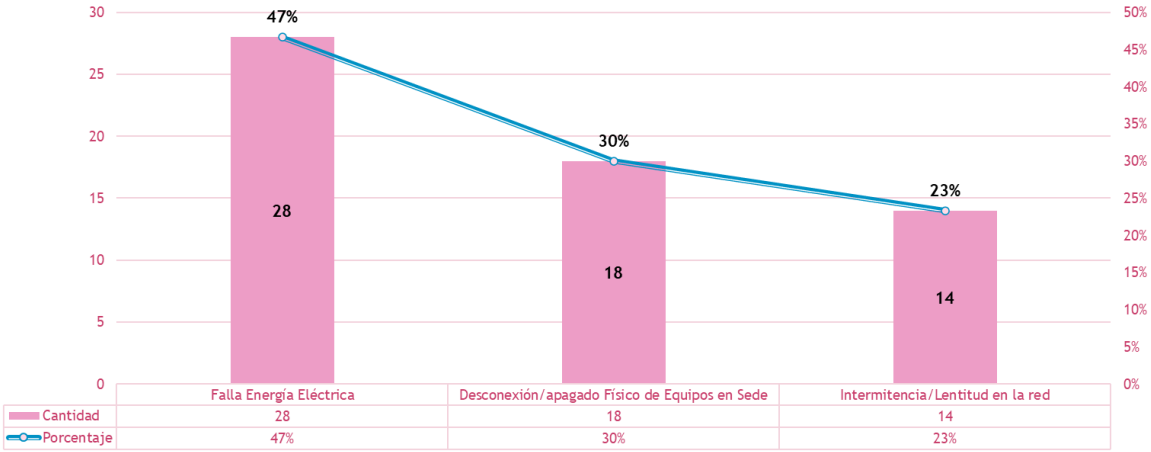


Ilustración 17 Causas de eventos generados por Starlink

- Al cierre del mes de agosto, se evidencia que 2 (3%) de los 60 casos gestionados se encuentran aún abiertos, lo que significa que el 97% casos fueron cerrados dentro del mes del análisis.
- Se listan 3 causas registradas durante el mes de agosto para la categoría Starlink, de las cuales la que más número de eventos tiene es por falla en energía eléctrica con 27 eventos equivalente al 45%, seguido de desconexión o apagado físico de equipos con 17 casos representando un 28% y finalizando con intermitencia/lentitud en la red con 14 eventos equivalentes a un 23% del total de los casos.
- Para incidentes con antenas Starlink se realizan validaciones de primer nivel con equipo de soporte en sitio, una vez realizadas las validaciones se adjunta al ticket las evidencias mediante el servicio “Redes y Conectividad” y se escala al equipo de redes quienes notifican la novedad al equipo responsable APICOM.
- Durante el mes de agosto se pudo observar que la falla en dichos puntos con este dispositivo Starlink se debió a efectos climáticos y por energía eléctrica, lo que ocasiono constantes caídas en este servicio y esto causa mucha intermitencia en los puntos que manejan esta tecnología.
- Hay casos que se evidenciaron durante el horario no hábil y, por lo tanto, no se determinaron las causas reales de las alarmas, debido a que estas subieron a los pocos minutos; estas fallas se atribuyen a intermitencias causadas por malas condiciones climáticas que del mismo modo afectan el servicio de energía.
- En otros casos en que se presentaron alarmas con el servicio de Starlink se pudo indagar que fueron por causa de apagado de equipos con el 28%, ya que este servicio es muy inestable en dichas sedes por la ubicación geográfica en la que se encuentran, los funcionarios prefieren apagar los dispositivos al finalizar su jornada laboral.
- Según lo registrado se evidencia que los casos suspendidos VS. Casos solucionados o cerrados del total de los 60 eventos registrados para la categoría Starlink durante el mes de

agosto, se reportan que el 97% de los casos fueron solucionados y el 3% se encuentran pendientes por validaciones en horario hábil.

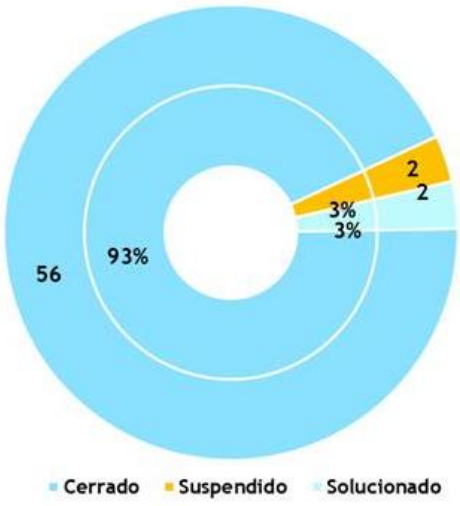


Ilustración 18 Casos suspendidos VS. Casos solucionados de Starlink

- **FortiGate**

Desde el centro de operaciones NOC durante el mes de agosto se gestionaron 89 incidentes relacionados con equipos de red FortiGate en diferentes sedes a nivel nacional, los cuales representaron el 16% del total de los casos, ocupando el segundo lugar.

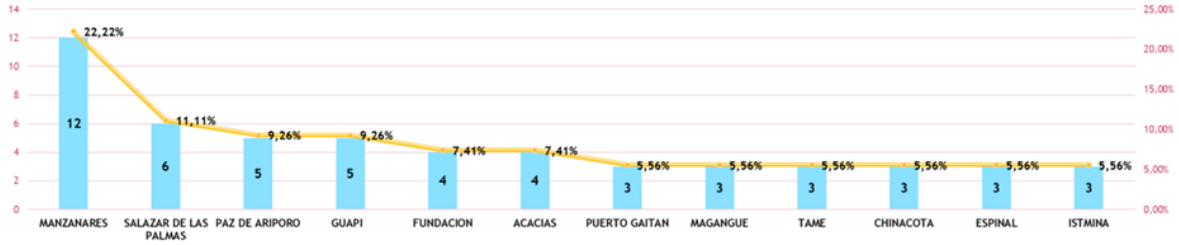
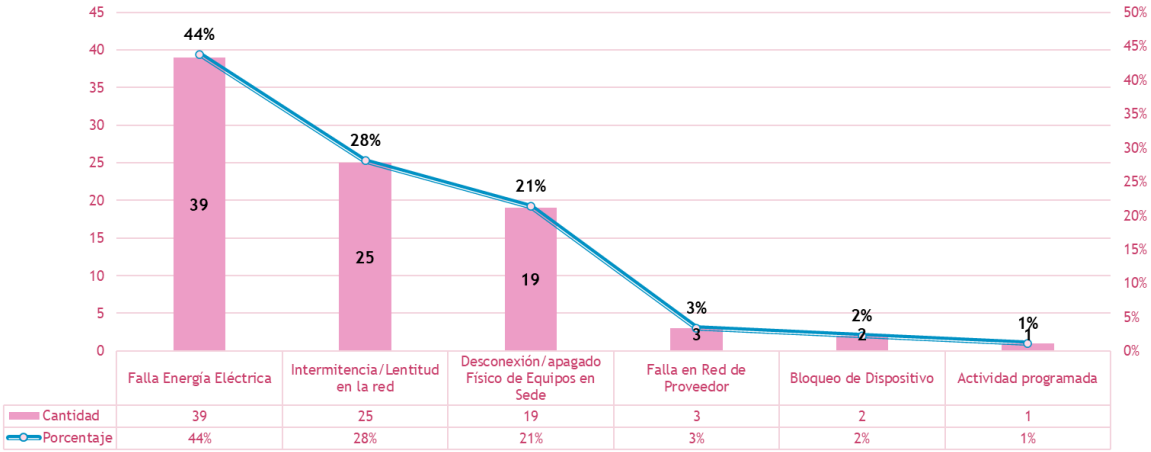


Ilustración 19 Top 10 Sedes afectadas por FortiGate

Durante el análisis del comportamiento de la red SD-WAN en el mes de agosto, se identificó una mayor frecuencia de afectación en las sedes de Manzanares y Salazar de las Palmas. Ambas sedes presentan una alta tasa de eventos críticos asociados al apagado de equipos y fallas eléctricas, 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). Sede como

Paz de Ariporo, Acacias y Guapi, presentan un porcentaje importante en intermitencias asociadas a la red.

Por otro lado, sedes como Fundación, reportan casos relacionados al apagado de equipos en la sede.



	Falla Energía Eléctrica	Intermitencia/Lentitud en la red	Desconexión/apagado Físico de Equipos en Sede	Falla en Red de Proveedor	Bloqueo de Dispositivo	Actividad programada
Cantidad	39	25	19	3	2	1
Porcentaje	44%	28%	21%	3%	2%	1%

Ilustración 20 Causas de eventos generados por FortiGate

- Al cierre del mes de agosto, se evidencia que 2 (2%) de los 89 casos gestionados se encuentran aún abiertos, lo que significa que el 98% casos fueron cerrados dentro del mes del análisis.
- Durante el mes de agosto, los dispositivos SD-WAN presentó un volumen moderado de alarmas, siendo la principal causa las fallas eléctricas con un 44% (39) ocasionadas por condiciones climáticas adversas y validadas por el soporte en sitio. Un 28% (25) 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.
- Seguido de desconexión/apagado físico de equipos en sede con un 21% (19) 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. Finalmente, De los 89 casos relacionados con los dispositivos SD-WAN, 87 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, el 2% de los casos esta pendiente por validación en horario hábil.

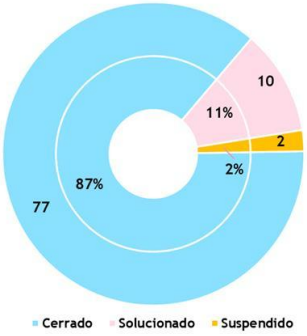


Ilustración 21 Casos suspendidos VS. Casos solucionados de FortiGate

- **Casos Escalados a Proveedor de Telecomunicaciones**

  Durante el mes de agosto se registraron 23 casos que fueron escalados y gestionados con proveedor ETB, de los cuales quedan 19 (83%) que registran en estado solucionado o cerrado y 4 (17%) en estado suspendido.

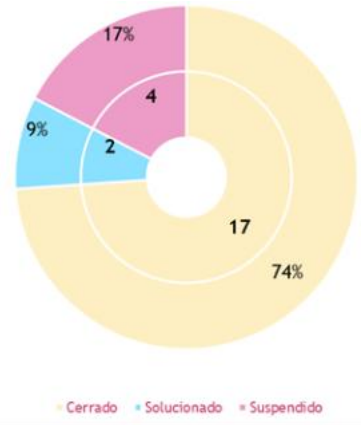


Ilustración 22 Casos suspendidos VS. Solucionados

- El caso en Aranda IM-145069 se relaciona al servicio RInternet_ETB_Villavicencio, el cual está suspendido en espera de parafiscales por parte de ETB para la visita técnica.
- El caso en Aranda IM-145930 se relaciona al servicio RInternet_ETB_Tunja, el cual está suspendido en espera de que soporte en sitio envié los descartes de primer nivel solicitados por el proveedor.
- El caso en Aranda IM-145897 se relaciona al servicio Router_Sahagun, el cual está suspendido en espera de RFO por parte de ETB, ya que esta se presentó debido a una falla masiva donde se confirma daño de la tarjeta de un transceiver.
- El caso en Aranda IM-145731 se relaciona al servicio Router_Florencia, el cual está suspendido en espera de RFO por parte de la última milla AZTECA, quien no ha informado cual fue el motivo de la falla.

Servicios Centrales

Servidores Windows
Durante agosto, el Centro de Operaciones de Red (NOC) gestionó 56 incidentes asociados a servidores Windows, equivalentes al 10% del total de casos registrados en el mes.

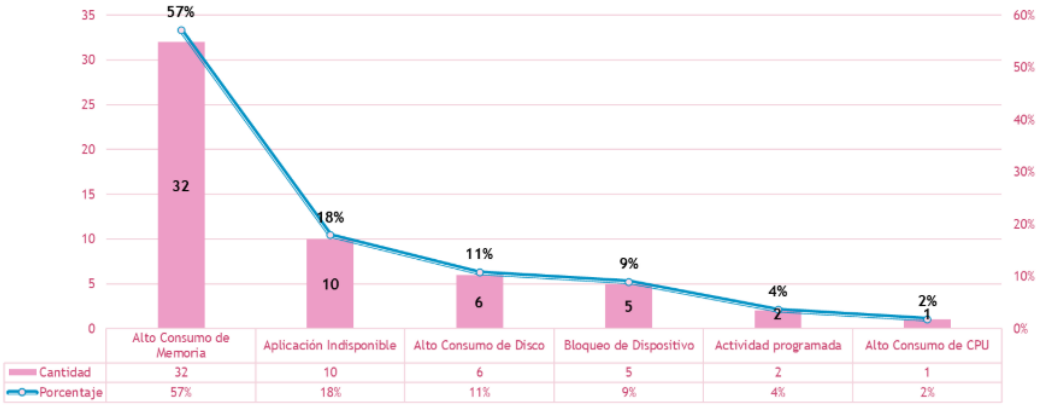


Ilustración 23 Causas de alarmas Servidores Windows

Al cierre del mes de agosto, se evidencia que 5 (9%) de los 56 casos gestionados se encuentran aún abiertos, lo que significa que el 91% casos fueron cerrados dentro del mes del análisis.

El alto consumo de memoria es el principal causante de eventos en el sistema, representando el 57% del total de incidentes, aplicación indisponible ocupa el segundo lugar con un 18% (10) y el alto consumo en disco con un 11%; estos dos últimos muestran una disminución importante en los casos en comparación con otros meses, lo que indica que los esfuerzos de mitigación deben centrarse prioritariamente en optimizar el rendimiento de la memoria.
Otros factores, Bloqueo de dispositivo, consumo de CPU y actividad programada, representan el 9% de los casos, a pesar de que tienen un impacto relativamente menor es recomendable la revisión de las aplicaciones que se están viendo afectadas.

La mitad de los eventos o recursos monitoreados están concentrados en un servidor:
MTSGRLBDSQL (51%)

Este representa el 51% del total, lo cual indica una alta carga o incidencia en este servidor específico. El resto de los servidores tienen una participación mucho menor, lo que sugiere una distribución desigual de la carga o de los eventos. Se recomienda priorizar la atención y evaluación de estos dos equipos para mitigar riesgos de rendimiento o disponibilidad.

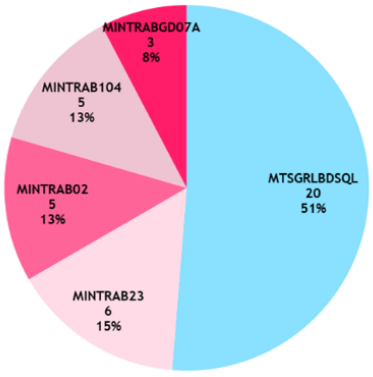


Ilustración 24 TOP 5 de servidores Windows con más alarmas

Se evidencia que, de los 56 eventos registrados durante el mes de agosto, quedan 51 eventos en estado cerrado y solucionado, 1 en estado suspendido y 4 casos en estado en proceso. lo cual refleja una efectiva y oportuna gestión por parte de los especialistas con los eventos reportados, reflejando un porcentaje del 91% de gestión de los casos.

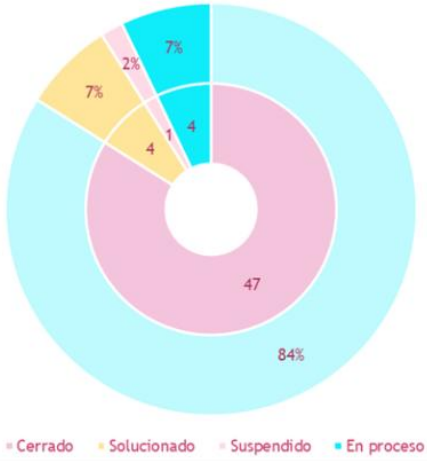


Ilustración 25 Casos suspendidos VS. Solucionados o cerrados Servidores Windows

Servidores Linux

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

.



Ilustración 26 21 Causas de alarmas Servidores Linux

Las causas principales de los eventos registrados muestran que la gran mayoría están asociadas a factores conocidos y potencialmente controlables. El bloqueo de dispositivo es la causa principal, con 3 casos (75%), seguido el apagado de servidores con 1 casos (25%).

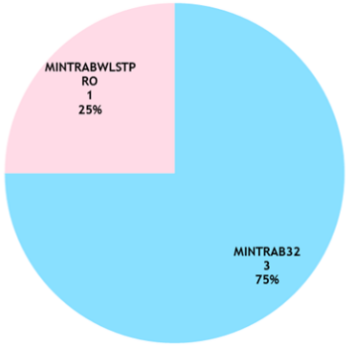


Ilustración 27 TOP 5 de Servidores Linux con más alertas

Se evidencia una mayor concentración de eventos en el servidor MINTRAB32, con 3 eventos, lo que representa el 75% del total. Por otro lado, el servidor MINTRABWLSTPRO registra solo 1 evento, equivalente al 25%. La cantidad de eventos registrados sobre el servidor MINTRAB158 se redujeron totalmente para este mes.

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

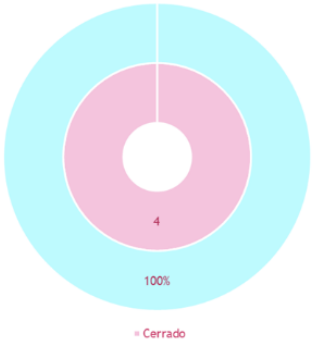
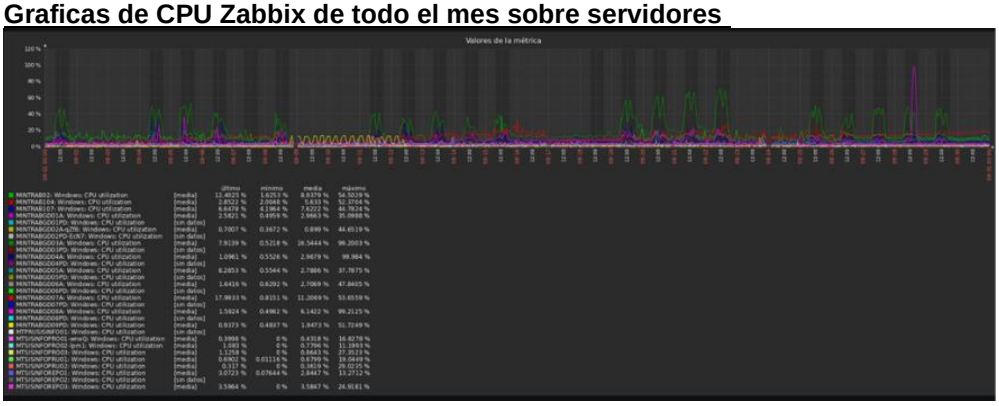


Ilustración 28 Casos suspendidos VS. Solucionados o cerrados Servidores Linux

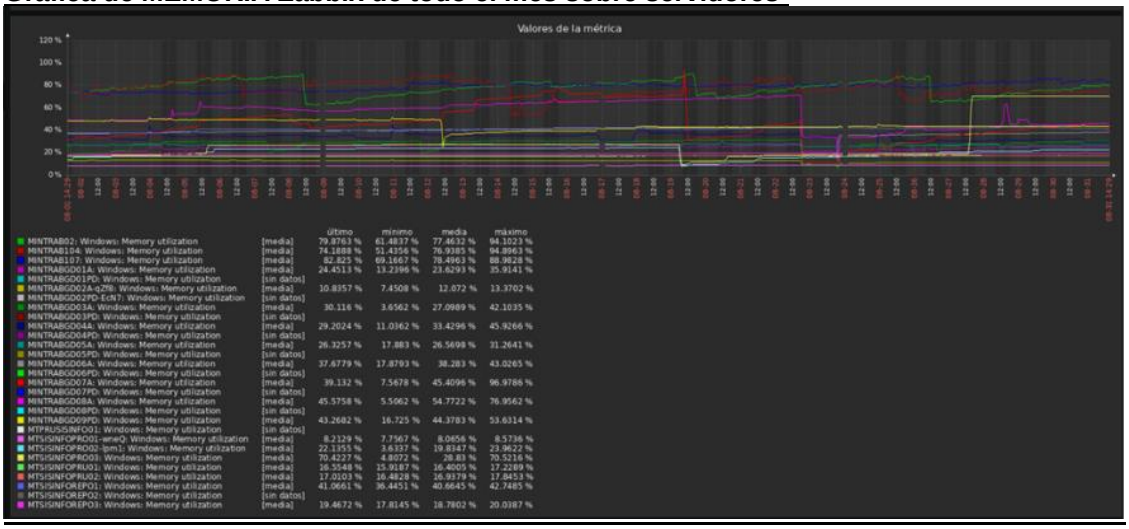
Graficas de CPU Zabbix de todo el mes sobre servidores



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

CPU
1. MINTRABGD03A 16.5444%
2. MINTRABGD07A 11.2069%
3. MINTRAB02 8.9379%
4. MINTRAB107 7.6222%
5. MINTRABGD08A 6.1422%

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 consumo de recursos de MEMORIA durante el mes.

MEMORIA
1. MINTRAB107 78.4963%
2. MINTRAB02 77.4632%
3. MINTRAB104 76.9385%
4. MINTRABGD08A 54.7722%
5. MINTRABGD07A 45.4096

Datacenter (Cali - Bogota)

Durante el mes de agosto, no se reportó ningún incidente relacionado a los Datacenters de Ministerio de Trabajo, lo cual es un indicador positivo en la estabilidad de los canales principales.

2.1.2.9. Práctica de Disponibilidad

Dentro del marco de la práctica de la disponibilidad del servicio se está trabajando en los procesos y las herramientas que permitan cumplir con los objetivos de disponibilidad definidos en la práctica. A continuación, se muestra la información correspondiente a la disponibilidad de los servicios para el periodo del 1 al 31 de agosto de 2025.

Servidores

Cantidad de dispositivos	Disponibilidad consolidada
123	99,97%

Tabla 20 Consolidado disponibilidad de servidores

Se presentó alarmas en el siguiente servidor, según los en el umbral de monitoreo del periodo.

Servidor	Disponibilidad	Aplicación
MTSGRLBDSQL	97,28%	Riesgos Laborales SQL

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 los cuales estuvieron disponibles 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	99,99%

Tabla 23 Consolidado disponibilidad de equipos Datacenter principal

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

Equipo	Disponibilidad
Fortimanager_SDWAN	100,00%
CXV-SWCORE1-RAT42-U44-8360	100,00%
CXV-SWCORE2-RAT42-U42-8360	100,00%
CXV-SWDELL1-RAS42-U43-S4148T	100,00%
CXV-SWDELL2-RAS42-U42-S4148T	100,00%
CXV-SWEDGE-RAT42-U40-6300	100,00%
CXV-SWACC-RAAT38-U41-6300	100,00%
CXV-FG-600F-SDWAN-HUB01	99,99%

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 estuvieron disponibles durante el periodo.

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

Tabla 26 Desagregado Disponibilidad de equipos Datacenter alterno

Redes y conectividad

Cantidad de dispositivos	Disponibilidad consolidada
505	*99,40%*

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	99,99%

Tabla 28 Consolidado disponibilidad de equipos de seguridad

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

Equipo	Disponible
MINTRABSUPERVISOR	100,00%
MINTRABVULNE01	100,00%
SOC_Fortianalyzer	100,00%
SOC_FortiDDOS	100,00%
SOC_SandBox	100,00%
SOC_WAF	100,00%
SOC_FW_Sede_Central	99,98%

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.
- Durante el mes, se realizó una verificación con el Líder de Infraestructura Centralizada sobre los Planes de Disponibilidad del servicio, fechas de seguimiento y ejecución del DRP de Infraestructura Centralizada.
- 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 32 pruebas de alta disponibilidad, de las cuales 24 han sido ejecutadas durante el 2025 por los servicios de los servicios Conectividad, Seguridad de la Información y Telefonía IP y se encuentran ejecutadas y aprobadas en los CAB.

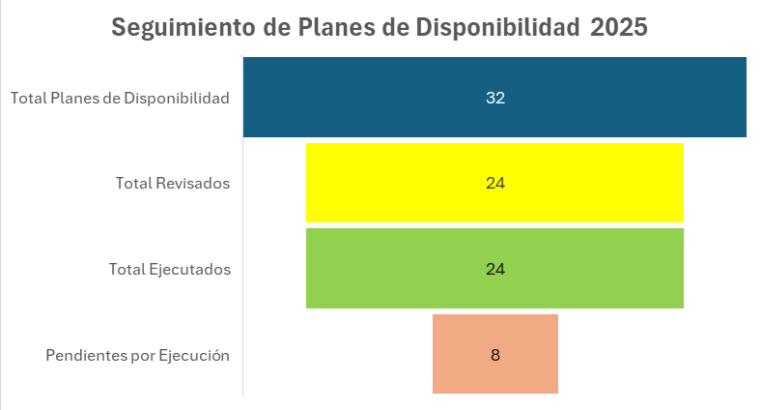


Ilustración 22 Seguimiento Pruebas de Disponibilidad

2.1.2.10. Práctica de Implementación

Dentro de la aplicación de la práctica, se desarrollaron procesos para apoyar a planificar, programar, ejecutar, controlar, aplicar pruebas e implementar nuevos servicios o incluir modificaciones de las funcionalidades de los aplicativos o sistemas de información en producción.

A continuación, se muestra la información correspondiente a la práctica de implementación para el periodo del 1 al 31 de agosto de 2025.

Actividades en curso:

- Revisión de los RFC ejecutadas durante el periodo, los cuales (23) 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 (3) 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 31/08/2025.

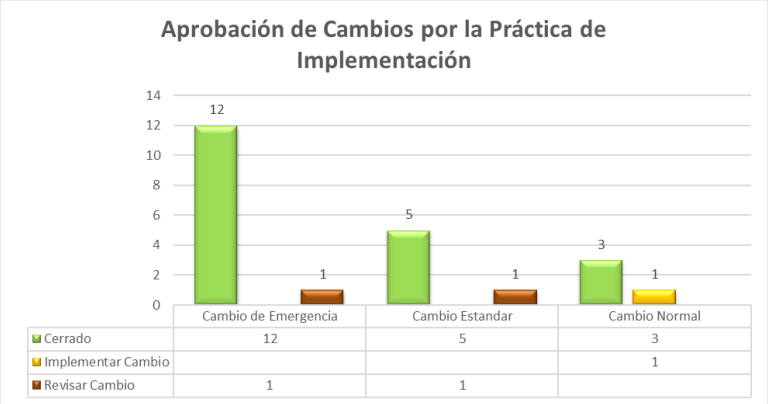


Ilustración 23 Seguimiento Práctica Implementación

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

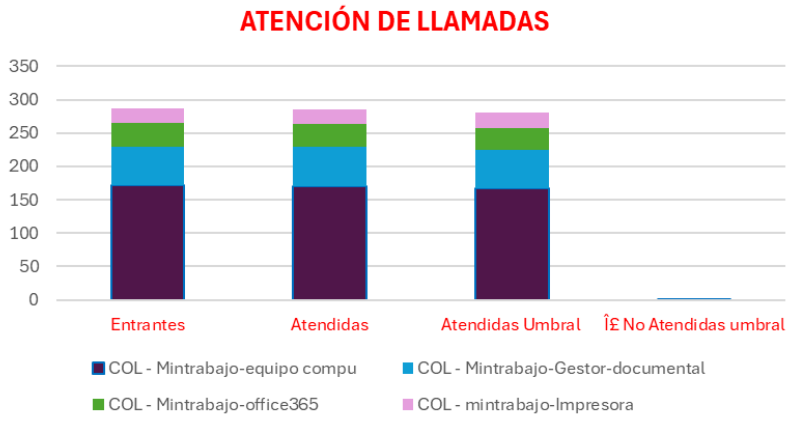
Seguimiento de cambios Implementa

2.2. Mesa de Servicios y Soporte en Sitio

A continuación, se relaciona la gestión desarrollada en el transcurso del mes de agosto, 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 agosto, en el Ministerio del trabajo a la MDS ingresaron 287 llamadas de usuarios finales para solicitar servicios de Soporte Tecnológico, a continuación, se discrimina la clasificación según el servicio solicitado:



Servicio	Entrantes	Atendidas	Atendidas Umbral	No Atendidas umbral	Abandonadas	No Atendidas
COL - Mintrabajo-equipo compu	172	171	168	1	0	1
COL - Mintrabajo-Gestor-documental	58	58	56	0	0	0

COL - Mintrabajo-office365	35	34	34	0	1	0
COL - mintrabajo-Impresora	22	22	22	0	0	0
TOTAL	287	285	280	1	1	1

Tabla 32 Atención de Llamadas

El servicio más solicitado a través de la atención de llamadas es: *Equipo de cómputo* con 172 llamadas entrantes, se atendieron 171 solicitudes, se observa: 1 llamada no atendidas en el umbral por que fue abandonada por el funcionario antes de los 20 segundos.

- Se valida la llamada tipificada como no atendida o abandonada la cual se presenta el día 05/08/2025 15:00:09
- Se procede con la respectiva validación donde se logra evidenciar que la misma se atribuye a una intermitencia presentada por la herramienta Numintec



El caso de fabricante para esta llamada es el ID Ticket 28150471975 donde indican que se debió a una latencia en troncales, lo que causo que la llamada no lograra ingresar al agente final de mesa de servicios.

- **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 agosto son las categorías: Cambio de contraseña, Servidor Windows: Asignación de licencia, Creación de usuarios, Configuración, Inactivar usuario, Cambio de grupo, permisos, Asesoría - Consulta, Crear/Modificar/Eliminar, para un total de 570 casos, en comparación con el mes de anterior se da un aumento del 14,21% que corresponde 81 casos. En la siguiente tabla se muestra el total de solicitudes para el servicio y el porcentaje correspondiente:

ADMINSTRACION DE SERVIDORES	TOTAL	PORCENTAJE(%)
Cambiar contraseña	170	29,82%
Servidor Windows	58	10,18%
Asignacion de licencia	57	10,00%
Creacion de usuario	47	8,25%
Configuracion	36	6,32%
Inactivar usuario	34	5,96%
Cambio de grupo	27	4,74%
Permisos	19	3,33%
Asesoria - Consulta	17	2,98%
Crear/Modificar/Eliminar	15	2,63%
Configuración MFA	14	2,46%

Retiro de Licencia	12	2,11%
Servidores	10	1,75%
Crear usuario	7	1,23%
Informes y Reportes	7	1,23%
Desbloquear usuario	6	1,05%
Habilitar usuario	6	1,05%
Servidor Linux	4	0,70%
Crear Backups	4	0,70%
Asignacion de permisos	3	0,53%
Aprovisionamiento	2	0,35%
Validar servidor	2	0,35%
Administracion de equipos	2	0,35%
Restaurar Backups	2	0,35%
Mantenimiento preventivo	2	0,35%
Backup	2	0,35%
Actualizacion de servidores	1	0,18%
Modificar usuarios	1	0,18%
Eliminar Hostname	1	0,18%
Creacion DNS	1	0,18%
Informes de usuarios	1	0,18%
Total general	**570**	**100,00%**

Tabla 33 Top 10 administración de servidores

Top 10 de Redes y Conectividad: para el mes de agosto se tiene las siguientes categorías más representativos de redes y conectividad, Solicitudes asociadas: Router, FortiGate, Revision estado del canal, Starlink , AP, Switch, Asesoría – Consulta, Sin servicio, Caída, Canal Internet, para un total de 757 casos. En comparación con el mes anterior se da un aumento del 42,14% que corresponde 319 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	PROCENTAJE(%)
Router	371	49,01%
FortiGate	137	18,10%
Revision estado del canal	111	14,66%
Starlink	60	7,93%
AP	34	4,49%
Switch	20	2,64%
Asesoria - Consulta	6	0,79%
Sin servicio	6	0,79%
Caida	4	0,53%
Canal Internet	3	0,40%
Incidente Mayor	1	0,13%
Informe de consumo canal	1	0,13%
Equipo Conectividad internet	1	0,13%
Configuraciones adicionales	1	0,13%

Informe de puertos	1	0,13%
Total general	**757**	**100,00%**

Tabla 34 Top 10 redes y conectividad

Top 10 de Seguridad Informática: durante el mes de agosto se tiene las siguientes categorías más representativas, de seguridad informática que corresponden a: Permitir acceso, Accesos por fuerza bruta, Asesoría - Consulta, Análisis de Correos, Seguridad Informática, Restringir servicio, Correo Malicioso, Crear política, Reportes Seguridad Informática, Ajuste de configuraciones, para un total de 61 casos. En comparación con el mes anterior, se da una disminución del 7,67% que corresponde a 147 casos.

SEGURIDAD INFORMATICA	TOTAL	PROCENTAJE(%)
Permitir acceso	9	14,75%
Accesos por fuerza bruta	7	11,48%
Asesoria - Consulta	6	9,84%
Análisis de Correos	5	8,20%
Seguridad Informática	4	6,56%
Restringir servicio	4	6,56%
Correo Malicioso (Phishing, Smishing, whaling, otros)	3	4,92%
Crear politica	3	4,92%
Reportes Seguridad Informática	3	4,92%
Ajuste de configuraciones (Crear - Eliminar)	2	3,28%
Análisis de evento	2	3,28%
Análisis vulnerabilidades	2	3,28%
Revisar correo malicioso	2	3,28%
Agregar puertos	2	3,28%
Modificacion VPN	2	3,28%
Incidente por Malware	1	1,64%
Reporte de eventos	1	1,64%
Agregar a listas negras	1	1,64%
Agregar a sitios permitidos	1	1,64%
Ajustar política	1	1,64%
Total general	**61**	**100,00%**

Tabla 35 Top 10 seguridad informática

Top 10 de Telefonía IP: Durante este periodo se gestionaron 64 casos de Telefonía IP que corresponden a: Gateway, Configuración de extensión Asesoría - Consulta, Asignación de Extensión, No ingresan llamadas, Falla - error, instalación - Configuración , Infraestructura de telefonía, Asignación y Configuración de red, En comparación del mes anterior se tiene una disminución de los casos del 34,02% que corresponde a 33 casos.

TELEFONIA IP	TOTAL	PROCENTAJE(%)
Gateway	44	68,75%
Configuracion de extension	6	9,38%
Asesoria - Consulta	3	4,69%
Asignacion de Extension	2	3,13%

No ingresan llamadas	2	3,13%
Falla - error	2	3,13%
Instalacion - Configuracion	2	3,13%
Infraestructura de telefonia	1	1,56%
Asignacion	1	1,56%
Configuracion de red	1	1,56%
Total general	**64**	**100,00%**

Tabla 36 Top Telefonía IP

Top 10 de Aplicaciones Especializadas: Para el mes de agosto se tienen los casos más representativos de la gestión de aplicaciones que corresponden a las siguientes categorías: Relanzamiento, Asesoría - Consulta, Asignar Radicado TYS, Asignación - Modificación Roles, Depuración Bandeja, Falla Funcional, Suspender - Falla radicación, Lentitud gestor, Suspender - Finalizar Radica TyS e Instalar - Configurar.
En comparación del mes anterior se tiene una disminución de los casos del 10,79% que corresponde a 100 casos, para un total de 826 casos.

APLICACIONES ESPECIALIZADAS	TOTAL	PROCENTAJE(%)
Relanzamiento	221	26,76%
Asesoria - Consulta	141	17,07%
Asignar Radicado TYS	112	13,56%
Asignacion - Modificacion Roles	84	10,17%
Depuración Bandeja	81	9,81%
Falla Funcional	49	5,93%
Falla radicacion	39	4,72%
Lentitud gestor	18	2,18%
Suspender - Finalizar Radica TyS	11	1,33%
Instalar - Configurar	11	1,33%
Solicitud depuracion carpeta	8	0,97%
SUITE VISION EMPRESARIAL (SVE)	8	0,97%
Falla - error	7	0,85%
Falla error - Producir documento	4	0,48%
Informes y Reportes	3	0,36%
No se encuentra radicado	3	0,36%
No genera sticker	3	0,36%
Falla - Error TYS	3	0,36%
No permite Aprobar y radicar	3	0,36%
Falla Error - Datacap	3	0,36%
Lentitud del servidor	2	0,24%
Falla - Error PQRSD	2	0,24%
Caida - Degradacion	2	0,24%
Falla	2	0,24%
No permite ingresar datos	1	0,12%

Gestor documental	1	0,12%
Caida del servidor	1	0,12%
Falla - Error ventanilla	1	0,12%
Portal Web	1	0,12%
Cobro Coactivo	1	0,12%
Total general	**826**	**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: Cargue de papel en impresora, Asesoria - Consulta, Cambio Toner, Configuracion, Instalacion - Configuracion, Actualización Bios, Aumento de cuota, Prestamo, Soporte Aplicaciones Office 365 y Asesoria Excel, En comparación del mes anterior se tiene una disminucion en los casos del 23,50% que corresponde a 1412 casos, para un total del mes de 4594 casos.

SOPORTE MICROINFROMATICA	TOTAL	PROCENTAJE(%)
Cargue de papel en impresora	731	15,91%
Asesoria - Consulta	609	13,26%
Cambio Toner	498	10,84%
Configuracion	486	10,58%
Instalacion - Configuracion	397	8,64%
Actualización Bios	362	7,88%
Aumento de cuota	217	4,72%
Prestamo	103	2,24%
Soporte Aplicaciones Office 365	95	2,07%
Asesoria Excel	94	2,05%
Asesoria Consulta	89	1,94%
Asesoria PDF	86	1,87%
Conectar a red Mintrabajo	74	1,61%
Instalacion y configuracion VPN	62	1,35%
Asesoria Word	58	1,26%
Asignación de equipo (portátil o PC)	56	1,22%
Mantenimiento preventivo	52	1,13%
Traslado - Movimiento	48	1,04%
Atasco	41	0,89%
Copia de informacion	37	0,81%
Solicitud Backup	31	0,67%
Instalación-Desinstalación	31	0,67%
No escanea	31	0,67%
Devolución de equipo (portátil o PC)	29	0,63%
No imprime	24	0,52%
Backup	22	0,48%
Falla - Error conexión a red	21	0,46%
Instalacion	17	0,37%
Solicitud instalacion	16	0,35%

Equipo Periférico	16	0,35%
Solicitud de cambio	15	0,33%
Envio y recepción de correos	14	0,30%
Borrado seguro Portátil	12	0,26%
Conectar a red Invitados	11	0,24%
Falla - error	10	0,22%
Instalación - Configuracion	8	0,17%
Cambio de unidad de imagen	8	0,17%
Eliminar Hostname	7	0,15%
No enciende	7	0,15%
Lentitud - Bloqueo	7	0,15%
Falla aplicación	6	0,13%
Equipo Portátil	6	0,13%
Asignar Pin	5	0,11%
Falla Aplicaciones Office 365	5	0,11%
Equipo Escritorio	4	0,09%
Falla Cargue pagina web	3	0,07%
Falla impresora	3	0,07%
Error de aplicación	3	0,07%
Daño fisico	3	0,07%
Borrado seguro PC	3	0,07%
Error sincronizacion	2	0,04%
Asesoria Power Point	2	0,04%
Falla Word	2	0,04%
Impresión deficiente	2	0,04%
Asesoria en ZIP	2	0,04%
Reportar Solicitud/Falla	2	0,04%
Equipo Impresora	1	0,02%
Falla Excel	1	0,02%
Falla PDF	1	0,02%
Configuracion de PST	1	0,02%
Falla instalacion	1	0,02%
Lentitud	1	0,02%
No conecta	1	0,02%
Falla General	1	0,02%
Falla- Error	1	0,02%
Total general	**4594**	**100,00%**

Tabla 38 Top 10 soporte microinformática

- **Análisis de Casos Anulados por Servicio**

Para este periodo se tiene 8 casos anulados de los siguientes servicios:

CASOS ANULADOS	TOTAL

Soporte Microinformática	4
Aplicaciones Especializadas	2
Herramientas de Gestión	1
Administración de servidores	1
Total general	**8**

Tabla 39 Casos Anulados por Servicio

- **Soporte Microinformático:** se tiene 4 casos, Cargue de papel en impresora, Traslado-movimiento anulados por duplicidad.
- **Aplicaciones especializadas:** se tiene 2 caso por: Portal Web y Asesoría – Consulta anulados por duplicidad.
- **Herramientas de Gestión:** se tiene 1 caso anulado por duplicidad Monitoreo desde Zabbix.
- **Administración de servidores:** se tiene 1 caso anulado por duplicidad Cambio urgente.

En comparación del mes anterior se evidencio una disminución del 19,51%, que corresponde a 33 casos.

- ## Análisis de Casos Suspendidos por Servicio

Para el periodo del mes de agosto, se dio un aumento de casos suspendidos del 46,62% que corresponde a 69 casos para un total de este mes de 148 de los siguientes servicios:

CASOS SUSPENDIDOS	TOTAL
Soporte Microinformática	64
Redes y Conectividad	48
Administración de servidores	16
Aplicaciones Especializadas	15
Seguridad informática	2
Herramientas de Gestión	1
Administración de Bases de Datos	1
Telefonía IP	1
Total general	**148**

Tabla 40 Casos Suspendidos por Servicio

- **Soporte Microinformática:** 64 casos suspendidos debido a que se ha solicitado información complementaria a los usuarios o están pendientes por disponibilidad del usuario: Cambio Tóner con 20 casos, Configuracion con 8 casos, Asesoria - Consulta con 6 casos, Solicitud Backup con 5 casos, Cambio de unidad de imagen con 4 casos, Equipo Portátil, Solicitud de cambio, Equipo Escritorio con 3 casos, Asignación de equipo (portátil o PC), Devolución de equipo (portátil o PC) con 2 casos, Asesoria Excel, Prestamo, No enciende, Daño físico, Aumento de cuota, Instalacion – Configuracion, Equipo Impresora y Lentitud con 1 caso.
- **Redes y Conectividad: 48** casos suspendidos debido a: Router con 29 casos, FortiGate con 11 casos, Starlink y AP con 2 casos, Informe de puertos, Sin servicio, Caida e Incidente Mayor, con 1 caso cada categoría.
- **Administración de servidores: 16** casos suspendidos por: Inactivar usuario con 5 casos, Configuracion, Permisos con 3 casos, Desbloquear usuario, Servidor Windows, Crear Backups, Asignacion de licencia, Crear/Modificar/Eliminar con 1 caso.
- **Aplicaciones Especializadas: 15** casos suspendidos debido a que se ha solicitado información complementaria a los usuarios o están pendientes por disponibilidad del usuario:

Asignación - Modificación Roles, con 6 casos, Asesoria – Consulta con 4 casos, Relanzamiento y Asignar Radicado TYS con 2 casos, Cobro Coactivo, con 1 caso cada categoría.

- **Seguridad informática: 2** casos suspendido debido a: Revisar correo malicioso y Permitir acceso con 1 caso cada categoría.
- Herramientas de Gestión**: 1** caso suspendido debido a: Agregar Host.
- **Administración de Bases de Datos**: 1 caso suspendidos debido a: Actualización de Registro.
- **Telefonía IP**: 1 caso suspendidos debido a: Configuración de troncales.

- **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 periodo no quedaron incidentes en estado solucionado.

SOPORTE_TERRITORIAL	TOTAL
Atasco	5
Falla - Error conexión a red	3
No imprime	2
Falla Word	1
Lentitud - Bloqueo	1
Envio y recepción de correos	1
Falla - error	1
Falla de sistema operativo	1
Total general	**15**

Tabla 41 Casos Suspendidos por Servicio

Requerimientos solucionados por la Mesa de Servicios: Para el mes de agosto quedaron 6 requerimientos solucionados por la mesa de servicios discriminados de la siguiente manera:

REQUERIMIENTOS SOLUCIONADOS MESA_DE_SERVICIOS	TOTAL
Habilitar usuario	1
SUITE VISION EMPRESARIAL (SVE)	1
Inactivar usuario	1
Asignación de equipo (portátil o PC)	1
Asesoria - Consulta	1
Asignacion de permisos	1

Total general	**6**

Tabla 42 Requerimientos solucionados por Mesa de Servicios

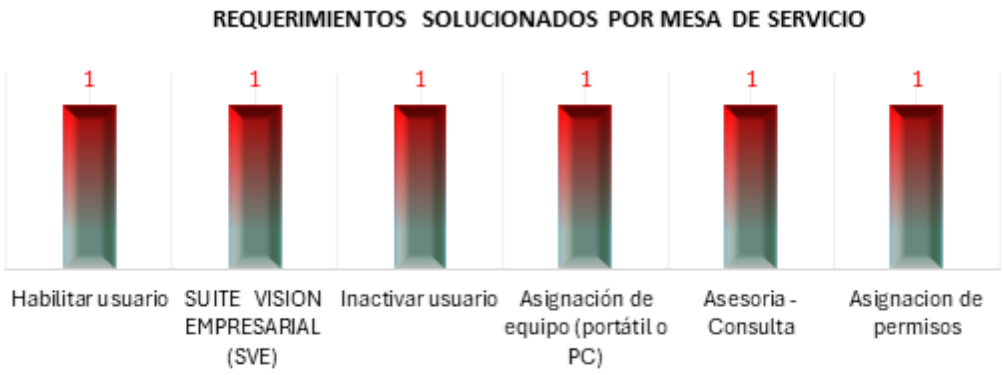


Ilustración 24 Requerimientos Solucionados por la Mesa de Servicios

Requerimientos solucionados por Soporte en sitio Bogotá: en el mes de agosto quedaron 4 requerimientos discriminados de la siguiente manera:

REQUERIMIENTOS SOLUCIONADOS POR SOPORTE EN SITIO	TOTAL
Devolución de equipo (portátil o PC)	1
Configuración	1
Asesoría - Consulta	1
Borrado seguro Portátil	1
Total general	**4**

Tabla 43 Requerimientos solucionados por Soporte en sitio



Ilustración 25 Requerimientos Solucionados por Soporte en sitio

Requerimientos solucionados por Soportes Territoriales: Para el mes de agosto no quedaron casos en estado solucionado de las territoriales.

- **Casos Cerrados por la Mesa de Servicios, Soporte en Sitio en Nivel Central y Sedes Territoriales.**

Casos Cerrados por la Mesa de Servicios: Se indica el top de 10 de Requerimientos cerrados por la mesa de servicios, para el mes de agosto se cerraron 671 casos, discriminados así: Asesoría – Consulta con 202 casos, Cambiar contraseña con 155 casos, Creación de usuario 47casos, Cambio de grupo con 26 casos, Configuracion con 16 casos, Instalacion y configuracion VPN con 13 casos, Instalacion – Configuracion con 13 casos, Asignación de equipo (portátil o PC) con 8 casos, Envio y recepción de correos con 8 casos, a comparación del mes anterior se evidencia una disminucion del 15,87%% que corresponden a 121 casos.

CERRADOS POR LA MESA DE SERVICIOS	TOTAL
Asesoria - Consulta	202
Cambiar contraseña	155
Creacion de usuario	47
Cambio de grupo	26
Inactivar usuario	24
Configuracion	16
Instalacion y configuracion VPN	13
Instalacion - Configuracion	13
Asignación de equipo (portátil o PC)	8
Envio y recepción de correos	8
Crear usuario	7
Prestamo	7
Aumento de cuota	6
Asignar Radicado TYS	6
Informes y Reportes	6
Relanzamiento	6
Habilitar usuario	5
Lentitud gestor	5
Cargue de papel en impresora	5
Solicitud Backup	5
Eliminar Hostname	5
Desbloquear usuario	5
Devolución de equipo (portátil o PC)	5
Depuración Bandeja	5
Falla Funcional	5
Mantenimiento preventivo	3
Asignacion - Modificacion Roles	3
Permisos	3
Traslado - Movimiento	2
SUITE VISION EMPRESARIAL (SVE)	2
Crear/Modificar/Eliminar	2
Reportar Solicitud/Falla	2
Soporte Aplicaciones Office 365	2
Ajuste de configuraciones (Crear - Eliminar)	2
Asignacion de permisos	1
Administracion de equipos	1
Borrado seguro Portátil	1
Instalación - Configuracion	1
Borrado seguro PC	1
Asesoria Consulta	1
Retiro de Licencia	1
Instalar - Configurar	1
Configuracion de PST	1
Crear Periodo de Manteniemiento	1
Revision estado del canal	1

Análisis de Correos	1
Conectar a red Mintrabajo	1
Accesos por fuerza bruta	1
Informes de usuarios	1
Falla aplicación	1
Solicitud de cambio	1
Asignacion de licencia	1
Crear Backups	1
Permitir acceso	1
Configuraciones adicionales	1
Asesoria PDF	1
Modificar usuarios	1
No escanea	1
Falla radicacion	1
Total general	**641**

Tabla 44 Casos cerrados por la mesa de servicios

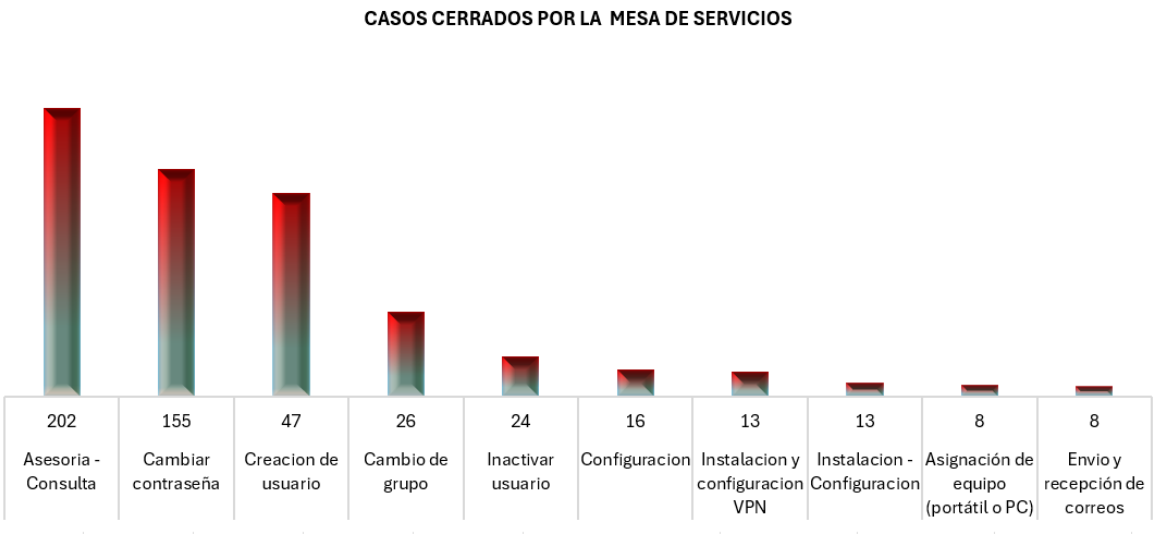


Ilustración 26 Casos cerrados por la mesa de servicios

Casos Cerrados por Soporte en Sitio: Se indica el top 10 de Requerimientos cerrados por soporte en sitio, para el mes de agosto se cerraron 2027 casos discriminados así: Cargue de papel en impresora con 482 casos, Asesoria – Consulta con 338 casos, Configuración con 335 casos, Instalacion - Configuracion con 196 casos, Revision estado del canal con 107 casos, Soporte Aplicaciones Office 365 con 59 casos, Prestamo con 54 casos, Conectar a red Mintrabajo con 53 casos, Asesoria Excel con 38 casos, Actualización Bios con 36 casos, a comparación con el mes anterior se tiene una disminucion del 13,52% que corresponde a 317 casos.

CERRADOS POR SOPORTE EN SITIO	TOTAL
Cargue de papel en impresora	482
Asesoria - Consulta	338
Configuracion	335
Instalacion - Configuracion	196
Revision estado del canal	107
Soporte Aplicaciones Office 365	59
Prestamo	54
Conectar a red Mintrabajo	53
Asesoria Excel	38
Actualización Bios	36
Instalacion y configuracion VPN	35

Asesoria PDF	24
Asesoria Word	20
Atasco	18
Instalación-Desinstalación	18
Asignación de equipo (portátil o PC)	17
Traslado - Movimiento	15
Cambiar contraseña	14
Mantenimiento preventivo	14
No imprime	13
Aumento de cuota	12
Backup	12
Solicitud instalacion	11
Cambio Toner	11
Conectar a red Invitados	10
Devolución de equipo (portátil o PC)	9
Borrado seguro Portátil	8
No escanea	7
Falla - Error conexión a red	6
Solicitud Backup	6
Copia de informacion	6
Solicitud de cambio	4
Equipo Periférico	4
Envio y recepción de correos	3
No enciende	3
Lentitud - Bloqueo	3
Asignacion - Modificacion Roles	2
Asesoria Power Point	2
Configuración MFA	2
Instalación - Configuracion	2
Asignar Pin	2
Equipo Portátil	2
Falla - error	2
Impresión deficiente	1
Asesoria en ZIP	1
No permite ingresar datos	1
Eliminar Hostname	1
Falla Word	1
Configuracion de extension	1
Falla General	1
Caida	1
Informes y Reportes	1
Falla aplicación	1
Falla radicacion	1
Error sincronizacion	1
Total general	**2027**

Tabla 45 Casos cerrados por soporte en sitio



Ilustración 27 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 agosto se cerraron 1796 casos discriminados así: Actualización BIOS con 3261 casos, Asesoría – Consulta con 254 casos, Cargue de papel en impresora con 201 casos, instalación - Configuración con 167 casos, Configuración con 55 casos, Cambio Tóner con 107 casos, Asesoría PDF con 61 casos, Asesoría Excel con 72 casos, Préstamo con 41 casos, Asesoría Word 38 casos, a comparación con el mes anterior se tiene una disminución del 11,81% que corresponde a 240 casos.

CASOS CERRADOS POR SOPORTE TERRITORIAL	TOTAL
Actualización Bios	326
Asesoria - Consulta	254
Cargue de papel en impresora	201
Instalacion - Configuracion	167
Configuracion	128
Cambio Toner	107
Asesoria PDF	61
Asesoria Excel	55
Prestamo	41
Asesoria Word	38
Mantenimiento preventivo	37
Soporte Aplicaciones Office 365	32
Copia de informacion	31
Traslado - Movimiento	27
Asignación de equipo (portátil o PC)	26
Atasco	23
Conectar a red Mintrabajo	20
Aumento de cuota	18
Instalacion	17
No escanea	16
Falla - Error conexión a red	15

Instalacion y configuracion VPN	14
Instalación-Desinstalación	13
No imprime	11
Solicitud Backup	8
Devolución de equipo (portátil o PC)	7
Solicitud de cambio	7
Falla - error	6
Solicitud instalacion	5
Backup	5
Instalación - Configuracion	5
Falla Aplicaciones Office 365	5
Instalar - Configurar	4
Lentitud - Bloqueo	4
Cambio de unidad de imagen	4
Falla aplicación	4
Falla impresora	3
Envio y recepción de correos	3
Asignar Pin	3
Error de aplicación	3
Sin servicio	3
No enciende	3
Falla Cargue pagina web	3
Falla	2
Borrado seguro Portátil	2
Reportar Solicitud/Falla	2
Daño fisico	2
Falla radicacion	2
Borrado seguro PC	2
Falla Funcional	2
Revision estado del canal	2
Falla instalacion	1
No genera sticker	1
Error sincronizacion	1
Equipo Periférico	1
Falla- Error	1
No conecta	1
Conectar a red Invitados	1
Asesoria en ZIP	1
Caida	1
Falla PDF	1
Caida del servidor	1
Asignar Radicado TYS	1
Falla Excel	1

Falla Word	1
No permite Aprobar y radicar	1
Impresión deficiente	1
Falla Error - Datacap	1
Total general	**1796**

Tabla 46 Casos cerrados por soporte en sitio

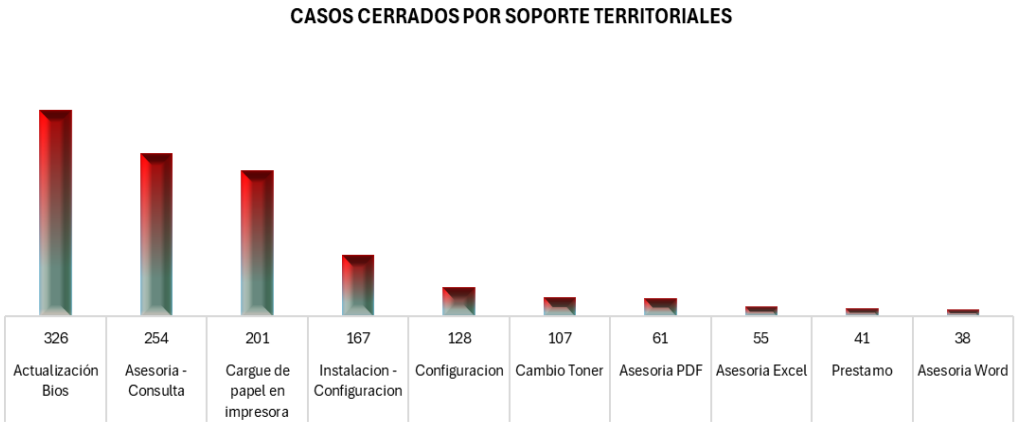


Ilustración 28 casos cerrados soporte territoriales

CASOS CERRADOS POR SOPORTE TERRITORIAL	TOTAL
Asesoria - Consulta	401
Cargue de papel en impresora	272
Configuracion	257
Instalacion - Configuracion	199
Asesoria Excel	94
Cambio Toner	94
Asesoria PDF	91
Asesoria Word	72
Soporte Aplicaciones Office 365	58
Mantenimiento preventivo	48
Prestamo	47
Conectar a red Mintrabajo	31
Atasco	27
No imprime	26
Instalacion y configuracion VPN	25
Instalacion	25
Traslado - Movimiento	24
Copia de informacion	22
Aumento de cuota	20
Falla - Error conexión a red	20
Instalación-Desinstalación	17

Falla - error	13
Solicitud instalacion	12
Asignación de equipo (portátil o PC)	11
Envio y recepción de correos	9
Devolución de equipo (portátil o PC)	9
No Escanea	8
Borrado seguro PC	7
Lentitud - Bloqueo	7
Solicitud Backup	6
Reportar Solicitud/Falla	6
Backup	5
Falla aplicación	5
Falla impresora	5
No enciende	5
Instalación - Configuracion	5
Asesoria en ZIP	4
Falla de sistema operativo	4
Asesoria Power Point	4
Falla Error - Datacap	3
Lentitud	3
Asignar Pin	3
Instalar - Configurar	2
Error de aplicación	2
No conecta	2
Falla PDF	2
Equipo Impresora	2
Borrado seguro Portátil	2
Falla Funcional	2
Falla Cargue pagina web	2
Asignar Radicado TYS	1
Cambio de unidad fusora	1
Zabbix	1
No permite Aprobar y radicar	1
Informes y Reportes	1
Daño Fisico	1
Cambio de unidad de imagen	1
Préstamo Equipo (portátil o PC)	1
Conectar a red Invitados	1
Falla Word	1
Falla Aplicativo	1
Impresión deficiente	1

Total general	2032

Tabla 47 Casos cerrados por Territoriales

- **Casos Atendidos a Usuarios VIP**

Durante este periodo se crearon 2044 solicitudes para ser atendidas por soporte en sitio, de estas solicitudes se evidenciaron 115 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_CUPLE	TOTAL
Incidentes	3	0	3
Requerimiento	112	0	112
Total general	**115**	**0**	**115**

Tabla 48 Casos usuarios VIP

Se atendieron 1929 solicitudes para el resto de los usuarios discriminados así:

TIPO DE CASO-NO-VIPS	CUMPLIMIENTO	NO_CUPLE	TOTAL
Incidentes	54		54
Requerimientos	1872	3	1875
Total general	**1926**	**3**	**1929**

Tabla 49 Casos usuarios Regulares

- **Medio de Ingreso de Casos**

Durante el período ingresaron a la mesa de servicio 6930 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:

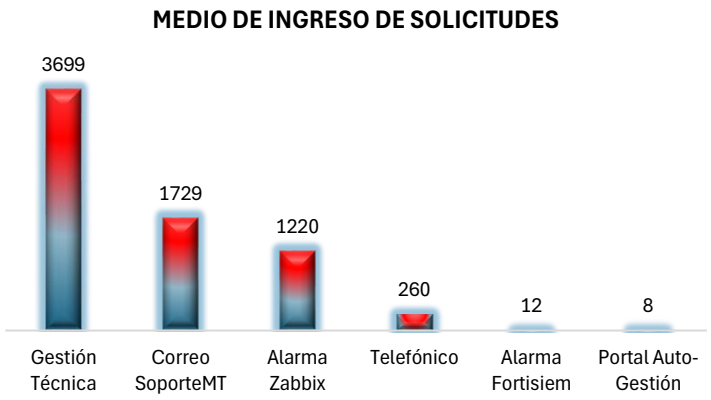


Ilustración 29 Modo de Ingreso de Solicitudes

Gestion técnica es el método más utilizado por los funcionarios del ministerio del trabajo, esta categoría hace referencia a solicitudes que directamente realizan las personas a los soportes, no ingresan a través de la mesa de servicios.

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

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

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

Durante el mes de agosto 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 requieren atención, entre estos, casos de Internet, Redes, Actualizaciones de Software, BIOS, Agentes instalados y mantenimiento de impresoras.

- Se inicia con las validaciones Peer Review y la forma de llevar a cabo la revisión por pares al momento de generar los informes que se le van a presentar a la Supervisión del contrato.

- Intervención de 1817 casos, dentro de los que se destacan: Actualización de BIOS, Asesorías –Consultas sobre aplicaciones de la línea base de software, Cargues de Papel, Configuraciones e Instalaciones de software y aplicaciones de ofimática, Cambio de Toner, Asesorías en PDF, Asesorías en Excel, Asesorías en Word y Prestamos de Elementos como unidades de CD y Videobeams, así como Equipos de cómputo.

- Se realizó el arreglo de la estructura del Rack en el Doncello, Granada / Meta y en Tuluá de acuerdo con la solicitud de los administradores de redes.

- Se continuó el proceso de actualización de la versión de BIOS en los equipos es escritorio y en los portátiles de acuerdo con los lineamientos a nivel nacional.

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

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

Para el período se realizaron las siguientes visitas:

Mes	Territorial	Sede	Servicio	Descripción	Caso
Agosto 2025	Atlántico	Baranoa	Asignación e instalación monitor cambiado por garantía serial VNAB8D6T	Se realiza la instalación y asignación del monitor indicado, se diligencia acta de asginación y se coloca en su puesto de trabajo. Se valida que queda operativo.	RF-141306
Agosto 2025	Valle del Cauca	Tuluá	Se solicita realizar pruebas de conexión de internet por fibra óptica en la sede del Ministerio del Trabajo ubicada en Tuluá.	durante la visita técnica no fue posible ejecutar las pruebas debido a que el proveedor de última milla no realizó la instalación del cable necesario entre los dispositivos Risecom y Bdcom	RF-141665
Agosto 2025	Vaupés	Mitú	Se desplaza personal del aliado con el propósito de migrar conexiones al nuevo switch adquirido por la UT y verificar el estado de la impresora reportada previamente por los usuarios de la sede	APICOM	N/A
Agosto 2025	Doncello	Caquetá	Validación de primer nivel en los equipos de comunicaciones del Doncello	En conjunto con el Ingeniero de redes Edwar Reyes se realizan pruebas directamente de la antena Starlink - al canal principal ETB, se realizan pruebas de conectividad con éxito y queda trabajando de	RF-141509

				manera correcta la inspección el Doncello	
Agosto 2025	Meta	Granada	Se desplaza Carol Gonzalez, técnico de soporte en sitio para verificación de conectividad a internet de los equipos de la inspección	El pasado 21 de agosto se realizó visita técnica en la cual se organizó el cableado de red e internet. Durante la intervención, se identificó que el punto de red asignado al equipo del funcionario Javier Díaz requiere cambio, ya que presenta condiciones que podrían afectar la estabilidad del servicio. Aunque el servicio quedó funcionando correctamente, se solicita a Infraestructura del Ministerio realizar la revisión y el reemplazo correspondiente del punto de red para evitar futuras afectaciones.	IM-142909 IM-141633
Agosto 2025	Meta	Cumaral	Se requiere actualización de la BIOS equipo Lenovo.	Se realiza la actualización del BIOS en el equipo solicitado, siguiendo los lineamientos establecidos. Se realizó respaldo previo de la información del usuario para garantizar la integridad de los datos. La actualización se ejecutó de manera controlada y documentada en horario no operativo. Posterior a la actualización, se efectuaron pruebas de funcionalidad y desempeño, confirmando la correcta operación del equipo de cómputo	RF-144792
Agosto 2025	Cundinamarca	Soacha	Cx Fortinet	Se realiza la migración de las conexiones en la inspección de Soacha. se realizan prueba de conectividad de forma satisfactoria, se verifica con los funcionarios acceso a las aplicativos Web y navegación en Internet	RF-145790
Agosto 2025	Barranquilla	Campo de la cruz	Se requiere actualización de la BIOS equipo Lenovo.	Se realiza actualización de la última versión de la BIOS en el equipo, se reinicia para aplicar los cambios y se valida que el equipo queda operativo	RF-145609
Agosto 2025	Cauca	Casa de Justicia	Usuario:orealpe Nombre:OlgaRealpe Piso:1 DT:Cauca Observaciones. Se requiere visita en sitio para validación de router.	Para solucionar el requerimiento del usuario se realizaron las siguientes actividades: -Se realizó desplazamiento a la sede del usuario, donde se validó la conexión física mediante revisión del patch cord. -Se ajustó la configuración DNS eliminando entradas incorrectas y estableciendo servidores válidos. -Se habilitó el acceso mediante ZTNA con credenciales del usuario, permitiendo conexión segura a los servicios internos. -Finalmente, se verificó conectividad a internet, VPN y acceso exitoso al Gestor Documental desde un enlace funcional.	RF-145655

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	99,37%	95,00%
MDS 2	Tiempo de solución de incidentes por soporte en sitio	99,51%	90,00%
MDS 3	Tiempo de solución de requerimientos por soporte en sitio	99,83%	90,00%
MDS 4	Tiempo de respuesta de la mesa de servicio	98,95%	85,00%
MDS 5	Abandono de llamadas	0,35%	Máximo el 8%
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.
- Recepción de licenciamiento O365.

Esto implica revisar regularmente la base de datos de usuarios para identificar cuantas inactivas, duplicadas o desactualizadas, y proceder con su eliminación o actualización según sea necesario. 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. Actualmente se está a espera del envío de la información de manera formal por parte de la entidad, pero se ha trabajado de manera articulada con la Oficina de Tecnologías de la Información, para fortalecer este ítem dentro de la entidad.

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. Actualmente se está trabajando para la postulación de apagado y des aprovisionamiento de servidores no productivos como cambio estándar, definiendo como actividad previa el backup completo de la máquina virtual y el retiro del monitoreo previo a la ejecución del control de cambios.

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.

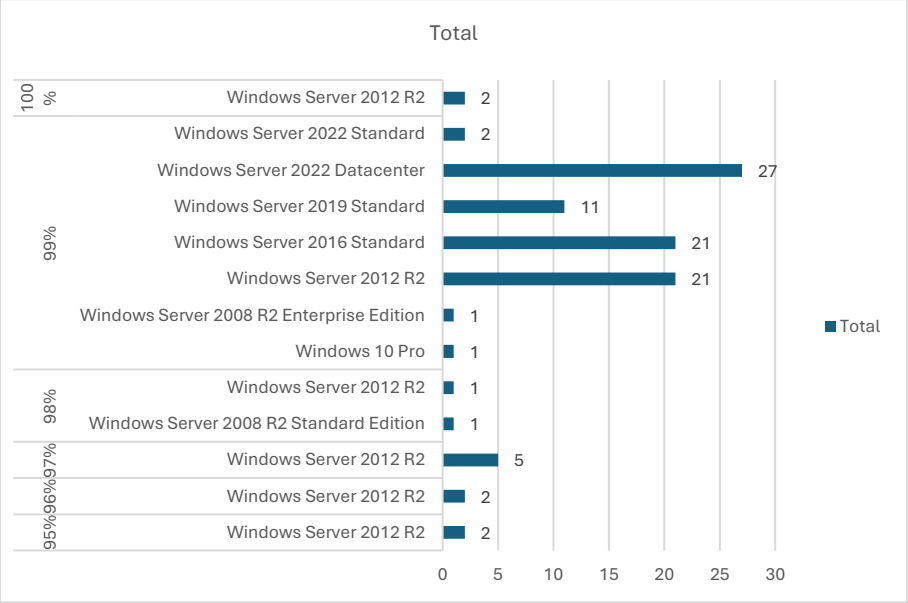


Ilustración 30 Cumplimiento WSUS

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. Se vio un crecimiento en la creación de casos de configuración de MFA y restablecimiento de contraseña debido a que en revisión de políticas, se pudo observar que los usuarios generaban bloqueo de cuenta de manera inconsciente al haber iniciado sesión en múltiples dispositivos habiendo grabado sus contraseñas anteriores, generando bloqueo de cuentas, restablecimiento de MFA y de credenciales. Se configura GPO para dar solución a este tema, pero solamente aplica para maquinas dentro del dominio de la entidad, en caso de no estar dentro del dominio, no es posible identificar el dispositivo que genera el bloqueo para liberar la sesión desde GPO. Adicional se da continuidad a los procesos de asignación de licencias O365 por demanda.

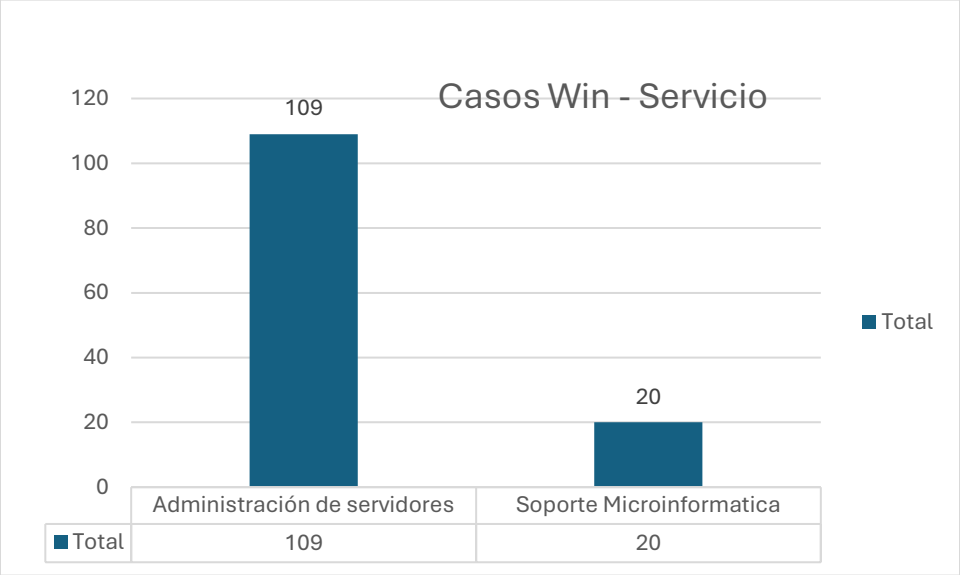


Ilustración 31 Estado final de los casos Windows

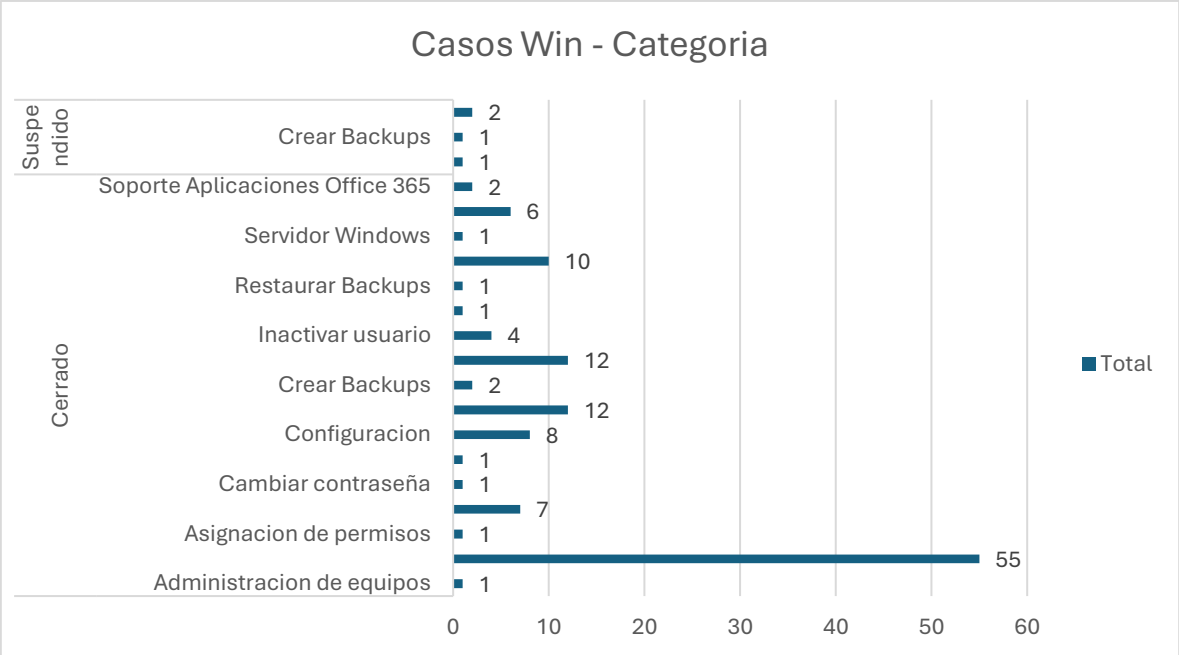


Ilustración 32 Casos por categorías Windows

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. Es importante mencionar que se ha venido creando diferentes VM asociados a nuevos servicios que aprovisionará el Ministerio del Trabajo pero en principio se encuentran en su fase de pruebas por lo cual solo se han creado VM de pruebas.

Se presentan incidentes asociados a los servidores de File Net que soportan el servicio de Gestor documental, este incidente no está asociado al componente de IBM pero si está asociado a la naturaleza de las máquinas virtuales las cuales previo a inicio de Operación en 2024, habían sido migradas por parte del anterior operador tecnológico a un entorno de virtualización desde un entorno físico y posteriormente migradas a hiper convergencia Hyper-V, tras diagnóstico del equipo Windows, se identifica que debido a los diferentes procesos por los cuales estas VM pasaron, algunos drivers generaban conflicto e inconvenientes en el consumo de servicios de AD, generando bloqueos sobre las máquinas virtuales, especialmente la que soporta el servicio de File Net, se realizan algunas configuraciones que permiten dar continuidad al servicio sin afectación, pero se propone un re aprovisionamiento del clúster debido a que realizar un montaje desde 0 de estas máquinas virtuales, permite realizar un aprovisionamiento y configuración en limpio de todo el servicio. Es importante mencionar que para realizar pruebas se están explorando opciones que no interfieran con el licenciamiento adquirido por la entidad, ya que la entidad no cuenta con licenciamiento suficiente para aprovisionar un ambiente de pruebas idóneo para testear cada componente y/o modulo.

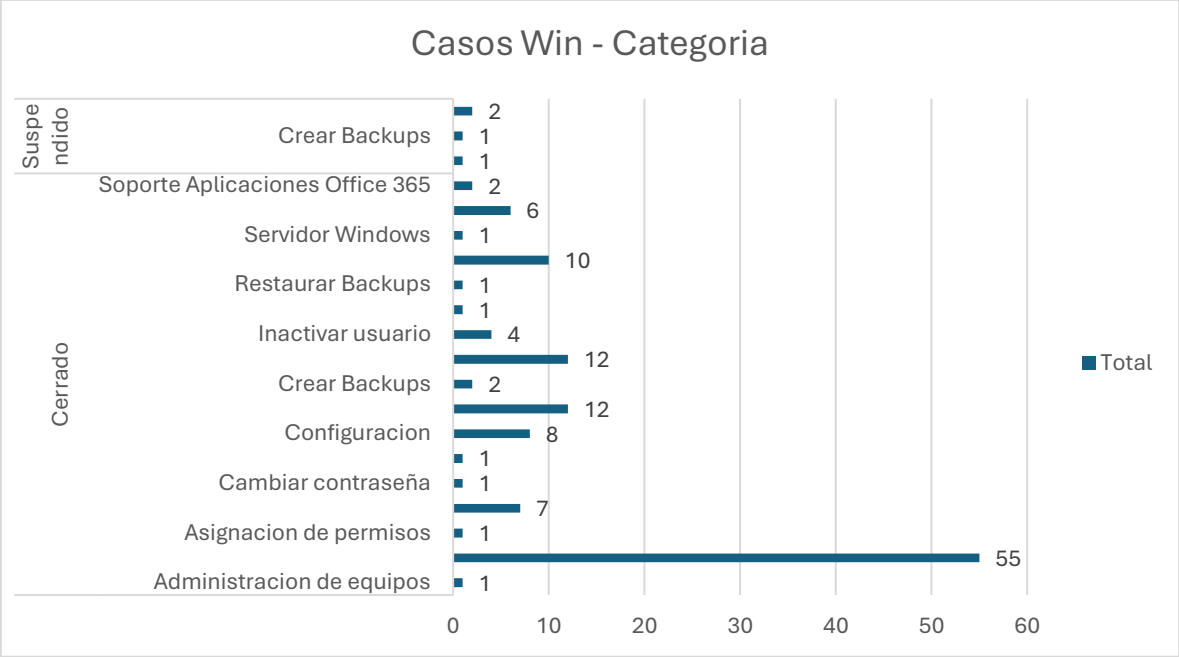


Ilustración 33 Estado final de los casos Nube privada

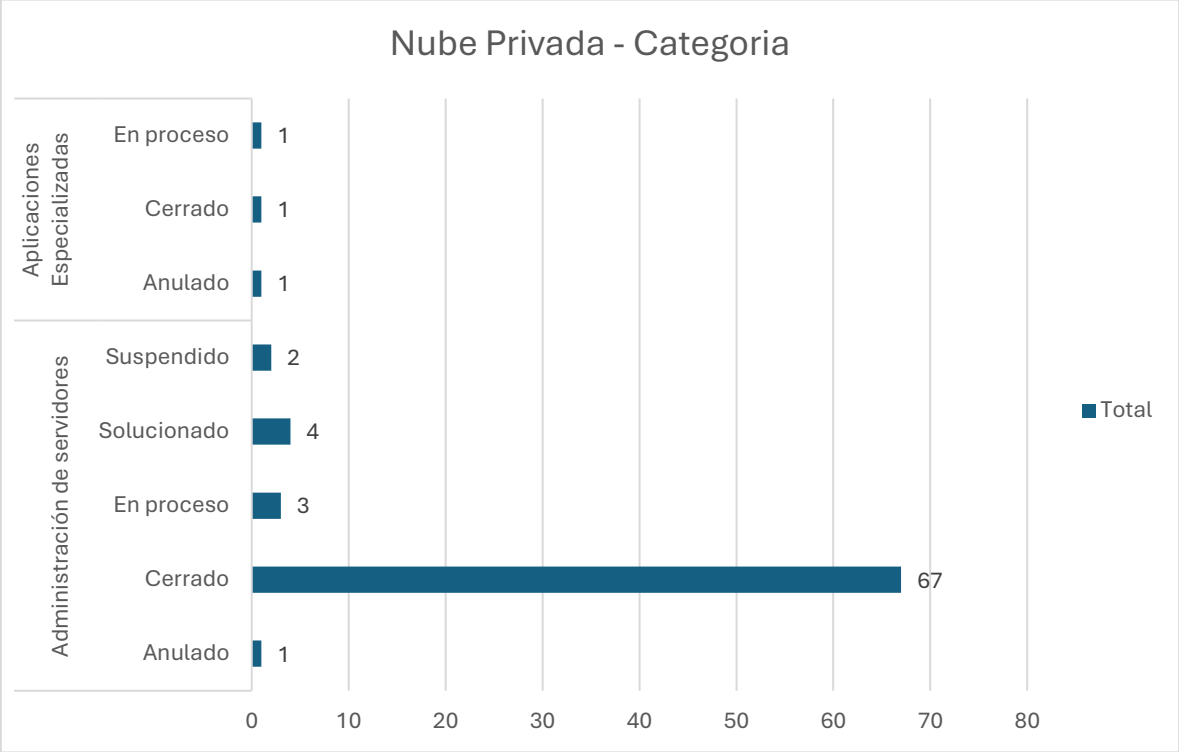


Ilustración 34 Casos por categoría Nube privada y pública

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	**626**	**2.7 TB**	**120 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, se esta trabajando en una política de retención de backups de usuario final, ya que estos backups están consumiendo una cantidad importante de almacenamiento en el file server y a largo plazo se puede convertir en una actividad y/o tarea demandante de almacenamiento y de tareas operativas que puede convertirse en una solución no sostenible dadas las capacidades de almacenamiento contratadas.:

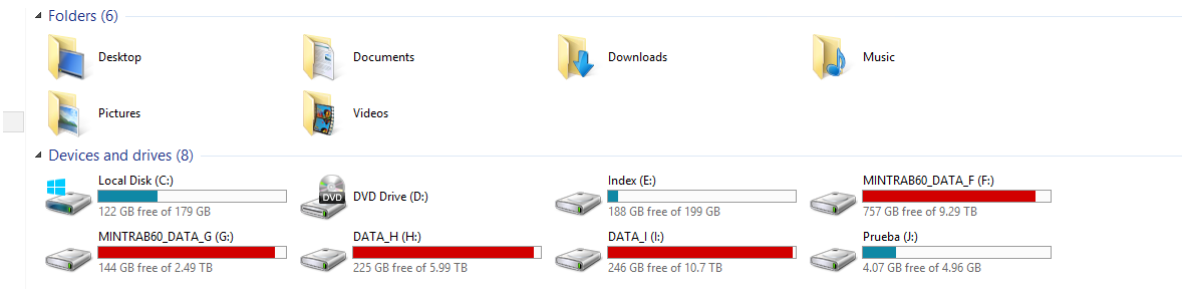


Ilustración 35 Estado File Server Mintrab60

Nube Pública

En el ejercicio de arquitectura para Azure, se ha enfatizado en la estructura actual, como se encuentra el Tenant a nivel de componente de infraestructura como servicio en nube y la interacción contra otros componentes de aplicación, ya sea en la misma nube pública, como conexiones hacia On Premises. Se definen los escenarios en donde se plantean cambios o mejoras sobre las propias implementaciones del Ministerio en el marco de la implementación de buenas prácticas para la gestión y administración de estos componentes.

Se 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.

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:

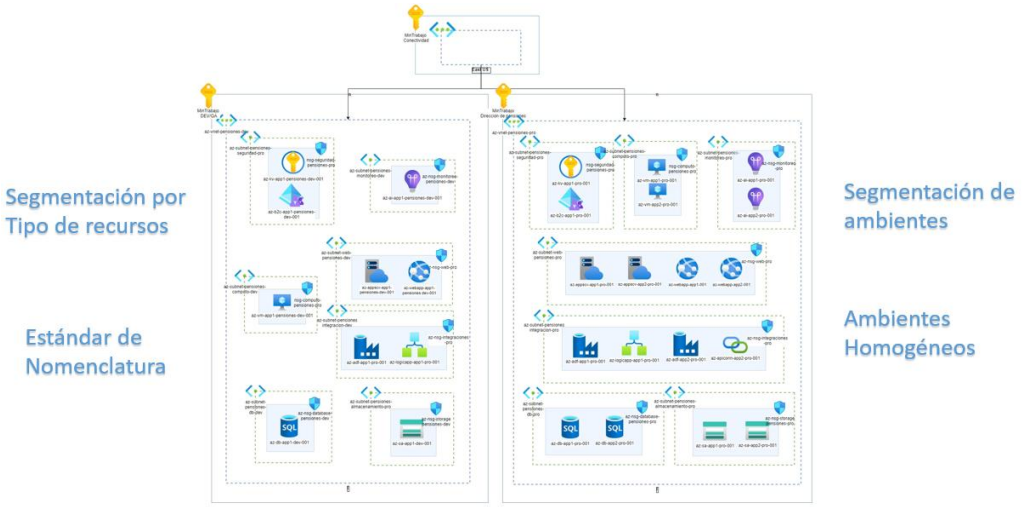


Ilustración 36 Proyección de Modelo de Suscripción

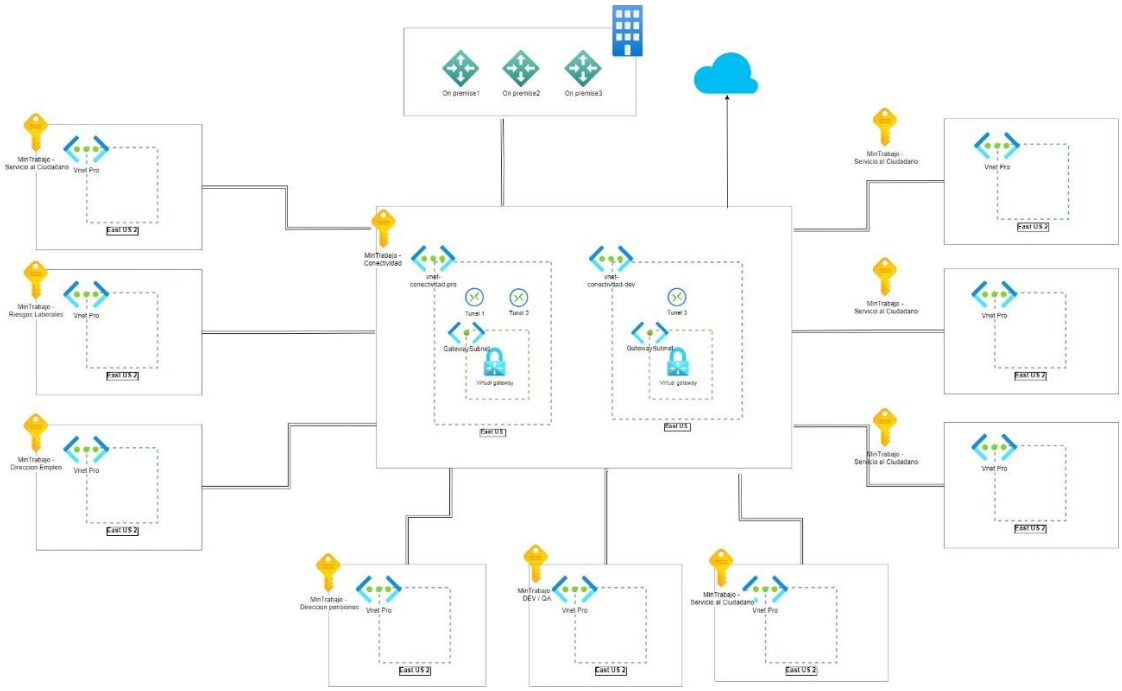


Ilustración 37 Modelo de Tenant bajo arquitectura

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.
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, solicitan ambiente de pruebas de la aplicación dentro de la suscripción de Dev-QA lo cual se realizó de manera satisfactoria y se creó template para implementación de avientes a través de Terraform empleando DevOps e Infraestructura como código para su implementación. Es importante mencionar que la entidad, durante todos sus despliegues anteriores no se había implementado una solución de despliegue continuo de recursos en Azure a través de DevOps, lo cual es un avance importante en materia de nube publica y de implementación de nuevos proyectos para la entidad en el futuro.

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 y de todos sus componentes de nube publica 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.

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

Objetivo: *El objetivo de esta política es garantizar que los empleados, contratistas y otros usuarios de los sistemas de información del Ministerio del trabajo tengan únicamente los privilegios necesarios para realizar sus funciones laborales, minimizando así los riesgos relacionados con el acceso no autorizado y la exposición de datos sensibles.*
Alcance: *Esta política es aplicable a todos los usuarios que interactúan con los sistemas de la organización, incluidos empleados, contratistas, proveedores, y cualquier otra parte externa que tenga acceso a los recursos informáticos de la empresa.*
El principio de privilegio de acceso mínimo es esencial para garantizar la seguridad operativa y proteger la integridad de los sistemas y datos de la organización. Todos los usuarios y administradores deben ser conscientes de su responsabilidad para mantener este principio y adherirse a los controles establecidos para gestionar los accesos de manera efectiva.

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

- *Asignación basada en roles: Los privilegios de acceso se deben asignar en función del rol específico del usuario dentro de la organización. No se debe otorgar acceso a más recursos de los que un usuario necesita para desempeñar su función.*
- *Acceso restringido a sistemas sensibles: El acceso a información crítica, confidencial o estratégica debe ser limitado solo a aquellos usuarios cuyo trabajo lo requiera. Los usuarios deben ser autorizados de forma explícita para acceder a estos sistemas, y la autorización debe ser revisada periódicamente.*
- *Revisión periódica de privilegios: Los privilegios de acceso deben ser revisados regularmente para asegurar que los usuarios mantengan únicamente los permisos necesarios para sus funciones actuales. Cualquier cambio en el rol o en las responsabilidades de un usuario debe conllevar una revisión inmediata de sus privilegios.*
- *Rechazo de accesos innecesarios: En ningún caso un usuario debe recibir acceso por defecto a sistemas, aplicaciones o datos que no estén directamente relacionados con sus responsabilidades. Todos los accesos adicionales deben ser solicitados, evaluados y aprobados por el responsable de seguridad.*

Importancia de Mantener el Principio de Privilegio de Acceso Mínimo

Mantener el principio de privilegio de acceso mínimo es crucial para la protección de la información sensible y la integridad de los sistemas de la organización. La asignación indebida de permisos o la falta de restricciones adecuadas puede dar lugar a los siguientes riesgos:

- *Acceso no autorizado: Usuarios con privilegios excesivos pueden acceder a información o sistemas para los cuales no están autorizados, exponiendo así datos confidenciales.*
- *Incremento de la superficie de ataque: Los usuarios con privilegios elevados, si se ven comprometidos, pueden proporcionar a los atacantes un punto de acceso para obtener más control sobre los sistemas de la organización.*
- *Errores humanos y mal uso: Incluso sin malicia, un usuario con privilegios innecesarios puede cometer errores que afecten la estabilidad o la seguridad de los sistemas, como la eliminación o modificación de datos importantes.*

Responsabilidades

Cada miembro de la organización debe:

- *Gestionar el acceso de acuerdo con los principios de esta política: Los administradores de sistemas y recursos son responsables de asegurarse de que los privilegios de acceso se asignen correctamente y se ajusten a las necesidades laborales de los usuarios.*

- *Solicitar cambios de privilegios a través de los canales adecuados: Cualquier solicitud para otorgar, modificar o eliminar privilegios debe ser canalizada a través del proceso formal de gestión de accesos de la organización.*
- *Reportar accesos sospechosos o actividades inusuales: Todos los usuarios deben estar atentos a comportamientos inusuales y reportarlos inmediatamente al departamento de seguridad o administración de sistemas.*

Seguridad: La seguridad de los sistemas y la protección de la información son fundamentales para el éxito y la continuidad de la organización. La implementación efectiva del principio de privilegio de acceso mínimo contribuye a la mitigación de los riesgos de seguridad, tales como:

- *Prevención de brechas de seguridad: Limitar el acceso de los usuarios solo a los recursos necesarios reduce significativamente la probabilidad de que un atacante pueda obtener acceso a información sensible en caso de que una cuenta de usuario sea comprometida.*
- *Auditoría y trazabilidad: Al aplicar el principio de privilegio mínimo, es más fácil realizar auditorías y seguimientos de las actividades de los usuarios. Si un incidente de seguridad ocurre, la trazabilidad de accesos y actividades será más clara y se podrá tomar acción correctiva rápidamente.*

La implementación de este lineamiento está del lado de la Oficina de Tecnologías de la Información de la entidad. Aún se encuentra en espera de retroalimentación de esta Oficina a la UT y Soporte informático.
Así mismo se ha venido realizando el acompañamiento en el Assesment realizado por GoToCloud para aplicaciones On Premises como lo son RUE, RUTEC y CEN, las cuales pretenden ser migradas a Azure. El Assesment ha venido avanzando en diferentes etapas, en donde se ha realizado:

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

Actualmente se está a espera del envío de la propuesta de arquitectura para validar el modelo IaaS o PaaS que se adopte mejor a las aplicaciones mencionadas y posteriormente la cotización para el aprovisionamiento de estos componentes y servicios en Azure.

Se realizaron las siguientes observaciones de los tableros de control en Power BI:

- Atenciones: la actualización desde el origen de datos 01/06/2024
- Capacitaciones y cieti: la actualización desde el origen de datos 01/05/2026
- centros entrenamiento: la actualización desde el origen de datos 02/08/2025
- teletrabajadores: la actualización desde el origen de datos 31/12/2023.
- El campo es paz total: la actualización desde el origen de datos 30/11/2023.
- Encuestas trabajo infantil - la actualización desde el origen de datos 28/07/2025
- Equipares Rurales - la actualización desde el origen de datos 02/06/2023.
- estado joven - la actualización desde el origen de datos 08/06/2023.
- Formándonos para la paz total: la actualización desde el origen de datos 30/09/2023 al 30/11/2023.
- Fortaleciendo Sueños_Jóvenes para la Paz: la actualización desde el origen de datos no contiene fechas.
- La comunidad mi causa: la actualización desde el origen de datos 31/12/2023
- Observatorio: la actualización desde el origen de datos 25/07/2025
- RUTEC: la actualización desde el origen de datos 09/11/2023

- Subsistema de Formación para el Trabajo: la actualización desde el origen de datos 09/11/2023

No se realizó la pausa de servicios de nube todo dado que se debe tener una sesión técnica y funcional, con el fin de que el área de la oficina de TIC como encargada de administrar costos del tenant el Ministerio de Trabajo sea quien pause los componentes que se evalúen en la misma sesión.

También se han remitido diferentes recordatorios a la Oficina TIC relacionado con las fechas de finalización del contrato Enterprise Agreement de Azure en el Tenant de la entidad las cuales están previstas para el mes de agosto de 2025, esto con el fin de que se realicen las respectivas validaciones a nivel de costos previo a la finalización del contrato y puedan realizar el ejercicio de Instancia reservada para los componentes que la propia Oficina TIC defina. Esto en el marco de la continuidad de los servicios de la Nube Pública y el aprovechamiento adecuado de los recursos/créditos aprovisionados en el Tenant, ya que el comportamiento de este tipo de recursos, como se ha mencionado en otras ocasiones; si no es aprovechado o reservado antes de la fecha fin del contrato, no son acumulables para la siguiente suscripción.

Es importante que se definan estos componentes (un inventario por suscripción y el tipo de instancia reservada) y se realice la reserva de manera adecuada dentro del portal. De igual forma informamos que esta acción debe realizarse desde la cuenta que administra el Contrato de EA (custodiada por la Oficina TIC de la entidad), ya que los costos y el manejo de recursos es alcance estrictamente de la entidad, ya que se trata de recursos públicos traducidos en créditos de Azure.

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 38 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. Se observa que se tuvieron picos altos de consumo sin afecta el rendimiento del canal , se observa un flujo estable de tráfico, se tuvo un consumo promedio de entrada de 344.68 Mbps y 477.39 Mbps de salida

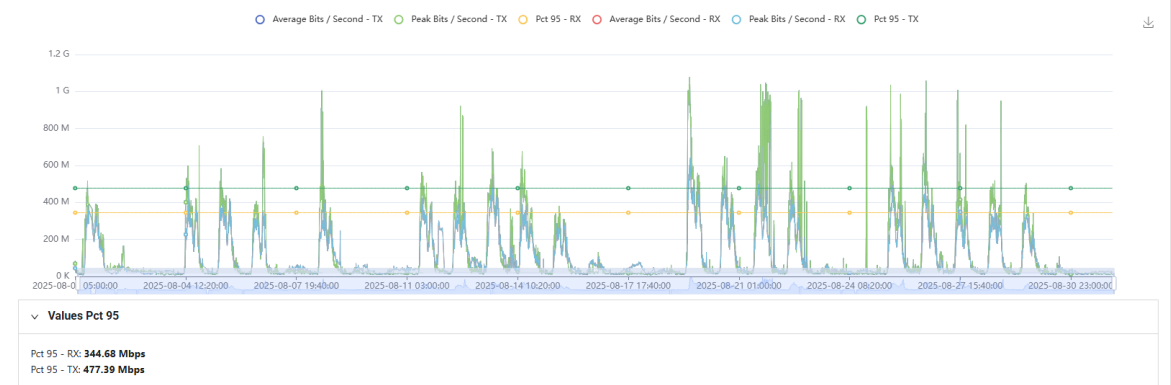


Ilustración 39 Grafica de consumo canal Internet Datacenter

Durante el mes de agosto 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.

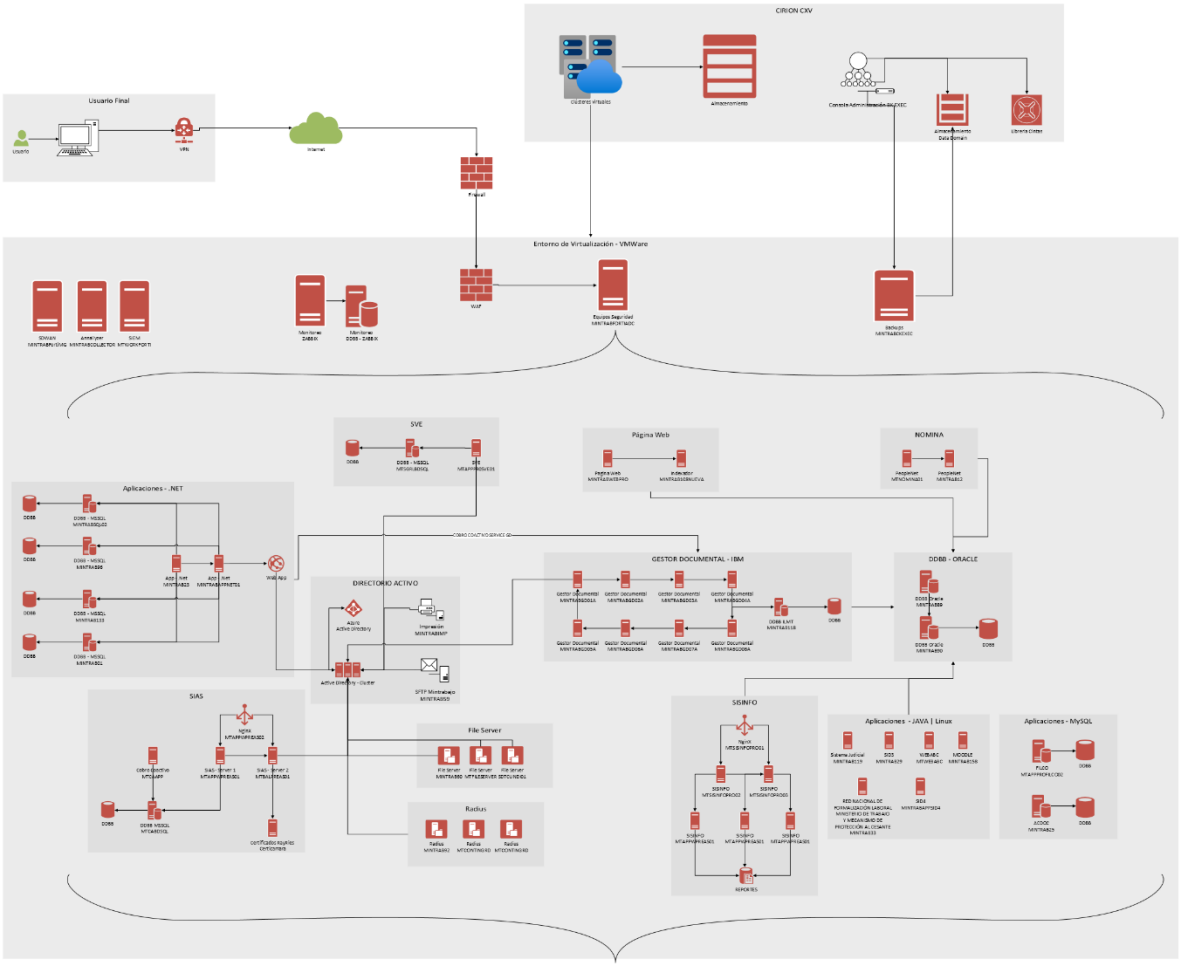
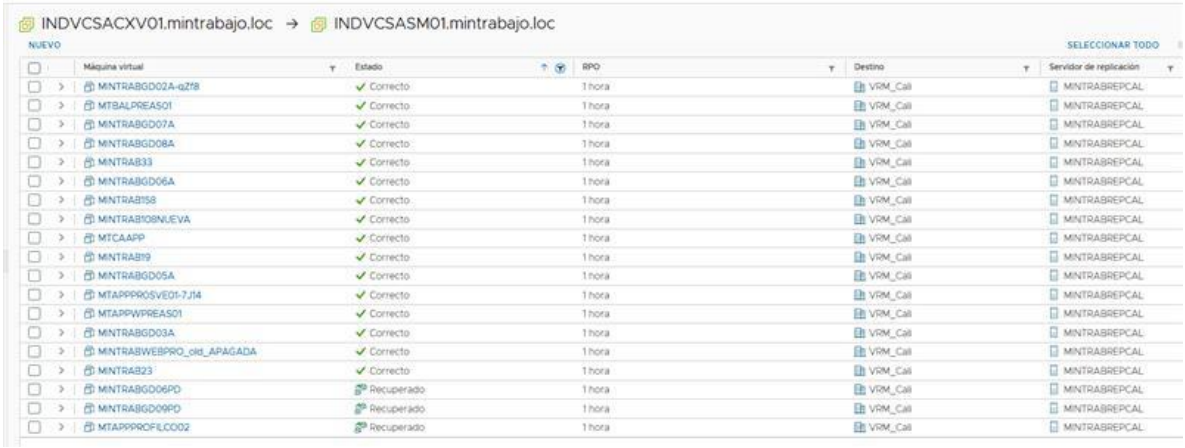


Ilustración 40 Diagrama Interoperabilidad Bogotá CXV

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
MINTRAB19	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
MTAPPPROFILCO02	Recuperado	1 hora	VRM_Cali	MINTRABREPCAL

Ilustración 41 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.
Durante el mes de julio se presenta inconvenientes en la replicación debido a que el versionamiento de uno de los componentes de VMWare VRM (Virtual Replication Manager) exigía la actualización a nueva versión, la cual fue realizada de manera satisfactoria en DataCenter de Cali, mitigando así los inconvenientes de replicación, de igual forma se realiza escalamiento a Broadcom para dejar trazabilidad de lo sucedido y obtener retroalimentación y mejores prácticas por parte del propio fabricante. Es Importante mencionar que, esta actividad no generó indisponibilidad de servicios productivos, al contrario, optimizo procesos de replicación y sincronización entre Datacenter.

Teniendo en cuenta lo anterior, se han venido realizando sesiones tecnicas entre los especialsitas de SOC, Redes y Nube Privada para realizar modificaciones a nivel de conectividad en el data center alterno para garantizar independencia en las VLAN para cada servicio alojado en este datacenter y una depuración de puertos necesarios para re direccionar trafico hacía el balanceador configurado en este datacenter. Esto en pro de mejorar los aspectos de seguridad, conectividad y sincronización entre los dos sites y garantizar una correcta replicación de los servicios.

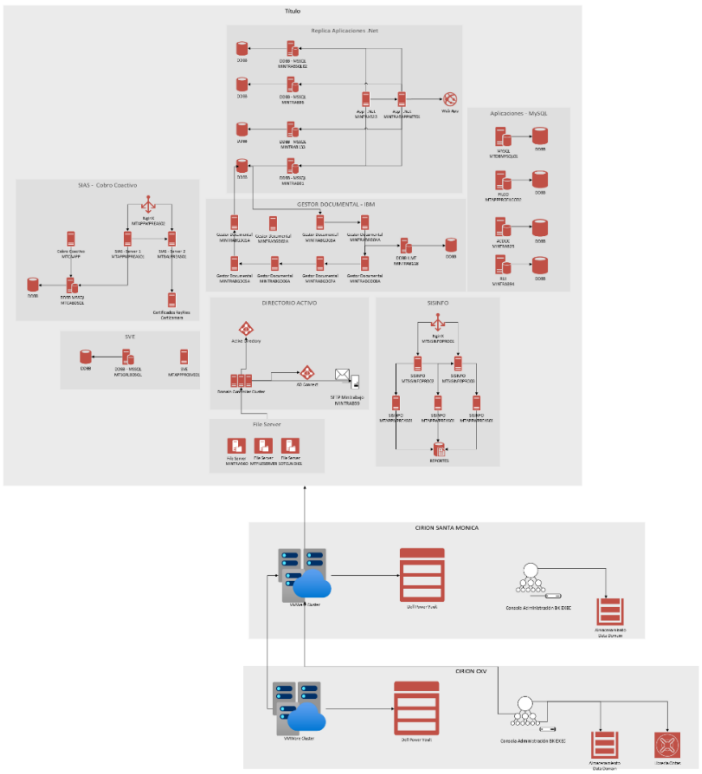


Ilustración 42 Diagrama de Replicación CXV - Santa Mónica

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 mantuvo activo con bajo tráfico durante el mes. Se observa que se tuvo un promedio de 760 Kbps de entrada y 170Kbps de salida. Se relaciona las graficas de consumo de ambos extremos

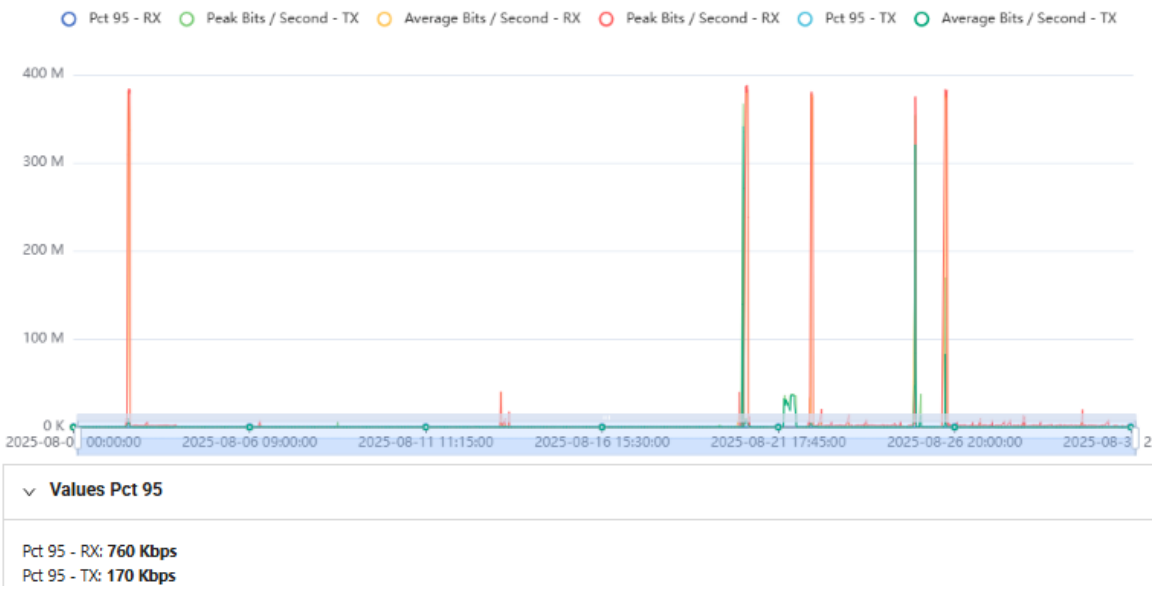


Ilustración *43* LANTOLAN extremo Bogotá

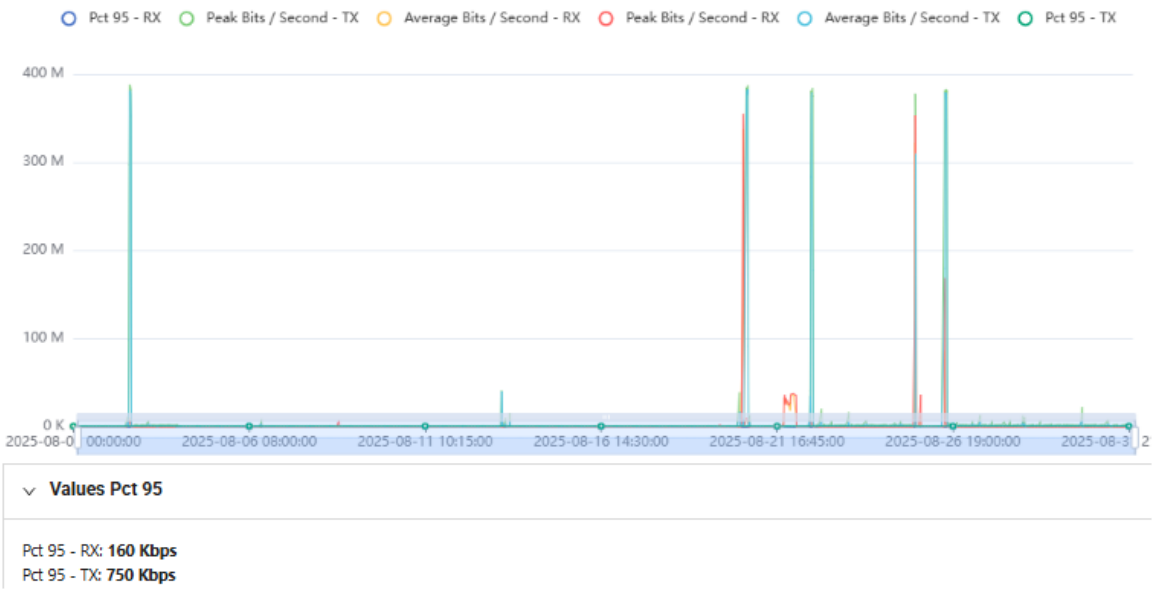


Ilustración *44* LANTOLAN extremo Cali

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.

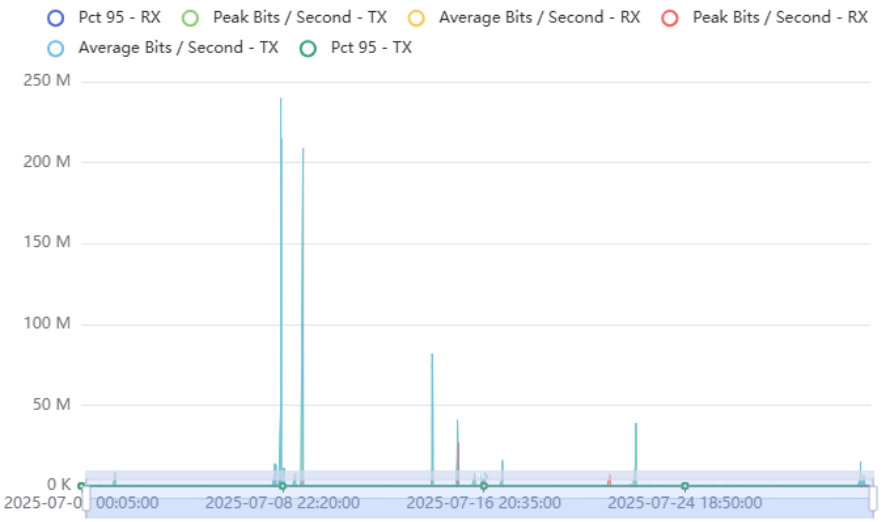


Ilustración *45* Estado canal de Internet DC Cali

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

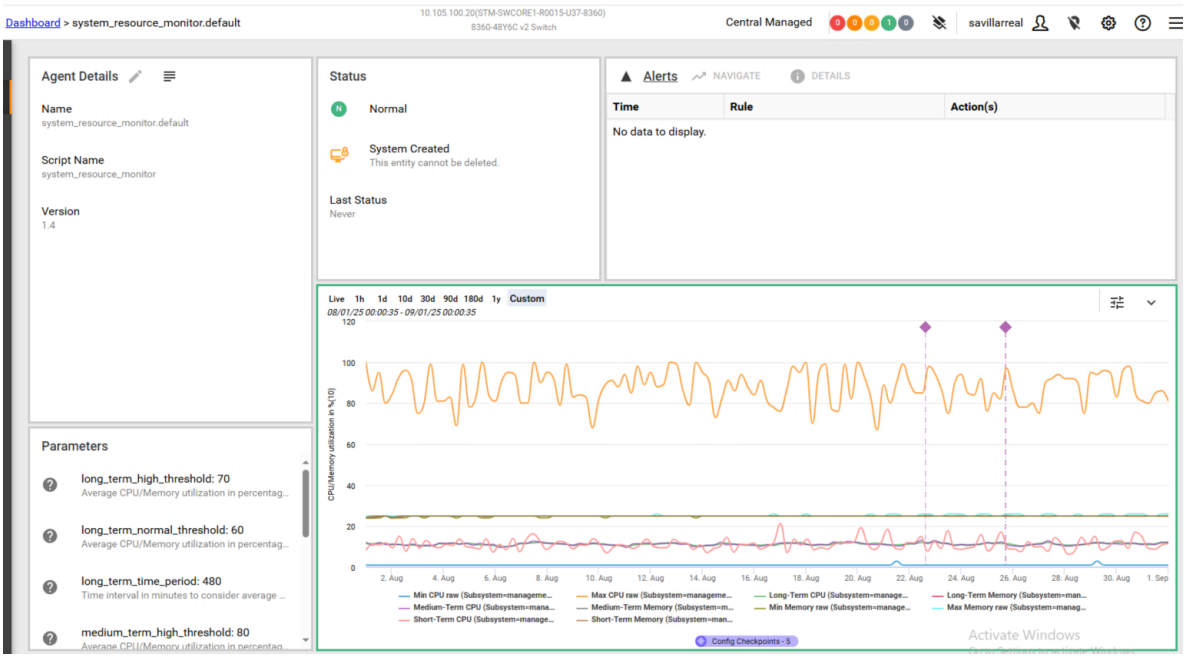


Ilustración 46 Estado SWCORE Datacenter alterno

Se verifica el canal MPLS de datacenter alterno, el cual se observa que se ha mantenido activo durante el mes de agosto, no se presentaron reportes de caídas de servicio. El trafico en este canal es bajo debido a que es el correspondiente al canal del centro alterno.

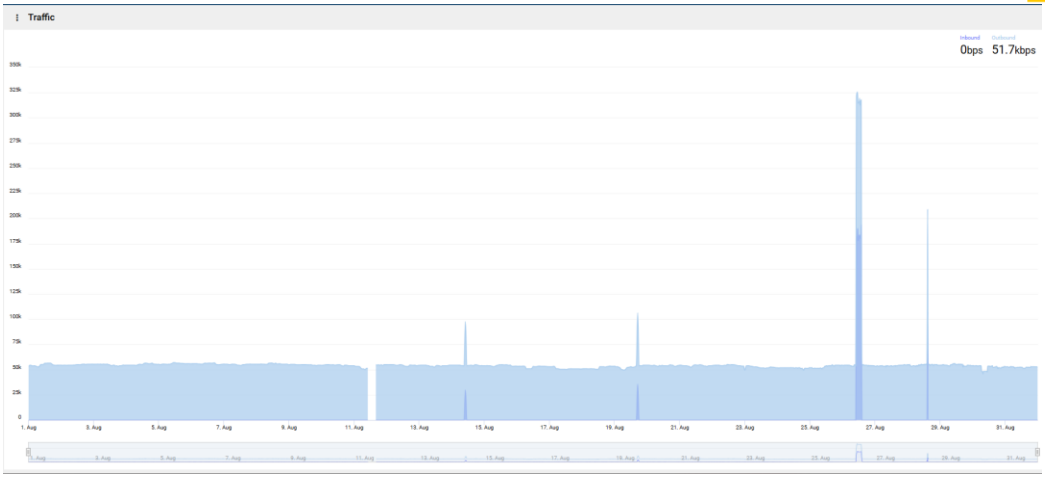


Ilustración 47 Estado canal MPLS DC Alterno

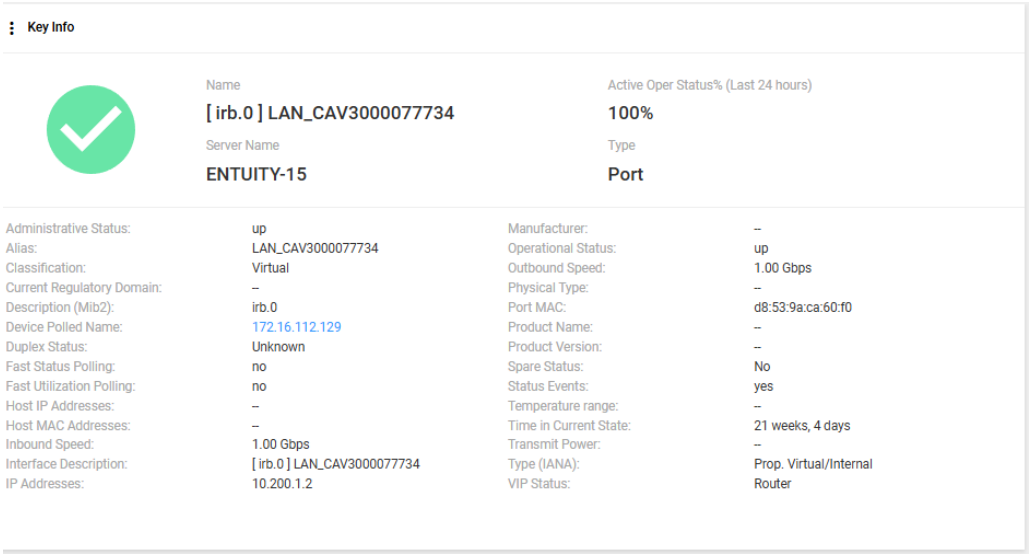


Ilustración 48 Estado interface de conexión equipo MPLS DC Alterno

Se verifica estado del equipo, donde se observa que no presento caídas ni bloqueos en su funcionamiento

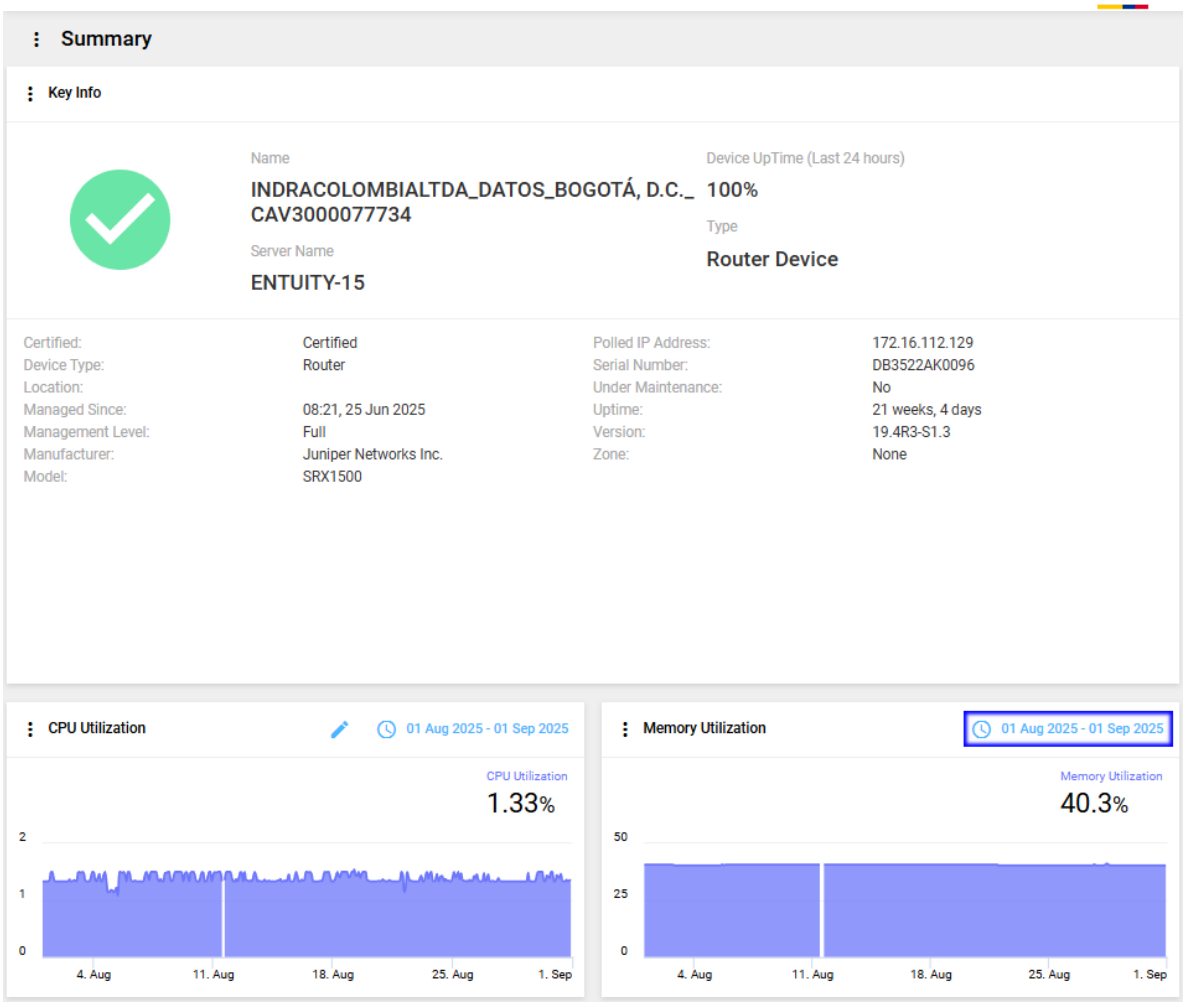


Ilustración 49 Estado equipo MPLS DC Alterno

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. Hasta el momento no se ha obtenido retroalimentación por parte de la entidad.
- Se comparte informe de estado actual a la entidad, tanto a la nueva Jefatura de la Oficina de Tecnologías de la Información como el nuevo Coordinador de Soporte informático.
- Se está a espera de retroalimentación de la documentación de File Server compartida y de la estrategia propuesta para la migración hacia un nuevo entorno.

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.

Es importante mencionar que la entidad no ha fortalecido o establecido una ruta para la retención de los backups de manera clara y concisa, por lo cual el equipo de trabajo creo el plan de backups y se definieron tiempos de retención de los mismos orientados a Infraestructura de acuerdo a las buenas practicas y experiencia del equipo de trabajo. No se definen tiempos claros para estos recursos ni para documentos virtuales, file server o backups de usuario final por parte de la entidad.

Se ha solicitado Instrucción a la entidad instrucción con respecto a los siguientes recursos los cuales se encuentran alojados en la Nube Privada de la entidad y por su grado de Obsolescencia critico y debido a que el sistema Operativo en el que se encuentran aprovisionados estos recursos se encuentra totalmente fuera de soporte, se requiere de una instrucción precisa y clara del cómo proceder con los siguientes recursos:

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

VM → SDTCUNDI01: Esta maquina virtual fue usado históricamente como un File Server (Servidor de archivos) para la Subdirección de IVC/Gestión Territorial. En la actualidad aloja información histórica de la entidad, pero no observamos una alta transaccionalidad hacía el servidor. Es requerido

se indique si es posible dar de baja este servidor y generar una copia de seguridad o si de lo contrario es requerido migrar esta información a un File Server en uso con sistema operativo actualizado. No obstante, existe la salvedad que dentro de este servidor se aloja la base de datos de Access de CUNDISSIT por lo cual se debe validar en donde alojar este recurso o que decisión se toma con respecto al mismo.

3.1.4. Aplicaciones Especializadas

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

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

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

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

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

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 ya fue configurado de la mera correcta para su despligue posteriomente a producción.

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

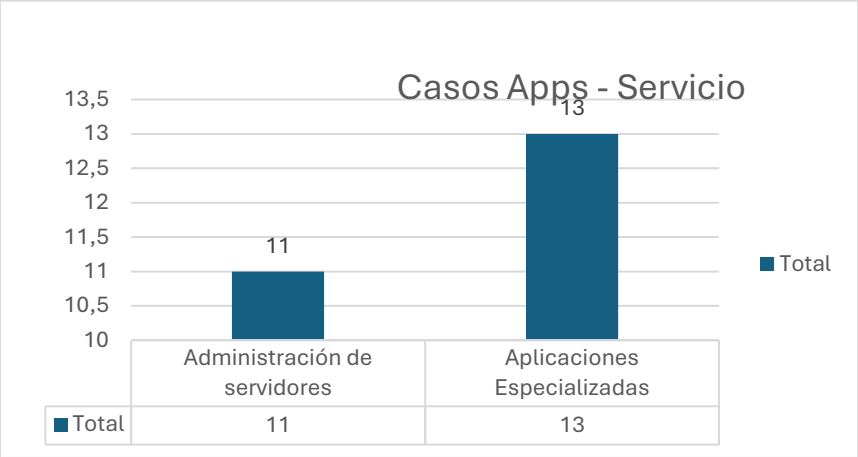


Ilustración *50* Estado final de casos – Aplicaciones Especializadas

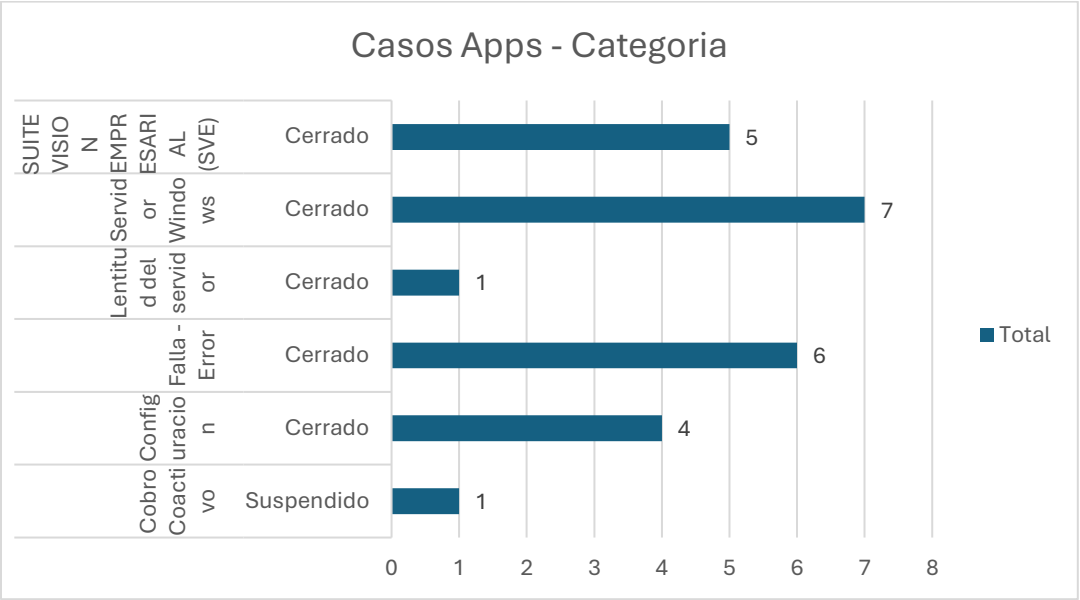


Ilustración 51 categorías Apps

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.
    - Se informan retrasos en los procesos de desarrollo del equipo de IVC y aun se esta a espera de información hacía la Oficina TIC y el Grupo de Soporte Informático.
- Tras avance en el desarrollo, la entidad determina que el sistema no se encuentra listo para salir a producción.

- **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 Página Web de la entidad y que es administrado actualmente por el área de Empleo.
- Se logra conexión entre FileNet y LifeRay, en validación de conexión entre DSpace y LifeRay o FileNet en su defecto.
    - Validando configuraciones de DDB PostGressSQL para migración de documentos a FileNet.

- **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 está 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	
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

Nombre App	Acceso actual	Funcionario	Observaciones
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. Tras este contexto, se realiza backup de todos los despliegues de las aplicaciones y fueron migradas a nuevos entornos sin cambiar el servidor de respuesta de la aplicación.

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 SIAS la cual se desplegará en Julio de 2025 (avance indicado en detalle anterior donde indican un retraso de 2 meses en el proceso de desarrollo por parte del equipo de IVC) según lo informado por el área de IVC. A la fecha de entrega del informe, SIAS no se encuentra con su nueva versión y FIVICOT se encuentra en fase de despliegue del ambiente productivo. Actualmente se estan realizando configuraciones que permitan independizar los sites app2 – app3 – app4 para que cada aplicación cuente con su DNS propio y así tener un orden y una accesibilidad mas clara a los sistemas de información de la entidad, ya que mas de 10 aplicaciones acceden con la misma URL variando el directorio de acceso, lo cual a futuro puede ser muy confuso para los usuarios. Se están realizando maniobras de content routing para independizar puertos DNS e IP publicas y así realizar este cambio de manera satisfactoria en ambiente productivo. Al ser una ventana de mantenimiento bastante critica es están realizando las planeaciones correspondientes para así ejecutarla de manera segmentadas, estructurada y satisfactoriamente en producción.

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

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

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

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

Item	Actividad	Responsable	Julio								
			9	10	11	12	13	14	15	16	17
1	Recepción SISGESTION Mintrabajo - DNP	DNP - Ministerio de trabajo - Unión Temporal TIC									
2	Recepción de medios por parte del Ministerio de Trabajo	Ministerio de trabajo - Unión Temporal TIC									
3	Validación de medio digital	Especialistas Unión Temporal TIC									
4	Ejecución de scripts de SQL	Especialista Bases de Datos SQL									
5	Instalar el complemento de Reporting Services para Visual Studio	Especialista Bases de Datos SQL - Especialista .Net									
6	Cambiar los datos de conexión en el web.config	Especialista .Net									
7	Modificar los niveles de seguridad configurados por defecto en la aplicación	Especialista .Net									
8	Compilar y publicar el sitio	Especialista .Net									
9	Desplegar en el servidor 172.20.22.64 (QA)	Especialista .Net									

Estado:
Ejecutado
En ejecución
No ejecutado

Tabla 59 Cronograma Implementación SISGESTIÓN

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

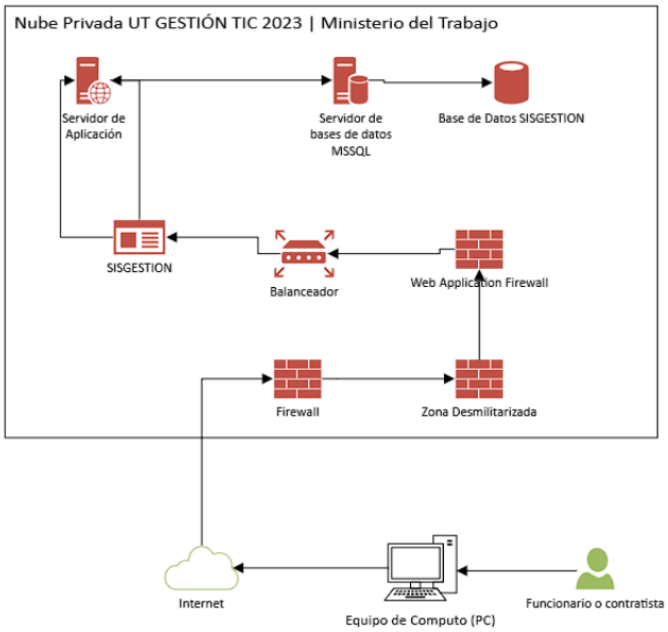


Ilustración 52 Arquitectura de la Aplicación Sugerida por la UT

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

- Instalación del complemento de Reporting Services en Visual Studio Para asegurar la carga completa de todos los proyectos incluidos en la solución SISGESTION, fue necesario instalar el complemento correspondiente a Reporting Services, el cual habilita el soporte para reportes dentro del entorno de desarrollo.
- Configuración de cadena de conexión Se actualizaron los datos de conexión dentro del archivo web.config de la aplicación, utilizando la información suministrada desde la parte de la base de datos, con el fin de enlazar correctamente la aplicación con la base de datos correspondiente.
- Ajustes de seguridad en el archivo de configuración. Se realizaron modificaciones en los niveles de seguridad definidos por defecto en la aplicación, permitiendo la autenticación a

través del protocolo HTTP. Para ello, se ajustó la propiedad correspondiente en el archivo web.config
- Compilación y publicación del sitio. Con las configuraciones anteriores completadas, se procedió a compilar la solución en Visual Studio y publicar el sitio para su posterior despliegue en el entorno designado.
- Despliegue en el servidor de pruebas (QA). La aplicación fue desplegada en el servidor correspondiente al ambiente de pruebas (QA), en el cual se realizan validaciones funcionales.
- Creación del sitio en IIS y configuración de puerto de salida Finalmente, se creó el sitio correspondiente en el servidor web IIS (Internet Information Services), configurando un puerto de salida específico para asegurar su accesibilidad dentro de la red del Ministerio.

Este proceso se desarrolló de forma controlada, documentando cada paso técnico relevante y asegurando que el sistema quedara disponible para las pruebas funcionales y validación por parte del equipo del Ministerio de Trabajo
Durante el proceso de despliegue del sistema SISGESTION se identificaron varios aspectos relevantes que deben ser tenidos en cuenta para la continuidad del proyecto, su estabilización y eventual puesta en producción:

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

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

- El sistema de información tiene una implementación muy similar a varias aplicaciones desarrolladas en lenguaje .NET que posee actualmente la entidad.
- El sistema de información viene de una transición de versionamiento de sistemas operativos y base de datos deprecado (versiones 2012) que actualmente, la versión que está siendo desarrollada y por liberar por parte del DNP (versión 2.0) posee una actualización a versiones 2019.
    - El equipo de Servicios Centrales de la UT se encuentra en proceso de actualización a versionamiento 2022 de Sistema Operativo Windows y de Base de datos SQL Server.
    - SISGESTION tiene aval y despliegue correcto en sistema operativo y base de datos 2019, no se ha probado por parte del DNP en versión 2022. Pueden existir problemas de compatibilidad, en principio debería funcionar de manera adecuada, pero lo ideal es que la aplicación sea probada en entornos 2022 para validar el funcionamiento adecuado en esta versión de sistema operativo y de base de datos.

- El sistema de información SISGESTION tiene una dependencia en su desarrollo con un componente INFRAGISTIC el cual es un componente que según informa el equipo de Tecnología de DNP, se encuentra fuera de soporte y se encuentran en etapa de desarrollo para eliminar la dependencia de este componente, el cual genera problemas de compatibilidad con los navegadores actuales (Google Chrome, Microsoft Edge y Mozilla Firefox) lo cual degrada la experiencia del usuario final, ya que la herramienta no se comporta de manera adecuada.
    - La versión que el DNP liberará (versión 2.0) posee actualizaciones que permite la compatibilidad y uso adecuado del sistema de información SISGESTION en Microsoft Edge y Google Chrome sin inconvenientes, pero es importante precisar que continua con el componente Infragistics que a futuro quedará obsoleto en un corto o mediano plazo.
- La aplicación se encuentra desarrollada en .Net Framework 4.5 y la versión de SISGESTION que actualmente están liberando esta actualizada a versión .Net Framework 4.7. La última versión disponible de .Net Framework es 4.8.1. La recomendación para aplicaciones nuevas es la migración a .Net Core o .Net 6/8.
    - Lo anteriormente mencionado requiere un proceso de reescritura del código fuente de la aplicación. Esto en función de que la aplicación no se quede obsoleta al corto plazo por los versionamientos de componente .NET Framework.
    - Es importante precisar que la obsolescencia de este tipo de componentes se ven reflejadas en vulnerabilidades de seguridad sobre las aplicaciones por falta de soporte por parte de su fabricante, en este caso Microsoft, que recomienda el desarrollo y la actualización de las aplicaciones a los versionamientos mencionados.
    - El estado actual de .NET Framework 4.7 por parte de Microsoft es el siguiente:
        - Solamente recibe actualizaciones o parches de seguridad hasta 2027 como máximo.
        - Tiene soporte limitado por parte de fabricante (Microsoft)
        - Se recomienda migrar a .NET 4.8 o .NET 6/8
- Es importante que las áreas funcionales/misionales de la entidad validen los flujos de cada proceso dentro del sistema de información y que estos se adecuen a su necesidad.
    - En caso de que exista alguna variante en el flujo, algún paso dentro del procedimiento, actividad adicional o que se deba eliminar implicaría intervenir el código de la aplicación. Es decir, la entidad debe contar con un equipo de desarrollo de software dedicado explícitamente a adecuar el sistema de información en términos de lógica de programación para que se alinee a las necesidades funcionales y misionales del Ministerio.
    - En caso de no recibir actualizaciones del software por parte del DNP, este equipo de desarrollo de software debe realizar el mantenimiento de la aplicación a nivel de la capa de aplicación (en caso de que surjan necesidades adicionales, modificación de módulos existentes, creación de nuevos flujos y demás).
    - Si la aplicación es intervenida en su lógica de programación por un equipo de Ministerio del Trabajo y en el futuro el DNP libera actualizaciones las cuales el Ministerio es aplicable, se deben realizar pruebas de compatibilidad entre las actualizaciones liberadas por el DNP y las adecuaciones realizadas por el equipo de Ministerio del Trabajo.
- El sistema de información del DNP cuenta con servicios de Firma electrónica con servicios de firma centralizada, el cual es un servicio que garantiza Integridad y autenticidad en los procesos de firma de documentos electrónicos.
    - Actualmente el Ministerio no cuenta con estos servicios adquiridos por lo cual, si se quiere implementar SISGESTION con todas las funcionalidades que DNP posee actualmente y libera en su versión 2.0. Se deben adquirir los servicios de firma electrónica, firma centralizada y certificados digitales para los actores dentro de la entidad que actuarían como firmantes dentro del sistema de información.
    - En caso de no acogerse a la modalidad de firma digital, se debería modificar el flujo para cambiar el paso de firma por un paso de aprobación o firma mecánica. Esto

también implicaría modificar el software para que se adecue a la decisión que tome la entidad.

- Ejecución de Scripts para creación de roles Estándar de acuerdo a lo remitido por parte del equipo de DNP.
- Se realizó conexión exitosa con el LDAP de la entidad, por lo cual los usuarios creados en SISGESTIÓN pueden iniciar sesión con su usuario y contraseña de dominio tras la creación del usuario en SISGESTION con el mismo domain name.

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

- Aspectos técnicos: ya fueron gestionados todos los ítems que pueden depender del Grupo de Soporte Informático y el equipo de servicios centrales de la UT.
  - Ya se configuró todo el entorno de servidores y base de datos para pruebas.
  - Se actualizó la imagen institucional del sistema.
  - Se ejecutaron los scripts de creación de roles.
  - Se realizó configuración con Active Directory.
  - Se suministraron usuarios administradores para creación de usuarios.
- Aspectos funcionales: Se deben establecer los líderes funcionales del sistema de información y de los procedimientos asociados dentro del sistema de información.
- Se deben establecer los usuarios que se deben crear en SISGESTIÓN para asignación de roles para posterior interacción dentro del sistema de información.
- Se deben crear los flujos tanto internos como el ya existente dentro del sistema de información para definir una ruta critica de los módulos o módulos de SISGESTION, así como inicio de las pruebas dentro del sistema de información por parte de los usuarios.

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

Se esta presentó el siguiente inconveniente sobre la aplicación COBRO COACTIVO, normalmente cuando ocurre este incidente se mitiga con apoyo del Ing. Rodrigo Barrera, la actividad consta de la generación de un Backup de la DDBB para realizar identificación de los registros que deben ser intervenidos (modificación o eliminación)

Diagnóstico del equipo de Apps Especializadas .NET:

Actualmente se está presentando un error en la aplicación de cobro coactivo, reportado por el usuario, el cual afecta el funcionamiento de los módulos Asignaciones y Sancionados.

Detalles del incidente:

- Al revisar los registros del servidor IIS, se evidencian errores HTTP 500 durante la carga de los métodos:

/Deudores/Grid/
/Asignaciones/Grid/

- No se cuenta con un log interno de la aplicación que permita ampliar el análisis.
- Se han realizado validaciones en el servidor y en la base de datos, sin encontrar eventos asociados que expliquen el comportamiento.

Dado que no ha sido posible identificar la causa raíz del error, podríamos escalar el caso para contactar al equipo de desarrollo correspondiente. Alternativamente, sería útil contar con:

- El código fuente de la aplicación.
- Un usuario técnico con acceso a los módulos afectados, que permita realizar pruebas y obtener mayor detalle del comportamiento.

Estos son los print reportados por el usuario:

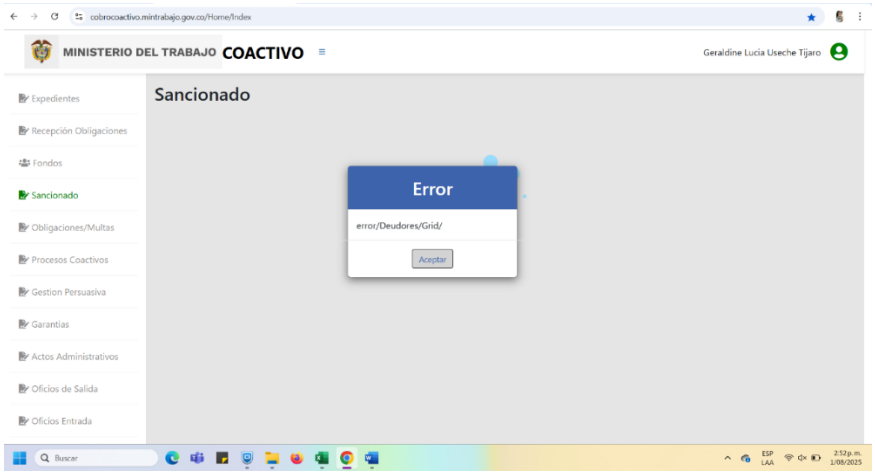


Ilustración 53 Error 1 CC

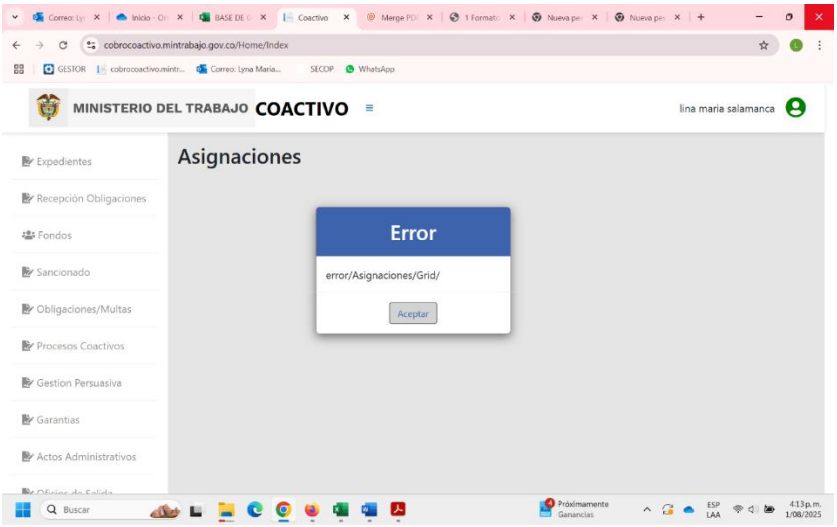


Ilustración 54 Error 2 CC

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 ejecuta paso a producción de las últimas versiones mencionadas en julio de 2025 de manera satisfactoria y sin errores en su despliegue.
- En etapa de pruebas para versión 7.4.

GESTOR DOCUMENTAL

A nivel de mantenimientos del gestor documental se realizaron actividades técnicas de mantenimiento en el marco de proceso de afinamiento y optimización, esto de acuerdo con la solicitud de ejecución por parte de la entidad, se plasman como evidencia los siguientes procedimientos:

Se hace entrega de información que justifica los procesos de mantenimiento del gestor documental

Plataforma - Aplicaciones

- Consultas lentas a los índices sobre los objetos de búsqueda de las tareas que se tiene en el portal de trabajo.
- Lentitud en la carga de información sobre las diferentes pantallas del proceso.
- Tener instancias innecesarias activas de proceso, generan peso a la aplicación ya que tiene toda la información cargada en el cache del servidor.
- No realizar borrado de los Documentos temporales de los File System en los diferentes servidores, se llenarían los espacios de almacenamiento y no permiten carga de más documentos y ejecución correcta de la plataforma.
- El no reinicio de las diferentes instancias del servidor de aplicaciones, ocasiona que se queden hilos pegados y hace que el procesamiento de los servidores físicos, estén en un alto procesamiento, esto genera lentitud y bloqueo de la plataforma.
- Se realiza primera ejecución productiva del módulo de envío de notificaciones el cual permite que el usuario tenga visibilidad de que radicados posee hace más de tres meses sin interacción y envía reporte notificando de que serán inactivadas de su perfil con el objeto de liberar la carga transacciona de la base de datos de la aplicación.
- Se ha observado un alto flujo de transacciones hacia la base de datos en comparación a meses anteriores, lo cual genera degradación del servicio si se analizan los aspectos como

transacciones inactivas, sesiones sin tráfico, radicados sin gestión, alto flujo de carga documental.

- Como se menciona en el apartado de Windows se generaron algunas indisponibilidades asociadas a la máquina virtual de FileNet, se está trabajando en la re implementación de este recurso para mitigar totalmente cualquier congelamiento de la máquina virtual.

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.

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

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

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:

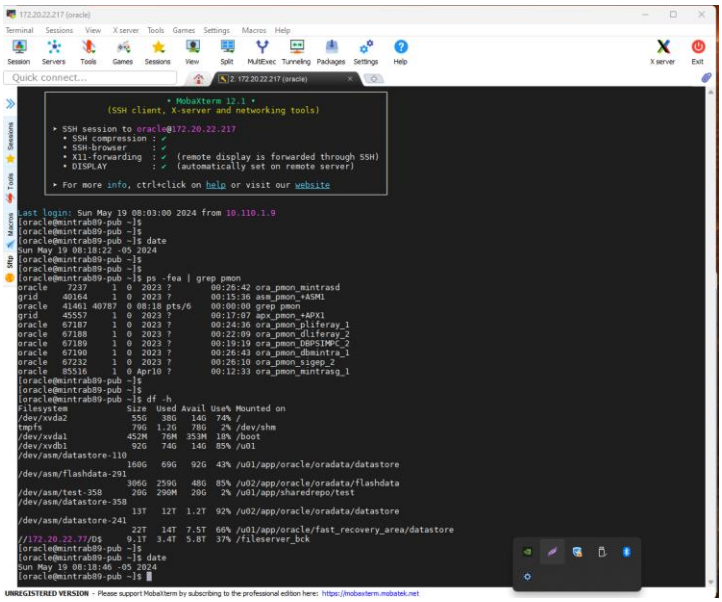


Ilustración 55 Estado pre-ventana

- **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

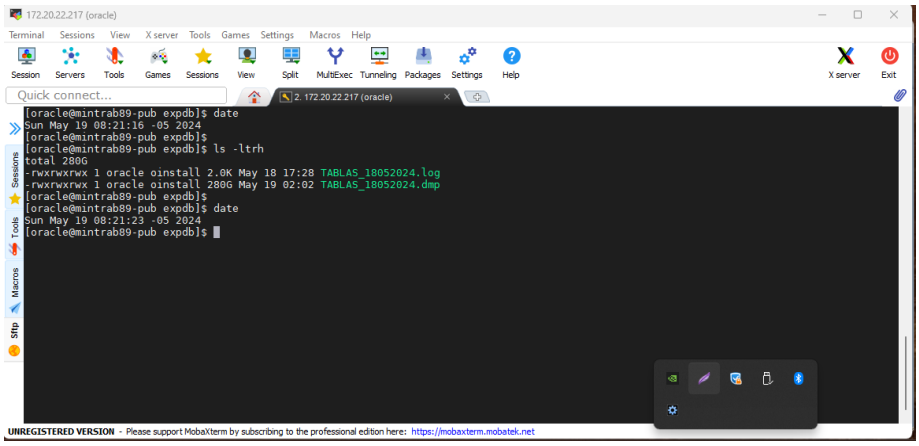


Ilustración 56 Generación de Backups DDBB

Validación tablas:

- **Tabla STORED_SYMBOL_TABLE:**

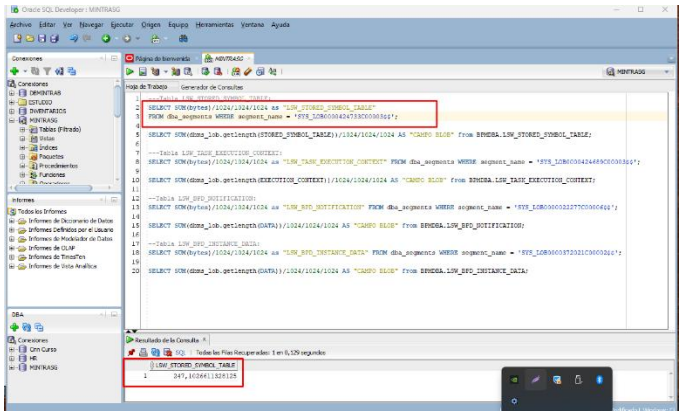


Ilustración 57 Validación Tablas DDBB

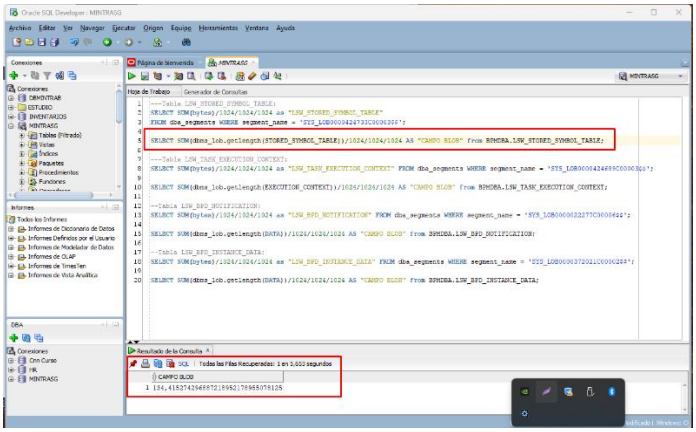


Ilustración 58 Validación Tablas DDBB

- **Tabla LSW_TASK_EXECUTION_CONTEXT:**

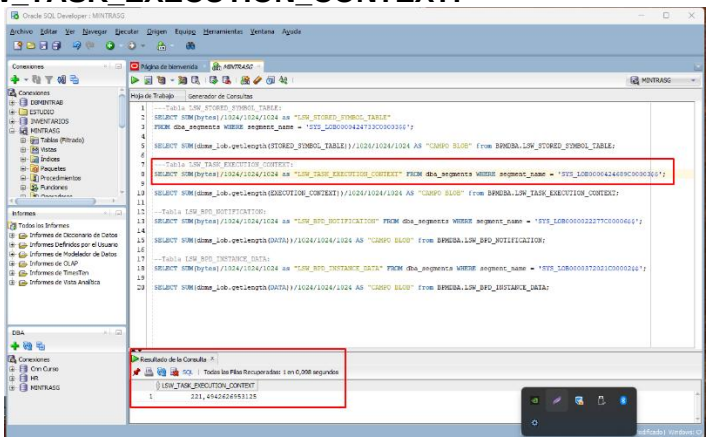


Ilustración 59 Validación Tablas DDBB

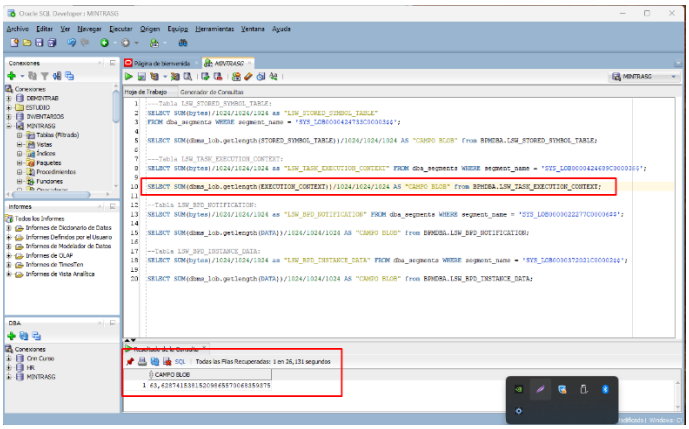


Ilustración 60 Validación Tablas DDBB

- **Tabla LSW_BPD_NOTIFICATION:**

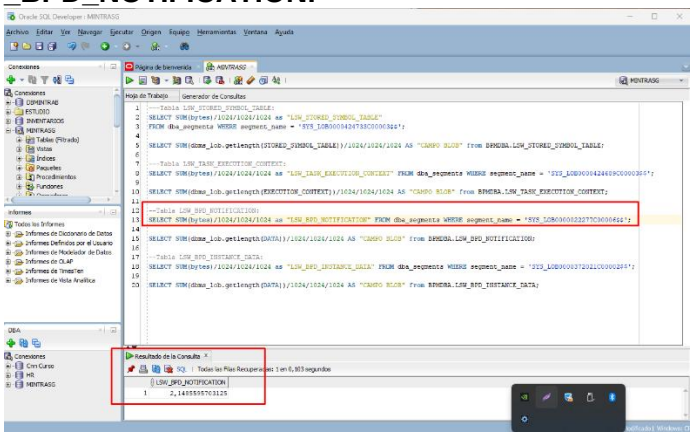


Ilustración 61 Validación Tablas DDBB

- **Tabla LSW_BPD_INSTANCE_DATA:**

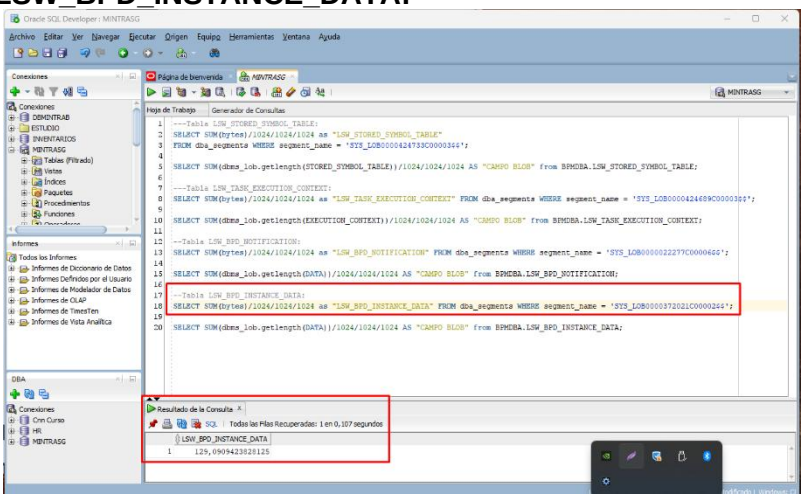


Ilustración 62 Validación Tablas DDBB

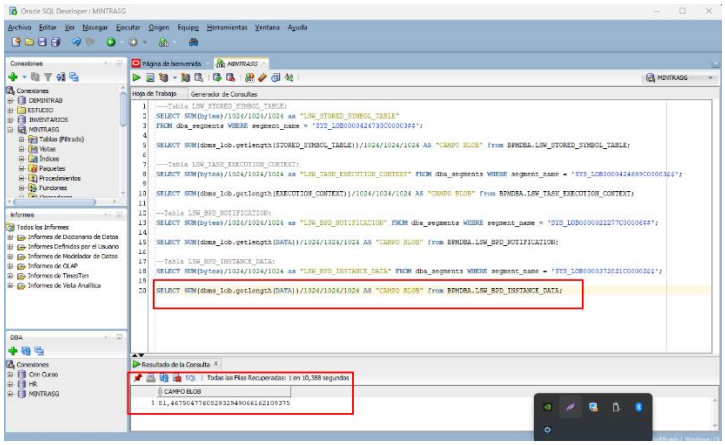


Ilustración 63 validación Tablas DDBB

- **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.

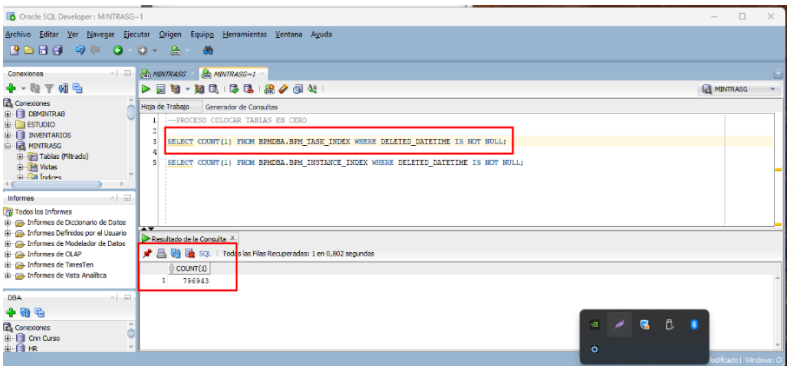


Ilustración 64 Verificación Registros

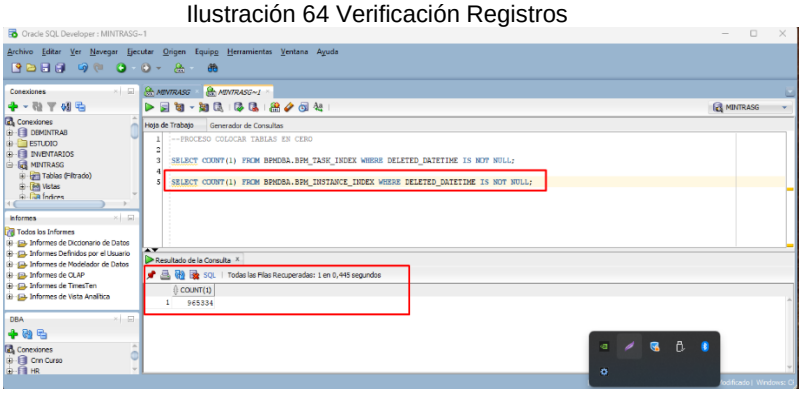


Ilustración 65 Verificación Registros

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

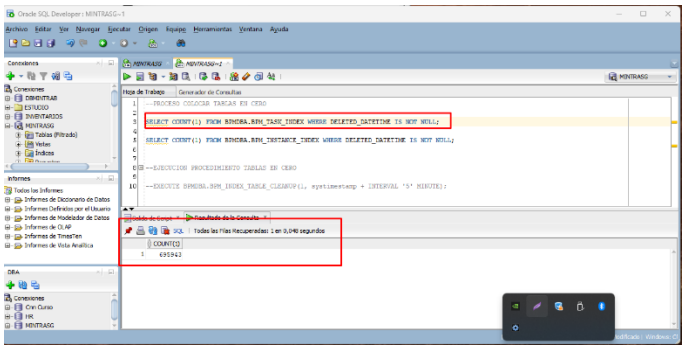


Ilustración 66 Verificación Registros tras ejecución de procesos

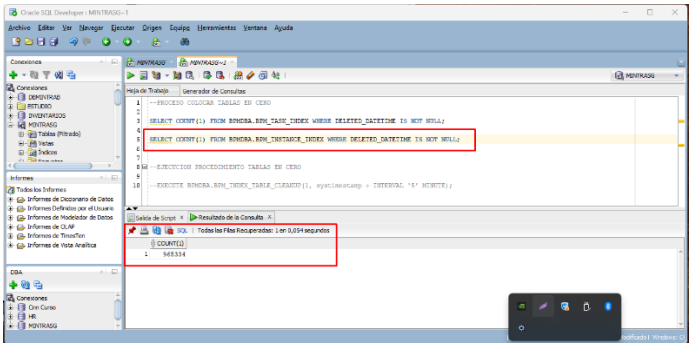


Ilustración 67 Validación de estado de tablas tras ejecución de procesos

- **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.

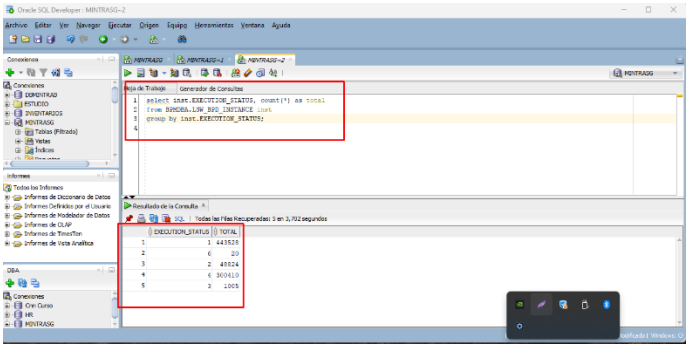


Ilustración 68 Estado de instancias DDDB

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

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

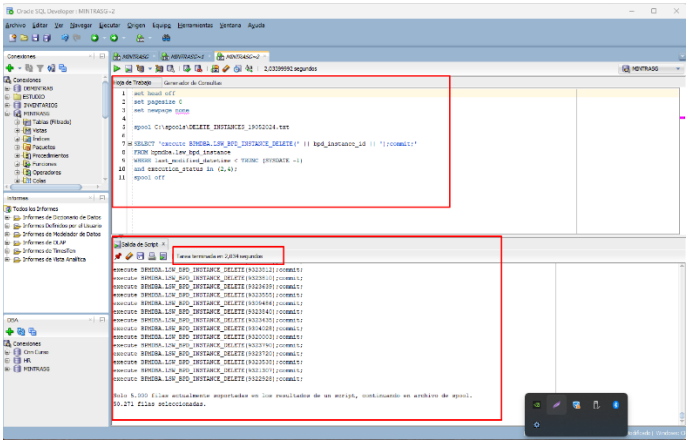


Ilustración 69 Eliminación de instancias

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

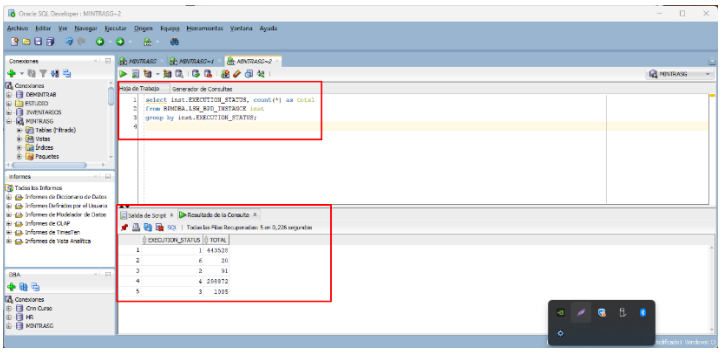


Ilustración 70 Disminución de instancias tras ejecución de proceso

Estado del servidor antes de la desfragmentación de tablas:

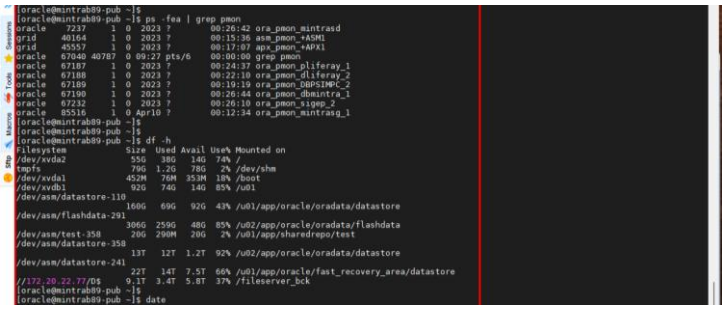


Ilustración 71 Estado del servidor - pre-desfragmentación

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:

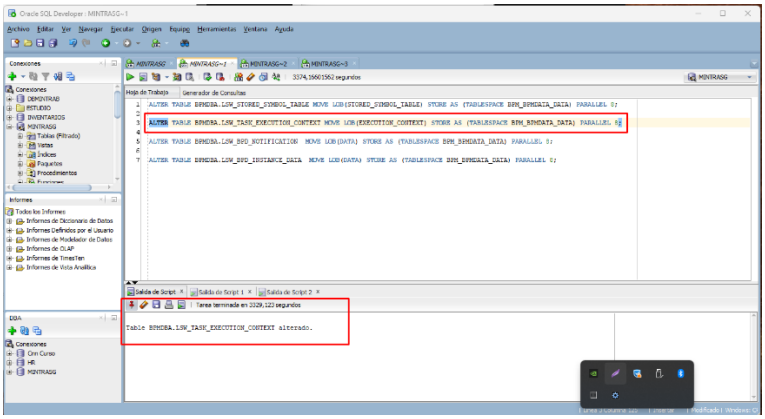


Ilustración 72 Ejecución desfragmentación

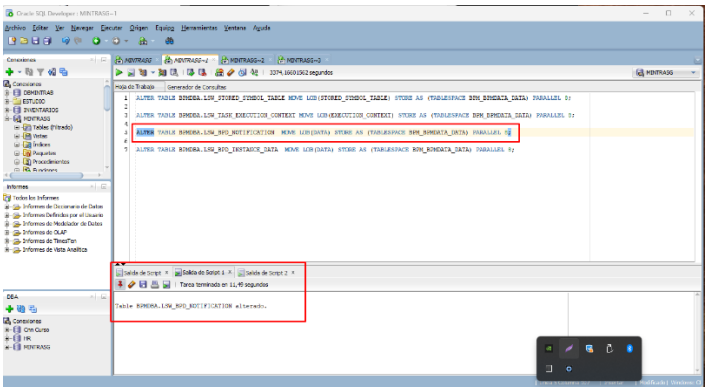


Ilustración 73 Ejecución desfragmentación

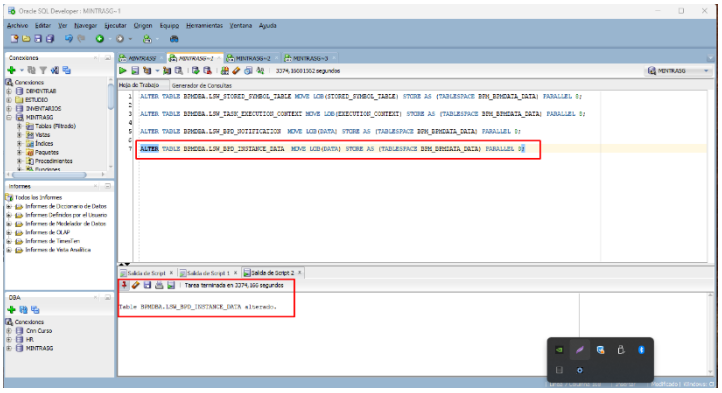


Ilustración 74 Ejecución desfragmentación

- **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.

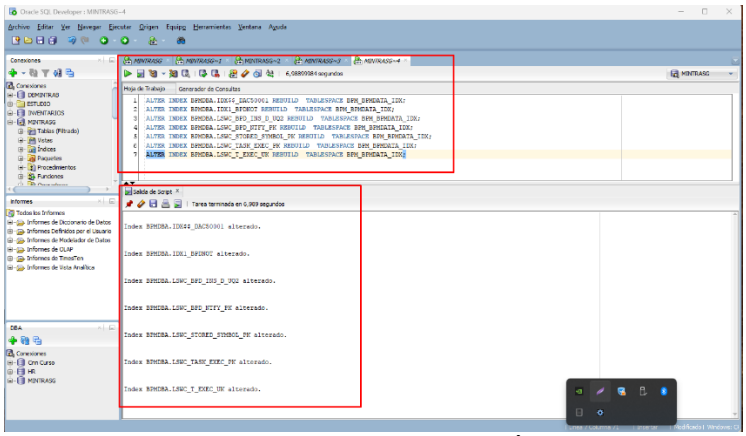


Ilustración 75 Reconstrucción de Índices

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

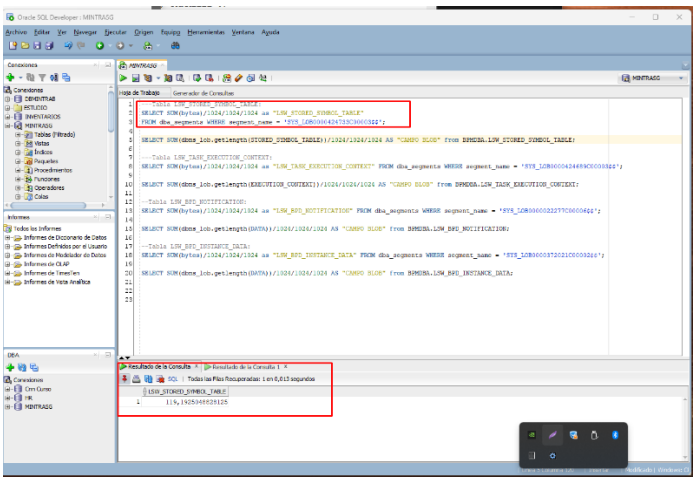


Ilustración 76 Validación de tamaños de tablas

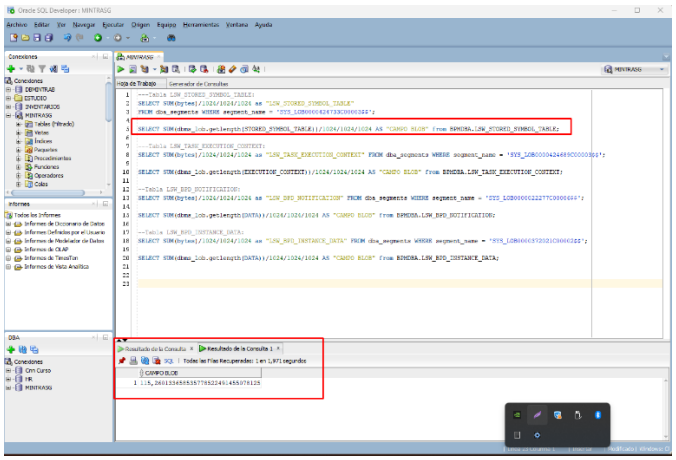


Ilustración 77 Validación de tamaños de tablas

- **Tabla LSW_TASK_EXECUTION_CONTEXT:**

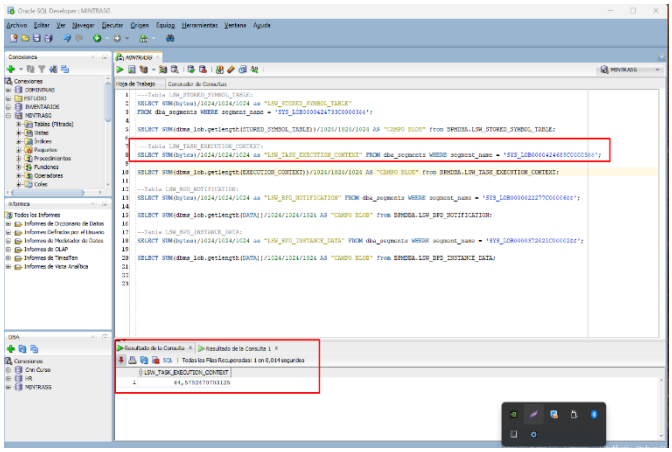


Ilustración 78 Validación de tamaños de tablas

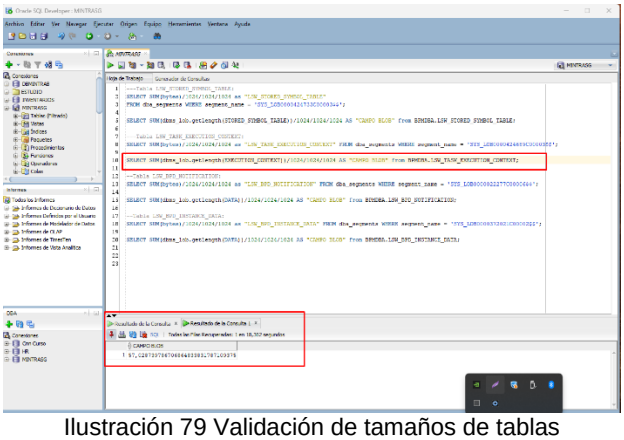


Ilustración 79 Validación de tamaños de tablas

- **Tabla LSW_BPD_NOTIFICATION:**

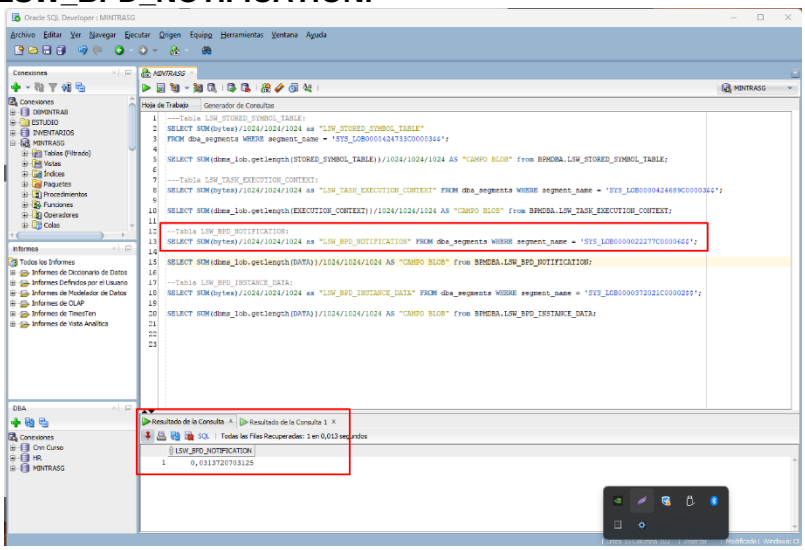


Ilustración 80 Validación de tamaños de tablas

- **Tabla LSW_BPD_INSTANCE_DATA:**

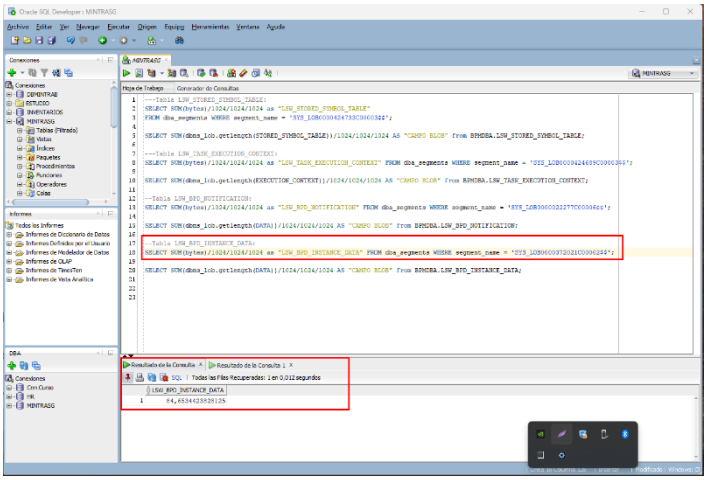


Ilustración 81 Validación de tamaños de tablas

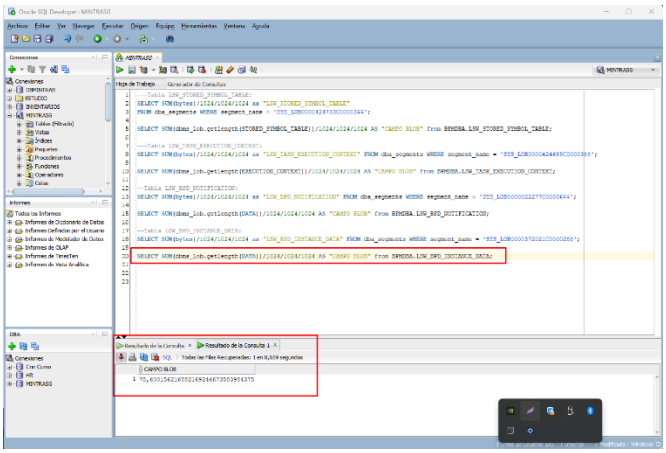


Ilustración 82 Validación de tamaños de tablas

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.

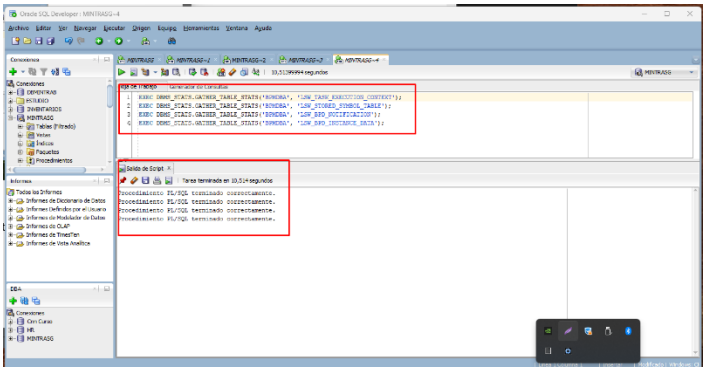


Ilustración 83 Ejecución de estadísticas de validación

Se procedió a 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 330 al mismo tiempo.

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 60 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.

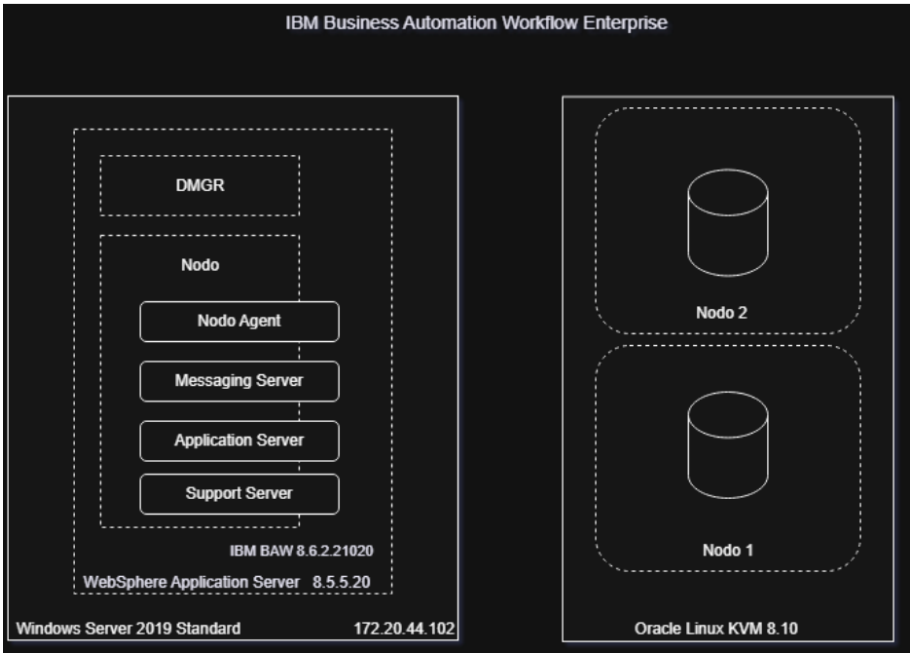


Ilustración 84 Diagrama BPM

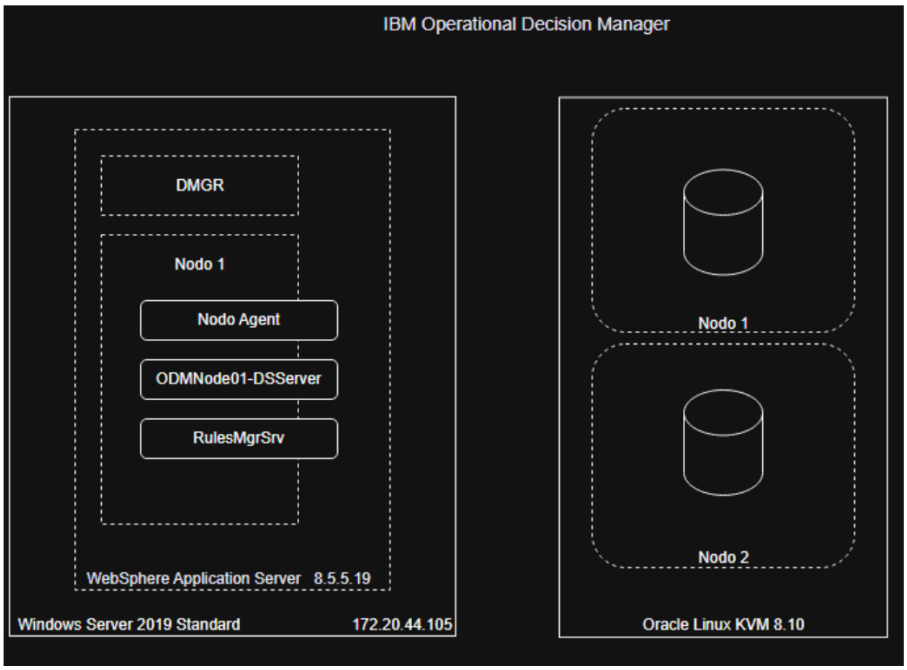


Ilustración 85 Diagrama ODM

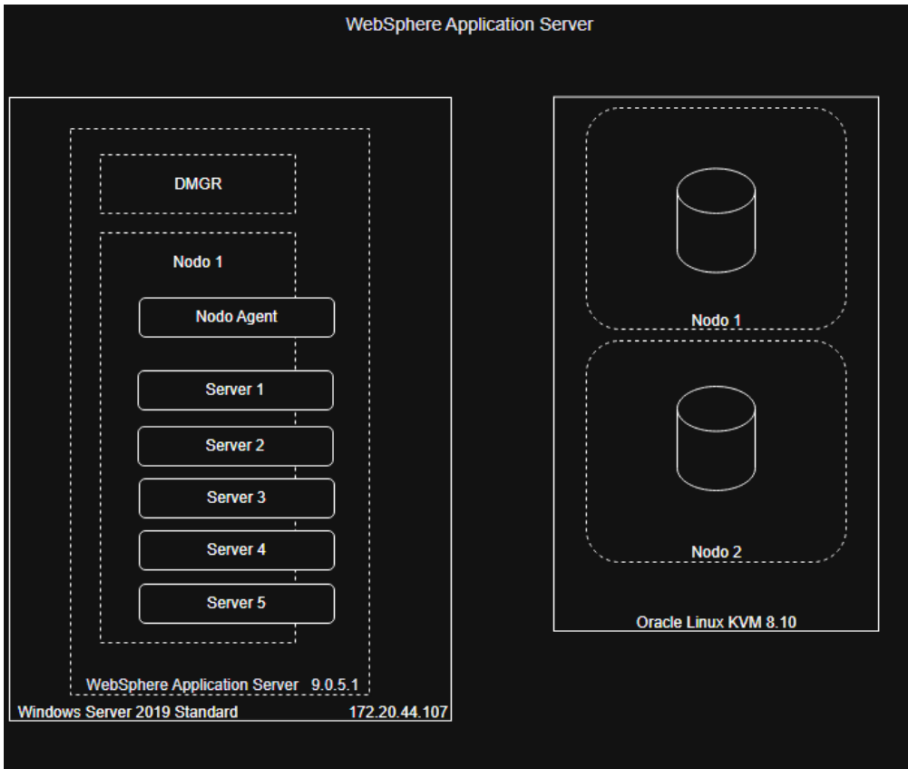


Ilustración 86 Diagrama WASND

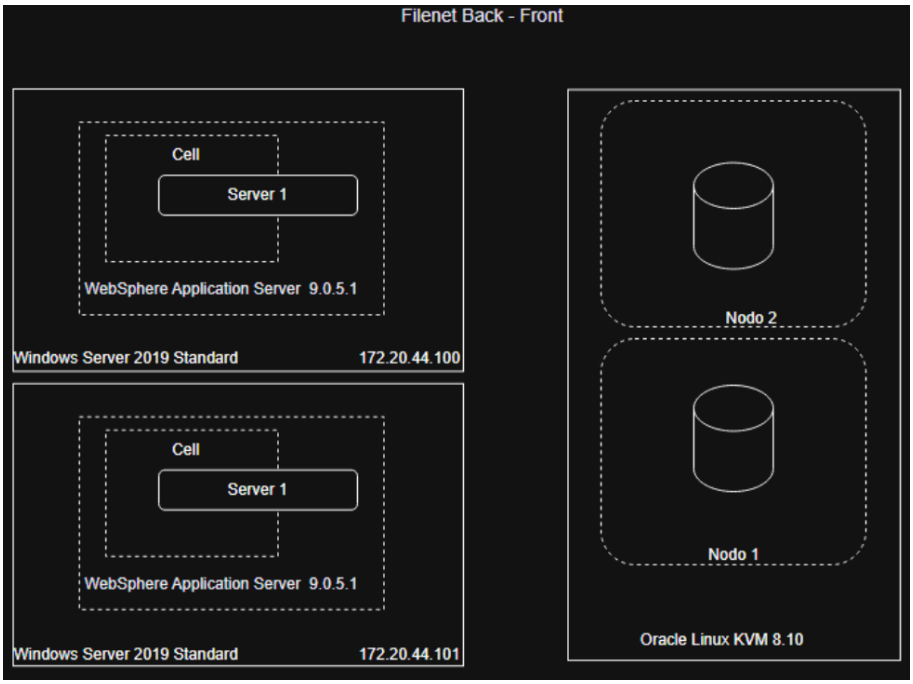


Ilustración 87 Diagrama FileNet Front

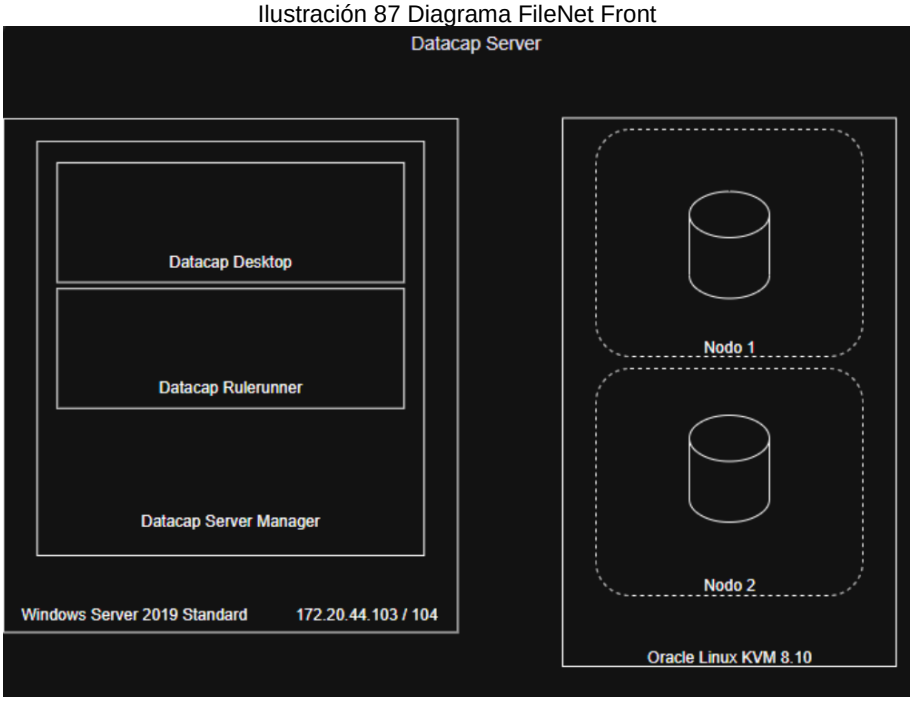


Ilustración 88 Diagrama Datacap

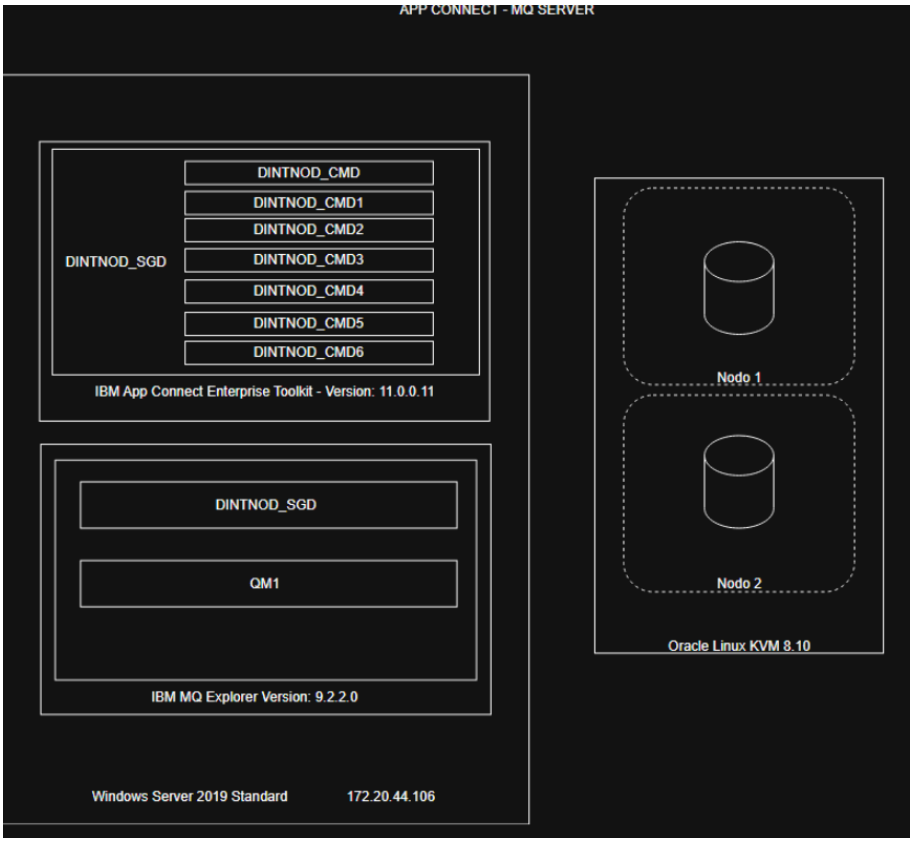


Ilustración 89 Diagrama App Connect

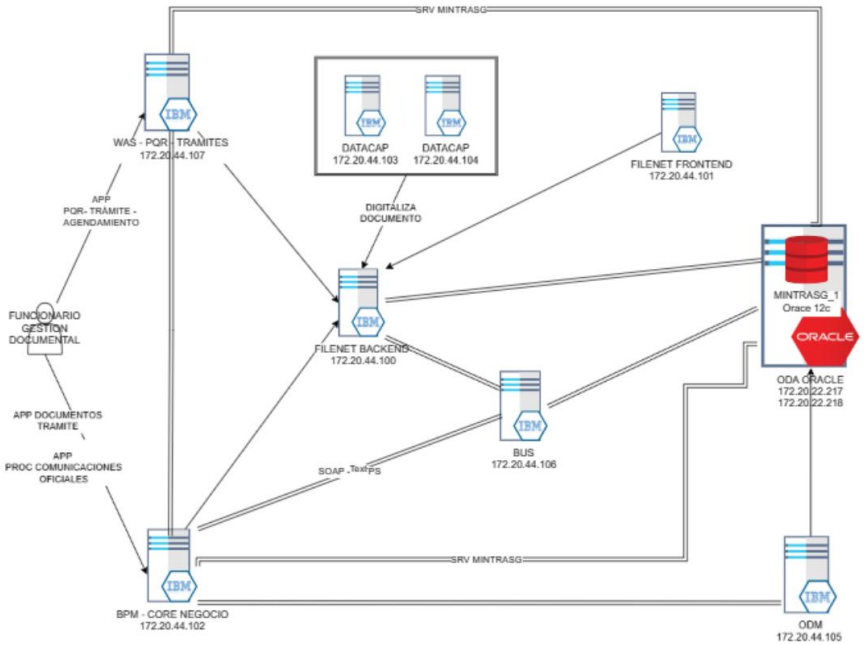


Ilustración 90 Arquitectura Gestor Documental

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 91 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 92 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 93 IBM Licenciamiento

Mes	Suma de Total Instancias
Enero 2025	111854
Febrero 2025	149070
Marzo 2025	148829
Abril 2025	135756
Mayo 2025	154121
Junio 2025	137472
Julio 2025	78502
Agosto 2025	92786
Total acumulado	**1.0083.90**

Tabla 61 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
Julio 2025	201882
Agosto 2025	190074
Total acumulado	**1.480.368**

Tabla 62 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
Julio 2025	79429
Agosto 2025	66811
Total, acumulado	**549.946**

Tabla 63 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 64 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 94 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 95 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.

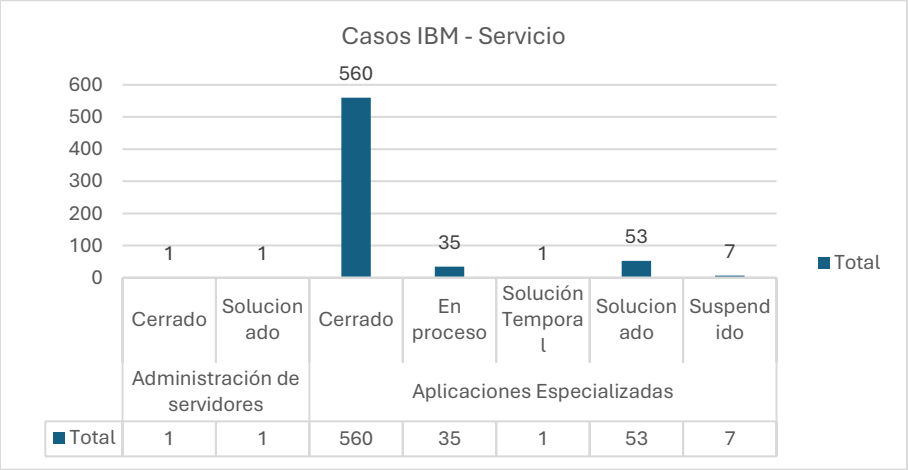


Ilustración 96 Casos IBM - Servicio

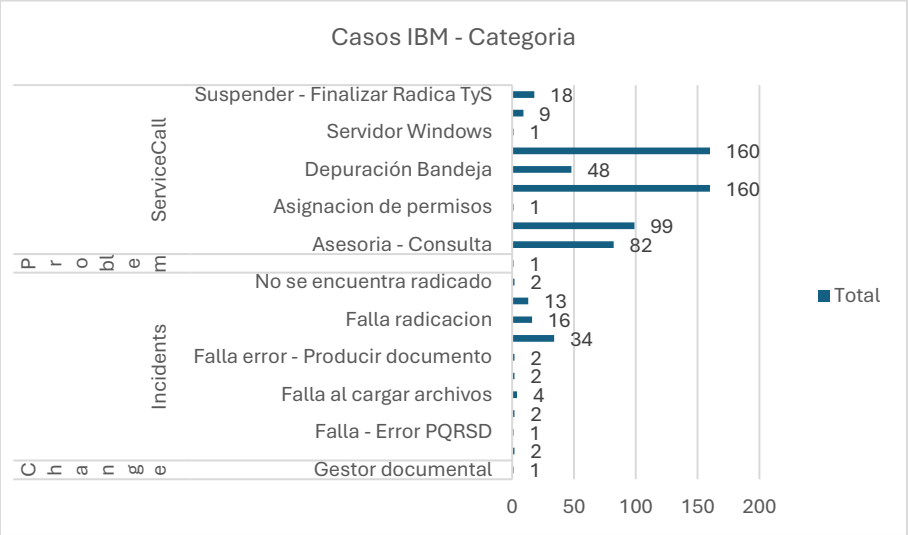


Ilustración 97 categoría DDBB

- **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 Coordinación del Grupo de Soporte Informático realizar un control sobre este tipo de solicitudes a áreas misionales/funcionales con el fin de poder estabilizar y canalizar de la mejor manera estas solicitudes para evitar problemas dentro de las aplicaciones y las bases de datos de la entidad.

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

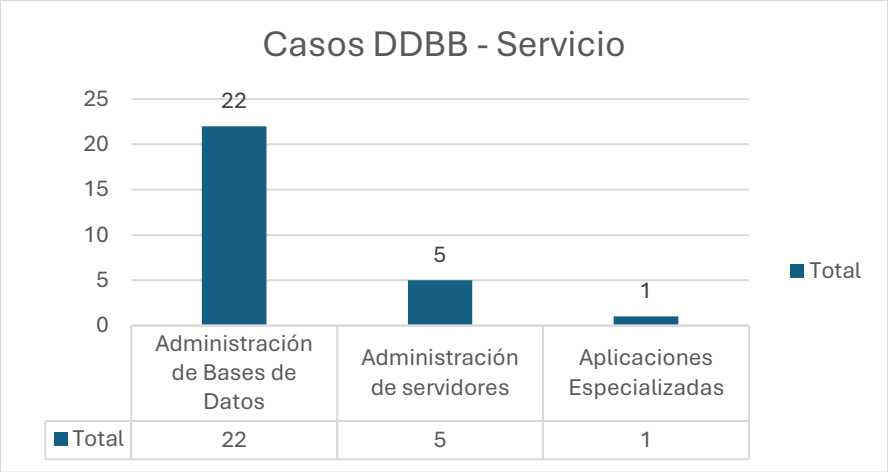


Ilustración 98 Casos DDBB por Servicio

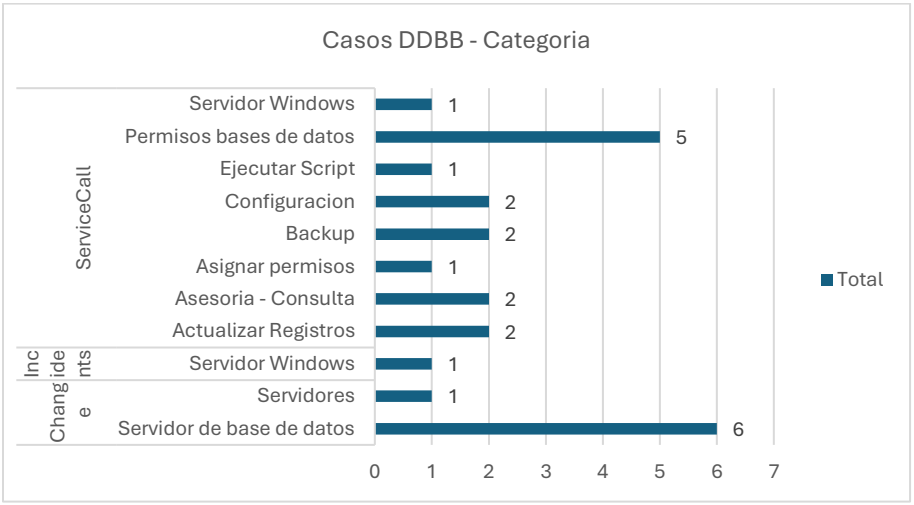


Ilustración 99 casos DDBB

- **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:

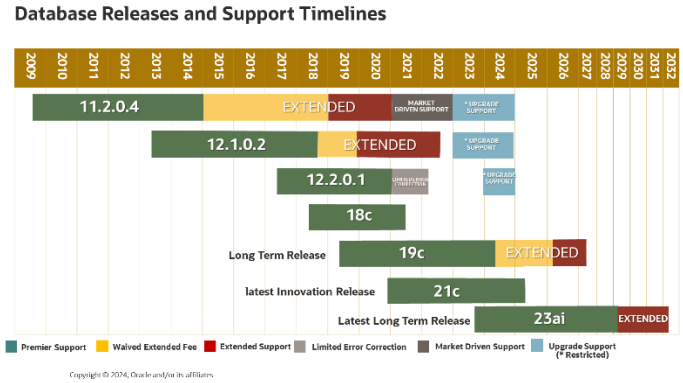


Ilustración *100* Estado Bases de Datos

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 65 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
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 66 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 67 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 101 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 102 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 103 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 104 Estadísticas Pool compartido

Tamaño base de datos MINSTRASG:

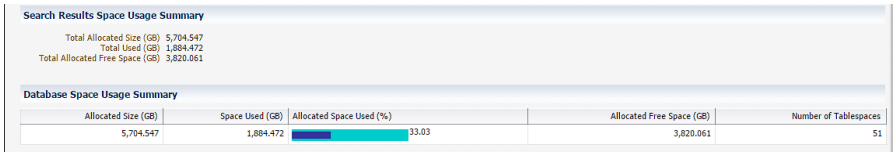


Ilustración 105 Tamaño DDBB

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 106 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

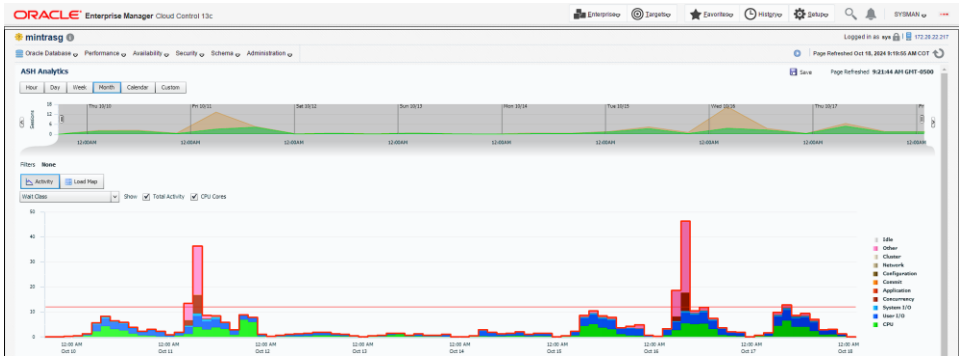


Ilustración 107 Rendimiento DDBB

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 108 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 109 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 110 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 111 Estadística Shared Pool

Tamaño base de datos DBMINTRA:

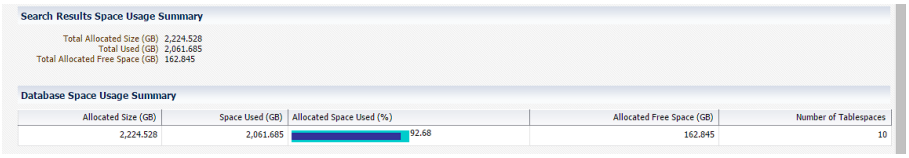


Ilustración 112 Tamaño DDBB DBMINTRA

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 113 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

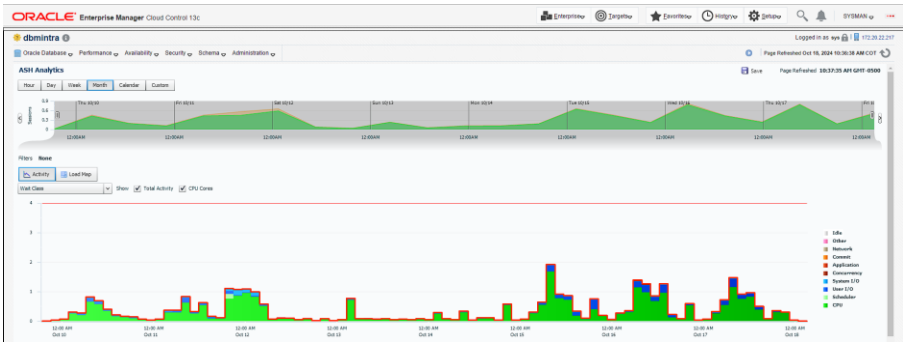


Ilustración 114 Rendimiento DDBB MINTRASG

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 115 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 116 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 117 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 118 Estadísticas Shared Pool

Tamaño base de datos PLIFERAY:

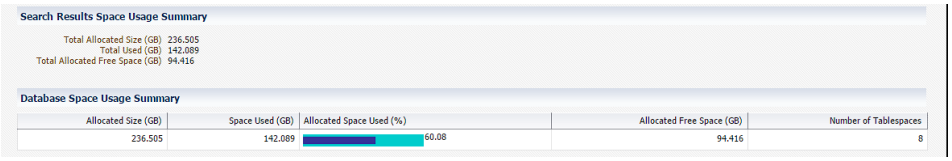


Ilustración 119 Tamaño DDBB PLifeRay

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 120 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

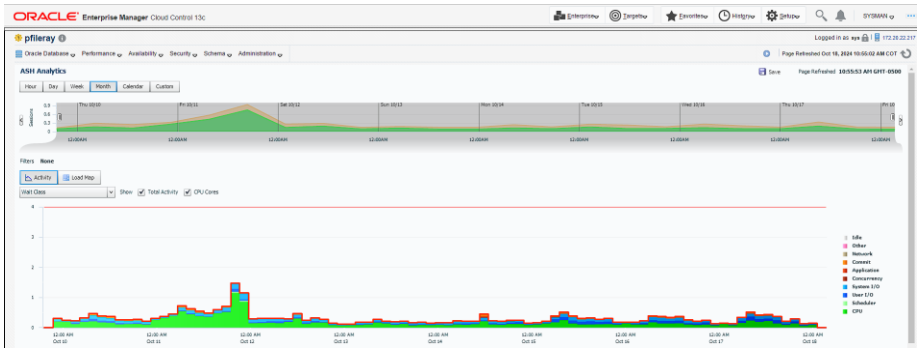


Ilustración 121 Rendimiento DDBB PlifeRay

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 122 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 123 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 124 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 125 Estadística Shared Pool

Tamaño base de datos SIGEP:

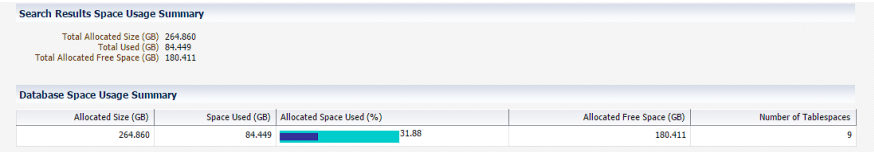


Ilustración 126 Tamaño DDBB SIGEP

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 127 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

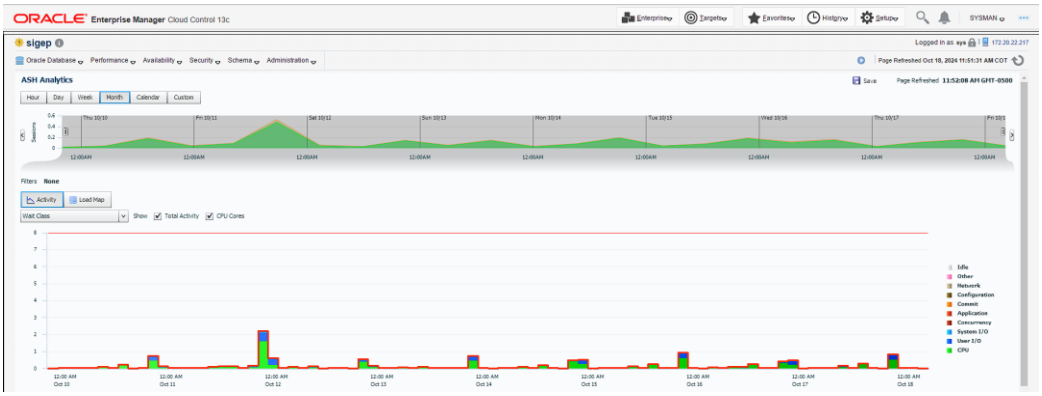


Ilustración 128 Rendimiento DDBB SIGEP

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 129 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 130 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 131 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 132 Estadística Shared Pool

Tamaño base de datos DBSIMPC:

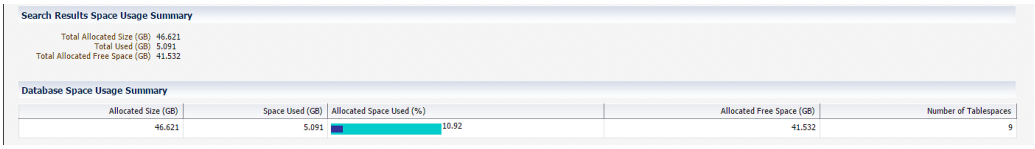


Ilustración 133 Tamaño DDBB SIMPC

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 134 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

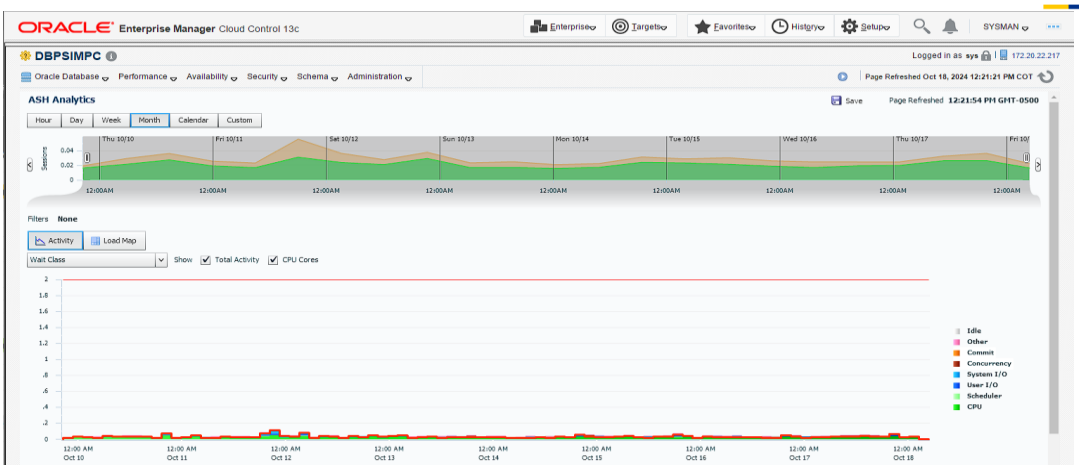


Ilustración 135 Rendimiento DDBB

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 136 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 137 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 138 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 139 Estadística Shared Pool

Tamaño base de datos MINTRASD:

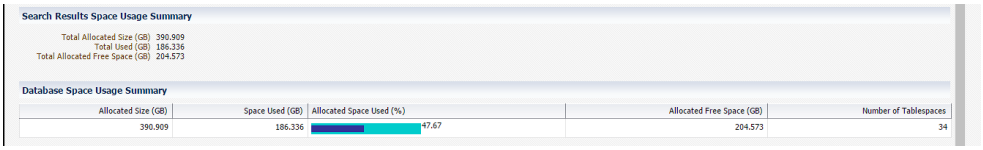


Ilustración 140 Tamaño DDBB MINTRASD

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 141 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

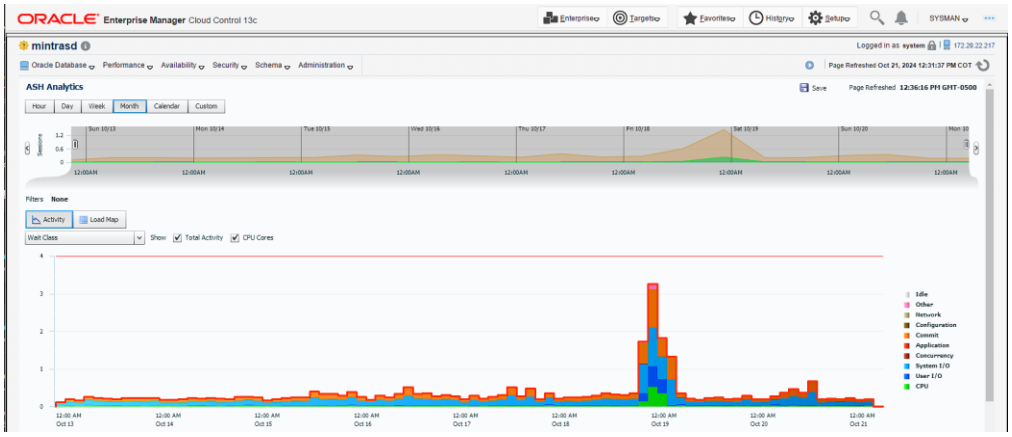


Ilustración 142 Rendimiento MINTRASD

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 143 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 144 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 145 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 146 Estadística Shared Pool

Tamaño base de datos MINTRASD:

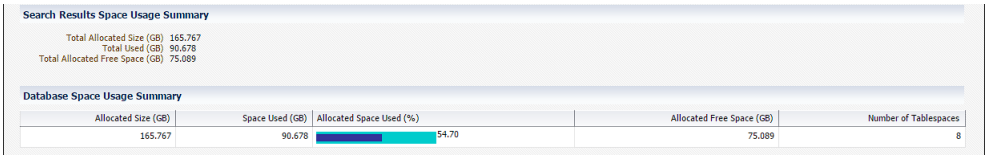


Ilustración 147 Tamaño DDBB

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 148 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

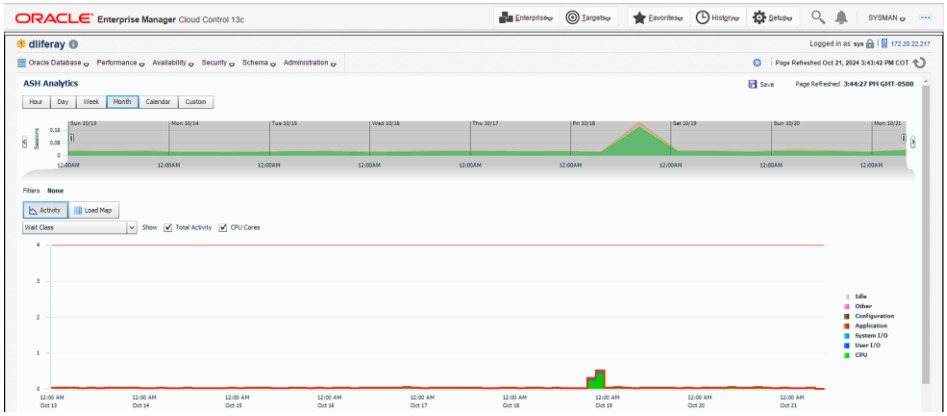


Ilustración 149 Rendimiento DDBB

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 SERVIDOR 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 150 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 151 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 152 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 153 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 154 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 155 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

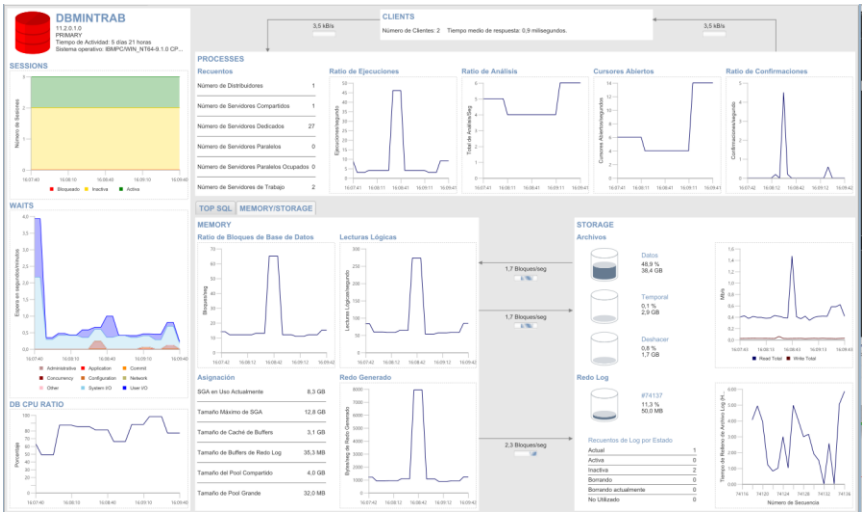


Ilustración 156 Rendimiento DDBB

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 157 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 158 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 159 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 160 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 161 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

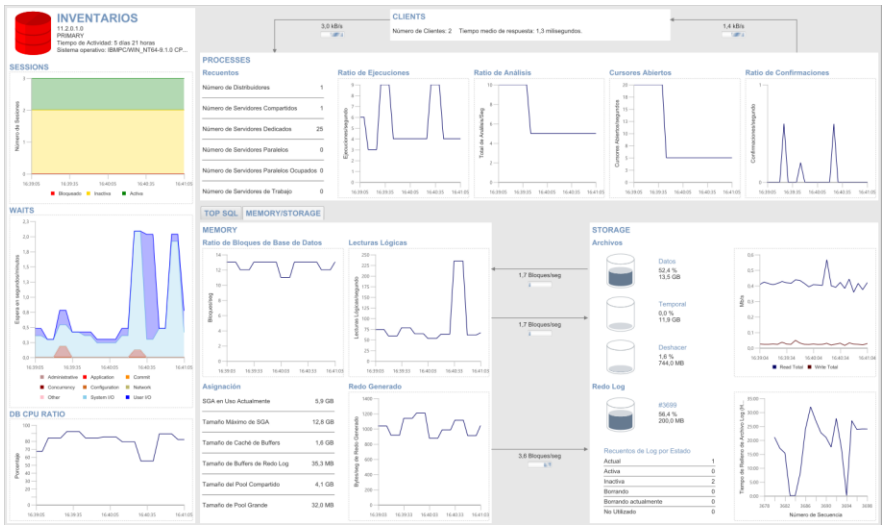


Ilustración 162 Comportamiento DDBB

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 163 Almacenamiento ASM

DISKGROUP DATA:

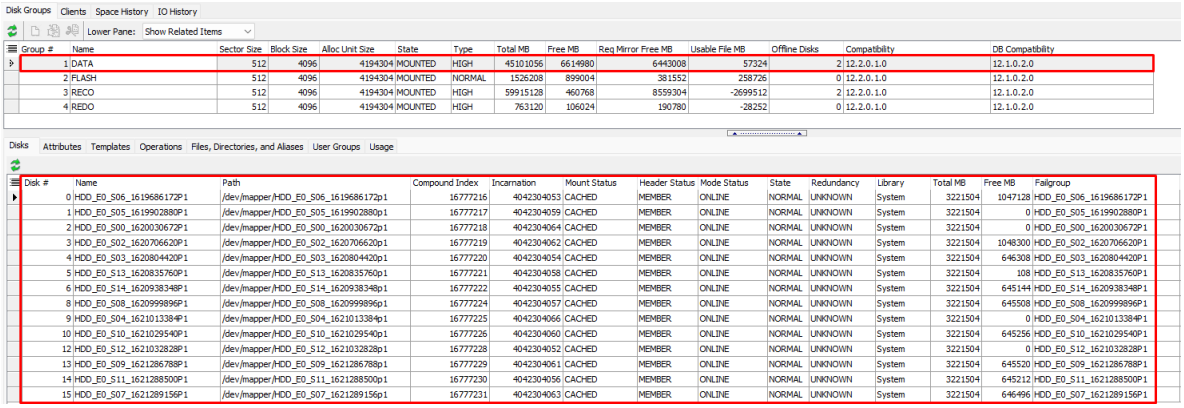


Ilustración 164 DiskGroup Data

DISKGROUP FLASH:

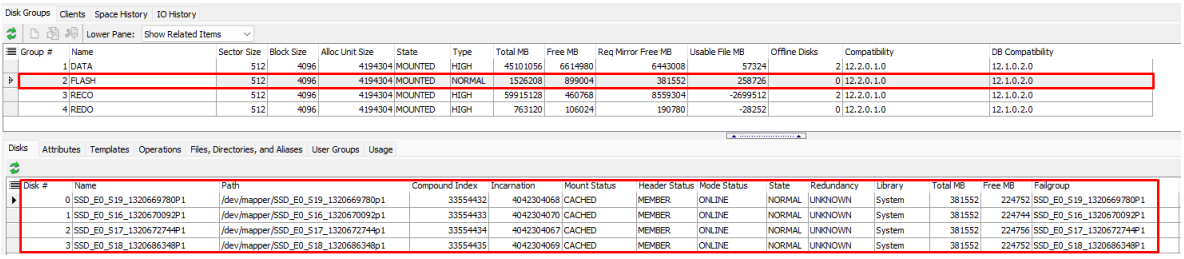


Ilustración 165 DiskGroup Flash

DISKGROUP RECO:

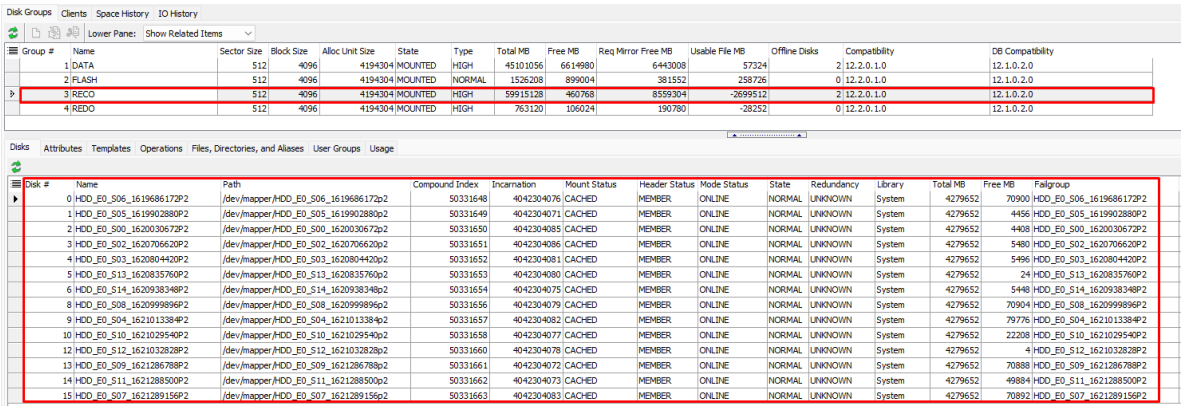


Ilustración 166 DiskGroup Reco

DISKGROUP REDO:

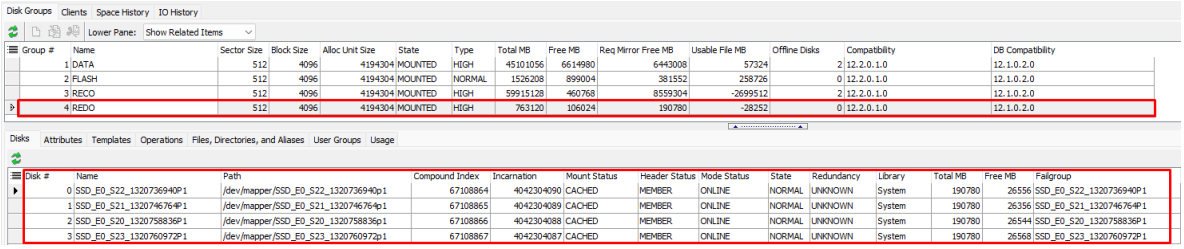


Ilustración 167 DiskGroup Redo

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 a 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 168 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 agosto de 2025, los firewalls de Fortinet mantuvieron un estado óptimo en cuanto a la seguridad perimetral. Se llevó a cabo una supervisión continua de la red para garantizar que solo el tráfico autorizado tenga acceso a los recursos internos. Se implementaron políticas de seguridad sólidas para proteger contra amenazas externas, realizando ajustes según las necesidades específicas del Ministerio de Trabajo.

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

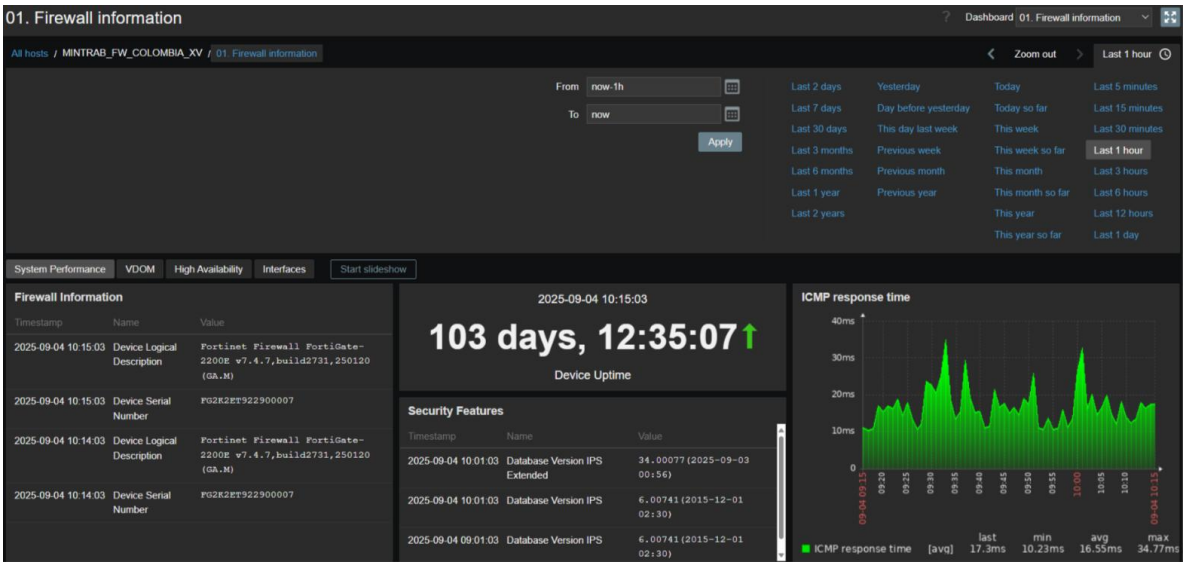


Ilustración*169* Disponibilidad firewall

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 agosto. Este análisis del resumen de ancho de banda proporciona una visión clara de los patrones de uso durante el periodo, permitiendo una mejor gestión y planificación de los recursos de red.

El tráfico recibido se mantuvo entre 5 y 15 TB diarios, con picos de alta demanda los días 5, 7, 19 y 23 de agosto. El tráfico enviado fue mucho menor (0 a 5 TB diarios), en línea con el perfil de consumo de una red institucional. El comportamiento general fue estable y sin anomalías.

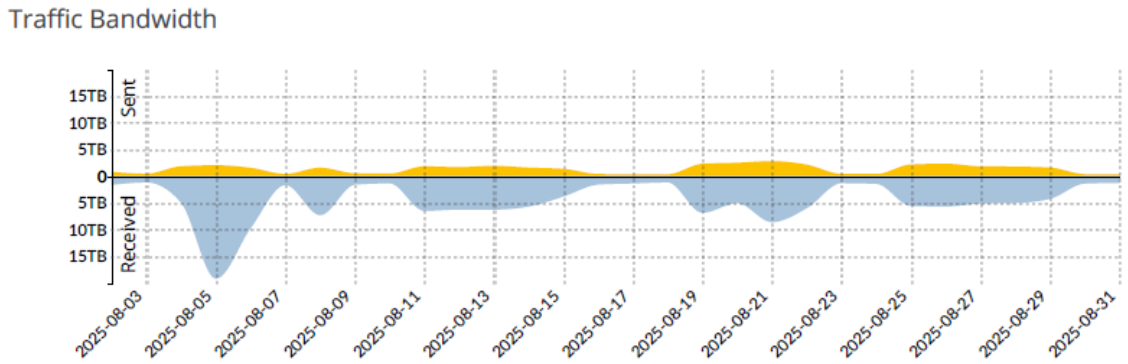


Ilustración*170* Comportamiento ancho de banda

Usuarios con mayor consumo de ancho banda

Esta imagen presenta un análisis del uso del ancho de banda por usuarios e IP's, centrándose en los 10 principales usuarios que generan tráfico en la red durante el período del mes de agosto. La identificación de los 10 principales usuarios de ancho de banda proporciona información valiosa sobre los patrones de uso de la red y los puntos críticos de congestión.

A continuación, se detallan los hallazgos más relevantes:

El análisis evidencia que un único usuario/servidor (172.20.22.251 servidor de backups) concentró más de 21 TB de tráfico, superando ampliamente al resto y generando más del 50% del consumo total. Los siguientes tres usuarios representan juntos cerca del 20%, mientras que el resto mantiene niveles estables y esperados.

Top Users by Bandwidth

#	User(or IP)	Bytes	Sent	Received
1	172.20.22.251			21.67 TB
2	172.28.28.38			6.09 TB
3	mduarteo			5.04 TB
4	172.20.44.102			4.56 TB
5	172.20.22.179			2.61 TB
6	172.16.64.12			2.10 TB
7	172.16.62.31			1.91 TB
8	172.20.44.106			1.20 TB
9	172.25.0.131			1.01 TB
10	172.20.22.32			936.04 GB

Ilustración *171* 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 julio. A continuación, se detallan los hallazgos más relevantes:

Top Users by Sessions

#	User (or IP)	Sessions
1	172.25.0.5	422,927,025
2	172.20.44.119	142,629,397
3	mduarteo	77,582,413
4	172.20.22.234	35,495,907
5	FORTINET	25,706,188
6	172.20.22.40	24,187,425
7	172.20.22.3	19,680,157
8	serviciosGestor	17,539,382
9	172.20.22.32	16,318,193
10	192.168.133.203	13,719,002

Ilustración*172* Top de usuarios

Durante agosto 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	HTTPS			38.28 TB
2	SMB			23.48 TB
3	TCP/902			20.80 TB
4	TCP/445			11.84 TB
5	SYSLOG			7.92 TB
6	TCP/1521			7.38 TB
7	Microsoft.365.Portal			6.77 TB
8	HTTP			6.55 TB
9	Microsoft.SharePoint			4.37 TB
10	Microsoft.Portal			4.31 TB

Ilustración *173* Top tráfico de aplicaciones

Observación	Descripción
Mayor Uso de Ancho de Aplicaciones empresarial	- Microsoft Portal 4.32 GB, indicando alta actividad colaborativa.
	- **Microsoft** SharePoint 4.31 TB, reflejando la importancia de servicios de red seguros y transferencia de archivos seguros y transferencia de archivos.

Tabla 68 Top tráfico de aplicaciones

Categoría de Aplicaciones por Ancho de banda

En agosto, 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:

HTTPS lidera con diferencia, alcanzando 38.28 TB de tráfico, lo que evidencia que la mayoría del consumo está relacionado con navegación web segura y aplicaciones basadas en internet.

Le siguen:

- SMB (23.48 TB): Uso intensivo de recursos compartidos y transferencia de archivos internos.
- TCP/902 (20.80 TB): Posiblemente asociado a servicios de administración remota (ej. VMware o similares).
- TCP/445 (11.84 TB): Tráfico vinculado a servicios de compartición en red (Microsoft Windows).

Aplicaciones misionales y corporativas como Microsoft 365 Portal, SharePoint y Microsoft.Portal también aparecen dentro del top 10, confirmando un alto uso de servicios en la nube.

Protocolos de infraestructura como SYSLOG (7.92 TB) y TCP/1521 (7.38 TB) (Oracle DB) reflejan la relevancia de la administración, registros y bases de datos en la operación institucional.

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 agosto

Authenticated Logins

#	User	Type	First Used	Total Number of Connections	Total Duration Connected(HH:MM:SS)
1	mcarrascal	ssl-tunnel	2025-08-03 15:42:50	139	139:15:03
2	contaccenter	ssl-tunnel	2025-08-04 08:10:54	134	188:00:51
3	yjordan	ssl-tunnel	2025-08-02 00:04:19	109	254:33:21
4	agente4	ssl-tunnel	2025-08-02 12:23:35	85	211:21:17
5	jmaestre	ssl-tunnel	2025-08-03 17:53:59	82	48:48:18
6	agendarl	ssl-tunnel	2025-08-04 09:31:46	77	160:45:35
7	rutraport	ssl-tunnel	2025-08-02 00:06:48	76	77:39:33
8	ablanco	ssl-tunnel	2025-08-03 11:01:31	75	98:24:50
9	rmurcia	ssl-tunnel	2025-08-02 07:08:22	73	93:10:05
10	jcalderonf	ssl-tunnel	2025-08-04 07:11:11	63	67:52:16
11	atobar	ssl-tunnel	2025-08-02 09:55:31	61	70:07:52
12	dfdiazd@noc_indra	ssl-tunnel	2025-08-02 06:56:03	58	421:07:40
13	lgarciam	ssl-tunnel	2025-08-03 04:43:58	55	160:27:15
14	vroman	ssl-tunnel	2025-08-04 08:00:02	55	44:03:46
15	melucumi	ssl-tunnel	2025-08-04 09:02:41	55	46:13:53

Ilustración 174 Top 15 Authenticated Logins by VPN Connections

Usuarios con Uso Frecuente:

Usuarios como contaccenter, mcarrascal, 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	3,290
2	fortinet	ssl-web	365
3	test	ssl-web	255
4	Test	ssl-web	211
5	test	ssl-web	206
6	guest	ssl-web	198
7	support	ssl-web	189
8	scan	ssl-web	189
9	scanner	ssl-web	178
10	User	ssl-web	160

Ilustración *175* 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 agosto de 2025, se generaron 177 eventos analizados, los cuales fueron limpiados de algún tipo de amenazas

Scan Statistics - Last 4 Weeks

Inputs	Pending	Processing	Malicious	High Risk	Medium Risk	Low Risk	Clean	Other	Total
Device	0	0	0	0	0	0	177	0	177
Adapter	0	0	0	0	0	0	0	0	0
On Demand	0	0	0	0	0	0	0	0	0
Network Share	0	0	0	0	0	0	0	0	0
Sniffer	0	0	0	0	0	0	0	0	0
URL	0	0	0	0	0	0	0	0	0
All Sources	0	0	0	0	0	0	177	0	177

Scan Performance - Last 7 Days

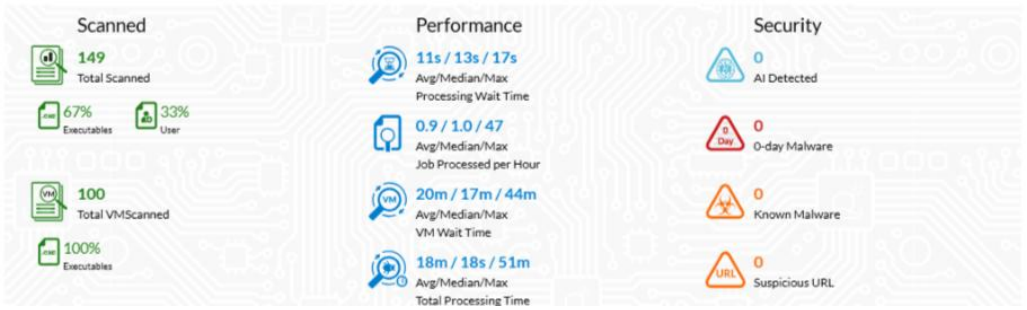


Ilustración 176 estadísticas de escaneo

Este informe de rendimiento proporciona un análisis detallado del comportamiento y la eficiencia de FortiSandbox durante el mes de agosto. Incluye estadísticas sobre la cantidad de archivos analizados, el rendimiento del sistema, la eficiencia en la detección de amenazas y recomendaciones para mejorar el rendimiento y la seguridad.

Performance

System Information

Firmware Version	v4.2.8 build0292 (GA)
Hostname	FSA1-MINTRABAJO
Serial Number	FSA2KET621000075
System Configuration	Last Backup: 2025-03-28 15:01
System Time	2025-09-04 11:00:07 -05
Unit Type	Primary
Uptime	159 day(s) 19 hour(s) 54 minute(s)
Username	eaguayara_css_e

System Resources

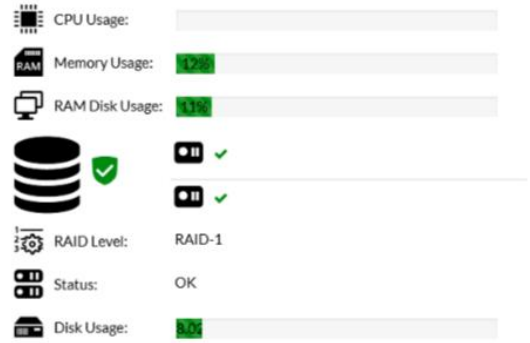


Ilustración *177* performance

Licencia Sandbox

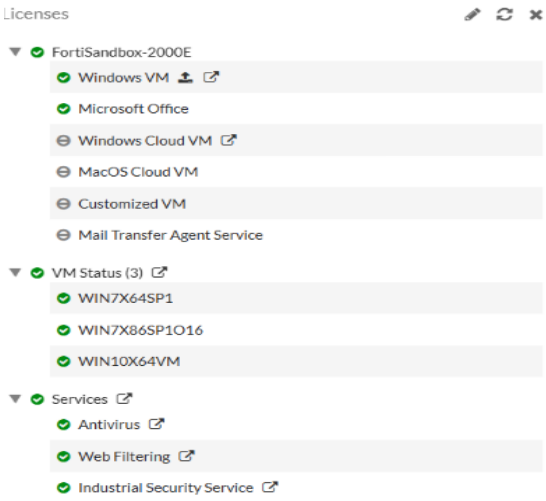


Ilustración *178* Licenciamiento

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:



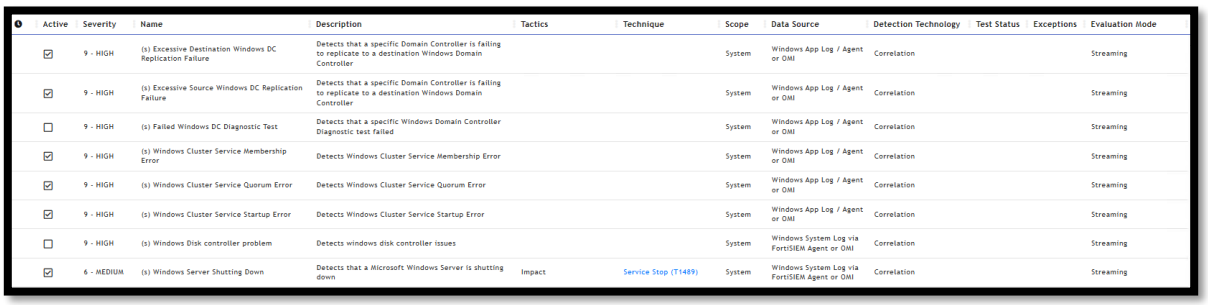
Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☑	8 - MEDIUM	(s) High Process CPU: Server	Detects high CPU usage by a server application on the basis of 3 consecutive measurements in a 15 minute period	Impact	Endpoint Denial 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 *179* 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.



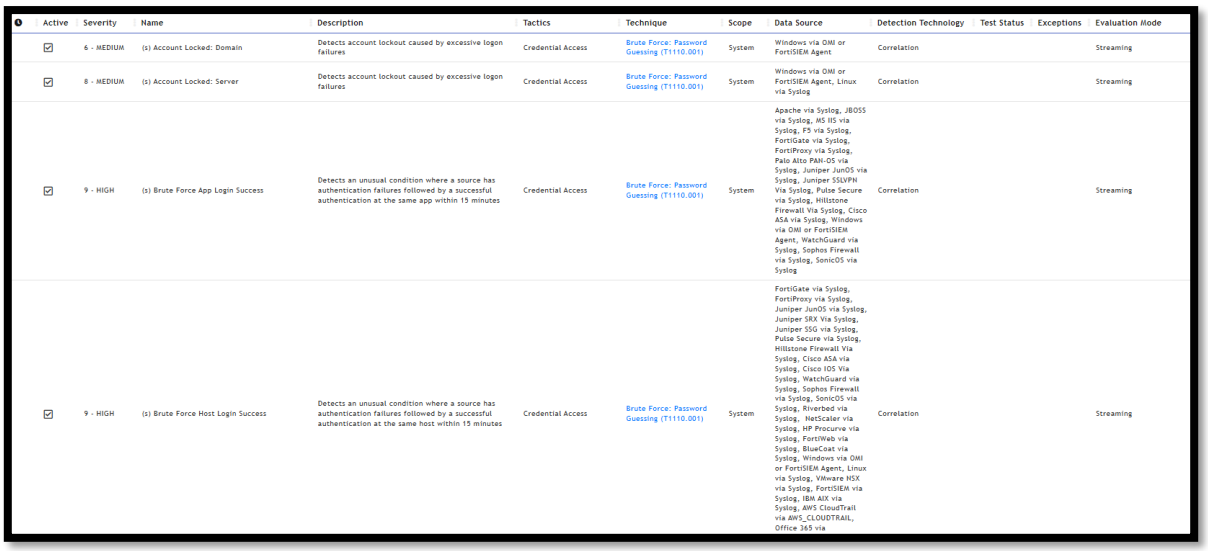
Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☐	4 - LOW	(s) Auto Service Stopped	Detects that an automatically running service stopped. Currently this works for windows servers and is detected via WMI.	Impact	Service Stop (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 *180* 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:

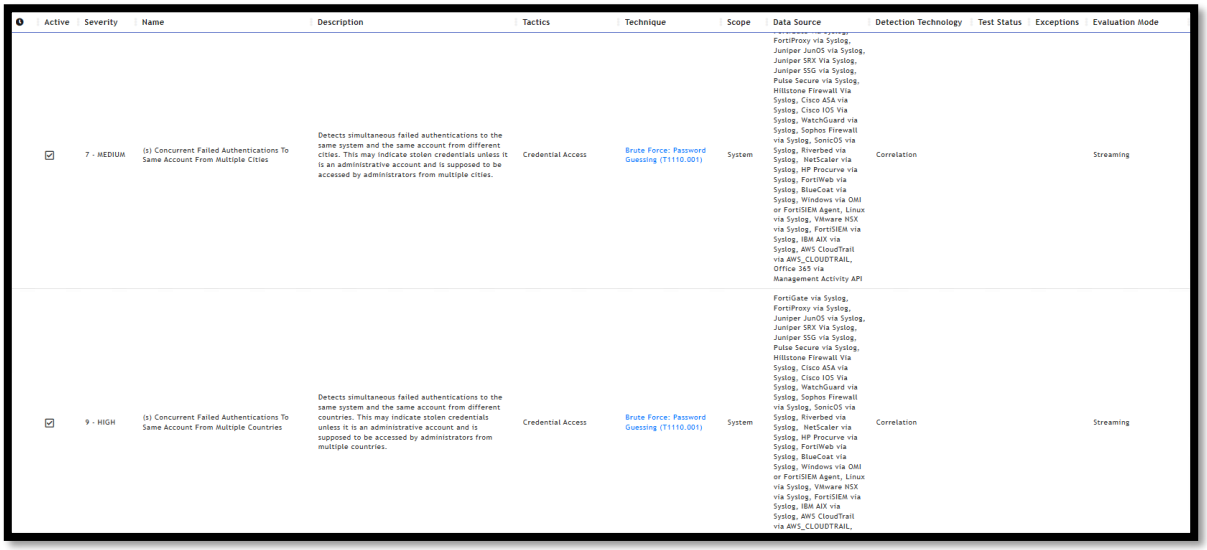
Los casos de uso de seguridad de autenticación en el FortiSIEM se centran en garantizar la integridad y la autenticidad de las credenciales de usuario en todos los dispositivos que tienen instalado el agente. Se muestran los casos Autenticación configurados para el ministerio de trabajo:



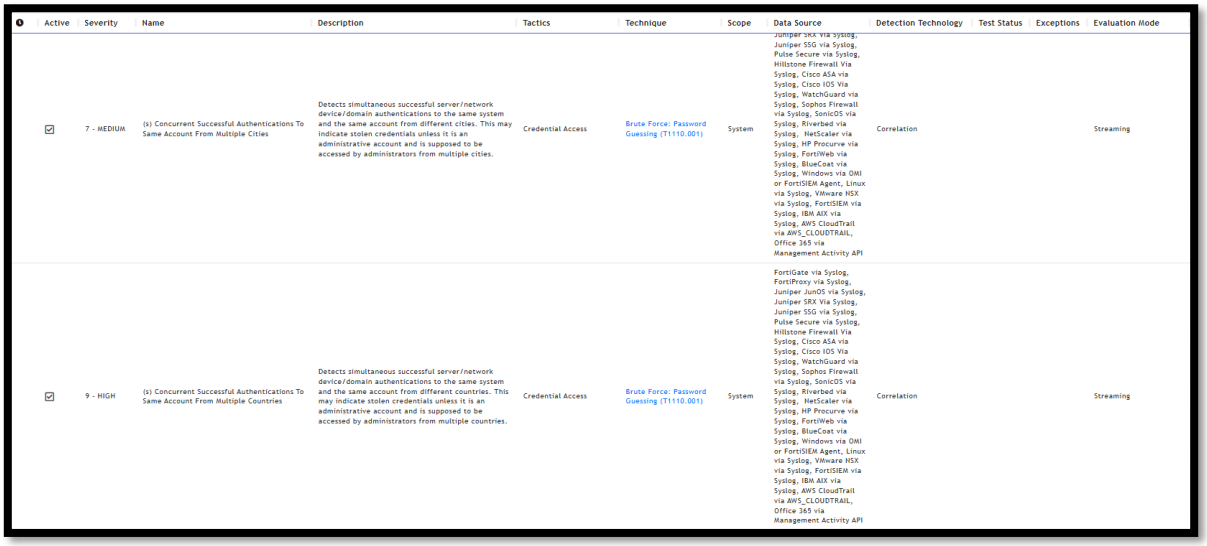
Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☑	6 - MEDIUM	(s) Account Locked: Domain	Detects account lockout caused by excessive logon failures	Credential Access	Brute Force: Password Guessing (T1110.001)	System	Windows 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 NSX 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.

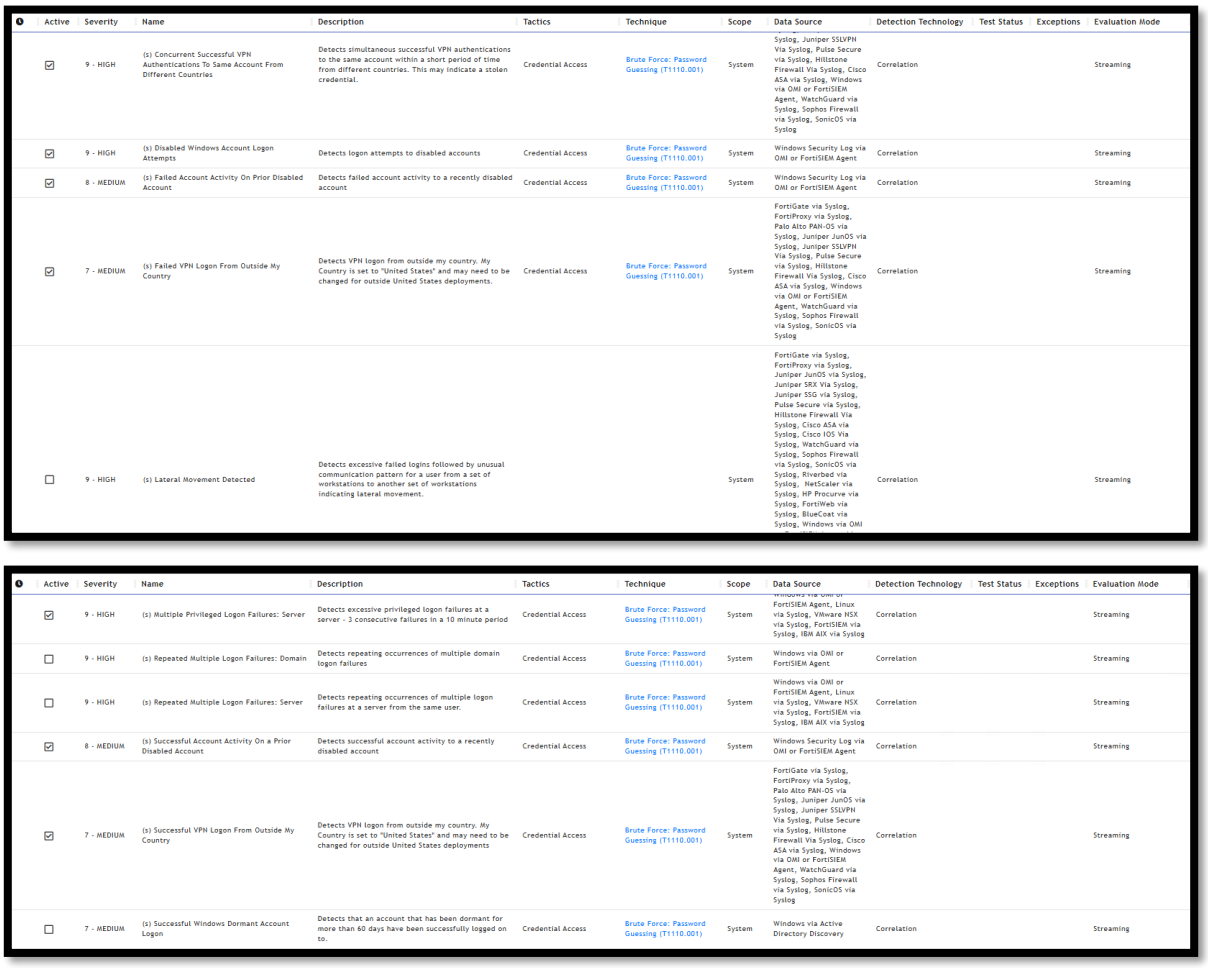
También se reportan bloqueos de cuentas por intentos excesivos de inicio de sesión fallido, lo que puede interrumpir servicios críticos.



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 HSX 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 HSX 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 HSX 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 HSX 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

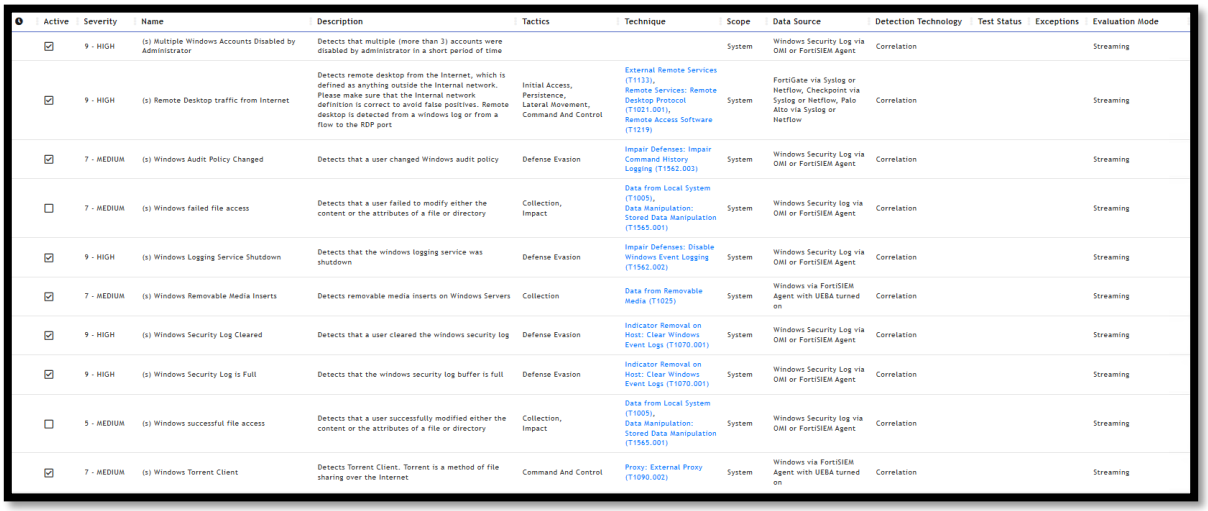
Ilustración *181* Autenticación de seguridad

Acciones tomadas:

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

3.1.6.3.4. Violación de políticas (Policy violation)

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



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

Ilustración *182* Violación de políticas

Acciones realizadas:

- Se validaron actividades de usuarios con privilegios que hayan deshabilitado cuentas o modificado políticas de auditoría con los especialistas de Windows.

- Se monitoreó continuamente la integridad de los registros de eventos, aplicando controles que impidan su alteración mediante los equipos perimetrales.

3.1.6.3.5. Overview incidentes

Durante el mes de agosto, en el FortiSIEM se registraron eventos en la plataforma que podrían representar un evento 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:

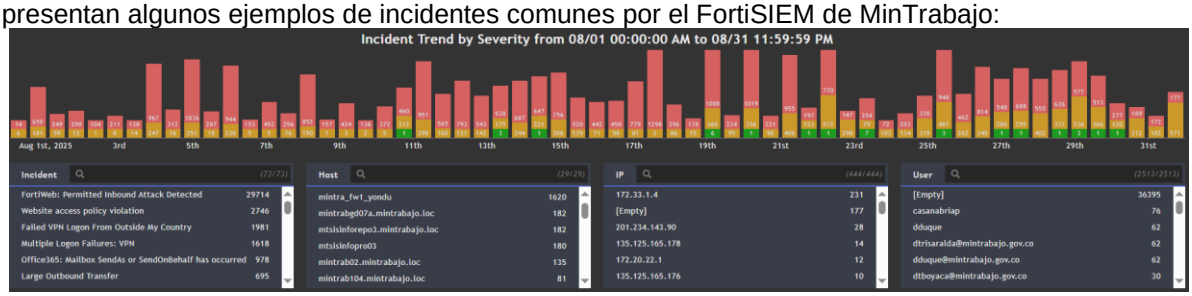


Ilustración *183* eventos detectados por el siem

Análisis de Incidentes – Agosto 2025

Categoría	Detalle	Datos Relevantes	Observaciones / Riesgos
Incidentes más frecuentes	1. *FortiWeb: Inbound Attack Detected* 2. *Website Access Policy Violation* 3. *Failed VPN Logon From Outside Country* 4. *Multiple VPN Login Failures* 5. *Office365 anomalías de correo*	29.714 ataques inbound detectados en FortiWeb 2.746 violaciones de políticas web 19.821 intentos de acceso VPN no autorizados	Alta exposición en aplicaciones web y accesos remotos.
Hosts más afectados	Servidores y equipos críticos con mayor volumen de incidentes	mintra_fwr1_yondu (1.620 eventos) mintrabogota.mintrabajo.loc (182) mtsisinforepo3.mintrabajo.loc	Equipos y servicios institucionales son objetivos recurrentes
IPs asociadas	Direcciones vinculadas a los eventos	Interna: 172.33.1.4 (231 eventos) Externa: 23.201.164.90 (28 eventos)	Posibles intentos de explotación desde IPs externas y anomalías en tráfico interno
Usuarios involucrados	Eventos atribuidos y no atribuidos	36.395 eventos sin usuario asignado Cuentas afectadas: casanabriap, ddoque, otriaralda@mintrabajo.gov.co	Actividad de usuarios administradores del AD

Intrusiones detectadas (FAZ)	Explotación de vulnerabilidades conocidas	Log4j (CVE-2021-44228) Heartbleed (CVE-2014-0160) Linux TCP SACK DoS (CVE-2019-11477) Total: 486 intentos críticos	Evidencia de vulnerabilidades históricas
Accesos VPN	Fallos de autenticación y actividad sospechosa	3.290 intentos fallidos de login VPN Usuarios legítimos con actividad frecuente: dfdiazd@noc_indra, yjordan, cabuitragoo	Eventos de fuerza bruta o *credential* se recomienda reforzar MFA y alertas de acceso anómalo.

Tabla 69 eventos detectados por el SIEM

3.1.6.4.6 Top Disponibilidad de servidores

La imagen proporciona un análisis de los servidores monitoreados por FortiSIEM, destacando los 10 servidores que generaron eventos de disponibilidad en términos de seguridad durante el mes de julio. Ofrece información valiosa sobre los patrones de disponibilidad de servidores en lo relacionado con la última fecha de reinicio. A continuación, se presentan los hallazgos más relevantes:

Los servidores con mayor tiempo de disponibilidad continua en los últimos 30 días sin presentar eventos son:

- MTSISINFO: con aproximadamente 22 días tiempo de actividad.
- mintrab03 y MINTRAB94: con tiempos cercanos a los 45 días.
- MTSISINFOREPO3: con más de 41 días activos sin reinicio.

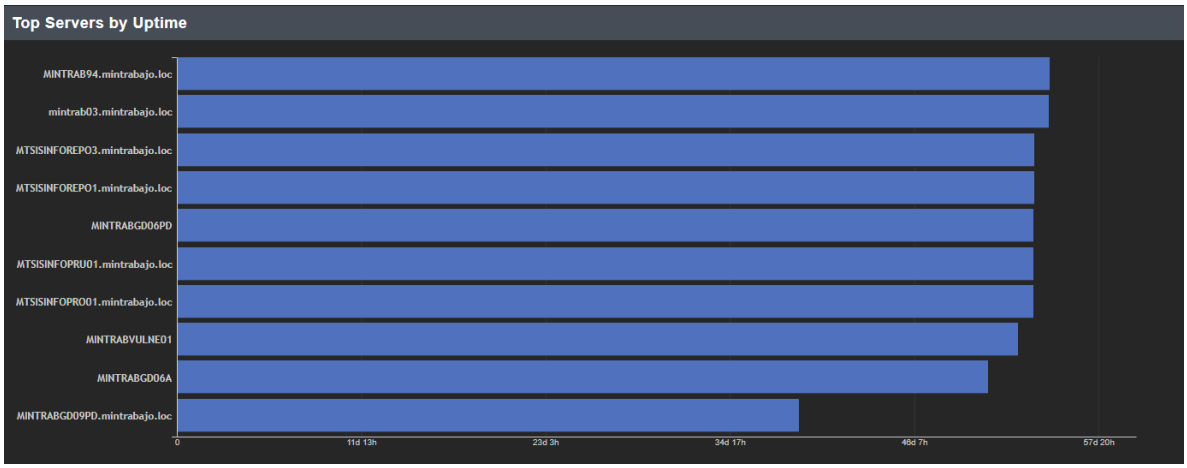


Ilustración 184 Disponibilidad de servidores- Seguridad

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: 280.35 TB
- HTTPS.BROWSER: 55.23 TB

FortiGate: Top Applications by Bandwidth

Application	Category	Total Bandwi...	Sent Bandwi...	SUM(Receive...
SSL	Network.Service	280.35 TB	120.71 TB	159.63 TB
HTTPS.BROWSER	Web.Client	55.23 TB	2.59 TB	52.64 TB
DTLS	Network.Service	51.96 TB	8.29 TB	43.67 TB
NTP	Network.Service	2.04 TB	1.11 TB	949.59 GB
ISAKMP	Network.Service	1.84 TB	367.85 GB	1.48 TB
MediaFire	Storage.Backup	1.76 TB	24 GB	1.73 TB
SSL_TLSv1.3	Network.Service	1.6 TB	67.73 GB	1.54 TB
Google.Services	General.Interest	1.36 TB	305.3 GB	1.07 TB
Amazon.CloudFront	Cloud.IT	1.23 TB	4.57 GB	1.22 TB
QUIC	Network.Service	1.08 TB	69.4 GB	1.01 TB

Ilustración 185 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.

Conclusiones

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

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

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

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

La ilustración representa los tipos de ataques más comunes identificados a través del WAF por fecha en un período que abarca el mes de agosto 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.

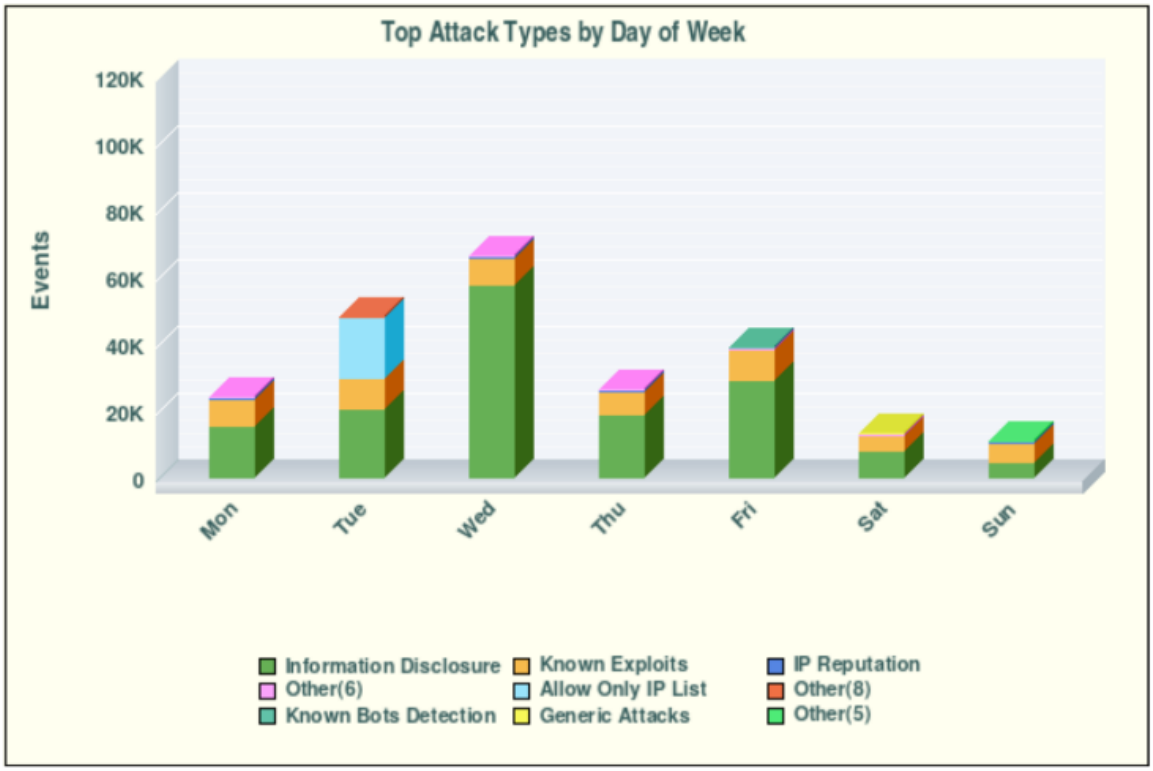


Ilustración 186 Top attack types

Information Disclosure (Divulgación de Información)

Eventos registrados: 18.8885 (80 % 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: 345 (1.4% 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: 135 (3.5% 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 agosto, no se registraron eventos de ataques de denegación de servicio distribuido (DDoS) a las aplicaciones publicadas en internet por el Ministerio de Trabajo.

Top Attacks

Attack	SPP	Direction	Drops	Events
State Anomalies: Foreign packet (Out of State)	Acceso_Web	Inbound	16,927	2
State Anomalies: Outside window	Acceso_Web	Inbound	11,335	4
State Anomalies: Outside window	PAGINA_MINTRABAJO	Inbound	2,651	4
State Anomalies: Foreign packet (Out of State)	PAGINA_MINTRABAJO	Inbound	1,820	2
State Anomalies: Foreign packet (Out of State)	APP_MINT	Inbound	650	3
State Anomalies: Outside window	APP_MINT	Inbound	496	4
SSL/TLS Version Anomaly	Acceso_Web	Inbound	87	2
SSL/TLS Version Anomaly	PAGINA_MINTRABAJO	Inbound	59	2
State Anomalies: Outside window	MOODLE	Inbound	39	2
State Anomalies: Foreign packet (Out of State)	MOODLE	Inbound	17	2

Ilustración 187 Top de ataques

Análisis Detallado:

Acceso_Web concentra el mayor número de paquetes bloqueados (16.927), 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 (11.335), 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 agosto, 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
cmgarcia@css_e	GUI(10.105.116.150)	2025-07-08	10:17:55
cmgarcia@css_e	GUI(10.105.116.150)	2025-07-08	10:16:43
cmgarcia@css_e	GUI(10.105.116.150)	2025-07-08	10:16:01
cmgarcia@css_e	GUI(10.105.116.150)	2025-07-08	10:16:00
cmgarcia@css_e	GUI(10.105.116.150)	2025-07-08	10:15:47
cmgarcia@css_e	GUI(10.105.116.150)	2025-07-08	10:15:45
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

Ilustración 188 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 agosto se registró un solo incidente atendidos dentro del servicios de seguridad informática:

Caso	Fecha de registro	Asunto	Grupo responsable	Categoría
IM-145147	27/08/2025 15:35	RV: ASESOR DE SEGURIDAD	SOC	Análisis de Correos

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
IM-145147	27/08/2025 15:35	RV: ASESOR DE SEGURIDAD	SOC	Análisis de Correos
RF-139316	1/08/2025 18:52	MINT // RF-138540 // Solicitud sobre información para dar respuesta a derecho de petición	SOC	Análisis vulnerabilidades
RF-140167	5/08/2025 17:08	MINTRABAJO // FortiSIEM Alert: TLP:RED - Mintrabajo - Office365: Suspicious File Type Uploaded	SOC	Análisis vulnerabilidades
RF-140302	6/08/2025 9:55	RV: Socialización de la nueva ley laboral y pensional	SOC	Permitir acceso
RF-140314	6/08/2025 10:22	SOLICITUD PERMISOS DE NAVEGACIÓN SECRETARIO GENERAL	SOC	Permitir acceso
RF-141282	12/08/2025 9:38	MINTRABAJO TLP:RED// Boletín Lite // TI - Efimer Trojan: Robo de criptomonedas y compromiso de sitios WordPress.	SOC	Agregar a listas negras
RF-141290	12/08/2025 9:53	Agregar Ip a regla papercut	SOC	Agregar puertos
RF-141379	12/08/2025 11:56	Conectividad de nuevo segmento WAF por VPN	SOC	Agregar puertos
RF-141743	13/08/2025 15:00	Solicitud de revision de access log hacia el portal web MinTrabajo	SOC	Reportes Seguridad Informática
RF-141981	14/08/2025 11:47	RV: Solicitud activación para consultar YouTube	SOC	Permitir acceso
RF-141995	14/08/2025 13:20	RV: Notificación Urgente: Proceso Penal Notificado - Juzgado 01, Chachagüí	SOC	Correo Malicioso (Phishing, Smishing, whaling, otros)
RF-142018	14/08/2025 14:55	CTI // Boletín Lite // TI - CVE-2025-25256: Grave vulnerabilidad en FortiSIEM permite ejecución remota no autenticada.	SOC	Seguridad Informática
RF-142108	14/08/2025 19:44	Alerta - Plataforma Fortinet SSL	SOC	Restringir servicio
RF-142109	14/08/2025 21:59	MINT // RF-142018 // Alerta - Plataforma Fortinet SSL	SOC	Restringir servicio
RF-142141	15/08/2025 8:36	Modificar ruta Magangué	SOC	Modificacion VPN
RF-142166	15/08/2025 9:29	RV: Plataforma Fortinet SSL	SOC	Accesos por fuerza bruta
RF-142171	15/08/2025 9:42	Boletín Lite // TI - Alerta preventiva - Posible campaña de fuerza bruta contra Fortinet SSL VPN	SOC	Modificacion VPN
RF-142280	15/08/2025 14:42	RV: Demanda formal por daños y perjuicios graves	SOC	Análisis de Correos

RF-142316	15/08/2025 16:12	Solicitud uso de YouTube	SOC	Permitir acceso
RF-142349	15/08/2025 16:59	RV: Solicitud uso de YouTube	SOC	Permitir acceso
RF-142353	15/08/2025 17:16	MINT // Conectividad de nuevo segmento WAF por VPN	SOC	Crear politica
RF-142354	15/08/2025 17:16	MINT // Regla TCP VR VMware	SOC	Crear politica
RF-142485	19/08/2025 7:59	RV: CASO LEGAL ACTIVO - Juzgado 07 Penal Municipal - Ibagué - Tolima	SOC	Correo Malicioso (Phishing, Smishing, whaling, otros)
RF-142519	19/08/2025 8:33	PERMISOS DE NAVEGACIÓN	SOC	Agregar a sitios permitidos
RF-142777	19/08/2025 16:58	Solicitud verificación correo sospechoso.	SOC	Análisis de Correos
RF-142798	20/08/2025 3:00	FortiSIEM Alert: TLP:RED - Mintrabajo - Possible Brute Force Alert Windows	SOC	Accesos por fuerza bruta
RF-143590	22/08/2025 7:05	RV: Consulta de acceso a RUTEC	SOC	Permitir acceso
RF-143613	22/08/2025 8:06	MINTRABAJO LTP:RED // Boletín // TI - Plague Linux Backdoor: Riesgo crítico para autenticación en sistemas Linux.	SOC	Restringir servicio
RF-143614	22/08/2025 8:11	MINTRABAJO TLP:RED // Boletín // TI - Ransomware “Blue Locker” dirigido contra el sector energético y gobierno de Pakistán.	SOC	Reportes Seguridad Informática
RF-143621	22/08/2025 8:18	RE: MINTRABAJO TLP:RED // Boletín // TI - Ransomware “Blue Locker” dirigido contra el sector energético y gobierno de Pakistán.	SOC	Incidente por Malware
RF-143626	22/08/2025 8:28	RE: MINTRABAJO LTP:RED // Boletín // TI - Plague Linux Backdoor: Riesgo crítico para autenticación en sistemas Linux.	SOC	Análisis de evento
RF-144471	26/08/2025 6:31	Acceso You Tube	SOC	Asesoria - Consulta
RF-144494	26/08/2025 8:09	Análisis correo sospechoso	SOC	Correo Malicioso (Phishing, Smishing, whaling, otros)
RF-144504	26/08/2025 8:21	MINTRABAJO TLP:RED// Boletín Lite // TI - Shamos; el nuevo malware que engaña a usuarios de macOS con reparaciones falsas.	SOC	Reportes Seguridad Informática
RF-144512	26/08/2025 8:34	MINTRABAJO TLP:RED // Boletín // TI - Nueva amenaza Linux; malware VShell se instala a través de nombres de archivo maliciosos en archivos RAR.	SOC	Permitir acceso
RF-144933	27/08/2025 8:10	MINTRABAJO LTP:RED // Boletín // TI - WarLock ransomware: ataque contra Colt Telecom deja servicios críticos fuera de línea y datos a la venta.	SOC	Restringir servicio
RF-145006	27/08/2025 10:51	RE: DU7DB4 ********** RAMA JUDICIAL DEL PODER PÚBLICO ********** NOTIFICACIÓN ELECTRÓNCIA ********** DU2839D	SOC	Revisar correo malicioso

Tabla 70 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 agosto:

- **Ejecución de archivos maliciosos**

Riesgo	Impacto	Probabilidad
Archivos ejecutables comunes pueden ser utilizados para distribuir malware, ransomware o puertas traseras.	Compromiso de la integridad, confidencialidad y disponibilidad de los sistemas	Alta, debido al uso frecuente de estos archivos y la falta de controles estrictos.

Tabla71 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.

Tabla72 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 73 Ataque de Phishing dirigidos

3. Medidas de Mitigación Recomendadas

Control y restricción de archivos ejecutables:

- Se realizó plan de trabajo para Implementar restricciones de ejecución de ejecutables en servidores y estaciones de trabajo.
- Se realizó unas listas blancas de software permitido.
- Monitoreo y análisis continuo de archivos sospechosos.

Gestión de vulnerabilidades:

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

Prevención y respuesta ante phishing:

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

3.1.6.8 Políticas y procedimiento de seguridad

Dentro las activades realizadas en el mes de agosto, 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.

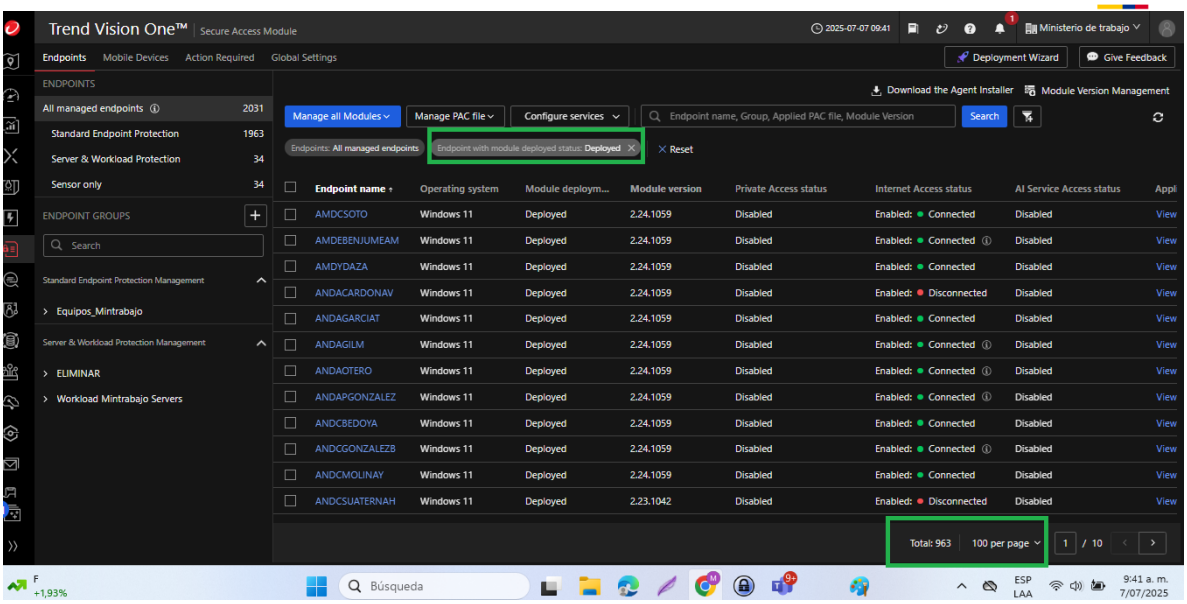


Ilustración 189 Políticas y procedimiento de seguridad

Esta cronología muestra que se compartieron boletines de forma proactiva y continua, cubriendo malware, vulnerabilidades críticas y alertas preventivas, lo que permitió anticipar riesgos y fortalecer la ciberseguridad institucional.

12/08/2025 – MINTRABAJO
Boletín Lite // TI – Efimer Trojan
Riesgo: Robo de criptomonedas y compromiso de sitios WordPress.

14/08/2025 – MINTRABAJO
Boletín Lite // TI – CVE-2025-25256
Vulnerabilidad crítica en FortiSIEM, permite ejecución remota no autenticada.

15/08/2025 – MINTRABAJO
Boletín Lite // TI – Alerta preventiva
Posible campaña de fuerza bruta contra Fortinet SSL VPN.

22/08/2025 – MINTRABAJO
Boletín // TI – Plague Linux Backdoor
Riesgo crítico para autenticación en sistemas Linux.

22/08/2025 – MINTRABAJO
Boletín // TI – Ransomware “Blue Locker”
Ataques dirigidos contra el sector energético y gobierno de Pakistán.

26/08/2025 – Mintr
Boletín Lite // TI – Shamos Malware
Nuevo malware que engaña a usuarios de macOS con reparaciones falsas.

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 01/08/2025 hasta el 31/07/2026	Vigente	**LIFERAY**

Tabla 74 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.

En proceso de actualización CI de los servicios de Serivioc Centrales

- 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	99,99%	99.95%
DC-3	Continuidad y disponibilidad del datacenter alterno	100,00%	99,60%
DC-4	Continuidad y disponibilidad de la plataforma de procesamiento, almacenamiento y respaldo	100,00%	99,70%

ID	Indicadores	Resultado	Meta
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	99,99%	99,90%
DC-9	Tiempo de solución de incidentes asociado a los servicios de administración, soporte y monitoreo	97,24%	90,00%
DC-10	Tiempo de solución de requerimientos asociado a los servicios de administración, soporte y monitoreo	99,86%	90,00%
DC-11	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 75 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 76 Medición ANS Nube Pública

3.2. No aplica

3.3. Conectividad WAN, SDWAN e Internet

3.3.1. Canales WAN

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

Se observa en la grafica de consumo, que el trafico fue estable durante el mes de agosto, no se observan caídas del canal.

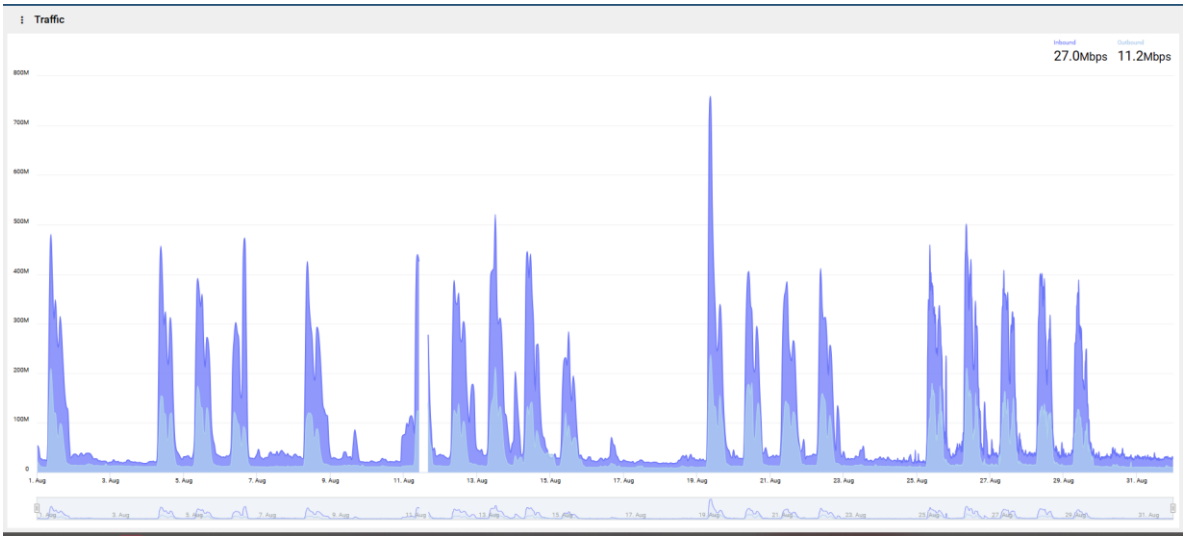


Ilustración 190. Grafica de consumo canal MPLS Datacenter

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

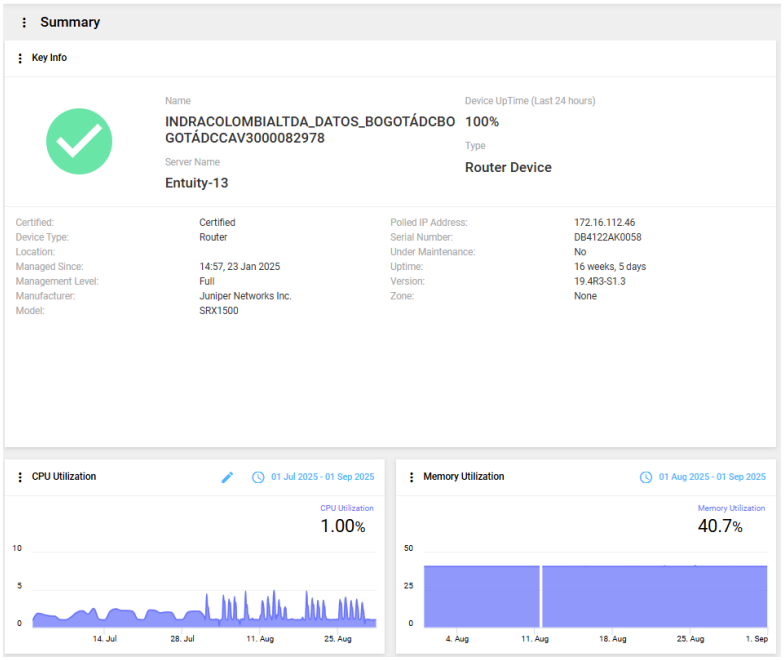


Ilustración 191 Uptime del equipo MPLS Datacenter

3.3.1.1. Incidentes de Conectividad

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

Dirección territorial	Disponibilidad	Caso Asociado
Sede Territorial Quibdó	97,21%	IM-140866
Sede Territorial Apartado, Antioquia	99,77%	IM-139386
Sede Territorial Barranquilla	99,89%	IM-145884
Sede Territorial Bogotá	96,23%	IM-142716
Sede Territorial Cartagena	97,22%	IM-140864
Sede Territorial Riohacha	99,76%	IM-143945
Sede Territorial Cúcuta	99,76%	IM-143945
Cisneros	97,81%	IM-144497
Magangué	81,88%	IM-140832
Soata	100,00%	IM-145946
El Doncello	97,66%	IM-140898
El Bordo Patía	94,42%	IM-140861
El Copey	99,51%	IM-143945
Caldas	93,75%	IM-144567
Istmina	93,43%	IM-144422
Lorica	99,56%	IM-145897
Montelíbano	99,51%	IM-143945
Fonseca	99,51%	IM-143945
Ciénaga	99,35%	IM-145884
Fundación	99,51%	IM-143945
Granada	99,05%	IM-142841
Los Patios	94,42%	IM-140863
Barbosa	94,34%	IM-140865
Puerto Wilches	94,42%	IM-140862
Espinal	98,77%	IM-144054

Tabla 77 Novedades servicio de internet

3.3.1.2. Topología Actual

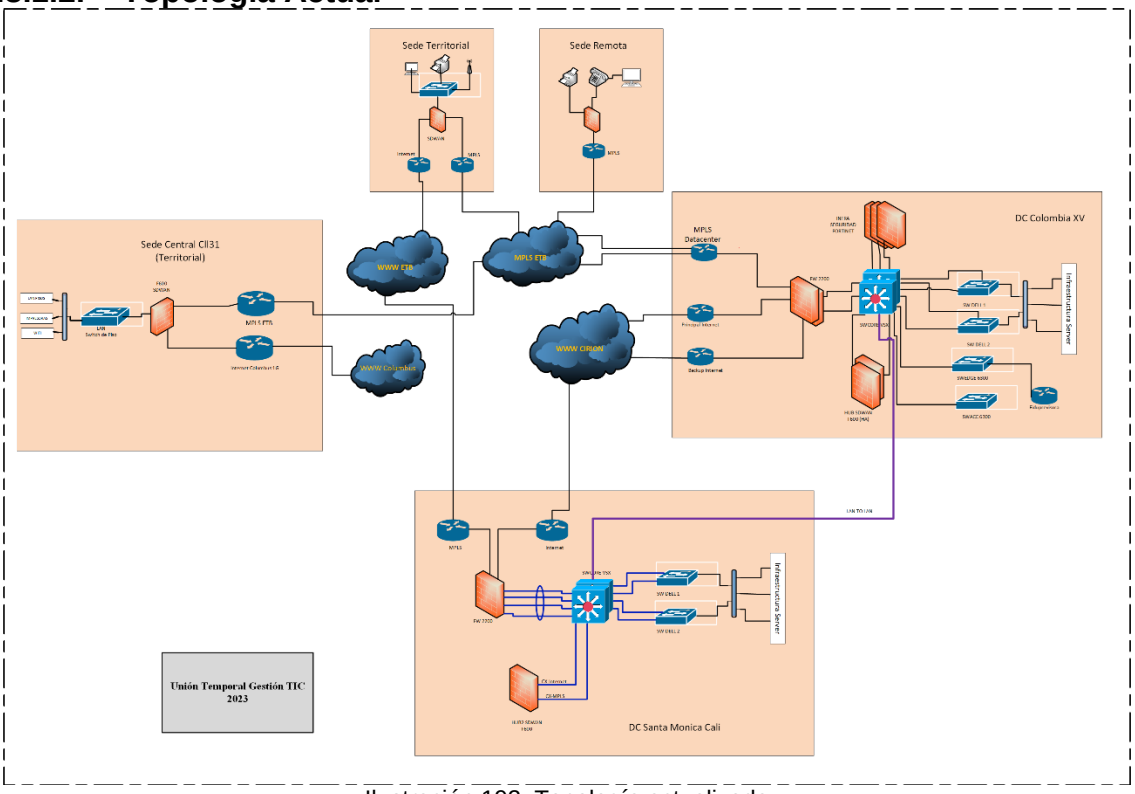


Ilustración 192. Topología actualizada

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.

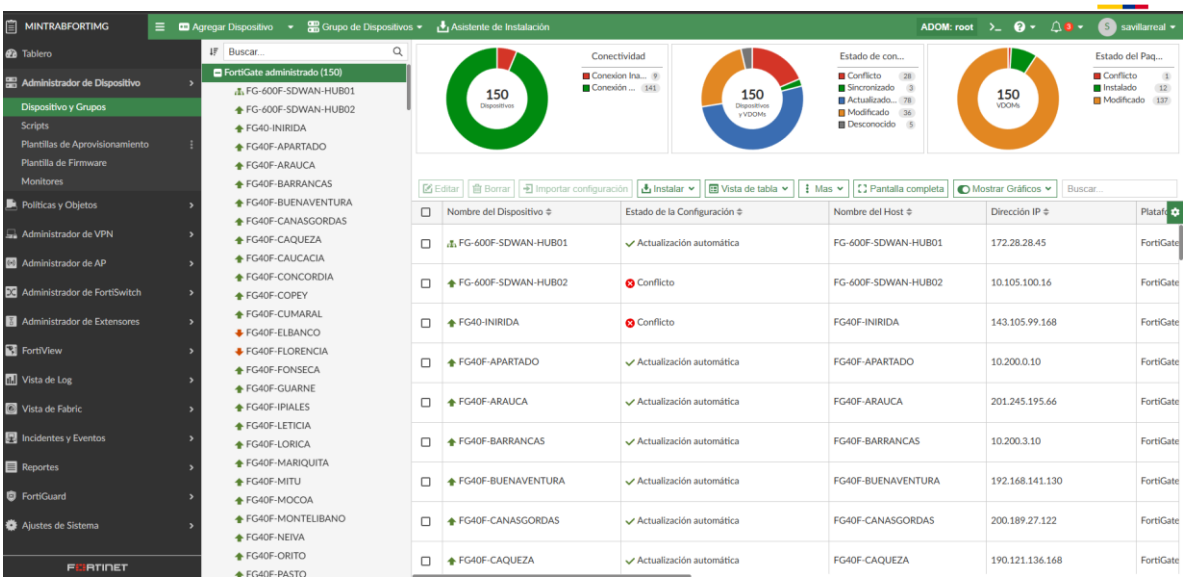


Ilustración 193. Interface Fortimanager

Desde el HUB SDWAN F600, en datacenter se observa el consumo promedio del canal MPLS, donde no se presenta saturación. Se observa que se tuvo un promedio de 181 Mbps de consumo con un máximo de 1.25 Gbps, este canal es de 2GB, con el tráfico generado se observa que no presentó saturación durante el mes.

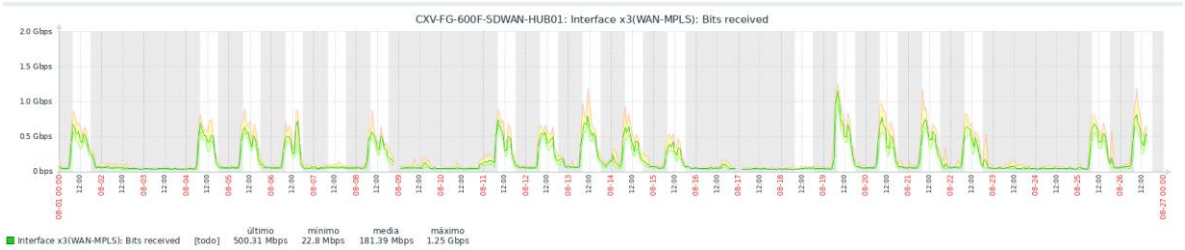


Ilustración 194. Interface MPLS HUB SDWAN

De igual forma, la interface de Internet del HUB no presenta saturación, por esta interface se establece el túnel Backup de las sedes territoriales. Se observa que se tuvo un promedio de 49.67Mbps de consumo en el mes donde se tuvo un máximo de 536 Mbps. Este canal es de 1GB, con el trafico generado en el mes, no se presentó saturación.

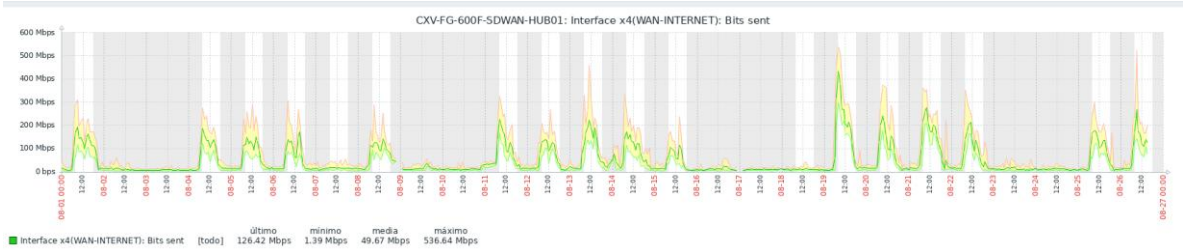


Ilustración 195 Interface Internet HUB SDWAN

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

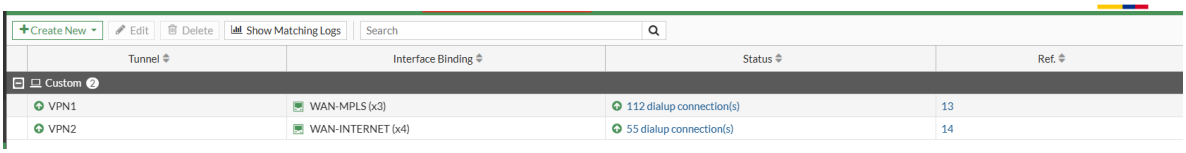


Ilustración 196. VPN SDWAN establecidas

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.

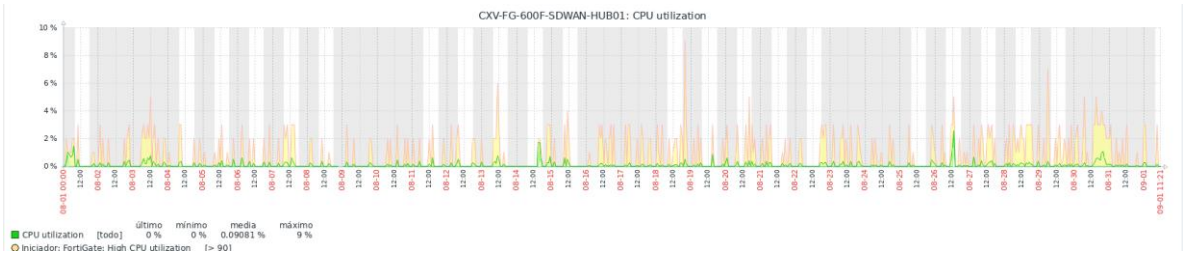


Ilustración 197. Estado HUB SDWAN Datacenter

Se verifica el estado del HA del equipo, donde se observa que se encuentra establecido y sincronizado, no se observan cambios en los roles entre los dos equipos, es decir no se ha presentado afectación sobre el equipo principal.

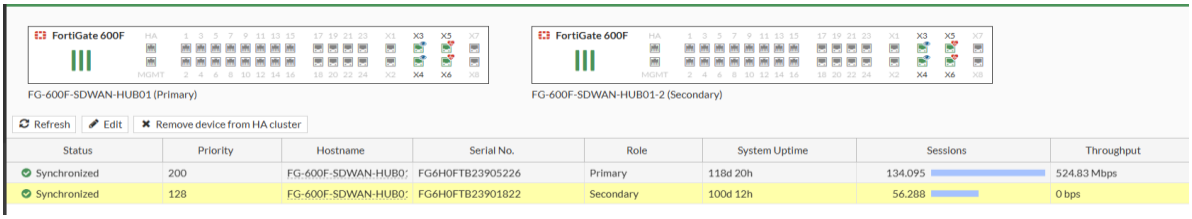


Ilustración 198. Estado HA HUB Sdwan

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

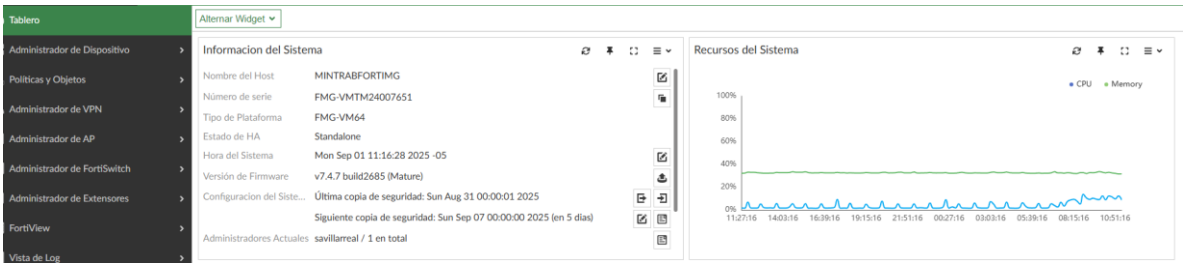


Ilustración 199. Recursos Fortimanager

- **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%

ID	Indicadores	Resultado	Meta
CWI-3	Continuidad y disponibilidad del servicio de WAN en sedes nacionales con doble enlace (principal MPLS + secundario Internet dedicado)	(*)	99,90%
CWI-4	Continuidad y disponibilidad del servicio de internet en Datacenter principal	100,00%	99,95%
CWI-5	Continuidad y disponibilidad del servicio de internet en Datacenter alterno	100,00%	99,70%
CWI-6	Continuidad y disponibilidad del servicio de WAN en Datacenter principal	100,00%	99,95%
CWI-7	Continuidad y disponibilidad del servicio de WAN en Datacenter alterno	100,00%	99,95%
CWI-8	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 78 Medición de ANS Conectividad WAN e Internet

(*) De acuerdo con la solicitud de la Coordinador del Grupo de Soporte Informático los valores de la continuidad y disponibilidad se encuentran desagregados en el archivo ANS Internet – MPLS y a continuación, se indica el detalle del mes de agosto:

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

Dirección territorial	Disponibilidad de Sede	Caso Asociado	% Penalidad	Valor Penalidad un enlace
Cisneros	97,81%	IM-144497	3%	$ 9.240
Magangue	81,88%	IM-140832	20%	$ 61.603
Soata	100,00%	IM-145946	10%	$ 30.801
El Doncello	97,66%	IM-140898	3%	$ 5.544
El Bordo Patia	94,42%	IM-140861	10%	$ 30.801
El Copey	99,51%	IM-143945	3%	$ 9.240
Caldas	93,75%	IM-144567	10%	$ 18.481
Istmina	93,43%	IM-144422	10%	$ 30.801
Lorica	99,56%	IM-145897	3%	$ 9.240
Montelíbano	99,51%	IM-143945	3%	$ 9.240
Fonseca	99,51%	IM-143945	3%	$ 9.240
Cienaga	99,35%	IM-145884	3%	$ 9.240
Fundacion	99,51%	IM-143945	3%	$ 9.240
Granada	99,05%	IM-142841	3%	$ 9.240
Los Patios	94,42%	IM-140863	10%	$ 30.801
Barbosa	94,34%	IM-140865	10%	$ 30.801
Puerto Wilches	94,42%	IM-140862	10%	$ 30.801
Espinal	98,77%	IM-144054	3%	$ 9.240
TOTAL				**$ 353.594**

Tabla 79 Desagregado sedes con novedad un solo enlace

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

Dirección territorial	Disponibilidad de Sede	Caso Asociado	% Penalidad	Valor Penalidad un enlace
Sede Territorial Quibdo	97,21%	IM-140866	3%	$ 36.567
Sede Territorial Apartado, Antioquia	99,77%	IM-139386	3%	$ 24.378
Sede Territorial Barranquilla	99,89%	IM-145884	3%	$ 60.946
Sede Territorial Bogotá	96,23%	IM-142716	3%	$ 121.891
Sede Territorial Cartagena	97,22%	IM-140864	3%	$ 36.567
Sede Territorial Riohacha	99,76%	IM-143945	3%	$ 36.567
Sede Territorial Cúcuta	99,76%	IM-143945	3%	$ 48.757
TOTAL				**$ 365.673**

Tabla 80 Desagregado sedes con novedad con doble enlace

4. LINEA DE SERVICIOS EN SEDE

4.1. Equipos de Cómputo de usuario final

Durante el periodo del informe, fueron atendidas 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 81 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 AGOSTO		
SEDE	**TIPO DE ELEMENTO**	**CANTIDAD**
DT Valle del Cauca	Portátil	2
DT Cesar	Portátil	1
DT Vaupés	Portátil	1
DT Cundinamarca	Escritorio	1
DT Caldas	Escritorio	2
DT Antioquia	Escritorio	1
OE Barrancabermeja	Portátil	1
DT Nariño	Escritorio	1
DT Risaralda	Escritorio	1
Nivel Central	Escritorio	9
Nivel Central	Portátil	6
DT Guajira	Escritorio	1

Tabla 82 Cantidades de equipos asignados nivel nacional

DEVOLUCION DE EQUIPOS AGOSTO		
SEDE	**TIPO DE ELEMENTO**	**CANTIDAD**
Puerto Boyacá	Escritorio	1
Nivel Central	Portátil	10
DT Valle del Cauca	Escritorio	1

Tabla 83 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 agosto, se reportó un total de 19 casos de garantía a corte del periodo. A continuación, se detallan los estados asociados a estos casos:

Estado de caso	Cantidad
Cerrado	13
Suspendido	6
Total	**19**

Tabla 84 Estado de casos de garantía.

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

ANS	Cerrado	Suspendido	Total
CUMPLE	13	6	19
Total	13	6	19

Tabla 85 ANS casos de garantía.

Fecha de Reporte	Serial	Parte	Falla	Sede	No. Caso	Estado
1/08/2025	HC3BBKWA	Diadema	No reproduce audio	Nivel Central	RF-139149	Cerrado
6/08/2025	HC3BEHCD	Diadema	Se escucha distorsionado	Nivel Central	RF-140238	Cerrado
6/08/2025	3B8112N	Cargador	No emite carga	Nivel Central	RF-140346	Cerrado
11/08/2025	MJ0LS5GB	PC	Equipo no enciende	San José del Guaviare	RF-141003	Suspendido
11/08/2025	PW0A3ATR	Portátil	No cargan las baterías a pesar de tener el cargador	cesar/Valledupar	RF-141048	Cerrado
11/08/2025	PW09Z36J	Portátil	Puerto de carga no funciona	Nivel central	RF-141101	Suspendido
12/08/2025	HC3BBLZA	Diadema	Mal funcionamiento	Medellín	RF-141303	Cerrado
12/08/2025	VNAA64GB	Monitor	Falla en monitor con líneas horizontales y distorsionada.	Manizales/Caldas	RF-141405	Cerrado
13/08/2025	HC3BBLNA	Diadema	falla en el parlante izquierdo	Medellín	RF-141705	Cerrado
14/08/2025	PW0A3BFT	Portátil	Falla en puerto de carga	Nivel Central	RF-141906	Suspendido
19/08/2025	PW09Z34M	Portátil	Equipos se reinicia solo	Nivel Central	RF-142490	Suspendido
19/08/2025	HC3BBMPE	Diadema	Se escucha distorsionado	Nivel central	RF-142491	Cerrado
19/08/2025	HC3BBN83	Diadema	Parlantes de los auriculares se escuchan como si fuera un eco a lo lejos e interferencia	Nivel central	RF-142611	Cerrado
20/08/2025	VNAA63G9	Monitor	presenta una línea verde horizontal permanente en la pantalla	Buenaventura	RF-142935	Suspendido
21/08/2025	HC3BBMLP	Diadema	Audio se escucha distorsionado y de mala calidad.	Nivel central	RF-143454	Cerrado
22/08/2025	VNAA626D	Monitor	presenta líneas blancas horizontales en la parte inferior del desplaye dificultando la visualización	Barranquilla	RF-143695	Suspendido
22/08/2025	HC3BBMXA	Diadema	No se escucha	Nivel Central	RF-143772	Cerrado
22/08/2025	HC3BBMD2	Diadema	No se escucha	Nivel Central	RF-143867	Cerrado
28/08/2025	HC3BBM3X	Diadema	No se escucha	Territorial Vta.	RF-145302	Cerrado

Tabla 86 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:

SINIESTROS O POR DAÑO DE USUARIO					
Funcionario	**Equipo**	**DT**	**Parte afectada**	**ESTADO**	**Caso Aseguradora/Lenovo**
Alcides Manuel Morales Ortega	MJ0LS5XL	Sincelejo/San Marcos	Se apaga y no enciende	Reportada ante la aseguradora	PRG_2025_1921454
Jesús Manuel Martinez Franco	PW0A3BEY	Montería	Golpes en esquinas	Se realiza visita y no cubre garantía por daño inducido	2025347408
Ana Mireya Escobar Tierradentro	MJ0S5TW	Popayán/Cauca	No enciende	Reportada ante aseguradora	PRG_2025_1766918
Pavel Santo Domingo	PW0A3CDZ	Nivel central	Derrame de líquidos	Reportado ante aseguradora	PRG_2025_3256134
Bernardo Ardila Fernandez	PW09Z34H	Valledupar	Golpes en esquinas	Se realiza visita y no cubre garantía por daño inducido	2024554288
Henrry Samir Gómez Ortiz	PW0A36X6	Nivel central	Robo	Pendiente respuesta por parte del MT	
Galia Lena Álvarez Hernández	PW0A3CHL	Nivel central	Golpes en esquinas	Pendiente funcionaria retorne el equipo	

Tabla 87 Equipos en siniestro

Instalaciones de Equipos y Entrega a Usuarios Finales:

Durante el período se recibe aval del Coordinador del Grupo de Soporte Informático para asignación de equipos de cómputo para Contratistas, Pasantes, Doble asignación de funcionarios, Salas de Conciliación y Contraloría.

Se recibe el listado de funcionarios con Condiciones Medicas Especiales, el coordinador del Grupo de Soporte informático solicita realizar el cambio de equipo para quienes tienen asignado portátil. Esta actividad está en curso según disponibilidad de los usuarios para cambio de equipo.

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

Tipo de equipo	Instalados
Portátil	937
Escritorio	1145
Total	2082

Tabla 88 *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, traslados, jubilaciones, entre otros.

DEVOLUCION DE EQUIPOS AGOSTO		
SEDE	**TIPO DE ELEMENTO**	**CANTIDAD**
Puerto Boyacá	Escritorio	1
Nivel Central	Portátil	10
DT Valle del Cauca	Escritorio	1

CANTIDAD DE EQUIPOS		
LUGAR	**PORTATIL**	**ESCRITORIO**
ALMACEN	183	27
OPERACIÓN	937	1145
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 agosto, desde la gestión de equipos de cómputo se relacionan las solicitudes de soporte atendidas para este servicio:

- Se registraron en Aranda un total de 19 solicitudes tipificadas así:
  - Incidentes – 0 caso
  - Requerimientos de Servicio – 19 casos.

- Al corte de mes quedaron en estado:
  - Cerrado – 13 casos.
  - Solucionado – 0 casos
  - Suspendido – 6 casos.
  - En Proceso – 0 caso.

- 17 casos corresponden a solicitudes de usuarios estándar y 2 a usuario VIP.

- La tabla que se muestra a continuación muestra los Grupos de Especialistas que dieron atención a las solicitudes del servicio:

Grupo responsable	Cantidad de solicitudes
Responsable Garantías Equipos	16
Gestor de Inventarios	3
Total general	**19**

Tabla 89 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	**19**
Equipo Periférico	11
Equipo Escritorio	4
Equipo Portátil	4
Total general	**19**

Tabla 90 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	100,00%	100,00%
EUF-2	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 91 Medición ANS Equipos de Usuario Final

4.2. Conectividad LAN y WLAN

A continuación, se relacionan las novedades y actividades relevantes gestionadas durante el mes:

- Se realizó gestión en la revisión y solución de alertas sobre dispositivos como Access Point con la colaboración de los soportes en sitio.
- Se realizó gestión y seguimiento a alertas sobres canales de comunicación para lograr el restablecimiento del servicio por parte del proveedor.
- Se trabajó en la remediación de vulnerabilidades reportados por el equipo del SOC.
- Se brindó apoyo la instalación y funcionamiento de nuevos puntos de red en la territorial de Florencia.
- Se realizó la reserva de IP para los dispositivos del secretario del ministro en piso 25.
- Se configuró la comunidad SNMPv3 en los access point Aruba.
- Se gestionó con ETB el cambio del enlace de última milla en la inspección de Tuluá.
- La UT instaló y aprovisionó un nuevo switch de 8 puertos para la territorial de Mitú con el propósito de organizar la conectividad LAN de la sede y tener disponibilidad de puertos para la conexión de la impresora Ricoh.
- Se realizó configuración de firewalls en modo switch para las oficinas de Leticia, Inírida, San Andres y Puerto Carreño, los equipos fueron enviados a las territoriales con el proposito de ampliar la disponibilidad de puertos LAN.
- Se trabajó con los soportes territoriales en la migración de conexiones y liberación de switches Apicom en las oficinas de Riosucio y Soacha.
- El 22/08/2025 se envía a la IT Magangué un nuevo equipo Fortinet como remplazo del anterior ya que se dañó por inundación y filtración de agua en la sede. Esto fue notificado vía correo electrónico al coordinador del Grupo de Soporte Informático.

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

- Los especialistas gestionaron un total de 13 solicitudes escaladas a través de la herramienta Aranda. Al corte del mes, 11 casos quedaron en estado Cerrado y 2 en estado suspendido, los casos obedecen a revisión y pruebas de red en canales de internet, revisión de alerta en dispositivos de red y entrega de información.

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

Categoría	Cantidad de solicitudes
AP	4
Starlink	2
asesoría - Consulta	1
Caída	1
Equipo Conectividad internet	1

Tabla 92 Top 5 de categorías en el Servicio de conectividad LAN-WLAN

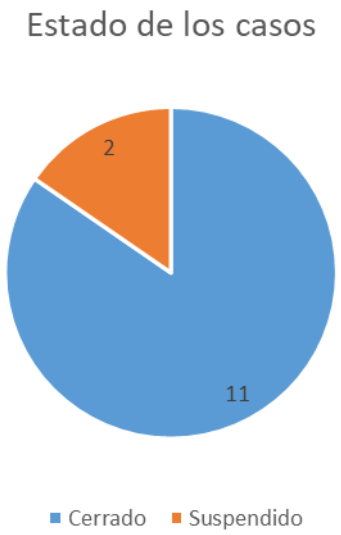


Ilustración 200 Estado de casos Redes y Conectividad

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 93 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 94 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

Dirección Territorial	Población y/o ciudad de ubicación	Cantidad Access Points
Territorial Atlántico	BARRANQUILLA	3
OE Barrancabermeja	BARRANCABERMEJA	2
Calle 32	BOGOTA	4
Territorial Bolívar	Cartagena	2
Territorial Boyacá	TUNJA	2
Territorial Caldas	MANIZALEZ	2
Territorial Caquetá	FLORENCIA	1
Territorial Casanare	YOPAL	2
Territorial Cauca	POPAYAN	2
Territorial Cesar	VALLEDUPAR	2
Territorial Chocó	QUIBDÓ	2
Territorial Córdoba	MONTERIA	2
Territorial Cundinamarca	FACATATIVÁ	2
Territorial Guajira	RIOHACHA	2
Territorial Huila	NEIVA	0
Territorial Magdalena	SANTA MARTA	2
Territorial Meta	VILLAVICENCIO	3
Territorial Nariño	PASTO	2
Territorial Norte de Santander	CÚCUTA	3
Territorial Putumayo	MOCOA	1
Territorial Quindío	ARMENIA	3
Territorial Risaralda	PEREIRA	2
Territorial Santander	BUCARAMANGA	1
Territorial Sucre	SINCELEJO	2
Territorial Tolima	IBAGUÉ	3*
OE Urabá Apartadó	APARTADÓ, ANTIOQUIA	2
Territorial Valle	CALI	4
OE Buenaventura	BUENAVENTURA	1
Sede Nivel Central	BOGOTA	49
	Total	**113**

Tabla 95 Distribución de puntos de acceso

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 96 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 97 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
ANTIOQUIA	AMAGA	1	Cerrada se envió teléfono a Medellín
CASANARE	MONTERREY	1	Cerrada
CAUCA	BOLIVAR	1	Cerrada
CORDOBA	TIERRA ALTA	1	Cerrada
QUINDIO	QUIMBAYA	1	Cerrada
QUINDIO	CALARCA	1	Cerrada
SUCRE	MAJAGUAL	1	Cerrada
TOLIMA	CASA DE JUSTICIA (IBAGUÉ)	1	Cerrada
TOLIMA	LÍBANO	1	Cerrada
	Total	**9(*)**	

Tabla 98 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 99 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 Nivel Central y DT	24
Pendientes definición de usuario por parte de la Coordinación del Grupo de Soporte Informático para asignación	6
Total	30

Tabla 100 Consolidado equipos MIFI

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

- **Gestión del servicio**

En el mes de agosto 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 monitoreo sobre las troncales para las opciones 2 y 0 configuradas en el IVR para atención al ciudadano con el nuevo aliado BPM.
- 01/08/2025: Durante el mes en curso se llevó a cabo el proceso de reducción de licenciamiento de Microsoft Teams Phone System, pasando de un total de 1700 licencias asignadas a 600, en cumplimiento de las políticas de uso y requerimientos actuales del servicio. Como parte de este proceso, se creó el grupo Grupo_Licencia_Telefono_Teams en Microsoft Entra ID (Azure Active Directory), con el objetivo de centralizar y automatizar la asignación de licencias a las cuentas que requieren acceso a funcionalidades de telefonía. Este grupo administra un total de 425 cuentas activas que mantienen licenciamiento vigente, correspondientes a usuarios que utilizan extensiones virtuales, dispositivos telefónicos asignados y aquellas solicitudes de activación aprobadas y ejecutadas durante el mes.



Licencias_08_2025.xl
sx

- 06/08/2025: Se realizó el proceso de configuración y aprovisionamiento de extensiones y asignación de licencias Teams Phone Standard en el tenant de Microsoft Teams para los usuarios solicitados. Se activaron 10 usuarios con extensión telefónica y licenciamiento. Los cambios fueron aplicados exitosamente. Se adjuntaron manuales de soporte y configuración para referencia. Estado actual: Todos los usuarios se encuentran activos.



SOLICITUD
PERMISOS PARA ACT



RE SOLICITUD PERMISOS PARA ACTIVACION LINEA TEAMS PARA LLAMADAS EXTERNAS BENEFICIARIOS PROGRAMAS MINISTERIO.msg

- Ejecución 22/08/2025 Cambio Estándar **RFC-142878** Actualización versión de telefonía.



RE Solicitud
RFC_Estandar-Telefon



VENTANA DE
MANTENIMIENTO DE

- El 27/08/2025 Se llevo a cabo proceso de configuración, asignación y capacitación con el usuario Raul Ocampo, en la cual se explicó el procedimiento para realizar llamadas a celulares, extensiones y líneas fijas.



RE Asignación ext.
virtual_Teams_Caso_F

- **Asignación de Licencias - Extensiones**

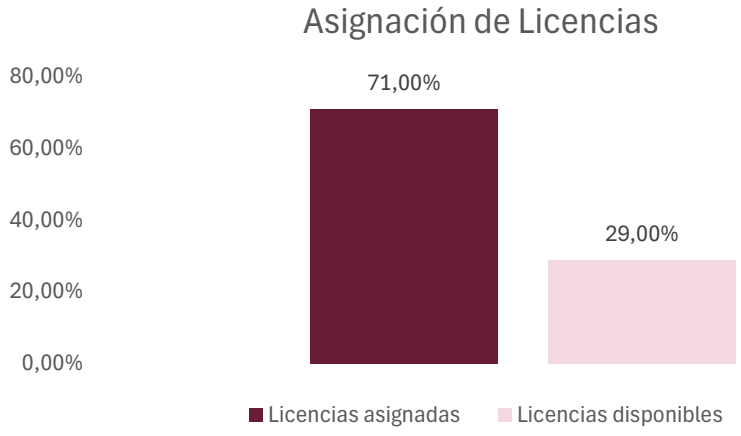


Ilustración *201*. Licencias y extensiones

Durante el mes en gestión, se han asignado un total de 425 extensiones a nivel nacional. Actualmente, permanecen disponibles 175 extensiones.

- **Estadísticas de Tráfico**

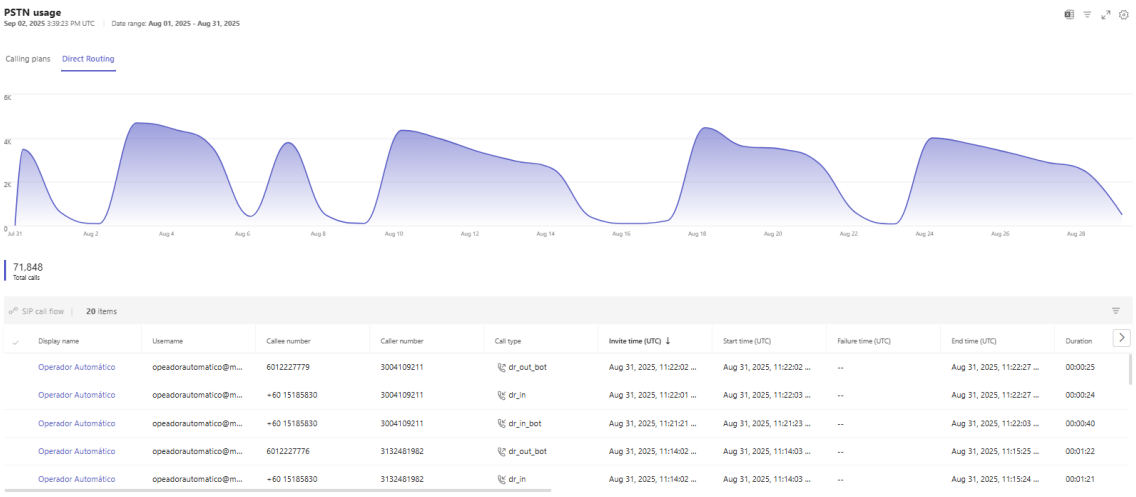


Ilustración 202 Estadística de tráfico

En la gráfica anterior se visualizan las tendencias de uso del servicio, en el periodo correspondiente al mes de agosto de 2025, donde se atendieron un total de 71,848 llamadas.

Servicio	Minutos Disponibles	Minutos Utilizados
Locales	Ilimitados	918.75
Celular	1000	868.19
Nacional	Ilimitados	364.12
Internacional	700	3.25
Total		2154.26

Tabla 101 Minutos, consumos

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

Con respecto a las llamadas realizadas a destinos larga distancia nacional en el mes de agosto de 2025, se identifica que se realizaron llamadas con una duración total de 364.12 minutos.

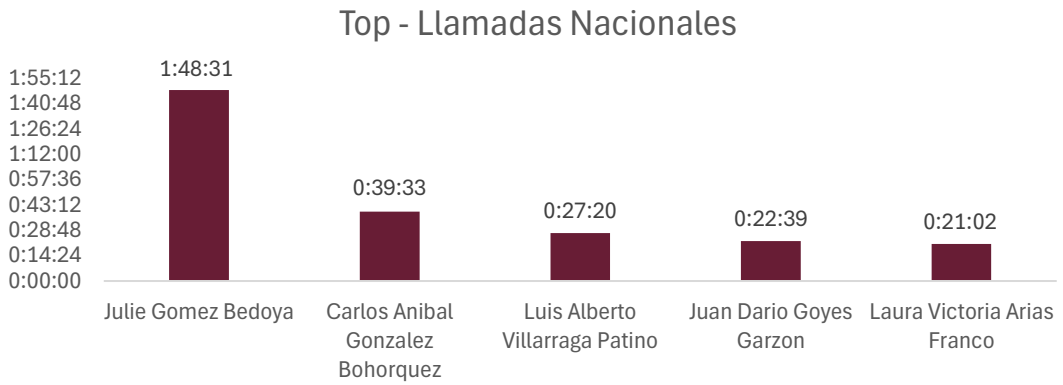


Ilustración 203 Top LDN

N°	Usuario	Área	Tiempo llamadas
1	Julie Gomez Bedoya	Grupo De Atención Al Ciudadano Y Tramites – DT Cali	01:48:31
2	Carlos Anibal Gonzalez Bohorquez	Grupo de Riesgos Laborales-Antioquia	00:39:33
3	Luis Alberto Villarraga Patino	Dirección de Riesgos Laborales – Bogotá	00:27:20
4	Juan Dario Goyes Garzon	Grupo de Dialogo Social - Antioquia	00:22:39
5	Laura Victoria Arias Franco	Direcciones Territoriales – Antioquia	00:21:02

Tabla 102 Top 5 llamadas LDN

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

Con respecto a las llamadas internacionales en el mes de agosto 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 204 Top LDI

Como se puede observar en el grafico anterior, se evidencia que, en el mes de agosto de 2025 se ha generado un consumo de llamada a destino internacional (España) por el administrador de telefonía, este a modo de prueba con el fin de validar la operatividad del servicio en las llamadas realizadas a larga distancia internacional.

N°	Usuario	Área	Tiempo llamadas
1	ADMINISTRADOR TELEFONIA	UT Gestión TIC 2023	00:03:25

Tabla 103 Top 5 llamadas LDI

- **Consumo de llamadas destinos celulares**

Con respecto a las llamadas realizadas a celular en el mes de agosto de 2025, se identifica que se realizaron llamadas con una duración total de 868.19 minutos.

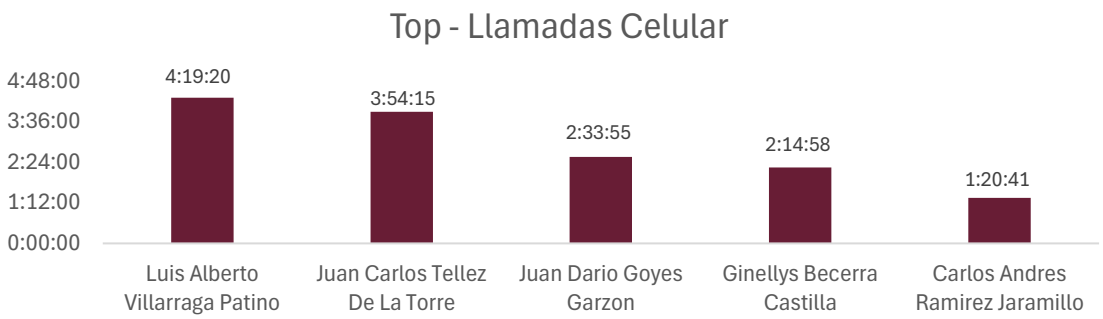


Ilustración 205 Top Celular

N°	Usuario	Área	Tiempo llamadas
1	Luis Alberto Villarraga Patino	Riesgos Laborales AMIRL – Sede Central Bogotá	04:19:20
2	Juan Carlos Tellez De La Torre	Grupo Interno de Trabajo Para las Victimas - Bogotá	03:54:15
3	Juan Dario Goyes Garzon	Grupo de Dialogo Social - Antioquia	02:33:55
4	Ginellys Becerra Castilla	Comunicaciones DT Bogotá	02:14:58
5	Carlos Andres Ramirez Jaramillo	Subdirección Administrativa y Financiera - Bogotá	01:20:41

Tabla 104 Top 5 llamadas Celular

- **Consumo de llamadas locales**

Con respecto a las llamadas realizadas a destinos locales en el mes de agosto de 2025, se identifica que se realizaron llamadas con una duración total de 918.75 minutos.

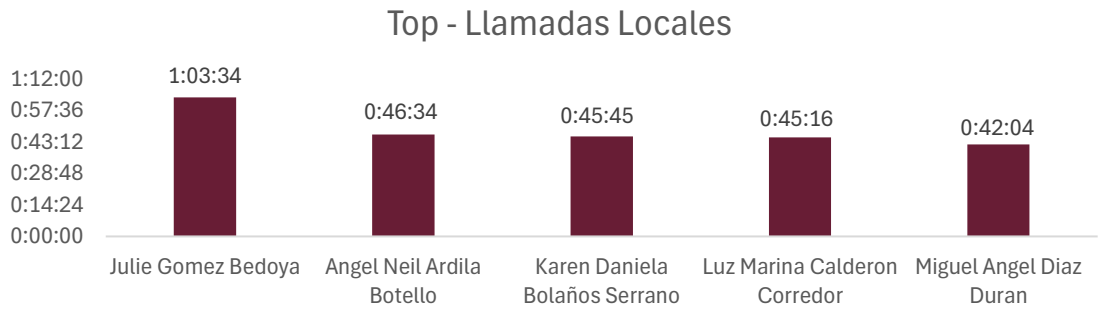


Ilustración 206 Top Local

N°	Usuario	Área	Tiempo llamadas
1	Julie Gomez Bedoya	Grupo De Atención Al Ciudadano Y Tramites – DT Cali	01:03:34
2	Angel Neil Ardila Botello	Grupo de Atención al Ciudadano	00:46:34
3	Karen Daniela Bolaños Serrano	Despacho del viceministro de relaciones laborales	00:45:45
4	Luz Marina Calderon Corredor	Grupo Interno De Trabajo De Nomina E Incapacidades	00:45:16
5	Miguel Angel Diaz Duran	ATC Y T Cundinamarca - Bogotá	00:42:04

Tabla 105 Top 5 llamadas locales

- **Capacitaciones y divulgaciones**

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



RE Asignación ext.
virtual_Teams_Caso_F

Ítem	Descripción	Fecha
1	Capacitación con el usuario Raul Ocampo, en la cual se explicó el procedimiento para realizar llamadas a celulares, extensiones y líneas fijas	27-08-2025

Tabla 106. 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

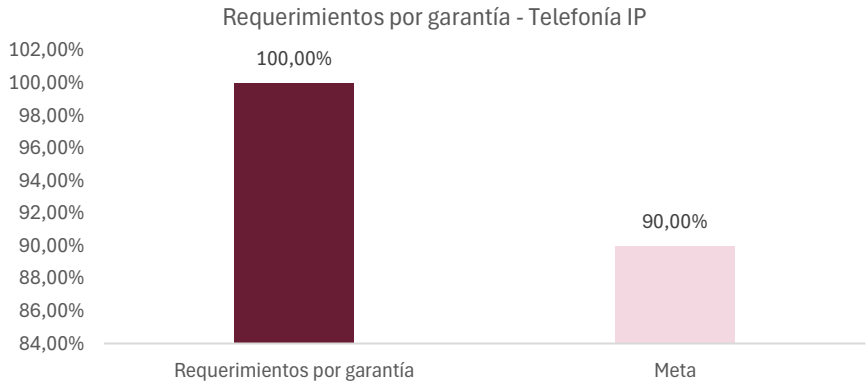


Ilustración *207* Requerimientos por garantía

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

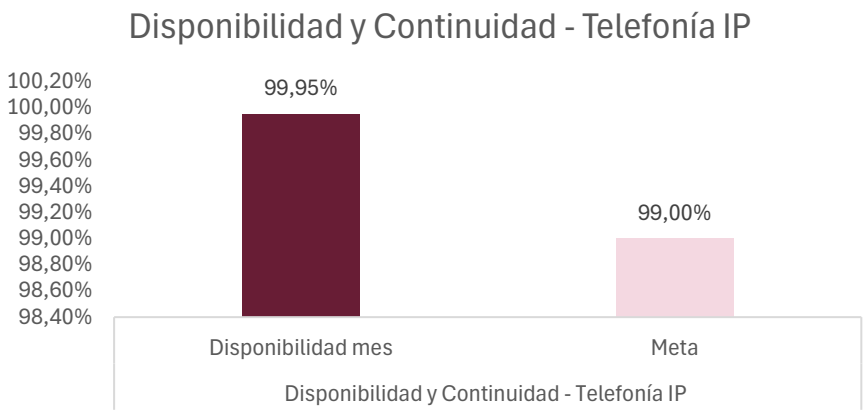


Ilustración 208 Disponibilidad y Continuidad TOIP

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

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

ID	Indicadores	Resultado	Meta
TIP-1	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
TIP-2	Continuidad y disponibilidad de los servicios de telefonía IP	99,95%	99,00%
TIP-3	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 107 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 108 Inventario de UPS – 10kVA

4.4.2. UPS 15 kVA

Durante la implementación de la solución del servicio para el cliente Ministerio del Trabajo no se realiza instalación de UPS de 15kVA, el detalle de esto se entregó a la Supervisora del Contrato del momento, en el INFORME UT GESTION TIC 2023 - ENTREGA LINEA DE SERVICIO EER UPS

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 109 Inventario de UPS – 20Kva

- **Gestión del servicio**

- Las UPS se encuentran instaladas y operativas según distribución dada por el cliente a nivel contractual, durante el período no se presentan fallas en el servicio que requieran cambios

de equipos en ninguna sede ni gestión de garantías que requiera reemplazo de partes/repuestos por parte de la UT.

- Se tienen las siguientes novedades que generan alertamientos en las UPS dispuestas por la UT, se aclara que se validó con el personal técnico y la atención de las novedades requieren ser solventadas por la entidad o por los responsables de los predios donde se encuentran ubicadas:
    - Se escala al ministerio en febrero 2025, novedad con la UPS en la territorial de Santander (Bucaramanga) propiedad de la UT, ya que se encontró que hay picos de voltaje de entrada con valores de 135V, se requiere hacer validación con la empresa proveedora de energía ya que de lo contrario sería necesario adquirir un regulador de voltaje para corregir las alertas que está presentando la UPS. Al cierre de este período no se tiene ningún avance por parte de la entidad.

    - Durante Julio 2025 se presentan alertamientos sobre la UPS de la DT Risaralda (Pereira), generando que se alarme, presente alarma sonora y deba ser reiniciada por el personal de soporte técnico. La UT coordina visita de técnico especialista a la sede el 29/07/2025 para verificar estado del equipo luego de los constantes alertamientos presentados, validar entrada y salida de voltaje UPS, validar estado de funcionamiento fluido eléctrico en la sede.
      En la revisión realizada se encuentra que la UPS se encuentra funcionando bien, recibe 2 fases de 110V, entregan energía regulada con normalidad. El problema está asociado a la red regulada del predio que está haciendo disparar el totalizador de la red regulada. Se requiere revisar toda la red regulada (tomas, breakers y el cableado).

      Acta de Servicio -UPS Pereira MInTrabajo.pd

      El 11/08/2025 se envía correo al coordinador del Grupo de Soporte Informático con la novedad del servicio de energía de la sede. El personal de soporte nos ha informado que se presentaron varios técnicos para verificar el tema eléctrico y la cotización de los servicios para solución de la falla, pero no se han tenido novedades por parte de la DT ni del responsable del predio.

      En el mes de agosto 2025 la entidad contrato personal que realizó verificación de los puntos regulados de la sede y cambio del tablero de distribución, a espera del informe correspondiente.

- **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 110 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 111 Inventario de impresoras para el servicio

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

- Para el mes de agosto, el responsable del servicio gestionó un total de 644 solicitudes escaladas a través de Aranda. Al corte del mes, 619 casos quedaron en estado Cerrado/Solucionado, 25 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 independizó el correo del servicio de escáner; el nuevo correo para dicha gestión es **srvscanner@mintrabajo.gov.co** (se realiza despliegue a nivel nacional el 4/08/2025).
- Durante el período se realiza cambio de inventario de la impresora de la DT Guaviare mientras se realizó proceso de garantía con el fabricante Ricoh.
- 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 en 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-146124; allí se relaciona el listado total de usuarios con el aprovisionamiento.

- 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
ricohpiso5a	Bogotá sede central	cjunco	Carlos Julio Junco Arenas	3124
ricohpiso19a	Bogotá sede central	pnustes	Patricia Celestial Nustes Barrera	2999
ricoh-cali-piso2-atc	Cali	gcolonia	Gustavo Adolfo Colonia Trochez	2641
ricoh-guadalaraja-buga-insp	Guadalaraja Buga	vfierro	Viviana Fierro Herrera	2356
ricoh-cali-piso2-atc	Cali	ruribe	Rafael Uribe Agredo	2008
ricohpiso23b	Bogotá sede central	ldleal	Luz Dary Leal Cotamo	1905
ricohpiso22a	Bogotá sede central	eacosta	Edgar Antonio Acosta Rojas	1802
ricoh-ibague-radicacion	Ibague	mnavarrog	Maria Alejandra Navarro Garcia	1782

ricoh-quindio-piso1-ppal	Quindio	lmillan	Lucy Evelyn Millan Muñoz	1704
ricoh-apartado-piso2-c	Apartado	tllanes	Tatiana Llanes Ibarguen	1696

Tabla 112 Consumo de impresiones por usuario - Impresoras B/N

Clics%20agosto%20total.xlsx

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

Nombre de la impresora	Ubicación	Blanco y negro
ricohpiso12a	Bogotá Sede Central	11929
ricohpiso5a	Bogotá Sede Central	11569
ricoh-bmanga-ofc305	Bucaramanga	10146
ricohcl32-rcc	Bogotá Calle32	10129
ricoh-cali-piso2-atc	Cali	9704
ricohpiso23b	Bogotá Sede Central	9528
ricoh-bmanga-ofc205	Bucaramanga	9327
ricohpiso10b	Bogotá Sede Central	8935
ricoh-cali-piso4	Cali	8831
ricohpiso19a	Bogotá Sede Central	8536

Tabla 113 Top 10 de impresoras con mayor uso

impresoras%20mas%20usadas%20agos

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

Nombre de la impresora	Ubicación	Nombre de Usuario	Nombre Completo	Color
ricohpiso25c	Bogotá sede central	mserrano	Malliber Serrano Nieto	1179
ricohpiso25c	Bogotá sede central	ymedinag	Yeisson Medina Gonzalez	96
ricohpiso25c	Bogotá sede central	bhernandez	Bibiana Hernandez Hernandez	74
ricohpiso25c	Bogotá sede central	dmmoreno	Daniela Marcela Moreno Garcia	12

Tabla114 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	1361	115228	85564	31025	116589	30108	3,9
D. T. Bogota	0	40527	29512	11015	40527	9801	4,1
D. T. Valle Del Cauca	0	40168	28392	11776	40168	12243	3,3
D. T. Santander	0	33744	23486	10258	33744	10359	3,3
D. T. Antioquia	0	26244	19546	6698	26244	7977	3,3
D. T. Norte De Santander	0	14746	9160	5586	14746	4477	3,3

D. T. Tolima	0	14143	9948	4195	14143	3834	3,7
D. T. Quindio	0	11350	8158	3192	11350	2557	4,4
D. T. Cundinamarca	0	11237	7454	3783	11237	3048	3,7
D. T. Huila	0	11048	7904	3144	11048	3115	3,5

Tabla115 Top oficinas



Informe%20por%20oficinas%20agosto.›

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).

Nombre de impresora	Ubicación	Copias
ricoh-medellin-iso1	Medellín	51.656
ricohcl32-gau-b	Bogotá Cll32	50.988
ricohcl32-rcc	Bogotá Cll32	44.910
ricoh-bmanga-ofc205	Bucaramanga	30.492
ricoh-cali-piso4	Cali	28.634
ricohpiso5b	Bogotá Sede Central	24.788
ricohcl32-gau-a	Bogotá Cll32	21.613
RICOH-BMANGA-OFC305	Bucaramanga	19.653
ricohpiso9a	Bogotá Sede Central	19.193
ricoh-monteria-piso2	Montería	18.432

Tabla 116 Top 10 impresoras más usadas del servicio de fotocopiado



Reporte%20copias%20agosto.xlsx

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



Transacciones%20Agosto.xlsx

Nombre de Usuario	Nombre Completo	Tipo de transacción	Total Cuota asignada	Número de veces que se aumento
nparra	Natalia Andrea Parra Lizarralde	ADJUST	1637	6
ybeltran	Yerson Daniel Beltran Martinez	ADJUST	1195	5
ccabrera	Carlos Andres Cabrera Mosquera	ADJUST	1288	4
crepizo	Carmen Elena Repizo Prado	ADJUST	1106	4
dpino	Daniela Pino Torres	ADJUST	1299	4
egonzalez	Edna Lucia Gonzalez Parra	ADJUST	961	4
esantana	Edgar Manuel Santana Castro	ADJUST	907	4
jargoti	Janeth Pilar Argoti Lagos	ADJUST	644	4
jegomez	Jorge Eduardo Gomez Rico	ADJUST	886	4
jtrujilloc	Jeraldyn Marcela Trujillo Chica	ADJUST	730	4

Tabla 117 Ampliación de cuota de impresión



Asignacion%20cuota%20Agosto.xlsx

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

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

	jun-25		jul-25		ago-25	
	Resmas Carta	Resmas Oficio	Resmas Carta	Resmas Oficio	Resmas Carta	Resmas Oficio
Total Resmas	660	516	565	358	401	267
Total Cajas por Tamaño	66	51,6	56,5	35,8	40,1	26,7
Total Cajas Enviadas	**117,6**		**92,3**		**66,8**	

Tabla 118 Despacho de papel a sedes del Ministerio del Trabajo

Durante el período, se despacharon a sedes del ministerio un total de 49 tóners para impresora B/N y 6 unidades de tambor.

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 119 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 120 Cargo mensual impresora color

4.6.4. No aplica

4.6.5. Multifuncional B/N rango medio – Clic de impresión

A continuación, se detallan las cantidades de clics de impresión correspondientes al mes de agosto de 2025:

MES	DETALLE	CANTIDAD
agosto	Multifuncional blanco y negro rango medio - Clic de impresión tóner y papel carta	**619.172**
	TOTAL	**619.172**

Tabla 121 Clics de impresión de agosto 2025 – Multifuncional B/N

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

Mes 2025	Junio	Julio	Agosto
Cantidad de clics consumidos	**547.351**	**686.509**	**619.172**

Tabla 122 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 **461.759** clics de impresión (esto incluye **5.388** de la impresora de contratos piso 8) y **157.413** de fotocopias para un total de **619.172** para este servicio, superando el estimado del mes por **169.172.**

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

4.6.6. Impresora Color rango medio – Clic de impresión

A continuación, se detallan las cantidades de clics de impresión de color correspondientes al mes agosto de 2025:

MES	DETALLE	CANTIDAD
Agosto	Impresora color rango medio - Cargo fijo mensual - Clic de impresión tóner y papel carta	**1.361**
	TOTAL	**1.361**

Tabla 123 Clics de Impresión de agosto 2025 – Impresora Color

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

Mes 2025	Junio	Julio	Agosto
Cantidad de clics consumidos	**961**	**2.131**	**1.361**

Tabla 124 tendencia de consumo de clics color

El consumo mensual establecido para el servicio por la entidad es de 1.500 clics de impresión en color para el único equipo de este tipo ubicado en Nivel Central; para el período del informe se presentó un consumo de **1.361** 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 125 Medición ANS Outsourcing de Impresión

4.7. Antivirus

A continuación, se presenta la información relacionada con la gestión del servicio de antivirus en el Ministerio de Trabajo, donde se pueden apreciar los siguientes detalles:

4.7.1. Instalaciones de antivirus en servidores

El antivirus TrendMicro ha mostrado un rendimiento sólido en la protección de los sistemas contra amenazas informáticas, manteniendo una alta tasa de detección y neutralizando diversas formas de software malicioso y otras vulnerabilidades de seguridad.

En agosto de 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.

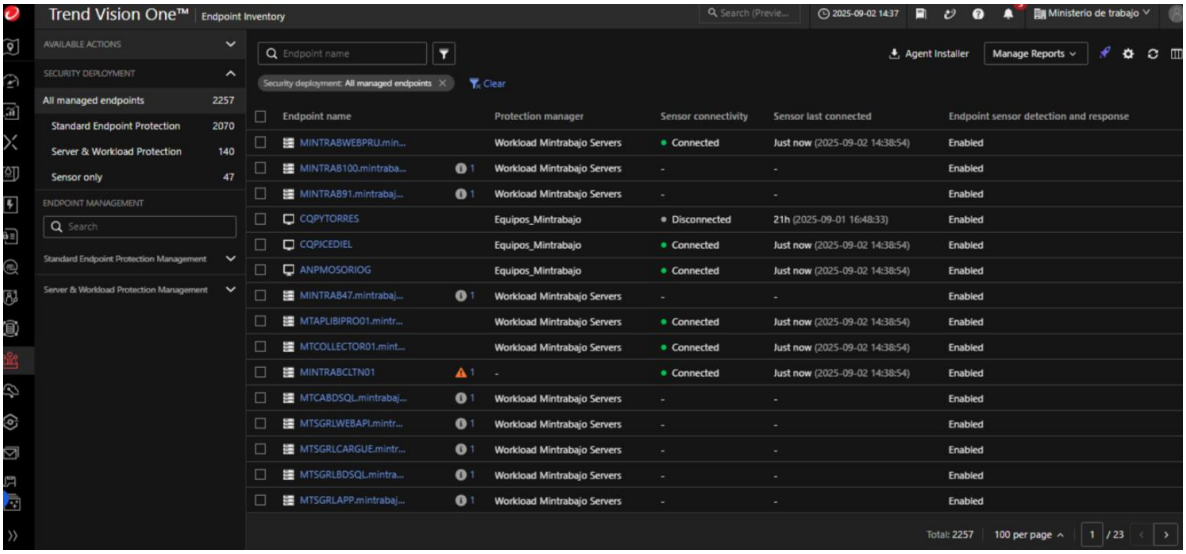


Ilustración 209 Equipos consola antivirus

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 (2070) de Mintrabajo, se cuenta con 2168 licencias, se tienen disponibles 90.

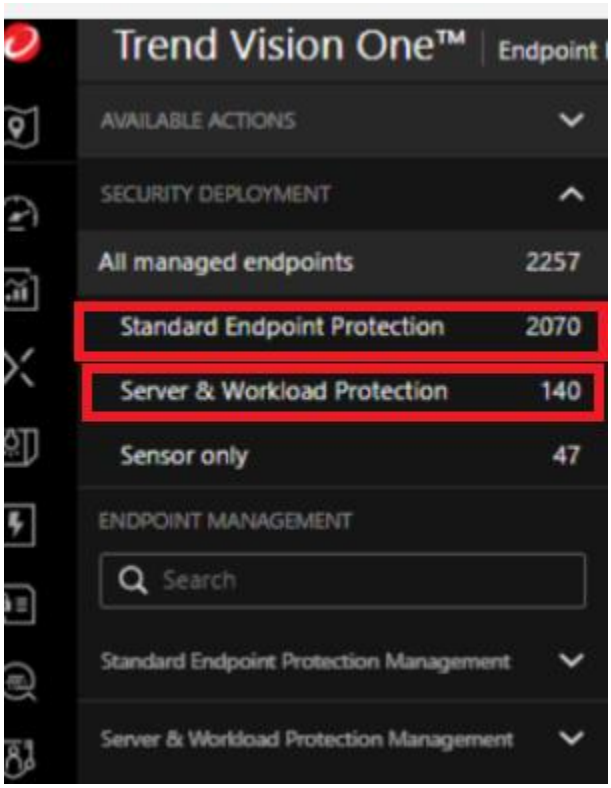


Ilustración 210 Gestión consola antivirus – equipos usuario final

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.

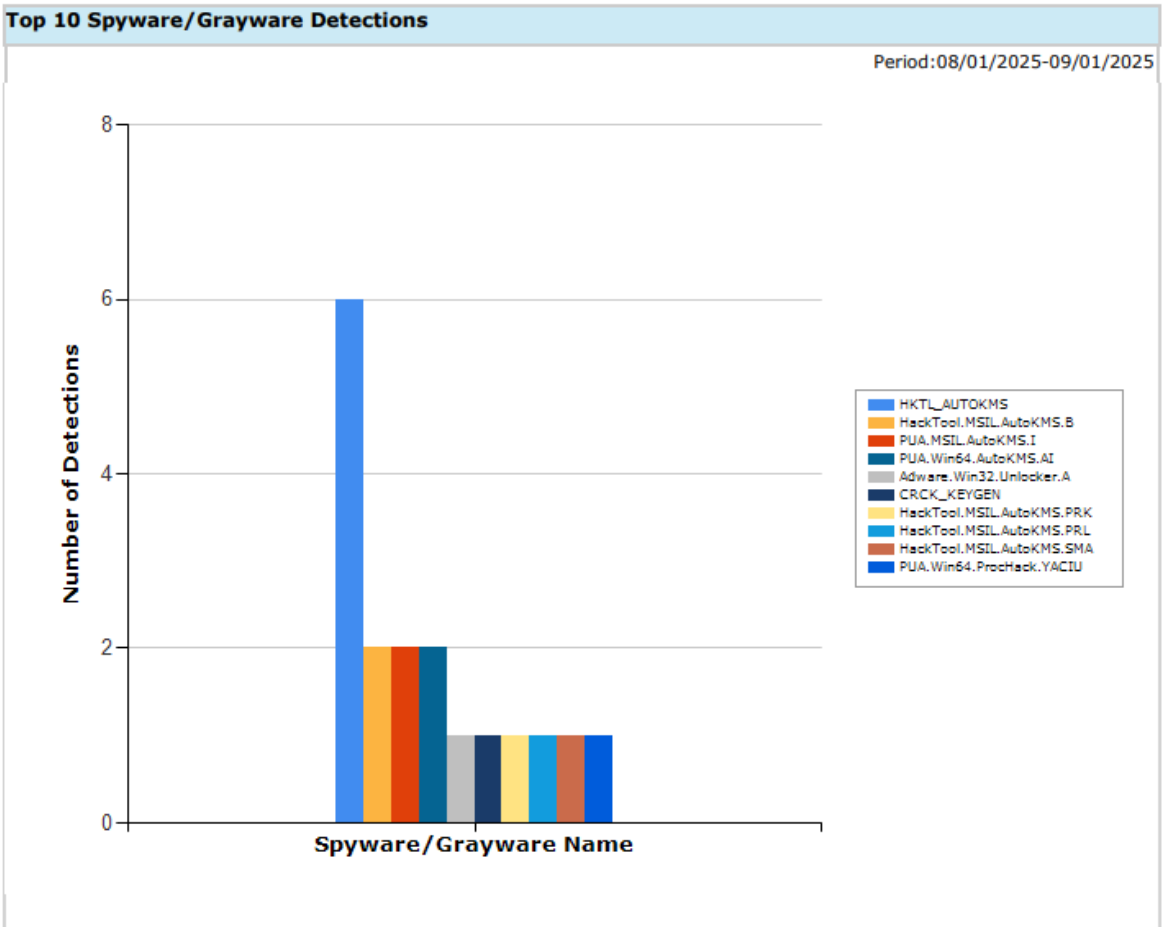


Ilustración 211 Top 10 Spyware

Top 10 Spyware/Grayware Detections		
Spyware/Grayware Name	# of Detections	Detected By
HKTL_AUTOKMS	6	Desktop (6)
HackTool.MSIL.AutoKMS.B	2	Desktop (2)
PUA.MSIL.AutoKMS.I	2	Desktop (2)
PUA.Win64.AutoKMS.AI	2	Desktop (2)
Adware.Win32.Unlocker.A	1	Desktop (1)
CRCK_KEYGEN	1	Desktop (1)
HackTool.MSIL.AutoKMS.PRK	1	Desktop (1)
HackTool.MSIL.AutoKMS.PRL	1	Desktop (1)
HackTool.MSIL.AutoKMS.SMA	1	Desktop (1)
PUA.Win64.ProcHack.YACIU	1	Desktop (1)

Tabla 126 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:

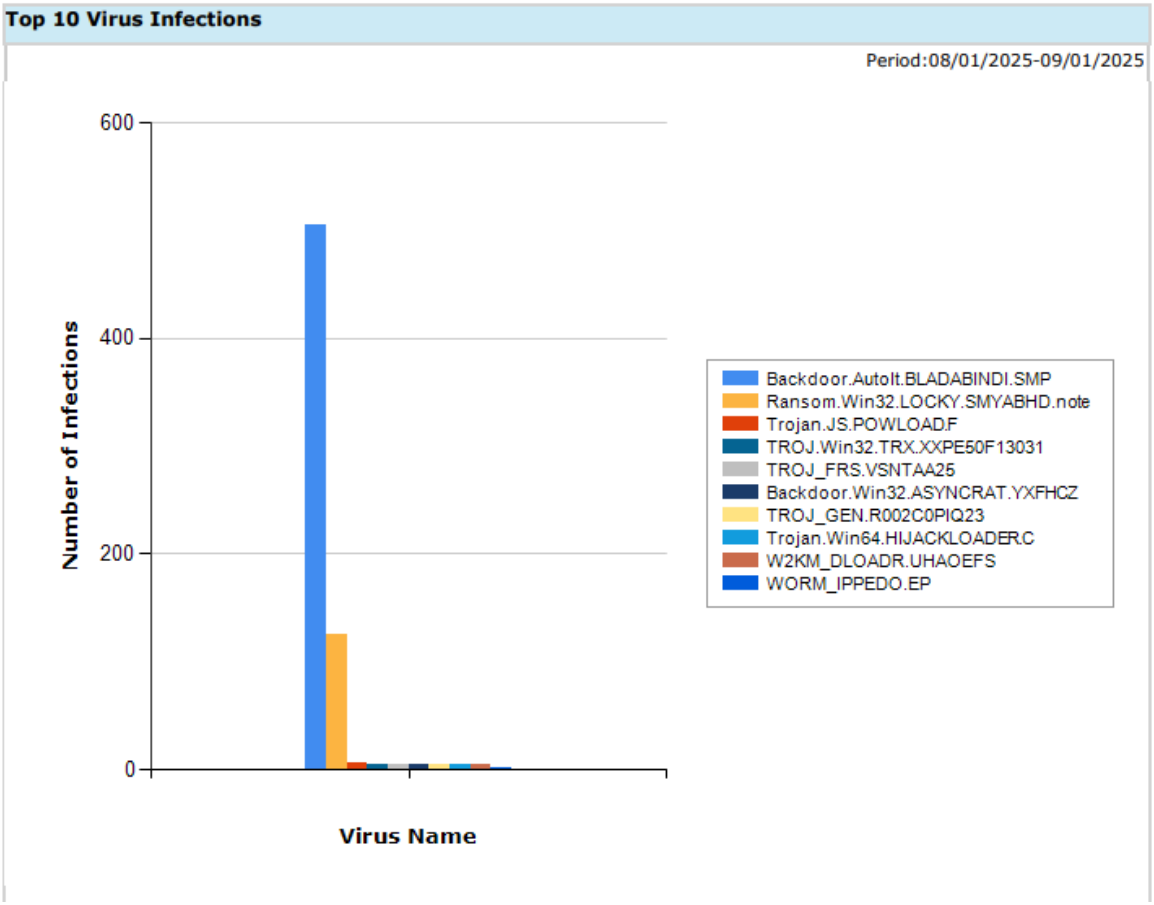


Ilustración 212 Top 10 virus detectados

Top 10 Virus Infections		
Virus Name	# of Infections	Detected By
Backdoor.AutoIt.BLADABINDI.SMP	506	Desktop (506)
Ransom.Win32.LOCKY.SMYABHD.note	125	Desktop (125)
Trojan.JS.POWLOAD.F	6	Desktop (6)
TROJ.Win32.TRX.XXPE50F13031	5	Desktop (5)
TROJ_FRS.VSNTAA25	5	Desktop (5)
Backdoor.Win32.ASYNCRAT.YXFHCZ	4	Desktop (4)
TROJ_GEN.R002C0PIQ23	4	Desktop (4)
Trojan.Win64.HIJACKLOADER.C	4	Desktop (4)
W2KM_DLOADR.UHAOEFS	4	Desktop (4)
WORM_IPPEDO.EP	2	Desktop (2)

Ilustración 213 Top infección virus

Aspecto	Detalle	Interpretación / Riesgo
Malware más prevalente	Backdoor.AutoIt.BLADABINDI.SMP con 506 infecciones	Es una amenaza de alto riesgo (backdoor/troyano), permite control remoto del equipo comprometido. Representa más del 70% del total de infecciones detectadas indica una campaña activa y extendida en la infraestructura.
Segundo más detectado	Ransom.Win32.LOCKY.SMYABHD.note con 125 infecciones	Variante de ransomware Locky, busca cifrar archivos y extorsionar. Su volumen representa un ~18% del total, lo que evidencia intentos serios de impacto operativo.
Otras amenazas	Infecciones aisladas (2 a 6 casos) como: Trojan.JS.POWLOAD.F, TROJ.Win32.TRX.XXPE50F13031, Backdoor.Win32.ASYNCRAT, Trojan.Win64.HIJACKLOADER, gusanos como WORM_IPPEDO.EP.	Aunque de menor volumen, son indicadores de intentos diversificados para obtener persistencia, robar credenciales o propagar malware en la red.
Vectores de infección	Todas las detecciones provienen de endpoints (Desktop)	Refleja que el punto más débil sigue siendo el usuario final. Los endpoints son la superficie principal de ataque.
Concentración de infecciones	2 tipos de malware (Backdoor.AutoIt y Ransom.Locky) concentran más del 90% de las detecciones totales	Esto indica campañas específicas y dirigidas, más que ataques dispersos.

Tabla 127 Descripción de virus

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 agosto 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 segundo 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 310 activos de TI.

En agosto, se alcanzó un registro de 301 activos de TI (97 %) de la línea base documentada en la herramienta.

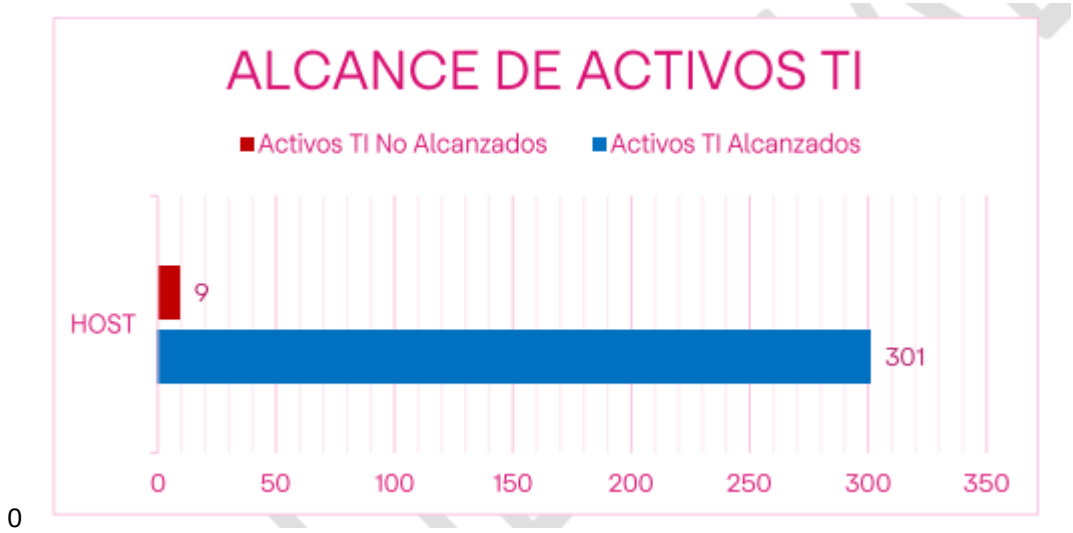


Ilustración 214 Gestión consola Nessus

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 II - WINDOWS DESKTOP	Vulnerability	Weekly on Sat at 12:30 AM	✔	August 30 at 1:05 AM
MINTRABAJO SEMANAL II - NETWORKING	Vulnerability	Weekly on Sat at 8:00 PM	✔	August 30 at 8:30 PM
MINTRABAJO SEMANAL II - FORTISIEM	Vulnerability	Weekly on Sat at 9:00 PM	✔	August 30 at 9:37 PM
MINTRABAJO SEMANAL II - VMWARE	Vulnerability	Weekly on Sat at 10:00 PM	✔	August 30 at 10:11 PM
MINTRABAJO SEMANAL II - LINUX	Vulnerability	Weekly on Sat at 11:00 PM	✔	August 30 at 11:51 PM
MINTRABAJO SEMANAL II - NO AUTH	Vulnerability	Weekly on Sun at 3:30 AM	✔	August 31 at 3:40 AM
MINTRABAJO SEMANAL II - WINDOWS SERVER	Vulnerability	Weekly on Sun at 9:00 PM	✔	September 1 at 12:41 ...

Ilustración 215 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
Julio 2025	76	472	1.292	481
Agosto 2025	69	422	1.278	308

Tabla 128 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 el activo TI con la mayor cantidad de vulnerabilidades identificadas corresponde al host (**172.20.22.42**), con un total de 104 hallazgos, corresponde a un servidor Rocky Linux release 8.9 (Green Obsidian) y la mayoría de las vulnerabilidades están asociadas a actualizaciones de seguridad para el paquete OpenSSL.
:

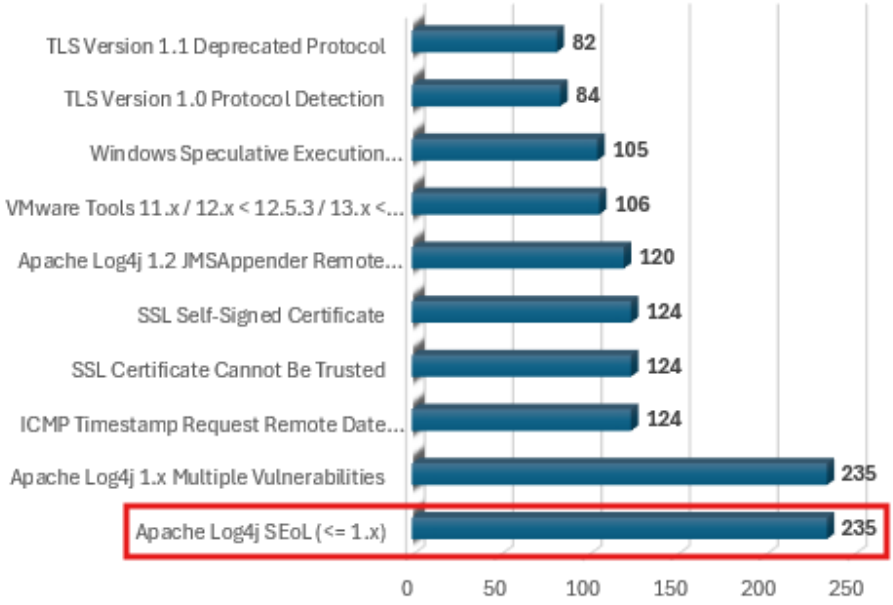


Tabla 129 TOP 10 - Activos más explotables

La vulnerabilidad más crítica identificada corresponde a "**KB5029304: Windows Server 2012 R2 Security Update (August 2023)**", con un total de 3 hallazgos, corresponde a un boletín de seguridad para el sistema operativo Windows Server 2012 R2, publicado en agosto de 2023 y que abarca varias vulnerabilidades que se remedian aplicando la actualización de seguridad emitida por el fabricante.

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 II 2025, el cual reportó un total de 3.257 vulnerabilidades TI en las severidades:

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

Durante el periodo de agosto del 2025, se remediaron un total de 347 vulnerabilidades, de las cuales, 50 fueron de severidad crítica, 51 de severidad alta, 64 de severidad media y 182 de severidad baja. Por otro lado, con relación a indicadores semestrales, se gestionaron un total de 1089 vulnerabilidades TI, de las cuales, 250 fueron de severidad crítica, 112 de severidad alta, 419 de severidad media y 308 de severidad baja.

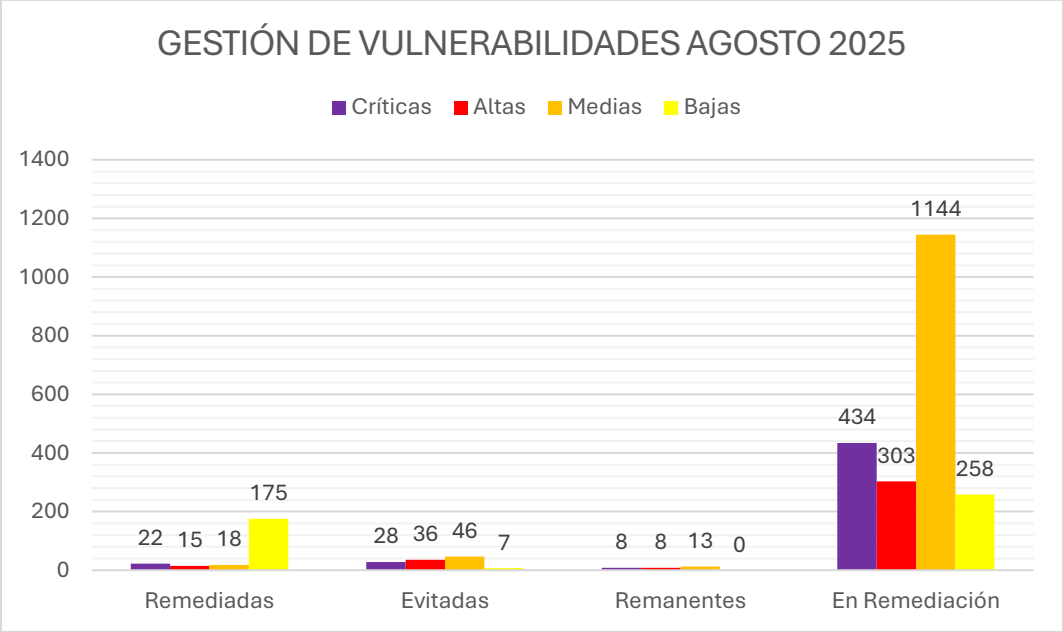


Ilustración 216 Vulnerabilidades gestionadas vs en remediación

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



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

4.7.5.6. Ethical Hacking Segundo semestre 2025

Se notifica que se procede con la tercera fase del **Ethical Hacking** del **segundo semestre 2025** para el proyecto Ministerio de Trabajo, de acuerdo con el cronograma de ejecución propuesto.

FASE	RIESGO	RESPONSABLE	PROGRESO	INICIO MM-DD-YYYY	DÍAS
Levantamiento de información	Riesgo medio	Daniel Castillo	**100%**	07/28/2025	5
Planeación de la Prueba	Riesgo medio	Daniel Castillo	**100%**	08/04/2025	5
Ejecución de Pruebas	Riesgo alto	Daniel Castillo	**100%**	08/11/2025	12
Documentación	Riesgo medio	Cristian Cuadros	**0%**	08/27/2025	5
Presentación de Resultados	Riesgo bajo	Daniel Castillo	**0%**	09/03/2025	5

Tabla 130 Ethical Hacking Segundo semestre

Esta cuarta fase corresponde a la clasificación y tabulación de los resultados, los cuales serán plasmados en tres documentos correspondientes al informe técnico, informe gerencial y la matriz de hallazgos. Estos tres documentos tienen la finalidad de proporcionar la documentación necesaria para comprender el riesgo de los hallazgos, así como un punto de partida para la remediación necesaria a aplicar sobre las aplicaciones web:

Por último, se define una prueba de caja blanca orientada a aplicaciones web con escenario hibrido, la cual se incluye un total de 8 aplicaciones web correspondientes a:

1. https://sve.mintrabajo.gov.co/suiteve/base/client (Externa)
2. https://www.mintrabajo.gov.co/web/guest (Externa)
3. https://app3.mintrabajo.gov.co/auth/login (Externa)
4. https://cobrocoactivo.mintrabajo.gov.co/ (Externa)
5. https://simpc.mintrabajo.gov.co/masterdata/ (Externa)
6. https://gestordocumental.mintrabajo.gov.co:9444/ProcessPortal/login.jsp (Interna)
7. http://sisgestionpru.mintrabajo.gov.co:8199/login (Interna)
8. https://sid3.mintrabajo.gov.co/ (Interna)

- **Medición de ANS Antivirus**

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

ID	Indicadores	Resultado	Meta
AV-1	Cobertura de antivirus	92,88%	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 131 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 217 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 132 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 agosto, se realizó la evaluación cuantitativa de la muestra de 309 casos documentados en la Herramienta de Gestión.

Para el cálculo Calidad Documental de Casos, se tienen en cuenta el número de criterios cumplidos Vs el número total de criterios, aplicando el peso porcentual para cada criterio.
Para esto, se evalúan por cada caso, los 13 criterios definidos, obteniendo el siguiente resultado:

Items Evaluados	ENC Cometidos	% Cumplimiento
1. Tipo de caso	0	100%
2. Asunto	2	99,9%
3. Descripción	1	99,9%
4. Prioridad	0	100%
5. Categoría	4	99,8%
6. Escalamiento	0	100%
7. Solución	6	99,8%
8. Estado del Caso	0	100%
9. Justificación Estado del Caso	0	100%
10. Periodicidad de seguimientos	0	100%
11. Descripción de seguimientos	0	100%
12. Ortografía y redacción	18	99,4%
13. Cumplimiento de ANS	2	99,9%

Tabla 133 Errores cometidos

Se identificaron 33 errores con un porcentaje de cumplimiento consolidado de 98,93%, lo cual se evidencia un aumento de 2 afectaciones al periodo anterior.

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 6 novedades por soluciones no claras o incompletas, 4 novedades por error en la categorización del ticket y 18 falencias en ortografía y redacción. De acuerdo con lo anterior, se realizará refuerzo con el equipo en sesión del mes de agosto, con el fin de retroalimentar a los servicios TIC sobre las afectaciones de documentación de casos.

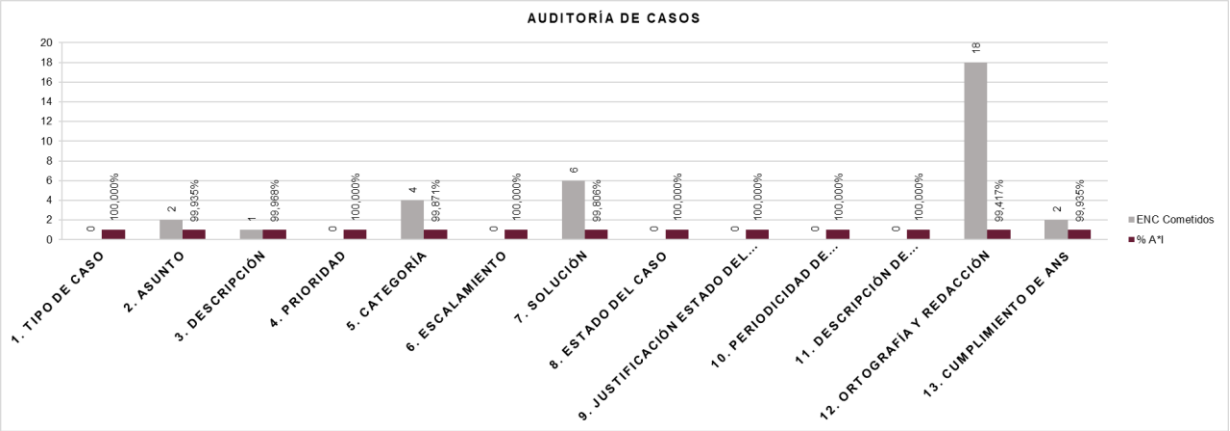


Ilustración 218 Resultados auditoria de casos

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 219 Precisión error no Critico de llamadas

PRECISIÓN ERROR CRÍTICO – PEC



Ilustración 220 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.

Criterios	Parámetros
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. - 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 134 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 135 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 136 Calificación Calidad llamadas

5.4 Evaluación de calidad de llamadas

En el mes de agosto 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	Agosto 2025	%
Escucha Activa	9	70%
Retroalimentación y manejo de esperas	3	90%
Empatía y adaptabilidad al usuario	2	93%
Asegura y Despedida	1	97%
Bienvenida y Personalización	0	100%
Soporte Primer Nivel	0	100%

PRECISIÓN ERROR CRÍTICO – PEC	Agosto 2025	%
Uso correcto Herramienta de Gestión	2	94%
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 137 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 32 llamadas evaluadas de las cuales se evidencia las siguientes afectaciones en el resultado global por categoría:

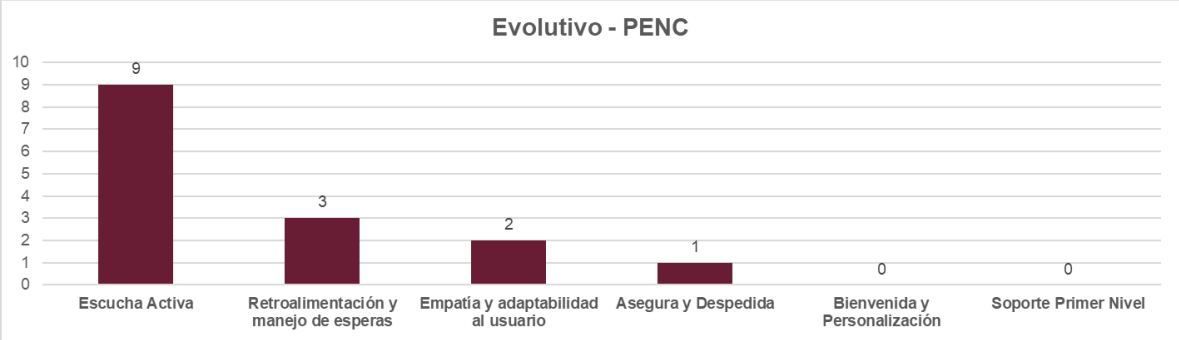


Ilustración 221 Resultados llamadas PENC

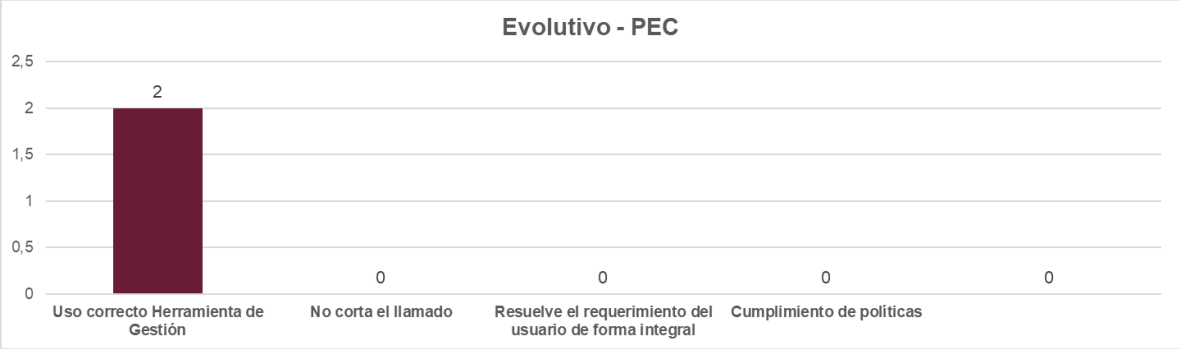


Ilustración 222 Resultados llamadas PEC

5.5 Práctica de Mejora

Dar a conocer las actividades de la Práctica de Mejora Continua correspondientes al periodo del 1 al 31 de agosto de 2025. Este apartado contiene información relevante sobre las acciones de mejora identificadas por los Servicios TIC durante el 2025.

Acciones 2025	Cantidad
Acciones Propuestas	26
Acciones En Proceso	6
Acciones Cerradas	20

Tabla 138 Seguimiento de Acciones de Mejora

En el siguiente gráfico, se evidencia que, de las 26 acciones de mejora identificadas, se encuentran ejecutas y cerradas 20 acciones de mejora, lo cual se cuenta con un cumplimiento de ejecución del tercer trimestre del 76,92% de los diferentes servicios TIC y Gestiones ITIL.

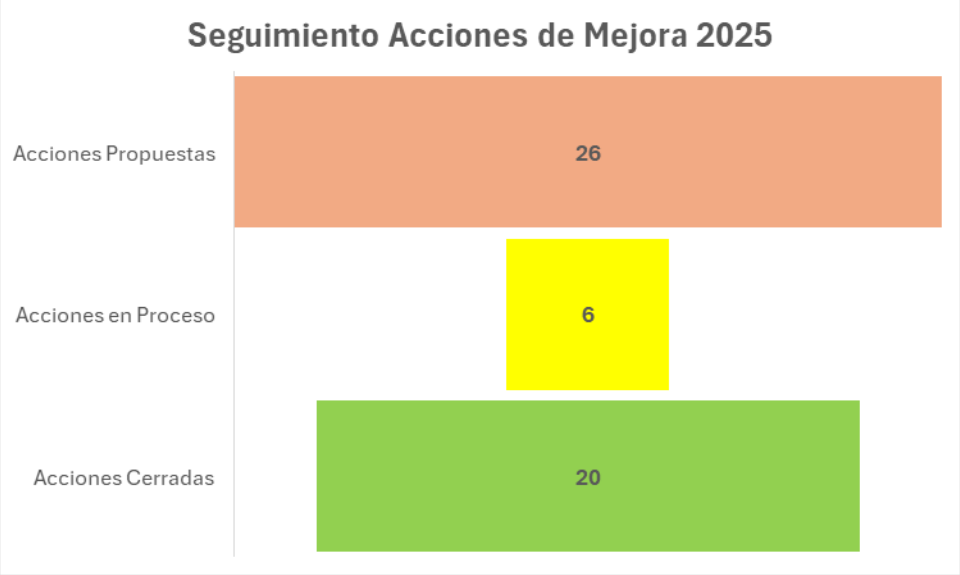


Ilustración 223 Seguimiento Práctica Mejora

Durante el inicio de la Practica de mejora, se realizaron diferentes actividades de socialización y capacitación, con el fin de establecer mecanismos de identificación y participación de los diferentes Servicios TIC, por lo tanto, para dar una medición al su cumplimiento de las acciones propuestas, se estableció el siguiente indicador trimestral:

Nombre	Fórmula	Meta	Periodicidad
Cumplimiento de las fechas previstas de las acciones de mejora registradas	**IMP**: Implementación de Mejoras de ITIL de servicios/gestiones	>= 70%	Trimestral
	AMI: Cantidad de Acciones ejecutadas en el periodo.		
	TAM: Total de Acciones planificadas para el período.		

Tabla 139 KPI Practica de Mejora

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

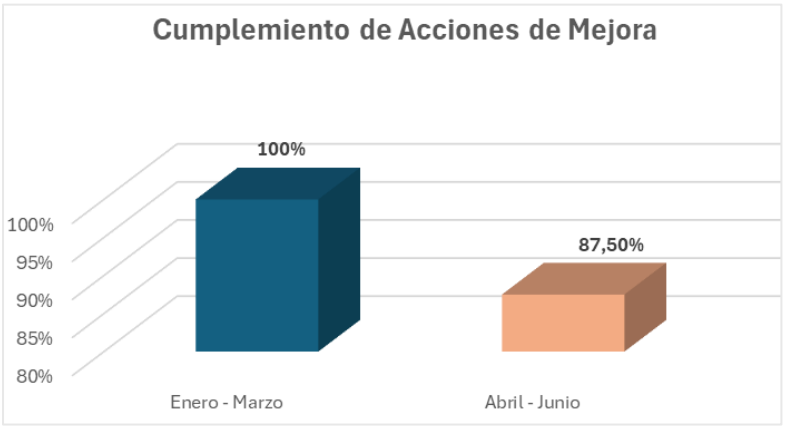


Ilustración 224 Resultado de Cumplimiento AM

La próxima medición se realizará para el mes de septiembre, lo cual se evidencia en la figura anterior el histórico del resultado del seguimiento de acciones de mejora de 2025.

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

SERVICIO/ PRÁCTICA	NOMBRE	DESCRIPCIÓN	¿MATERIALIZADO?	ACCIONES PARA REALIZAR
Mesa de servicios	Desborde de solicitudes (vía correo electrónico y/o llamadas) en la Mesa de Servicios	Aumento eventual de la cantidad de solicitudes que supera la capacidad de atención de los Agentes de la Mesa de servicios	NO	No se ha presentado desborde de solicitudes
Mesa de servicios	Riesgo de seguridad de la información que comprometan la confidencialidad, integridad o disponibilidad de la información.	Posibilidad de uso indebido de la cuenta genérica del cliente, asignada para la Mesa de servicios	NO	No se ha presentado dicha situación.
Soporte en sitio	Incumplimiento de los compromisos pactados por atención de actividades urgentes - no planeadas	Solicitud de realización de actividades urgentes no planeadas que afectan la prestación del servicio de acuerdo con lo planeado	NO	No se ha presentado dicha situación.
Todas las prácticas	Deficiencias en la adopción de las prácticas de ITIL	Resistencia a la adopción de las prácticas de ITIL por las partes interesadas	NO	Se proporcionó capacitación a los involucrados
Práctica de Activos	Posibilidad de pérdida de inventario	La pérdida de inventario se produce cuando las cantidades reales del inventario son inferiores a las registradas en el módulo de gestión	NO	Se realizó seguimiento con el equipo de trabajo para revisar los compromisos de la práctica
Todos	Ausencia del personal asignado	Ausencia del personal, encargado de gestionar, administrar y operar los servicios.	NO	El personal asignado estuvo disponible durante el periodo.
Todos	Indisponibilidad de la nube privada que afecte la prestación de servicios de TI	Falla en la prestación de los servicios de TI por falla en la infraestructura de TI provista por la UT	NO	Se dispuso de la infraestructura y recursos que soportan las estrategias de contingencia y recuperación. El suministro del servicio de energía eléctrica fue normal en los sitios alternos. 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	NO	Se dispuso de la infraestructura y recursos que soportan las estrategias de contingencia y

SERVICIO/ PRÁCTICA	NOMBRE	DESCRIPCIÓN	¿MATERIALIZADO?	ACCIONES PARA REALIZAR
		alojada en Datacenter Cirion Colombia XV		recuperación. El suministro del servicio de energía eléctrica fue normal en los sitios alternos. Se realización de copias de respaldo de las bases de datos, información y sistemas de información se realiza de acuerdo con la política institucional de copias de respaldo.
Servicios centrales Servicios en sede	Fallas en los servicios de TI que afecten las actividades de la entidad producto realizar cambios no programados	Presentación de incidentes en la infraestructura tecnológica	NO	Se cuenta con los procedimientos y documentación de la práctica para que los cambios se registren y ejecuten adecuadamente
SD -WAN	Falla en la infraestructura del servicio instalada en DC	Falla de uno o varios equipos que se encuentran provistos en el DC	NO	No se ha presentado dicha situación Se está trabajando en el cronograma de pruebas de disponibilidad de los diferentes servicios
LAN /WLAN	Falla en Switch Core / switch de borde	Indisponibilidad del servicio de conectividad por falla del switch core	NO	El servicio de conectividad ha estado disponible
Todos	Ausencia del personal asignado	Ausencia del personal, encargado de gestionar, administrar y operar los servicios.	NO	El personal asignado estuvo disponible durante el periodo.
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 140 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	169172	$23.684.080
	Subtotal	27.663.992

Tabla 141 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	99,37%	95,00%
	Tiempo de solución de incidentes por soporte en sitio	99,51%	90,00%
	Tiempo de solución de requerimientos por soporte en sitio	99,83%	90,00%
	Tiempo de respuesta de la mesa de servicio	98,95%	85,00%
	Abandono de llamadas	0,35%	Máximo 8,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Equipos de usuario final	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
ANTIVIRUS	Cobertura de antivirus	92,88%	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	99,99%	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	99,99%	99,90%
	Tiempo de solución de incidentes asociado a los servicios de administración, soporte y monitoreo	97,24%	90,00%
	Tiempo de solución de requerimientos asociado a los servicios de administración, soporte y monitoreo	99,86%	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%

Área	Nombre Indicador	Resultado	Meta
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Conectividad WAN e Internet	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Continuidad y disponibilidad del servicio de WAN en sedes nacionales con un solo enlace	(*)	99,60%
	Continuidad y disponibilidad del servicio de WAN en sedes nacionales con doble enlace (principal MPLS + secundario Internet dedicado)	(*)	99,90%
	Continuidad y disponibilidad del servicio de internet en Datacenter principal	100,00%	99,95%
	Continuidad y disponibilidad del servicio de internet en Datacenter alterno	100,00%	99,70%
	Continuidad y disponibilidad del servicio de WAN en Datacenter principal	100,00%	99,95%
	Continuidad y disponibilidad del servicio de WAN en Datacenter alterno	100,00%	99,95%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 142 Medición de Acuerdos de Niveles de Servicio agosto 2025

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

Novedades ANS MDS 4 y 5: El día 05/08/2025 a las 15:00:09 se presentó una llamada tipificada como *no atendida/abandonada*. Tras la validación correspondiente, se evidenció que la causa no fue atribuible a la Mesa de Servicios, sino a una intermitencia en la herramienta Numintec.
El fabricante, mediante el ID Ticket 28150471975, informó que la situación se originó por latencia en las troncales, lo cual impidió que la llamada ingresara al agente final de la Mesa de Servicios.
Por lo tanto, esta novedad no afecta el cumplimiento del ANS, ya que no corresponde a una falta de atención por parte de los agentes de Mesa.

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 Coordinador del Grupo de Soporte Informático dentro del tiempo comprometido.

9. ANEXOS

- Certificación_backup_servidores
- Consumo de cuotas agosto
- detalle_llamadas_recibidas_(01.08.2025-31.08.2025)
- Datos_Mintrabajo_agosto

FIN DEL DOCUMENTO