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

Septiembre de 2025

DOCUMENTO/ ARCHIVO	
Código:	**Informe Gestión - Unión Temporal Gestión TIC 2023**
Nombre Archivo:	**Informe Gestión - Unión Temporal Gestión TIC 2023 – Septiembre 2025**
Fecha:	8/10/2025
Versión:	1

REGISTRO DE CAMBIOS			
Versión	**Páginas**	**Fecha Modificación**	**Motivo del cambio**
1	202	08/10/2025	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 12
Objetivo 12
Alcance 12
Definición de Siglas y Expresiones Técnicas 13
1 GERENCIA Y/O ADMINISTRACIÓN 15
2 LÍNEA DE GESTIÓN DE SERVICIOS 15
2.1. Gestión del Servicio 15
2.1.2. Prácticas ITIL 4 20
2.1.2.1. Práctica Acuerdos Niveles de Servicio (ANS) 20
2.1.2.2. Práctica Habilitación de Cambios 21
2.1.2.3. Práctica Gestión de Activos 22
2.1.2.4. Práctica Catálogo de servicios 23
2.1.2.5. Práctica de Problemas 25
2.1.2.6. Práctica de Incidentes 26
2.1.2.7. Práctica de Requerimientos 32
2.1.2.8. Práctica de Eventos 36
2.1.2.9. Práctica de Disponibilidad 48
2.1.2.10. Práctica de Implementación 51
2.2 Mesa de Servicios y Soporte en Sitio 52
3 LINEA DE SERVICIOS CENTRALES 67
3.1 Datacenter 67
3.1.1 Datacenter Principal 67
3.1.2 Datacenter Alterno y DRP 78
3.1.3 Procesamiento, Almacenamiento y Respaldo 82
3.1.4 Aplicaciones Especializadas 87
3.1.5 No aplica 133
3.1.6 Seguridad Informática 133
3.1.6.1 Firewalls de nueva generación 133
3.1.6.2 Sandbox – Amenazas día 0 139
3.1.6.3 SIEM - Solución de correlación de eventos de seguridad, disponibilidad y recursos 142
3.1.6.4 WAF - Servicio de tipo “Firewall de Aplicaciones Web” 147
3.1.6.5 Solución de Anti-DDoS 149
3.1.6.6 Casos atendidos de los servicios de seguridad 150
3.1.6.7 Análisis de riesgo 151
3.1.6.8 Políticas y procedimiento de seguridad 153
3.1.7 Licenciamiento 154
3.1.8 Administración, soporte y monitoreo 154
3.2 No aplica 155
3.3 Conectividad WAN, SDWAN e Internet 155
3.3.1 Canales WAN 155
3.3.1.1 Incidentes de Conectividad 156
3.3.1.2 Topología Actual 157
3.3.2 Canales SDWAN e Internet Dedicado 157
4 LINEA DE SERVICIOS EN SEDE 161
4.1 Equipos de Cómputo de usuario final 161
4.1.1 Equipos de Escritorio 165
4.1.2 Equipos Portátiles 165
4.2 Conectividad LAN y WLAN 166
4.2.1 Switch CORE Sede Principal 168
4.2.2 Switch para conexiones perimetrales (EDGE) en sede principal 168
4.2.3 Switch de acceso 24 puertos 168
4.2.4 Switch de acceso 48 puertos 168
4.2.5 Puntos de Acceso 169
4.3 Telefonía IP 170
4.3.1 Teléfono Gama Media 170
4.3.2 Teléfono Gama Baja 171
4.3.3 Troncales SIP 172
4.3.4 No Aplica 172

4.3.5 No Aplica ... 172
4.3.6 Módems 4G – Con plan de 50 Gbps ... 172
4.4 Energía Regulada UPS ... 178
4.4.1 UPS 10 kVA ... 179
4.4.2 UPS 15 kVA ... 179
4.4.3 UPS 20 kVA ... 179
4.5 No aplica ... 181
4.6 Outsourcing de Impresión ... 181
4.6.1 No aplica ... 184
4.6.2 Multifuncional B/N rango medio – Cargo fijo mensual ... 184
4.6.3 Impresora Color rango medio – Cargo fijo mensual ... 184
4.6.4 No aplica ... 185
4.6.5 Multifuncional B/N rango medio – Clic de impresión ... 185
4.6.6 Impresora Color rango medio – Clic de impresión ... 185
4.7 Antivirus ... 186
4.7.1 Instalaciones de antivirus en servidores ... 186
4.7.2 Instalación de antivirus PCs usuarios final ... 186
4.7.3 Top 10 spyware ... 187
4.7.4 Top 10 Virus Detectados ... 188
4.7.5 Servicio de Vulnerabilidades ... 192
4.7.5.1 Inventario y licenciamiento ... 193
4.7.5.2 Escaneos programados ... 193
4.7.5.3 TOP 10 – Vulnerabilidades más explotables ... 194
4.7.5.4 Estrategia de remediación y/o mitigación ... 194
4.7.5.5 Resumen de mitigación efectuada ... 195
4.7.5.6 Ethical Hacking Segundo semestre 2025 ... 196
5 GESTIÓN DE CALIDAD DE INFORMACIÓN ... 197
5.1 Evaluación calidad documental de casos ... 197
5.2 Evaluación de calidad de llamadas ... 198
5.3 Práctica de Mejora ... 199
6 GESTION DE RIESGOS ... 201
7 BOLSA DE RECURSOS ... 204
8 MEDICIÓN DE ACUERDOS DE NIVEL DE SERVICIO ... 204
9 ANEXOS ... 206

Índice de Tablas

Tabla 1 Atención de solicitudes por Grupo de Especialista ... 18
Tabla 2 Disposición de residuos ... 18
Tabla 3 Tipificación de los cambios ... 21
Tabla 4 Medición Indicador Porcentaje de Cambios Exitosos ... 22
Tabla 5 KPI Práctica Catálogo de Servicios ... 25
Tabla 6 Consolidado problemas identificados ... 26
Tabla 7 Estados Incidentes ... 26
Tabla 8 Top 10 Incidentes ... 27
Tabla 9 Incidentes Suspendidos ... 28
Tabla 10 Incidentes Mayores ... 30
Tabla 11 Medición de KPIs ... 31
Tabla 12 Estados de Requerimientos ... 32
Tabla 13 Seguimiento del Backlog Suspendidos ... 33

Tabla 14 Top 10 de Solicitudes 34
Tabla 15 Detalle de KIP Practica de Requerimientos....34
Tabla 16 Casos reabiertos 36
Tabla 17 KPI Práctica de Eventos 37
Tabla 18 Consolidado disponibilidad de servidores 49
Tabla 19 Consolidado disponibilidad de Directorio Activo 49
Tabla 20 Desagregado de Disponibilidad Directorio Activo 49
Tabla 21 Consolidado disponibilidad de equipos Datacenter principal 49
Tabla 22 Desagregado de Disponibilidad Datacenter Principal 49
Tabla 23 Consolidado disponibilidad de equipos Datacenter alterno....50
Tabla 24 Desagregado Disponibilidad de equipos Datacenter alterno....50
Tabla 25 Consolidado disponibilidad de equipos redes y conectividad....50
Tabla 26 Consolidado disponibilidad de equipos de seguridad 50
Tabla 27 Disponibilidad de equipos Seguridad de la Información....50
Tabla 28 Consolidado disponibilidad de equipos de telefonía 51
Tabla 29 Consolidado disponibilidad de plataforma antivirus 51
Tabla 30 Llamadas Atendida por la Mesa de Servicio....53
Tabla 31 Casos anulados por Servicio 53
Tabla 32 Casos Suspendidos por Servicio 54
Tabla 33 Incidentes Solucionados por Soporte en Sitio 55
Tabla 34 Incidentes Solucionados por Soporte Territorial 56
Tabla 35 Requerimientos Solucionados por Mesa de Servicio....57
Tabla 36 Requerimientos Solucionados por Soporte en Sitio....58
Tabla 37 Requerimientos Solucionados por Territoriales 59
Tabla 38 Casos Cerrados por la Mesa de Servicios 61
Tabla 39 Casos Cerrados por Soporte en Sitio....63
Tabla 40 Top 10 Casos Cerrados por Soportes Territoriales....64
Tabla 41 Casos Atendidos usuarios VIPS 64
Tabla 42 Casos Atendidos usuarios 64
Tabla 43 Medios de Ingreso de Casos 64
Tabla 44 Visitas a Sedes sin Soporte 66
Tabla 45 Medición de ANS Mesa de servicios 67
Tabla 46 Capacidades contractuales....71
Tabla 47 Consumo de capacidad con servidores para desaprovisionar + ambientes de pruebas)..71

Tabla 48 Consumo de capacidad Sin servidores para desaprovisionar con ambientes de pruebas 71
Tabla 49 Consumo de capacidad Sin servidores para desaprovisionar sin ambientes de pruebas .71
Tabla 50 Consumo de capacidad Servidores Pruebas y Desarrollo 72
Tabla 51 Consumo de capacidad actual 72
Tabla 52 Maquinas desaprovisionadas propiedad de la entidad 87
Tabla 53 Suma Instancias 107
Tabla 54 Total Docs 107
Tabla 55 Total Radicados 107
Tabla 56 Dimensionamiento Servers IBM - Virtualización Optima 108
Tabla 57 Apps & DDBB Oracle 110
Tabla 58 Escenario de Capacidades Oracle - Estado de consumo Actual 111
Tabla 59 Escenario de Capacidades Oracle - Total de recursos empleados 111
Tabla 60 Tendencia de uso de ancho de banda 134
Tabla 61 usuarios con mayor consumo de ancho de banda 135
Tabla 62 Top de usuarios por sesiones 136
Tabla 63 Top de aplicaciones 137
Tabla 64 Consolidado de indicadores 138
Tabla 65 Tipos de incidentes 146
Tabla 66 Reporte de requerimientos septiembre 151
Tabla 67 Vulnerabilidades en la infraestructura 152
Tabla 68 Vulnerabilidades en la infraestructura 152
Tabla 69 ataques de phishing 152
Tabla 70 Licenciamiento 154
Tabla 71 Medición ANS Datacenter 155
Tabla 72 Medición ANS Nube Pública 155
Tabla 73 Incidentes de conectividad 157
Tabla 74 Medición de ANS Conectividad WAN e Internet 160
Tabla 75 Desagregado sedes con novedad un solo enlace 161
Tabla *76* Desagregado sedes con novedad con doble enlace 161
Tabla *77* Cantidades de equipos a distribuir a nivel nacional 161
Tabla 78 Cantidades de equipos asignados nivel nacional 162
Tabla 79 Cantidades de equipos por devolución nivel nacional 162
Tabla 80 Estado de casos de garantía. 162
Tabla 81 ANS casos de garantía. 163

Tabla 82 ANS Relación casos de garantía 163
Tabla 83 Equipos en siniestro 163
Tabla 84 *Avance instalación de equipos* 164
Tabla 85 Devolución de equipos 164
Tabla 86 cantidad de equipos 164
Tabla 87 Solicitudes de Equipos Usuario Final – Según Grupo Responsable 165
Tabla 88 Solicitudes de Equipos Usuario Final – Según Grupo Responsable 165
Tabla 89 Medición ANS Equipos de Usuario Final 166
Tabla 90 Top 5 de categorías en el Servicio de conectividad LAN-WLAN 167
Tabla 91 Distribución y Cantidades de switch 24 puertos 168
Tabla 92 Distribución y Cantidades de Switch 48 puertos 169
Tabla 93 Distribución de puntos de acceso 170
Tabla 94 Medición ANS LAN y WLAN 170
Tabla 95 Equipos gama media 171
Tabla 96 Sedes cerradas 171
Tabla 97 Consolidado de teléfonos gama baja 171
Tabla 98 Consolidado equipos MIFI 172
Tabla 99 Minutos, consumos 174
Tabla 100 Top 5 consumo de llamadas 175
Tabla 101 Top 5 llamadas LDI 175
Tabla 102 Top 5 llamadas Celular 176
Tabla 103 Top 5 llamadas locales 177
Tabla 104 Capacitaciones y divulgaciones 177
Tabla 105 Medición ANS Telefonía IP 178
Tabla 106 Inventario de UPS – 10kVA 179
Tabla 107 Inventario de UPS – 20Kva 180
Tabla 108 Medición ANS Energía Eléctrica UPS 180
Tabla 109 Inventario de impresoras para el servicio 181
Tabla 110 Consumo de impresiones por usuario - Impresoras B/N 182
Tabla 111Top 10 de impresoras con mayor uso 182
Tabla 112 Top usuarios impresión a color 183
Tabla 113 Top oficinas 183
Tabla 114 Top 10 impresoras más usadas del servicio de fotocopiado 183
Tabla 115 Ampliación de cuota de impresión 184

Tabla 116 Despacho de papel a sedes del Ministerio del Trabajo 184
Tabla 117 Cargo mensual multifuncional rango medio 184
Tabla 118 Cargo mensual impresora color 184
Tabla 119 Clics de impresión de septiembre 2025 – Multifuncional B/N 185
Tabla 120Tendencia de consumo de clics B/N 185
Tabla 121 Clics de Impresión de septiembre 2025 – Impresora Color 185
Tabla 122 Tendencia de consumo de clics color 185
Tabla 123 Medición ANS Outsourcing de Impresión 186
Tabla 124 Descripción de virus 189
Tabla 125 Top 5 Equipos 189
Tabla 126 Medición de ANS Antivirus 197
Tabla 127 Errores cometidos 198
Tabla 128 Resultado de criterios y parámetros - Calidad de llamadas 199
Tabla 129 KPI Practica de Mejora 200
Tabla 130 Gestión de riesgos 204
Tabla 131 Bolsa de Recursos 204
Tabla 132 Medición de Acuerdos de Niveles de Servicio septiembre 2025 205

Índice de Ilustraciones

Ilustración 1 Estado final de casos al corte del período 17
Ilustración 2 Creación de categorías 24
Ilustración 3 Socialización de categorías 24
Ilustración 4 Socialización actualización matriz de escalamiento 25
Ilustración 5 efectividad de resolución de incidentes 31
Ilustración 6 Porcentaje de incidentes abiertos 32
Ilustración 7 KPI Efectividad de Resolución de Requerimientos de Servicio 35
Ilustración 8 Requerimientos de Reabiertos en el periodo 35
Ilustración 9 Top de incidentes por sedes 38
Ilustración 10 Top de incidentes por sedes 39
Ilustración 11 eventos por sedes routers 40
Ilustración 12 Top de causas por sedes switches 40
Ilustración 13 Top de eventos por sedes Access point 41
Ilustración 14 Top de causas por sedes Access point 42
Ilustración 15 Top de eventos por sedes Starlink 42
Ilustración 16 Top de causas por sedes Starlink 43
Ilustración 17 Top de incidentes por sedes fortigate 44
Ilustración 18 Top de causas por sedes fortigate 44
Ilustración 19 Top de eventos windows 45
Ilustración 20 Top de servidores windows 46
Ilustración 21 Top de causas eventos linux 46
Ilustración 22 Top de servidores linux 47
Ilustración 23 Seguimiento Pruebas de Disponibilidad 51
Ilustración 24 Seguimiento Práctica Implementación 52

Ilustración 25 Llamadas Atendidas 53
Ilustración 26 Incidentes Solucionados por Soporte en Sitio 55
Ilustración 27 Incidentes Solucionados por Territoriales 56
Ilustración 28 Requerimientos Solucionados por Mesa de Servicio 57
Ilustración 29 Requerimientos Solucionados por Soporte en Sitio 58
Ilustración 30 Requerimientos Solucionados por Territoriales 59
Ilustración 31 Requerimientos Solucionados por Territoriales 61
Ilustración 32 Casos Cerrados por Soorte en Stio 63
Ilustración 33 *Requerimientos Solucionados por Territoriales* 65
Ilustración 34 Cumplimiento WSUS 68
Ilustración 35 Casos Win Servicio 69
Ilustración 36 Estado final de los casos Nube privada 70
Ilustración 37 Casos por categoría Nube privada y pública 70
Ilustración 38 Comportamiento SWCORE Datacenter Colombia XV 76
Ilustración 39 Sincronización HA de los Switch Core 77
Ilustración 40 Grafica de consumo canal Internet Datacenter 77
Ilustración 41 Captura de imagen máquinas virtuales 78
Ilustración 42 Escenario de pruebas Aplicaciones y AD 79
Ilustración 43 Extremo DC Bogotá 79
Ilustración 44 Extremo DC Cali 80
Ilustración 45 Estado canal de Internet DC Cali 80
Ilustración 46 Estado SWCORE Datacenter alterno 81
Ilustración 47 Estado HA SWCORE Datacenter alterno 81
Ilustración 48 Consumo canal MPLS DC Alterno 82
Ilustración 49 Estado Router MPLS DC Alterno 82
Ilustración 50 Casos App Servicio 89
Ilustración 51 Casos App Categoría 89
Ilustración 52 Tamaño Archivo Sindical 90
Ilustración 53 Tamaño IIS 91
Ilustración 54 Casos IBM Servicio 100
Ilustración 55 Casos IBM - categoría 100
Ilustración 56 Diagrama BP 101
Ilustración 57 Diagrama ODM 102
Ilustración 58 Diagrama WASND 102
Ilustración 59 Diagrama FileNet Front 103
Ilustración 60 Diagrama Datacap 103
Ilustración 61 Diagrama App Connect 104
Ilustración 62 Arquitectura Gestor Documental 104
Ilustración 63 Capacidades VM Gestor Documental 105
Ilustración 64 Licenciamiento Oracle 105
Ilustración 65 IBM Licenciamiento 106
Ilustración 66 Estado Bases de Datos 110
Ilustración 67 Información base de datos – Servidor 112
Ilustración 68 Estadísticas CPU 112
Ilustración 69 Estadísticas Memoria 112
Ilustración 70 Estadísticas Pool compartido 112
Ilustración 71 Tamaño DDBB 113
Ilustración 72 Tamaño Esquema DDBB 113
Ilustración 73 Rendimiento DDBB 113
Ilustración 74 DDBB por Server 114
Ilustración 75 Host e Instancia CPU 114
Ilustración 76 Estadísticas Memoria 114
Ilustración 77 Estadística Shared Pool 114
Ilustración 78 Tamaño DDBB DBMINTRA 115
Ilustración 79 Tamaño Esquema DDBB 115
Ilustración 80 Rendimiento DDBB MINTRASG 115

Ilustración 81 Información DDBB PLIFERAY....116
Ilustración 82 Host e Instancia CPU....116
Ilustración 83 Estadísticas Memoria....116
Ilustración 84 Estadísticas Shared Pool....116
Ilustración 85 Tamaño DDBB PLifeRay....116
Ilustración 86 Tamaño Esquemas DDBB....117
Ilustración 87 Rendimiento DDBB PlifeRay....117
Ilustración 88 Información DDBB SIGEP....118
Ilustración 89 Estadística Host e Instancia....118
Ilustración 90 Estadística Memoria....118
Ilustración 91 Estadística Shared Pool....118
Ilustración 92 Tamaño DDBB SIGEP....119
Ilustración 93 Tamaño Esquema DDBB....119
Ilustración 94 Rendimiento DDBB SIGEP....119
Ilustración 95 Información DDBB DBSIMPC....120
Ilustración 96 Estadística CPU....120
Ilustración 97 Estadística Memoria....120
Ilustración 98 Estadística Shared Pool....121
Ilustración 99 Tamaño DDBB SIMPC....121
Ilustración 100 Tamaño Esquema DDBB....121
Ilustración 101 Rendimiento DDBB....121
Ilustración 102 Información servidor DBBB....122
Ilustración 103 Host e Instancia CPU....122
Ilustración 104 Estadística memoria....122
Ilustración 105 Estadística Shared Pool....123
Ilustración 106 Tamaño DDBB MINTRASD....123
Ilustración 107 Tamaño Esquemas....123
Ilustración 108 Rendimiento MINTRASD....124
Ilustración 109 Información Server DDBB....124
Ilustración 110 Host e Instancia CPU....124
Ilustración 111 Estadística Memoria....125
Ilustración 176 Estadística Shared Pool....125
Ilustración 113 Tamaño DDBB....125
Ilustración 114 Tamaño DDBB....125
Ilustración 115 Rendimiento DDBB....126
Ilustración 116 Información Server DDBB....126
Ilustración 117 Host e Instancia CPU....127
Ilustración 118 Estadística Memoria....127
Ilustración 119 Estadística Shared Pool....127
Ilustración 120 Tamaño DDBB....127
Ilustración 121 Tamaño Esquemas DDBB....128
Ilustración 122 Rendimiento DDBB....128
Ilustración 123 Información Server DDBB....129
Ilustración 124 Estadística CPU....129
Ilustración 125 Estadística Memoria....129
Ilustración 126 Estadística Shared Pool....130
Ilustración 127 Tamaño Esquemas DDBB....130
Ilustración 128 Comportamiento DDBB....131
Ilustración 129 Almacenamiento ASM....131
Ilustración 130 DiskGroup Data....131
Ilustración 131 DiskGroup Flash....132
Ilustración 132 DiskGroup Reco....132
Ilustración 133 DiskGroup Redo....132
Ilustración 134 Licenciamiento adicional componente IBM....132
Ilustración 135 Firewall de nueva generación.....133
Ilustración 136 Comportamiento ancho de banda....134

Ilustración 137 Tendencia de uso de ancho de banda....135
Ilustración 138 Top de usuarios por números de sesiones....136
Ilustración 139 Top de aplicaciones....137
Ilustración 140 Top de Autenticación....138
Ilustración 141 sesiones fallidas....139
Ilustración 142 Reporte mensual septiembre....140
Ilustración 143 Captura de pantalla perfomance....141
Ilustración 144 licencia sandbox....141
Ilustración 145 licencia sandbox....142
Ilustración 146 Detalle de latencia o errores....143
Ilustración 147 detalle de problemas en servicios....143
Ilustración 148 Detalle casos de uso....144
Ilustración 149 Detalle de alertas....144
Ilustración 150 Detalle de alertas....145
Ilustración 151 Detalle de incidentes....145
Ilustración 152 Detalle servidores....146
Ilustración 153 Detalle fortigate....147
Ilustración 154Top attack types....148
Ilustración 155 Top de ataques....149
Ilustración 156 Políticas y procedimientos....153
Ilustración 157 Consumo canal MPLS DC Principal....156
Ilustración 158 Estado Router MPLS DC Principal....156
Ilustración 159 Topología actualizada....157
Ilustración 160 Interface Fortimanager....158
Ilustración 161 Interface MPLS HUB SDWAN....158
Ilustración 162 Interface Internet HUB SDWAN....158
Ilustración 163 VPN SDWAN establecidas....159
Ilustración 164 Estado HUB SDWAN Datacenter....159
Ilustración 165 Estado HA HUB Sdwan....159
Ilustración 166 Recursos Fortimanager....160
Ilustración 167 Estado de casos Redes y Conectividad....167
Ilustración 168 Asignación de licencias....173
Ilustración 169 Comportamiento de tráfico....174
Ilustración 170 Top llamadas nacionales....174
Ilustración 171 llamada internacional de prueba....175
Ilustración 172 Top Celular....176
Ilustración 173 Top Local....176
Ilustración 174 Requerimientos por garantía....177
Ilustración 175 Disponibilidad y Continuidad TOIP....178
Ilustración 176 Equipos consola antivirus....186
Ilustración 177 Gestión consola antivirus – equipos usuario final....187
Ilustración 178 Top spayware....188
Ilustración 179 Top 10 virus detectado....188
Ilustración 180 HUPGGARCIAO....190
Ilustración 181 BOPDZARATE....190
Ilustración 182 CQDYMONTILLAG....190
Ilustración 183 BOPLSALAMANCAP....191
Ilustración 184 CNDDQUEVEDO....191
Ilustración 185 Eventos Ransomware....192
Ilustración 186 captura eventos ransonware....192
Ilustración 187 *Gestión consola Nessus*....193
Ilustración 188 *Escaneos programados*....194
Ilustración 189 TOP 10 - Activos más explotables....194
Ilustración 190 Vulnerabilidades gestionadas vs en remediación....195
Ilustración 191 captura envío de correo gestión de vulnerabilidades....196
Ilustración 192 Cronograma Ethical Hacking....196

Ilustración 193 Resultados auditoria de casos....198
Ilustración 194 Resultado de criterios y parámetros - Calidad de llamadas....199
Ilustración 195 Seguimiento Práctica Mejora....200
Ilustración 196 Resultado de Cumplimiento AM....201

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 septiembre 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 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 SVE, Pagina WEB, SICIP, DBSIMPC-SIGEP), Conectividad de Red, mantenimiento de UPS Piso 22 en Nivel Central.

- Información de interés sobre **correo malicioso recibido en cuentas del dominio de la entidad** y el modo de proceder. Esta información se divulgó a través de la cuenta de SoporteMT y de fondo de pantalla en equipos institucionales:



¡INFORMACION
IMPORTANTE CORRE

- 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.



¡INFORMACIÓN
IMPORTANTE CONTR

- **Canales de atención** disponibles para comunicarse con la **Mesa de Servicios** del Grupo de Soporte Informático.
- El 10/09/2025 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 el **Procedimiento de Incidentes de Seguridad Digital**.



Solicitud Fondo de
Pantalla.msg

- 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:
Divulgación de las piezas propuestas actualizadas para dar a conocer a los usuarios finales los lineamientos de OneDrive para que 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. 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 septiembre 2025 se registraron en la herramienta ITSM 7372 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: 6541
  - Incidentes: 807
  - Cambios: 24
  - Problemas: 0
- Casos Anulados: 6 - 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 septiembre 2025:

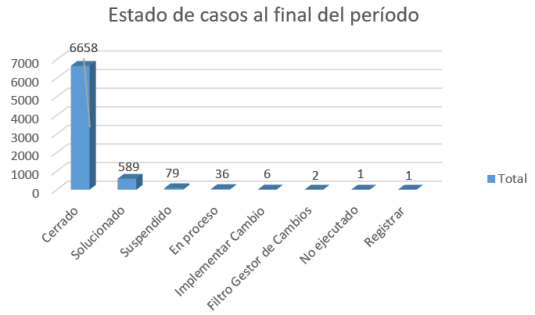


Ilustración 1 Estado final de casos al corte del período

- Gestión por parte de los grupos de especialistas:

Grupo Responsable	Cantidad de casos gestionados	Porcentaje (%)
Responsable_Soporte_Territoriales	2750	37,30
Responsable_Soporte_Bogota	1836	24,91
Responsable_Mesa_De_Servicio	785	10,65
Responsable_Soporte_Impresoras	701	9,51
Especialistas_IBM	484	6,57
NOC	428	5,81
Especialista_Telefonía_IP	69	0,94
Responsable_De_Servidores_Windows	69	0,94
Especialista Nube Privada	52	0,71
SOC	52	0,71
Especialista Herramientas de Gestion	42	0,57
Especialista Base de datos	28	0,38
Especialista Redes	23	0,31
Responsable Garantías Equipos	16	0,22
Especialista Nube Publica	10	0,14
Almacenamiento y Backups	8	0,11
Especialista Aplicaciones .Net	7	0,09
Liferay	3	0,04
Responsable_de_Energia Electrica Regulada - UPS	3	0,04

Gestión del Servicio	3	0,04
Gestor de Inventarios	3	0,04
TOTAL	**7372**	**100,0**

Tabla 1 Atención de solicitudes por Grupo de Especialista

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 se gestionó recolección de residuos por parte del proveedor SUMA Desarrollo Ambiental para la DT Atlántico el 9/09/2025. Los residuos y cantidades se relacionan a continuación:

Residuos	Unidades
Cartuchos y tóner de impresoras de oficina	45
Unidades de Imagen - RAEE	4

Tabla 2 Disposición de residuos

f. Implementación IPV6

Durante el periodo, LACNIC confirmó que aún no han recibido los documentos, en seguimiento con el Grupo de Gestión Documental para validar procedimiento de rastreo de guía internacional.

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 realizó 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.
- 19/09/2025: El equipo de procesos realizó sesión de reinducción de Gestión de Activos al equipo de soportes de territorio vía Microsoft Teams. Definición de activos, CMDB, manejo de estados en Aranda, lineamientos, software no permitido, flujo del proceso, relación con otras prácticas Itil, instructivos asociados, nuevos formatos a utilizar.
- El 22/09/2025 el equipo de procesos luego de la sesión de socialización de la Práctica de Activos realizó envío vía correo electrónico de los formatos de Asignación, Devolución y Checklist de equipos, con el fin de estandarizar y controlar el proceso de gestión de activos, asegurando la trazabilidad desde la asignación

hasta la devolución, así como la verificación del estado de los equipos mediante el checklist correspondiente.

- El 18, 19, 25 de septiembre el equipo de procesos realizó refuerzo al equipo de MDS, SS y especialistas asociado con la correcta tipificación y categorización de Incidentes y Requerimientos en Aranda, con ejemplos claros y reales de errores comunes y cómo corregirlos. Refuerzo en temas de calidad documental y ortografía, manejo de estados, ANS.
- El 24/09/2025 el equipo de procesos envió a todo el equipo de trabajo los Lineamientos de la Generación de Casos en Aranda para la devolución de equipos (Mesa de Servicio y Soporte en Sitio).

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 gestionaron los permisos de acceso y autorización de salida, se aclara que esta actividad continuará para el siguiente período: Delcop: 1 sede.
- Se realizó sesión virtual con personal de ETB para iniciar proceso de retiro de elementos de conectividad que aún se encuentran en instalaciones del ministerio. Se acuerda flujo de trabajo para verificación de inventario, gestión de notificación a cliente y atención de la orden de trabajo por parte de ETB.
- El Coordinador del Grupo de Soporte Informático brindó el 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. Se está revisando desde que buzón se enviará la encuesta.
- Se reitera 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.
- Se finalizó el proceso de delegación al personal de MDS la actividad para realizar la búsqueda y exportación de información de una cuenta de usuario en eDiscovery, estas solicitudes están siendo atendidas y resueltas en primer y segundo nivel sin necesidad de realizar un escalamiento a especialistas de Windows. La delegación incluyó la generación y socialización de un instructivo con las actividades a desarrollar y la definición de los flujos de trabajo según los escenarios posibles.
- Se reitera novedad escalada al Coordinador del Grupo de Soporte Informático relacionada con 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 apoyo para que la dependencia responsable de este equipo pueda emitir una respuesta formal a la directora de la OE con el propósito de oficializar las acciones que se desarrollarían para esta UPS.
- 17, 18 y 19 de septiembre la UT apoyó a la Oficina TIC en la auditoría interna del estándar ISO27001: 2022 – Control 8, en las sesiones donde están involucrados los

servicios de TI a cargo de la UT y entrega de evidencias correspondientes. Esta auditoria estuvo a cargo de la empresa FiveStrategy.

- Se gestionó la creación del flujo para solicitudes de habilitación de puertos USB con las siguientes actividades:
  - El 24/09/2025 se recibió correo electrónico de Oficina TICs solicitando divulgación de fondo de pantalla y pieza desde Soporte MT para divulgación de que **a partir del 1 de octubre se bloquearán los puertos USB** en los equipos del nivel central del Ministerio del Trabajo para el uso de dispositivos de almacenamiento externo.
  - 24/09/2025: Desde la línea de Gestión de Servicios y el Equipo de Procesos se realizó la creación del flujo, parametrización en la herramienta de gestión.
  - Presentación al Coordinador del Grupo de Soporte Informático, configuración de Aranda para la gestión de solicitudes en Aranda
  - 25/09/2025: Socialización del flujo al equipo de mesa, SOC, SS Territorio y Bogotá, Oficina TIC.
  - Se realizó afinamiento de notas en el flujo
  - Se replicó por correo con todos los interesados y se inició operación desde el 29/09/2025.

2.1.1. Herramienta de Gestión ITSM

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

- Se realizó el aumento de los procesos de pingers que permite que Zabbix pueda realizar todas las solicitudes de ping a los hosts monitoreados
- Se realizó el aumento de los procesos de Unreachable que permite que Zabbix pueda realizar verificaciones adicionales cuando un host deja de responder a ping a los hosts monitoreados
- Se configuró el monitoreo a nuevos servidores Linux, dentro de su configuración está el agente ZBX y las métricas básicas.
- Se realizó la creación de categorías para la tipificación de casos y ajustes en las categorías para evitar que categorías de otros tipos de casos se mezclen.
- Se realizó la creación de un ANS de 84 horas.
- Se reconfiguraron las categorías para la toma de nuevos ANS.
- Se realizó la configuración de categorías para evitar que se puedan seleccionar categorías padres al crear casos.
- Se realizó la creación de la categoría routers en la CMDB junto con su flujo de estados.

2.1.2. Prácticas ITIL 4

2.1.2.1. Práctica Acuerdos Niveles de Servicio (ANS)

Dar a conocer las actividades de la Práctica Acuerdos Niveles de Servicios correspondientes al periodo del 1 al 30 de septiembre de 2025. Este apartado contiene información relevante sobre actividades realizadas y novedades presentadas.
Durante el periodo, se realizó seguimiento y control a los ANS que se tienen parametrizados en la herramienta, y con cada uno de los líderes de servicio, validando su cumplimiento de

acuerdo con lo definido contractualmente. Ver Numeral 7. MEDICIÓN DE ACUERDOS DE NIVEL DE SERVICIO.

2.1.2.2. Práctica Habilitación de Cambios

Dar a conocer las actividades de la Práctica Habilitación de Cambios correspondientes al periodo del 1 al 30 de septiembre de 2025. Este apartado contiene información relevante sobre actividades realizadas y novedades presentadas.

- **Tipificación de los cambios**

Durante el mes de septiembre de 2025 se gestionaron 24 casos tipificados como Cambios, clasificados en las siguientes categorías:

Servicio	No	Porcentaje
Administración de Bases de Datos.Servidor de base de datos	7	29,17%
Administración de servidores.Servidores	7	29,17%
Aplicaciones Especializadas.Portal Web	2	8,33%
Herramientas de Gestión.Aranda	2	8,33%
Aplicaciones Especializadas.SICIP	1	4,17%
AplicacionesEspecializadas.Aplicaciones especializadas	1	4,17%
Energía Eléctrica Regulada - UPS	1	4,17%
Redes y Conectividad.Implementacion AP	1	4,17%
Redes y Conectividad.Servicio SDWAN	1	4,17%
Telefonía IP.Infraestructura de telefonia	1	4,17%
Total	**24**	**100%**

Tabla 3 Tipificación de los cambios

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

- **Relación casos registrados**

A continuación, se presenta la relación de casos registrados del 1 al 30 de septiembre de 2025, en total se crearon 24 casos de los cuales se gestionaron 13 como cambios de normales y 11 cambios estándar:

- **Cambios por estado**

Al corte del 30 de septiembre, quince (15) casos quedaron estado Cerrado, dos (2) en estado filtro gestor de cambios, seis (6) en implementar cambio y un (1) caso quedo en No ejecutado.

- **Medición Indicador Porcentaje de Cambios Exitosos**

Nombre	Descripción / Fórmula	Meta	Periodicidad	Resultado Septiembre

Porcentaje de cambios exitosos.	**PCE = (NCE/TCI)*100** Donde: **PCE:** Precisión **NCE:** Numero de Cambios Exitosos **TCI:** Total de Cambios implementados	80%	Mensual	PCE: 23/24*100 PCE: 95.83%

Tabla 4 Medición Indicador Porcentaje de Cambios Exitosos

Durante el mes de septiembre de 2025 se presentó un (1) cambio no ejecutado correspondiente al RFC-148753 – Redes y Conectividad (Implementación AP), cuyo motivo fue la inasistencia del proveedor a la sesión programada para realizar las pruebas de conmutación. Como acción correctiva, se definió la reprogramación de la actividad con el fin de garantizar la validación del canal MPLS y su enlace de respaldo.
El indicador **Porcentaje de Cambios Exitosos (PCE)** alcanzó un resultado de **95,83%**, superando la meta establecida del 80%. Este comportamiento refleja la adecuada gestión de la práctica de Habilitación de Cambios, evidenciando una alta efectividad en la planeación y ejecución de las solicitudes registradas durante el periodo.

2.1.2.3. Práctica Gestión de Activos

Durante septiembre de 2025, la Práctica de Gestión de Activos ejecutó diversas acciones 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.

- Gestión de Software

Se elaboró el Plan de Trabajo para la Gestión de Software, en cumplimiento de lo solicitado en el marco de la Auditoría Interna ISO27001 – Control 8 (2022). Dicho plan tiene como objetivo definir y formalizar las actividades, procedimientos y responsabilidades relacionadas con la gestión de software, asegurando el control de los activos de información y la seguridad de la organización.

La propuesta incluye:
- Clasificación del software (permitido / no permitido).
- Procedimientos de gestión ante la detección o solicitud de nuevo software.
- Registro y clasificación en la herramienta ITSM.
- Gestión de actualizaciones de software.

Los responsables claves definidos son:
- Práctica de Activos: Identificación, clasificación y control.
- Práctica de Requerimientos: Definición de flujos y documentación.
- Mesa de Servicios: Gestión de solicitudes e instalación.
- SOC: Concepto de seguridad.
- Oficina TICs: Coordinación, revisión y aprobación.
- Próximos pasos establecidos:
- Socializar el borrador del plan con la Oficina TICs.
- Ajustar según comentarios recibidos.
- Iniciar la ejecución conforme al cronograma aprobado.

- Socialización de la gestión de activos

Se adelantó la socialización de la gestión de activos, dirigida a los equipos de soporte a nivel central y territorial, con el fin de reforzar los lineamientos establecidos y garantizar la correcta administración de los recursos tecnológicos.

- Conexión remota a través de Aranda

Se ejecutaron pruebas en la herramienta Aranda y se programó la socialización de la conexión remota, orientada a informar al equipo de trabajo y estandarizar su uso. La actividad contempla la realización de capacitaciones dirigidas tanto al personal de territorio como al nivel central, asegurando la adopción homogénea de la plataforma en los procesos de soporte y gestión remota.

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:
Durante el mes de septiembre se llevaron a cabo sesiones presenciales de refuerzo y capacitación por equipos, en las cuales se abordaron los siguientes temas: categorización, matriz de escalamiento, tipificación, cumplimiento de ANS, documentación de apertura y cierre, validaciones de primer nivel, reapertura de tickets, notificaciones desde la herramienta Aranda y encuestas de satisfacción.
En cada sesión se realizaron ejercicios prácticos, se evaluaron los temas tratados y se resolvieron las dudas planteadas por los participantes, con el objetivo de fortalecer las buenas prácticas en la gestión de casos.

- **Creación de Nuevas Categorías**

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

Creación Antivirus – Actualización



Creación SISINFO-Asesoría-Consulta

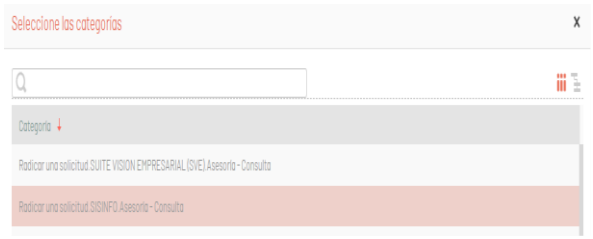


Ilustración 2 Creación de categorías

En conjunto con la práctica de ANS y Requerimientos y el líder de Herramientas, se revisó y actualizó el catálogo de servicios conforme a las necesidades operativas. De igual forma, se ajustaron los ANS según lo establecido contractualmente y se reflejaron dichos cambios en la herramienta Aranda. Así mismo, se socializó con todo el equipo mediante correo y sesiones cortas.

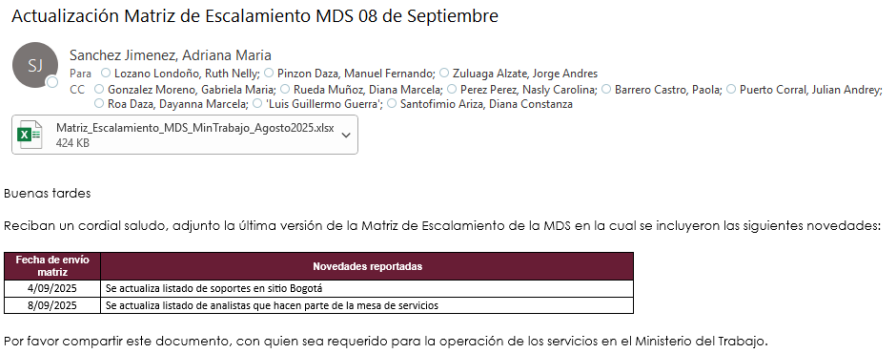


Ilustración 3 Socialización de categorías

Se realizó la actualización de los grupos resolutores en Aranda, incluyendo la revisión y ajuste de sus integrantes, de acuerdo con los movimientos internos y cambios operativos.

Matriz de Escalamiento

Se realizó actualización de la matriz de escalamiento y se socializó con todo el equipo informando los cambios ejecutados.



Actualización Matriz de Escalamiento MDS 08 de Septiembre

Sanchez Jimenez, Adriana Maria
Para Lozano Londoño, Ruth Nelly; Pinzon Daza, Manuel Fernando; Zuluaga Alzate, Jorge Andres
CC Gonzalez Moreno, Gabriela Maria; Rueda Muñoz, Diana Marcela; Perez Perez, Nasly Carolina; Barrero Castro, Paola; Puerto Corral, Julian Andrey; Roa Daza, Dayanna Marcela; 'Luis Guillermo Guerra'; Santofimio Ariza, Diana Constanza

Matriz_Escalamiento_MDS_MinTrabajo_Agosto2025.xlsx
424 KB

Buenas tardes

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

Fecha de envío matriz	Novedades reportadas
4/09/2025	Se actualiza listado de soportes en sitio Bogotá
8/09/2025	Se actualiza listado de analistas que hacen parte de la mesa de servicios

Por favor compartir este documento, con quien sea requerido para la operación de los servicios en el Ministerio del Trabajo.

Ilustración 4 Socialización actualización matriz de escalamiento

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 Septiembre
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= (4/4)*100 EF= 100%

Tabla 5 KPI Práctica Catálogo de Servicios

2.1.2.5. Práctica de Problemas

Dar a conocer las actividades de la Práctica de Problemas correspondientes al periodo del 1 al 30 de septiembre 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 6 Consolidado problemas identificados

Durante el mes de septiembre se realizó seguimiento al caso 137015 asociado con el Gestor Documental
Avances: Frente al servidor actual se ha realizado monitoreo del comportamiento del servidor y se evidencia estabilidad del servidor y de los servicios asociados al gestor documental.
Frente a la configuración del servidor nuevo se están realizando sesiones de trabajo con IBM con el propósito de diagnosticar la aplicación del gestor documental e identificar posibles ajustes a la configuración de las versiones que soportan la aplicación.

2.1.2.6. Práctica de Incidentes

Este apartado presenta un resumen de las actividades realizadas en el marco de la Práctica de Incidentes durante el periodo comprendido entre el 1 y el 30 de septiembre de 2025. Se incluye información relevante sobre los incidentes registrados, las acciones ejecutadas y las novedades ocurridas.

Durante el período del informe, se registraron 807 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	Cuenta de Estado
Cerrado	724
Solucionado	67
Suspendido	14
En proceso	2
Total general	**807**

Tabla 7 Estados Incidentes

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

Estado	Cuenta de Jerarquía	Observaciones
Reportar una falla.Alarma Zabbix.Router	225	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	91	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	79	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.Falla impresora.No imprime	44	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.Falla impresora.Atasco	38	Novedades por atasco de papel en el mecanismo de alimentación de las bandejas de las impresoras
Reportar una falla.Gestor Documental.Falla radicacion	37	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.Gestor Documental.Falla Funcional	35	
Reportar una falla.Alarma Zabbix.AP	26	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.Equipo de computo.Falla - Error conexión a red	22	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, desconexión de cable LAN y problemas con controladores.
Reportar una falla.Aplicaciones Office 365.Envio y recepción de correos	17	Novedades debido a actualizaciones del navegador, vencimiento de contraseñas, información guardada en caché. Etc.

Tabla 8 Top 10 Incidentes

- **Casos Suspendidos**

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

Etiquetas de fila	junio	agosto	septiembre	Total general
Especialistas_IBM			2	2
Especialista Redes			2	1
Responsable_Soporte_Impresoras	1			1
Responsable Garantías Equipos			1	1
Especialista_Telefonía_IP			1	1
Responsable_Soporte_Territoriales			1	1
Especialista Aplicaciones .Net		1		1
NOC			8	8
Nube Privada			1	1
Total general	**1**	**1**	**16**	**17**

Tabla 9 Incidentes Suspendidos

Durante el período comprendido entre junio y septiembre se registraron 17 incidentes suspendidos, septiembre (16 casos), lo que representa más del 90% del total.
El grupo NOC concentró la mayor cantidad de suspensiones con 8 casos los cuales corresponden a tickets escalados al proveedor de telecomunicaciones, equivalente al 47% del total. Le siguen los grupos Especialistas IBM, Especialista Redes, Responsable Soporte Impresoras, Responsable Garantías Equipos, Especialista Telefonía IP, Responsable Soporte Territoriales, Especialista Aplicaciones .Net y Nube Privada, cada uno con 1 caso a cierre del mes de medición.
Durante el período algunos casos permanecen en estado suspendido, ya que corresponden a los procesos de evaluación y diagnóstico con el cliente, especialistas y proveedores.

- **Incidentes Mayores**

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

Ticket arada	Servicio afectado	Novedad	Causa raíz	Acciones realizadas para restablecer el servicio	Afectación de usuarios	Estado aranda	Fecha inicio	Fecha fin	Tiempo de indisponibilidad
IM-146838	**Internet**	Falla masiva Zona Sur Occidental	Aperturas en los BB Primarios de los siguientes tramos: Neiva-Pasto, Neiva-Mocoa y Florencia-Mocoa (Tramo: Villa Garzón - El Juano). Popayán-Yumbo y Popayán-Manizales (Tramo: Jamundí - Suárez). Popayán-Neiva (Tramo: Popayán - Pital).	Le informamos que la interrupción de servicio reportada como una caída ha sido resuelta. La falla se debió a una saturación en nuestra red en los departamentos del sur occidente del país. Causa de la falla: La saturación fue provocada por una serie de aperturas en los BB Primarios de los siguientes tramos: Neiva-Pasto, Neiva-Mocoa y Florencia-Mocoa (Tramo: Villa Garzón - El Juano). Popayán-Yumbo y Popayán-Manizales (Tramo: Jamundí - Suárez). Popayán-Neiva (Tramo: Popayán - Pital). El diagnóstico principal del incidente fue un corte en la red ocasionado por trabajos de terceros, específicamente en el tramo Jamundí-Suarez. Solución aplicada: Para resolver la incidencia, nuestro personal técnico recuperó la reserva de fibra afectada y procedió a la instalación de una …	Mocoa, orito, Pasto, Guapi, Puerto Asis, Tuquerres, Unión, Mocoa	Cerrado	3/09/2025	3/09/2025	4 hr 37 min

				(continúa igual que en el primer correo). Solución aplicada: Para resolver la incidencia, nuestro personal técnico recuperó la reserva de fibra afectada y procedió a la instalación de una caja de empalme en el punto del corte. Estado del servicio: La falla fue superada y el servicio se restableció por completo a las 13:28 del 03/09/2025.					
IM-148844	**Internet**	Apertura Incidente Mayor Sin Internet Cll 32	Corte en la red de fibra óptica en la Calle 34, con aperturas adicionales en distintos tramos, lo que generó degradación y posterior indisponibilidad del servicio	Reparación de las aperturas en la fibra óptica. Mediciones de potencia y trazas para ubicar puntos de afectación. Validación de niveles de señal en central. Reinicio de puerto en central para estabilización del servicio. Confirmación final de normalización mediante pruebas de conectividad (Ping WAN).	Ususarios Calle 32	Cerrado	10/09/2025	15/09/2025	5 dias
IM-152345	**Internet**	Incidente Mayor Sin internet Zona Norte	se presentó apertura de fibra del tramo CAUCASIA - SALITRAL y equipo aislado de CHIQUINQUIRÁ que abre el camino hacia ZIPAQUIRÁ, estos tramos son las rutas principal y protección para las tgs reportadas de nogales.	por parte del back office de huawei se modificó el enrutamiento y pasarlo al camino por san carlos con lo cual se suben las tgs.	Barranquilla, fundación, chiriguana, fonseca, palto, cienaga, barrancas, sahagun, planeta rica, lorica, montelibano, cerete, la jagua, Agustin codazzi, san marcos, copey, bosconia magangue, baranoa, carme de bolibar, tolu, rioacha, valledupar	Cerrado	24/09/2025	24/09/2025	25 minutos
IM-152650	**Internet**	Incidente Mayor Sin internet departamentos de Caquetá y Putumayo	Corte de fibra por vandalismo	Se solventa apertura del enlace San Jose de Fragua – Mocoa; causando caída de BB Primario Neiva – Mocoa, Neiva –	Florencia Doncello Puerto asís Doncello Orito	Cerrado	24/09/2025	25/09/2025	17 h 48 min

				Pasto, Florencia – Mocoa; Se pierde gestión de los dwdm de Florencia, y San Jose de Fragua; BB Secundario Mocoa – Puerto Caycedo; afectando los nodos de Puerto Caycedo, Orito, Valle de Guamuez, San Miguel, Puerto Asis, Morelia, Valparaiso, Solita, Belen de los Andaquies, Albania, San Jose de Fragua, Curillo, La Montañita, Milan, Solano, El Paujil, Cartagena de Chaira, El Doncello, Puerto Rico, San Vicente del Caguan. Se confirma servicio operativo					
IM-153080	**Internet**	Falla con el Servicio de Internet zona central país	apertura en la fibra a 4515 metros, troncal 70685 hilos 3 y 4 daño	el personal técnico realizó mediciones en la central evidenciando apertura en la fibra a 4515 metros, troncal 70685 hilos 3 y 4 daño. El personal de correctivo informa que se ubica cable vandalizado en la avenida 68 # 4b-22. Se observan los equipos operativos, luego de las labores realizadas por el personal de correctivo	Router_Espinal Router_Ibague Router_Neiva Router_Popayan Router_Orito RInternet_ETB_Ibague Router_Guapi	Cerrado	26/09/2025	26/09/2025	4 h 48 min

Tabla 10 Incidentes Mayores

- **Otras Actividades**

  - Se realizó seguimiento a incidentes en backlog, para la documentación y cierre de casos pendientes de gestión.
  - Desde la gestión ITIL se realizaron auditorias de casos en los que se ha evidenciado oportunidades de mejora, las cuales son compartidas mediante correo a los especialistas a quienes se les realiza retroalimentación, con base a las novedades encontradas en cada caso.
  - Se realizó refuerzo de la gestión de incidentes y requerimientos a todo el equipo de manera presencial en la que se trataron temas relacionados a la categorización, definición de incidentes y requerimientos, tipificación, validaciones de primer nivel, documentación de apertura y cierre, seguimiento y gestión de casos en backlog.

De acuerdo con lo definido en la Guía Operacional de la Práctica de Incidentes, se establecieron los siguientes Indicadores (KPI), con el fin de establecer métricas que apoyen a la operación de los servicios TI:

Nombre	Descripción / Fórmula	Meta	Periodicidad	Resultado Septiembre

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=789/807*100 EF= 97,7%
Porcentaje de Incidentes Reabiertos en el Periodo	RRP: Porcentaje de casos Reabiertos en el periodo. IFS: Incidentes solucionadas en el período. IFR: Incidentes Reabiertos en el período.	<2%	Mensual	RRP= 0/791*100 RRP= 0%

Tabla 11 Medición de KPIs

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

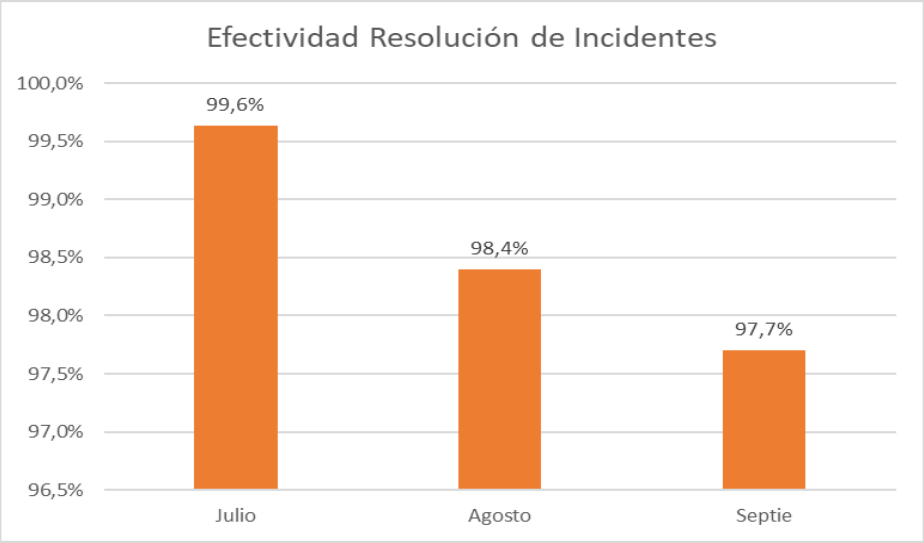


Ilustración 5 efectividad de resolución de incidentes

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

- Julio: 99,6%
- Agosto: 98.4%
- Septiembre: 97.7%

Se evidenció disminución en el valor del KPI debido a la afectación del ANS en 2 de los 789 casos que fueron solucionados, es importante mencionar que el cálculo mensual depende de la cantidad de incidentes reportados en la herramienta de gestión durante cada mes, el desempeño sigue siendo satisfactorio. Como parte de la gestión de la práctica, se realizó retroalimentación con el equipo haciendo énfasis en la documentación y cumplimiento de los ANS definidos por cada servicio.

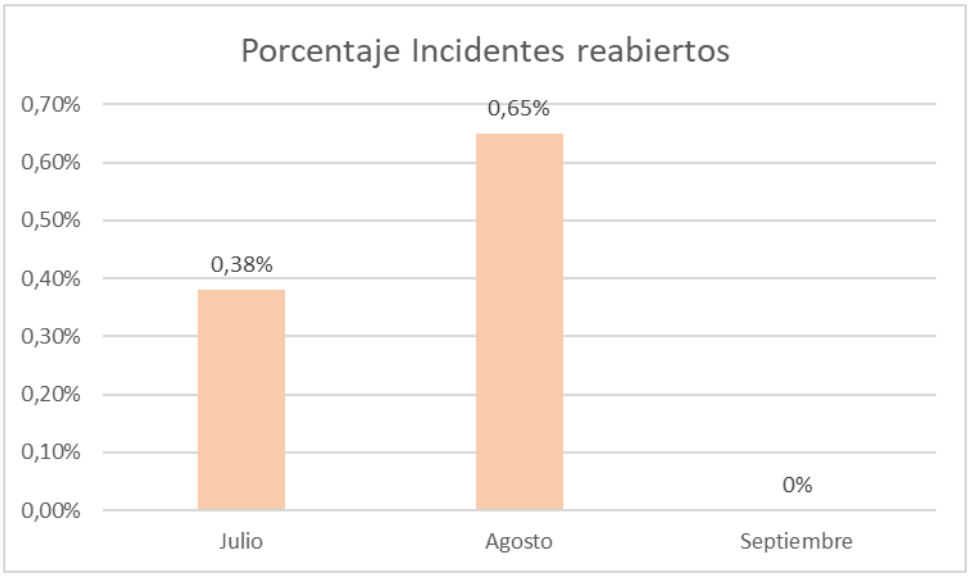


Ilustración 6 Porcentaje de incidentes abiertos

Durante el tercer trimestre, el porcentaje de incidentes reabiertos se mantuvo muy por debajo de la meta del 2%, para el mes de septiembre, en incidentes no se presentaron reaperturas:

- Julio: 0,38%
- Agosto: 0.65%
- Septiembre: 0%

A pesar de la disminución, el resultado sigue siendo favorable y refleja una adecuada gestión de incidentes.

2.1.2.7. Práctica de Requerimientos

Dar a conocer las actividades de la Práctica de Requerimientos correspondientes al periodo del 1 al 30 de septiembre 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 7107 casos tipo requerimiento quedando en los siguientes estados:

Estado	Casos
Cerrado	6342
Solucionado	610
Suspendido	112
En proceso	38
Anulado	4
Registrar	1

Tabla 12 Estados de Requerimientos

- Durante el mes, se presentaron 4 casos en estado anulado, los cuales corresponden a duplicidad 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 agosto al periodo actual.

Grupo Responsable	Agosto	Septiembre
Especialista Aplicaciones .Net	1	1
Especialista Herramientas de Gestion	1	1
Especialista Nube Privada	2	1
Especialista Nube Publica	2	6
Especialista Redes	1	0
Especialista_Telefonía_IP	1	0
SOC	2	6
Especialistas_IBM	7	4
Responsable Garantías Equipos	7	1
Responsable_De_Servidores_Windows	4	0
Responsable_Mesa_De_Servicio	20	28
Responsable_Soporte_Bogota	10	18
Responsable_Soporte_Impresoras	24	10
Responsable_Soporte_Territoriales	15	30
Total por Periodo	**97**	**112**

Tabla 13 Seguimiento del Backlog Suspendidos

En el inicio del período, se identificaron 97 casos suspendidos correspondientes al backlog del mes de agosto de 2025. Se realizaron seguimientos semanales de las solicitudes en estado abierto, logrando la solución de 85 casos a través de la herramienta de Gestión Aranda de los anteriores periodos. Para el cierre del mes, quedaron pendientes 112 casos en el mes de septiembre, 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:

Solicitud	Casos
Radicar una solicitud.Impresora.Cargue de papel en impresora	1012
Radicar una solicitud.Impresora.Cambio Tóner	448
Radicar una solicitud.Equipo de cómputo. Actualización Bios	389
Radicar una solicitud.Impresora.Aumento de cuota	379
Radicar una solicitud.Impresora.Instalacion - Configuración	179
Radicar una solicitud.One drive. Configuración	176
Radicar una solicitud. Directorio activo. Cambiar contraseña	175

Radicar una solicitud.Equipo de cómputo. Configuración	174
Radicar una solicitud. Gestor documental. Relanzamiento	166
Radicar una solicitud. Correo Electronico.Asesoria - Consulta	166

Tabla 14 Top 10 de Solicitudes

- Se realizó seguimiento a requerimientos en backlog, enviando correos a los especialistas para la documentación y cierre de casos pendientes.
- Desde la Práctica de ITIL se realizan auditorias de casos en los que se evidencian oportunidades de mejora, compartidas por correo a los especialistas a quienes se les hace retroalimentación, con base en las novedades encontradas en cada ticket.
- Durante el mes, se llevaron a cabo sesiones presenciales de refuerzo y capacitación por equipos, en las cuales se abordaron los siguientes temas: categorización, matriz de escalamiento, tipificación, cumplimiento de ANS, documentación de apertura y cierre, validaciones de primer nivel, reapertura de tickets, notificaciones desde la herramienta Aranda y encuestas de satisfacción. Por lo anterior en cada sesión se realizaron ejercicios prácticos, se evaluaron los temas tratados y se resolvieron las dudas planteadas por los participantes, con el objetivo de fortalecer las buenas prácticas en la gestión de casos.

De acuerdo con la Guía Operacional de la Práctica de Requerimientos, se estableció los siguientes Indicadores (KPI) con el fin de establecer métricas que apoyen a la operación de los servicios TI:

Nombre	Descripción / Fórmula	Meta	Periodicidad	Resultado del Periodo
Porcentaje de efectividad en resolución de Requerimientos de servicio.	**EF=(RFS/RFR) *100**	80%	Mensual	**EF=** 7084/7107*100
	EF: Efectividad en solución de Requerimientos.			
	RFS: Requerimientos solucionados que cumplen el ANS en el período.			**EF= 99.68%**
	RFR: Requerimientos registradas en el período.			
Porcentaje de Requerimientos Reabiertos en el Periodo	**RRP:** Porcentaje de casos Reabiertos en el periodo.	<2%	Mensual	**RRP=** 4/6956*100
	RFR: Requerimientos Reabiertos en el período.			**RRP= 0,058%**
	RFS: Requerimientos solucionadas en el período.			

Tabla 15 Detalle de KIP Practica de Requerimientos

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

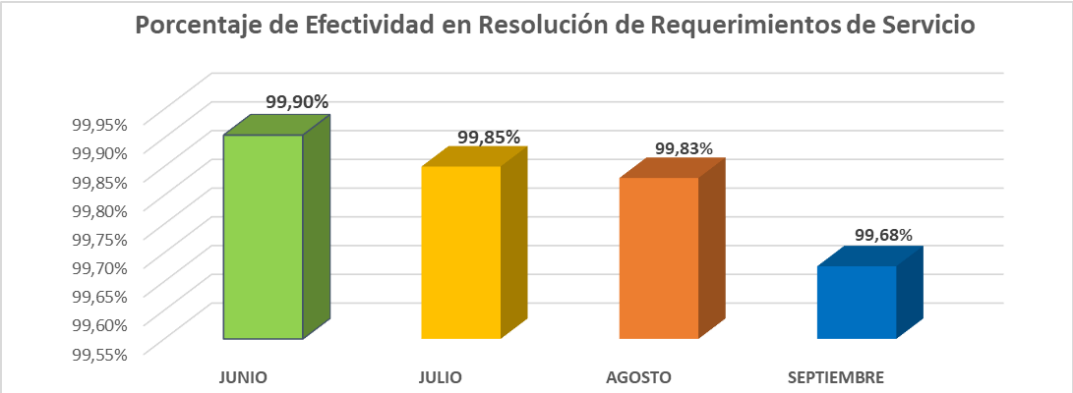


Ilustración 7 KPI Efectividad de Resolución de Requerimientos de Servicio

Durante el periodo, se evidencia el cumplimiento del 99.68% en efectividad de la solución de los requerimientos, los cuales se verifica de 7107 casos registrados en los diferentes canales oficinales de la Mesa de Servicio que fueron solucionados, 7084 casos cumplieron con los tiempos del ANS para dar una respuesta efectiva al usuario y 23 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.

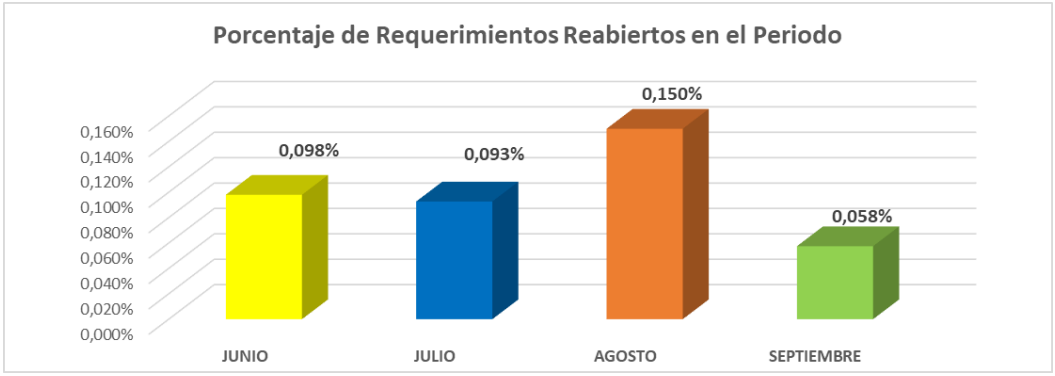


Ilustración 8 Requerimientos de Reabiertos en el periodo

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 4 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-146575	Radicar una solicitud.Servicios. Asignacion de Extensión	Especialista Telefonía IP	Usuario se comunica solicitando configuración para realizar llamadas externas desde teams, indica que es la primera vez que usaría este servicio.	Por parte de Servicio de Telefonía realiza el proceso de asignación de la extensión virtual de Teams y se adjunta el manual de uso, lo cual se da por solucionado el caso, pero el usuario indica en la encuesta de Satisfacción no está de acuerdo con la respuesta y necesita una asistencia remota, lo cual el especialista se comunica con el usuario y confirma que ya puede realizar llamadas.

RF-146658	Radicar una solicitud.Equipo de cómputo. Asignación de equipo (portátil o PC)	Responsable Soporte Bogotá	Usuario solicita la asignación de un equipo de cómputo para un nuevo contratista de la entidad.	Por parte del Soporte en Sitio realiza la asignación del equipo de Cómputo y firma el acta de entrega del equipo en buenas condiciones, pero después de 2 horas haber entregado el Usuario reabre el caso y manifiesta que realizará la devolución porque equipo que presento daño en la tecla **Supr**, por lo anterior se realizó arreglo del daño del equipo y se entrega nuevamente al contratista en buenas condiciones.
RF-147368	Radicar una solicitud.Microsoft Teams.Asesoria - Consulta	Responsable MDS	Usuario solicita configurar el correo de Voz, por lo tanto, se genera caso para su revisión.	Por parte del Agente de MDS realiza la revisión e indica al usuario por favor enviar al correo electrónico las pruebas del Correo de voz, ya que no se escucha el audio y se toma como informativo, pero el usuario en la encuesta indica que necesita es licencia de teams y es una solicitud diferente a la indicada en la descripción del caso y se da por solucionado.
RF-153924	Radicar una solicitud.Gestor documental.Relanzamiento	Especialistas_IBM	Solicitan la asignación de los radicados N° 13EE2025717600100015794 y 13EE2025717600100012972, que fueron redireccionados por la DT Valle al Inspector Helmer Antonio Atehortúa sean asignados a la Dra. Keyla Micolta	Por parte del especialista indica se realizó la gestión, pero de Soly Acosta, pero al revisar la reapertura la usuaria indica no han sido reasignados estos radicados a Dra. Keila Micolta, por lo tanto, el especialista realiza la revisión y aclaración de la solución entregada frente a los procesos de la entidad y se cierra el caso.

Tabla 16 Casos reabiertos

2.1.2.8. Práctica de Eventos

Para el mes de septiembre, 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 670 casos escalados mediante la herramienta de gestión de los cuales 476 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**

✓ Se realiza el aumento de los procesos de pingers que permite que zabbix pueda realizar todas las solicitudes de ping a los hosts monitoreados
✓ Se realiza el aumento de los procesos de Unreachable que permite que zabbix pueda realizar verificaciones adicionales cuando un host deja de responder a ping a los hosts monitoreados
✓ Se configuro el monitoreo a nuevos servidores linux, dentro de su configuración está el agente ZBX y las métricas básicas
✓ 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.

- **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.

De acuerdo con la Guía Operacional de la Práctica de Eventos, se estableció el siguiente Indicador (KPI), con el fin de establecer métricas que apoyen a la operación de los servicios TI

Nombre	Descripción / Fórmula	Meta	Periodicidad	Resultado Septiembre
Efectividad de la Gestión de eventos	ECE: (CEA/ CEC) *100 ECE: Porcentaje de eficacia de los tickets generados por alarmas CEC: Cantidad de tickets creados por alarmas en el periodo. CEA: Cantidad de tickets solucionados por alarmas en el periodo	80%	Mensual	ECE= (488/476)*100 EF= 97,7%

Tabla 17 KPI Práctica de Eventos

- **Informe Operación NOC**

La labor del equipo del Centro de Diagnóstico y Operaciones (CDO) permitió identificar y gestionar un total de 476 incidentes, lo cual evidencia una capacidad operativa y de respuesta ante eventos críticos.

Los routers fueron el componente con mayor incidencia, concentrando el 47% de los casos del mes de septiembre (225 incidentes). Esto está asociado a factores como la inestabilidad de la red eléctrica en zonas remotas o condiciones ambientales adversas. Se recomienda evaluar la continuidad del servicio con proveedores alternos o implementar mecanismos de respaldo electrico.

Los dispositivos FortiGate representaron el 19% de los casos (88 incidentes), eventos causados por falla en la energía comercial, apagado de equipos por parte de los funcionarios e intermitencias en el servicio en horario no hábil. En los eventos que se presentaron en horario no hábil no se logró determinar la causa raíz por falta de señalización de los equipos y pruebas de primer nivel por parte del personal en sitio.

Para este mes se identificó un incremento en los casos reportados por Antenas Starlink, los cuales se encuentran en el tercer lugar, representando un 17% de los casos (82 incidentes). Estas antenas son mayormente afectadas por temas eléctricos o condiciones ambientales en las sedes, de igual forma apagado de los equipos por parte de los funcionarios.

Los servidores Windows en cuarto lugar representan el 8% (39 incidentes), identificando este mes una disminución del 2% en comparación con el mes anterior, con solo 5 casos, representando el 1% del total de los casos.

Los Access Points ocupan el 5to lugar con un 6% (26 incidentes) del total, cifra la cual se mantiene en comparación con los meses anteriores.
Los dispositivos Switches, Canal de Internet y UPS en conjunto reflejan una baja incidencia con el 3% (11 incidentes) del total de los casos.

Redes y Conectividad
Routers: se gestionaron 225 incidentes relacionados con equipos de red Routers en diferentes sedes a nivel nacional, los cuales representaron el 47% de los casos, 2% menos en comparación con meses anteriores. A continuación, se relacionan las sedes afectadas

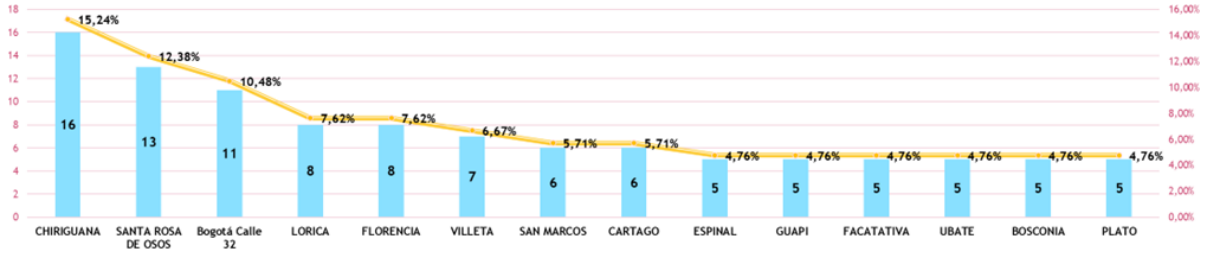


Ilustración 9 Top de incidentes por sedes

De acuerdo con las novedades presentadas, Chiriguaná se consolida como la sede con mayor número de incidentes, registrando 16 casos. La causa predominante en todos ellos es la desconexión o apagado físico de equipos por parte de los funcionarios al finalizar su jornada laboral, lo que genera alarmas en Zabbix fuera del horario hábil. Esta práctica, aunque preventiva frente a fluctuaciones eléctricas, impacta negativamente en la disponibilidad del monitoreo y genera desvíos operativos.

Santa Rosa de Osos ocupa el segundo lugar con 13 casos, de los cuales más del 70% corresponden a intermitencias o lentitud en la red de corta duración (menos de 20 minutos).

Bogotá Calle 32 se posiciona en el tercer lugar del TOP 10 con 11 casos. La causa principal de estos incidentes corresponde a una combinación de factores atribuibles a fallas en la red del proveedor de conectividad, con informes de aperturas de fibra, 3 casos corresponden a desconexión o apagado físico de equipos en sede generalmente fuera de horario laboral. 2 casos se clasifican como bloqueo de dispositivo o reinicio del servidor/enrutador. 1 caso está relacionado con problemas de cableado UTP en el rack local.

Las sedes de Florencia y Lorica, ambas con 8 casos cada una relacionada a routers, presentan una alta dependencia de la estabilidad del servicio eléctrico local. En Florencia, el 87.5% de los incidentes se deben a fallas eléctricas con un evento adicional atribuido a falla de fibra del proveedor de conectividad. En Lorica, el 75% de los casos también se asocian a fallas eléctricas, complementados con un caso de apagado manual de equipos y otro de intermitencia en la red probablemente derivado de reinicios post-falla eléctrica.

Villeta se posiciona en el TOP 10 de sedes con más incidentes en routers con 7 casos. La mayoría de estos eventos (86%) están directamente relacionados con fallas eléctricas en la zona, las cuales generan desconexiones prolongadas o intermitencias en la conectividad.

Las sedes de Espinal, Guapi, Facatativá, Ubaté, Bosconia y Plato, con 5 casos cada una (4.76% del total de incidentes en routers), presentan un patrón mixto, pero claramente dominado por la inestabilidad eléctrica. En Espinal, Guapi, Facatativá y Plato, el 100% de los eventos se atribuye a fallas eléctricas. Por otro lado, Ubaté y Bosconia combinan fallas eléctricas con apagado de equipos por parte del personal del Ministerio, lo que refleja una respuesta preventiva ante la misma problemática.

A continuación, se relacionan las causas que generaron afectación en los routers

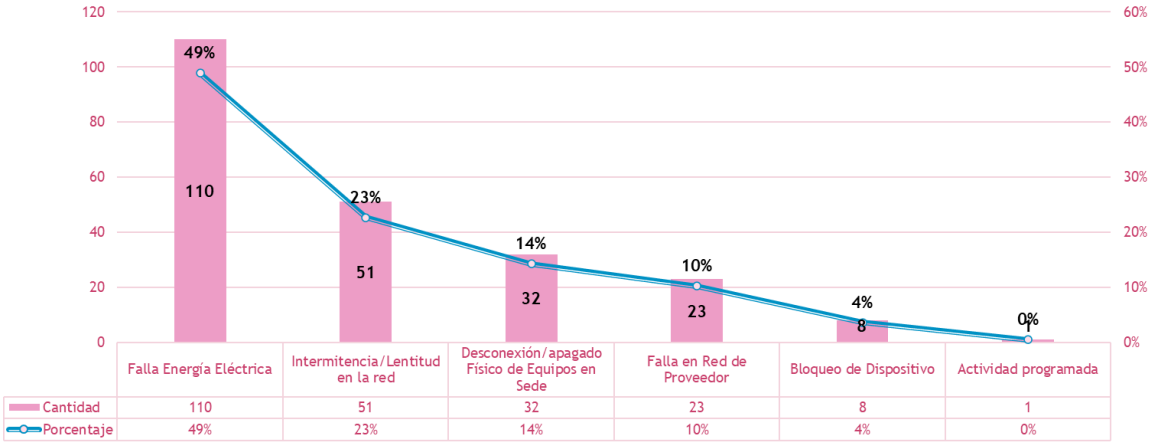


Ilustración 10 Top de incidentes por sedes

Las fallas por energía eléctrica representan el 48% de los casos (108), afecta principalmente a zonas remotas o rurales como Florencia, Lorica, Villeta, Mitú, Puerto Carreño, Guapi, Espinal, Facatativá, Plato y Maicao, entre otras, donde la red eléctrica es inestable o está sujeta a cortes prolongados. El 23% (51) de los casos están por intermitencias y lentitud en la red, este tipo de incidencias se concentra en regiones con conectividad limitada o infraestructura de telecomunicaciones precaria (por ejemplo, Santa Rosa de Osos, Cartago, Tuluá, Mocoa y San Vicente del Chucurí). Las intermitencias suelen ser de corta duración (menos de 30 minutos), pero se repiten con frecuencia, generando múltiples alarmas. En varios casos, estas intermitencias son consecuencia indirecta de reinicios posteriores a fallas eléctricas.
El 14% (31) de los casos están relacionados a apagado de equipos, sedes como Chiriguaná, San Marcos, Ubaté, Bosconia, Manizales (Manzanares), Puerto López y Sabanalarga reportan este comportamiento de forma recurrente. Los funcionarios

apagan los dispositivos al finalizar su jornada laboral como medida preventiva ante fluctuaciones eléctricas, con la intención de proteger el hardware.

El 10% (22) de los casos están relacionados a fallas en la red del proveedor, se observa una disminución significativa en comparación con meses anteriores, lo que refleja una mejora en la estabilidad de los enlaces y una gestión más eficaz con los proveedores. Las sedes más afectadas por este tipo de falla incluyen Bogotá Calle 32, Cúcuta, Pasto, Turbo, Garzón y Cartago, donde se reportaron aperturas de fibra, migraciones de troncales o fallas en equipos de planta externa.

Switches

Durante el mes de septiembre se generaron 8 casos referentes a Switches en la herramienta de monitoreo Zabbix en diferentes sedes, los cuales representan el 2% del total de los casos

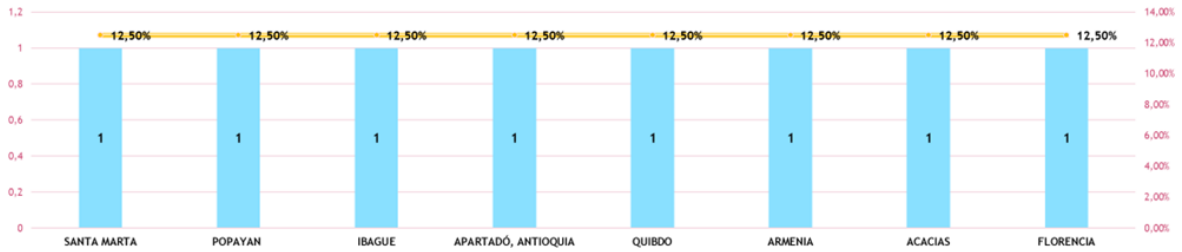


Ilustración 11 eventos por sedes routers

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

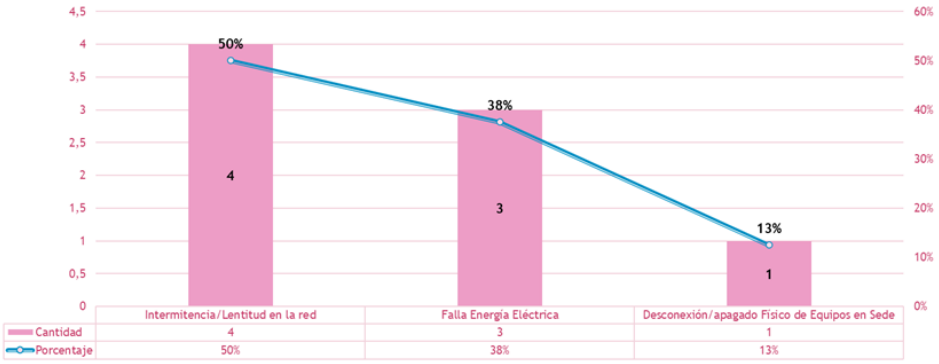


Ilustración 12 Top de causas por sedes switches

Se listan 3 diferentes causas para la categoría de Switches registradas durante el periodo del mes de septiembre.

3 de los 8 casos (38%) están directamente relacionados con fallas eléctricas: Santa Marta, Apartadó, Armenia y Florencia.

4 casos (50%) se atribuyen a intermitencia o lentitud en la red, sin evidencia de falla del proveedor: Acacias, Ibagué, Popayán y Quibdó.

1 caso (13%) corresponde a Armenia, clasificado como apagado de equipos por parte de los funcionarios.

Access Point

Durante el mes de septiembre se gestionaron 26 incidentes asociados a equipos de red WLAN – Access Point en distintas sedes a nivel nacional, los cuales representan el 6% del total de casos reportados. Estos eventos fueron abordados dentro de los niveles de servicio establecidos, sin afectación crítica a la operación general de la red.

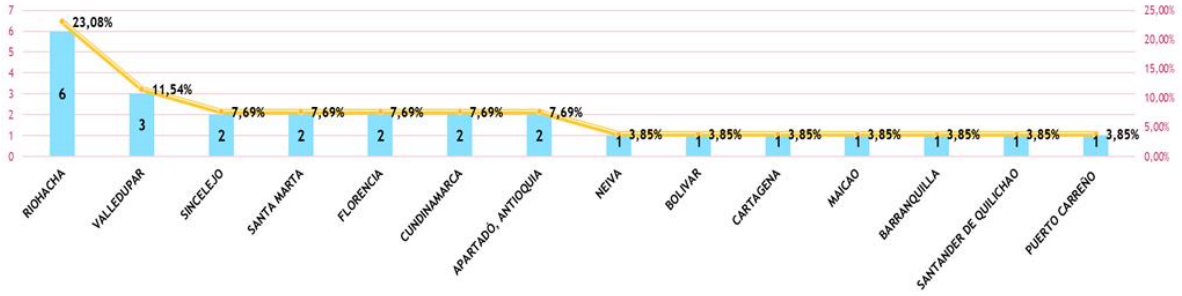


Ilustración 13 Top de eventos por sedes Access point

Durante el mes de septiembre se evidencia que la sede con mayor número de eventos relacionados con Access Point es Riohacha, con 6 casos que representan el 23% del total de los casos, conservando el primer lugar en el TOP. Causa predominante: Bloqueo de dispositivo (4 casos, 67%), seguido por desconexión/apagado físico de equipos en sede (2 casos, 33%). En múltiples ocasiones, el soporte en sitio reporta que los APs requieren reinicio manual debido a bloqueos recurrentes.

Le sigue Valledupar con 3 casos (11%), manteniendo su posición en los últimos meses. Causas: 2 casos por desconexión/apagado físico de equipos y 1 por falla eléctrica. Los funcionarios reconocen apagar los equipos al finalizar la jornada laboral como medida preventiva ante fluctuaciones eléctricas.

Las sedes Sincelejo, Santa Marta, Florencia, Cundinamarca y Apartadó reportan 2 casos cada una (7% del total): Sincelejo: ambos casos por bloqueo de dispositivo, resueltos mediante reinicio físico. Santa Marta: ambos atribuidos a falla eléctrica, con intermitencias de corta duración (menos de 4 horas). Florencia: un caso por falla eléctrica y otro por bloqueo de AP. Cundinamarca: ambos casos clasificados como intermitencia/lentitud en la red, sin falla eléctrica confirmada. Apartadó: un caso por bloqueo de dispositivo y otro por falla eléctrica.

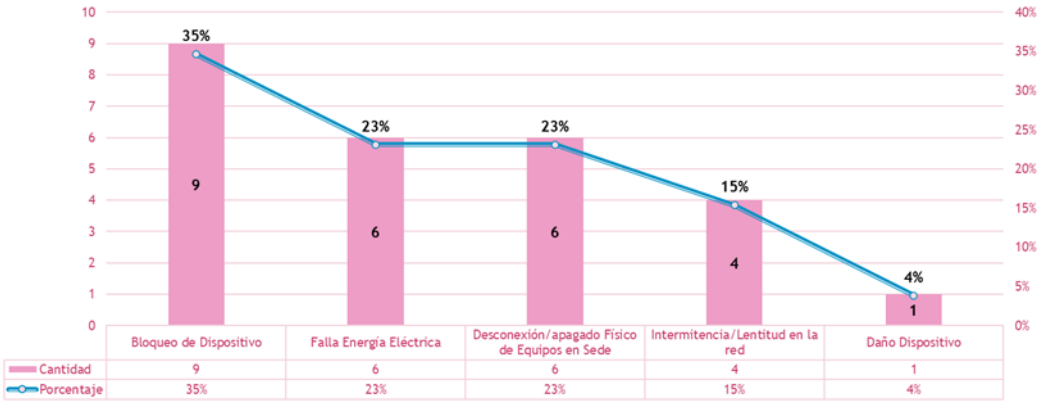


Ilustración 14 Top de causas por sedes Access point

Se evidencian 5 causas de fallas para el periodo del mes de septiembre con relación a los dispositivos Access Point.

El 65% de los incidentes en APs (17 de 26) están directamente relacionados con fallas eléctricas o prácticas de apagado manual por parte del personal, lo que refuerza la necesidad crítica de implementar UPS en sedes con alta recurrencia (especialmente Río hacha, Santa Marta, Florencia y Puerto Carreño).

El 31% de los casos (8 de 26) corresponden a bloqueos de dispositivo, un patrón preocupante en sedes como Río hacha, Sincelejo y Santander de Quilichao.

Starlink

Durante el mes de septiembre se gestionaron 82 incidentes relacionados con equipos de red Starlink en diferentes sedes a nivel nacional, los cuales representan el 17% del total de los casos, evidenciándose que para este mes se aumentó un 6% la cantidad de casos.

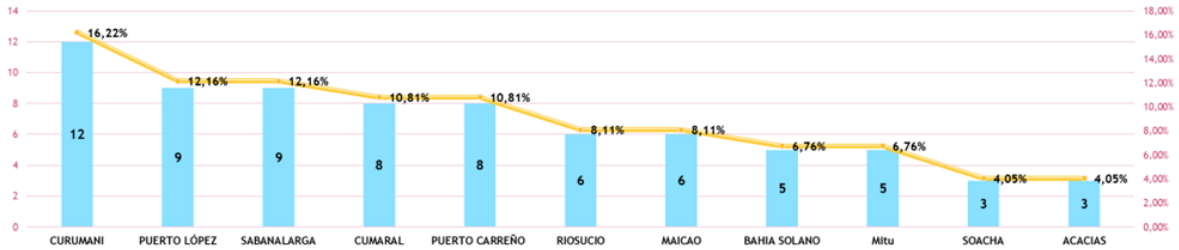


Ilustración 15 Top de eventos por sedes Starlink

Para el mes de septiembre el TOP 5 de las sedes con mayor número de eventos generados para la categoría de Starlink fueron Curumani con 12 eventos, representando un 16%, la cual se mantiene en primer lugar y se observa un aumento de casos, Puerto López sube en el TOP con 9 casos, lo cual representa el 12% de los casos, junto con Sabana Larga, Cumaral con Puerto Carreño con 8 eventos, representando el 10%, sedes que también se mantiene en el TOP, Riosucio

la cual se mantiene en el TOP y Maicao que ingresa al TOP con 6 casos, presentando el 8%.

Las fallas eléctricas son la causa predominante en la mayoría de las sedes del TOP, 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, Bahía Solano, Maicao y Acacias tiene un número importante de casos asociados a fallas con el proveedor.

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

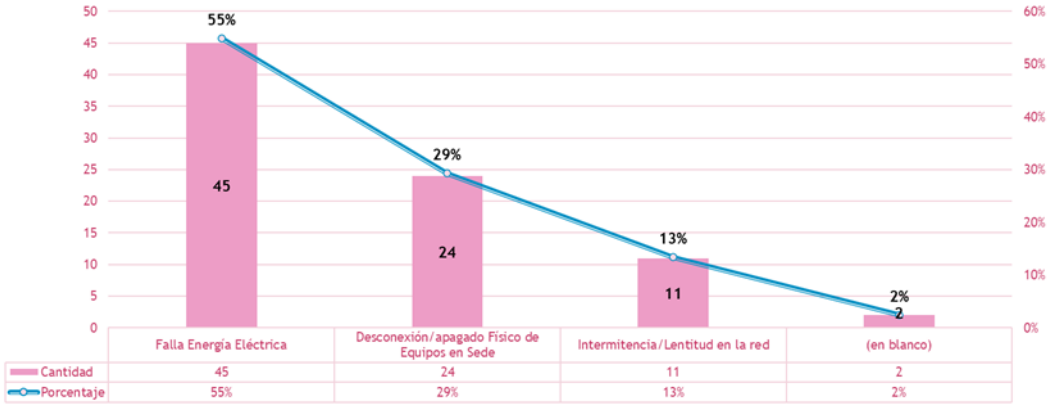


Ilustración 16 Top de causas por sedes Starlink

Durante el mes de septiembre se pudo observar que la falla en dichos puntos con este dispositivo Starlink se debió a efectos climáticos y por energía eléctrica, lo que ocasionó 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 29%, ya que el fluido eléctrico es muy inestable en dichas sedes por la ubicación geográfica en la que se encuentran las sedes y los funcionarios prefieren apagar los dispositivos al finalizar su jornada laboral.

Fortigate

Durante el mes de septiembre se gestionaron 88 incidentes relacionados con equipos de red FortiGate en diferentes sedes a nivel nacional, los cuales representaron el 19% del total de los casos, ocupando el segundo lugar.

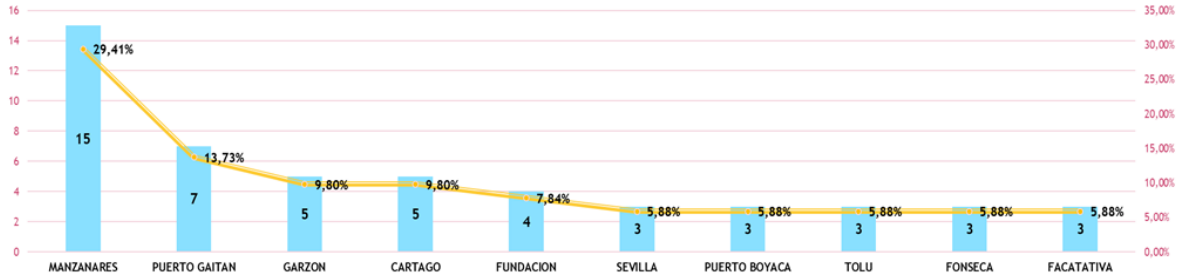


Ilustración 17 Top de incidentes por sedes fortigate

Durante el análisis del comportamiento de la red SD-WAN en el mes de septiembre, se identificó una mayor frecuencia de afectación en las sedes de Manzanares, mantenimiento su lugar en los últimos 2 meses, con un 29% (15) seguido de Puerto Gaitán con un 13% (7), 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.

Por otro lado, Garzón y Cartago con un 9% (5), presentan una alta tasa de intermitencias a nivel de red, las cuales no superan los 30 minutos de indisponibilidad. Aunque con un porcentaje más bajo del 5%, las sedes Sevilla, Tolú y Fonseca también presentan un alto porcentaje de intermitencia.
Sedes como Facatativá y Puerto Boyacá, también presentan un alto porcentaje de eventos por fallas de energía eléctrica.

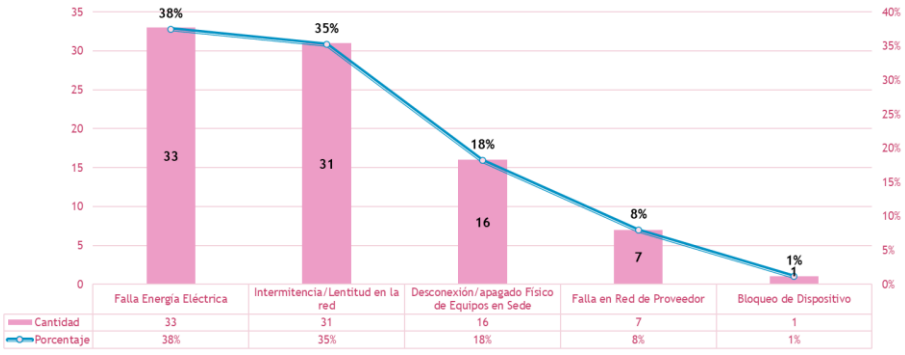


Ilustración 18 Top de causas por sedes fortigate

Durante el mes de septiembre, los dispositivos SD-WAN presentaron un leve aumento en el volumen de alarmas, siendo la principal causa las fallas eléctricas con un 38% (33) ocasionadas por condiciones climáticas adversas, validadas por el soporte en sitio.

Un 35% (31) 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. Para este mes se observa un aumento del 2% de las fallas por Intermitencias.

Seguido de desconexión/apagado físico de equipos en sede con un 17% (15) 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.

Casos Escalados a Proveedor de Telecomunicaciones

Durante el mes de septiembre se registraron 31 casos que fueron escalados y gestionados con proveedor ETB, de los cuales quedan 29 (94%) que registran en estado solucionado o cerrado y 2 (6%) en estado suspendido:

El caso en Aranda IM-153699 se relaciona al servicio Router_Mariquita, el cual está suspendido en espera de avances por parte del proveedor de última milla UFINET.

El caso en Aranda IM-153186 se relaciona al servicio Router_Bosconia, el cual está suspendido en espera de avances por parte del proveedor de última milla UFINET.

Servicios Centrales

Servidores Windows

Durante septiembre, el Centro de Operaciones de Red (NOC) gestionó 39 incidentes asociados a servidores Windows, equivalentes al 8% del total de casos registrados en el mes.

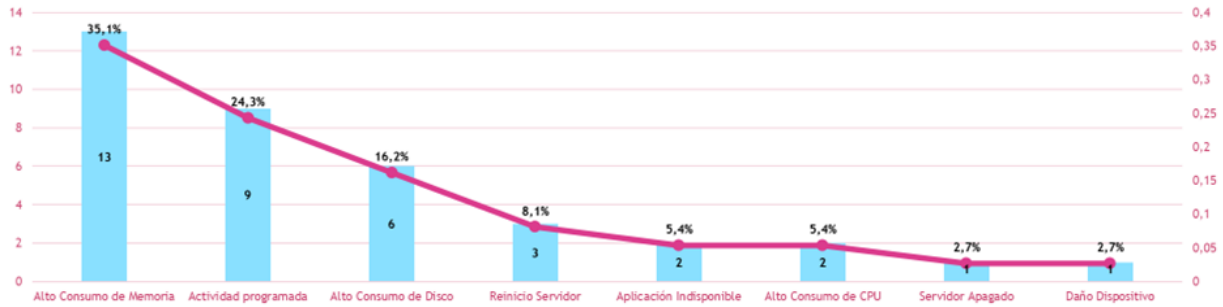


Ilustración 19 Top de eventos windows

El alto consumo de memoria es el principal causante de eventos en el sistema, representando el 35% del total de incidentes, actividad programada representa el 24%, evidenciando un aumento considerable a comparación del mes pasado y el

alto consumo en disco, con un 16% mostrando una disminución importante en los casos en comparación con otros meses.

Otros factores, reinicio de servidor, aplicación indisponible, consumo de CPU y servidor apagado, representan el 24% de los casos.

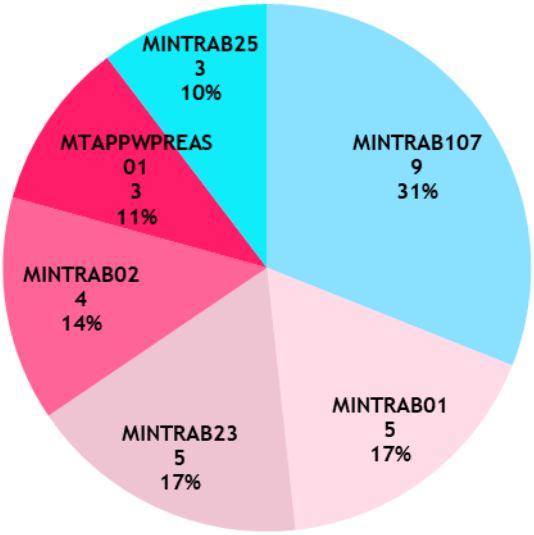


Ilustración 20 Top de servidores windows

El servidor MINTRAB107 representa el 31% del total, todos los casos relacionados a alto consumo de memoria, lo cual indica una alta carga o incidencia en este servidor específico.
Para este mes se observa que el servidor MINTRAB01 presenta 5 casos de los cuales todos están relacionados a actividades programadas mediante RFC 153627

Servidores Linux

Durante septiembre, el Centro de Operaciones de Red (NOC) gestionó 5 incidentes asociados a servidores Linux, equivalentes al 1% del total de casos registrados en el mes.

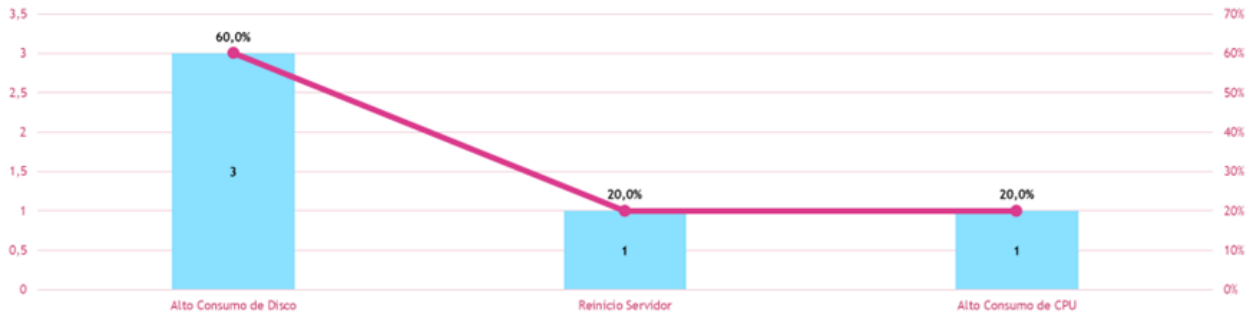


Ilustración 21 Top de causas eventos linux

Las causas principales de los eventos registrados muestran que la gran mayoría están asociadas a factores conocidos y potencialmente controlables. El alto consumo en disco representando un 60% (3) de los casos, seguido de reinicio de servidor y alto consumo en CPU con un 20% (1).

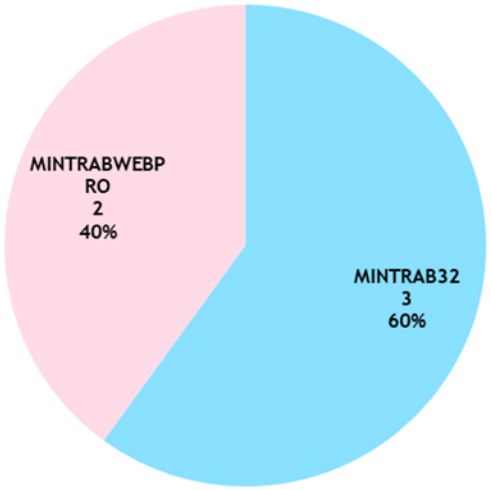
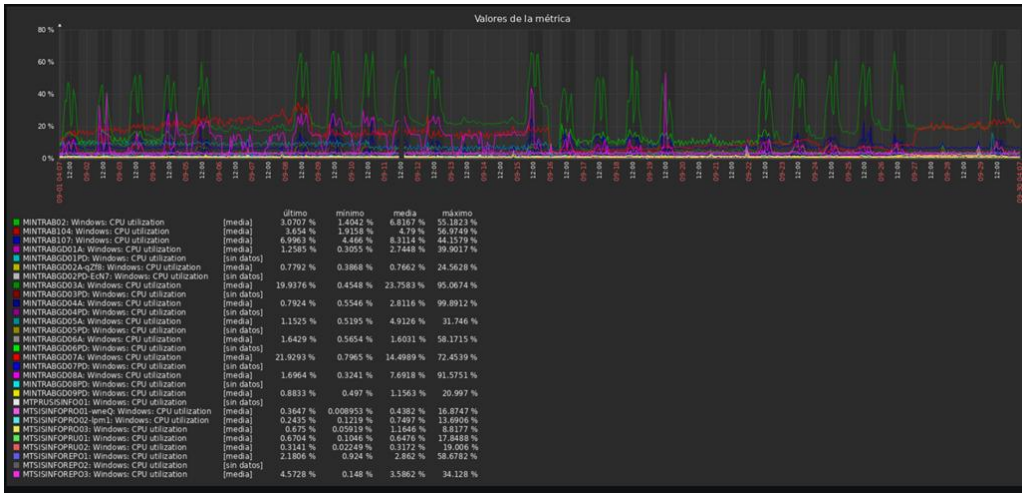


Ilustración 22 Top de servidores linux

Se evidencia una mayor concentración de eventos en el servidor MINTRAB32, con 3 eventos, lo que representa el 50% del total debido a alto consumo en el disco C. MINTRABWEBPRO registra 3 eventos, equivalente al 50%, uno de estos casos debido actividad programada mediante RFC 153627, lo de más por alto consumo en disco.

Gráficas de CPU zabbix de todo el mes sobre servidores



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

CPU

MINTRABGD03A 23.7583%
MINTRABGD07A 14.4989%
MINTRAB107 8.3114%
MINTRABGD08A 7.6918%
MINTRAB02 6.8167%

Gráfica de MEMORIA zabbix de todo el mes sobre servidores



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

MEMORIA

MINTRAB107 79.2899%
MINTRAB02 78.6616%
MINTRAB104 70.1959%
MINTRABGD07A 50.6227%
MTSISINFOPRO03 47.6133%

Datacenter (Cali - Bogotá)

Durante el mes de septiembre, no se reportó ningún incidente relacionado a los Datacenter 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 30 de septiembre de 2025.

Servidores

Cantidad de dispositivos	Disponibilidad consolidada
124	99,99%

Tabla 18 Consolidado disponibilidad de servidores

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

Servidor	Disponibilidad	Aplicación
MINTRAB23	99,86%	Aplicaciones NET

Directorio Activo

Cantidad de dispositivos	Disponibilidad consolidada
3	100,00%

Tabla 19 Consolidado disponibilidad de Directorio Activo

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

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

Tabla 20 Desagregado de Disponibilidad Directorio Activo

Datacenter Principal

Cantidad de dispositivos	Disponibilidad consolidada
8	100,00%

Tabla 21 Consolidado disponibilidad de equipos Datacenter principal

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

Equipo	Disponibilidad
Fortimanager_SDWAN	100,00%
CXV-SWCORE1-RAT42-U44-8360	100,00%
CXV-SWCORE2-RAT42-U42-8360	100,00%
CXV-SWDELL1-RAS42-U43-S4148T	100,00%
CXV-SWDELL2-RAS42-U42-S4148T	100,00%
CXV-SWEDGE-RAT42-U40-6300	100,00%
CXV-SWACC-RAAT38-U41-6300	100,00%
CXV-FG-600F-SDWAN-HUB02	100,00%

Tabla 22 Desagregado de Disponibilidad Datacenter Principal

Datacenter Alterno

Cantidad de dispositivos	Disponibilidad consolidada
4	100%

Tabla 23 Consolidado disponibilidad de equipos Datacenter alterno

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

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

Tabla 24 Desagregado Disponibilidad de equipos Datacenter alterno

Redes y conectividad

Cantidad de dispositivos	Disponibilidad consolidada
506	97,87%

Tabla 25 Consolidado disponibilidad de equipos redes y conectividad

Durante el periodo, se realizó constante monitoreo y seguimiento de la disponibilidad de los canales principales y secundarios de internet, con el fin de prever alguna novedad en el servicio y dar una respuesta oportuna desde el NOC y Lideres de Servicio de Conectividad.

Seguridad

Cantidad de dispositivos	Disponibilidad consolidada
6	100,00%

Tabla 26 Consolidado disponibilidad de equipos de seguridad

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

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

Tabla 27 Disponibilidad de equipos Seguridad de la Información

Telefonía

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

Tabla 28 Consolidado disponibilidad de equipos de telefonía

Antivirus

Cantidad de dispositivos	Disponibilidad consolidada
1	100%

Tabla 29 Consolidado disponibilidad de plataforma antivirus

Actividades de la Practica de Disponibilidad:

- Seguimiento a los resultados de los cambios presentados en el CAB por partes de especialistas que afecten la disponibilidad del servicio.
- Se presenta en la siguiente gráfica el seguimiento de la planeación y ejecución del calendario de pruebas de alta disponibilidad de los servicios e infraestructura, se programó realizar 33 pruebas de alta disponibilidad, de las cuales 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.

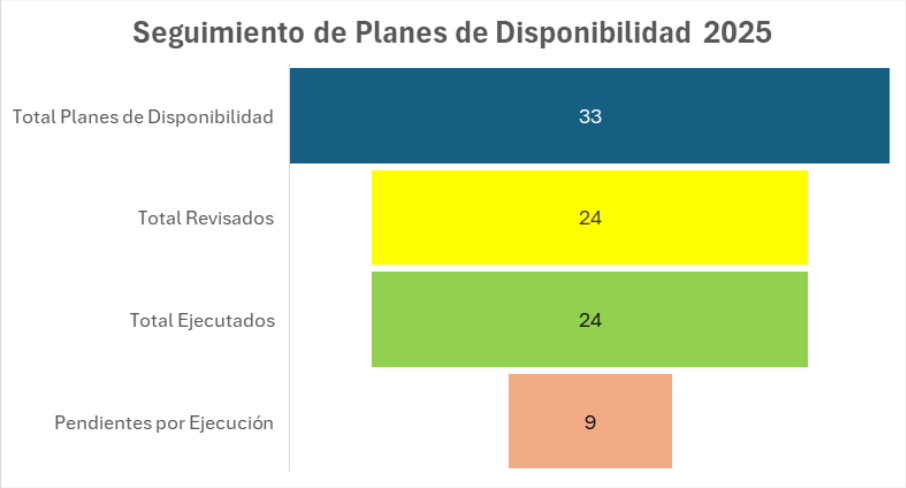


Ilustración 23 Seguimiento Pruebas de Disponibilidad

2.1.2.10. Práctica de Implementación

Dentro de la aplicación de la práctica, se desarrollaron procesos para apoyar a planificar, programar, ejecutar, controlar, aplicar pruebas e implementar nuevos servicios o incluir modificaciones de las funcionalidades de los aplicativos o sistemas de información en producción.
A continuación, se muestra la información correspondiente a la práctica de implementación para el periodo del 1 al 30 de septiembre de 2025.

Actividades en curso:

Revisión de los RFC ejecutadas durante el periodo, los cuales (21) 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 (6) casos abiertos a la espera de entrega de las evidencias por parte los especialistas, en proceso de revisión, en implementación o por aprobación al corte del 30/09/2025.

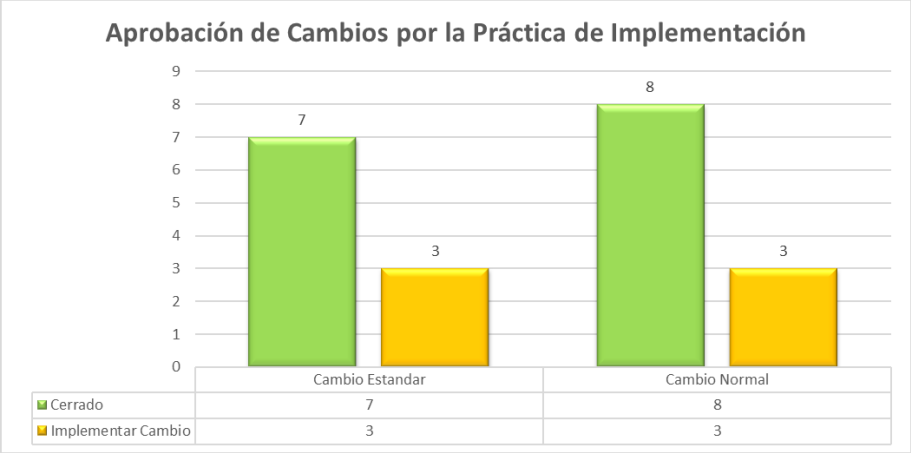


Ilustración 24 Seguimiento Práctica Implementación

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 septiembre, 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 septiembre, en el Ministerio del trabajo a la MDS ingresaron 284 llamadas de usuarios finales para solicitar servicios de Soporte Tecnológico, a continuación, se discrimina la clasificación según el servicio solicitado:

Servicio	Entrantes	Atendidas	Atendidas Umbral	Sumatoria No Atendidas umbral	Abandonadas	No Atendidas
COL - Mintrabajo-equipo compu	173	168	168	2	4	1
COL - Mintrabajo-Gestor-documental	49	48	48	0	0	1
COL - Mintrabajo-office365	47	47	46	0	0	0
COL - mintrabajo-Impresora	15	15	15	0	0	0
TOTAL	284	278	277	2	4	2

Tabla 30 Llamadas Atendida por la Mesa de Servicio

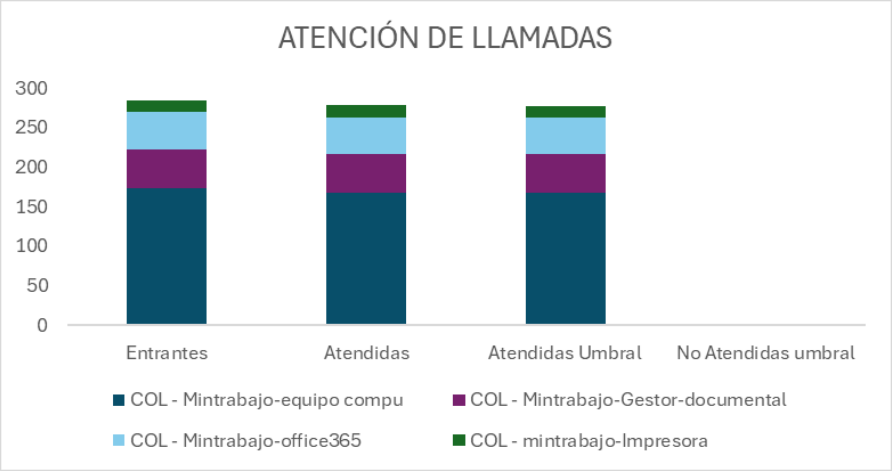


Ilustración 25 Llamadas Atendidas

El servicio más solicitado a través de la atención de llamadas es: Equipo de cómputo con 172 llamadas entrantes, se atendieron 173 solicitudes, se observa: 2 llamadas no atendidas en el umbral por que fue abandonadas por el funcionario antes de los 20 segundos.

- Casos Registrados por Categoría de Servicio

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

- Análisis de Casos Anulados por Servicio

Para este periodo se tiene 6 casos anulados de los siguientes servicios:

CASOS ANULADOS	TOTAL
Aplicaciones Especializadas	2
Soporte Microinformática	2
Redes y Conectividad	1
Seguridad informática	1
Total general	**6**

Tabla 31 Casos anulados por Servicio

- **Soporte Microinformático:** se tiene 2 casos, Soporte Aplicaciones Office 365, Microsoft Teams, Asesoría – Consulta anulados por duplicidad.
- **Aplicaciones especializadas:** se tiene 2 caso por: RFC Normal para parchado de servidores Linux y RFC: Solicitud de aprobación de cambio para mitigar vulnerabilidades de seguridad del Portal Web, anulados por duplicidad.
- **Redes y Conectividad:** se tiene 1 caso anulado por Revisión estado del canal.
- **Seguridad informática:** se tiene 1 caso anulado por Validación Habilitación Puertos USB.

En comparación del mes anterior se evidencio una disminución del 25%, que corresponde a 2 casos.

- Análisis de Casos Suspendidos por Servicio

Para el periodo del mes de septiembre, se dio una disminución de casos suspendidos del 46,62% que corresponde a 69 casos para un total de este mes de 79 casos de los siguientes servicios:

CASOS SUSPENDIDOS	TOTAL
Soporte Microinformática	33
Administración de servidores	14
Aplicaciones Especializadas	12
Redes y Conectividad	10
Seguridad informática	8
Telefonía IP	1
Herramientas de Gestión	1
Total general	**79**

Tabla 32 Casos Suspendidos por Servicio

- **Soporte Microinformática:** 33 casos suspendidos debido a que se ha solicitado información complementaria a los usuarios o están pendientes por disponibilidad del usuario: Cambio Tóner con 10 casos, Asesoría - Consulta con 3 casos, Configuración con 3 casos, Solicitud Backup, Equipo Periférico, Equipo Portátil con 2 casos, cada categoría, Equipo Escritorio, instalación y configuración VPN , Cambio de unidad fusora, Mantenimiento preventivo, Falla Cargue página web, Traslado – Movimiento, Falla de sistema operativo, instalación – Configuración con 1 caso.
- **Administración de servidores**: 14 casos suspendidos por: Inactivar usuario con 9 casos, Configuración, Servidor Windows, Configuración, Administración de equipos, actualización de servidores, Apagar servidor con 1 caso.
- **Aplicaciones Especializadas:** 12 casos suspendidos debido a que se ha solicitado información complementaria a los usuarios o están pendientes por: Gestor documental. Asesoría - Consulta, con 3 casos, Gestor documental. Asignar Radicado TYS, Servidor de aplicaciones. Instalar – Configurar con 2 casos, SICIP. Informes y Reportes, Gestor documental. Relanzamiento, solicitud. SICIP.Asesoría – Consulta, falla. Gestor Documental, SICIP.Asesoría – Consulta, con 1 caso cada categoría.
- **Redes y Conectividad:** 10 casos suspendidos debido a: Router con 5 casos, Starlink y FortiGate con 2 casos cada categoría, Degradación con 1 caso.

- **Seguridad informática: 8** casos suspendido debido a: Habilitación Puertos USB con 6 casos, Firewall.Permitir acceso, SOC.Análisis vulnerabilidades con 1 caso cada categoría.
- **Telefonía IP**: 1 caso suspendidos debido a: Softphone.Falla - error.
- Herramientas de Gestión**: 1** caso suspendido debido a: Creación /Modificación /Eliminación Funcionalidades Aranda.

- Análisis General de Casos Solucionados - Incidentes y Requerimientos

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

Incidentes solucionados por Soporte en sitio: Para este periodo quedaron 10 incidentes en estado solucionado.

SOPORTE_EN_SITIO	TOTAL
Envio y recepción de correos	3
Falla - error	1
Falla Aplicaciones Office 365	2
Falla Error - Datacap	1
Falla General	1
Lentitud	1
No imprime	1
Total general	**10**

Tabla 33 Incidentes Solucionados por Soporte en Sitio

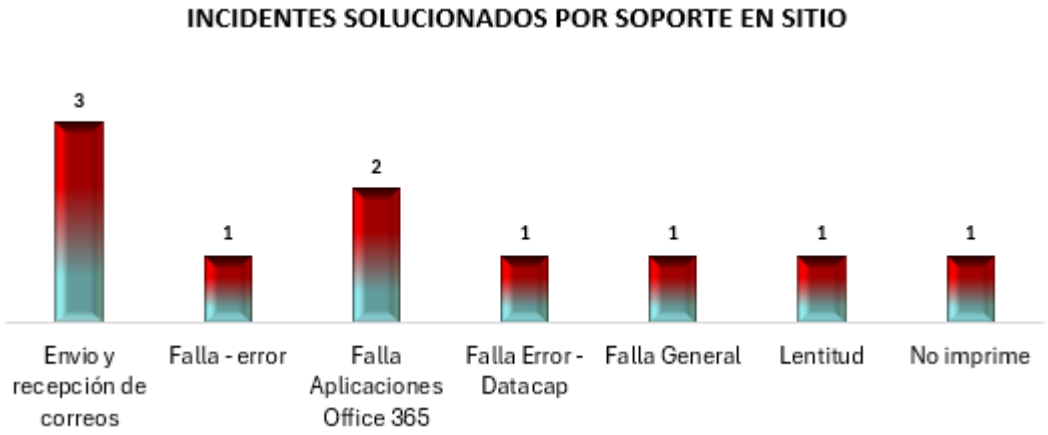


Ilustración 26 Incidentes Solucionados por Soporte en Sitio

Incidentes solucionados por Soporte Territoriales: para periodo quedaron 5 incidentes en estado solucionado.

SOPORTE_TERRITORIAL	TOTAL
Atasco	2
Falla - Error conexión a red	1
Falla aplicación	1
Falla Cargue pagina web	1
Total general	**5**

Tabla 34 Incidentes Solucionados por Soporte Territorial

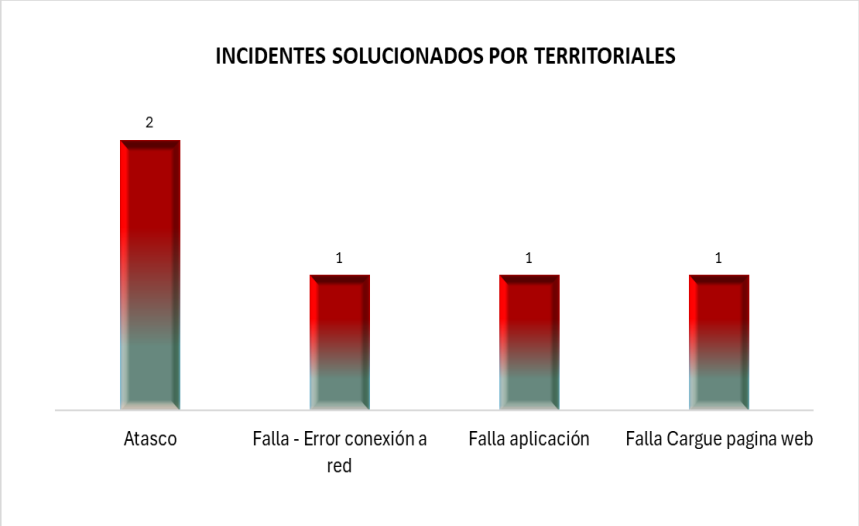


Ilustración 27 Incidentes Solucionados por Territoriales

Requerimientos solucionados por la Mesa de Servicios: Para el mes de septiembre quedaron 61 requerimientos solucionados por la mesa de servicios discriminados de la siguiente manera:

REQUERIMIENTOS SOLUCIONADOS MESA_DE_SERVICIOS	TOTAL
Asesoría - Consulta	19
Cambiar contraseña	17
Cambio de grupo	6
Creación de usuario	4
Instalación y configuración VPN	2
Reportar Solicitud/Falla	2
Relanzamiento	2
Configuración	1
Crear/Modificar/Eliminar	1
Permitir acceso	1
Inactivar usuario	1
Habilitación Puertos USB	1

Instalación - Configuración	1
Crear política	1
Análisis de evento	1
Depuración Bandeja	1
Total general	**61**

Tabla 35 Requerimientos Solucionados por Mesa de Servicio

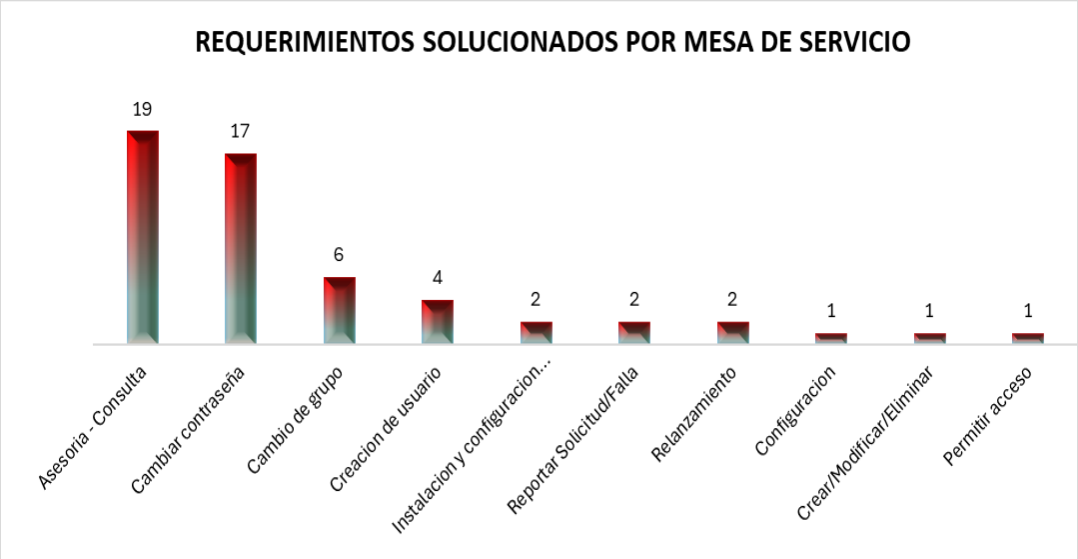


Ilustración 28 Requerimientos Solucionados por Mesa de Servicio

Requerimientos solucionados por Soporte en sitio Bogotá: en el mes de septiembre quedaron 144 requerimientos discriminados de la siguiente manera:

REQUERIMIENTOS SOLUCIONADOS POR SOPORTE EN SITIO	TOTAL
Cargue de papel en impresora	42
Asesoría - Consulta	23
Instalación - Configuración	14
Cambiar contraseña	12
Actualización BIOS	11
Configuración	10
Préstamo	9
Solicitud instalación	3
Instalación - Configuración	2
Soporte Aplicaciones Office 365	2
Asesoría PDF	2
Asesoría Word	2
Asesoría Excel	2
Traslado - Movimiento	1
Conectar a red Mintrabajo	1
Instalación y configuración VPN	1

Eliminar Hostname	1
Aumento de cuota	1
Instalación-Desinstalación	1
Reportar Solicitud/Falla	1
Solicitud Backup	1
Asesoría Consulta	1
Devolución de equipo (portátil o PC)	1
Total general	**144**

Tabla 36 Requerimientos Solucionados por Soporte en Sitio

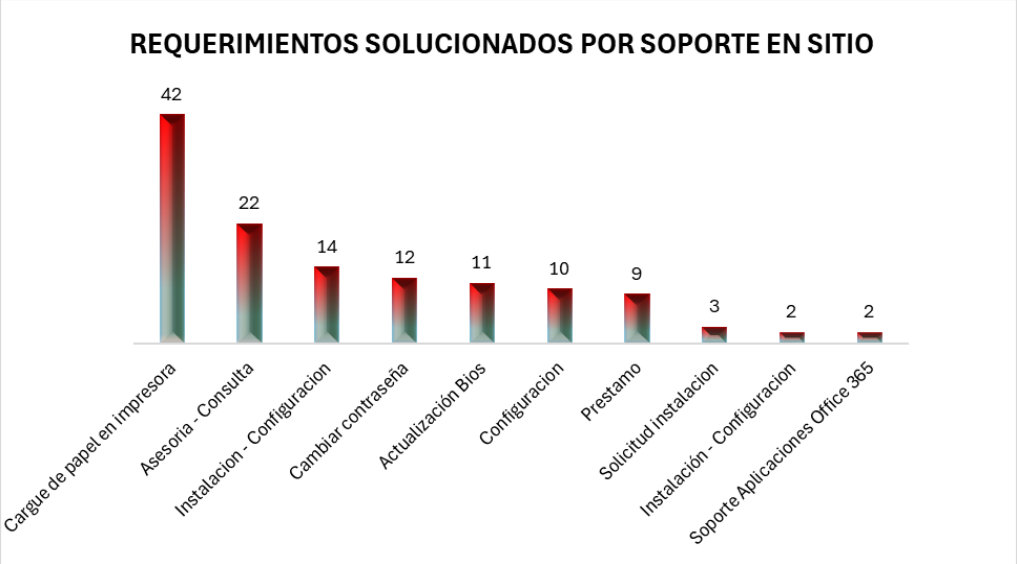


Ilustración 29 Requerimientos Solucionados por Soporte en Sitio

Requerimientos solucionados por Soportes Territoriales: Para el mes de septiembre quedaron 205 casos en estado solucionado de las territoriales.

REQUERIMIENTOS SOLUCIONADOS POR TERRITORIALES	TOTAL
Asesoría Excel	44
Configuración	35
Asesoría - Consulta	31
Cargue de papel en impresora	18
Instalación - Configuración	14
Actualización BIOS	11
Asesoría PDF	7
Asignación de equipo (portátil o PC)	6
Cambio Tóner	5
Traslado - Movimiento	4
Prestamos	4
Asesoría Word	4

Devolución de equipo (portátil o PC)	3
Soporte Aplicaciones Office 365	3
Conectar a red Mintrabajo	3
Copia de información	2
Revisión estado del canal	2
Cambiar contraseña	2
Aumento de cuota	2
Análisis de Correos	1
Mantenimiento preventivo	1
Instalación y configuración VPN	1
Revisar correo malicioso	1
Total general	**205**

Tabla 37 Requerimientos Solucionados por Territoriales

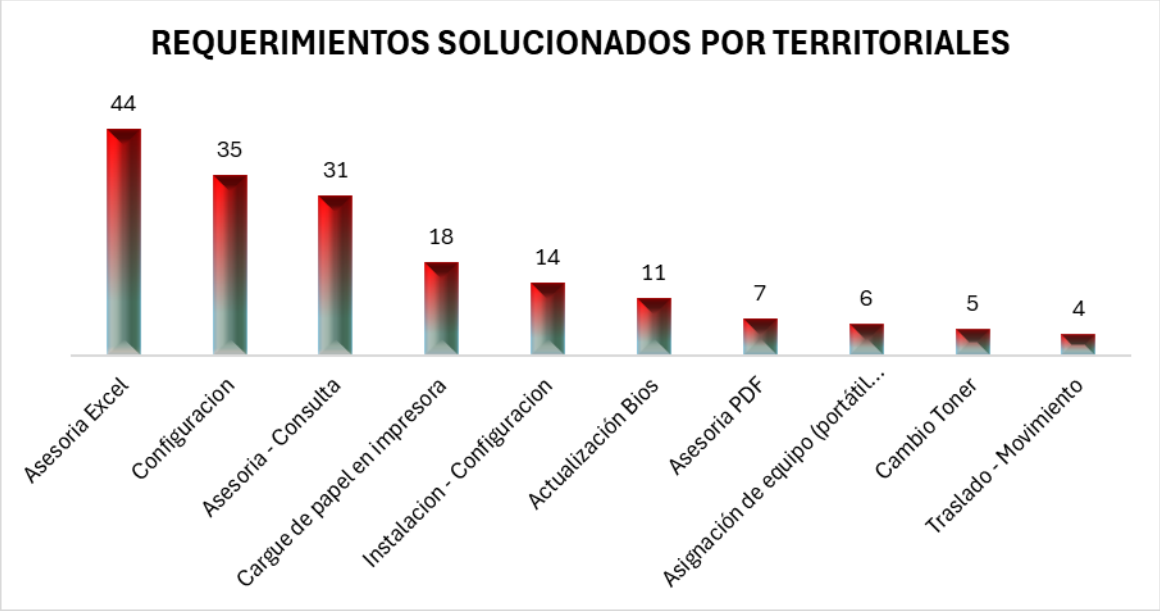


Ilustración 30 Requerimientos Solucionados por Territoriales

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

Casos Cerrados por la Mesa de Servicios: Se indica el top de 10 de Requerimientos cerrados por la mesa de servicios, para el mes de septiembre se cerraron 707 casos, discriminados así: Asesoría – Consulta con 278 casos, Cambiar contraseña con 115 casos, Creación de usuario 81 casos, Cambio de grupo con 40 casos, Inactivar usuario con 24 casos, Aumento de cuota con 20 casos, Relanzamiento y Habilitar usuario con 13 casos, Asignar Radicado TYS con 11 casos, Prestamos con 10 casos, a comparación del mes anterior se evidencia una aumento del 9,33% que corresponden a 66 casos.

CERRADOS POR LA MESA DE SERVICIOS	TOTAL
Asesoría - Consulta	278
Cambiar contraseña	115
Creación de usuario	81
Cambio de grupo	40
Inactivar usuario	24
Aumento de cuota	20
Relanzamiento	13
Habilitar usuario	13
Asignar Radicado TYS	11
Préstamo	10
Configuración	10
Falla Funcional	9
Crear usuario	8
Asignación de equipo (portátil o PC)	7
Backup	6
Caída - Degradación	6
Instalación y configuración VPN	6
Modificar usuarios	4
Lentitud gestora	3
Equipo Datacenter Principal	3
Instalación - Configuración	3
Análisis de evento	3
Accesos por fuerza bruta	2
Asignación - Modificación Roles	2
Creación de VPN	2
Reportar Solicitud/Falla	2
Falla radicación	2
Soporte Aplicaciones Office 365	2
Informes de usuarios	2
Informes y Reportes	2
Reporte de Vulnerabilidades	1
Asignacion de permisos	1
Configuración MFA	1
Apagar servidor	1
Eliminar Hostname	1
Permitir acceso	1
Asesoria Consulta	1
Asesoria Excel	1

Retiro de Licencia	1
Agregar puertos	1
Desbloquear usuario	1
Solicitud Backup	1
Equipo Escritorio	1
Ajustar política	1
Instalar - Configurar	1
Suspender - Finalizar Radica TyS	1
Mantenimiento preventivo	1
Traslado - Movimiento	1
Total general	**707**

Tabla 38 Casos Cerrados por la Mesa de Servicios

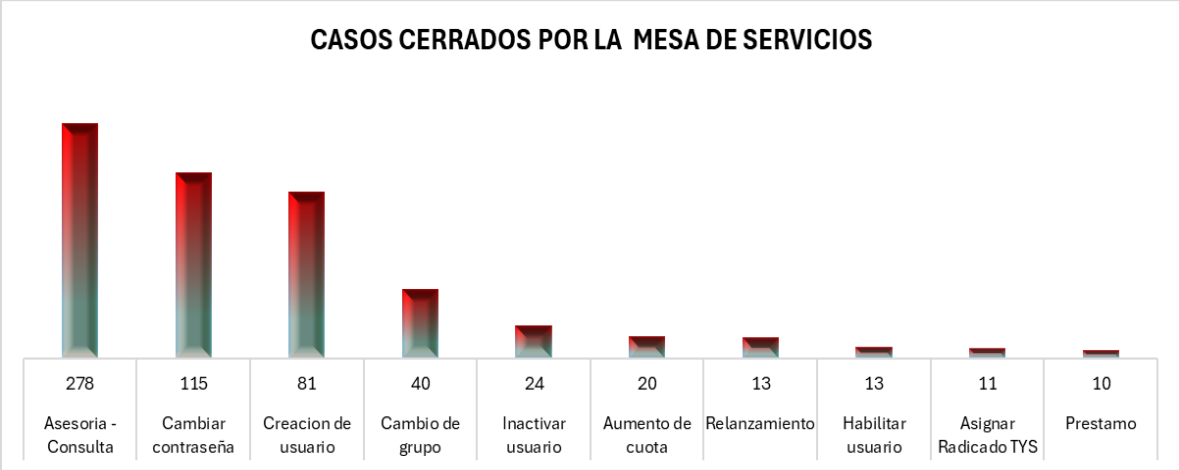


Ilustración 31 Requerimientos Solucionados por Territoriales

Casos Cerrados por Soporte en Sitio: Se indica el top 10 de Requerimientos cerrados por soporte en sitio, para el mes de septiembre se cerraron 1660 casos discriminados así: Cargue de papel en impresora con 432 casos, Asesoría - Consulta con 271 casos, Configuración con 172 casos, Instalación - Configuración con 142 casos, Actualización BIOS con 140 casos, Prestamos con 72 casos, Soporte Aplicaciones Office 365 con 46 casos, Revisión estado del canal con 40 casos, Instalación y configuración VPN con 31 casos, Conectar a red Mintrabajo con 26 casos, a comparación con el mes anterior se tiene una disminución del 18,10% que corresponde a 367 casos.

CERRADOS POR SOPORTE EN SITIO	TOTAL
Cargue de papel en impresora	432
Asesoría - Consulta	271
Configuración	172
Instalación - Configuración	142
Actualización BIOS	140
Préstamo	72
Soporte Aplicaciones Office 365	46

Revision estado del canal	40
Instalación y configuración VPN	31
Conectar a red Mintrabajo	26
Asesoría Excel	24
No imprime	22
Cambiar contraseña	21
Traslado - Movimiento	21
Asesoría Word	21
Aumento de cuota	17
Atasco	16
Asesoría PDF	15
Conectar a red Invitados	12
Instalación - Configuración	12
Asignación de equipo (portátil o PC)	12
Backup	9
Falla - Error conexión a red	7
No enciende	7
Envió y recepción de correos	7
Cambio Tóner	6
Solicitud instalación	5
Instalación-Desinstalación	4
Devolución de equipo (portátil o PC)	4
Lentitud - Bloqueo	4
Crear/Modificar/Eliminar	3
Asesoría en ZIP	3
Borrado seguro Portátil	3
Falla Excel	2
Copia de información	2
Falla Word	2
Solicitud Backup	2
Falla Aplicaciones Office 365	2
Mantenimiento preventivo	2
Asesoría Power Point	2
Falla - error	2
Cambio de unidad fusora	1
Equipo Periférico	1
Inactivar usuario	1
Asignar Pin	1
Solicitud de cambio	1
Daño físico	1

Borrado seguro PC	1
Asesoría - Consulta	1
Informes y Reportes	1
Falla Funcional	1
Error de aplicación	1
Revisar correo malicioso	1
Error sincronización	1
Falla impresora	1
No enfoca	1
Falla radicación	1
Cambio de unidad de imagen	1
Total general	**1660**

Tabla 39 Casos Cerrados por Soporte en Sitio

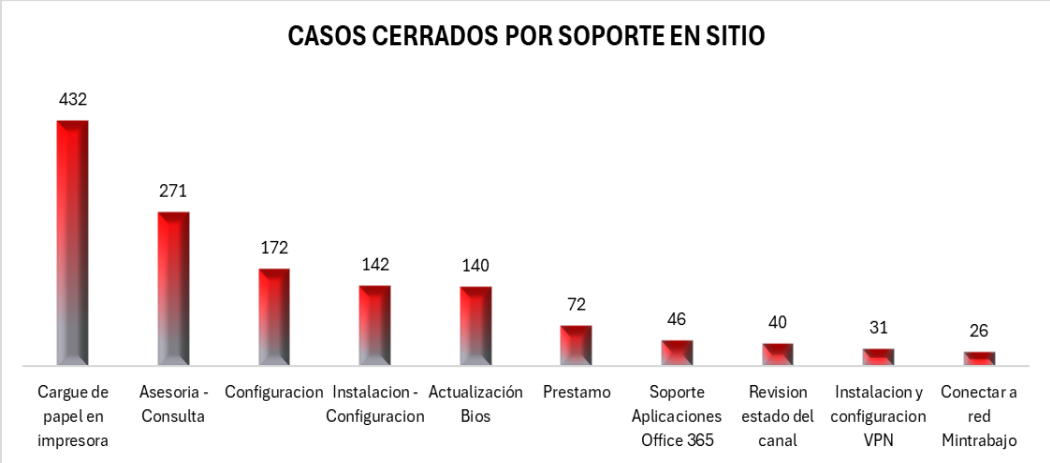


Ilustración 32 Casos Cerrados por Soorte en Stio

Casos Cerrados por soporte en sitio Territoriales: Se indica el top 10 de Requerimientos cerrados por soporte en Territorio, para el mes de septiembre se cerraron 2549 casos discriminados así: Asesoría – Consulta con 457 casos, Cargue de papel en impresora con 372 casos, Configuración con 320 casos, Instalación - Configuración con 264 casos, Actualización BIOS con 235 casos, Asesoría Excel con 126 casos, Mantenimiento Preventivo con 98 casos, Asesoría Word con 98 casos, Cambio Tóner con 81 casos, Asesoría PDF con 79 casos.

CATEGORIA	CANTIDAD
Asesoría - Consulta	457
Cargue de papel en impresora	354
Configuración	288
Instalación - Configuración	250
Actualización Bios	224
Mantenimiento Preventivo	98

Asesoria Word	85
Asesoría Excel	82
Cambio Tóner	76
Asesoría PDF	72

Tabla 40 Top 10 Casos Cerrados por Soportes Territoriales

- Casos Atendidos a Usuarios VIPS

Durante este periodo se crearon 1836 solicitudes para ser atendidas por soporte en sitio, de estas solicitudes se evidenciaron 109 casos creados para VIPS los cuales fueron atendidos y solucionados dentro de los ANS establecidos por la entidad, discriminados a continuación por tipo de caso:

TIPO DE CASO_VIPS	CUMPLIMIENTO	NO_CUPLE	TOTAL
Incidentes	1		1
Requerimientos	69	1	70
Total general	**70**	**1**	**71**

Tabla 41 Casos Atendidos usuarios VIPS

Se atendieron 1765 solicitudes para el resto de los usuarios discriminados así:

TIPO DE CASO-NO-VIPS	CUMPLIMIENTO	NO_CUPLE	TOTAL
Incidentes	87		87
Requerimientos	1675	3	1678
Total general	**1762**	**3**	**1765**

Tabla 42 Casos Atendidos usuarios

- Medio de Ingreso de Casos

Durante el período ingresaron a la mesa de servicio 7371 casos a través de los diferentes medios que se tiene habilitados para la atención de solicitudes, como son correo, extensión telefónica, portal de autogestión, alarma de Zabbix, casos creados de forma automática por las diferentes herramientas:

MEDIO DE INGRESO DE CASOS	TOTAL
Gestión Técnica	4404
Correo SoporteMT	1747
Alarma Zabbix	930
Telefónico	257
Alarma Fortisiem	28
Portal Autogestión	3
Case Creador Mesa de Servicios	2
Total general	**7371**

Tabla 43 Medios de Ingreso de Casos

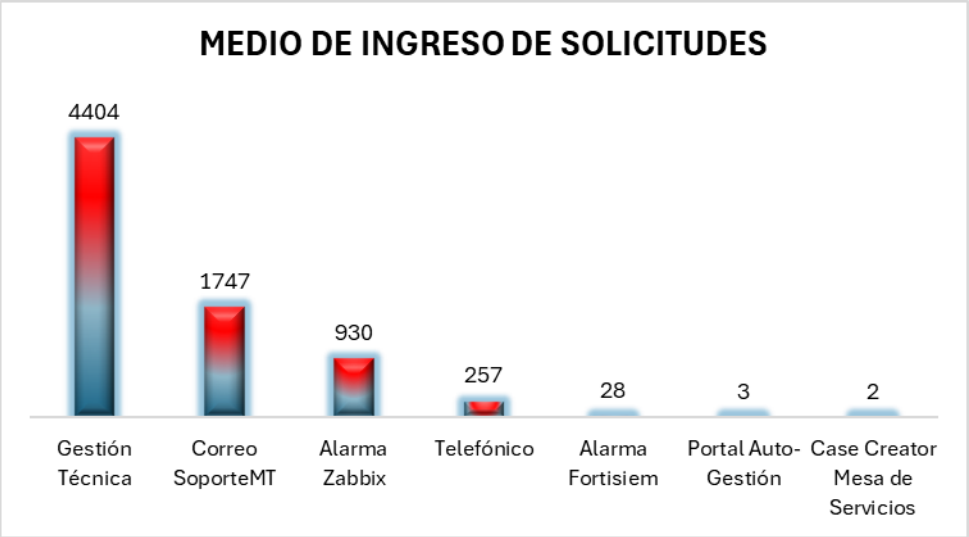


Ilustración 33 *Requerimientos Solucionados por Territoriales*

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 septiembre 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 septiembre de 2025 los profesionales de soporte en sitio territoriales llevaron a cabo las siguientes acciones:

Visita a 12 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.

Intervención de 2813 casos, dentro de los que se destacan: Asesorías –Consultas sobre aplicaciones de la línea base de software, Cargues de Papel en las impresoras de las diferentes Sedes, Configuraciones e Instalaciones de software y aplicaciones de ofimática, Actualización de BIOS, Asesorías en Excel, Mantenimiento Preventivo de Impresoras, Asesoria Word, Cambio de Toner y Asesorías en PDF.

Se realizó el arreglo de la estructura del Rack en Barranquilla y en Popayán de acuerdo con la solicitud de los administradores de redes.

Se terminó el proceso de actualización de la versión de BIOS en los equipos es escritorio y en los portátiles que se encuentran en las sedes de acuerdo con los lineamientos a nivel

nacional, quedando pendiente los equipos que están fuera de las oficinas y de los usuarios no han regresado a las Sedes.

- 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
Sep 2025	Valle	Buenaventura	Actualización BIOS	Se ejecutó el proceso de actualización de la BIOS siguiendo las instrucciones técnicas del fabricante, asegurando que el equipo permaneciera conectado a la corriente durante la instalación.	RF-147872
Sep 2025	Cordoba	Lorica	Movimiento de equipos	Se realiza el traslado e instalación de equipos de cómputo y periféricos de impresión, requerido por procesos de adecuación física	RF-148474
Sep 2025	Guajira	Barrancas	Reconexión de Equipos	Se realiza la reconexión de los cables de red y los de corriente, una vez conectado los equipos se realiza una prueba de conexión a internet desde el equipo de escritorio, se obtiene resultados positivos con la conexión a la red del ministerio de trabajo.	RF-147293
Sep 2025	Apartadó	Turbo	Actualización BIOS	Se ejecutó el proceso de actualización de la BIOS siguiendo las instrucciones técnicas del fabricante, asegurando que el equipo permaneciera conectado a la corriente durante la instalación.	RF-149304
Sep 2025	Cundinamarca	Villeta	Actualización BIOS	Se ejecutó el proceso de actualización de la BIOS siguiendo las instrucciones técnicas del fabricante, asegurando que el equipo permaneciera conectado a la corriente durante la instalación.	RF-149228
Sep 2025	Apartadó	Turbo	Internet y Navegación	Se realiza visita a oficina Turbo, se evidencia servicio operativo, última milla, proveedor informa que la causa fue: daño en el domo por vandalismo. La solución fue: personal de infraestructura realizó la reposición del elemento hurtado, garantizando así el total funcionamiento del enlace	IM-149277
Sep 2025	Valle	Palmira	Actualización BIOS	Se ejecutó el proceso de actualización de la BIOS siguiendo las instrucciones técnicas del fabricante, asegurando que el equipo permaneciera conectado a la corriente durante la instalación.	RF-151005
Sep 2025	Cundinamarca	Soacha	Internet y Navegación	Se realiza revisión de la conexión del equipo a la red en la cual se evidencia deterioro en el cable de red, el cual ocasiona la intermitencia y en ocasiones falla de conectividad, se procede con el cambio de cable y ajuste en las conexiones de red	RF-152071
Sep 2025	Valle	Buga	Internet y Navegación	Se realiza verificación de los equipos locales y del estado de red interna luego de la intervención del proveedor, sin encontrar fallas físicas ni conflictos de configuración	RF-151859
Sep 2025	Magdalena	Fundación	Internet y Navegación	se validan las conexiones de red evidenciando que el cable se encuentra con deterioro. se procede a realizar cambio de del cableado. se realizan pruebas de manera exitosa	RF-150596

Tabla 44 Visitas a Sedes sin Soporte

- Medición ANS Mesa de Servicios

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

Area	Nombre del Indicador	Resultado	Meta
Mesa de Servicio	Tiempo de atención de solicitudes por soporte en sitio	99,33%	95,00%
	Tiempo de solución de incidentes por soporte en sitio	100,00%	90,00%
	Tiempo de solución de requerimientos por soporte en sitio	99,79%	90,00%
	Tiempo de respuesta de la mesa de servicio	100,00%	85,00%
	Abandono de llamadas	0,70%	Maximo 8,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 45 Medición de ANS Mesa de servicios

3 LINEA DE SERVICIOS CENTRALES

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

3.1 Datacenter Principal

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

Se observó un comportamiento de crecimiento la asignación de licencias de Office 365 reportados a través de ARANDA, donde se realizó la atención de 91 requerimientos asociados a esta categoría del servicio de Windows, así como la creación, modificación de usuarios que mantiene un reporte de 20 casos para el mes de septiembre. De la mano de asignación de licencias se atendieron 16 requerimiento asociados a configuración de MFA y 10 casos adicionales de apoyo en configuraciones del servicio de Office 365. Las categorías restantes asociadas al servicio de Windows se mantienen con un reporte bajo reflejando la estabilidad del servicio de cara a usuario final. De la mano de los procesos de administración, se realiza depuración de los equipos de usuario final reportados como inactivos y se procede con la depuración de 402 equipos movido a a la UO de Deshabilitados_Equipos.

De igual forma el equipo de Windows realizó la ventana de parchado sobre la infraestructura Windows Server 2016-2019 y 2022 así como el parchado individual de los servidores con OS 2012 R2. Se excluyen del parchado los servidores versión 2008 debido a su obsolescencia y el impedimento de instalación de actualizaciones ya que se encuentran fuera de soporte.

De acuerdo con solicitud expresa de la entidad, se procede con la ejecución de comando Shell para la purga de correo electrónico con Asunto: *¡Atención! Entrega de bono*

cumpleaños - Segundo trimestre 2025 (junio-julio-agosto). El cual contenía información sensible y fue enviado de manera masiva.

Dentro de las labores de administración se encuentran actividades tales como revisar regularmente la base de datos de usuarios para identificar cuantas inactivas, duplicadas o desactualizadas, y proceder con su eliminación o actualización según sea necesario. 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.

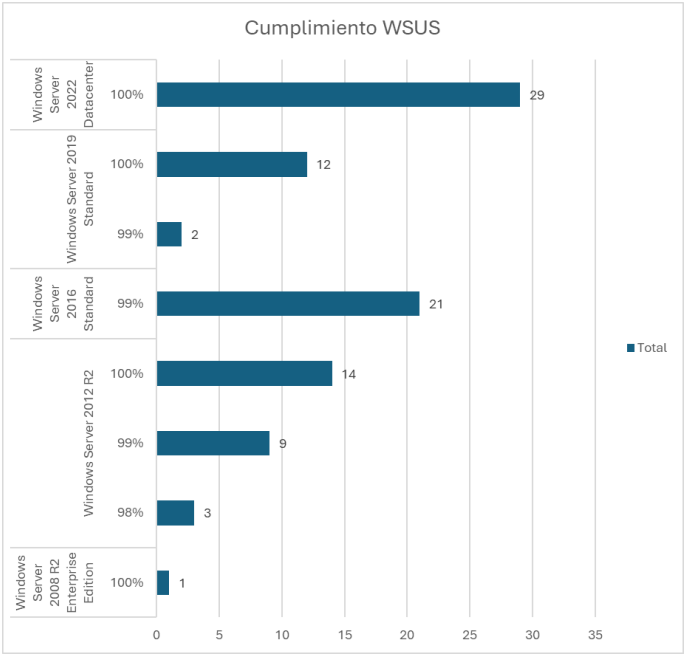


Ilustración 34 Cumplimiento WSUS

La interacción de los requerimientos de servicio asociados al equipo de trabajo de Windows está relacionada en su gran mayoría a asesoría y consultas que generan los funcionarios con respecto al funcionamiento de los servicios de Office 365 a los cuales tienen acceso,

seguido por los casos en donde se requiere de algún tipo de configuración sobre sus cuentas, shared mailbox o servicios a los que acceden. Se ha reducido la solicitud de generación de backups significativamente con respecto a meses anteriores y es un comportamiento habitual en el reporte mensual de este tipo de casos.

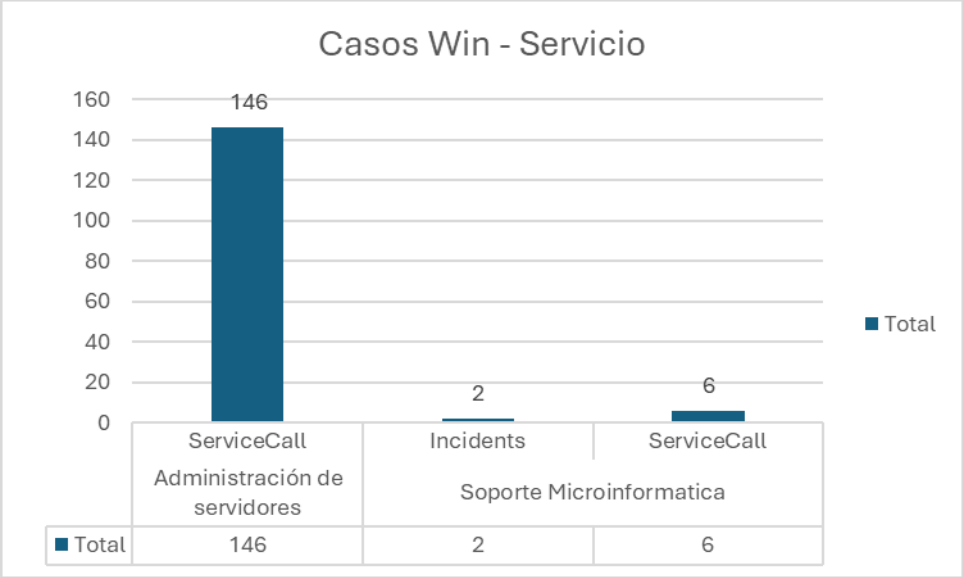


Ilustración 35 Casos Win Servicio

Con respecto a los requerimientos del servicio de Nube privada su categorización nos indica que el comportamiento de reportes asociados a servidores Windows es de mayor demanda en el proyecto, asociado a configuraciones de servicios, revisión de consumo de capacidades a través de alertamientos de la herramienta de Monitoreo Zabbix o solicitud de accesos a carpetas compartidas del servicio de File Server. Se ha venido trabajando articuladamente con la Coordinación de Soporte Informático manteniendo informado del comportamiento de la nube privada y sus capacidades. Así como el apoyo transversal en los proyectos escalados por las áreas funcionales. Es importante mencionar que se ha venido creando diferentes VM asociados a nuevos servicios que aprovisionará el Ministerio del Trabajo, pero en principio se encuentran en su fase de pruebas por lo cual solo se han creado VM de pruebas.

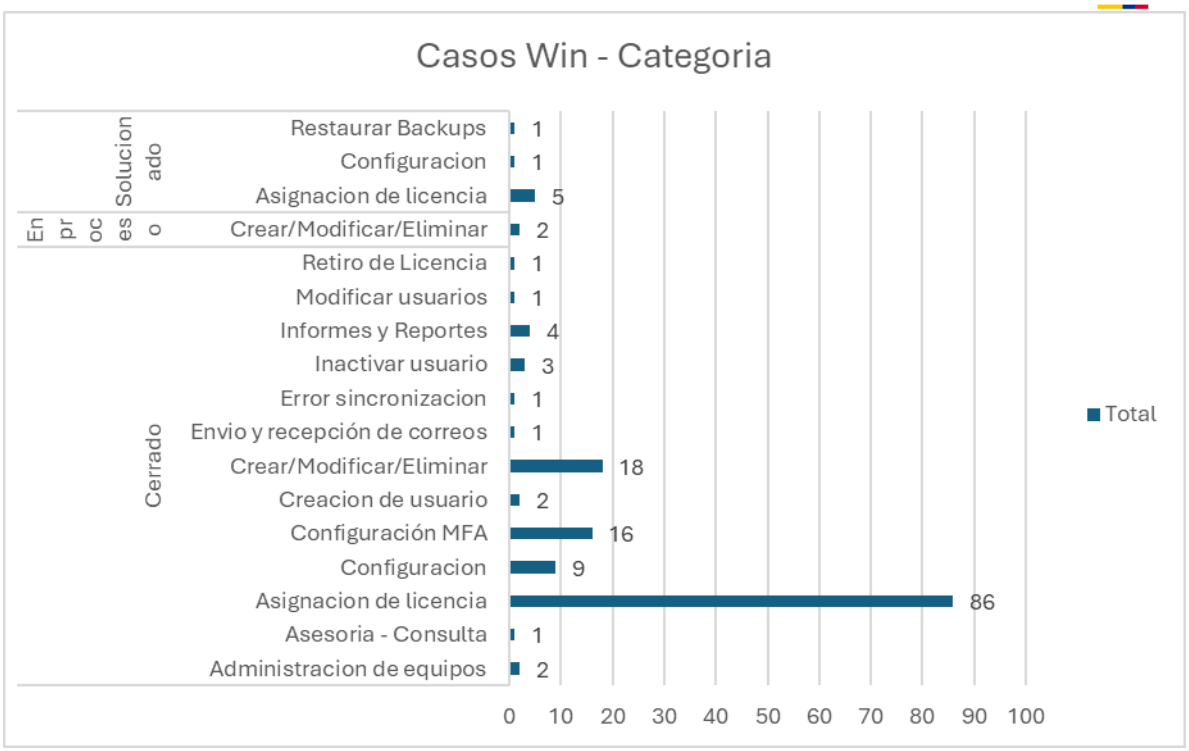


Ilustración 36 Estado final de los casos Nube privada

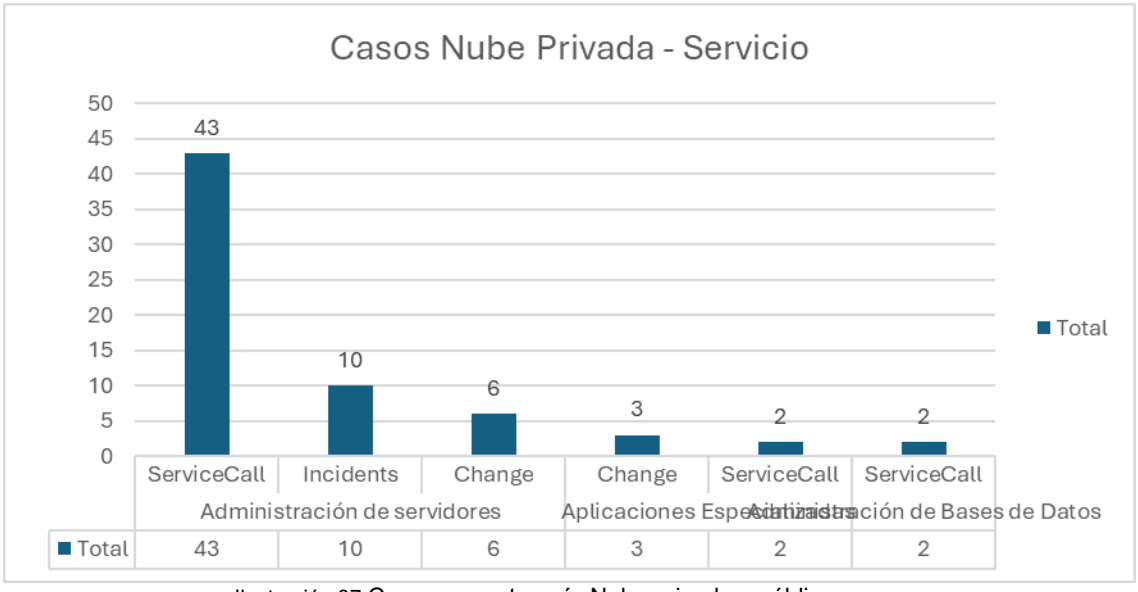


Ilustración 37 Casos por categoría Nube privada y pública

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 46 Capacidades contractuales

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 47 Consumo de capacidad con servidores para desaprovisionar + ambientes de pruebas)

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 48 Consumo de capacidad Sin servidores para desaprovisionar con ambientes de pruebas

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

Tabla 49 Consumo de capacidad Sin servidores para desaprovisionar sin ambientes 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 50 Consumo de capacidad Servidores Pruebas y Desarrollo

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 51 Consumo de capacidad actual

Es importante mencionar que, en el proceso de redimensionamiento de la nube privada de la entidad, los ambientes de pruebas son los que están 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 está trabajando en una política de retención de backups de usuario final, ya que estos backups están consumiendo una cantidad importante de almacenamiento en el file server y a largo plazo se puede convertir en una actividad y/o tarea demandante de almacenamiento y de tareas operativas que puede convertirse en una solución no sostenible dadas las capacidades de almacenamiento contratadas.:

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.

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.

De acuerdo con lo anterior se realizó el inventario de flujos creados en Microsoft Fabric y de tablero Power Bi incluyendo componentes que hacen parte de la solución de la cual hace parte el sistema SICIP.

Se observa que tras una ventana de mantenimiento ejecutada por el proveedor Global Hits se han venido presentando inconsistencias en el aplicativo SICIP en los siguientes módulos:

Asignación de roles
Asignación de desplazamientos
Cargue de archivos en varios tramites
Usuarios sin poder asignar tramites

Estas inconsistencias se han generado desde el día 24 de agosto y reportadas a inicio de septiembre por el área funcional.
Como aclaración la última actualización que se realizó en el aplicativo fue la modificación de validar valores nulos que llegaran desde la base de datos de Oracle, las modificaciones en código no deberían afectar los demás flujos dado que llegan a la tabla temporal de dbo.

Correspondencia. Se esta a espera de retroalimentación por parte del proveedor en mención.

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

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

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

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

Responsabilidades

Cada miembro de la organización debe:

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

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

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

Así mismo, se 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.

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

- Atenciones: la actualización desde el origen de datos 01/06/2024
- Capacitaciones y cieti: la actualización desde el origen de datos 01/05/2026
- 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. Hasta el momento no se ha realizado la pausa de servicios ni se ha obtenido retroalimentación acerca del tema.

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

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

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

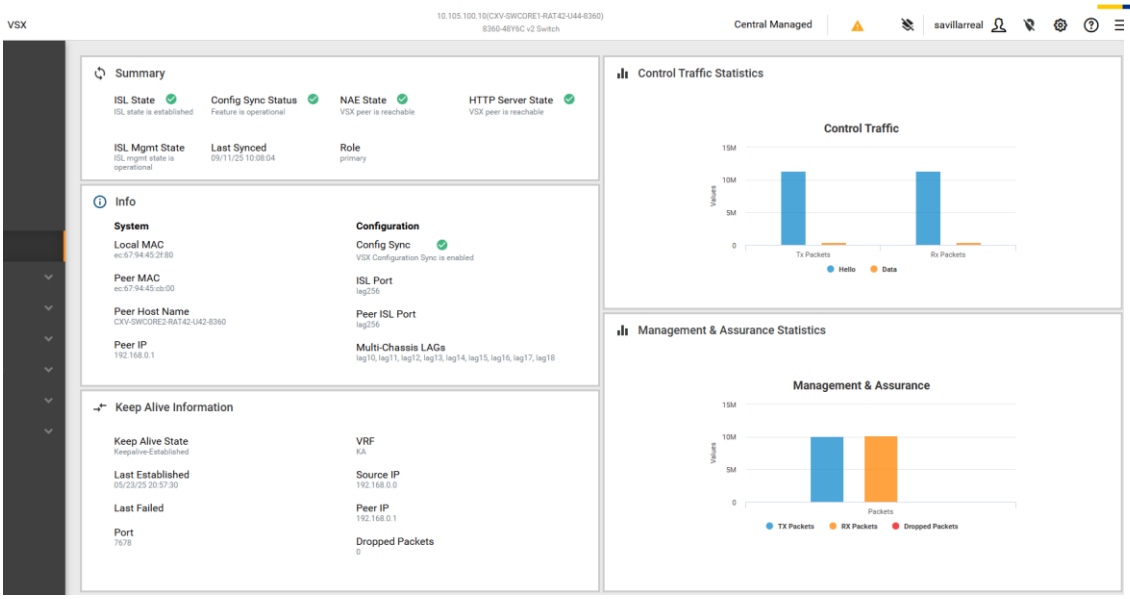


Ilustración 39 Sincronización HA de los Switch Core

El canal centralizado de Internet en Datacenter se mantuvo estable, la navegación de todas las sedes se ve reflejado en este canal. Se relaciona gráfica de comportamiento del canal de Internet en Datacenter, donde se observa que no se tuvieron caídas de servicio. Se observa que se tuvieron picos altos de consumo sin afecta el rendimiento del canal, se observa un flujo estable de tráfico, se tuvo un consumo promedio de entrada de 321.71 Mbps y 513.62 Mbps de salida

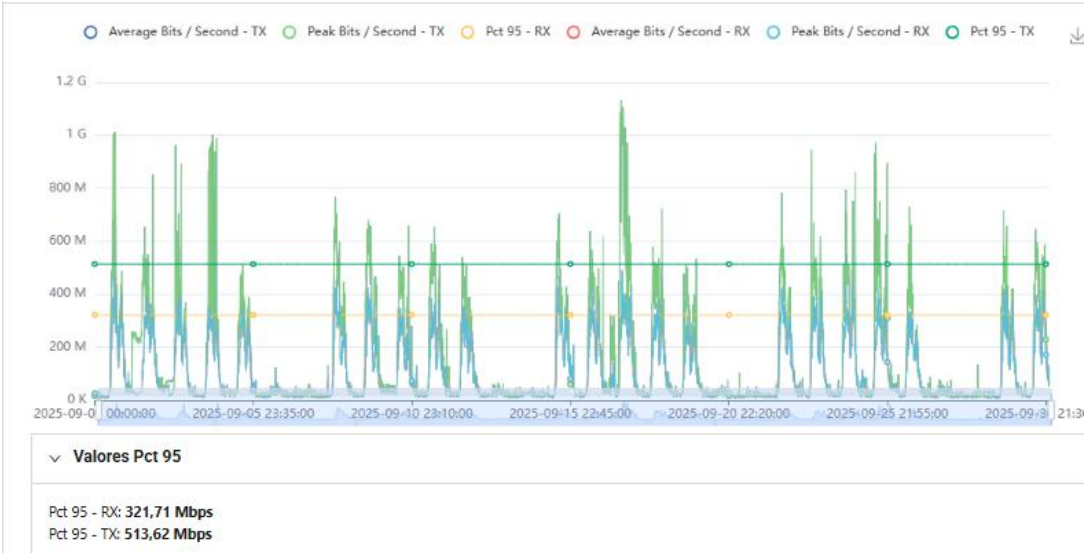


Ilustración 40 Grafica de consumo canal Internet Datacenter

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

3.1.1 Datacenter Alterno y DRP

Se validaron procesos, actividades relacionadas con la migración y sincronización a través de VMware que permitan una correcta visualización de los recursos a replicar de Datacenter a Datacenter. Se valida procesos y actividades de sincronización a través de VMware que permitan una correcta visualización de los recursos a replicar de Datacenter a Datacenter. Se continuó con las actividades de fase 1 para DRP priorizando la replicación de controladores de dominio para así garantizar procesos de autenticación de usuario final y aplicación. Se añaden privilegios de visualización entre VLAN para garantizar comunicación de cada servicio aprovisionado en el entorno aislado de DRP, esto con el fin de evitar problemas de comunicación entre recursos y garantizar un escenario de replicación adecuado.

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

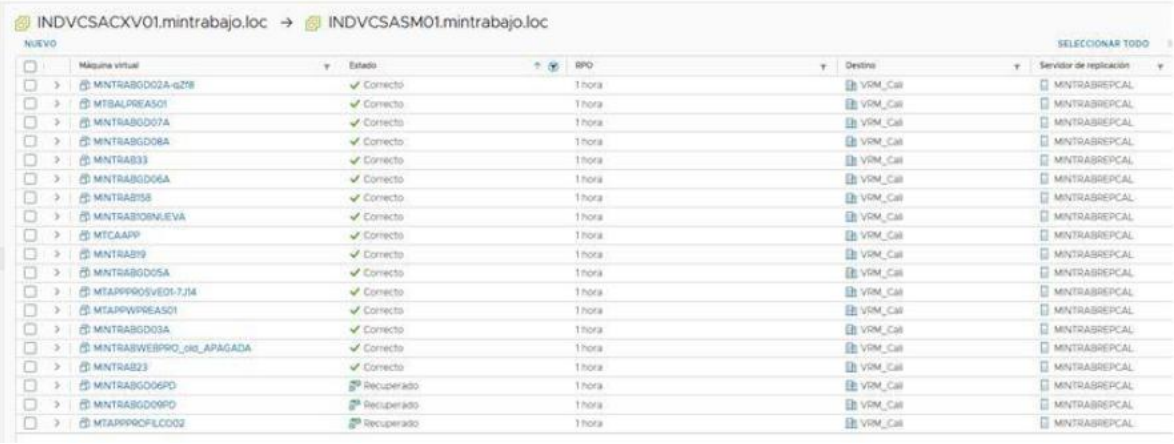


Ilustración 41 Captura de imagen máquinas virtuales

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

Actualmente se están realizando las adecuaciones de segmentación de red para preparar el escenario de pruebas para el último trimestre del año de cara a las aplicaciones .NET de acuerdo con lo socializado con la entidad.

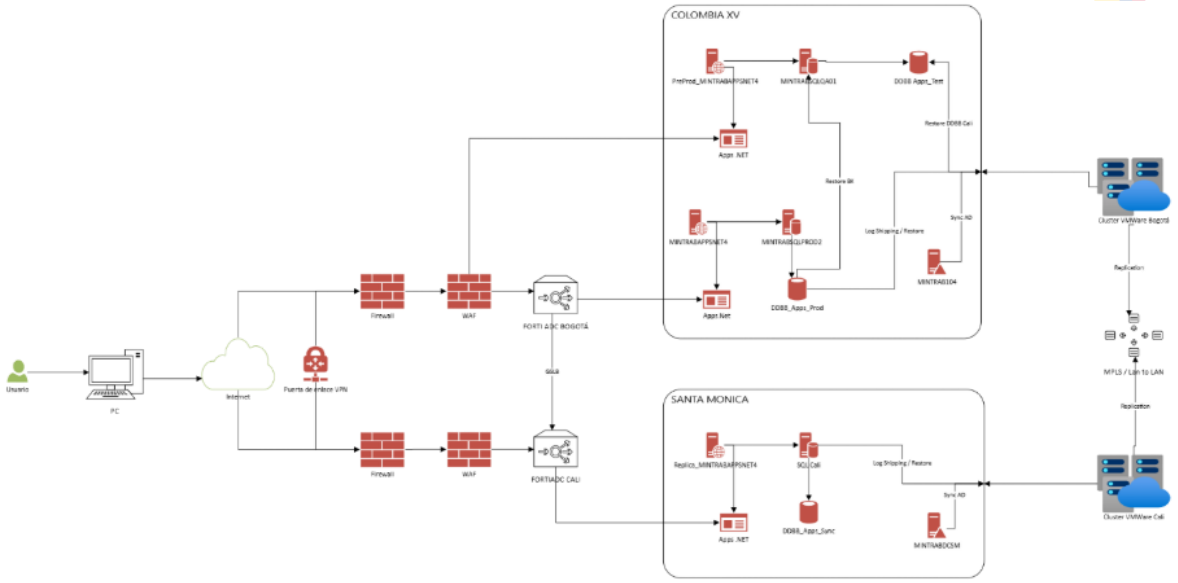


Ilustración 42 Escenario de pruebas Aplicaciones y AD

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 100 Kbps de entrada y 120Kbps de salida. Se relaciona las gráficas de consumo de ambos extremos

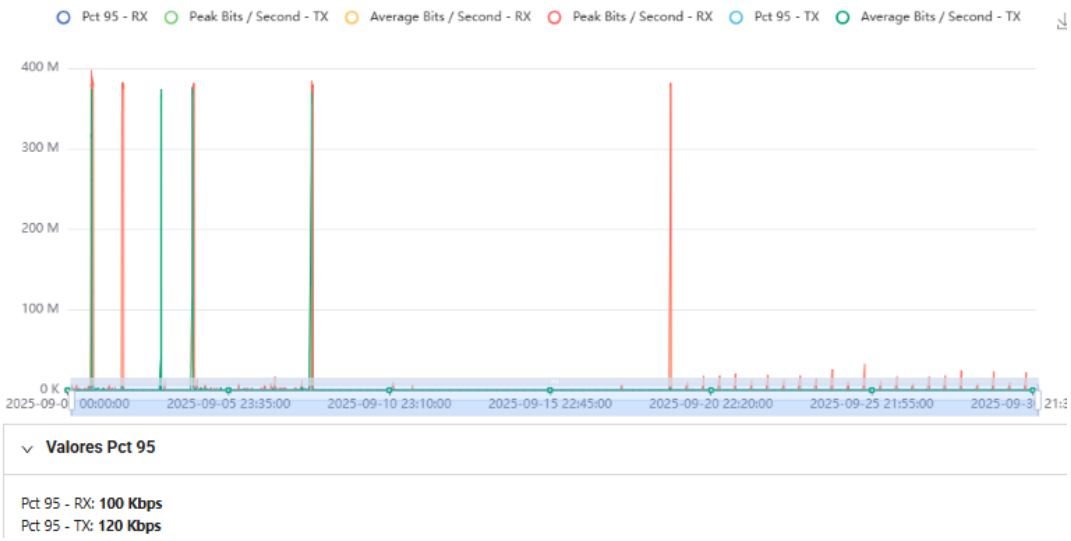


Ilustración 43 Extremo DC Bogotá

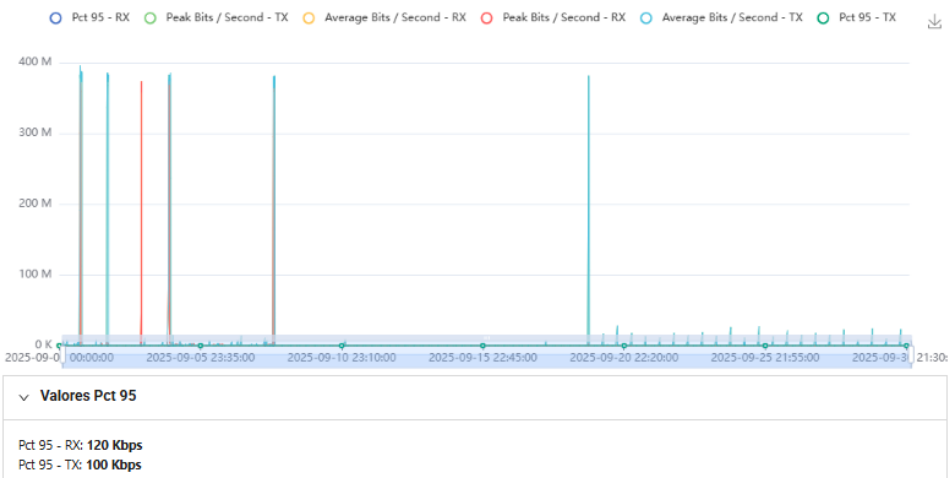


Ilustración 44 Extremo DC Cali

El canal de Internet de datacenter alterno se encuentra operativo, se observa que el canal tiene poco tráfico ya que el tráfico general se usa el canal ubicado en DC Principal.

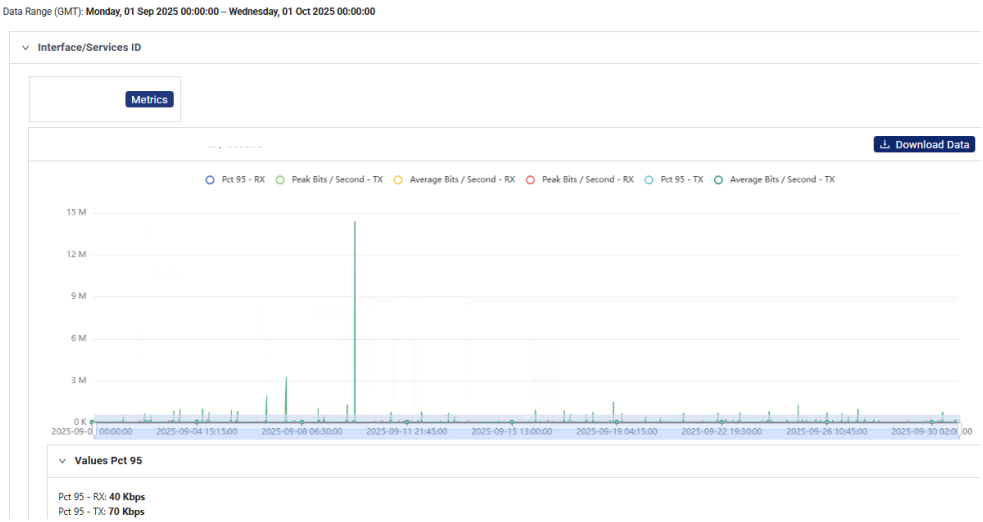


Ilustración 45 Estado canal de Internet DC Cali

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

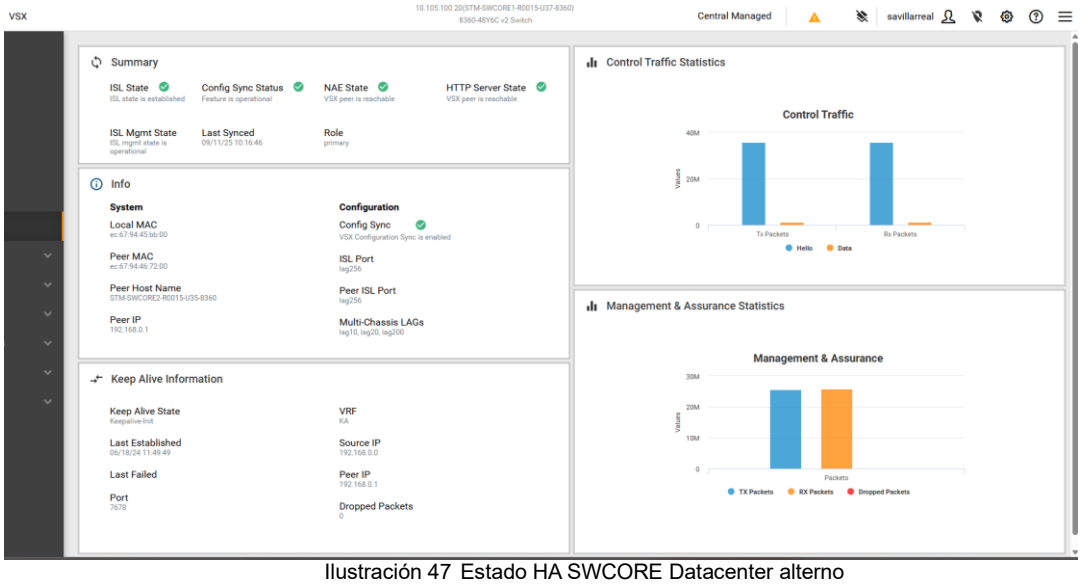


Ilustración 47 Estado HA SWCORE Datacenter alterno

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

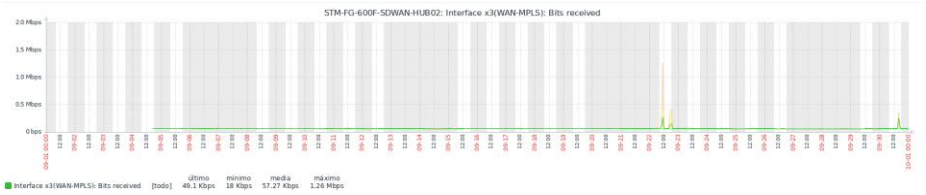


Ilustración 48 Consumo canal MPLS DC Alterno

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

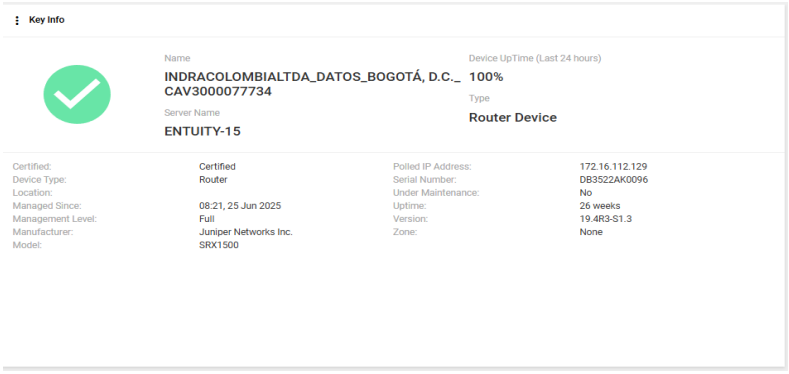


Ilustración 49 Estado Router MPLS DC Alterno

3.1.2 Procesamiento, Almacenamiento y Respaldo

- Servidores Windows e Infraestructura Virtualizada

Se mantuvo la validación periódica de la topología y la arquitectura del Directorio Activo como un componente esencial para asegurar su correcto funcionamiento y su alineación con las necesidades y los objetivos empresariales. Esta validación garantiza la escalabilidad y la flexibilidad del sistema para adaptarse a futuros cambios en la infraestructura o en los requisitos del negocio, esto en el marco de la implementación de nueva infraestructura tecnológica y de la sincronización de máquinas virtuales al nuevo vCenter de VMWare.

Se continúa con la ejecución del plan de backups en donde se generan respaldos completos de todas las máquinas virtuales críticas alojadas en VMWare, este plan de backup en la actualidad se ejecuta los viernes en la noche generando un backup full de la semana de cada máquina y su almacenamiento, garantizando un punto de retorno semanal en caso de contingencia o incidencia crítica, durante los procesos de afinamiento se ha identificado la criticidad y propuestas de planes de backups totales e incrementales para estas. En donde se identificaron máquinas que, por su criticidad y servicios alojados, ameritan un plan de Backup incremental diario, ya sea de discos, base de datos o máquina virtual completa,

dependiendo del escenario y el tipo de máquina virtual. A este plan de Backups se han añadido servidores que han sufrido intervenciones técnicas con finalidad de adecuar la infraestructura virtualizada y depurar máquinas virtuales que no se encuentran en uso por parte de la entidad, pero sí que consumen capacidades que pueden ser aprovechadas por los entornos productivos.

Es importante mencionar que el escenario de arquitectura de la entidad actual ha permitido como operador de servicios tecnológicos, identificar diversas acciones de mejora que se han venido ejecutando de manera transversal desde el inicio del contrato, pero es importante dar visibilidad de los escenarios observados. Durante los procesos de afinamiento y egreso de equipos no productivos en Datacenter se logra visualizar componentes en estado sensible que podrían poner en riesgo la disponibilidad de servicios críticos como lo es el sistema de información histórica de nómina. Se observa que el servidor físico que aloja la máquina MINTRAB13 es un Dell (PowerEdge 2950) con fecha de salida a mercado 19/10/2015 y cuenta con un OS SUSE Linux Enterprise Server 11 (i586) con fecha de salida al mercado 24/10/2016.

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

Se dio visibilidad de esta situación para realizar las maniobras técnicas correspondientes de manera coordinada con el proveedor de este software a la entidad durante el mes de julio de 2024 se realizó esta sesión, en donde se identifican los servidores productivos como parte del escenario de virtualización de la entidad y que su proceso de migración a nuevos servidores de aplicación puede surtirse de la mano del área funcional. 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 estos orientados a Infraestructura de acuerdo a las buenas prácticas y experiencia del equipo de trabajo. No se definen tiempos claros para estos recursos ni para documentos virtuales, file server o backups de usuario final por parte de la entidad.

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

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

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

A la fecha el equipo de Ministerio no ha confirmado el proceder con la maquina SDTCUNDI01 la cual continúa encendida y sin retroalimentación por parte de la entidad.

Para la maquinas MINTRAB25 que se encuentra en un escenario similar, se inicio el proceso de migración a Windows Server 2022 y validar funcionamiento de los componentes de capa media alojados en la maquina MINTRAB25 en nuevo versionamiento, con el fin de garantizar una actualización de OS y componente de Capa media y poder dar de baja esta infraestructura.

De acuerdo con los procesos de migración a OS 2022, se confirma que también se han venido realizando apagados controlados bajo RFC estándar de Infraestructura obsoleta en desuso y tras autorización previa de la entidad, lo cual ha generado reducción de vulnerabilidades sobre la nube privada y depuración de las capacidades adicionales que consumían previo a migraciones de OS 2022

Hostname	IP	Numero RFC
MINTRAB33	172.20.22.22	RFC-153285
MINTRAB91	172.20.22.127	RFC-153278

Tabla 52 Maquinas desaprovisionadas propiedad de la entidad

3.1.3 Aplicaciones Especializadas

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

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

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

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 despliegue posteriormente a producción.

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

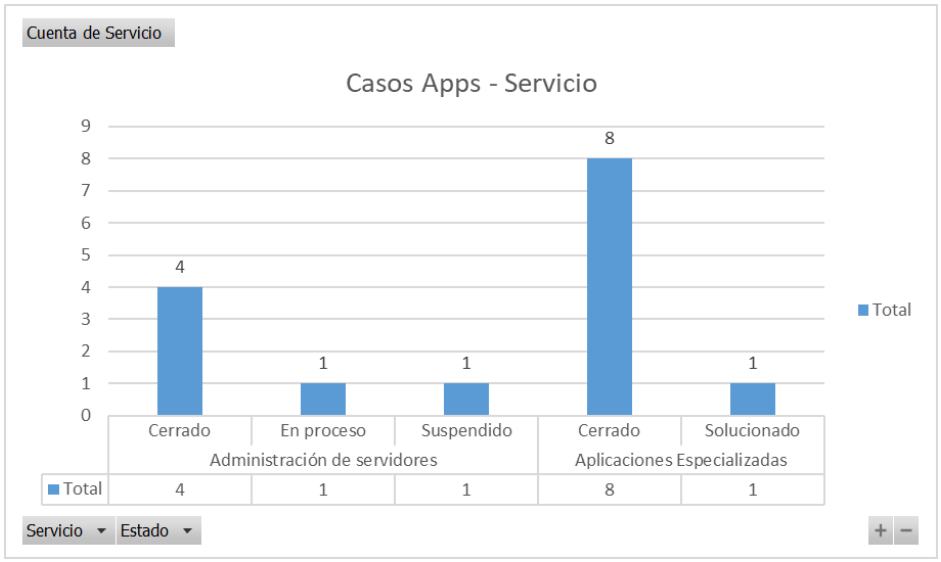


Ilustración 50 Casos App Servicio

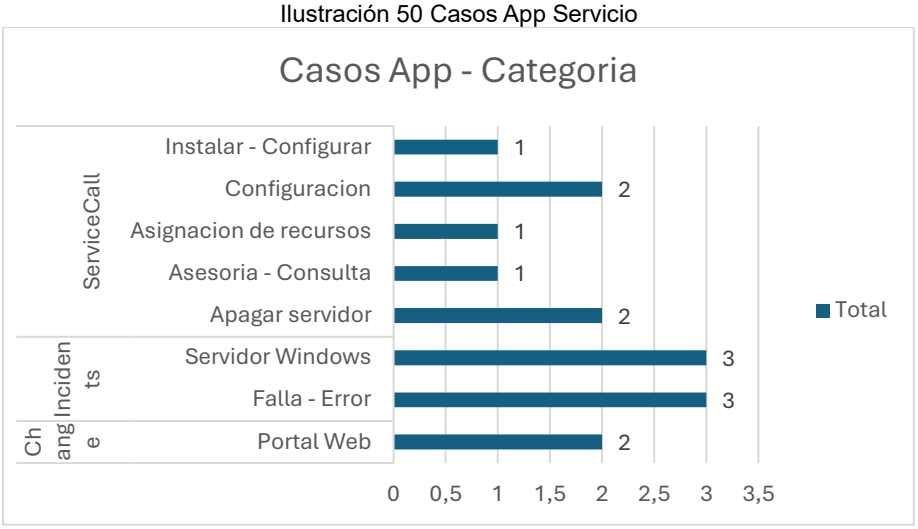


Ilustración 51 Casos App Categoría

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

Escenario SIAS:
Pendientes:

- IVC recopilaría la información de los sindicatos que accederían al sistema para escalar la creación de usuarios VPN que tengan estrictamente acceso a SIAS y a ningún otro recurso tecnológico. Esta información actualmente no ha sido remitida para iniciar con el proceso de creación de usuarios.
- 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 aún se está a espera de información hacía la Oficina TIC y el Grupo de Soporte Informático.

- Tras avance en el desarrollo, la entidad determina que el sistema no se encuentra listo para salir a producción.

De acuerdo con los tickets RF-154278, RF-154044, RF-154384 y el IM-154045, se ha identificado que en el servidor 172.20.42.101 - MTAPPWPREAS01 el disco C: ha superado el umbral del 90% de ocupación.

La causa principal corresponde al crecimiento de la carpeta asociada a IIS, lo que incrementa el riesgo de que el sistema quede sin espacio disponible. Al tratarse de la unidad C:, donde reside el sistema operativo, esto podría generar indisponibilidad del servidor y afectar la continuidad del servicio.

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

Se comparten las evidencias de dicho umbral.

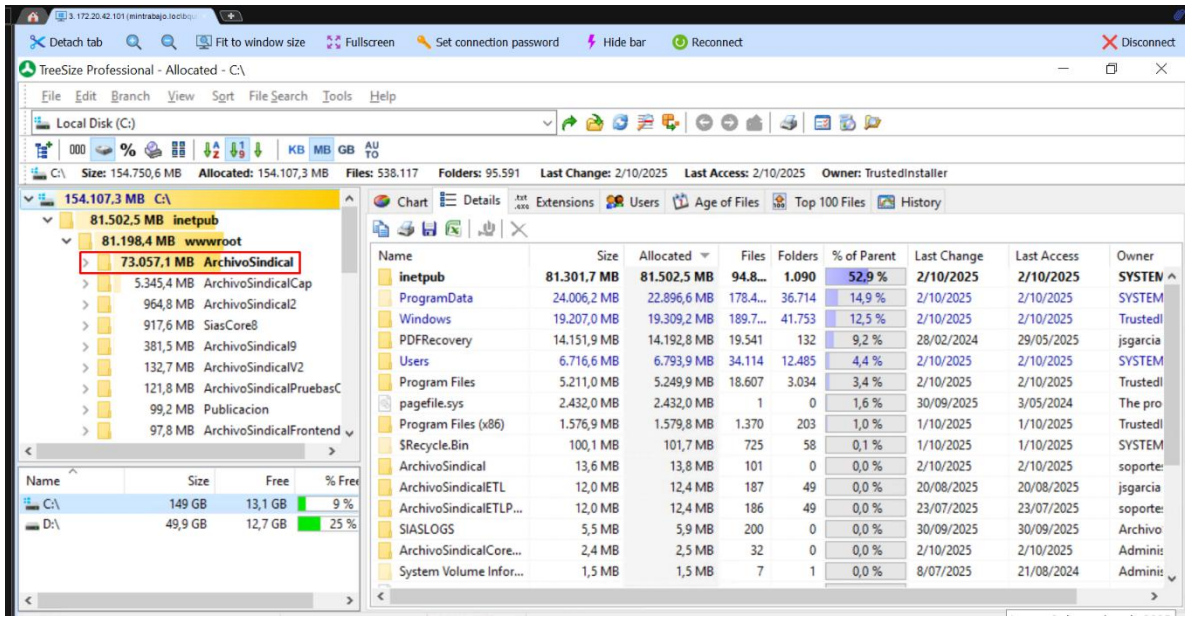


Ilustración 52 Tamaño Archivo Sindical

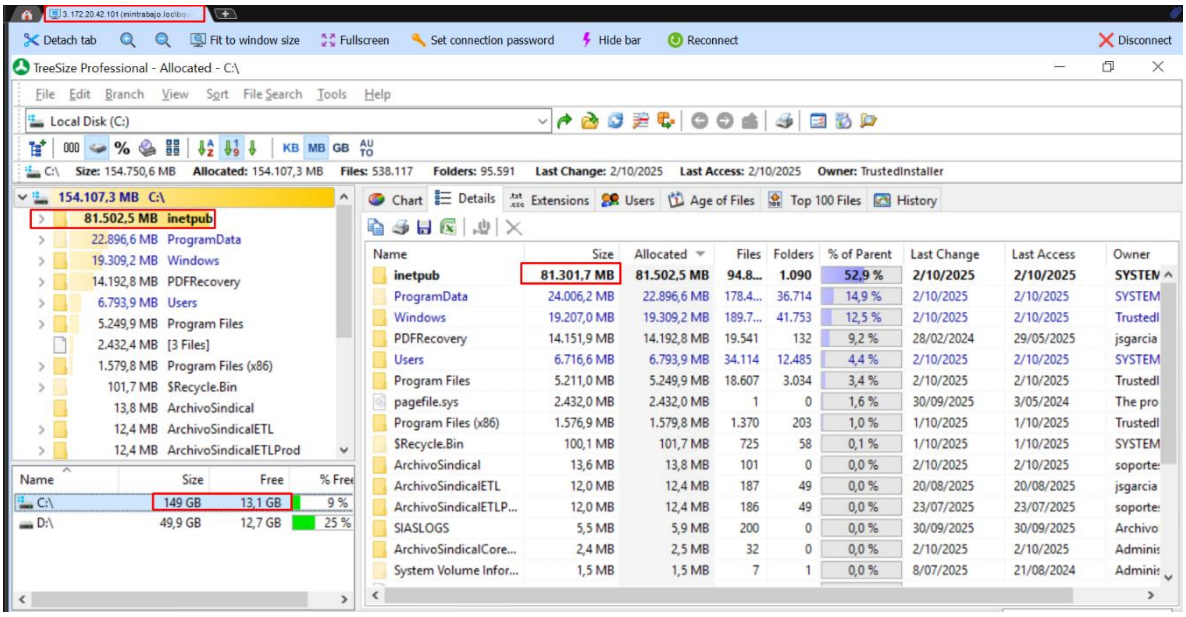


Ilustración 53 Tamaño IIS

Escenario FILCO:

Pendientes:

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

- Es necesario crear los tipos documentales (Nombres y campos) por lo cual es requerida esta matriz de información de los documentos que se necesitan sincronizar con el micrositio de la página web.

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

Migración Aplicaciones .NET

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

transferencia del sistema para su validación y uso por parte del equipo del Ministerio.

4. Alcance del despliegue: Es importante resaltar que el alcance de este despliegue corresponde únicamente a la instalación técnica del sistema y su puesta en marcha en un entorno de pruebas. Las actividades de ajuste funcional, adecuación del código fuente, integración con sistemas existentes y mejoras de rendimiento deberán contemplarse en fases posteriores.

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

- El sistema de información tiene una implementación muy similar a varias aplicaciones desarrolladas en lenguaje .NET que posee actualmente la entidad.
- El sistema de información viene de una transición de versionamiento de sistemas operativos y base de datos deprecado (versiones 2012) que actualmente, la versión que está siendo desarrollada y por liberar por parte del DNP (versión 2.0) posee una actualización a versiones 2019.
    - El equipo de Servicios Centrales de la UT se encuentra en proceso de actualización a versionamiento 2022 de Sistema Operativo Windows y de Base de datos SQL Server.
    - SISGESTION tiene aval y despliegue correcto en sistema operativo y base de datos 2019, no se ha probado por parte del DNP en versión 2022. Pueden existir problemas de compatibilidad, en principio debería funcionar de manera adecuada, pero lo ideal es que la aplicación sea probada en entornos 2022 para validar el funcionamiento adecuado en esta versión de sistema operativo y de base de datos.
- El sistema de información SISGESTION tiene una dependencia en su desarrollo con un componente INFRAGISTIC el cual es un componente que según informa el equipo de Tecnología de DNP, se encuentra fuera de soporte y se encuentran en etapa de desarrollo para eliminar la dependencia de este componente, el cual genera problemas de compatibilidad con los navegadores actuales (Google Chrome, Microsoft Edge y Mozilla Firefox) lo cual degrada la experiencia del usuario final, ya que la herramienta no se comporta de manera adecuada. o La versión que el DNP liberará (versión 2.0) posee actualizaciones que permite la compatibilidad y uso adecuado del sistema de información SISGESTION en Microsoft Edge y Google Chrome sin inconvenientes, pero es importante precisar que continua con el componente Infragistics que a futuro quedará obsoleto en un corto o mediano plazo

- La aplicación se encuentra desarrollada en .Net Framework 4.5 y la versión de SISGESTION que actualmente están liberando esta actualizada a versión .Net Framework 4.7. La última versión disponible de .Net Framework es 4.8.1. La recomendación para aplicaciones nuevas es la migración a .Net Core o .Net 6/8. o Lo anteriormente mencionado requiere un proceso de reescritura del código fuente de la aplicación. Esto en función de que la aplicación no se quede obsoleta al corto plazo por los versionamientos de componente .NET Framework. o Es importante precisar que la obsolescencia de este tipo de componentes se ven reflejadas en vulnerabilidades de seguridad sobre las aplicaciones por falta de soporte por parte de su fabricante, en este caso Microsoft, que recomienda el

desarrollo y la actualización de las aplicaciones a los versionamientos mencionados.
    - El estado actual de .NET Framework 4.7 por parte de Microsoft es el siguiente:
    - Solamente recibe actualizaciones o parches de seguridad hasta 2027 como máximo.
    - Tiene soporte limitado por parte de fabricante (Microsoft)
    - Se recomienda migrar a .NET 4.8 o .NET 6/8
- Es importante que las áreas funcionales/misionales de la entidad validen los flujos de cada proceso dentro del sistema de información y que estos se adecuen a su necesidad.
    - En caso de que exista alguna variante en el flujo, algún paso dentro del procedimiento, actividad adicional o que se deba eliminar implicaría intervenir el código de la aplicación. Es decir, la entidad debe contar con un equipo de desarrollo de software dedicado explícitamente a adecuar el sistema de información en términos de lógica de programación para que se alinee a las necesidades funcionales y misionales del Ministerio. o En caso de no recibir actualizaciones del software por parte del DNP, este equipo de desarrollo de software debe realizar el mantenimiento de la aplicación a nivel de la capa de aplicación (en caso de que surjan necesidades adicionales, modificación de módulos existentes, creación de nuevos flujos y demás).
    - Si la aplicación es intervenida en su lógica de programación por un equipo de Ministerio del Trabajo y en el futuro el DNP libera actualizaciones las cuales el Ministerio es aplicable, se deben realizar pruebas de compatibilidad entre las actualizaciones liberadas por el DNP y las adecuaciones realizadas por el equipo de Ministerio del Trabajo.
- El sistema de información del DNP cuenta con servicios de Firma electrónica con servicios de firma centralizada, el cual es un servicio que garantiza Integridad y autenticidad en los procesos de firma de documentos electrónicos.
    - Actualmente el Ministerio no cuenta con estos servicios adquiridos por lo cual, si se quiere implementar SISGESTION con todas las funcionalidades que DNP posee actualmente y libera en su versión 2.0. Se deben adquirir los servicios de firma electrónica, firma centralizada y certificados digitales para los actores dentro de la entidad que actuarían como firmantes dentro del sistema de información.
    - En caso de no acogerse a la modalidad de firma digital, se debería modificar el flujo para cambiar el paso de firma por un paso de aprobación o firma mecánica. Esto también implicaría modificar el software para que se adecue a la decisión que tome la entidad.
- Ejecución de Scripts para creación de roles Estándar de acuerdo con lo remitido por parte del equipo de DNP.
- Se realizó conexión exitosa con el LDAP de la entidad, por lo cual los usuarios creados en SISGESTIÓN pueden iniciar sesión con su usuario y contraseña de dominio tras la creación del usuario en SISGESTION con el mismo domain name.

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

- Aspectos técnicos: ya fueron gestionados todos los ítems que pueden depender del Grupo de Soporte Informático y el equipo de servicios centrales de la UT.

- Ya se configuró todo el entorno de servidores y base de datos para pruebas.
- Se actualizó la imagen institucional del sistema. o Se ejecutaron los scripts de creación de roles. o Se realizó configuración con Active Directory.
- Se suministraron usuarios administradores para creación de usuarios.

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

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

Migración Portal Web

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

- Se realizó la migración de forma exitosa a versión 7.2 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.
- Se esta apoyando el desarrollo de un nuevo Organigrama para publicación en el portal. En validación de plantillas.

GESTOR DOCUMENTAL

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

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

Plataforma – Aplicaciones

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

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

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

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

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

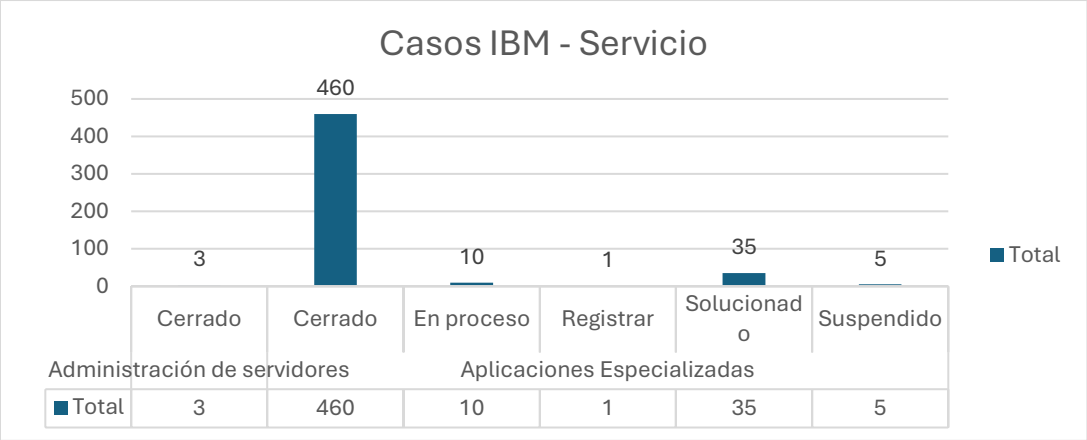


Ilustración 54 Casos *IBM Servicio*

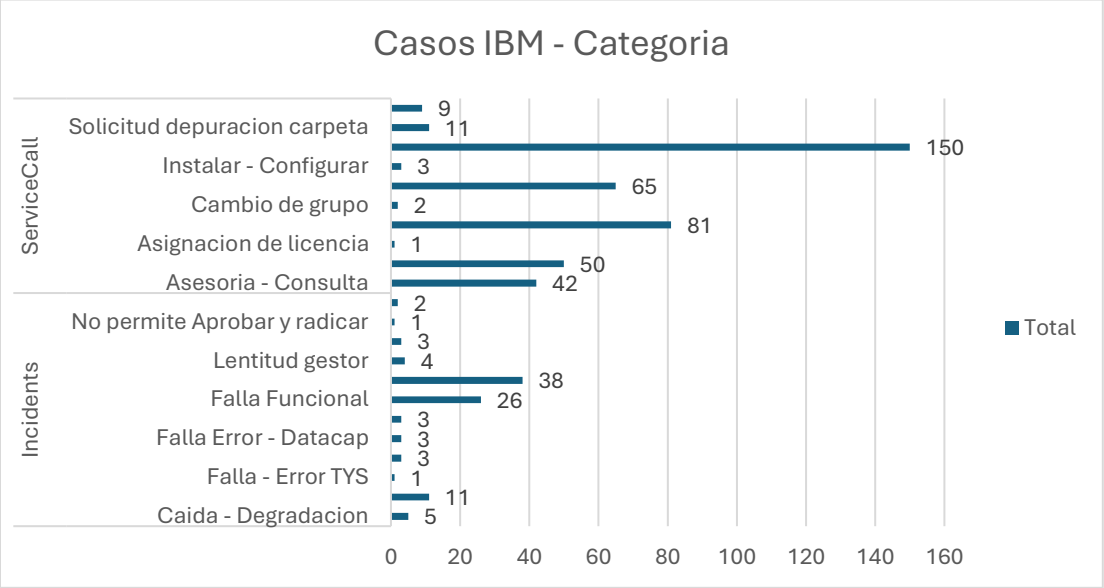


Ilustración 55 Casos IBM - categoría

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

- Relanzamiento de tareas (150 casos) Asociado a diferentes razones dentro de la operación, como redistribución de tareas, errores funcionales, depuración de instancias entre otros.
- Radicar una solicitud - Asignar Radicado TYS (81 casos) Las causas principales están asociadas a la reasignación y asignación de actividades que fueron cerradas por tiempo, así como a solicitudes inactivas debido a mantenimiento del sistema 2024.
- Radicar una solicitud - Depuración de Bandeja (65 casos) Eliminación de casos activos una vez el proceso de documentos ha sido transferido al módulo de Instrumentos Archivísticos, conforme al ciclo de vida documental.
- Radicar una solicitud - Asignación/Modificación de Roles (50 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 - Asesoría/Consulta (42 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.

Se observa una disminución de radicación de casos de manera significativa con respecto al mes anterior, en donde se reportaban flujos de casos de más de 400 casos por categoría, durante septiembre se observa una reducción de más de 300 requerimientos para categorías como asignación de radicados.

Se adjunta la infraestructura actual que soporta la solución de Gestión Documental de la entidad, así como su distribución de licenciamiento.

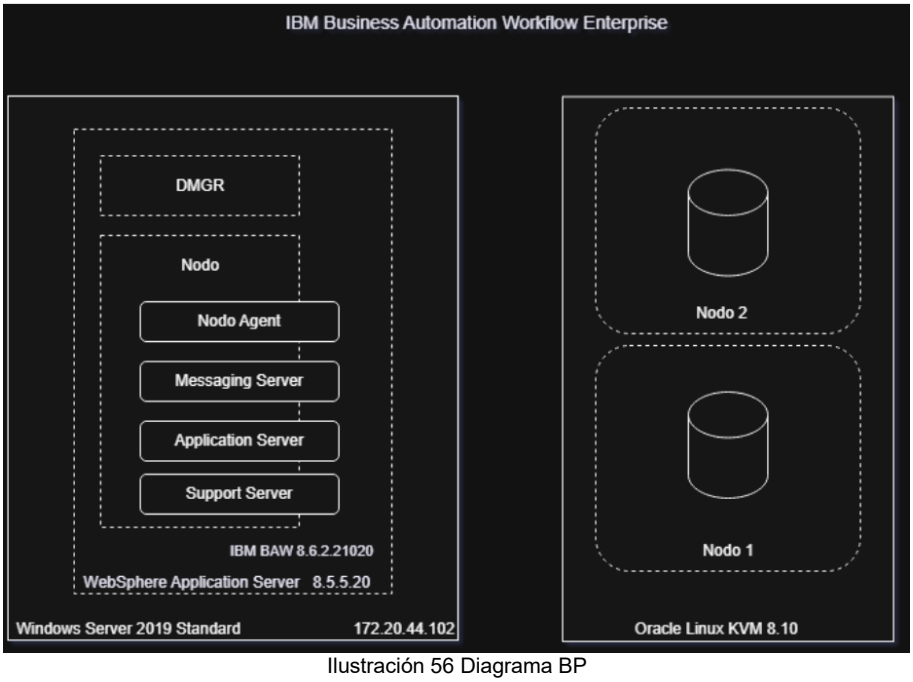


Ilustración 56 Diagrama BP

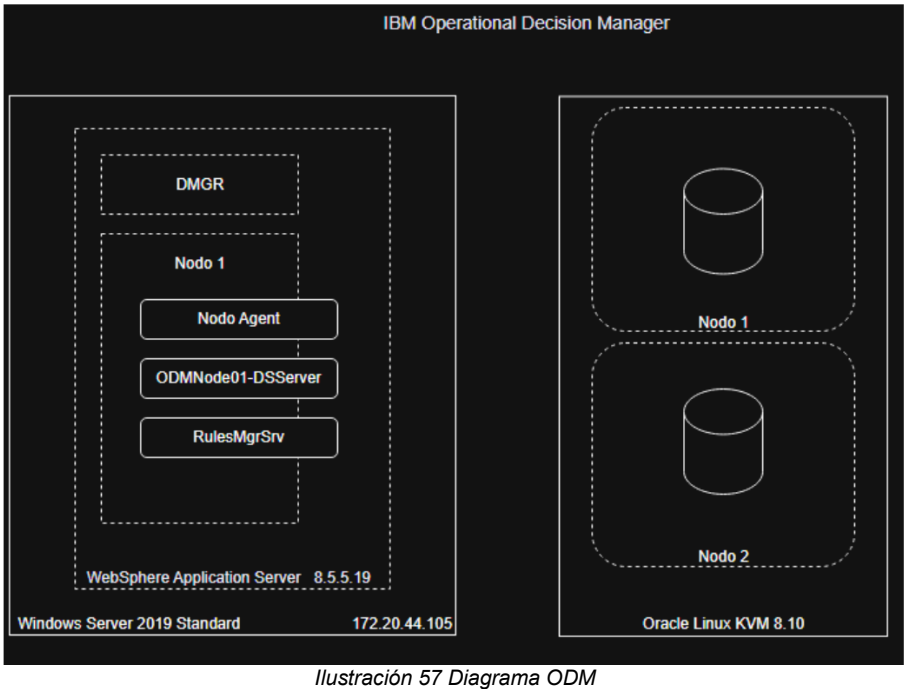


Ilustración 57 Diagrama ODM

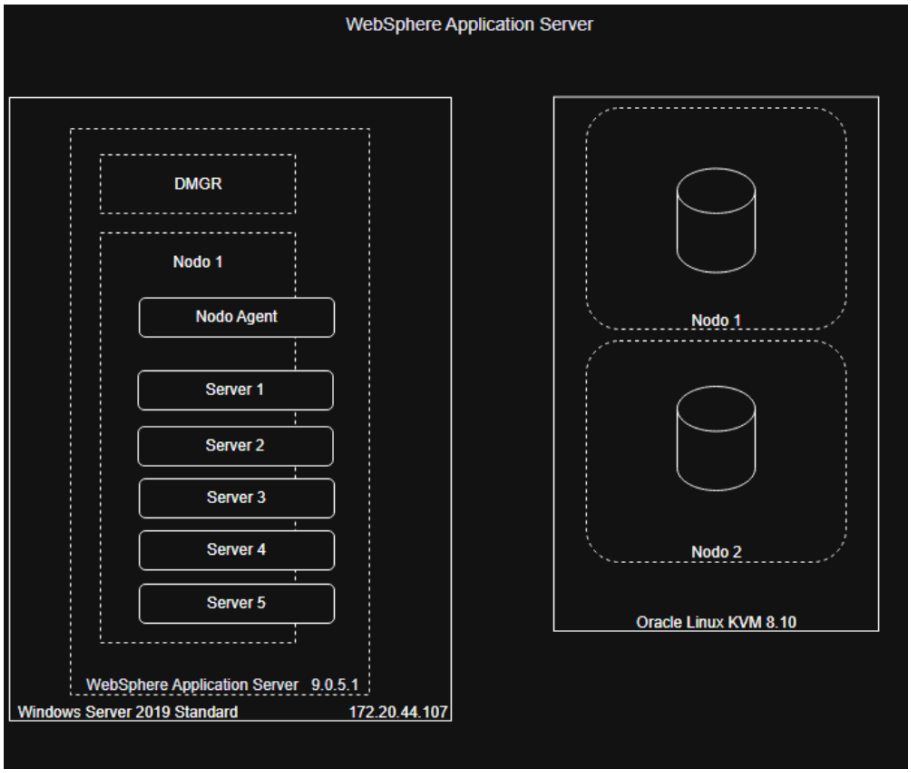


Ilustración 58 Diagrama WASND

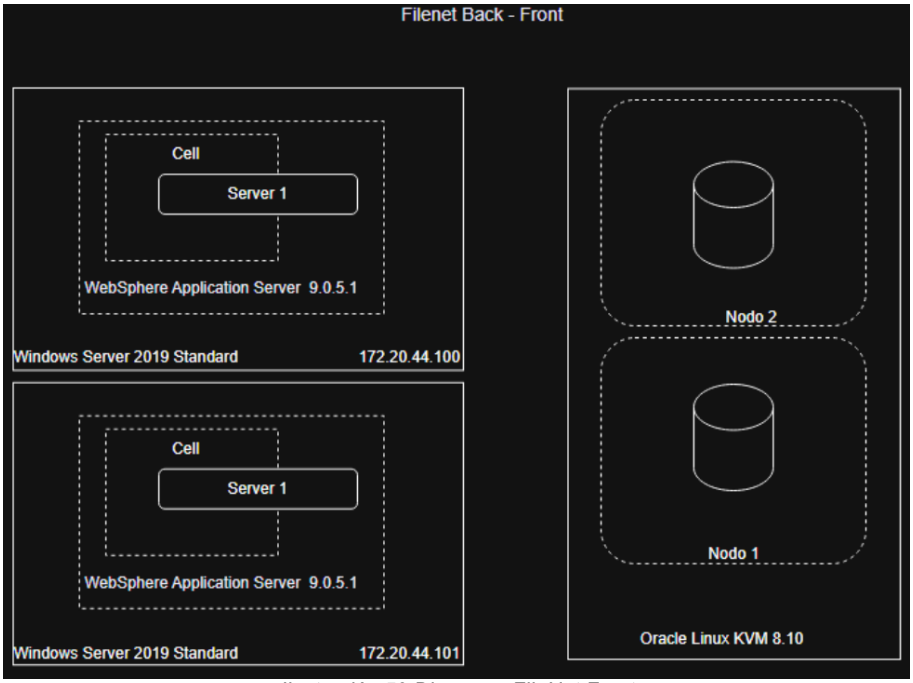


Ilustración 59 Diagrama FileNet Front

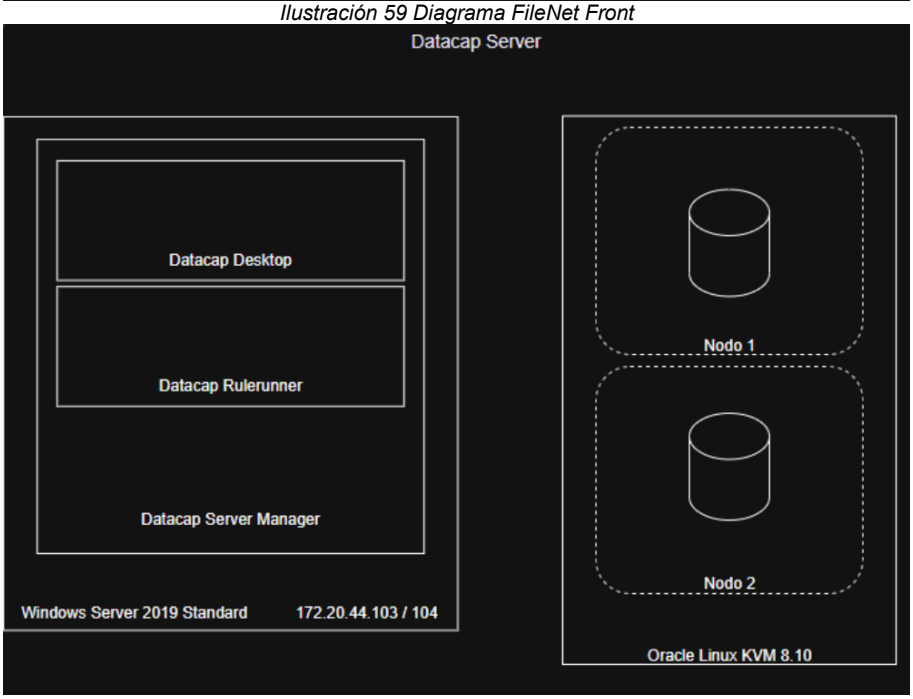


Ilustración 60 Diagrama Datacap

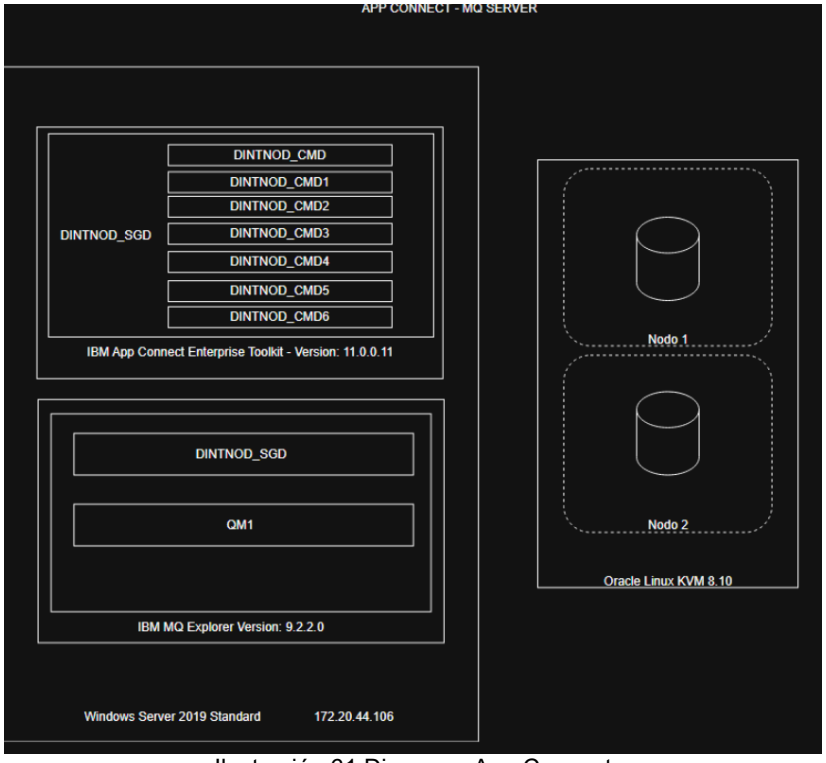


Ilustración 61 Diagrama App Connect

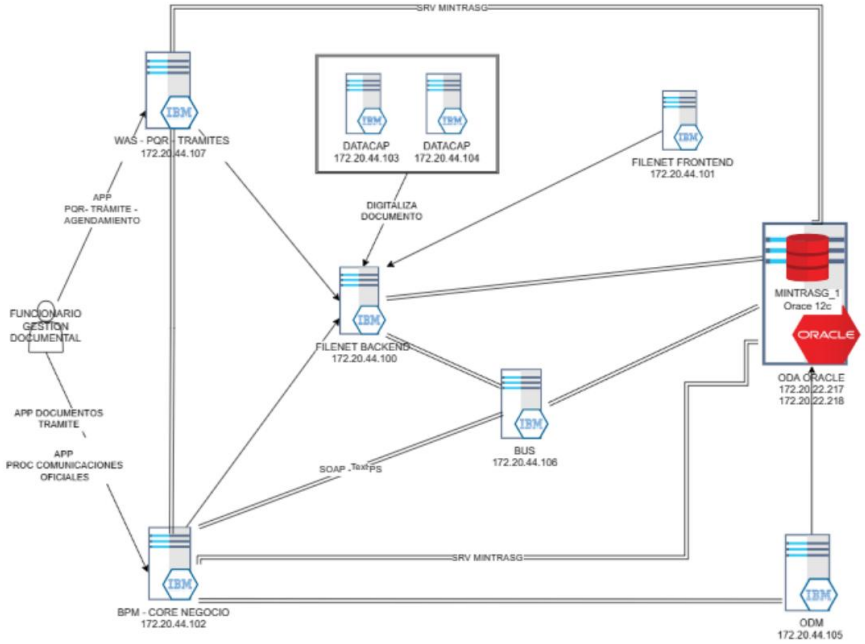


Ilustración 62 Arquitectura Gestor Documental

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 63 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 64 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 65 IBM Licenciamiento

Mes	Suma de Total Instancias
Enero 2025	111854
Febrero 2025	149070
Marzo 2025	148829
Abril 2025	135756
Mayo 2025	154121
Junio 2025	137472
Julio 2025	78502
Agosto 2025	92786
Septiembre 2025	164424
Total acumulado	**1.172.814**

Tabla 53 Suma Instancias

Mes	Suma de Total Documentos
Enero 2025	149454
Febrero 2025	183729
Marzo 2025	193697
Abril 2025	180888
Mayo 2025	204354
Junio 2025	178790
Julio 2025	201882
Agosto 2025	190074
Septiembre 2025	208044
Total acumulado	**1.688.412**

Tabla 54 Total Docs

Mes	Suma de Total radicados
Enero 2025	59197
Febrero 2025	70194
Marzo 2025	72317
Abril 2025	64370
Mayo 2025	73694
Junio 2025	63934
Julio 2025	79429
Agosto 2025	66811
Septiembre 2025	73473
Total, acumulado	**623.419**

Tabla 55 Total Radicados

De acuerdo con el funcionamiento actual del sistema de gestión documental, se exponen las capacidades actuales contrastadas con las capacidades requeridas a nivel de Cores asignados a las máquinas virtuales aprovisionadas para la puesta en marcha del Gestor documental. Es importante mencionar que estas capacidades solamente enmarcan ampliación para funcionamiento del escenario actual, es decir una optimización del sistema actual sin incluir nuevos desarrollos o funcionalidades ya que estas deben ser dimensionadas y expuestas de manera específica para plasmar el crecimiento de las capacidades de los contenedores del componente IBM.

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

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

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

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

Tabla 56 Dimensionamiento Servers IBM - Virtualización Optima

- Estado de las Bases de Datos

A nivel del servicio que soporta las bases de datos de la entidad, los especialistas MSSQL y Oracle han realizado diferentes actividades para dar diagnóstico y estado actual de las aplicaciones a nivel transaccional, de capacidad y de almacenamiento, identificando diferentes acciones de mejora para el gestor documental, que posee una criticidad elevada para la misionalidad y la funcionalidad del ministerio.

Se han presentado diferentes controles de cambios para las bases de datos alojadas y soportadas por MSSQL, cambios relacionados con ventanas de mantenimiento, estabilización, Backup, migraciones de versión y de base de datos, reinicios asociados a ventanas de mantenimiento, ejecución de scripts entre otras actividades descritas dentro de cada RFC. Según las acciones de mejora identificadas en cada ventana de mantenimiento, se han construido documentos, topologías e informes asociados a las indisponibilidades (asociadas a ventanas de mantenimiento, procesos de estabilización de proceso de bases de datos y afinamiento de servicio) de los servicios soportados desde bases de datos. Se realizó el cargue de los archivos planos recibidos vía FTP desde el Ministerio de Salud dicha tarea se realizó sobre las tablas que ya están definidas para ser cargadas en la Base de Datos de PILA.

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

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

- Estado de las Bases de Datos – Oracle Gestor Documental

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

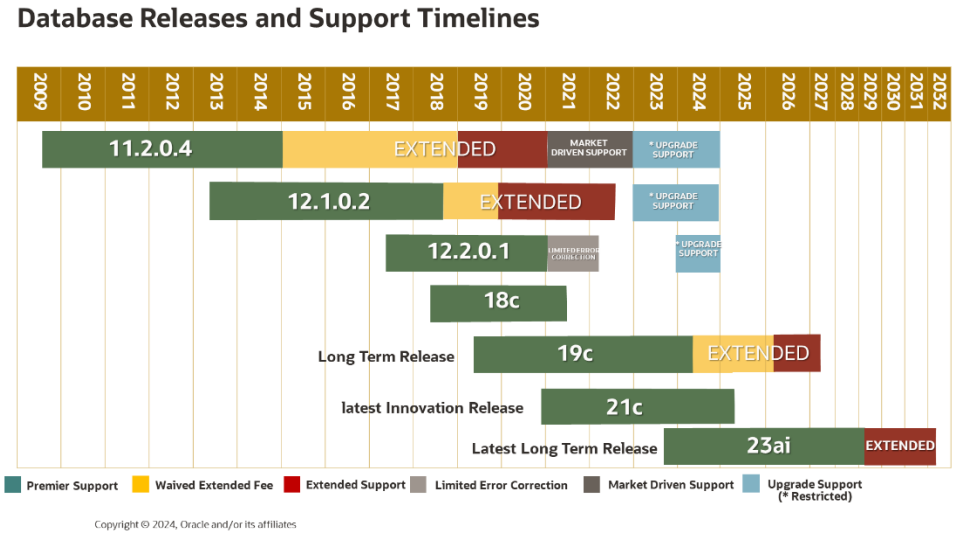


Ilustración 66 Estado Bases de Datos

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 57 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 58 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 59 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 67 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 68 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 69 Estadísticas Memoria

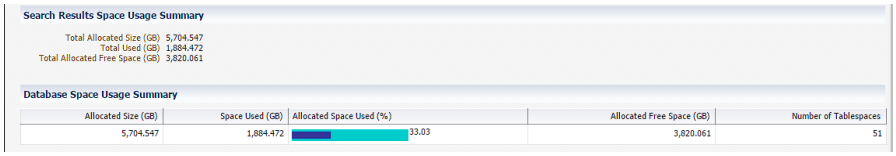
Estadísticas del shared pool: La siguiente estadística muestra el tamaño utilizado para el almacenamiento de las estructuras compartidas por la sesiones de la base de datos (sentencias sql, objetos de diccionario y estructuras de ejecución) como tal se puede dar un diagnóstico para poder evaluar el aumento 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 70 Estadísticas Pool compartido

Tamaño base de datos MINSTRASG:



Search Results Space Usage Summary

Total Allocated Size (GB) 5,704.547
Total Used (GB) 1,884.472
Total Allocated Free Space (GB) 3,820.061

Database Space Usage Summary

Allocated Size (GB)	Space Used (GB)	Allocated Space Used (%)	Allocated Free Space (GB)	Number of Tablespaces
5,704.547	1,884.472	33.03	3,820.061	51

Ilustración 71 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 72 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

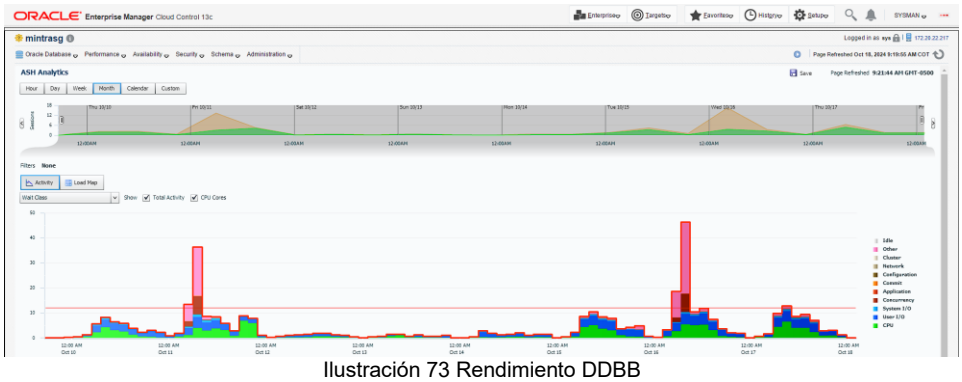


Ilustración 73 Rendimiento DDBB

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 74 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 75 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 76 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 77 Estadística Shared Pool

Tamaño base de datos DBMINTRA:

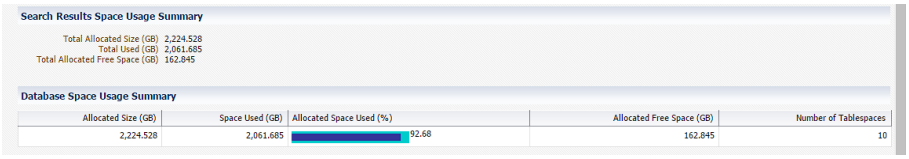


Ilustración 78 Tamaño DDBB DBMINTRA

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 79 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

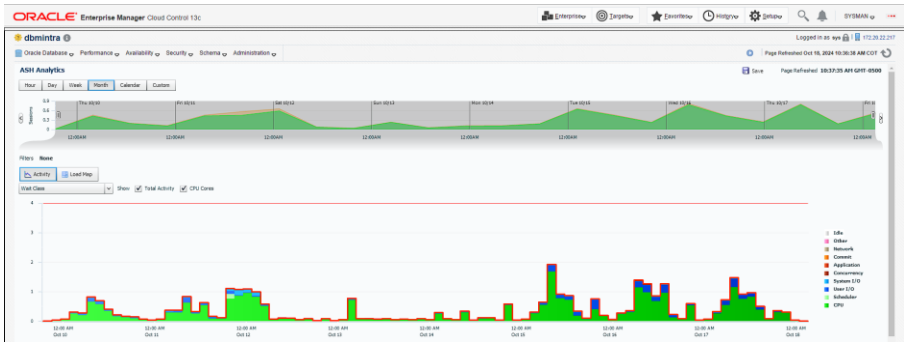


Ilustración 80 Rendimiento DDBB MINTRASG

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 81 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 82 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 83 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 84 Estadísticas Shared Pool

Tamaño base de datos PLIFERAY:

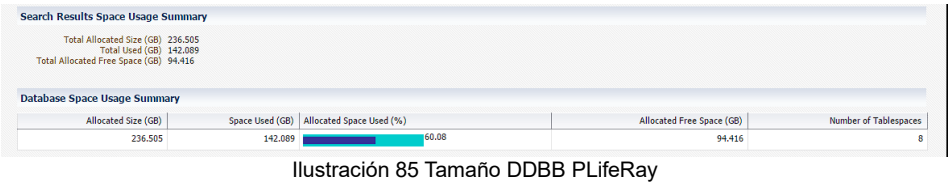


Ilustración 85 Tamaño DDBB PLifeRay

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 86 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

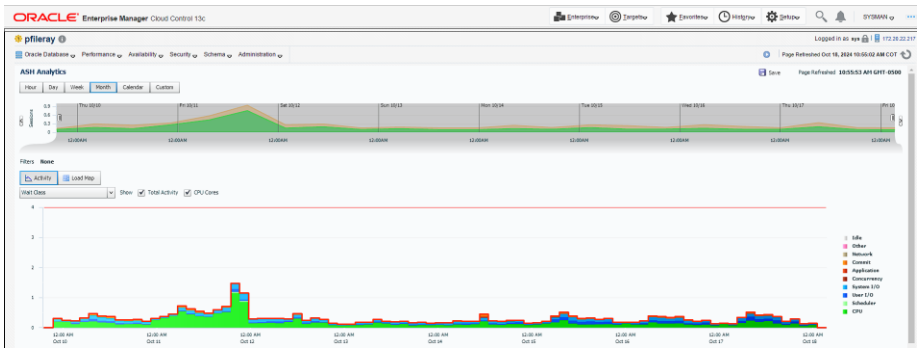


Ilustración 87 Rendimiento DDBB PlifeRay

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 88 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 89 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 90 Estadística Memoria

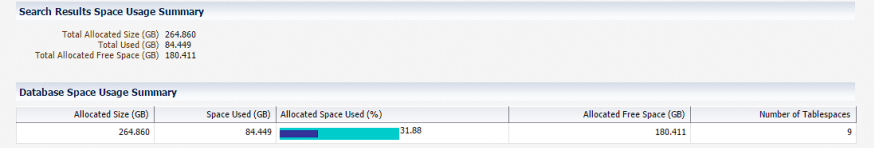
Shared pool, para el caso de la BD SIGEP (Nomina) se observa que los usos de la SGA son idénticos entre los snapshots del reporte.

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 91 Estadística Shared Pool

Tamaño base de datos SIGEP:



Search Results Space Usage Summary

Total Allocated Size (GB) 264.860
Total Used (GB) 84.449
Total Allocated Free Space (GB) 180.411

Database Space Usage Summary

Allocated Size (GB)	Space Used (GB)	Allocated Space Used (%)	Allocated Free Space (GB)	Number of Tablespaces
264.860	84.449	31.88	180.411	9

Ilustración 92 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 93 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

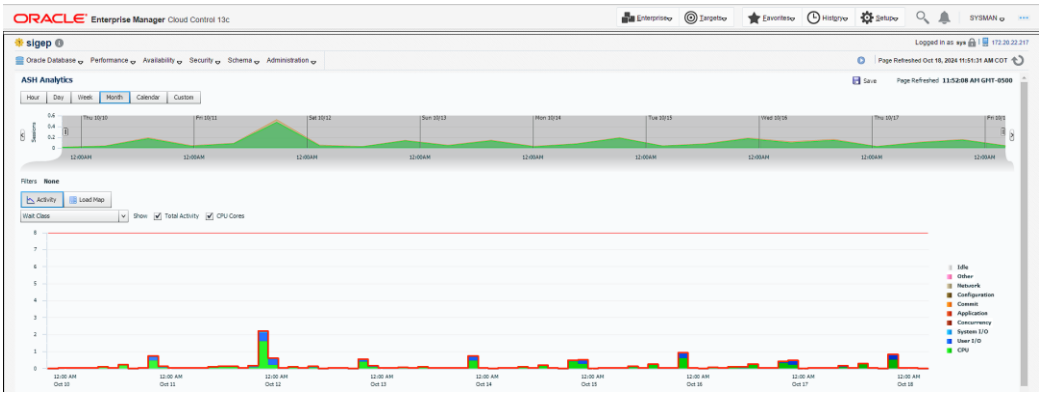


Ilustración 94 Rendimiento DDBB SIGEP

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 95 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 96 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 97 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 98 Estadística Shared Pool

Tamaño base de datos DBSIMPC:

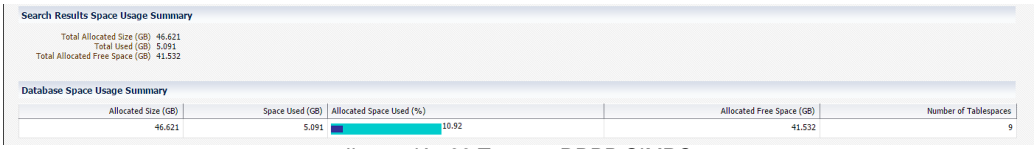


Ilustración 99 Tamaño DDBB SIMPC

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 100 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

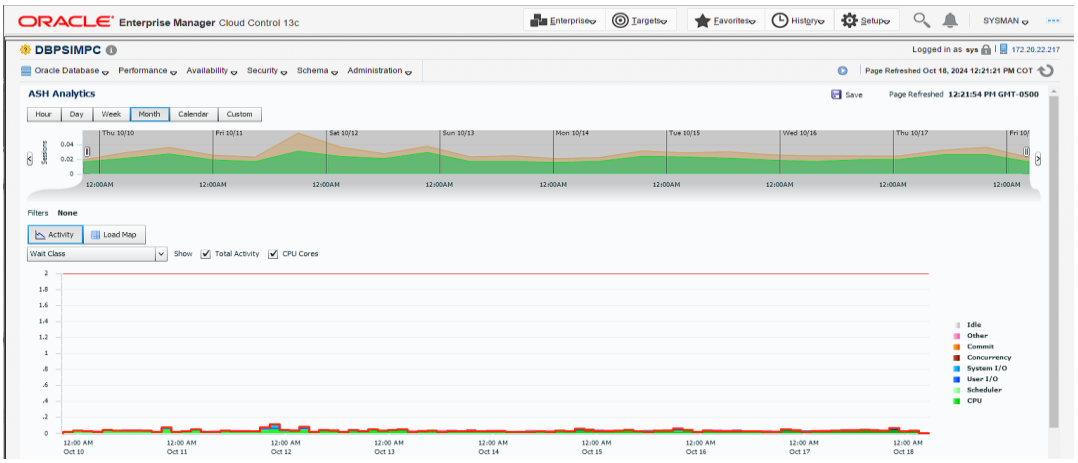


Ilustración 101 Rendimiento DDBB

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 102 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 103 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 104 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 105 Estadística Shared Pool

Tamaño base de datos MINTRASD:

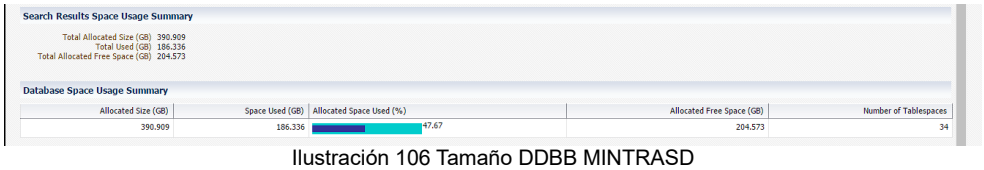


Ilustración 106 Tamaño DDBB MINTRASD

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 107 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

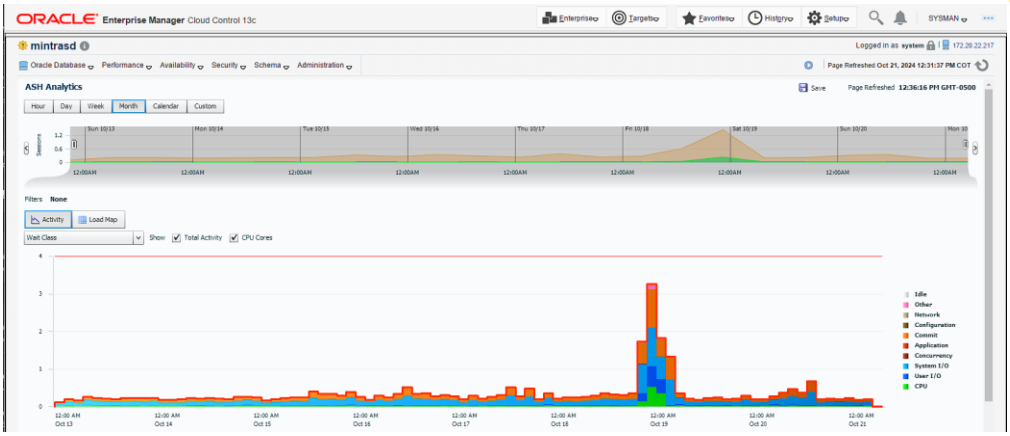


Ilustración 108 Rendimiento MINTRASD

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 109 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 110 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 111 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 112 Estadística Shared Pool

Tamaño base de datos MINTRASD:

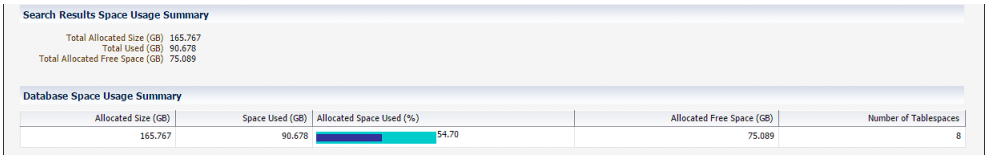


Ilustración 113 Tamaño DDBB

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 114 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

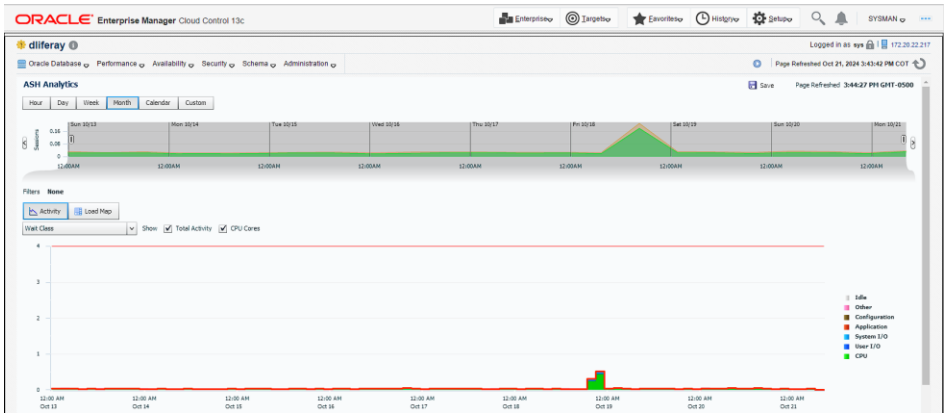


Ilustración 115 Rendimiento DDBB

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

1. BASES DE DATOS VERSION 11G SERVDIOR 172.20.22.107

3.1 Base de datos DBMINTRA

Información base de datos – Servidor:

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

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

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

Ilustración 116 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 117 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 118 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 119 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 120 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 121 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 122 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 123 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 124 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 125 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 126 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 127 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

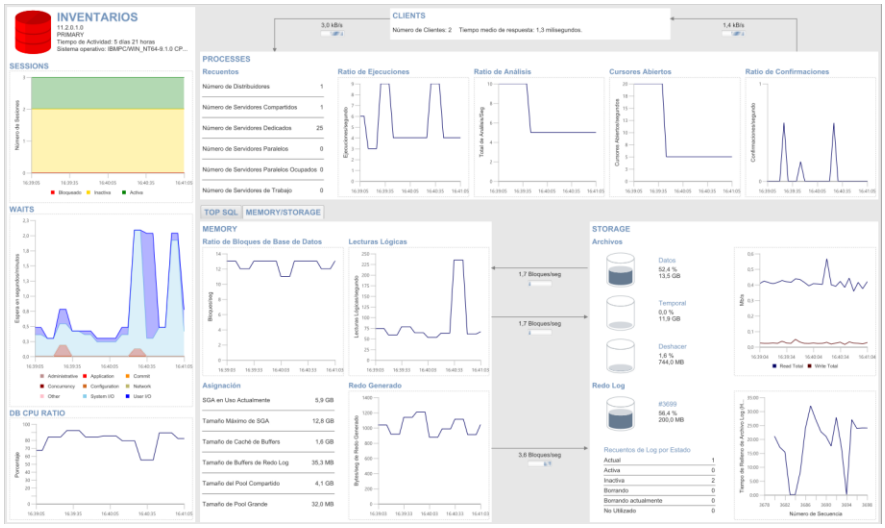


Ilustración 128 Comportamiento DDBB

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 129 Almacenamiento ASM

DISKGROUP DATA:

Disk Groups | Clients | Space History | IO History

Lower Pane: Show Related Items

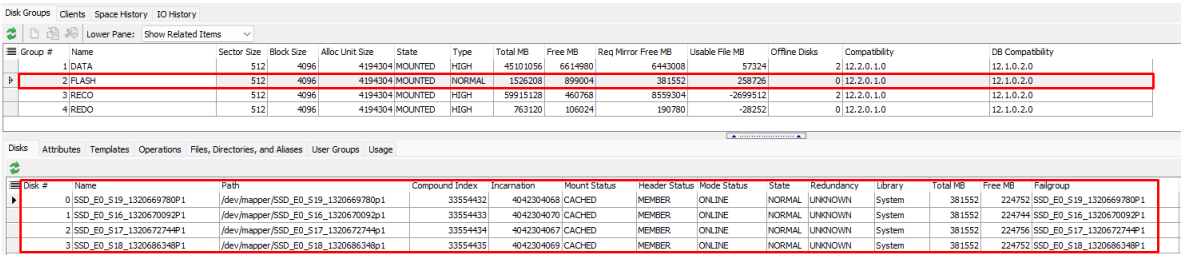
Group #	Name	Sector Size	Block Size	Alloc Unit Size	State	Type	Total MB	Free MB	Req Mirror Free MB	Usable File MB	Offline Disks	Compatibility	DB Compatibility
1	DATA	512	4096	4194304	MOUNTED	HIGH	45101056	6614980	6443008	57324	2	12.2.0.1.0	12.1.0.2.0
2	FLASH	512	4096	4194304	MOUNTED	NORMAL	1526208	899004	381552	258726	0	12.2.0.1.0	12.1.0.2.0
3	RECO	512	4096	4194304	MOUNTED	HIGH	59915128	460768	8559304	-2699512	2	12.2.0.1.0	12.1.0.2.0
4	REDO	512	4096	4194304	MOUNTED	HIGH	763120	106024	190780	-28252	0	12.2.0.1.0	12.1.0.2.0

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

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

Ilustración 130 DiskGroup Data

DISKGROUP FLASH:

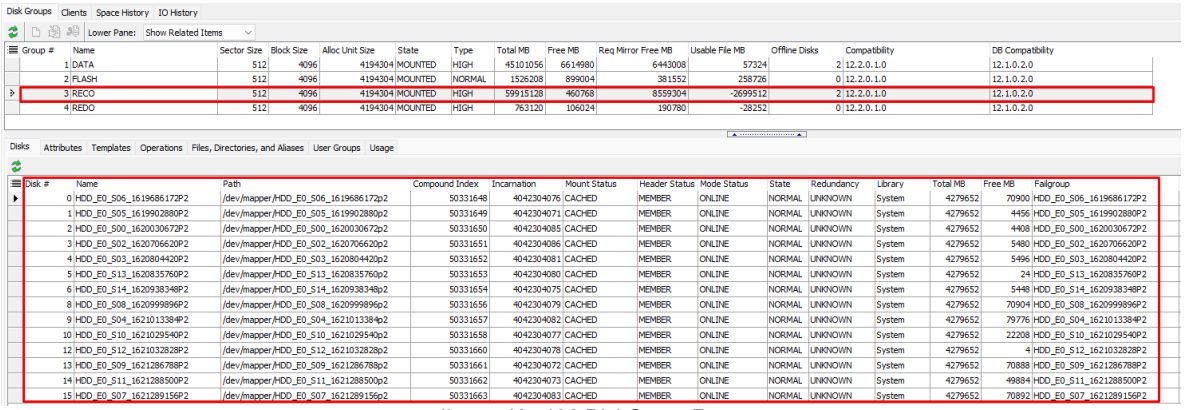


Group #	Name	Sector Size	Block Size	Alloc Unit Size	State	Type	Total MB	Free MB	Req Mirror Free MB	Usable File MB	Offline Disks	Compatibility	DB Compatibility
1	DATA	512	4096	4194304	MOUNTED	HIGH	45101056	6614980	6443008	57324	2	12.2.0.1.0	12.1.0.2.0
2	FLASH	512	4096	4194304	MOUNTED	NORMAL	1526208	899004	381552	258726	0	12.2.0.1.0	12.1.0.2.0
3	RECO	512	4096	4194304	MOUNTED	HIGH	59915128	460768	8559304	-2699512	2	12.2.0.1.0	12.1.0.2.0
4	REDO	512	4096	4194304	MOUNTED	HIGH	763120	106024	190780	-28252	0	12.2.0.1.0	12.1.0.2.0

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

Ilustración 131 DiskGroup Flash

DISKGROUP RECO:

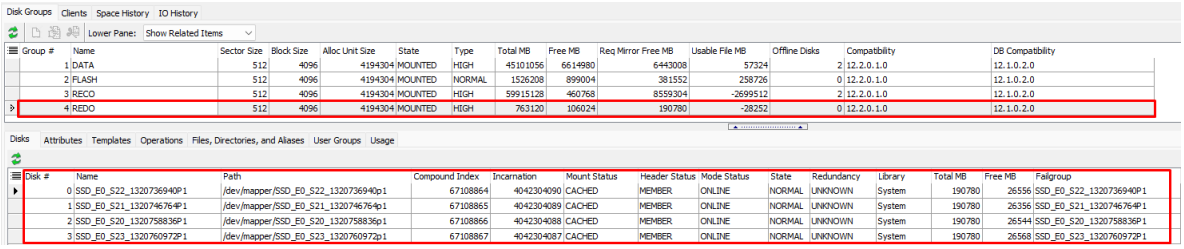


Group #	Name	Sector Size	Block Size	Alloc Unit Size	State	Type	Total MB	Free MB	Req Mirror Free MB	Usable File MB	Offline Disks	Compatibility	DB Compatibility
1	DATA	512	4096	4194304	MOUNTED	HIGH	45101056	6614980	6443008	57324	2	12.2.0.1.0	12.1.0.2.0
2	FLASH	512	4096	4194304	MOUNTED	NORMAL	1526208	899004	381552	258726	0	12.2.0.1.0	12.1.0.2.0
3	RECO	512	4096	4194304	MOUNTED	HIGH	59915128	460768	8559304	-2699512	2	12.2.0.1.0	12.1.0.2.0
4	REDO	512	4096	4194304	MOUNTED	HIGH	763120	106024	190780	-28252	0	12.2.0.1.0	12.1.0.2.0

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

Ilustración 132 DiskGroup Reco

DISKGROUP REDO:



Group #	Name	Sector Size	Block Size	Alloc Unit Size	State	Type	Total MB	Free MB	Req Mirror Free MB	Usable File MB	Offline Disks	Compatibility	DB Compatibility
1	DATA	512	4096	4194304	MOUNTED	HIGH	45101056	6614980	6443008	57324	2	12.2.0.1.0	12.1.0.2.0
2	FLASH	512	4096	4194304	MOUNTED	NORMAL	1526208	899004	381552	258726	0	12.2.0.1.0	12.1.0.2.0
3	RECO	512	4096	4194304	MOUNTED	HIGH	59915128	460768	8559304	-2699512	2	12.2.0.1.0	12.1.0.2.0
4	REDO	512	4096	4194304	MOUNTED	HIGH	763120	106024	190780	-28252	0	12.2.0.1.0	12.1.0.2.0

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

Ilustración 133 DiskGroup Redo

De acuerdo con lo definido contractualmente la distribución de licenciamiento sobre la capa de aplicación es la siguiente:

- Servidor WANSD: 7 cores asignados actualmente a transición a 8 cores.
- Servidor BAW: 5 Cores asignados actualmente a transición a 6 cores.
- Servidor BUS Conectó: 3 Cores asignados actualmente à transición a 4 Cores.

Esto se traduce en licenciamiento de componente IBM de la siguiente forma:

P/N	DESCRIPCION	QTY
D03S0LL	IBM App Connect Standard Processor Value Unit (PVU) License + SW Subscription & Support 12 Months	70
D20RULL	IBM Cloud Pak for Business Automation Virtual Processor Core License + SW Subscription & Support 12 Months	10
D55WJLL	IBM WebSphere Application Server Network Deployment Processor Value Unit (PVU) License + SW Subscription & Support 12 Months	70

Ilustración 134 Licenciamiento adicional componente IBM

3.1.4 No aplica

3.1.5 Seguridad Informática

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

3.1.5.1 Firewalls de nueva generación

Durante septiembre 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.

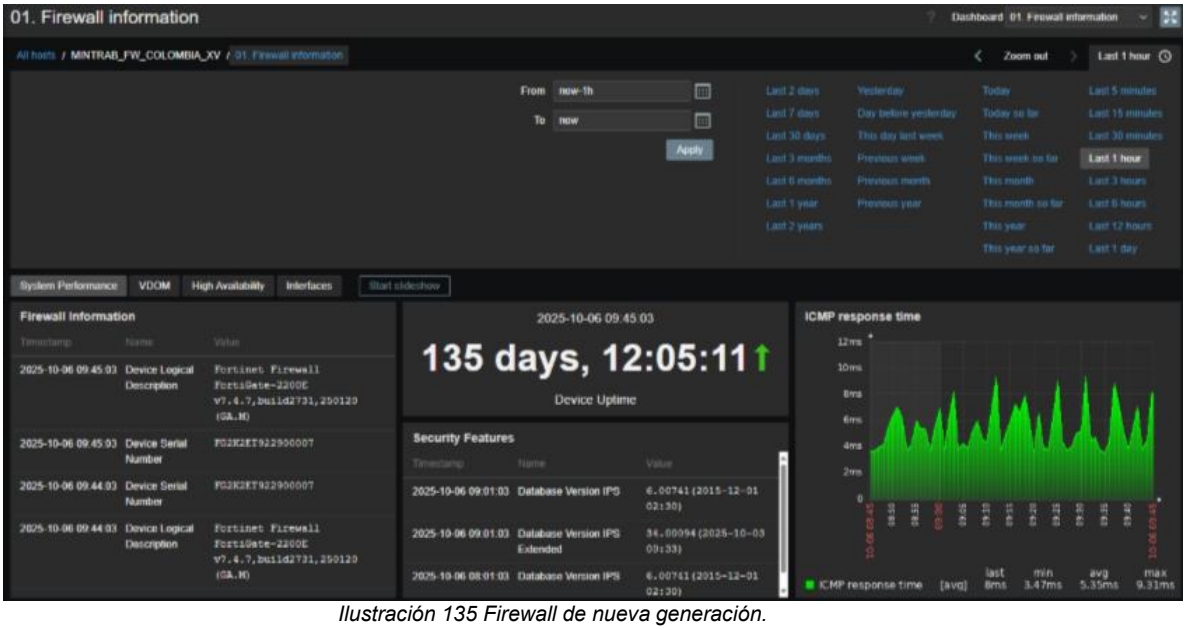


Ilustración 135 Firewall de nueva generación.

El Informe de aplicaciones y ancho de banda de Fortinet proporciona una visión detallada para identificar las aplicaciones y usuarios en la red que están utilizando la mayor cantidad de ancho de banda y presentando los mayores riesgos. Este informe, resume los hallazgos y ofrece una evaluación global del riesgo, junto con acciones recomendadas para abordarlos de manera efectiva.

Ancho de Banda
Se presenta un resumen del uso de ancho de banda y el número de sesiones durante el período del mes de septiembre. Este análisis del resumen de ancho de banda proporciona

una visión clara de los patrones de uso durante el periodo, permitiendo una mejor gestión y planificación de los recursos de red.

Elemento	Observación
Tendencia general	Se mantiene un patrón de tráfico estable, con oscilaciones regulares cada 2-3 días. No se evidencian picos anómalos que indiquen transferencia masiva o fuga de información.
Volumen promedio	Entre 6 TB y 10 TB diarios combinados (envío + recepción). El tráfico recibido predomina (color azul), lo que refleja un uso intensivo de servicios en la nube y descargas institucionales.
Tráfico enviado (amarillo)	Permanece estable, con valores medios de 1 TB-2 TB diarios, lo que sugiere una carga normal de sincronización y respaldo hacia repositorios o portales externos.
Días de mayor actividad	5 de septiembre, 12 de septiembre y 24 de septiembre: incremento puntual de tráfico recibido cercano a 9 TB. Se asocia a operaciones de actualización o transferencia de datos de sistemas gubernamentales (M365, SIIF, SECoP).
Días de menor tráfico	9-10 de septiembre y 27-29 de septiembre: reducción temporal del volumen; puede coincidir con fines de semana o mantenimiento programado.
Comportamiento esperado	La curva refleja un entorno controlado y con balance normal entre subida y bajada, sin evidencias de congestión, saturación ni exfiltración.

Tabla 60 Tendencia de uso de ancho de banda

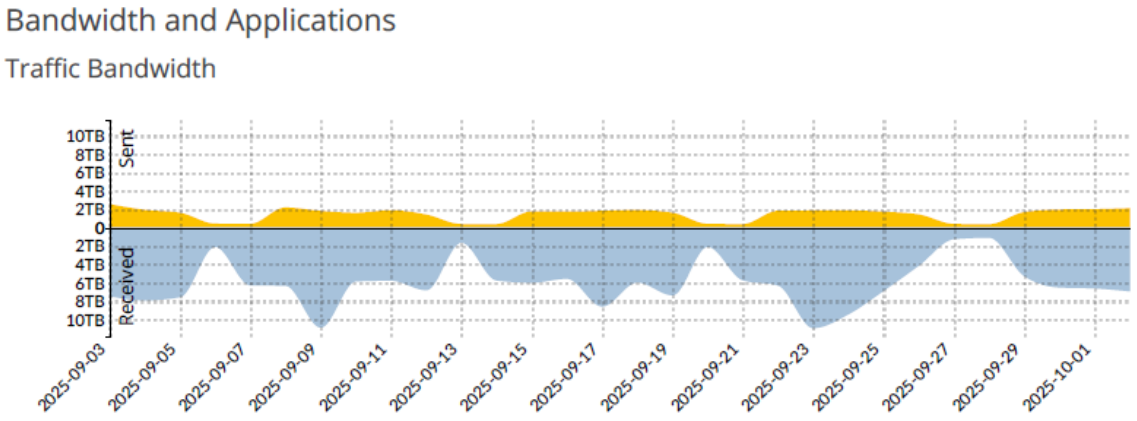


Ilustración 136 Comportamiento ancho de banda

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 septiembre . La identificación de los 10 principales usuarios de ancho de banda

proporciona información valiosa sobre los patrones de uso de la red y los puntos críticos de congestión.
A continuación, se detallan los hallazgos más relevantes:

N°	Usuario/IP	Total, de datos (aprox.)	Observaciones
1	172.20.22.251	**50.33 TB**	Tráfico extremadamente alto, servidor de almacenamiento, backup (MINTRABCKEXEC.mintrabajo.loc).
2	mduarteo	**6.58 TB**	Usuario con alto consumo. Requiere validar si se relaciona con actividades administrativas o técnicas (por ejemplo, transferencia de informes o copias de respaldo).
3	172.28.28.38	**6.19 TB**	IP interna — podría corresponder a servidor de aplicaciones o gestión. Revisar patrón de uso.
4	172.20.44.102	**5.03 TB**	Posible servidor de Gestos Documental
5–10	Resto de IPs internas	Entre **1–2 TB** cada una	Tráfico normal para estaciones o servidores secundarios. “ADMINBCK” (10.º) destaca como usuario de **respaldo**, con ~1 TB.

Tabla 61 usuarios con mayor consumo de ancho de banda

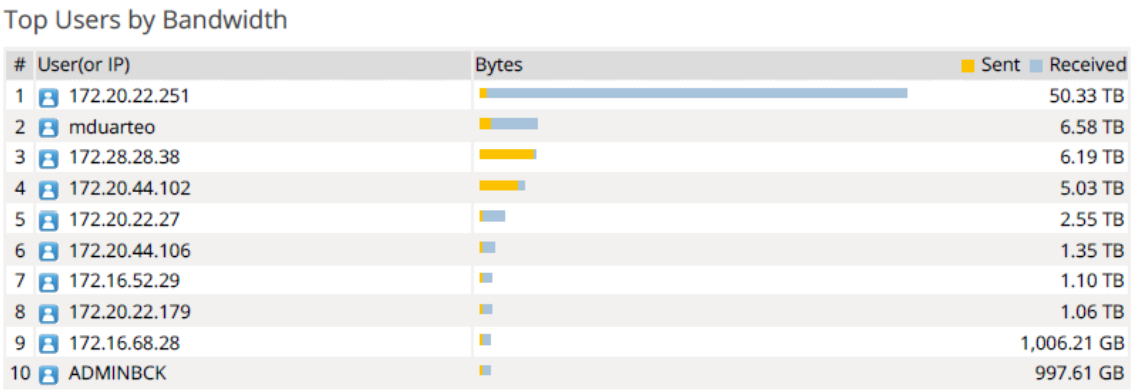


Ilustración 137 Tendencia de uso de ancho de banda

Top de usuarios por número de sesiones

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

Top Users by Sessions

#	User (or IP)	Sessions
1	172.25.0.5	199,861,954
2	mduarteo	90,695,223
3	172.20.22.234	30,186,147
4	FORTINET	26,946,671
5	172.20.22.3	18,630,562
6	172.20.22.40	16,556,039
7	172.20.22.32	16,270,588
8	172.16.11.126	15,302,461
9	172.16.62.37	12,563,783
10	172.20.22.228	12,387,947

Ilustración 138 Top de usuarios por números de sesiones

Análisis Top Users by Sessions

N°	Usuario/IP	Sesiones	Observaciones
1	**172.25.0.5**	**199,861,954**	IP con la mayor cantidad de conexiones. Muy probablemente corresponde a un **servidor interno o sistema de autenticación/proxy**, encargado de canalizar solicitudes de múltiples usuarios.
2	**mduarteo**	**90,695,223**	Usuario con actividad muy elevada. Puede estar vinculado a gestion de alguna plataforma(Mireya Duarte Osma)
3	**172.20.22.234**	**30,186,147**	Servidor interno asociado a un controlador de dominio.
4	**FORTINET**	**26,946,671**	Tráfico legítimo del sistema de seguridad (firewall, antivirus o gestión de eventos).
5	**Resto de IPs internas (rango 172.16–172.22)**	Entre **12 y 18 millones de sesiones**	Volumen esperado para servicios de autenticación, proxy, o endpoints activos de red.

Tabla 62 Top de usuarios por sesiones

Top Applications by Bandwidth

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

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	TCP/902			49.68 TB
2	HTTPS			41.23 TB
3	SMB			23.94 TB
4	TCP/445			12.18 TB
5	SYSLOG			8.37 TB
6	Microsoft.365.Portal			8.24 TB
7	TCP/1521			8.15 TB
8	HTTP			8.07 TB
9	Microsoft.Portal			5.79 TB
10	Microsoft.SharePoint			5.29 TB

Ilustración 139 Top de aplicaciones

N°	Aplicación	Descripción
1. TCP/902	49.68 TB	Puerto comúnmente usado para VMware ESXi (administración de máquinas virtuales). Indica alto volumen de sincronización o replicación de entornos virtualizados.
2. HTTPS	41.23 TB	Tráfico web cifrado — servicios cloud, correo, portales institucionales. Representa la base del tráfico corporativo seguro.
3. SMB (Server Message Block)	23.94 TB	Protocolo de compartición de archivos en red. Muestra alto uso de repositorios compartidos internos.
4. TCP/445	12.18 TB	Asociado también a SMB y autenticación Windows (Active Directory). Indica intenso intercambio de archivos y autenticaciones.
5. SYSLOG	8.37 TB	Transmisión de logs desde dispositivos hacia el FortiAnalyzer o SIEM. Tráfico esperado y saludable para monitoreo de seguridad.
6. Microsoft 365 Portal	8.24 TB	Acceso y sincronización de servicios en la nube (OneDrive, Outlook, Teams).
7. TCP/1521	8.15 TB	Puerto usado por Oracle Database. Indica consultas o réplicas intensivas en bases de datos institucionales.
8. HTTP	8.07 TB	Tráfico no cifrado. Nivel bajo comparado con HTTPS, lo que refleja correcta adopción de canales seguros.
9. Microsoft.Portal	5.79 TB	Tráfico asociado a la autenticación y uso de portales de Microsoft 365.
10. Microsoft.SharePoint	5.29 TB	Uso activo de bibliotecas documentales internas y colaboración en línea.

Tabla 63 Top de aplicaciones

Top 15 Authenticated Logins by VPN Connections

La imagen corresponde al apartado “Authenticated Logins” del informe perimetral de septiembre 2025 del Ministerio de Trabajo (MinTrabajo), y presenta el comportamiento de los usuarios que se conectaron por VPN (SSL-Tunnel) durante el periodo analizado.

Authenticated Logins

#	User	Type	First Used	Total Number of Connections	Total Duration Connected(HH:MM:SS)
1	jmaestre	ssl-tunnel	2025-09-03 08:08:44	122	168:11:47
2	mcarrascal	ssl-tunnel	2025-09-03 08:33:56	116	184:45:33
3	cjimenez	ssl-tunnel	2025-09-03 09:52:28	110	113:30:10
4	agente4	ssl-tunnel	2025-09-03 04:08:55	107	191:26:00
5	contaccenter	ssl-tunnel	2025-09-03 07:02:32	102	236:43:03
6	yjordan	ssl-tunnel	2025-09-03 00:05:31	101	241:25:50
7	dfdiazd@noc_indra	ssl-tunnel	2025-09-03 00:03:12	94	613:02:01
8	ablanco	ssl-tunnel	2025-09-04 08:17:34	91	90:58:00
9	jcalderonf	ssl-tunnel	2025-09-03 09:00:49	89	117:06:24
10	cabuitragoo	ssl-tunnel	2025-09-03 00:06:51	74	276:34:05
11	rmurcia	ssl-tunnel	2025-09-03 04:58:17	72	75:33:55
12	jdduque	ssl-tunnel	2025-09-03 11:22:30	71	156:23:42
13	ctobos	ssl-tunnel	2025-09-03 08:15:30	66	40:06:32
14	smosquera	ssl-tunnel	2025-09-03 10:47:15	64	55:38:03
15	vsolano	ssl-tunnel	2025-09-03 07:47:19	62	95:06:52

Ilustración 140 Top de Autenticación

Indicador	Descripción
Tipo de conexión	Todas las sesiones son mediante SSL-Tunnel, lo que indica que los usuarios accedieron a la red institucional a través del portal VPN seguro de FortiGate.
Usuarios más activos	Los usuarios dfdiazd@noc_indra, contaccenter, yjordan, y cabuitragoo presentan las mayores duraciones acumuladas de conexión.
Mayor duración total	dfdiazd@noc_indra con 613 horas (25 días conectados), lo que indica conexión permanente de monitoreo o soporte remoto.
Mayor cantidad de conexiones	jmaestre (122), mcarrascal (116) y cjimenez (110). Suelen corresponder a usuarios operativos o administrativos con múltiples sesiones diarias.
Duraciones elevadas (>200 h)	contaccenter, yjordan, cabuitragoo; usuarios de atención y soporte que mantienen sesiones prolongadas.
Duraciones medias (100 h–190 h)	agente4, mcarrascal, jcalderonf, jduque. Patrón normal para personal técnico o administrativo remoto.
Duraciones bajas (<100 h)	ablanco, ctobos, smosquera, vsolano. Usuarios con conexión eventual o parcial.

Tabla 64 Consolidado de indicadores

Failed Login Attempts by User

Esta imagen corresponde al apartado “Failed Login Attempts” del informe perimetral de septiembre 2025 del Ministerio de Trabajo (MinTrabajo).

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

Failed Login Attempts

#	User	Type	Total Number of Failed Attempts
1	administrator	ssl-web	5,685
2	Administrator	ssl-web	4,118
3	admin	ssl-web	2,499
4	User	ssl-web	1,464
5	Administrador	ssl-web	1,067
6	test	ssl-web	724
7	administrador	ssl-web	529
8	Guest	ssl-web	507
9	Admin	ssl-web	459
10	scanner	ssl-web	457

Ilustración 141 sesiones fallidas

Análisis

Durante septiembre 2025 se registraron múltiples intentos fallidos de acceso VPN, orientados a cuentas administrativas genéricas, lo que confirma la presencia de actividad automatizada externa (fuerza bruta).

El sistema respondió correctamente, sin accesos exitosos detectados, pero se recomienda reforzar la autenticación multifactor (MFA), aplicar bloqueo por IP, y eliminar cuentas por defecto para reducir la exposición perimetral.

3.1.5.2 Sandbox – Amenazas día 0

El servicio de Sandbox para el Ministerio del Trabajo se utiliza para crear entornos aislados y seguros donde se pueden ejecutar archivos o programas sospechosos para analizar su comportamiento. La función principal del Sandbox es detectar y analizar posibles amenazas de seguridad, como malware o software malicioso, sin comprometer la seguridad del sistema principal. Para el mes de septiembre de 2025, se generaron 182 eventos analizados, los cuales fueron limpiados de algún tipo de amenazas

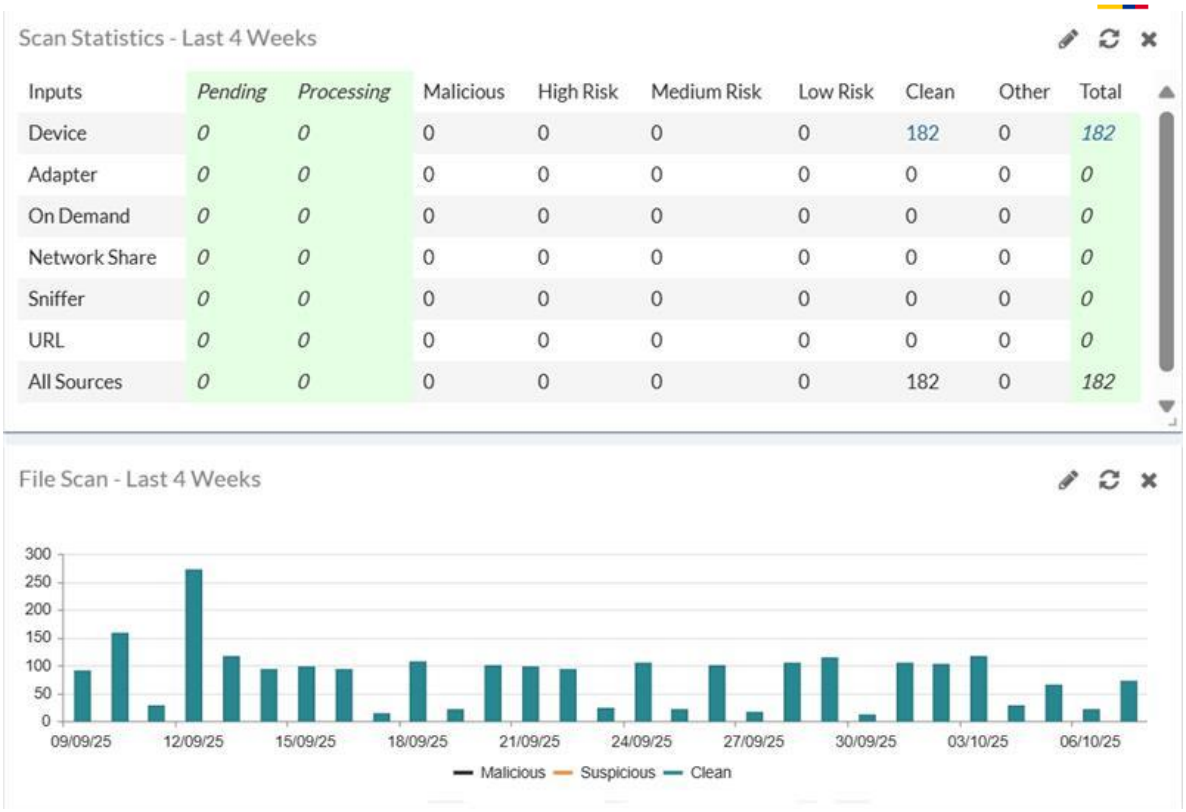


Ilustración 142 Reporte mensual septiembre

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

Performance

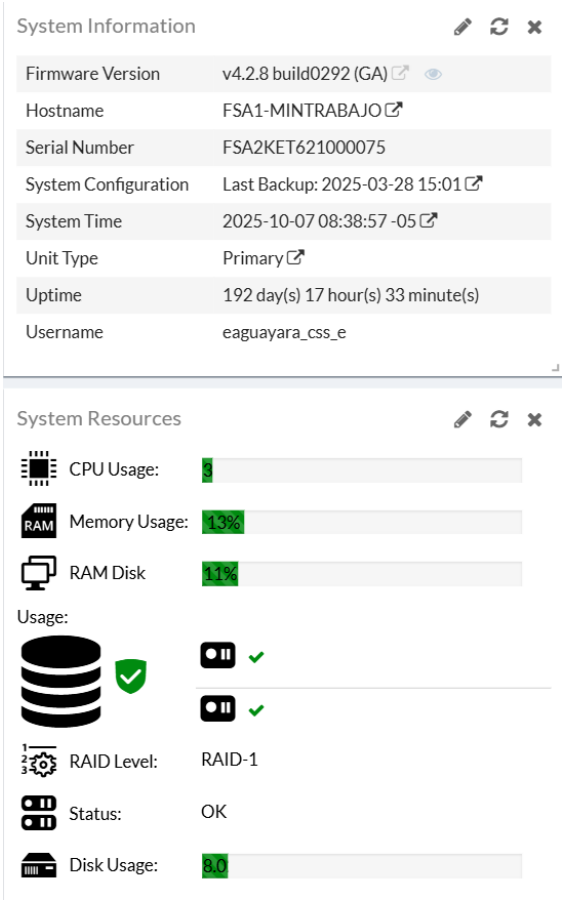


Ilustración 143 Captura de pantalla perfomance

Licencia Sandbox

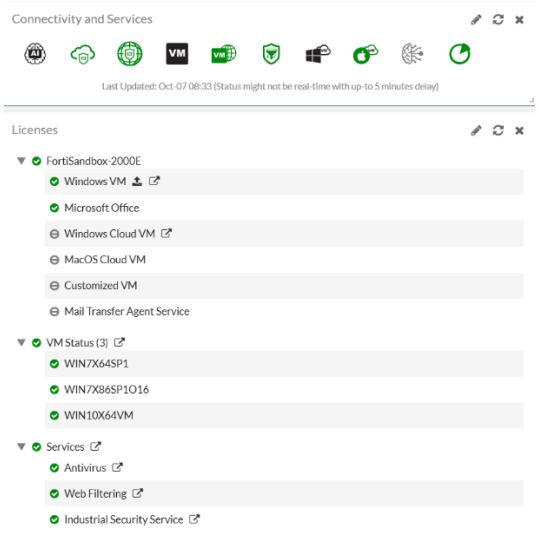


Ilustración 144 licencia sandbox

3.1.5.3 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 3 successive readings in a 10 minute interval	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent, Linux via SNMP	Correlation			Streaming
	☑	9 - HIGH	(s) Server Disk Latency Critical	Detects that server disk I/O latency has reached a critical level (greater than 50 msec) based on 2 successive readings in a 10 minute interval	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent, Linux via SNMP	Correlation			Streaming
	☑	5 - MEDIUM	(s) Server Disk Latency Warning	Detects that server disk I/O latency has reached a warning level (between 20 and 50 msec) based on 2 successive readings in a 10 minute interval	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent, Linux via SNMP	Correlation			Streaming
	☑	9 - HIGH	(s) Server Disk Space Critical	Detects that server disk space usage has reached a critical level (greater than 95% and free disk less than 100 MB) based on 2 successive readings in a 10 minute interval	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent, Linux via SNMP	Correlation			Streaming
	☑	5 - MEDIUM	(s) Server Disk space Warning	Detects that server disk space usage has reached a warning level (utilization between 90% and 95% and free disk still greater than 100 MB) based on 2 successive readings in a 10 minute interval	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent, Linux via SNMP	Correlation			Streaming
	☑	9 - HIGH	(s) Server Intf Error Critical	Detects that a server interface errors has reached a critical level (greater than 5% based on 2 successive readings in a 10 minute interval	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent, Linux via SNMP	Correlation			Streaming
	☑	5 - MEDIUM	(s) Server Intf Error Warning	Detects that a server interface error has reached a warning level (utilization between 1% and 5% based on 2 successive readings in a 10 minute interval	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent, Linux	Correlation			Streaming

Ilustración 145 licencia sandbox

3.1.6.3.2 Disponibilidad (Availability)

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

- **Uso excesivo de CPU o memoria (RAM)**, que puede indicar aplicaciones fuera de control, procesos maliciosos o configuraciones inadecuadas.

- **Latencia o errores de entrada/salida en disco**, que pueden reflejar problemas con el hardware de almacenamiento o cuellos de botella en el rendimiento de las aplicaciones

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

Ilustración 146 Detalle de latencia o errores

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

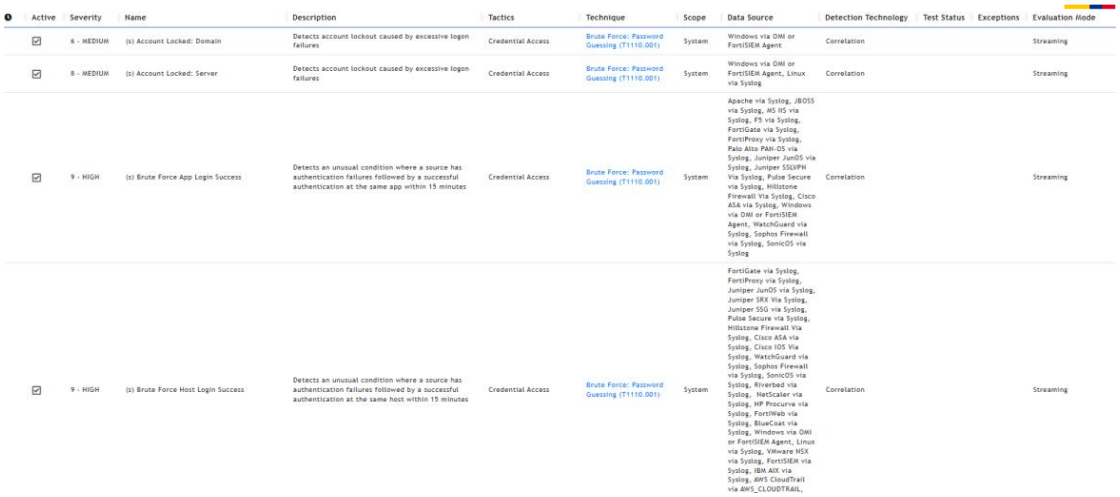
Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☐	4 - LOW	(s) Auto Service Stopped	Detects that an automatically running service stopped. Currently this works for windows servers and is detected via WMI.	Impact	Service Stop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

Ilustración 147 detalle de problemas en servicios

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

3.1.6.3.3. Seguridad (Security) Autenticación:

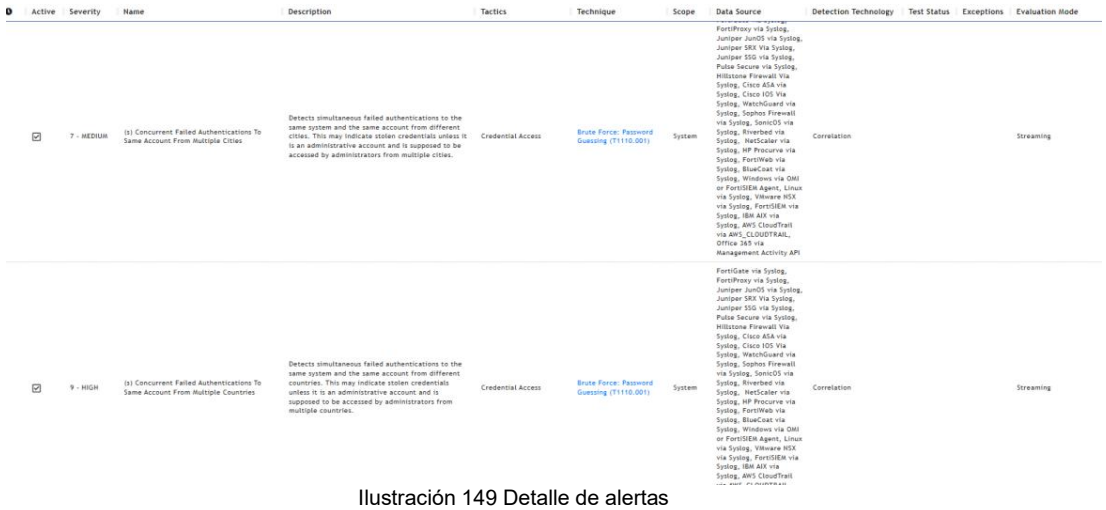
Los casos de uso de seguridad de autenticación en el FortiSIEM se centran en garantizar la integridad y la autenticidad de las credenciales de usuario en todos los dispositivos que tienen instalado el agente. Se muestran los casos Autenticación configurados para el ministerio de trabajo:



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

Ilustración 148 Detalle casos de uso

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



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

Ilustración 149 Detalle de alertas

Acciones tomadas:

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

3.1.6.3.4. Violación de políticas (Policy violation)

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

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

Ilustración 150 Detalle de alertas

Acciones realizadas

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

3.1.6.3.5. Overview incidentes

Durante septiembre 2025, el perímetro de MinTrabajo bloqueó más de 23.000 ataques web y 2.000 intentos de acceso VPN no autorizados, sin evidencia de intrusión exitosa. El entorno mantiene una postura de seguridad robusta.

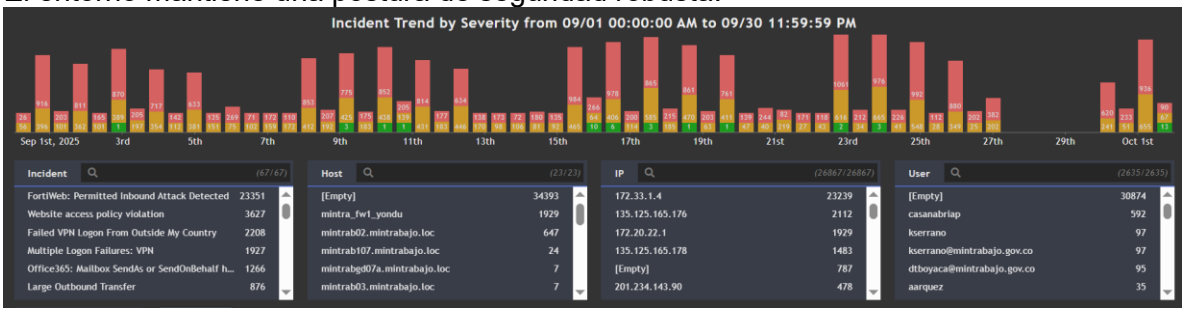


Ilustración 151 Detalle de incidentes

Análisis de incidentes

Tipo de incidente	Descripción	Volumen	Observaciones
FortiWeb: Permitted Inbound Attack Detected	Intentos de acceso web con patrones de ataque conocidos (SQLi, Path Traversal).	23,351	Ataques bloqueados exitosamente. Refleja actividad constante desde Internet.
Website access policy violation	Intentos de acceso a sitios o recursos no permitidos.	3,627	Usuarios internos intentando navegar fuera de las políticas de seguridad.
Failed VPN Logon From Outside My Country	Intentos de autenticación VPN desde IPs extranjeras.	2,028	Indica intentos de acceso remoto no autorizados, posiblemente automatizados.
Multiple Logon Failures: VPN	Múltiples fallos de autenticación seguidos.	1,927	Podría asociarse a errores de credenciales o fuerza bruta.
Office365: Mailbox SendAs/SendOnBehalf	Intentos de envío desde buzones compartidos.	1,126	Actividad legítima, pero debe auditarse por riesgo de spoofing o abuso.
Large Outbound Transfer	Tráfico saliente superior al umbral definido.	876	Indica posible carga o transferencia de grandes archivos; requiere validación.

Tabla 65 Tipos de incidentes

3.1.6.4.6 Top Disponibilidad de servidores

La imagen proporciona un análisis de los servidores monitoreados por FortiSIEM, destacando los 10 servidores que generaron eventos de disponibilidad en términos de seguridad durante el mes de 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 4 días tiempo de actividad.
- mintrab03 y MINTRAB94: con tiempos cercanos a los 5 días.
- MTSISINFOREPO3: con más de 4 días activos sin reinicio.

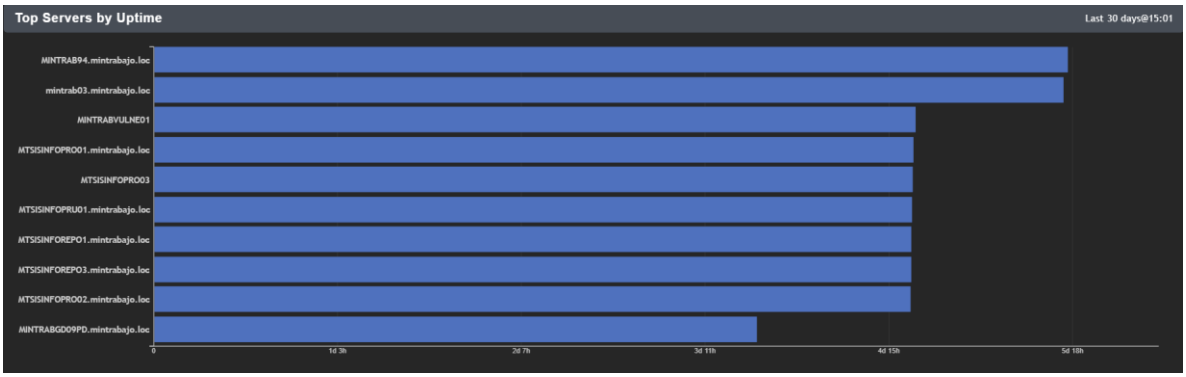


Ilustración 152 Detalle servidores

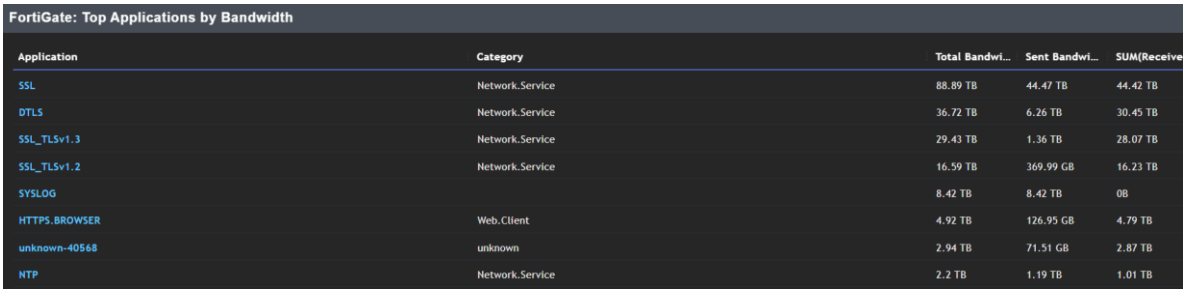
3.1.6.4.7 Top Aplicaciones por Bandwidth

Durante el último mes, el análisis del tráfico de red revela un uso intensivo de aplicaciones cifradas y servicios en la nube. El tráfico se concentra en protocolos seguros como HTTPS

y SSL, lo cual indica una alta cantidad de navegación web y conexiones protegidas. También se observa un uso significativo de aplicaciones de mensajería y plataformas publicitarias, así como una fuerte participación de direcciones IP internas específicas.

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

- SSL, Network.Service: 44.42 TB
- HTTPS.BROWSER: 4.79TB



FortiGate: Top Applications by Bandwidth

Application	Category	Total Bandwi...	Sent Bandwi...	SUM(Receive
SSL	Network.Service	88.89 TB	44.47 TB	44.42 TB
DTLS	Network.Service	36.72 TB	6.26 TB	30.45 TB
SSL_TLSv1.3	Network.Service	29.43 TB	1.36 TB	28.07 TB
SSL_TLSv1.2	Network.Service	16.59 TB	369.99 GB	16.23 TB
SYSLOG		8.42 TB	8.42 TB	0B
HTTPS.BROWSER	Web.Client	4.92 TB	126.95 GB	4.79 TB
unknown-40568	unknown	2.94 TB	71.51 GB	2.87 TB
NTP	Network.Service	2.2 TB	1.19 TB	1.01 TB

Ilustración 153 Detalle fortigate

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

Conclusiones

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

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

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

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

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

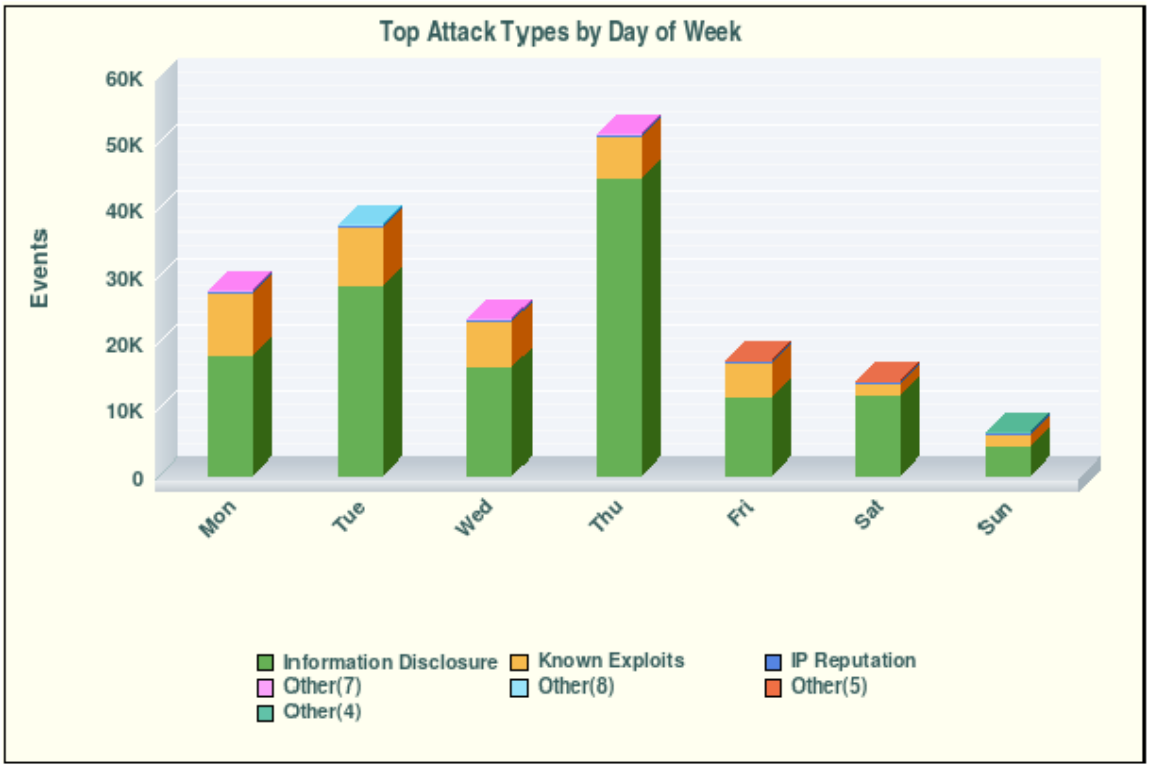


Ilustración 154Top attack types

Análisis

Information Disclosure
Eventos registrados: **180491** (59 % 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: 128 (2.44% 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: 145 (3.9% 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.

3.1.5.5 Solución de Anti-DDoS

Durante el período del mes de septiembre, 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)	PAGINA_MINTRABAJO	Outbound	311	22
State Anomalies: Foreign packet (Out of State)	GESTOR_DOC_MINT	Outbound	30	2

Ilustración 155 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 (22), lo que sugiere riesgo en aplicaciones web institucionales.

3.1.6.5.1 Login Fallidos

Durante el mes de septiembre, no se registraron eventos de inicio de sesión fallidos, los cuales no fueron detectados por la herramienta de seguridad implementada por la UT contra ataques de denegación de servicio (DDoS). Es de aclarar que estos intentos de inicios de sesión corresponden a los ingresos que realizaron los especialistas que atienden el servicio. A continuación, se presentan los hallazgos más destacados:

3.1.5.6 Casos atendidos de los servicios de seguridad

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

3.1.5.6.1 Incidentes

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

3.1.5.6.2 Requerimientos

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

No. Caso	Fecha Registro	Asunto	Grupo Responsable	Categoria
RF-146015	1/09/2025 8:32	RV: Notificación de Inconsistencias en su Declaración de Renta .	SOC	Revisar correo malicioso
RF-146018	1/09/2025 8:39	Solicitud de revisión	SOC	Análisis de Correos
RF-146234	1/09/2025 15:15	RE: COMPARECENCIA OBLIGATORIA – DEMANDA POR AFECTACIÓN PATRIMONIAL – JUZGADO 005	SOC	Análisis de Correos
RF-146398	2/09/2025 8:58	Revisión de correo	SOC	Revisar correo malicioso
RF-146478	2/09/2025 10:40	Retorno de Ruta Segmento Magangué	SOC	Crear politica
RF-146650	2/09/2025 15:33	urgente bloquear dominios maliciosos	SOC	Agregar a listas negras
RF-146671	2/09/2025 15:57	Solicitud de revisión de confiabilidad de correo electrónico	SOC	Remediación vulnerabilidades (equipos ciberseguridad)
RF-146888	3/09/2025 11:05	Correo sospechoso	SOC	Revisar correo malicioso
RF-146910	3/09/2025 11:39	Boletín CNSD-20250830-001 Alerta Campaña de Phishing	SOC	Análisis vulnerabilidades
RF-146977	3/09/2025 14:22	RE: Solicitud SOC - Adicción ip	SOC	Crear politica
RF-147260	4/09/2025 10:21	RV: Puertos TCP y UDP - ESXi	SOC	Agregar puertos
RF-147262	4/09/2025 10:22	RV: Puertos TCP y UDP 902	SOC	Crear Politicas
RF-147577	5/09/2025 8:15	Solicitud de confirmación para abrir correo	SOC	Análisis de Correos
RF-147747	5/09/2025 14:44	Solicitud VPN - CPS-MT-543-2025 - Auditoria	SOC	Falla aplicación
RF-147950	8/09/2025 7:23	RV: CRONOGRAMA PLAN NACIONAL DE EDUCACIÓN MULTIMODAL 2025 DEL 01 AL 05 DE SEPTIEMBRE.	SOC	Agregar a sitios permitidos
RF-148087	8/09/2025 10:34	RV: Solicitud reunión DIMAR	SOC	Revisar correo malicioso
RF-148396	9/09/2025 8:14	MINTRABAJO TLP:RED// Boletín // TI - KillSec; Ataques selectivos contra infraestructuras críticas.	SOC	Agregar a listas negras
RF-148848	10/09/2025 9:20	MINTRABAJO TLP:RED// Boletín // TI - Archivos SVG; de imagen inofensiva a arma de phishing y distribución de malware.	SOC	Análisis vulnerabilidades
RF-148875	10/09/2025 10:05	RV: TR923D ******** NOTIFICACIÓN ELECTRÓNICA DE SENTENCIA JUDICIAL POR EMBARGO ****** TR93DK	SOC	Análisis de Correos
RF-148994	10/09/2025 14:30	RE: MINTRABAJO TLP:RED// Boletín // TI - KillSec; Ataques selectivos contra infraestructuras críticas.	SOC	Instalación de agente
RF-149162	11/09/2025 9:09	RV: INFORMACIÓN IMPORTANTE SOBRE PROCESOS VIGENTES	SOC	Análisis de Correos
RF-149223	11/09/2025 10:11	Correo Malicioso	SOC	Revisar correo malicioso
RF-149246	11/09/2025 11:13	Correo Malicioso	SOC	Análisis de Correos

RF-149258	11/09/2025 11:38	CORREO MALICIOSO	SOC	Revisar correo malicioso
RF-149805	15/09/2025 8:52	FortiSIEM Alert: TLP:RED - Mintrabajo - Office365: Suspicious File Type Uploaded	SOC	Revisar correo malicioso
RF-149839	15/09/2025 9:49	Sitio restringido - Página confama	SOC	Agregar a sitios permitidos
RF-150247	16/09/2025 9:16	MINTRABAJO TLP:RED// Boletín Lite // TI - Múltiples paquetes NPM comprometidos por el malware Scavenger.	SOC	Crear politica
RF-150253	16/09/2025 9:19	FortiSIEM Alert: TLP:RED - Mintrabajo - Possible Brute Force Alert Windows	SOC	Accesos por fuerza bruta
RF-150258	16/09/2025 9:24	MINTRABAJO TLP:RED// Cyberspike Villager como sucesor de Cobalt Strike en el contexto de Amenazas Persistentes impulsadas por IA (AiPT).	SOC	Crear politica
RF-150399	16/09/2025 15:00	SOLICITUD AVERIGUACION DECENDENCIA DE ESTE CORREO	SOC	Revisar correo malicioso
RF-150411	16/09/2025 15:26	CORREOS SOSPECHOSOS	SOC	Análisis de Correos
RF-150560	17/09/2025 9:45	Correo sospechoso	SOC	Revisar correo malicioso
RF-150561	17/09/2025 9:52	Correo sospechoso	SOC	Revisar correo malicioso
RF-150675	17/09/2025 13:53	RV: COMUNICADO FORMAL A TRAVÉS DE NOTIFICACIÓN VIRTUAL	SOC	Análisis de Correos
RF-151018	18/09/2025 11:00	FortiSIEM Alert: TLP:RED - Mintrabajo - Possible Brute Force Alert Windows	SOC	Accesos por fuerza bruta
RF-151030	18/09/2025 11:13	Correo sospechoso	SOC	Revisar correo malicioso
RF-151315	19/09/2025 10:49	Mintrabajo - Command interpreter in Windows cmd or powershell	SOC	Análisis de evento
RF-151385	19/09/2025 14:45	RE: Solicitud de escaneo de amenazas en carpeta compartida BCP 2025	SOC	Análisis vulnerabilidades
RF-151550	22/09/2025 9:01	RE: correo malicioso 890900608;ALMACENES ÉXITO S.A;HS181067839;01;EXITO CHAPINERO	SOC	Análisis de Correos
RF-151659	22/09/2025 11:27	FortiSIEM Alert: TLP:RED - Mintrabajo - Command interpreter in Windows cmd or powershell	SOC	Análisis de evento
RF-152189	23/09/2025 16:11	RV: Citación oficial – Demanda en su contra	SOC	Revisar correo malicioso
RF-152336	24/09/2025 9:38	RV: Bloqueo de puestos USB	SOC	Habilitación Puertos USB
RF-152357	24/09/2025 10:05	Correo sospechoso	SOC	Revisar correo malicioso
RF-152394	24/09/2025 10:34	Correo sospechoso	SOC	Revisar correo malicioso
RF-152417	24/09/2025 10:54	Bloqueo Categoria Games mintrabajo	SOC	Crear politica
RF-152533	24/09/2025 15:00	Urgente Inconsistencias en su Declaración de Renta	SOC	Reporte de Vulnerabilidades
RF-153092	26/09/2025 10:48	RE: Bloqueo de puestos USB	SOC	Habilitación Puertos USB
RF-153398	29/09/2025 8:32	SOLICITUD HABILITAR PUERTO USB GRUPO DE TUTELAS	SOC	Habilitación Puertos USB
RF-153467	29/09/2025 10:59	Creación Política de Denegación Servicio Timestamp Firewall SOC	SOC	Crear politica
RF-153485	29/09/2025 11:40	RV: Bloqueo de puestos USB	SOC	Habilitación Puertos USB
RF-153677	29/09/2025 18:01	SOLICITUD HABILITAR PUERTOS USB	SOC	Habilitación Puertos USB
RF-153694	30/09/2025 1:57	Bajar publicación de SIMPC	SOC	Eliminación de activo

Tabla 66 Reporte de requerimientos septiembre

3.1.5.7 Análisis de riesgo

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

- Ejecución de archivos maliciosos

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

Tabla 67 Vulnerabilidades en la infraestructura

- **Vulnerabilidades en la infraestructura**

Riesgo	Impacto	Probabilidad
La infraestructura de TI presenta vulnerabilidades que pueden ser explotadas por atacantes	Acceso no autorizado, escalamiento de privilegios y explotación de fallos en la red	Media-Alta, dependiendo de la criticidad de las vulnerabilidades detectadas.

Tabla 68 Vulnerabilidades en la infraestructura

- **Ataques de Phishing dirigidos**

Riesgo	Impacto	Probabilidad
intentos de phishing dirigidos a altos funcionarios, como el ministro de Trabajo, con el objetivo de robo de credenciales o entrega de malware.	intentos de phishing dirigidos a altos funcionarios, como el ministro de Trabajo, con el objetivo de robo de credenciales o entrega de malware.	alta, debido al uso constante de correos electrónicos en la comunicación oficial.

Tabla 69 ataques de phishing

3. Medidas de Mitigación Recomendadas

Control y restricción de archivos ejecutables:

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

Gestión de vulnerabilidades:

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

Prevención y respuesta ante phishing:

- Se tiene Implementado de filtros avanzados de correo electrónico y autenticación multifactor (MFA).

- Se realizó análisis a los correos sospechosos y reporte inmediato de intentos de phishing.

3.1.5.8 Políticas y procedimiento de seguridad

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

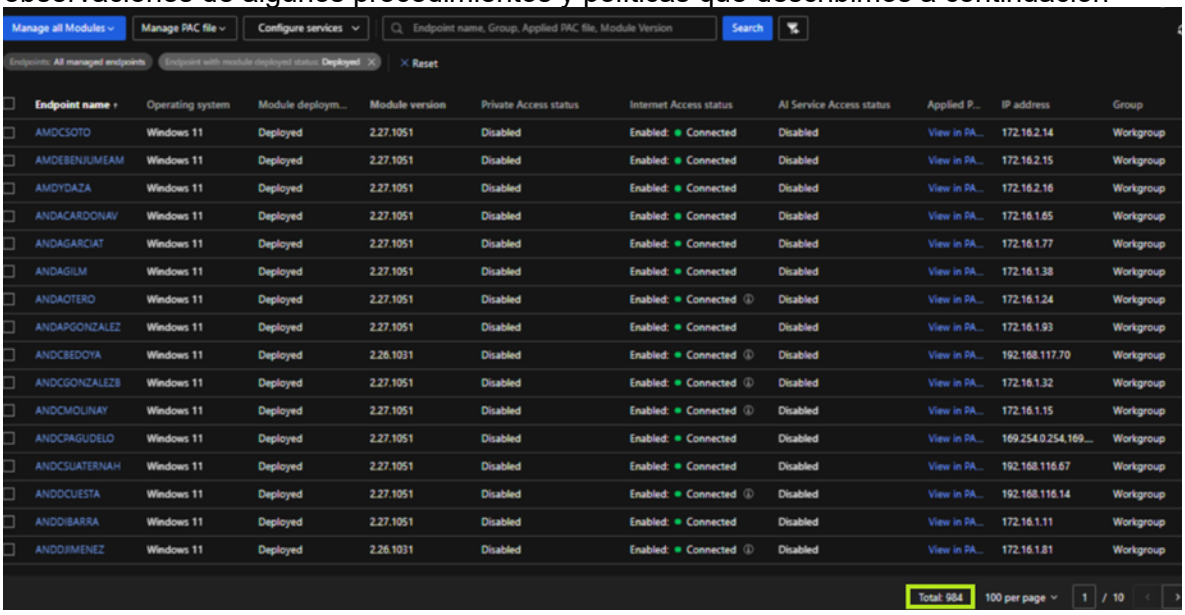


Ilustración 156 Políticas y procedimientos

Actualmente, el servicio de Zero Trust Network Access (ZTNA) se encuentra en proceso de ajuste y optimización de las reglas de acceso a Internet. A la fecha, se han desplegado 984 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

09/09/2025 – MINTRABAJO
Boletín Lite // TI – KillSec
Riesgo: Ataques selectivos contra infraestructuras críticas.

09/09/2025 – MINTRABAJO
Boletín Lite // TI – Vulnerabilidad CVE-2025-38352
Vulnerabilidad crítica en Vulnerabilidad de condición de carrera en el kernel de Linux.

10/09/2025 – MINTRABAJO
Boletín Lite // TI – Alerta Archivos SVG
arma de phishing y distribución de malware.

16/09/2025 – MINTRABAJO
Boletín // TI – paquetes NPM
Riesgo Múltiples paquetes NPM comprometidos por el malware Scave.

22/08/2025 – MINTRABAJO
Boletín // TI – **Cyberspike Village**
Ataques dirigidos contra el sector energético y gobierno de Pakistán.

16/09/2025 – Mintr
Boletín Lite // TI – Shamos Malware
Nuevo malware sucesor de Cobalt Strike en el contexto de Amenazas Persistentes impulsadas por IA (AiPT).

3.1.6 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 70 Licenciamiento

3.1.7 Administración, soporte y monitoreo

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

- En proceso de 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 la línea de Servicios Centrales

Almacenamiento

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

Medición ANS Datacenter y Nube Pública

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

ID	Indicadores	Resultado	Meta
DC-1	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
DC-2	Continuidad y disponibilidad del datacenter principal	100,00%	99.95%
DC-3	Continuidad y disponibilidad del datacenter alterno	100,00%	99,60%
DC-4	Continuidad y disponibilidad de la plataforma de procesamiento, almacenamiento y respaldo	99,99%	99,70%
DC-5	Tiempo de solución de incidentes asociado a los servicios de aplicaciones especializadas	97,93%	90,00%
DC-6	Tiempo de solución de requerimientos asociado a los servicios de aplicaciones especializadas	100,00%	90,00%
DC-7	Continuidad y disponibilidad de los servicios de directorio activo	100,00%	99,60%
DC-8	Continuidad y disponibilidad de los servicios de seguridad informática	100,00%	99,90%
DC-9	Tiempo de solución de incidentes asociado a los servicios de administración, soporte y monitoreo	99,09%	90,00%
DC-10	Tiempo de solución de requerimientos asociado a los servicios de administración, soporte y monitoreo	99,72%	90,00%
DC-11	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 71 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 72 Medición ANS Nube Pública

3.2 No aplica

3.3 Conectividad WAN, SDWAN e Internet

3.3.1 Canales WAN

A nivel de canales WAN, se prestó el servicio en cada sede territorial de forma estable, no obstante, en las sedes donde se presentó algún tipo de falla se generó el

respectivo caso con el proveedor de conectividad, los incidentes presentados se ven reflejados en el ítem 3.3.1.1.
Se observa en la gráfica de consumo, que el tráfico fue estable durante el mes de septiembre, no se observan caídas del canal, se tiene un consumo promedio de 190.67Mbps y se presentó un pico de 1.31 Gbps.

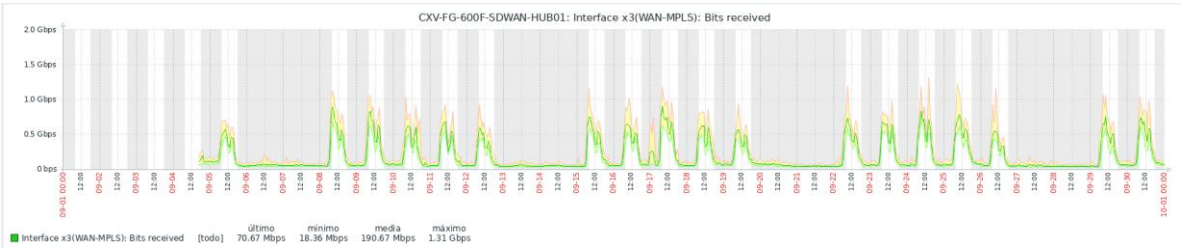


Ilustración 157 Consumo canal MPLS DC Principal

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

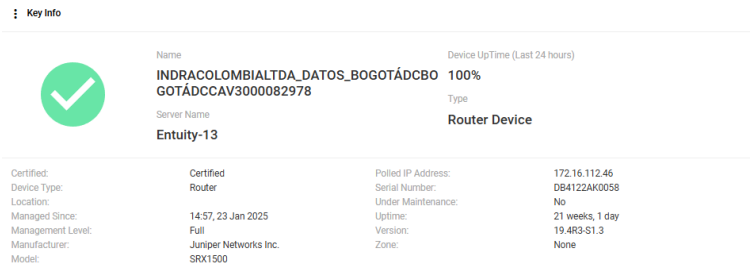


Ilustración 158 Estado Router MPLS DC Principal

3.3.1.1 Incidentes de Conectividad

Durante el mes de septiembre, 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 Florencia	91,35%	IM-149103
Sede Territorial Popayan	99,67%	IM-153080
Sede Territorial Neiva	99,67%	IM-153080
Sede Territorial Villavicencio	99,78%	IM-149047
Sede Territorial Ibague	99,67%	IM-153080
Concordia	97,50%	IM-152675
Sede Centro Calle 32	91,76%	IM-152468
Guapi	99,33%	IM-153080
Santander De Quilichao	93,59%	IM-146436
Bosconia	86,85%	IM-152345
Caldas	90,22%	IM-148158

Ubate	96,33%	IM-148653
Pitalito	99,35%	IM-147942
Granada	98,72%	IM-146769
Puerto Gaitan	97,54%	IM-152678
Tumaco	90,43%	IM-153296
Sede Territorial Cucuta	98,27%	IM-153340
Orito	99,33%	IM-153080
Espinal	99,33%	IM-153080
Turbo	56,92%	IM-149277
Cartago	96,97%	IM-149332
Palmira	80,58%	IM-148956
Sevilla	96,97%	IM-149334

Tabla 73 Incidentes de conectividad

3.3.2.1 Topología Actual

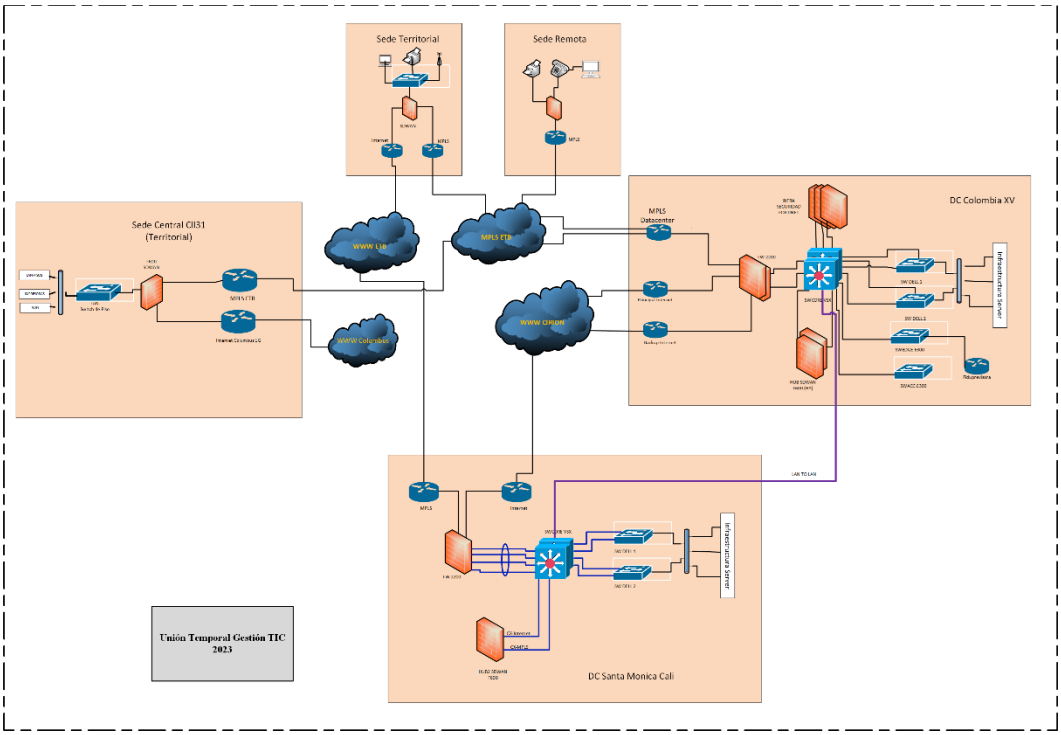


Ilustración 159 Topología actualizada

3.3.2 Canales SDWAN e Internet Dedicado

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

A nivel SDWAN se tienen los equipos registrados en la plataforma Fortimanager, desde donde se observa el estado de los equipos de las sedes territoriales e inspecciones, al igual que el estado de los túneles SDWAN establecidos contra el HUB SDWAN en Datacenter, se tienen 151 equipos registrados en esta plataforma.

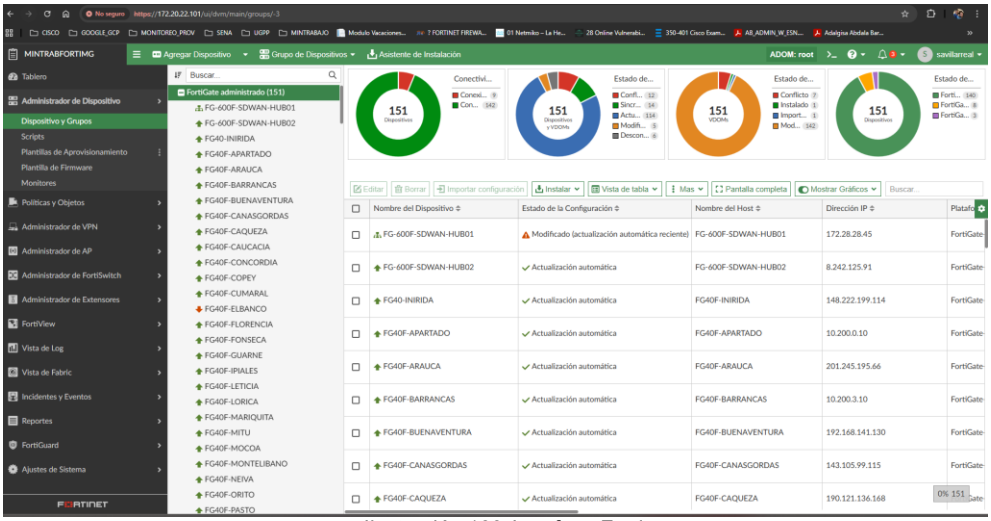


Ilustración 160 Interface Fortimanager

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 190.67 Mbps de consumo con un máximo de 1.31 Gbps, este canal es de 2GB, con el tráfico generado se observa que no presentó saturación durante el mes

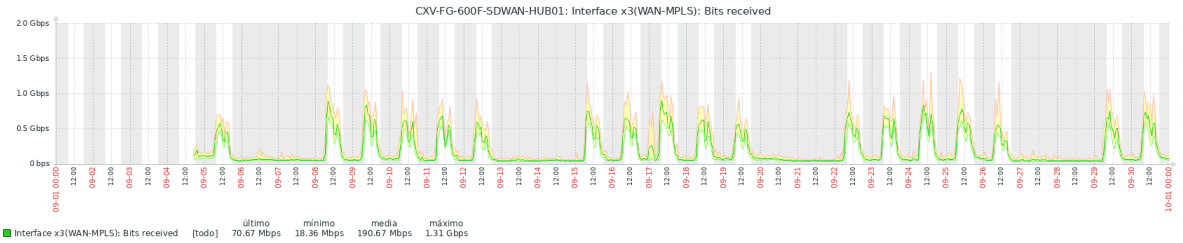


Ilustración 161 Interface MPLS HUB SDWAN

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.

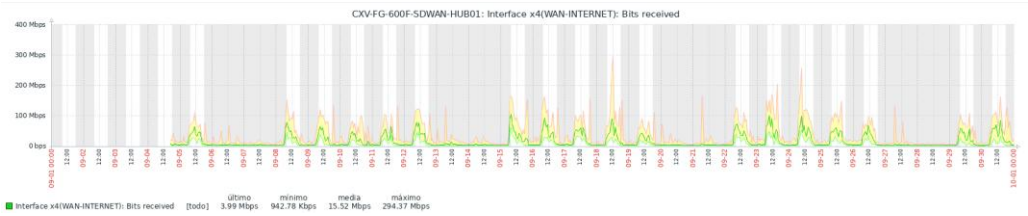


Ilustración 162 Interface Internet HUB SDWAN

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

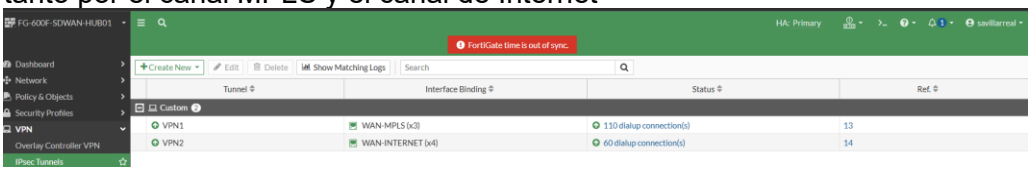


Ilustración 163 VPN SDWAN establecidas

El comportamiento del HUB SDWAN en cuanto a memoria y CPU, se observa que no ha tenido alto procesamiento, se ha tenido un promedio del 19.3278% de utilización de memoria y 0.06566% de CPU, el equipo ha trabajado de forma estable sin presentar picos que causen algún bloqueo o algún reinicio de este.

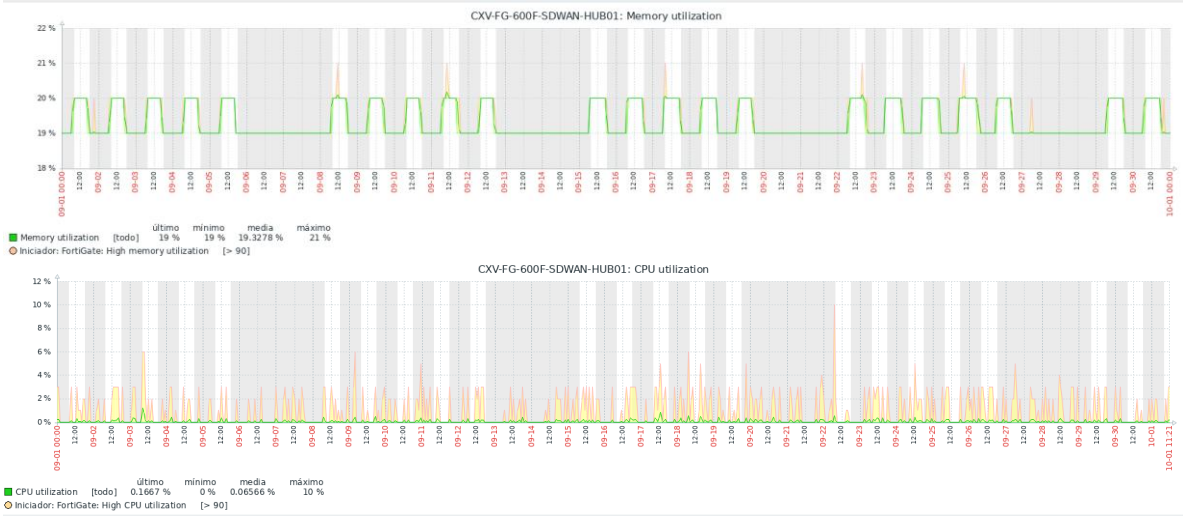


Ilustración 164 Estado HUB SDWAN Datacenter

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.

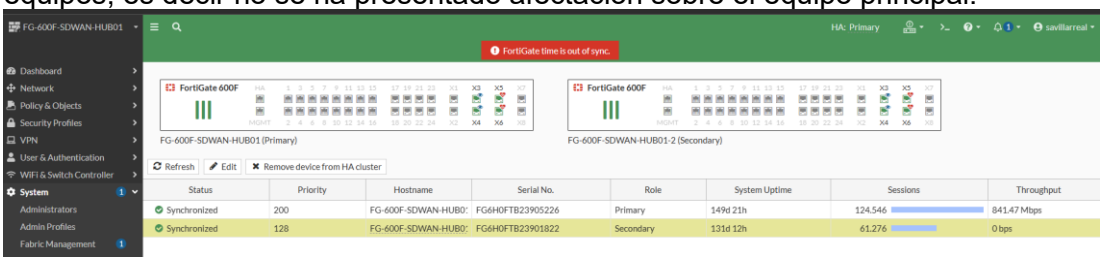


Ilustración 165 Estado HA HUB Sdwan

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

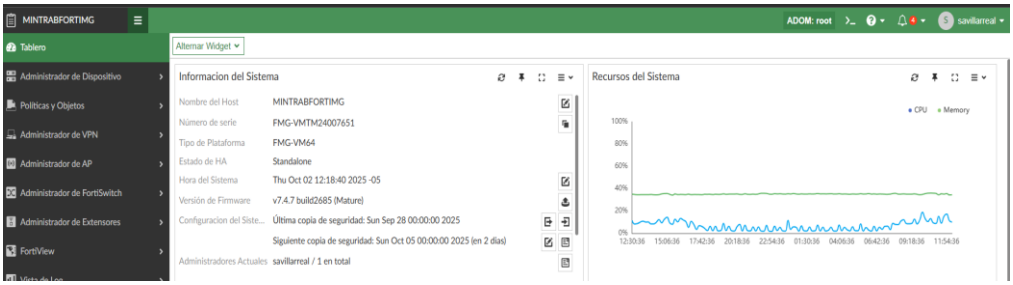


Ilustración 166 Recursos Fortimanager

Otras novedades del servicio:
Se instaló en las sede San Andres un FW F60 con el propósito de ampliar los puertos LAN y unificar conexiones locales que naveguen a través del FW.

Medición de ANS Conectividad WAN e Internet
A continuación, el resultado de la medición de los ANS:

ID	Indicadores	Resultado	Meta
CWI-1	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
CWI-2	Continuidad y disponibilidad del servicio de WAN en sedes nacionales con un solo enlace	(*)	99,60%
CWI-3	Continuidad y disponibilidad del servicio de WAN en sedes nacionales con doble enlace (principal MPLS + secundario Internet dedicado)	100,00%	99,90%
CWI-4	Continuidad y disponibilidad del servicio de internet en Datacenter principal	100,00%	99,95%
CWI-5	Continuidad y disponibilidad del servicio de internet en Datacenter alterno	100,00%	99,70%
CWI-6	Continuidad y disponibilidad del servicio de WAN en Datacenter principal	100,00%	99,95%
CWI-7	Continuidad y disponibilidad del servicio de WAN en Datacenter alterno	100,00%	99,95%
CWI-8	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 74 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 septiembre:

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

Dirección Territorial	Disponibilidad	Caso Asociado	% Penalidad	Valor Penalidad un enlace
Concordia	97,50%	IM-152675	3%	$ 9.240
Guapi	99,33%	IM-153080	3%	$ 9.240
Santander De Quilichao	93,59%	IM-146436	10%	$ 77.004
Bosconia	86,85%	IM-152345	20%	$ 61.603
Caldas	90,22%	IM-148158	10%	$ 18.481
Ubaté	96,33%	IM-148653	3%	$ 9.240
Pitalito	99,35%	IM-147942	3%	$ 9.240
Granada	98,72%	IM-146769	3%	$ 9.240

Puerto Gaitán	97,54%	IM-152678	3%	$ 9.240
Tumaco	90,43%	IM-153296	10%	$ 30.801
Orito	99,33%	IM-153080	3%	$ 9.240
Espinal	99,33%	IM-153080	3%	$ 9.240
Turbo	56,92%	IM-149277	100%	$ 308.015
Cartago	96,97%	IM-149332	3%	$ 9.240
Palmira	80,58%	IM-148956	20%	$ 61.603
Sevilla	96,97%	IM-149334	3%	$ 9.240
Total				**$ 649.911**

Tabla 75 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	Caso Asociado	% Penalidad	Valor Penalidad doble enlace
Sede Territorial Florencia	91,35%	IM-149103	10%	$ 81.261
Sede Territorial Popayán	99,67%	IM-153080	3%	$ 36.567
Sede Territorial Neiva	99,67%	IM-153080	3%	$ 36.567
Sede Territorial Villavicencio	99,78%	IM-149047	3%	$ 36.567
Sede Territorial Ibagué	99,67%	IM-153080	3%	$ 48.757
Sede Centro Calle 32	91,76%	IM-152468	10%	$ 406.304
Sede Territorial Cúcuta	98,27%	IM-153340	3%	$ 48.757
Total				**$ 694.781**

Tabla 76 Desagregado sedes con novedad con doble enlace

4 LINEA DE SERVICIOS EN SEDE

4.1 Equipos de Cómputo de usuario final

Durante el período correspondiente a este informe, se atendieron solicitudes relacionadas con la revisión, pruebas, retiro y asignación de equipos de cómputo. Asimismo, se brindó soporte a las novedades presentadas en el parque computacional Lenovo.
A continuación, se presentan los equipos en operación durante el período, conforme al Anexo de Distribución de Equipos, detallados de la siguiente manera:

Ítem	Cantidad
Equipos de escritorio	1172
Equipos portátiles	1000
Equipos adicionales	120
Total	2292

Tabla 77 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 SEPTIEMBRE		
SEDE	**TIPO DE ELEMENTO**	**CANTIDAD**
DT BOLIVAR	PORTATIL	4
DT CALDAS	PORTATIL	1
DT META	PORTATIL	8
DT HUILA	ESCRITORIO	1
DT NORTE DE SANTANDER	PORTATIL	2
DT QUINDIO	PORTATIL	1
DT RISARALDA	PORTATIL	1
DT SANTANDER	PORTATIL	4
DT SUCRE	PORTATIL	2
DT VALLE DEL CAUCA	PORTATIL	2
NIVEL CENTRAL	PORTATIL	13
TOTAL		**39**

Tabla 78 Cantidades de equipos asignados nivel nacional

DEVOLUCION DE EQUIPOS SEPTIEMBRE		
SEDE	**TIPO DE ELEMENTO**	**CANTIDAD**
DT CAUCA	ESCRITORIO	2
DT CAUCA	PORTATIL	2
NIVEL CENTRAL	PORTATIL	11
TOTAL		**15**

Tabla 79 Cantidades de equipos por devolución nivel nacional

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

Gestión de Garantías:

Durante el mes de septiembre, se reportó un total de 15 casos de garantía a corte del periodo. A continuación, se detallan los estados asociados a estos casos:

Estado de caso	Cantidad
Cerrado	9
Solucionado	1
Suspendido	5
Total	15

Tabla 80 Estado de casos de garantía.

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

ANS	Cerrado	Solucionado	Suspendido	Total
CUMPLE	9	1	5	15
Total	9	1	5	15

Tabla 81 ANS casos de garantía.

Fecha de Reporte	Serial	Parte	Falla	Sede	No. Caso	Estado
23/09/2025	HC3BBL70	Diadema	Falla en diadema	Nivel central	RF-152017	Cerrado
23/09/2025	HC3BBMWG	Diadema	Falla en diadema	Nivel central	RF-151998	Cerrado
22/09/2025	HC3BBLR2	Diadema	Intermitencia	Nivel central	RF-151544	Cerrado
17/09/2025	HC3BBMX2	Diadema	Sonido Bajo	Nivel central	RF-150668	Cerrado
5/09/2025	PW0A3CK9	Portátil	No da imagen	Nivel central	RF-147596	Cerrado
3/09/2025	HC3BBMWP	Diadema	El sonido se distorsiona	Nivel central	RF-146867	Cerrado
3/09/2025	HC3BBMNK	Diadema	presenta fallas en el audio y demás.	DT Caldas	RF-146824	Cerrado
3/09/2025	PW0A0FMT	Portátil	Mancha blanca en la pantalla	Nivel central	RF-146800	Cerrado
1/09/2025	PW09Z36F	Portátil	No carga	Nivel central	RF-146203	Cerrado
24/09/2025	HC3BBLY5	Diadema	Mal funcionamiento	Barrancabermeja	RF-152436	Solucionado
29/09/2025	SPW0A3CK3	Portátil	Hurto	Nivel central	RF-153463	Suspendido
25/09/2025	MJ0LV008	Escritorio	Falla interna	Nivel central	RF-152901	Suspendido
25/09/2025	HC3BBN4L	Diadema	Falla en audio	Cali	RF-152822	Suspendido
25/09/2025	HC3B8DNX	Diadema	Aislamiento de sonido	DT Cauca	RF-152797	Suspendido
23/09/2025	PW09Z34N	Portátil	Desprendimiento de la tecla SHIFT	Nivel central	RF-152111	Suspendido

Tabla 82 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					
Funcionario	Equipo	DT	Parte afectada	ESTADO	Caso Aseguradora/Lenovo
Pavel Santodomingo	PW0A3CDZ	NIVEL CENTRAL	Derrame de líquidos	Reportado ante aseguradora	2025046910
Bernardo Ardila Fernández	PW09Z34H	DT CESAR	Golpes en esquinas	Pendiente revisión con la coordinación	2024554288
Galia Lena Álvarez Hernández	PW0A3CHL	NIVEL CENTRAL	Golpes en esquinas	Funcionaria no ha regresado el equipo	
Ana Mireya Escobar Tierradentro	MJ0S5TW	DT CAUCA	No enciende	Pendiente reposición del equipo	PRG_2025_1766918
Alcides Manuel Morales Ortega	MJ0LS5XL	INSP.SAN MARCOS	Se apaga y no enciende	Pendiente reposición del equipo	PRG_2025_1921454
Jesús Manuel Martínez Franco	PW0A3BEY	DT CORDOBA	Golpes en esquinas	Pendiente revisión con la coordinación	2025347408
William Ricardo Álvarez Gómez	PW0A3CK3	NIVEL CENTRAL	Hurto	Reportado ante aseguradora	

Tabla 83 Equipos en siniestro

Instalaciones de Equipos y Entrega a Usuarios Finales:

Durante el período del presente informe, se recibió el aval por parte del Coordinador del Grupo de Soporte Informático para la asignación de equipos de cómputo destinados a contratistas, pasantes, casos de doble asignación para funcionarios, salas de conciliación y la Contraloría.

Adicionalmente, se recibió el listado de funcionarios con condiciones médicas especiales. En este sentido, el Coordinador del Grupo de Soporte Informático solicitó realizar el cambio de equipo a aquellos funcionarios que actualmente tienen asignado un equipo portátil. Esta actividad se encuentra en curso y su avance depende de la disponibilidad de los usuarios para efectuar el respectivo cambio.

A continuación, se presenta el parque computacional instalado en la entidad con corte al final del período reportado:

TIPO DE EQUIPO	CANTIDAD INSTALADA
Portátil	965
Escritorio	1142
Total	2107

Tabla 84 *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 de septiembre se gestionaron devoluciones de elementos asociados a novedades de funcionarios, tales como retiros, traslados, jubilaciones, entre otros.

DEVOLUCION DE EQUIPOS SEPTIEMBRE		
SEDE	TIPO DE ELEMENTO	CANTIDAD
DT CAUCA	ESCRITORIO	2
DT CAUCA	PORTATIL	2
NIVELCENTRAL	PORTATIL	11

Tabla 85 Devolución de equipos

CANTIDAD DE EQUIPOS		
LUGAR	PORTATIL	ESCRITORIO
ALMACEN	155	30
OPERACIÓN	965	1142
TOTAL	1120	1172

Tabla 86 cantidad de equipos

4.1.1 Equipos de Escritorio

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

4.1.2 Equipos Portátiles

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

- Se registraron en Aranda un total de 15 solicitudes tipificadas así:
  - Incidentes – 0 casos
  - Requerimientos de Servicio – 15 casos.

- Al corte de mes quedaron en estado:
  - Cerrado – 9 casos.
  - Solucionado – 1 casos
  - Suspendido – 5 casos.
  - En Proceso – 0 caso.

- 14 casos corresponden a solicitudes de usuarios estándar y 1 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
Gestor de inventarios	1
Gestor de garantías	14
Total, general	15

Tabla 87 Solicitudes de Equipos Usuario Final – Según Grupo Responsable

- La tabla que se muestra a continuación indica las categorías en las que fueron clasificados estos casos en Aranda:

Tipificación / Categoría	Cantidad de Solicitudes
Incidentes	
Requerimientos	15
Equipo Periférico	9
Equipo Escritorio	1
Equipo Portátil	5
Total	15

Tabla 88 Solicitudes de Equipos Usuario Final – Según Grupo Responsable

- 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	95,83%	90,00%
EUF-2	Cumplimiento en la entrega del informe	100,00%	100,00%

Tabla 89 Medición ANS Equipos de Usuario Final

4.2 Conectividad LAN y WLAN

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

- El 1/09/2025 en el marco del proceso contractual de la Auditoría de Seguridad de la Información, la oficina TICs solicita las direcciones IP de los elementos teleinformáticos sobre la infraestructura de la entidad. Se comparte la información requerida.



RE_ GESTIÓN -
Solicitud de direccion

- 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 realizó depuración de políticas sin tráfico firewall Nivel Central.
- Se gestionó el retiro de switches de nuestro aliado Apicom que no estaban en uso en oficinas del ministerio.
- Se trabajó con el soporte territorial de Cauca la desconexión de switch Planet y se centralizó conexiones en switch Aruba que se encuentra soportado en el contrato.



RE_ Revisión Switch
Marca Planet Territori

- Junto con el aliado de la UT, Apicom se ejecutó ventana de revisión y mantenimiento de UPS en piso 22 de Nivel Central, para verificar carga de baterías.
- Se gestionó visitas de Site Survey con Tigo UNE para mejorar el servicio de conectividad en oficinas del ministerio.
- El 8/09/2025 se da respuesta al cliente sobre la revisión de consumo de ancho de banda de las sedes Neiva, Plata y Pitalito, con base en un comunicado recibido del Director Territorial.

RE_ Validación Ancho de banda Direccion Te

- Se remiten correos electrónicos al Coordinador del Grupo de Soporte informático informando que en la Inspección de Trabajo de Cumaral el usuario altera las conexiones para evitar navegar por el equipo de seguridad Fortinet, por ende genera constantes alertas de caída del servicio en la inspección a nivel de monitoreo.

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

- Los especialistas gestionaron un total de 27 solicitudes escaladas a través de la herramienta Aranda. Al corte del mes, 20 casos quedaron en estado Cerrado, 1 en estado Implementar Cambio, 1 en No ejecutado, 3 en estado Solucionado, 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
FortiGate	5
Degradacion	4
Switch	4
Asesoria - Consulta	3
Canal Internet	2

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

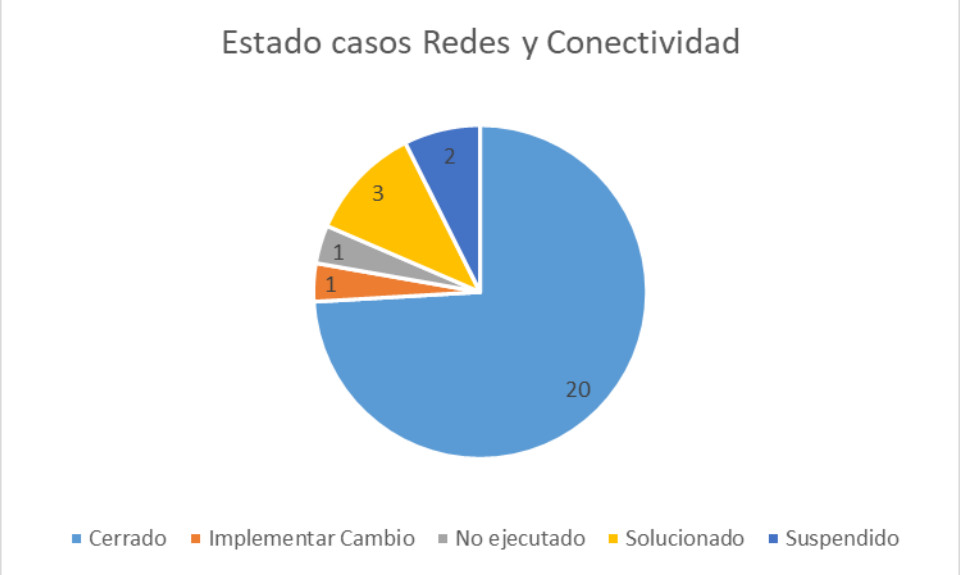


Ilustración 167 Estado de casos Redes y Conectividad

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

4.2.1 Switch CORE Sede Principal

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

4.2.2 Switch para conexiones perimetrales (EDGE) en sede principal

Se encuentra operativo en Datacenter recibiendo las conexiones del canal de internet y conexiones perimetrales.

4.2.3 Switch de acceso 24 puertos

Se encuentran operativos y en monitoreo los siguientes equipos:

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

Tabla 91 Distribución y Cantidades de switch 24 puertos

(*) Se instaló 1 equipo adicional en la Territorial Valle del Cauca en la ciudad de Cali.

4.2.4 Switch de acceso 48 puertos

Se encuentran operativos y en monitoreo los siguientes equipos:

Dirección Territorial	Población y/o ciudad de ubicación	Cantidad switches 48 puertos
Territorial Antioquia	MEDELLIN	4*
Territorial Arauca	ARAUCA	1
Territorial Atlántico	BARRANQUILLA	2
OE Barrancabermeja	BARRANCABERMEJA	1
Calle 32	BOGOTA	5
Territorial Bolívar	Cartagena	1
Territorial Boyacá	TUNJA	1

Territorial Caldas	MANIZALEZ	1
Territorial Cauca	POPAYAN	1
Territorial Cesar	VALLEDUPAR	1
Territorial Chocó	QUIBDÓ	1
Territorial Córdoba	MONTERIA	1
Territorial Cundinamarca	FACATATIVÁ	1
Territorial Guajira	RIOHACHA	1
Territorial Huila	NEIVA	1
Territorial Magdalena	SANTA MARTA	1
Territorial Meta	VILLAVICENCIO	1
Territorial Nariño	PASTO	1
Territorial Norte de Santander	CÚCUTA	1
Territorial Quindío	ARMENIA	1
Territorial Risaralda	PEREIRA	1
Territorial Santander	BUCARAMANGA	2
Territorial Sucre	SINCELEJO	1
Territorial Tolima	IBAGUÉ	1
OE Urabá Apartadó	APARTADÓ	1
Territorial Valle	CALI	2
OE Buenaventura	BUENAVENTURA	1
Sede Nivel Central	BOGOTA	34*
	Total	**71**

Tabla 92 Distribución y Cantidades de Switch 48 puertos

(*) Se instalaron 8 equipos adicionales en las siguientes sedes:

Sede Nivel Central P19: 3 de 48 puertos
P24: 2 de 48 puertos
P25: 2 de 48 puertos
Medellín 1 de 48 puertos

4.2.5 Puntos de Acceso

Se encuentran operativos y en monitoreo los siguientes equipos:

Dirección Territorial	Población y/o ciudad de ubicación	Cantidad Access Points
Territorial Antioquia	MEDELLIN	4
Territorial Arauca	ARAUCA	1
Territorial Atlántico	BARRANQUILLA	3
OE Barrancabermeja	BARRANCABERMEJA	2
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 93 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 y se instaló en el piso 25 de sede central.

- Medición de ANS LAN y WLAN

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

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

Tabla 94 Medición ANS LAN y WLAN

4.3 Telefonía IP

Este servicio comprende Terminales HardPhone compatibles Teams Phone.

4.3.1 Teléfono Gama Media

Se cuenta con los siguientes equipos:

Dirección territorial	Población y/o ciudad de ubicación	Cantidad teléfonos Gama Media
Territorial Antioquia	MEDELLIN	1
Territorial Atlántico	BARRANQUILLA	1
Territorial Bogotá	BOGOTA	1
Territorial Santander	BUCARAMANGA	1
Territorial Valle	CALI	1
Sede Nivel Central BOGOTA	BOGOTA	45*
	Total	**50**

Tabla 95 Equipos gama media

(*) Novedades en la instalación de teléfonos

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

4.3.2 Teléfono Gama Baja

La totalidad de los equipos de telefonía tanto de gama media como de gama baja fueron puestos a disposición para el servicio y se encuentran en cada sede de acuerdo con el anexo de distribución de equipos.

Se indica a continuación las novedades presentadas en la operación de los 350 teléfonos de gama baja:

Dirección territorial	Población y/o ciudad de ubicación	Cantidad teléfonos Gama Baja	Novedad
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 96 Sedes cerradas

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

Tabla 97 Consolidado de teléfonos gama baja

Adicionalmente el servicio de Telefonía IP incluye:

4.3.3 Troncales SIP

La troncal SIP estuvo operativa y funcionando adecuadamente. Se dispuso de la troncal SIP con el proveedor de atención al ciudadano BPM, en el cual el redireccionamiento de llamadas de las opciones 0 y 2, se encuentra operando de manera satisfactoria. Adicional se crea el menú de operadora para el grupo “1070” soporte IVC el cual continúa operando de manera correcta.

4.3.4 No Aplica

4.3.5 No Aplica

4.3.6 Módems 4G – Con plan de 50 Gbps

A continuación, se mencionan los equipos entregados en Nivel Central para el servicio de MIFI en la medida en que la Entidad ha informado los usuarios que los van a utilizar.

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

Tabla 98 Consolidado equipos MIFI

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

- Gestión del servicio

En el mes de septiembre 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.
  - 15/09/2025: Durante el mes en curso se realizó la asignación de un dispositivo MIFI a la sede de Popayán (para Casa de Justicia no para la DT). El equipo fue previamente aprovisionado y configurado para garantizar su correcto funcionamiento. Posteriormente, se efectuó el envío a la sede, donde se confirmó la recepción del dispositivo y la validación de su operatividad. Se entegó junto con un Mini Nano USB.



RE_ Solicitud MiFi +
Adaptador WiFi.msg

-

- 10/09/2025: Por solicitud de LGG se asigna un MiFi a la contratista Diana Esperanza Lopez Rios de Secretaria General Piso 25.



RE_ Asignación MiFi -
Usuaria Secretaria Ge

- Durante el mes en curso se realizó el proceso de configuración y aprovisionamiento de extensiones y asignación de licencias Teams Phone Standard en el tenant de Microsoft Teams para dos usuarios solicitados. Los cambios fueron aplicados exitosamente. Se adjuntaron manuales de soporte y configuración para referencia. Estado actual: Todos los usuarios se encuentran activos – casos RF-149769 y RF-146575.



Asignación ext.
virtual_Teams_Caso_F



Asignación ext.
virtual_Teams_Caso_F

- Asignación de Licencias – Extensiones

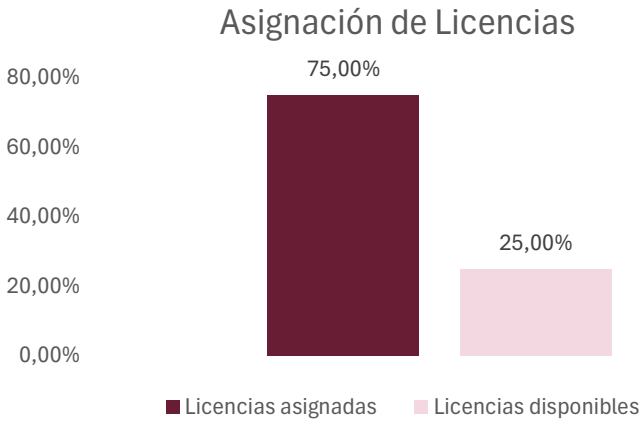


Ilustración 168 Asignación de licencias

Durante el mes en gestión, se han asignado un total de 452 extensiones a nivel nacional. Actualmente, permanecen disponibles 148 extensiones.

- Estadísticas de Tráfico

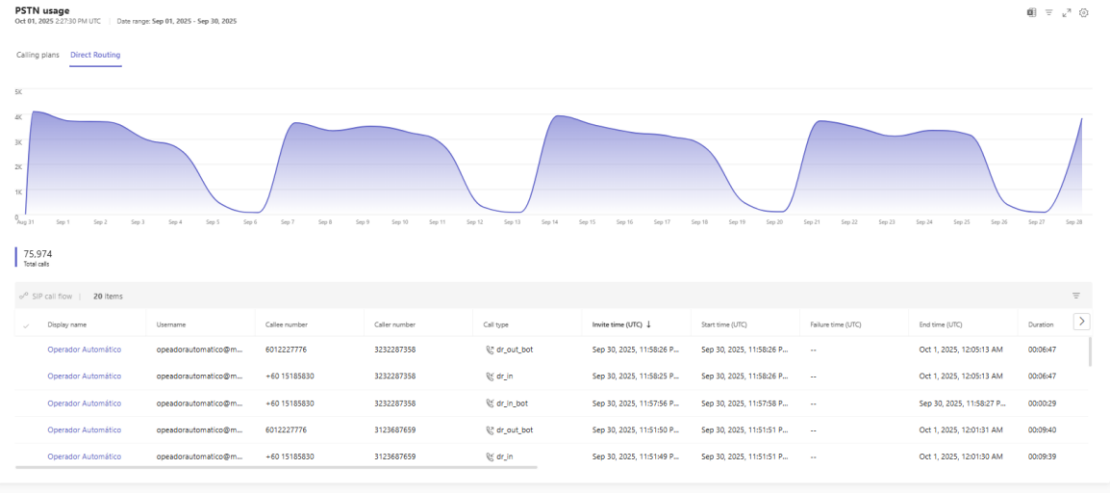


Ilustración 169 Comportamiento de tráfico

En la gráfica anterior se visualizan las tendencias de uso del servicio, en el periodo correspondiente al mes de septiembre de 2025, donde se atendieron un total de 75,974 llamadas.

Servicio	Minutos Disponibles	Minutos Utilizados
Locales	Ilimitados	683.46
Celular	1000	833.05
Nacional	Ilimitados	524.20
Internacional	700	4.4
Total		2045.11

Tabla 99 Minutos, consumos

- Consumo de llamadas LDN (Larga Distancia Nacional)

Con respecto a las llamadas realizadas a destinos larga distancia nacional en el mes de septiembre de 2025, se identifica que se realizaron llamadas con una duración total de 524.2 minutos.

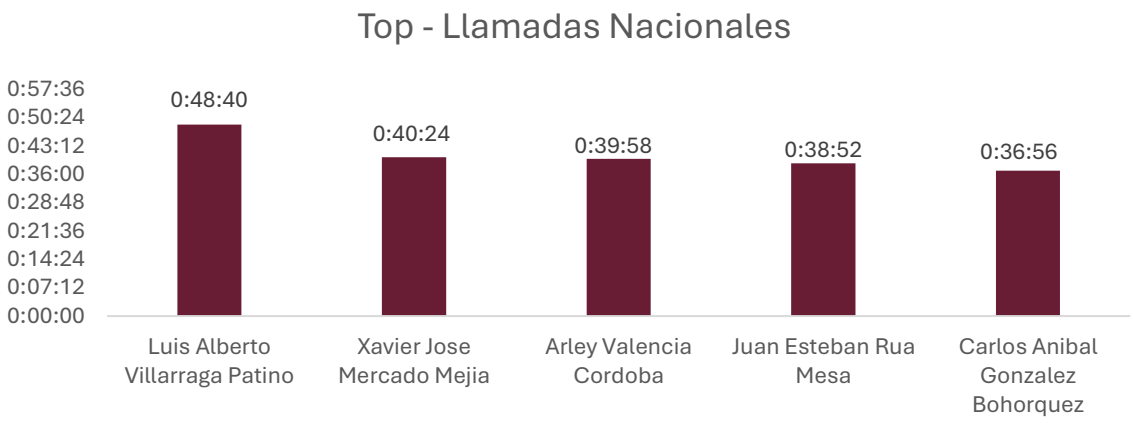


Ilustración 170 Top llamadas nacionales

N°	Usuario	Área	Tiempo llamadas

1	Luis Alberto Villarraga Patino	Dirección de Riesgos Laborales – Sede Central Bogotá	0:48:40
2	Xavier Jose Mercado Mejia	Grupo De Atencion Al Ciudadano Y Tramites – DT Antioquia	0:40:24
3	Arley Valencia Cordoba	Despacho Oficina Especial – Araba Apartado	0:39:58
4	Juan Esteban Rua Mesa	Grupo de Resolución de Conflictos – Conciliación – DT Antioquia	0:38:52
5	Carlos Anibal Gonzalez Bohorquez	Grupo de Riesgos Laborales Antioquia	0:36:56

Tabla 100 Top 5 consumo de llamadas

- Consumo de llamadas LDI (Larga Distancia Internacional)

Con respecto a las llamadas internacionales en el mes de septiembre 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 171 llamada internacional de prueba

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

N°	Usuario	Área	Tiempo llamadas
1	Administrador Telefonía	OTI	0:04:43

Tabla 101 Top 5 llamadas LDI

- Consumo de llamadas destinos celulares

Con respecto a las llamadas realizadas a celular en el mes de septiembre de 2025, se identifica que se realizaron llamadas con una duración total de 833.05 minutos.

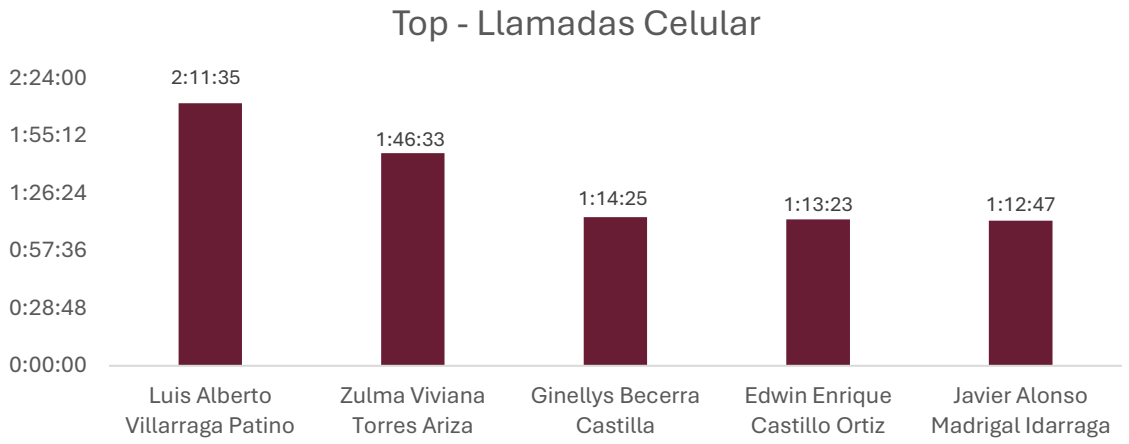


Ilustración 172 Top Celular

N°	Usuario	Área	Tiempo llamadas
1	Luis Alberto Villarraga Patino	Dirección de Riesgos Laborales – Sede Central Bogotá	2:11:35
2	Zulma Viviana Torres Ariza	Comunicaciones DT Bogotá	1:46:33
3	Ginellys Becerra Castilla	Comunicaciones GEEG DT Bogotá	1:14:25
4	Edwin Enrique Castillo Ortiz	Despacho Oficina Especial – Barrancabermeja	1:13:23
5	Javier Alonso Madrigal Idarraga	Grupo de Resolución de Conflictos – Conciliación – DT Antioquia	1:12:47

Tabla 102 Top 5 llamadas Celular

- Consumo de llamadas locales

Con respecto a las llamadas realizadas a destinos locales en el mes de septiembre de 2025, se identifica que se realizaron llamadas con una duración total de 683.46 minutos.

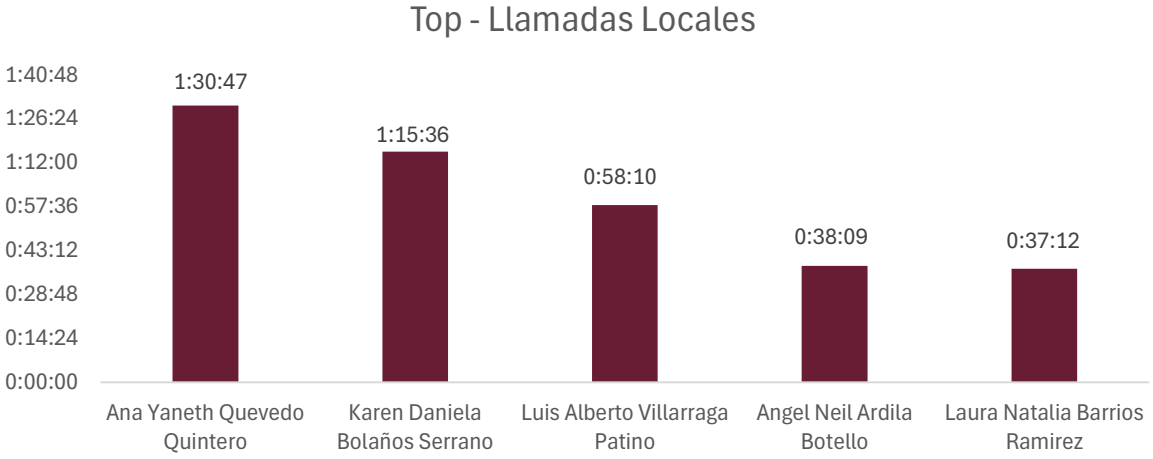


Ilustración 173 Top Local

N°	Usuario	Área	Tiempo llamadas
1	Ana Yaneth Quevedo Quintero	Auxiliar Administrativo / Dirección de pensiones y otras prestaciones – Sede Central Bogotá	1:30:47
2	Karen Daniela Bolaños Serrano	Despacho del viceministro de relaciones laborales e inspección – Sede Central Bogotá	1:15:36
3	Luis Alberto Villarraga Patino	Dirección de Riesgos Laborales – Sede Central Bogotá	0:58:10
4	Angel Neil Ardila Botello	Grupo de Atención al ciudadano – Sede Central Bogotá	0:38:09
5	Laura Natalia Barrios Ramirez	Subdirección Administrativa y Financiera – Sede Central Bogotá	0:37:12

Tabla 103 Top 5 llamadas locales

- Capacitaciones y divulgaciones

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

Ítem	Descripción	Fecha
1	Procedimiento para la identificación de fallas en los Gateways por parte de los soportes en sitio y la revisión posterior cuando se presenten fallas eléctricas en las territoriales.	3-09-2025

Tabla 104 Capacitaciones y divulgaciones

- Mejores Prácticas

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

- Medición de ANS – Telefonía IP

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

TIP-1 Tiempo de solución de requerimientos de garantía



Ilustración 174 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

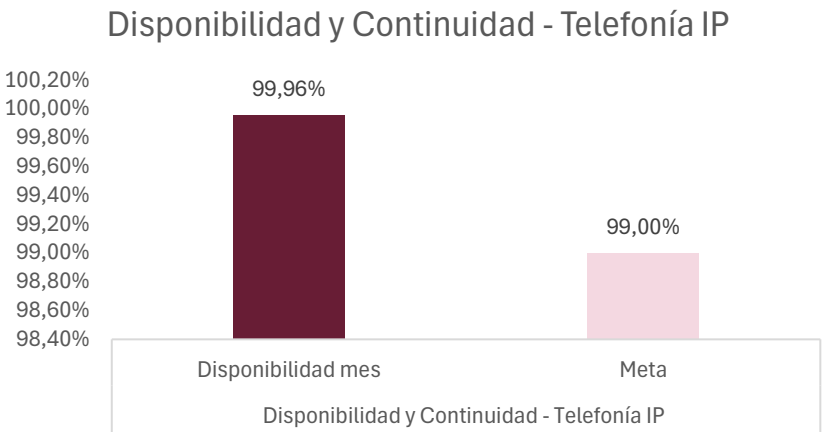


Ilustración 175 Disponibilidad y Continuidad TOIP

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

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

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

Tabla 105 Medición ANS Telefonía IP

4.4 Energía Regulada UPS

El servicio de Energía Regulada UPS comprende las sedes indicadas por la Entidad dentro de los anexos técnicos del contrato, con una distribución de equipos por locación así:

- SEDE NIVEL CENTRAL (14 equipos)
- TERRITORIAL TOLIMA (1 equipo)
- TERRITORIAL BOYACÁ (1 equipo)
- TERRITORIAL BOLÍVAR (1 equipo)
- TERRITORIAL CALDAS (1 equipo)
- TERRITORIAL RISARALDA (1 equipo)
- OE BARRANCABERMEJA (1 equipo)

- TERRITORIAL SANTANDER (1 equipo)
- TERRITORIAL ANTIOQUIA (1 equipo)

TOTAL EQUIPOS: 22

4.4.1 UPS 10 kVA

SEDE	POBLACIÓN Y/O CIUDAD	UBICACIÓN EN LA SEDE	CANTIDAD DE TOMACORRIENTES ASOCIADAS	MARCA	REFERENCIA UPS	NUMERO DE SERIE UPS
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 25	63	ABLEREX	KRONOS UL10D	TD8062B8B001
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 24	53	ABLEREX	KRONOS UL10D	TD7049D7F0002
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 3	53	ABLEREX	KRONOS UL10D	TD7049D7F0001
TERRITORIAL TOLIMA	IBAGUÉ	Centro de Cableado piso 5	39	ABLEREX	AB-MSIII10000	MA6133C9M0007
TERRITORIAL BOYACÁ	TUNJA	Centro de cableado sótano	27	ABLEREX	AB-MSIII10000	MA8007CAB0015
TERRITORIAL BOLÍVAR	CARTAGENA	Cuarto Técnico en el primer piso, debajo de las escaleras	54	ABLEREX	AB-MSIII10000	MA6133C9M0060
TERRITORIAL CALDAS	MANIZALES	Centro de cableado principal piso 3	44	ABLEREX	AB-MSIII10000	MA8007CAB0037
TERRITORIAL RISARALDA	PEREIRA	Centro de cableado piso 4 contiguo al auditorio	32	ABLEREX	AB-MSIII10000	MA6133C9M0043

Tabla 106 Inventario de UPS – 10kVA

4.4.2 UPS 15 kVA

Durante la implementación de la solución del servicio para el cliente Ministerio del Trabajo no se realiza instalación de UPS de 15kVA, el detalle de esto se entregó a la 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 107 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:
o 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.

El 16/09/2025 se realiza visita en DT Risaralda para revisión conjunta de UPS, donde se ejecutó la maniobra de reconexión de los barrajes de tierra del tablero de distribución regulado y de la transferencia manual bypass hacia la Puesta a Tierra (SPT) del edificio en el Piso 4, garantizando así la correcta derivación a tierra. Esto permitió que los voltajes flotantes en el neutro de salida del UPS desaparecieron, ya que al estar referenciado a tierra los potenciales residuales quedaron eliminados.

Se confirma que la UPS se encuentra operativa, sin novedades, no presenta daños físicos ni electrónicos, se adjunta el informe completo que comparte nuestro aliado y que describen las acciones implementadas.

- Medición de ANS Energía regulada

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

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

Tabla 108 Medición ANS Energía Eléctrica UPS

4.5 No aplica

4.6 Outsourcing de Impresión

El servicio de Outsourcing de impresión contempla los siguientes equipos distribuidos a nivel nacional para la prestación del servicio, así:

Referencia	Tipo	Cantidad
Ricoh IM430	Blanco y Negro	265
Ricoh IMC400F	Color	1

Tabla 109 Inventario de impresoras para el servicio

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

- Para el mes de septiembre, el responsable del servicio gestionó un total de 754 solicitudes escaladas a través de Aranda. Al corte del mes, 744 casos quedaron en estado Cerrado/Solucionado, 10 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 **srvscanner@mintrabajo.gov.co** para asegurar que se cuente con espacio disponible o generar la depuración correspondiente para evitar novedades en la prestación del servicio; actualmente se encuentra al 30% de la capacidad total del almacenamiento (capacidad total 100gb).
- El administrador del servicio de outsourcing de impresión remitió semanalmente vía correo electrónico al Coordinador del Grupo de Soporte Informático 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-154239; allí se relaciona el listado total de usuarios con el aprovisionamiento.
- El Coordinador del Grupo de Soporte Informático solicitó hacer entrega de dos cajas de resmas de tamaño carta en el piso 5 en el área de Talento Humano de Nivel Central para continuar con la copia y correspondiente archivo de los permisos sindicales
- El 12/09/2025 se habilita con el apoyo del soporte del piso y el administrador del servicio dejaron operativa la nueva impresora para el Grupo de Control Interno Disciplinario en el Piso 18. A continuación de relacionan los datos del equipo y registro fotográfico:

IP	Nombre	Serial	Ubicación	Estado	Fecha
172.23.37.5	RICOHPISO18ODC2	3353PA50157	Edificio Central kra 7 # 31-10 PISO18	Activa	12/09/2025



RE_ Asignacion Impresora .msg

- 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	3492
ricohpiso19a	Bogotá Sede central	pnustes	Patricia Celestial Nustes Barrera	3349
ricoh-ibague-radicacion	Ibagué	mnavarrog	Maria Alejandra Navarro Garcia	2821
ricoh-bmanga-ofc205	Bucaramanga	lberbeo	Laura Daniela Berbeo Ardila	2439
ricoh-cali-piso2-atc	Cali	gcolonia	Gustavo Adolfo Colonia Trochez	2352
ricoh-bmanga-ofc305	Bucaramanga	amateus	Andrea Johana Mateus Parra	2141
ricohcl32-rcc	Bogotá calle32	ncalderonp	Natalia Calderon Paez	2012
ricoh-cali-piso2-atc	Cali	mquinonesp	Mildreth Quinonez Peinado	1915
ricoh-cali-piso2-grcc	Cali	gvargas	Gloria Patricia Vargas	1881
ricoh-apartado-piso2-c	apartado	tllanes	Tatiana Llanes Ibarguen	1836

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

Clics septiembre.xlsx

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

Nombre de la impresora	Ubicación	Blanco y negro
ricohcl32-rcc	Bogotá calle32	13511
ricohpiso5a	Bogotá sede central	14128
ricohpiso10b	Bogotá sede central	11498
ricoh-bmanga-ofc205	Bucaramanga	12611
ricoh-cali-piso3	Cali	12700
ricohpiso19a	Bogotá sede central	11630
ricoh-cali-piso4	cali	15439
ricohpiso12a	Bogotá sede central	11287
ricohpiso9a	Bogotá sede central	9061
ricoh-medellin-piso3	Medellín	10707

Tabla 111Top 10 de impresoras con mayor uso

Impresoras mas usadas septiembre.x

- 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	1831
ricohpiso25c	Bogotá Sede central	ymedinag	Yeisson Medina Gonzalez	441
ricohpiso25c	Bogotá Sede central	bhernandez	Bibiana Hernandez Hernandez	18

ricohpiso25c	Bogotá Sede central	jrojas	Juanita Rojas Rodriguez	7

Tabla 112 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	Realizados Trabajos	Promedio de Páginas por trabajo
Centrales Dt	2297	119499	88998	32798	121796	33864	3,6
D. T. Valle Del Cauca	0	57817	42972	14845	57817	17361	3,3
D. T. Bogota	0	52272	35870	16402	52272	15044	3,5
D. T. Santander	0	40981	27476	13505	40981	12783	3,2
D. T. Antioquia	0	37998	28022	9976	37998	11369	3,3
D. T. Norte De Santander	0	16342	10120	6222	16342	5605	2,9
D. T. Tolima	0	16198	11554	4644	16198	4302	3,8
D. T. Risaralda	0	13860	9854	4006	13860	4957	2,8
D. T. Meta	0	13377	9498	3879	13377	4162	3,2
D. T. Huila	0	12245	8108	4137	12245	3898	3,1

Tabla 113 Top oficinas

Informe por oficinas septiembre.

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

Impresora	Ubicación	Copias
ricoh-medellin-piso1	Medellín	52.972
ricohcl32-gau-b	Bogotá cll32	52.626
ricohcl32-rcc	Bogotá cll32	45.742
ricohpiso5b	Bogotá sede central	39.794
ricoh-bmanga-ofc205	Bucaramanga	32.055
ricoh-cali-piso4	cali	29.700
ricohcl32-gau-a	Bogotá cll32	22.649
ricoh-bmanga-OFC305	Bucaramanga	20.660
ricoh-monteria-piso2	monteria	20.161
ricohpiso9a	Bogotá sede central	19.698

Tabla 114 Top 10 impresoras más usadas del servicio de fotocopiado

copias septiembre.xlsx

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

Nombre de Usuario	Nombre Completo	Transacción	Total Cuota asignada	Veces que se aumento
jzuluaga	Juan Felipe Zuluaga Malagon	ADJUST	1286	7
asanchez	Alfonso Sanchez Carrillo	ADJUST	1622	6
ebecerra	Eileen Becerra Gomez	ADJUST	1218	6
gvargas	Gloria Patricia Vargas	ADJUST	1788	6
mmorenoma	Maria Camila Moreno Mayuza	ADJUST	1870	6
mnavarrog	Maria Alejandra Navarro Garcia	ADJUST	2667	6
ncalderonp	Natalia Calderon Paez	ADJUST	4549	6
amateus	Andrea Johana Mateus Parra	ADJUST	2161	5
dpena	Diana Lorena Pena Baena	ADJUST	1227	5
fplata	Francisco Antonio Plata Jaimes	ADJUST	1163	5

Tabla 115 Ampliación de cuota de impresión



Asignacion de Saldo Septiembre.xl

- 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:

	jul-25		ago-25		sep-25	
	Resmas Carta	Resmas Oficio	Resmas Carta	Resmas Oficio	Resmas Carta	Resmas Oficio
Total Resmas	565	358	401	267	454	74
Total Cajas por Tamaño	56,5	35,8	40,1	26,7	45,4	7,4
Total Cajas Enviadas	**92,3**		**66,8**		**52,8**	

Tabla 116 Despacho de papel a sedes del Ministerio del Trabajo

Durante el período, se despacharon a sedes del ministerio un total de 16 tóners para impresora B/N, 3 unidades de tambor y 1 unidad fusora.

4.6.1 No aplica

4.6.2 Multifuncional B/N rango medio – Cargo fijo mensual

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

Tabla 117 Cargo mensual multifuncional rango medio

4.6.3 Impresora Color rango medio – Cargo fijo mensual

Descripción	Unidad	Cantidad
Impresora color rango medio - Cargo fijo mensual	Unidad-mes	1

Tabla 118 Cargo mensual impresora color

4.6.4 No aplica

4.6.5 Multifuncional B/N rango medio – Clic de impresión

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

MES	DETALLE	CANTIDAD
septiembre	Multifuncional blanco y negro rango medio - Clic de impresión tóner y papel carta	**571.449**
	TOTAL	**571.449**

Tabla 119 Clics de impresión de septiembre 2025 – Multifuncional B/N

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

Mes 2025	Julio	Agosto	Septiembre
Cantidad de clics consumidos	686.509	619.172	571.449

Tabla 120Tendencia 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 530.467 clics de impresión (esto incluye 6.390 de la impresora de contratos piso 8) y 40.982 de fotocopias para un total de 571.449 para este servicio, superando el estimado del mes por 121.449.

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 septiembre de 2025:

MES	DETALLE	CANTIDAD
Septiembre	Impresora color rango medio - Cargo fijo mensual - Clic de impresión tóner y papel carta	**2.297**
	TOTAL	**2.297**

Tabla 121 Clics de Impresión de septiembre 2025 – Impresora Color

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

Mes 2025	Julio	Agosto	Septiembre
Cantidad de clics consumidos	2.131	1.361	2.297

Tabla 122 Tendencia de consumo de clics color

El consumo mensual establecido para el servicio por la entidad es de 1.500 clics de impresión en color para el único equipo de este tipo ubicado en Nivel Central; para el período del informe se presentó un consumo de **2.297** clics para este servicio, superando el estimado del mes por 797.

- Medición de ANS Outsourcing de impresión

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

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

Tabla 123 Medición ANS Outsourcing de Impresión

4.7 Antivirus

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

4.7.1 Instalaciones de antivirus en servidores

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

En septiembre 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.

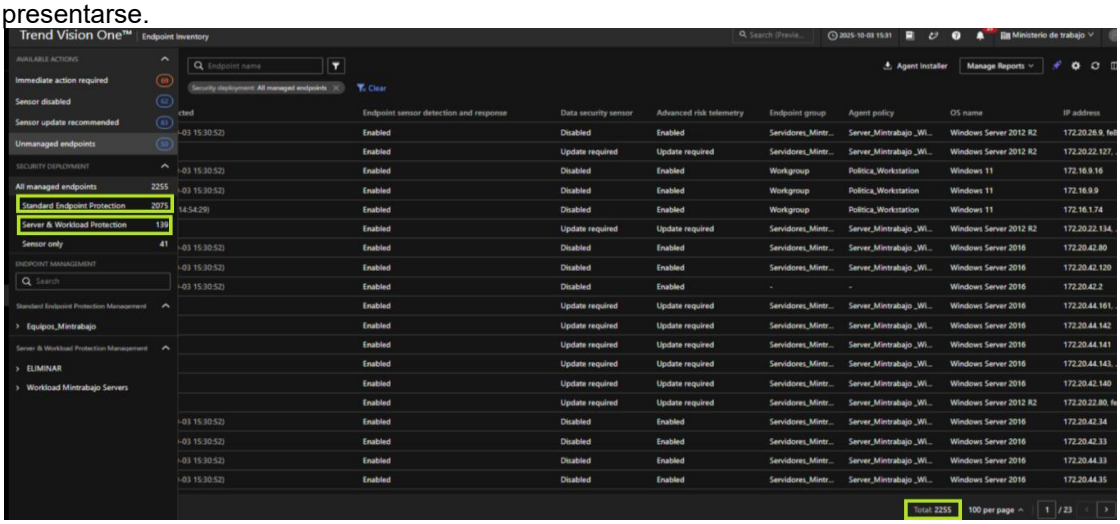


Ilustración 176 Equipos consola antivirus

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 2255 licencias, se tienen disponibles 92.

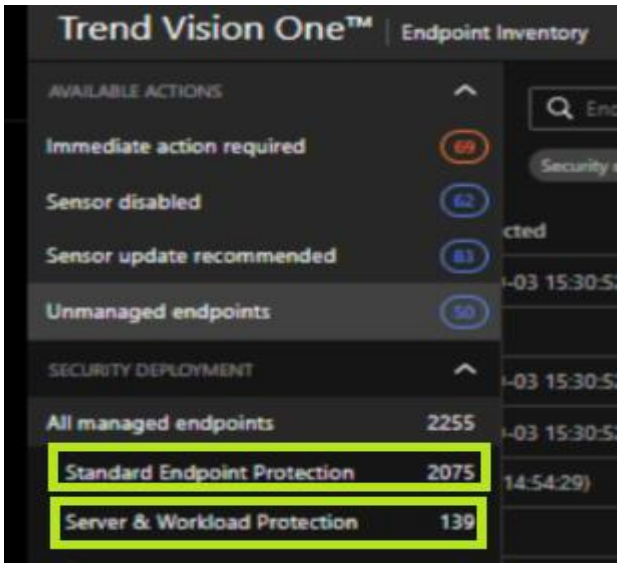


Ilustración 177 Gestión consola antivirus – equipos usuario final

4.7.3 Top 10 spyware

Durante el período 01/09/2025 al 01/10/2025, se registraron 13 detecciones de spyware y grayware en los equipos de escritorio del Ministerio de Trabajo.

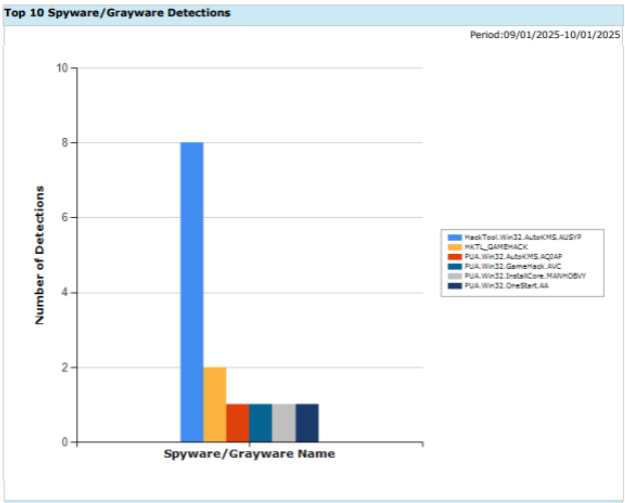
- El mayor número de casos corresponde a la herramienta HackTool.Win32.AutoKMS.AUSYP (8 detecciones), relacionada con el uso de software no licenciado o activadores de Windows.

- El resto de las detecciones corresponden a programas potencialmente no deseados (PUA) como GameHack, InstallCore y OneStart, de bajo impacto pero que representan riesgo por instalación de software no autorizado.

Conclusión

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

- 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.



Top 10 Spyware/Grayware Detections

Spyware/Grayware Name	# of Detections	Detected By
HackTool.Win32.AutoKMS.AUSYP	8	Desktop (8)
HKTL_GAMEHACK	2	Desktop (2)
PUA.Win32.AutoKMS.AQJAP	1	Desktop (1)
PUA.Win32.GameHack.AVC	1	Desktop (1)
PUA.Win32.InstallCore.MANHOBVY	1	Desktop (1)
PUA.Win32.OneStart.AA	1	Desktop (1)

Ilustración 178 Top spayware

4.7.4 Top 10 Virus Detectados

Durante el mes analizado, los eventos detectados por la plataforma TrendMicro se detectaron un total de 58 eventos, lo que permite evaluar el grado de riesgo asociado a cada actividad observada en los Endpoint

Análisis de los Datos:

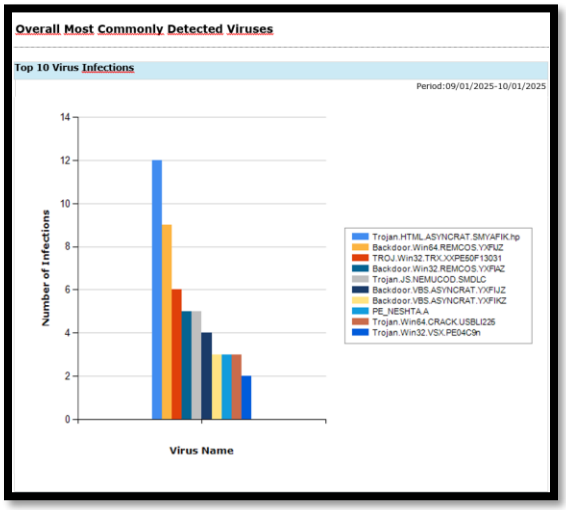


Ilustración 179 Top 10 virus detectado

Aspecto	Detalle	Interpretación / Riesgo
Trojan.HTML.ASYNCRAT.SMYAFIK.hp	12 infecciones detectadas	Troyano de acceso remoto (RAT) que permite el control total del equipo comprometido. Alta probabilidad de exfiltración de información y persistencia.
Backdoor.Win64.REMCOS.YXFJIZ	9 infecciones detectadas	Malware tipo Backdoor que permite el control remoto del sistema, ejecución de comandos y robo de información. Riesgo alto de persistencia.
TROJ.Win32.TRX.XXPE50F13031	6 infecciones detectadas	Troyano genérico con capacidad de descarga de payloads adicionales. Puede ser usado como vector de entrada para otros ataques.
Backdoor.Win32.REMCOS.YXFIAZ	5 infecciones detectadas	Variante de REMCOS RAT de 32 bits; se comunica con servidores C2 externos. Riesgo alto de robo de información.
Trojan.JS.NEMUCOD.SMDLC	5 infecciones detectadas	Troyano distribuido por correos con archivos JavaScript maliciosos. Puede descargar ransomware. Riesgo alto de cifrado de información.
Backdoor.VBS.ASYNCRAT.YXFJIZ	4 infecciones detectadas	Variante de AsyncRAT ejecutada mediante scripts VBS, orientada a control remoto y robo de credenciales.
Backdoor.VBS.ASYNCRAT.YXFIKZ	3 infecciones detectadas	Versión modificada del RAT anterior; busca evadir detección mediante cambios en el script.
PE_NESHITA.A	3 infecciones detectadas	Malware polimórfico que se oculta en procesos del sistema (stealth/rootkit). Riesgo crítico de persistencia.
Trojan.Win64.CRACK.USBLI225	3 infecciones detectadas	Troyano asociado al uso de software no licenciado; se propaga por USB.
Trojan.Win32.VSX.PE04C9n	2 infecciones detectadas	Troyano genérico con funciones de recopilación de datos. Riesgo medio.

Tabla 124 Descripción de virus

TOP 5 EQUIPOS

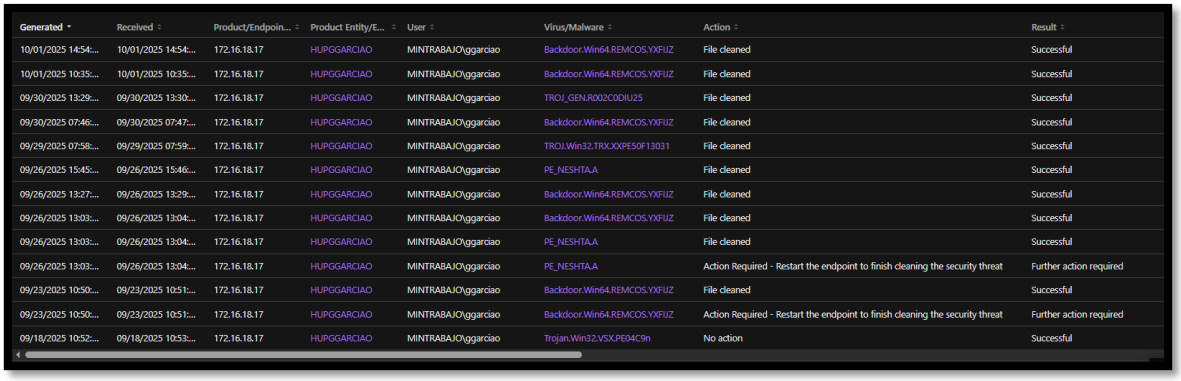
A continuación, se genera un top 5 de las amenazas durante el mes de septiembre 2025:

Product Entity/Endpoint	Virus/Malware
HUPGGARCIAO	Backdoor.Win64.REMCOS.YXFIJZ
BOPDZARATE	Trojan.HTML.ASYNCRAT.SMYAFIK.hp
CQDYMONTILLAG	Trojan.JS.NEMUCOD.SMDLC
BOPLSALAMANCAP	Backdoor.VBS.ASYNCRAT.YXFIJZ
CNDDQUEVEDO	Trojan.HTML.ASYNCRAT.SMYAFIK.hp

Tabla 125 Top 5 Equipos

HUPGGARCIAO
La detección en el equipo se debe por Backdoor.Win64.REMCOS.YXFIJZ. Este tipo de Malware que realiza actividades sin el conocimiento del usuario. Estas actividades suelen

incluir el establecimiento de conexiones de acceso remoto, la captura de entradas del teclado, la recopilación de información del sistema, la descarga y carga de archivos, la instalación de otro malware en el sistema infectado. Los archivos fueron limpiados por la solución TrendMicro. Sin embargo se requiere de la revisión del equipo por interacciones persistentes bloqueadas.

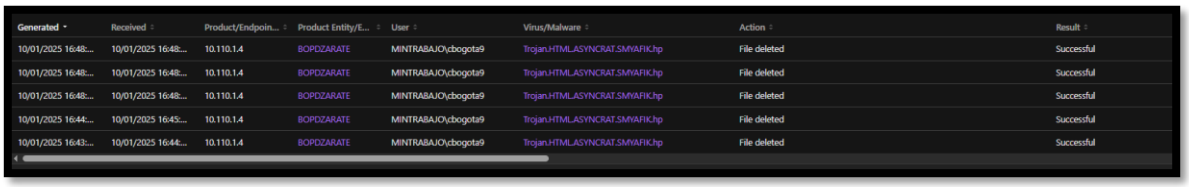


Generated	Received	Product/Endpoin...	Product Entity/E...	User	Virus/Malware	Action	Result
10/01/2025 14:54:...	10/01/2025 14:54:...	172.16.18.17	HUPGGARCIAO	MINTRABAJO\ggarciao	Backdoor.Win64.REMCOS.YXFIJZ	File cleaned	Successful
10/01/2025 10:35:...	10/01/2025 10:35:...	172.16.18.17	HUPGGARCIAO	MINTRABAJO\ggarciao	Backdoor.Win64.REMCOS.YXFIJZ	File cleaned	Successful
09/30/2025 13:29:...	09/30/2025 13:30:...	172.16.18.17	HUPGGARCIAO	MINTRABAJO\ggarciao	TROJ_GEN.R002C0DIU25	File cleaned	Successful
09/30/2025 07:46:...	09/30/2025 07:47:...	172.16.18.17	HUPGGARCIAO	MINTRABAJO\ggarciao	Backdoor.Win64.REMCOS.YXFIJZ	File cleaned	Successful
09/29/2025 07:58:...	09/29/2025 07:59:...	172.16.18.17	HUPGGARCIAO	MINTRABAJO\ggarciao	TROJ.Win32.TRX.XXPE50F13031	File cleaned	Successful
09/26/2025 15:45:...	09/26/2025 15:46:...	172.16.18.17	HUPGGARCIAO	MINTRABAJO\ggarciao	PE_NESHTA.A	File cleaned	Successful
09/26/2025 13:27:...	09/26/2025 13:29:...	172.16.18.17	HUPGGARCIAO	MINTRABAJO\ggarciao	Backdoor.Win64.REMCOS.YXFIJZ	File cleaned	Successful
09/26/2025 13:03:...	09/26/2025 13:04:...	172.16.18.17	HUPGGARCIAO	MINTRABAJO\ggarciao	Backdoor.Win64.REMCOS.YXFIJZ	File cleaned	Successful
09/26/2025 13:03:...	09/26/2025 13:04:...	172.16.18.17	HUPGGARCIAO	MINTRABAJO\ggarciao	PE_NESHTA.A	File cleaned	Successful
09/26/2025 13:03:...	09/26/2025 13:04:...	172.16.18.17	HUPGGARCIAO	MINTRABAJO\ggarciao	PE_NESHTA.A	Action Required - Restart the endpoint to finish cleaning the security threat	Further action required
09/23/2025 10:50:...	09/23/2025 10:51:...	172.16.18.17	HUPGGARCIAO	MINTRABAJO\ggarciao	Backdoor.Win64.REMCOS.YXFIJZ	File cleaned	Successful
09/23/2025 10:50:...	09/23/2025 10:51:...	172.16.18.17	HUPGGARCIAO	MINTRABAJO\ggarciao	Backdoor.Win64.REMCOS.YXFIJZ	Action Required - Restart the endpoint to finish cleaning the security threat	Further action required
09/18/2025 10:52:...	09/18/2025 10:53:...	172.16.18.17	HUPGGARCIAO	MINTRABAJO\ggarciao	Trojan.Win32.VSX.PE04C9n	No action	Successful

Ilustración 180 HUPGGARCIAO

BOPDZARATE

La detección en el equipo se debe por Trojan.HTML.ASYNCRAT.SMYAFIK.hp Un troyano es un tipo de malware que realiza actividades sin el conocimiento del usuario. Estas actividades suelen incluir el establecimiento de conexiones de acceso remoto, la captura de entradas del teclado, la recopilación de información del sistema, la descarga y carga de archivos, la instalación de otro malware en el sistema infectado, la realización de ataques de denegación de servicio (DDoS) y la ejecución o finalización de procesos, y en su totalidad los eventos fueron controlados por el antivirus

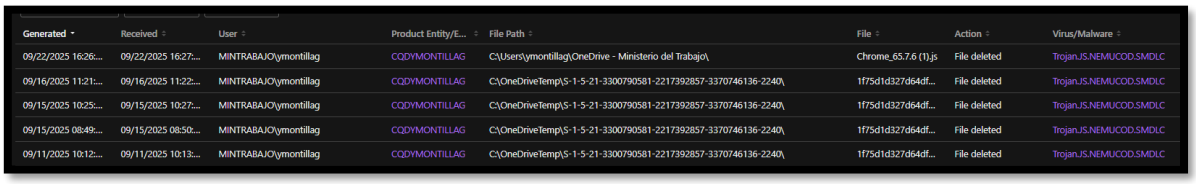


Generated	Received	Product/Endpoin...	Product Entity/E...	User	Virus/Malware	Action	Result
10/01/2025 16:48:...	10/01/2025 16:48:...	10.110.1.4	BOPDZARATE	MINTRABAJO\cbogota9	Trojan.HTML.ASYNCRAT.SMYAFIK.hp	File deleted	Successful
10/01/2025 16:48:...	10/01/2025 16:48:...	10.110.1.4	BOPDZARATE	MINTRABAJO\cbogota9	Trojan.HTML.ASYNCRAT.SMYAFIK.hp	File deleted	Successful
10/01/2025 16:48:...	10/01/2025 16:48:...	10.110.1.4	BOPDZARATE	MINTRABAJO\cbogota9	Trojan.HTML.ASYNCRAT.SMYAFIK.hp	File deleted	Successful
10/01/2025 16:44:...	10/01/2025 16:45:...	10.110.1.4	BOPDZARATE	MINTRABAJO\cbogota9	Trojan.HTML.ASYNCRAT.SMYAFIK.hp	File deleted	Successful
10/01/2025 16:43:...	10/01/2025 16:44:...	10.110.1.4	BOPDZARATE	MINTRABAJO\cbogota9	Trojan.HTML.ASYNCRAT.SMYAFIK.hp	File deleted	Successful

Ilustración 181 BOPDZARATE

CQDYMONTILLAG

La detección en el equipo se debe por Trojan.JS.NEMUCOD.SMDLC Un programa troyano es un malware que no puede propagarse automáticamente a otros sistemas. Los troyanos suelen descargarse de internet e instalarse por usuarios desprevenidos. En su totalidad los eventos fueron controlados por el antivirus

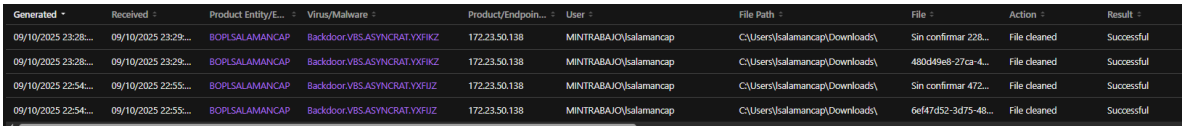


Generated	Received	User	Product Entity/E...	File Path	File	Action	Virus/Malware
09/22/2025 16:26:...	09/22/2025 16:27:...	MINTRABAJO\ymontillag	CQDYMONTILLAG	C:\Users\ymontillag\OneDrive - Ministerio del Trabajo\	Chrome_65.7.6 (1).js	File deleted	Trojan.JS.NEMUCOD.SMDLC
09/16/2025 11:21:...	09/16/2025 11:22:...	MINTRABAJO\ymontillag	CQDYMONTILLAG	C:\OneDriveTemp\S-1-5-21-3300790581-2217392857-3370746136-2240\	1f75d1d327d64df...	File deleted	Trojan.JS.NEMUCOD.SMDLC
09/15/2025 10:25:...	09/15/2025 10:27:...	MINTRABAJO\ymontillag	CQDYMONTILLAG	C:\OneDriveTemp\S-1-5-21-3300790581-2217392857-3370746136-2240\	1f75d1d327d64df...	File deleted	Trojan.JS.NEMUCOD.SMDLC
09/15/2025 08:49:...	09/15/2025 08:50:...	MINTRABAJO\ymontillag	CQDYMONTILLAG	C:\OneDriveTemp\S-1-5-21-3300790581-2217392857-3370746136-2240\	1f75d1d327d64df...	File deleted	Trojan.JS.NEMUCOD.SMDLC
09/11/2025 10:12:...	09/11/2025 10:13:...	MINTRABAJO\ymontillag	CQDYMONTILLAG	C:\OneDriveTemp\S-1-5-21-3300790581-2217392857-3370746136-2240\	1f75d1d327d64df...	File deleted	Trojan.JS.NEMUCOD.SMDLC

Ilustración 182 CQDYMONTILLAG

BOPLSALAMANCAP

La detección en el equipo se debe por Backdoor.VBS.ASYNCRAT.YXFIJZ Un programa de puerta trasera es un troyano diseñado específicamente para permitir que usuarios maliciosos manipulen remotamente los sistemas afectados. Como todos los troyanos, las puertas traseras no se propagan automáticamente. Son instaladas inadvertidamente por usuarios desprevenidos o intencionalmente por usuarios maliciosos. En su totalidad los eventos fueron controlados por el antivirus

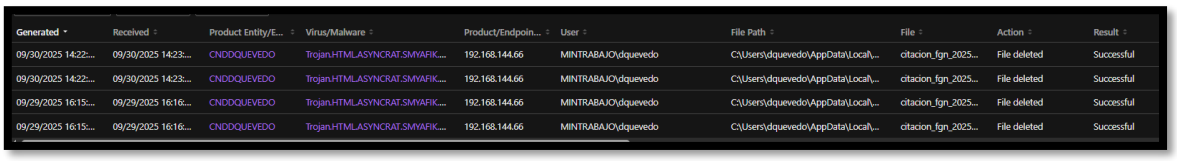


Generated	Received	Product Entity/E...	Virus/Malware	Product/Endpoin...	User	File Path	File	Action	Result
09/10/2025 23:28:...	09/10/2025 23:29:...	BOPLSALAMANCAP	Backdoor.VBS.ASYNCRAT.YXFIKZ	172.23.50.138	MINTRABAJO\lsalamancap	C:\Users\lsalamancap\Downloads\	Sin confirmar 228...	File cleaned	Successful
09/10/2025 23:28:...	09/10/2025 23:29:...	BOPLSALAMANCAP	Backdoor.VBS.ASYNCRAT.YXFIKZ	172.23.50.138	MINTRABAJO\lsalamancap	C:\Users\lsalamancap\Downloads\	480d49e8-27ca-4...	File cleaned	Successful
09/10/2025 22:54:...	09/10/2025 22:55:...	BOPLSALAMANCAP	Backdoor.VBS.ASYNCRAT.YXFIJZ	172.23.50.138	MINTRABAJO\lsalamancap	C:\Users\lsalamancap\Downloads\	Sin confirmar 472...	File cleaned	Successful
09/10/2025 22:54:...	09/10/2025 22:55:...	BOPLSALAMANCAP	Backdoor.VBS.ASYNCRAT.YXFIJZ	172.23.50.138	MINTRABAJO\lsalamancap	C:\Users\lsalamancap\Downloads\	6ef47d52-3d75-48...	File cleaned	Successful

Ilustración 183 BOPLSALAMANCAP

CNDDQUEVEDO

La detección en el equipo se debe por Trojan.HTML.ASYNCRAT.SMYAFIK.hp Un programa de puerta trasera es un troyano diseñado específicamente para permitir que usuarios maliciosos manipulen remotamente los sistemas afectados. Como todos los troyanos, las puertas traseras no se propagan automáticamente. Son instaladas inadvertidamente por usuarios desprevenidos o intencionalmente por usuarios maliciosos. En su totalidad los eventos fueron controlados por el antivirus



Generated	Received	Product Entity/E...	Virus/Malware	Product/Endpoin...	User	File Path	File	Action	Result
09/30/2025 14:22:...	09/30/2025 14:23:...	CNDDQUEVEDO	Trojan.HTML.ASYNCRAT.SMYAFIK....	192.168.144.66	MINTRABAJO\dquevedo	C:\Users\dquevedo\AppData\Local\...	citacion_fgn_2025...	File deleted	Successful
09/30/2025 14:22:...	09/30/2025 14:23:...	CNDDQUEVEDO	Trojan.HTML.ASYNCRAT.SMYAFIK....	192.168.144.66	MINTRABAJO\dquevedo	C:\Users\dquevedo\AppData\Local\...	citacion_fgn_2025...	File deleted	Successful
09/29/2025 16:15:...	09/29/2025 16:16:...	CNDDQUEVEDO	Trojan.HTML.ASYNCRAT.SMYAFIK....	192.168.144.66	MINTRABAJO\dquevedo	C:\Users\dquevedo\AppData\Local\...	citacion_fgn_2025...	File deleted	Successful
09/29/2025 16:15:...	09/29/2025 16:16:...	CNDDQUEVEDO	Trojan.HTML.ASYNCRAT.SMYAFIK....	192.168.144.66	MINTRABAJO\dquevedo	C:\Users\dquevedo\AppData\Local\...	citacion_fgn_2025...	File deleted	Successful

Ilustración 184 CNDDQUEVEDO

Eventos Ransomware

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

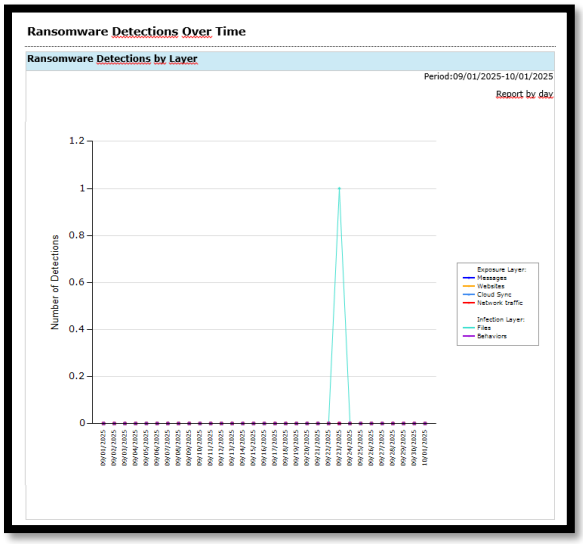


Ilustración 185 Eventos Ransomware

En el mes de septiembre 2025, se presentaron eventos escalados por detección de malware Ransomware, estas detenciones se realizaron en su gran mayoría en la carpeta C:\Users\ggarciao\AppData\Roaming\BELLOS_Persistent.exe las detecciones realizadas en su totalidad fueron controladas por la solución y enviadas a cuarentena. Se solicita como método de prevención validar el equipo de ggarcia hostname HUPGGARCIAO el cual se encuentra aislado de la red por riesgo de detección de familiar de malwares Remcos.

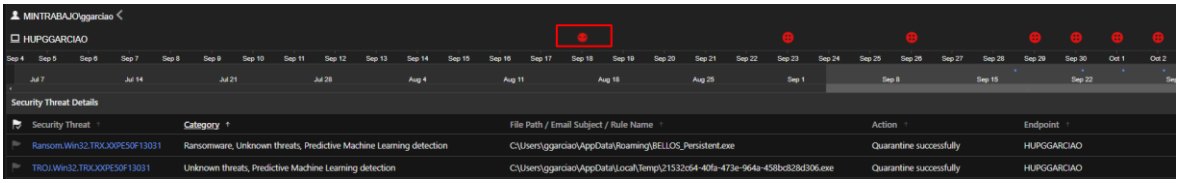


Ilustración 186 captura eventos ransonware

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

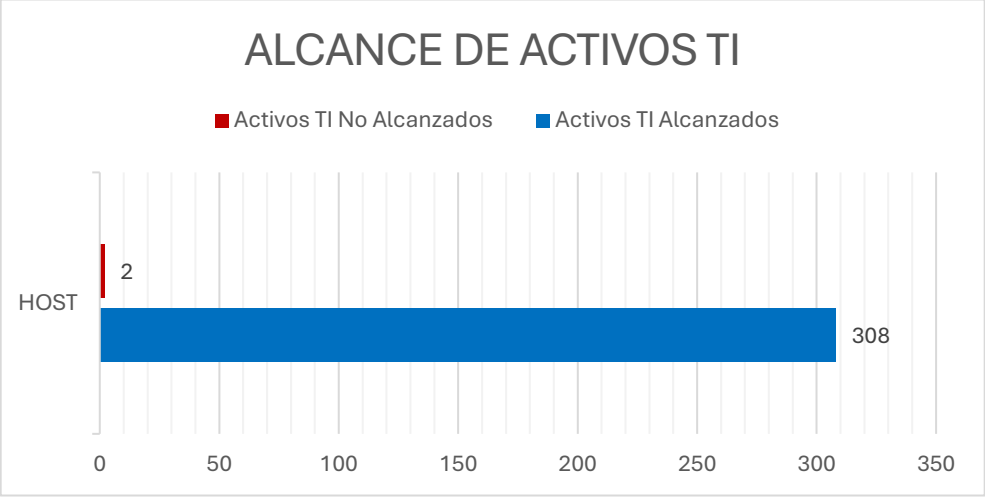


Ilustración 187 *Gestión consola Nessus*

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
2025 SEMANAL II - WINDOWS DESKTOP	Vulnerability	Weekly on Sat at 12:30 AM	September 27 at 1:04 ...
2025 SEMANAL II - NETWORKING	Vulnerability	Weekly on Sat at 8:00 PM	September 27 at 8:36 ...
2025 SEMANAL II - FORTISIEM	Vulnerability	Weekly on Sat at 9:00 PM	September 27 at 9:37 ...
2025 SEMANAL II - VMWARE	Vulnerability	Weekly on Sat at 10:00 PM	September 27 at 10:12...
2025 SEMANAL II - LINUX	Vulnerability	Weekly on Sat at 11:00 PM	September 27 at 11:46...
2025 SEMANAL II - NO AUTH	Vulnerability	Weekly on Sun at 3:30 AM	September 28 at 3:40 ...
2025 SEMANAL II - WINDOWS SERVER	Vulnerability	Weekly on Sun at 9:00 PM	September 29 at 12:40...

Ilustración 188 *Escaneos programados*

- Clasificación de Prioridad de Vulnerabilidad por Instancias Totales (VPR)

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

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

4.7.5.3 TOP 10 – Vulnerabilidades más explotables

Al cierre de septiembre del 2025, el activo TI con la mayor cantidad de vulnerabilidades identificadas corresponde al host (172.20.44.101), con un total de 96 hallazgos, corresponde a un servidor Microsoft Windows Server 2019 Standard Build 17763 y la mayoría de las vulnerabilidades están asociadas a actualizaciones de seguridad para la librería Apache Log4j.

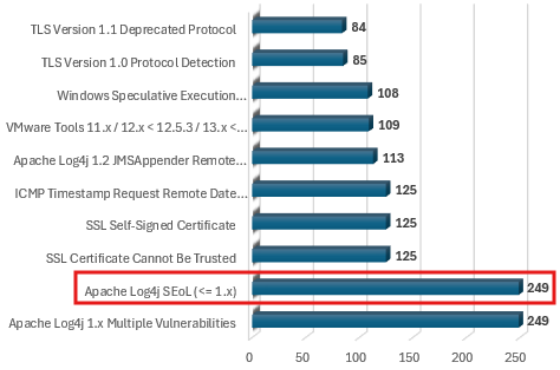


Ilustración 189 TOP 10 - Activos más explotables

Al cierre de septiembre 2025, la vulnerabilidad más crítica identificada corresponde a “Docker Desktop < 4.44.3 Container Escape”, con un total de 4 hallazgos, corresponde a una actualización de seguridad para el software Docker Desktop, publicada en agosto del

2025 y que mitiga el CVE-2025-9074 que permite la ejecución de comandos privilegiados a través del Docker Engine API.

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 septiembre del 2025, se remediaron un total de 114 vulnerabilidades, de las cuales, 20 fueron de severidad crítica, 39 de severidad alta, 53 de severidad media y 2 de severidad baja. Por otro lado, con relación a indicadores semestrales, se gestionaron un total de 1.164 vulnerabilidades TI, de las cuales, 250 fueron de severidad crítica, 143 de severidad alta, 457 de severidad media y 314 de severidad baja.

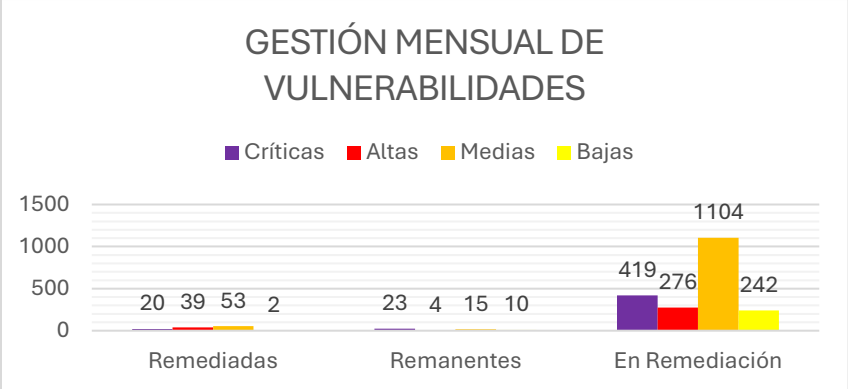


Ilustración 190 Vulnerabilidades gestionadas vs en remediación

Anexo Vulnerabilidades

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

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

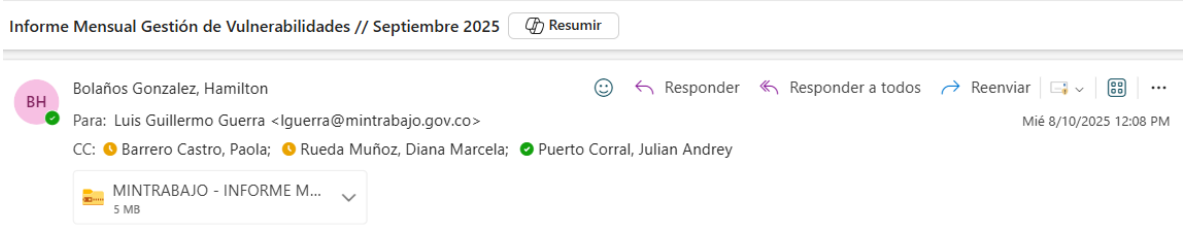


Ilustración 191 captura envío de correo gestión de vulnerabilidades

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	**100%**	08/27/2025	5
Presentación de Resultados	Riesgo bajo	Daniel Castillo	**100%**	09/03/2025	5

Ilustración 192 Cronograma Ethical Hacking

Se dio por terminado con la documentación necesaria para la entrega formal de la actividad, es decir, el informe técnico, el informe gerencial y la matriz de hallazgos, se envío correo con los hallazgos.

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	95,85%	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 126 Medición de ANS Antivirus

5 GESTIÓN DE CALIDAD DE INFORMACIÓN

Este apartado tiene el propósito de brindar la información de las evaluaciones de la calidad documental de los casos y la calidad de las llamadas realizadas al personal de Mesa de Servicios, Soporte en Sitio y Especialistas, con el propósito de identificar acciones de mejora en la prestación de los servicios:

- Calidad documental de Casos: Realizando la revisión y cumplimiento de los criterios definidos en la calidad documental de los casos registrados en la herramienta de gestión.
- Calidad de Llamadas: Realizando la revisión y cumplimiento de los criterios definidos en los casos atendidos por el centro de servicio por medio de llamadas telefónicas.

A continuación, se detalla la metodología utilizada para la realización de las evaluaciones:

5.1 Evaluación calidad documental de casos

En Septiembre, se realizó la evaluación cuantitativa de la muestra de 233 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	2	99,91%
2. Asunto	0	100,00%
3. Descripción	0	100,00%
4. Prioridad	0	100,00%
5. Categoría	6	99,74%
6. Escalamiento	0	100,00%
7. Solución	6	99,74%
8. Estado del Caso	2	99,91%
9. Justificación Estado del Caso	3	99,87%
10. Periodicidad de seguimientos	3	99,87%

11. Descripción de seguimientos	4	99,83%
12. Ortografía y redacción	10	99,57%
13. Cumplimiento de ANS	2	99,91%

Tabla 127 Errores cometidos

Se identificaron 38 errores con un porcentaje de cumplimiento consolidado de 98,37%.
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 10 novedades de ortografia y redacción, 4 novedades por CI y 6 novedades por categoria y solución

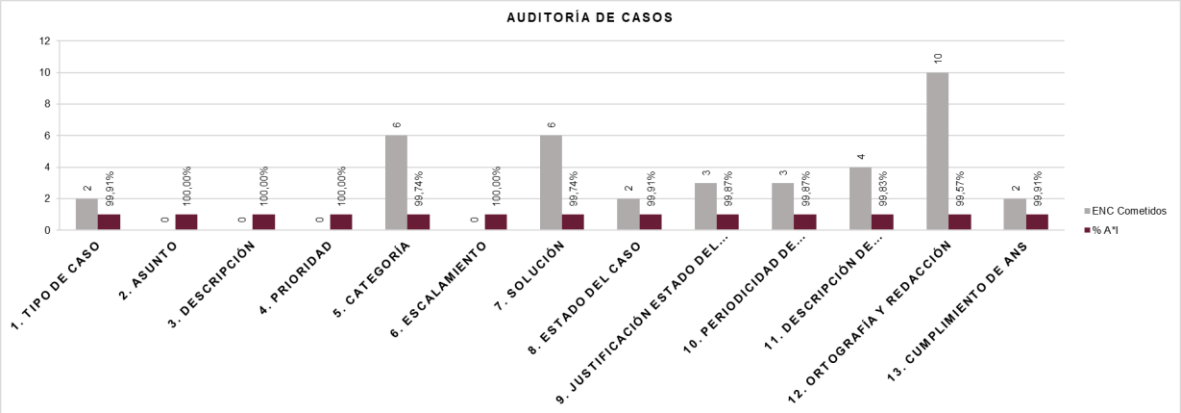


Ilustración 193 Resultados auditoria de casos

5.2 Evaluación de calidad de llamadas

En el mes de septiembre 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:

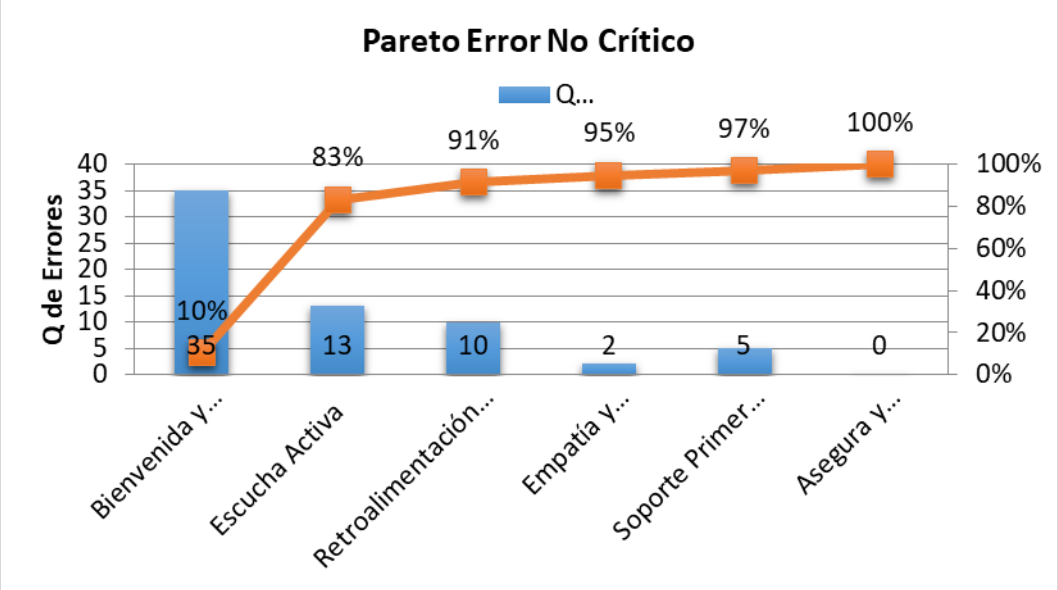
	ENC		
#	Practica medida	Q errores	Frec
1	Bienvenida y Personalización	35	10%
2	Escucha Activa	13	83%
3	Retroalimentación y manejo de esperas	10	91%
4	Empatía y adaptabilidad al usuario	2	95%
5	Soporte Primer Nivel	5	97%
6	Asegura y Despedida	0	100%

	EC		
#	Practica medida	Q errores	Frec
1	Atiende con respeto al usuario	14	100%
2	Cumplimiento de políticas	2	100%
3	No corta el llamado	1	90%

4	**Resuelve el requerimiento del usuario de forma integral**	**0**	**100%**
5	**Uso correcto Herramienta de registro**	**1**	**90%**

Tabla 128 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 llamadas evaluadas de las cuales se evidencia las siguientes afectaciones en el resultado global por categoría:



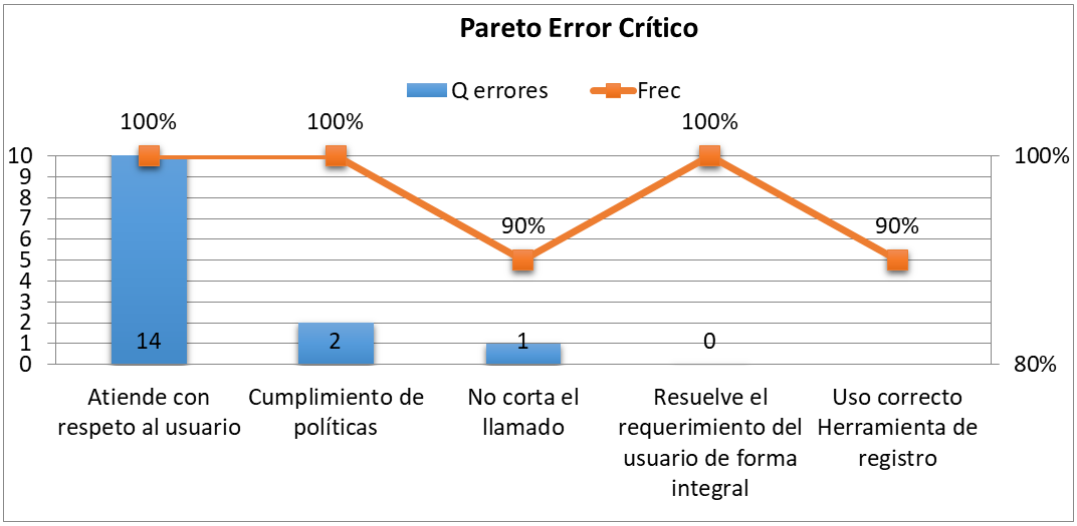


Ilustración 194 Resultado de criterios y parámetros - Calidad de llamadas

5.3 Práctica de Mejora

Dar a conocer las actividades de la Práctica de Mejora Continua correspondientes al periodo del 1 al 30 de septiembre de 2025. Este apartado contiene información relevante sobre las acciones de mejora identificadas por los Servicios TIC durante el 2025.

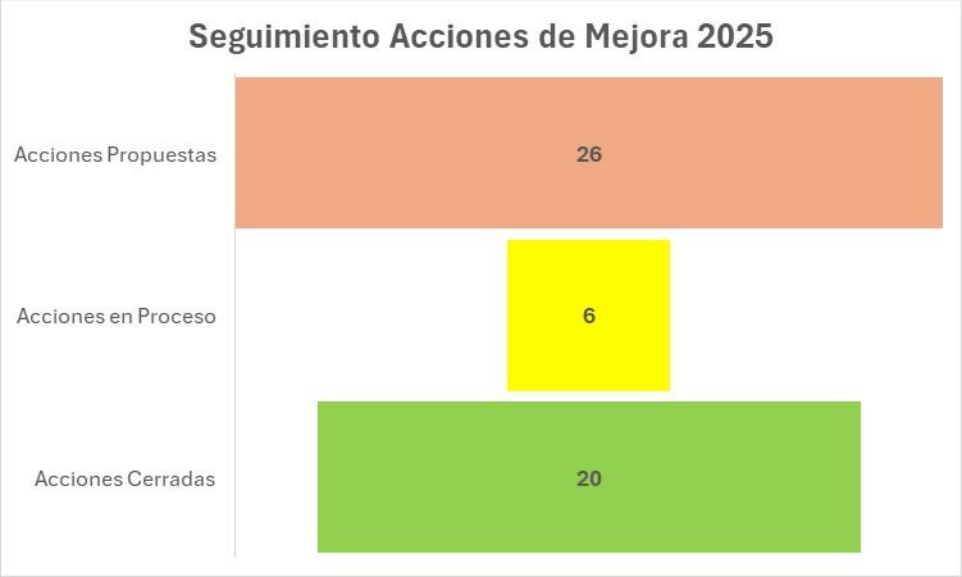


Ilustración 195 Seguimiento Práctica Mejora

En el anterior 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.

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 129 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:

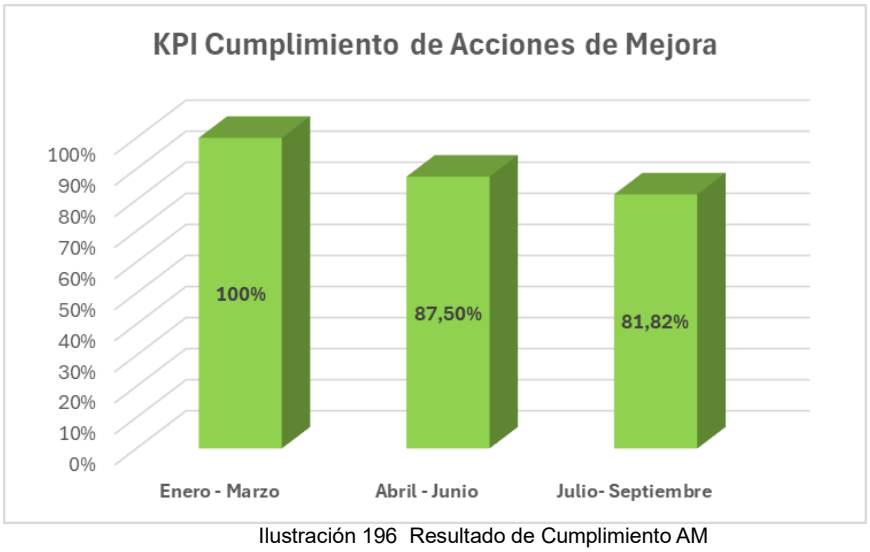


Ilustración 196 Resultado de Cumplimiento AM

Se evidencia el cumplimiento para el periodo de Julio a septiembre del 81,82% en efectividad de las 11 acciones de mejoras propuestas fueron 9 acciones ejecutadas y cerradas durante este periodo y cumplieron con las evidencias de cierre, las 3 acciones pendiente de fin de ejecución, se encuentra previstas para cierre durante el 4 trimestre del 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.c o	NO	El correo electrónico institucional ha estado disponible
Mesa de servicios	Imposibilidad de contacto por la línea telefónica de la mesa de servicios	Falla en el ingreso de las llamadas a la mesa de servicios	NO	La línea telefónica ha estado disponible
Mesa de servicios	Desborde de solicitudes (vía correo electrónico y/o llamadas) en la Mesa de Servicios	Aumento eventual de la cantidad de solicitudes que supera la capacidad de atención de los Agentes de la Mesa de servicios	NO	No se ha presentado desborde de solicitudes
Mesa de servicios	Riesgo de seguridad de la información que comprometan la confidencialidad, integridad o disponibilidad de la información.	Posibilidad de uso indebido de la cuenta genérica del cliente, asignada para la Mesa de servicios	NO	No se ha presentado dicha situación.
Soporte en sitio	Incumplimiento de los compromisos pactados por atención de actividades urgentes - no planeadas	Solicitud de realización de actividades urgentes no planeadas que afectan la prestación del servicio de acuerdo con lo planeado	NO	No se ha presentado dicha situación.
Todas las prácticas	Deficiencias en la adopción de las prácticas de ITIL	Resistencia a la adopción de las prácticas de ITIL por las partes interesadas	NO	Se proporcionó capacitación a los involucrados
Práctica de Activos	Posibilidad de pérdida de inventario	La pérdida de inventario se produce cuando las cantidades reales del inventario son inferiores a las registradas en el módulo de gestión	NO	Se realizó seguimiento con el equipo de trabajo para revisar los compromisos de la práctica
Todos	Ausencia del personal asignado	Ausencia del personal, encargado de gestionar, administrar y operar los servicios.	NO	El personal asignado estuvo disponible durante el periodo.
Todos	Indisponibilidad de la nube privada que afecte la prestación de servicios de TI	Falla en la prestación de los servicios de TI por falla en la infraestructura de TI provista por la UT	NO	Se dispuso de la infraestructura y recursos que soportan las estrategias de contingencia y recuperación. El suministro del servicio de energía eléctrica fue normal en los sitios alternos. Se realización copias de respaldo de las bases de datos, información y sistemas de información se realiza de acuerdo con la política institucional de copias de respaldo.
Todos	Pérdida de información	Falla en la generación de las copias de respaldo de la información centralizada	NO	Se realizan pruebas de restauración de backups generados por la herramienta definida para el proyecto

Todos	Pérdida de disponibilidad	Perdida de disponibilidad de la infraestructura que soporta los servicios y activos de información de TI	NO	No se ha presentado dicha situación.
Todos	Pérdida de integridad	La ausencia de actualizaciones de seguridad en las aplicaciones podría poner en riesgo la integridad y disponibilidad de los sistemas, permitiendo la ejecución de código malicioso.	NO	Se realizó la planeación del primer ejercicio de Ethical Hacking. Se ejecutaron de manera oportuna y permanente las actualizaciones y controles necesarios para remediar las vulnerabilidades detectadas durante las pruebas de seguridad.
DRP	Indisponibilidad de servicios de TI	Indisponibilidad de la Infraestructura principal alojada en Datacenter Cirion Colombia XV	NO	Se dispuso de la infraestructura y recursos que soportan las estrategias de contingencia y recuperación. El suministro del servicio de energía eléctrica fue normal en los sitios alternos. Se realización de copias de respaldo de las bases de datos, información y sistemas de información se realiza de acuerdo con la política institucional de copias de respaldo.
Servicios centrales Servicios en sede	Fallas en los servicios de TI que afecten las actividades de la entidad producto realizar cambios no programados	Presentación de incidentes en la infraestructura tecnológica	NO	Se cuenta con los procedimientos y documentación de la práctica para que los cambios se registren y ejecuten adecuadamente
SD -WAN	Falla en la infraestructura del servicio instalada en DC	Falla de uno o varios equipos que se encuentran provistos en el DC	NO	No se ha presentado dicha situación Se está trabajando en el cronograma de pruebas de disponibilidad de los diferentes servicios
LAN /WLAN	Falla en Switch Core / switch de borde	Indisponibilidad del servicio de conectividad por falla del switch core	NO	El servicio de conectividad ha estado disponible
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 130 Gestión de riesgos

7 BOLSA DE RECURSOS

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

Descripción	Cantidad	Precio total antes de IVA
Switch de acceso 48 puertos	8	$3.949.912
Clics adicionales blanco y negro	121.449	$17.002.860
Clics adicionales color	797	$458.275
	Subtotal	$21.411.047

Tabla 131 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	99,33%	95,00%
	Tiempo de solución de incidentes por soporte en sitio	100,00%	90,00%
	Tiempo de solución de requerimientos por soporte en sitio	99,79%	90,00%
	Tiempo de respuesta de la mesa de servicio	100,00%	85,00%
	Abandono de llamadas	0,70%	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	95,83%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
ANTIVIRUS	Cobertura de antivirus	95,85%	95,00%
	Continuidad y disponibilidad de la plataforma	100,00%	98,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
LAN y WLAN	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Energía Regulada	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Datacenter	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Continuidad y disponibilidad del datacenter principal	100,00%	99.95%
	Continuidad y disponibilidad del datacenter alterno	100,00%	99,60%
	Continuidad y disponibilidad de la plataforma de procesamiento, almacenamiento y respaldo	99,99%	99,70%
	Tiempo de solución de incidentes asociado a los servicios de aplicaciones especializadas	97,93%	90,00%
	Tiempo de solución de requerimientos asociado a los servicios de aplicaciones especializadas	100,00%	90,00%
	Continuidad y disponibilidad de los servicios de directorio activo	100,00%	99,60%
	Continuidad y disponibilidad de los servicios de seguridad informática	100,00%	99,90%
	Tiempo de solución de incidentes asociado a los servicios de administración, soporte y monitoreo	99,09%	90,00%
	Tiempo de solución de requerimientos asociado a los servicios de administración, soporte y monitoreo	99,72%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Nube pública	Continuidad y disponibilidad de la nube pública	100,00%	99,90%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Outsourcing de impresión	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Telefonía IP	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Continuidad y disponibilidad de los servicios de telefonía IP	99,96%	99,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Conectividad WAN e Internet	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Continuidad y disponibilidad del servicio de WAN en sedes nacionales con un solo enlace	(*)	99,60%
	Continuidad y disponibilidad del servicio de WAN en sedes nacionales con doble enlace (principal MPLS + secundario Internet dedicado)	(*)	99,90%
	Continuidad y disponibilidad del servicio de internet en Datacenter principal	100,00%	99,95%
	Continuidad y disponibilidad del servicio de internet en Datacenter alterno	100,00%	99,70%
	Continuidad y disponibilidad del servicio de WAN en Datacenter principal	100,00%	99,95%
	Continuidad y disponibilidad del servicio de WAN en Datacenter alterno	100,00%	99,95%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 132 Medición de Acuerdos de Niveles de Servicio septiembre 2025

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

Cumplimiento en la entrega del informe de gestión mensual para todos los servicios Meta de cumplimiento del indicador del 100%, se entrega el informe a la Supervisión del Contrato y Coordinador del Grupo de Soporte Informático dentro del tiempo comprometido.

9 ANEXOS

- Certificación_backup_servidores
- Consumo de cuotas septiembre
- detalle_llamadas_recibidas_(01.09.2025-30.09.2025)
- Datos_Mintrabajo_septiembre

FIN DEL DOCUMENTO