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

Noviembre de 2025

DOCUMENTO/ ARCHIVO	
Código:	**Informe Gestión - Unión Temporal Gestión TIC 2023**
Nombre Archivo:	**Informe Gestión - Unión Temporal Gestión TIC 2023 – Noviembre 2025**
Fecha:	9/12/2025
Versión:	1

REGISTRO DE CAMBIOS			
Versión	**Páginas**	**Fecha Modificación**	**Motivo del cambio**
1	211	9/12/2025	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 10
Objetivo 10
Alcance 10
Definición de Siglas y Expresiones Técnicas 11
1 GERENCIA Y/O ADMINISTRACIÓN 12
2 LÍNEA DE GESTIÓN DE SERVICIOS 12
2.1. Gestión del Servicio 12
2.1.2. Prácticas ITIL 4 19
2.1.2.1. Práctica Acuerdos Niveles de Servicio (ANS) 19
2.1.2.2. Práctica Habilitación de Cambios 20
2.1.2.3. Práctica Gestión de Activos 21
2.1.2.4. Práctica Catálogo de servicios 22
2.1.2.5. Práctica de Problemas 24
2.1.2.6. Práctica de Incidentes 25
2.1.2.7. Práctica de Requerimientos 30
2.1.2.8. Práctica de Eventos 35
2.1.2.9. Práctica de Disponibilidad 50
2.1.2.10. Práctica de Implementación 52
2.2 Mesa de Servicios y Soporte en Sitio 53
3 LINEA DE SERVICIOS CENTRALES 66
3.1 Datacenter Principal 66
3.1.1 Datacenter Alterno y DRP 76
3.1.2 Procesamiento, Almacenamiento y Respaldo 81
3.1.3 Aplicaciones Especializadas 86
3.1.4 No aplica 133
3.1.5 Seguridad Informática 133
3.1.5.1 Firewalls de nueva generación 133
3.1.5.2 Sandbox – Amenazas día 0 139
3.1.5.3 SIEM - Solución de correlación de eventos de seguridad, disponibilidad y recursos 142
3.1.5.4 WAF - Servicio de tipo “Firewall de Aplicaciones Web” 148
3.1.5.5 Solución de Anti-DDoS 149
3.1.5.6 Casos atendidos de los servicios de seguridad 150
3.1.5.7 Análisis de riesgo 152
3.1.5.8 Políticas y procedimiento de seguridad 153
3.1.6 Licenciamiento 154
3.1.7 Administración, soporte y monitoreo 154
3.2 No aplica 156
3.3 Conectividad WAN, SDWAN e Internet 156
3.3.1 Canales WAN 156
3.3.1.1 Incidentes de Conectividad 157
3.3.1.2 Topología Actual 159
3.3.2 Canales SDWAN e Internet Dedicado 159
4 LINEA DE SERVICIOS EN SEDE 164
4.1 Equipos de Cómputo de usuario final 164
4.1.1 Equipos de Escritorio 168
4.1.2 Equipos Portátiles 168
4.2 Conectividad LAN y WLAN 170
4.2.1 Switch CORE Sede Principal 171
4.2.2 Switch para conexiones perimetrales (EDGE) en sede principal 171

4.2.3 Switch de acceso 24 puertos 171
4.2.4 Switch de acceso 48 puertos 172
4.2.5 Puntos de Acceso 173
4.3 Telefonía IP 174
4.3.1 Teléfono Gama Media 174
4.3.2 Teléfono Gama Baja 174
4.3.3 Troncales SIP 175
4.3.4 No Aplica 175
4.3.5 No Aplica 175
4.3.6 Módems 4G – Con plan de 50 Gbps 175
4.4 Energía Regulada UPS 181
4.4.1 UPS 10 kVA 181
4.4.2 UPS 15 kVA 182
4.4.3 UPS 20 kVA 182
4.5 No aplica 184
4.6 Outsourcing de Impresión 184
4.6.1 No aplica 188
4.6.2 Multifuncional B/N rango medio – Cargo fijo mensual 189
4.6.3 Impresora Color rango medio – Cargo fijo mensual 189
4.6.4 No aplica 189
4.6.5 Multifuncional B/N rango medio – Clic de impresión 189
4.6.6 Impresora Color rango medio – Clic de impresión 189
4.7 Antivirus 190
4.7.1 Instalaciones de antivirus en servidores 190
4.7.2 Instalación de antivirus PCs usuarios final 191
4.7.3 Top 10 Virus Detectados 192
4.7.4 Servicio de Vulnerabilidades 198
4.7.4.1 Inventario y licenciamiento 198
4.7.4.2 Escaneos programados 199
4.7.4.3 TOP 10 – Vulnerabilidades más explotables 200
4.7.4.4 Estrategia de remediación y/o mitigación 200
4.7.4.5 Resumen de mitigación efectuada 201
4.7.4.6 Prueba de Vulnerabilidades Semestre II 2025 202
5 GESTIÓN DE CALIDAD DE INFORMACIÓN 203
5.1 Evaluación calidad documental de casos 203
5.2 Evaluación de calidad de llamadas 204
5.3 Práctica de Mejora 205
6 GESTION DE RIESGOS 206
7 BOLSA DE RECURSOS 209
8 MEDICIÓN DE ACUERDOS DE NIVEL DE SERVICIO 209
9 ANEXOS 211

Índice de Tablas

Tabla 1 Atención de solicitudes por Grupo de Especialista 19
Tabla 2 Tipificación de los cambios 20
Tabla 3 Medición Indicador Porcentaje de Cambios Exitosos 21
Tabla 4 KPI Práctica Catálogo de Servicios 24
Tabla 5 Consolidado problemas identificados 24
Tabla 6 Estados Incidentes 25
Tabla 7 Top 10 Incidentes 26
Tabla 8 Incidentes Suspendidos 26
Tabla 9 Incidentes Mayores 29

Tabla 10 Medición de KPIs 29
Tabla 11 Estados de Requerimientos 31
Tabla 12 Seguimiento del Backlog Suspendidos 31
Tabla 13 Top 10 de Solicitudes 32
Tabla 14 Detalle de KIP Practica de Requerimientos 32
Tabla 15 Casos reabiertos 35
Tabla 16 KPI Práctica de Eventos 36
Tabla 17 Consolidado disponibilidad de servidores 50
Tabla 18 Consolidado disponibilidad de Directorio Activo 50
Tabla 19 Desagregado de Disponibilidad Directorio Activo 50
Tabla 20 Consolidado disponibilidad de equipos Datacenter principal 50
Tabla 21 Desagregado de Disponibilidad Datacenter Principal 51
Tabla 22 Consolidado disponibilidad de equipos Datacenter alterno 51
Tabla 23 Desagregado Disponibilidad de equipos Datacenter alterno 51
Tabla 24 Consolidado disponibilidad de equipos redes y conectividad 51
Tabla 25 Consolidado disponibilidad de equipos de seguridad 51
Tabla 26 Disponibilidad de equipos Seguridad de la Información 51
Tabla 27 Consolidado disponibilidad de equipos de telefonía 52
Tabla 28 Consolidado disponibilidad de plataforma antivirus 52
Tabla 29 Llamadas Atendida por la Mesa de Servicio 53
Tabla 30 Casos anulados por Servicio 54
Tabla 31 Casos Suspendidos por Servicio 55
Tabla 32 Requerimientos Solucionados por Soporte en Sitio 56
Tabla 33 Requerimientos Solucionados por Territoriales 56
Tabla 34 Casos Cerrados por la Mesa de Servicios 58
Tabla 35 Casos Cerrados por Soporte en Sitio 60
Tabla 36 Top 10 Casos Cerrados por Soportes Territoriales 61
Tabla 37 Casos Atendidos usuarios VIPs 62
Tabla 38 Casos Atendidos usuarios 62
Tabla 39 Medios de Ingreso de Casos 63
Tabla 40 Visitas a Sedes sin Soporte 65
Tabla 41 Medición de ANS Mesa de servicios 66
Tabla 42 Capacidades contractuales 69
Tabla 43 Capacidades contractuales 69
Tabla 44 Consumo de capacidad con servidores para desaprovisionar + ambientes de pruebas) 69
Tabla 45 Consumo de capacidad Sin servidores para desaprovisionar con ambientes de pruebas 69
Tabla 46 Consumo de capacidad Sin servidores para desaprovisionar sin ambientes de pruebas 69
Tabla 47 Consumo de capacidad Servidores Pruebas y Desarrollo 70
Tabla 48 Consumo de capacidad actual 70
Tabla 49 Suma Instancias 107
Tabla 50 Total Docs 108
Tabla 51 Total Radicados 108
Tabla 52 Dimensionamiento Servers IBM - Virtualización Optima 109
Tabla 53 Apps & DDBB Oracle 111
Tabla 54 Escenario de Capacidades Oracle - Estado de consumo Actual 112
Tabla 55 Escenario de Capacidades Oracle - Total de recursos empleados 112
Tabla 56 Tendencia de uso de ancho de banda 134
Tabla 57 usuarios con mayor consumo de ancho de banda 135
Tabla 58 Top de usuarios por sesiones 136
Tabla 59 Top de aplicaciones 137
Tabla 60 Consolidado de indicadores 139
Tabla 61 Tipos de incidentes 146
Tabla 62 Reporte de requerimientos noviembre 152
Tabla 63 Vulnerabilidades en la infraestructura 152
Tabla 64 Vulnerabilidades en la infraestructura 152
Tabla 65 ataques de phishing 152
Tabla 66 Licenciamiento 154
Tabla 67 Medición ANS Datacenter 156
Tabla 68 Medición ANS Nube Pública 156
Tabla 69 Incidentes de conectividad 158
Tabla 70 Medición de ANS Conectividad WAN e Internet 162
Tabla 71 Desagregado sedes con novedad un solo enlace 164
Tabla 72 Desagregado sedes con novedad con doble enlace 164

Tabla 73 Cantidades de equipos a distribuir a nivel nacional 165
Tabla 74 Cantidades de equipos asignados nivel nacional 165
Tabla 75 Cantidades de equipos por devolución nivel nacional 165
Tabla 76 Estado de casos de garantía. 165
Tabla 77 ANS casos de garantía 166
Tabla 78 ANS Relación casos de garantía 166
Tabla 79 Equipos en siniestro 167
Tabla 80 *Parque Computacional Instalado* 168
Tabla 81 Devolución de equipos 168
Tabla 82 cantidad de equipos 168
Tabla 83 Solicitudes de Equipos Usuario Final – Según Grupo Responsable 169
Tabla 84 Solicitudes de Equipos Usuario Final – Según Grupo Responsable 169
Tabla 85 Medición ANS Equipos de Usuario Final 169
Tabla 86 Top 5 de categorías en el Servicio de conectividad LAN-WLAN 171
Tabla 87 Distribución y Cantidades de switch 24 puertos 172
Tabla 88 Distribución y Cantidades de Switch 48 puertos 172
Tabla 89 Distribución de puntos de acceso 173
Tabla 90 Medición ANS LAN y WLAN 174
Tabla 91 Equipos gama media 174
Tabla 92 Sedes cerradas 175
Tabla 93 Consolidado de teléfonos gama baja 175
Tabla 94 Consolidado equipos MIFI 175
Tabla 95 Minutos, consumos 177
Tabla 96 Top 5 consumo de llamadas 178
Tabla 97 Top 5 llamadas LDI 178
Tabla 98 Top 5 llamadas Celular 179
Tabla 99 Top 5 llamadas locales 180
Tabla 100 Medición ANS Telefonía IP 181
Tabla 101 Inventario de UPS – 10kVA 182
Tabla 102 Inventario de UPS – 20Kva 183
Tabla 103 Medición ANS Energía Eléctrica UPS 184
Tabla 104 Inventario de impresoras para el servicio 185
Tabla 105 Consumo de impresiones por usuario - Impresoras B/N 186
Tabla 106Top 10 de impresoras con mayor uso 186
Tabla 107 Top usuarios impresión a color 187
Tabla 108 Top oficinas 187
Tabla 109 Top 10 impresoras más usadas del servicio de fotocopiado 187
Tabla 110 Ampliación de cuota de impresión 188
Tabla 111 Despacho de papel a sedes del Ministerio del Trabajo 188
Tabla 112 Cargo mensual multifuncional rango medio 189
Tabla 113 Cargo mensual impresora color 189
Tabla 114 Clics de impresión de noviembre 2025 – Multifuncional B/N 189
Tabla 115 Tendencia de consumo de clics B/N 189
Tabla 116 Clics de Impresión de noviembre 2025 – Impresora Color 190
Tabla 117 Tendencia de consumo de clics color 190
Tabla 118 Medición ANS Outsourcing de Impresión 190
Tabla 119 Descripción de virus 193
Tabla 120 *Top 5 Equipos* 194
Tabla 121 Medición de ANS Antivirus 203
Tabla 122 Errores cometidos 204
Tabla 123 Resultado de criterios y parámetros - Calidad de llamadas 205
Tabla 124 KPI Practica de Mejora 205
Tabla 125 Gestión de riesgos 208
Tabla 126 Bolsa de Recursos 209
Tabla 127 Medición de Acuerdos de Niveles de Servicio noviembre 2025 211

Índice de Ilustraciones

Ilustración 1 Estado final de casos al corte del período 18
Ilustración 2 asignación grupo resolutor 22
Ilustración 3 creación categoría incidente mayor 23
Ilustración 4 Actualización usuarios VIP 23
Ilustración 5 Efectividad de resolución de incidentes 29
Ilustración 6 Porcentaje de incidentes abiertos 30

Ilustración 7 KPI Efectividad de Resolución de Requerimientos de Servicio....33
Ilustración 8 Requerimientos de Reabiertos en el periodo....33
Ilustración 9 Top de incidentes por sedes....37
Ilustración 10 Top de incidentes por sedes....38
Ilustración 11 eventos por sedes routers....39
Ilustración 12 Top de causas por sedes switches....39
Ilustración 13 Top de eventos por sedes Access Point....40
Ilustración 14 15Top de causas por sedes Access point....41
Ilustración 16 Top de eventos por sedes Starlink....42
Ilustración 17 Top de causas por sedes Starlink....43
Ilustración 18 Top de incidentes por sedes fortigate....44
Ilustración 19 Top de causas por sedes fortigate....45
Ilustración 20 Top de eventos Windows....46
Ilustración 21 Top de servidores Windows....47
Ilustración 22 Top de causas eventos linux....47
Ilustración 23 Top de servidores linux....48
Ilustración 24 Seguimiento Pruebas de Disponibilidad....52
Ilustración 25 Seguimiento Práctica Implementación....53
Ilustración 26 Llamadas Atendidas....54
Ilustración 27 Requerimientos Solucionados por Soporte en Sitio....56
Ilustración 28 Requerimientos Solucionados por Territoriales....57
Ilustración 29 Requerimientos Solucionados por Territoriales....58
Ilustración 30 Casos Cerrados por Soporte en Sitio....60
Ilustración 31 Casos Cerrados por Territoriales....62
Ilustración 32 *Medio de ingreso solicitudes*....63
Ilustración 33 Cumplimiento WSUS....67
Ilustración 34 Casos Win Servicio....68
Ilustración 35 Estado final de los casos Windows....68
Ilustración 36 Azure Migrate....73
Ilustración 37 Comportamiento SWCORE Datacenter Colombia XV....75
Ilustración 38 Sincronización HA de los Switch Core....75
Ilustración 39 Grafica de consumo canal Internet Datacenter....76
Ilustración 40 Captura de imagen máquinas virtuales....76
Ilustración 41 Escenario de pruebas Aplicaciones y AD....77
Ilustración 42 Extremo DC Bogotá....78
Ilustración 43 Extremo DC Cali....78
Ilustración 44 Estado canal de Internet DC Cali....79
Ilustración 45 Estado SWCORE Datacenter alterno....79
Ilustración 46 Estado HA SWCORE Datacenter alterno....80
Ilustración 47 Consumo canal MPLS DC Alterno....80
Ilustración 48 Estado Router MPLS DC Alterno....81
Ilustración 49 Casos App Servicio....88
Ilustración 50 Casos App Categoría....88
Ilustración 51 Tamaño Archivo Sindical....90
Ilustración 52 Tamaño IIS....90
Ilustración 53 Casos IBM Servicio....99
Ilustración 54 Casos IBM - categoría....99
Ilustración 55 Diagrama BP....102
Ilustración 56 Diagrama ODM....102
Ilustración 57 Diagrama WASND....103
Ilustración 58 Diagrama FileNet Front....103
Ilustración 59 Diagrama Datacap....104
Ilustración 60 Diagrama App Connect....104
Ilustración 61 Arquitectura Gestor Documental....105
Ilustración 62 Capacidades VM Gestor Documental....105
Ilustración 63 Licenciamiento Oracle....106
Ilustración 64 IBM Licenciamiento....107
Ilustración 65 Estado Bases de Datos....110
Ilustración 66 Información base de datos – Servidor....112
Ilustración 67 Estadísticas CPU....112
Ilustración 68 Estadísticas Memoria....113
Ilustración 69 Estadísticas Pool compartido....113
Ilustración 70 Tamaño DDBB....113

Ilustración 71 Tamaño Esquema DDBB....113
Ilustración 72 Rendimiento DDBB....114
Ilustración 73 DDBB por Server....114
Ilustración 74 Host e Instancia CPU....114
Ilustración 75 Estadísticas Memoria....115
Ilustración 76 Estadística Shared Pool....115
Ilustración 77 Tamaño DDBB DBMINTRA....115
Ilustración 78 Tamaño Esquema DDBB....115
Ilustración 79 Rendimiento DDBB MINTRASG....116
Ilustración 80 Información DDBB PLIFERAY....116
Ilustración 81 Host e Instancia CPU....116
Ilustración 82 Estadísticas Memoria....117
Ilustración 83 Estadísticas Shared Pool....117
Ilustración 84 Tamaño DDBB PLifeRay....117
Ilustración 85 Tamaño Esquemas DDBB....117
Ilustración 86 Rendimiento DDBB PlifeRay....118
Ilustración 87 Información DDBB SIGEP....118
Ilustración 88 Estadística Host e Instancia....118
Ilustración 89 Estadística Memoria....119
Ilustración 90 Estadística Shared Pool....119
Ilustración 91 Tamaño DDBB SIGEP....119
Ilustración 92 Tamaño Esquema DDBB....119
Ilustración 93 Rendimiento DDBB SIGEP....120
Ilustración 94 Información DDBB DBSIMPC....120
Ilustración 95 Estadística CPU....120
Ilustración 96 Estadística Memoria....121
Ilustración 97 Estadística Shared Pool....121
Ilustración 98 Tamaño DDBB SIMPC....121
Ilustración 99 Tamaño Esquema DDBB....121
Ilustración 100 Rendimiento DDBB....122
Ilustración 101 Información servidor DBBB....122
Ilustración 102 Host e Instancia CPU....122
Ilustración 103 Estadística memoria....123
Ilustración 104 Estadística Shared Pool....123
Ilustración 105 Tamaño DDBB MINTRASD....123
Ilustración 106 Tamaño Esquemas....123
Ilustración 107 Rendimiento MINTRASD....124
Ilustración 108 Información Server DDBB....124
Ilustración 109 Host e Instancia CPU....125
Ilustración 110 Estadística Memoria....125
Ilustración 111 Estadística Shared Pool....125
Ilustración 112 Tamaño DDBB....125
Ilustración 113 Tamaño DDBB....126
Ilustración 114 Rendimiento DDBB....126
Ilustración 115 Información Server DDBB....127
Ilustración 116 Host e Instancia CPU....127
Ilustración 117 Estadística Memoria....127
Ilustración 118 Estadística Shared Pool....128
Ilustración 119 Tamaño DDBB....128
Ilustración 120 Tamaño Esquemas DDBB....128
Ilustración 121 Rendimiento DDBB....129
Ilustración 122 Información Server DDBB....129
Ilustración 123 Estadística CPU....129
Ilustración 124 Estadística Memoria....130
Ilustración 125 Estadística Shared Pool....130
Ilustración 126 Tamaño Esquemas DDBB....130
Ilustración 127 Comportamiento DDBB....131
Ilustración 128 Almacenamiento ASM....131
Ilustración 129 DiskGroup Data....132
Ilustración 130 DiskGroup Flash....132
Ilustración 131 DiskGroup Reco....132
Ilustración 132 DiskGroup Redo....132
Ilustración 133 Licenciamiento adicional componente IBM....133

Ilustración *134* Firewall de nueva generación. 133
Ilustración 135 Comportamiento ancho de banda....134
Ilustración 136 Tendencia de uso de ancho de banda....135
Ilustración 137 Top de usuarios por números de sesiones 136
Ilustración 138 Top de aplicaciones 137
Ilustración 139 Top de Autenticación 138
Ilustración 140 sesiones fallidas....139
Ilustración 141 Reporte mensual noviembre 140
Ilustración 142 Captura de pantalla perfomance....141
Ilustración 143 licencia sandbox....141
Ilustración 144 licencia sandbox....142
Ilustración 145 Detalle de latencia o errores 143
Ilustración 146 detalle de problemas en servicios....143
Ilustración 147 Detalle casos de uso....144
Ilustración 148 Detalle de alertas 144
Ilustración 149 Detalle de alertas 145
Ilustración 150 Detalle de incidentes....145
Ilustración 151 Detalle servidores 147
Ilustración 152 Detalle fortigate....147
Ilustración 153 Top attack types....148
Ilustración 154 Top de ataques....149
Ilustración 155 Consumo canal MPLS DC Principal....156
Ilustración 156 Estado Router MPLS DC Principal....157
Ilustración 157 Topología actualizada....159
Ilustración 158 Interface Fortimanager....160
Ilustración 159 Interface MPLS HUB SDWAN....160
Ilustración 160 Interface Internet HUB SDWAN 160
Ilustración 161 VPN SDWAN establecidas....161
Ilustración 162 Estado HUB SDWAN Datacenter....161
Ilustración 163 Estado HA HUB Sdwan....161
Ilustración 164 Recursos Fortimanager....162
Ilustración 165 Estado de casos Redes y Conectividad 171
Ilustración 166 Asignación de licencias....176
Ilustración 167 Comportamiento de tráfico 177
Ilustración 168 Top llamadas nacionales....177
Ilustración 169 llamada internacional de prueba 178
Ilustración 170 Top Celular 179
Ilustración 171 Top Local 179
Ilustración 172 Requerimientos por garantía....180
Ilustración 173 Disponibilidad y Continuidad TOIP....181
Ilustración 174 Equipos consola antivirus....191
Ilustración 175 Gestión consola antivirus – equipos usuario final....191
Ilustración 176 Top 10 virus detectado....192
Ilustración 177 HUPGGARCIAO 195
Ilustración 178 BOPDZARATE....195
Ilustración *179 CQDYMONTILLAG* 196
Ilustración 180 BOPLSALAMANCAP....196
Ilustración 181 CNDDQUEVEDO....197
Ilustración 182 Eventos Ransomware....197
Ilustración 183 captura eventos ransonware....198
Ilustración 184 *Gestión consola Nessus*....199
Ilustración 185 *Escaneos programados* 199
Ilustración 186 TOP 10 - Activos más explotables 200
Ilustración 187 Vulnerabilidades gestionadas vs en remediación....201
Ilustración 188 captura envío de correo gestión de vulnerabilidades 202
Ilustración 189 Cronograma Ethical Hacking....202
Ilustración 190 Resultados auditoria de casos 204
Ilustración 191 Seguimiento Práctica Mejora 205
Ilustración 192 Resultado de Cumplimiento AM....206

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 noviembre 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:

Se realiza apoyo a la operación de los servicios con la elaboración y posterior envío de diferentes comunicados y divulgación de información a través de la cuenta de Soporte MT, los comunicados se orientaron a:

- **Incidentes mayores e intermitencias** presentadas en la operación de los servicios y/o aplicaciones.
- **Ventanas de mantenimiento programadas** sobre la infraestructura tecnológica y/o aplicaciones avaladas bajo los lineamientos de la práctica de habilitación de cambios: Bases de datos del Gestor Documental, Conectividad de red, Servidores de Bases de Datos (Archivo sindical, Cobro coactivo, Fivicot, Moodle, Rutraport, Siriti, SISGestion, Suite Vision Empresarial - SVE), SIRITI, BBDD SISINFO, Aplicativo SICIP, Microsoft Fabric (tableros de control), Mantenimiento eléctrico en Nivel Central por trabajos preventivos en UPS, Portal WEB.
- Aspectos claves para **creación de contraseñas seguras** de acceso a la red, los sistemas de información y aplicaciones; así mismo, se recuerda que no se deben almacenar contraseñas en navegadores de equipos de cómputo por seguridad de la información y para evitar el bloqueo de usuarios en el dominio por políticas internas.



¡INFORMACIÓN
IMPORTANTE CONTR

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



¡INFORMACIÓN
IMPORTANTE USO DE

- Promoción del **diligenciamiento de la encuesta de satisfacción de los servicios de tecnologías de la información**, se brindan indicaciones de como diligenciarla.



¡INFORMACIÓN
IMPORTANTE ENCUE

- Divulgación del instructivo de **activación y uso del Agente Virtual Teams Aranda** que permite a los usuarios tener un canal adicional para crear, consultar y verificar información de los casos que solicitan a la Mesa de Servicios del Grupo de Soporte Informático.



¡INFORMACIÓN
IMPORTANTE AGENT

- Divulgación del instructivo de **uso del Portal de Autogestión de Aranda** que permite a los usuarios tener un canal adicional para crear, consultar y verificar información de los casos que solicitan a la Mesa de Servicios del Grupo de Soporte Informático.



¡INFORMACIÓN
IMPORTANTE PORTA

- El 4/11/2025 se brinda apoyo a la Oficina TICs en la divulgación de mensaje a través de Soporte MT relacionado con el **lineamiento de bloqueo de puertos USB en los equipos institucionales** con el fin de mitigar los riesgos de fuga de información y accesos no autorizados. Se especifica la manera de gestionar las exclusiones a través de la Mesa de Servicios. El mensaje se ha replicado de forma periódica según la instrucción.



¡INFORMACIÓN
IMPORTANTE BLOQU

- El 01/11/2025, 04/11/2025 y 5/11/2025 se informa a los usuarios de Nivel Central y la DT Bogotá la mejora relacionada con la **actualización de la interfaz de usuario de las impresoras Ricoh**, se da instrucción del código de acceso y los manuales para hacer uso de los servicios de la impresora. Posterior a esto se remitieron mensajes según la actualización que se realizó en las Direcciones Territoriales.





¡INFORMACIÓN
IMPORTANTE MEJOR
¡INFORMACIÓN
IMPORTANTE VENTA
¡INFORMACIÓN
IMPORTANTE VENTA

- Lineamientos para la **instalación automática de actualizaciones de Windows** en los equipos de cómputo corporativos.



¡INFORMACIÓN
IMPORTANTE INSTAL

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



¡INFORMACIÓN
IMPORTANTE NOVED

b. Traslados y novedades de sedes:

- **Anserma / Caldas:** Por remodelación física de la alcaldía del municipio, la sede fue trasladada temporalmente el 8/03/2025 a un local cercano 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:** La sede estaba cerrada y apagada desde el 27/06/2025 ya que el inspector se retiró por pensión; el 18/11/2025 se posesiona nuevo funcionario para la inspección.
- **Santafe de Antioquia / Antioquia:** Se recibe notificación por parte del Coordinador del Grupo de Soporte Informático de la reubicación del inspector de trabajo LUIS ANIBAL MENDOZA SIERRA a la IT Santafe de Antioquia a través de la resolución 2288. Se adelantan las siguientes acciones por parte de la UT:
    - Se solicita gestionar con el soporte de la DT la actualización de actas de equipo de cómputo considerando que el usuario se desplazará con el equipo portátil que tiene asignado en la DT.
    - Se realiza el envío de un firewall Fortigate FG-40F con su respectivo cargador a la DT para tenerlo disponible una vez el usuario se traslade.
    - El equipo de redes confirma que el enlace de ETB de la sede está activo, el día de la apertura con el apoyo del técnico se revisaran todos los temas de conectividad.
    - El teléfono IP que era de esa inspección fue movido a la DT Antioquia por un usuario el año pasado, en ese sentido, se solicitó gestionar con el soporte que se realice la entrega de un teléfono para que sea movido y ubicado en la inspección.
    - La impresora Ricoh que siempre ha estado en la inspección tiene serial 3353PA50542, una vez se coordine el técnico para el 1/12/2025 se realizará la puesta en operación. El suministro de papel de impresión para la apertura ya se tiene disponible en la DT.

- **Segovia / Antioquia:** Informan que se hizo traslado de la inspección de trabajo el 23/10/2025 y por un tiempo de 6 meses aproximadamente, mientras se efectúan las reparaciones locativas en las instalaciones de la Casa de Justicia (lugar donde está ubicada la inspección). Estaremos atentos al retorno para verificar la conexión adecuada de elementos y operación normal de la inspección.



Traslado temporal IT SEGOVIA.msg

- **DT Vaupés / Mitú:** El 13/11/2025 sin previa notificación, se realiza el acompañamiento por parte de la UT Gestión TIC 2023 para el traslado de sede de la DT Vaupes a una nueva ubicación. Se gestiona disponibilidad de recurso técnico para brindar el acompañamiento, desinstalación de antena Starlink, desconexión de equipos de comunicaciones, embalaje de equipos de usuario final.

  El 18/11/2025 se coordina recurso técnico para la instalación de la antena Starlink para brindar conectividad, y debido a que la sede no cuenta con cableado estructurado, el coordinador del Grupo de Soporte Informático solicita realizar validación y cotización de instalación de puntos de red con canaleta plástica no certificados a los puntos de red de usuario final.
  Se incluye correo con las actividades realizadas por parte de la UT: Instalación de equipos en puestos de trabajo, instalación de antena Starlink en el predio, conexión de firewall y switch a la Starlink para conectividad LAN, conexión de dos equipos de cómputo a la red con cableado provisional, conexión de la impresora Ricoh al server.



RE_ Permisos de acceso Mitu - Instalaci

- **Cañas Gordas / Antioquia:** El 15/10/2025 por temas de salud, la funcionaria Marisol Palacios y por aproximadamente por tres (3) meses, fue trasladada temporalmente a trabajar en la DT Antioquia, por lo que la inspección está cerrada sin atención a público.

- **El Doncello / Caquetá:** Se deja en mantenimiento en Zabbix la sede ya que el funcionario asignado estará de permiso y vacaciones desde el 28/11/2025 y hasta el 2/02/2026, deja equipos apagados.

c. **Plan de trabajo documentos SIG para publicación en la SVE:** Durante el período, el equipo de procesos trabajó en la actualización la documentación de las prácticas en la plantilla dada por la Oficina Asesora de Planeación (OAP) para su estandarización. Se remite paquete al Coordinador del Grupo de Soporte informático, quien a su vez el 25/11/2025 envía paquete de documentos de las practicas ITIL a la OAP solicitando validación, codificación y publicación en la SVE. A espera de respuesta de dicha dependencia.



RV_ Plan de trabajo documentos SIG Acue

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

e. **Implementación IPV6:** Durante el periodo, LACNIC confirmó recepción de los documentos del Secretario General, pidió un documento formal que lo faculte como Ordenador del Gasto en el ministerio. Posterior a esto se recibe aval de la documentación, se pide y se genera link de actualización de pagos del pool y se gestiona lo correspondiente por parte de la UT.

El 27/11/2025 se recibe el pool asignado por LACNIC para el Ministerio del Trabajo, se tiene en proceso por parte del equipo la actualización del plan de trabajo de implementación.


Designacao do Bloco 2801_15_400___48.m


RE_ Re__## 192603 IPv6 EU - Ministe

El 11/11/2025 se remite información a la Oficina TICs sobre el estado de la implementación de IPV6 en el MinTrabajo, lo anterior para que la entidad cuente con la información requerida para presentarse en los retos de máxima velocidad que organiza el MinTIC.


RE_ Solicitud información IPV6 para


RE_ Solicitud información IPV6 para

f. **Otras actividades**

- El Coordinador del Grupo de Soporte Informático indica que la **Encuesta de percepción del personal de Soporte en Sitio Territorial** se puede remitir desde la cuenta de correo de Soporte MT. Durante el período se envió el comunicado a los Directores Territoriales, al cierre del periodo solo se han recibido 8 de 30 respuestas. Se continuará enviando el comunicado hasta obtener una muestra mayor.

- El 11/11/2025 **se solventa la novedad del punto de red con falla del Access Point de Popayán**, luego de las reiteradas novedades de desconexión del AP de Popayán y en vista que la entidad no cuenta con presupuesto para hacer la revisión del cableado estructurado del punto, se gestiona por parte de la UT el desplazamiento de un recurso para realizar la reubicación del AP, se asume el costo del acondicionamiento del punto de red con canaleta e instalación del AP, logrando dar solución a los inconvenientes que se tenían con el equipo, los dos Access Point dispuestos en la sede se dejaron operativos. Se notifica al coordinador del Grupo de Soporte Informático mediante correo electrónico:


RE_ Solicitud Revisión y Certificació

- El 06/11/2025 se realiza **revisión** conjunta con el equipo de procesos, el Coordinador de MDS y SS Bogotá el ***documento Lineamiento Específico Gestión de Cuentas de Usuario y Cuentas Especiales*** **emitido por la Oficina TICs**, debido a que se tenían varias actividades que no se encontraban definidas en cuanto a roles y entregables por parte de la UT y del Grupo de Soporte Informático,

se remite vía correo electrónico las observaciones correspondientes con el propósito sean revisadas, definidas y ajustadas por parte de la Oficina TICs. A espera de recibir el documento ajustado.



RE_ Lineamiento
Gestión de Usuarios V

- El 11/11/2025 se realiza **revisión** conjunta con el equipo de procesos del documento ***ODI POLÍTICA DE GESTION DE INCIDENTES DE SEGURIDAD y ODI PROCEDIMIENTO GESTION DE INCIDENTES*** **emitido por la Oficina TICs**, debido a que se tenían varias actividades que no se encontraban definidas en cuanto a roles y entregables por parte de la UT y del Grupo de Soporte Informático, se remite vía correo electrónico las observaciones correspondientes con el propósito sean revisadas, definidas y ajustadas por parte de la Oficina TICs. A espera de recibir el documento ajustado.



Comentarios Politica
y procedimiento gesti

- Se realiza por parte de la UT la **renovación de la Póliza Todo Riesgo**, se remite por correo electrónico al Coordinador del Grupo de Soporte Informático.



Documentos
renovación póliza tod

- El 27/11/2025 se realiza **instalación de la antena Starlink en la DT Caquetá / Florencia** como contingencia del servicio de conectividad.



Antena Starlink - DT
Caquetá.msg

- **Divulgaciones al equipo de trabajo:**
  - El 4/11/2025 la gestora de la práctica de incidentes socializa mediante correo electrónico una mejora orientada a la marcación de usuarios VIP en un campo específico de AD por parte del personal de la MDS, con el propósito de mantener actualizada la información de los usuarios que tienen estos roles ya que son gestionadas las novedades desde el primer nivel de soporte.
  - El 27/11/2025 la gestora de la práctica de problemas realiza divulgación mediante correo electrónico al equipo de especialistas de la UT sobre los Aspectos claves de la Practica ITIL Problemas, que incluye: definición de problema, identificación de causa raíz, en que momento se determina que es un problema, como se realiza la revisión y cierre de estos casos, medición de la eficacia de la solución.

g. Volumetría de Solicitudes Gestionadas:

En el mes de noviembre 2025 se registraron en la herramienta ITSM 6715 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: 5943
  - Incidentes: 734
  - Cambios: 38
  - Problemas: 0
- Casos Anulados: 3 - 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 noviembre 2025:

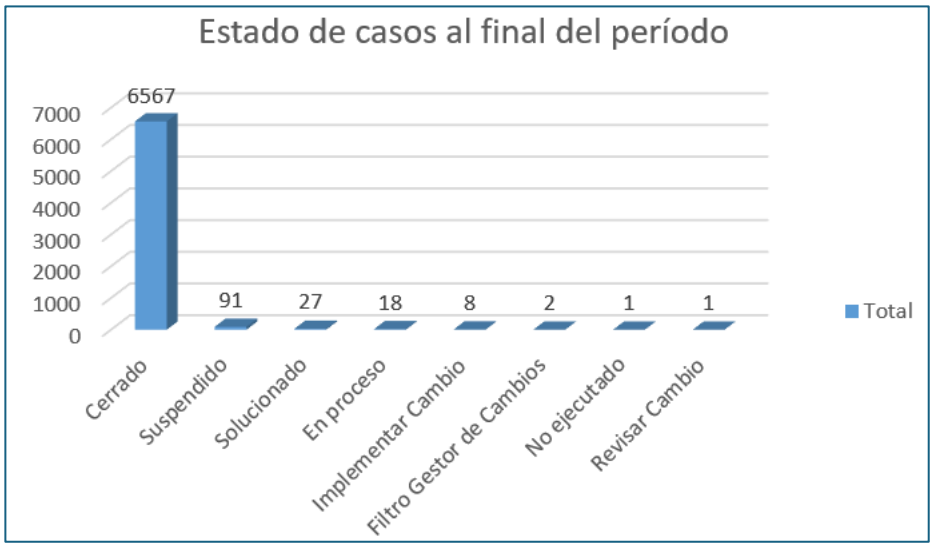


Ilustración 1 Estado final de casos al corte del período

- Gestión por parte de los grupos de especialistas:

Grupo Responsable	Cantidad de casos gestionados	Porcentaje (%)
Responsable_Soporte_Territoriales	2132	31,75
Responsable_Soporte_Bogota	1531	22,80
Responsable_Mesa_De_Servicio	1017	15,15
Responsable_Soporte_Impresoras	692	10,31
NOC	486	7,24
Especialistas_IBM	354	5,27
Responsable_De_Servidores_Windows	100	1,49
Especialista_Telefonía_IP	99	1,47
SOC	84	1,25
Especialista Base de datos	45	0,67
Especialista Nube Privada	44	0,66
Especialista Herramientas de Gestion	26	0,39

Gestor de Inventarios	25	0,37
Especialista Redes	25	0,37
Responsable Garantías Equipos	20	0,30
Almacenamiento y Backups	10	0,15
Especialista Nube Publica	9	0,13
Especialista Aplicaciones .Net	6	0,09
Gestión del Servicio	4	0,06
Responsable_de_Energia Electrica Regulada - UPS	3	0,04
Liferay	2	0,03
Especialista Aplicaciones JAVA	1	0,01
TOTAL	**6715**	**100**

Tabla 1 Atención de solicitudes por Grupo de Especialista

2.1.1. Herramienta de Gestión ITSM

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

- Afinamiento de métricas para toma de temperatura de baterías y entorno para UPS
- Creación de tablero de monitoreo de temperaturas de las UPS.
- Optimización script de creación de mantenimientos permitiendo enviar información detallada de por qué se solicitó el mantenimiento.
- Afinamiento de alertamientos por degradación de canales de internet, se iniciará con el canal de Columbus.
- Se realizó validación de todos los hosts relacionados a impresoras para garantizar el monitoreo de los equipos en Zabbix.
- Optimización en la selección de categoría durante la creación de casos automáticos del servicio de impresión, mejorando la precisión.
- Creación categorías para clasificación de casos de alertas de Zabbix por impresoras inaccesibles.
- Implementación para la gestión de incidentes mayores desde Aranda ASMS.
- Afinamiento de reporte para seguimiento de incidentes mayores por medio de AQM.
- Creación reporte para seguimiento de versiones de 890.
- Optimización de regla de notificaciones de casos asignados, la regla ya no se basa en el estado del caso si no que realiza la notificación cuando cambia el especialista responsable del caso.
- Actualización de la herramienta Aranda Device Managemnet a la versión 9.23.2.12
- Actualización de la herramienta Aranda Query Manager a la versión 9.41.2
- El 28/11/2025 se realiza cambio de contraseña del buzón de SoporteMT como buena práctica para temas de seguridad y acceso, se hace controlado para hacer los cambios requeridos en AD y Aranda, bajo el caso Aranda RFC-167530.

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

- **Tipificación de los cambios**

Durante el mes de noviembre de 2025 se gestionaron 38 casos tipificados como Cambios, clasificados en las siguientes categorías:

Servicio	No	Porcentaje
Administración de servidores	12	31,58%
Administración de Bases de Datos	11	28,95%
Soporte Microinformática	5	13,16%
Aplicaciones Especializadas	3	7,89%
Herramientas de Gestión	3	7,89%
Energía Eléctrica Regulada - UPS	2	5,26%
Redes y Conectividad	2	5,26%
Total	**38**	**100,00%**

Tabla 2 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 noviembre de 2025, en total se crearon 38 casos de los cuales se gestionaron 25 como cambios de normales, 6 cambios como de emergencia y 7 cambios como estándar



Sesion_HC_Noviembre.xlsx

- **Cambios por estado**

Al corte del 30 de noviembre, veintiséis (26) casos quedaron estado Cerrado, dos (2) en estado filtro gestor de cambios, dos (2) en revisar cambio, siete (7) en implementar cambio y un (1) caso quedo en No ejecutado.

- **Medición Indicador Porcentaje de Cambios Exitosos**

Nombre	Descripción / Fórmula	Meta	Periodicidad	Resultado
Porcentaje de cambios exitosos.	**PCE = (NCE/TCI)*100** Donde: **PCE:** Precisión **NCE:** Numero de Cambios Exitosos **TCI:** Total de Cambios implementados	80%	Mensual	PCE: 28/28*100 PCE: 100%

Tabla 3 Medición Indicador Porcentaje de Cambios Exitosos

Durante el periodo evaluado, el Gestor de Cambios realizó la verificación y clasificación de las 38 solicitudes registradas, de las cuales 28 fueron programadas e implementadas como cambios. Este proceso de revisión permitió garantizar que cada solicitud cumpliera con los criterios establecidos, asegurando un flujo de trabajo controlado, seguro y completamente trazable.

Del total de cambios implementados (TCI = 28), 28 fueron ejecutados de manera exitosa (NCE), lo que se refleja en un Porcentaje de Cambios Exitosos (PCE) de 100%, superando ampliamente la meta definida del 80%.

Este resultado evidencia la efectividad de la práctica, al garantizar que los cambios se ejecuten conforme a los procedimientos establecidos, minimizando riesgos operativos y asegurando la continuidad de los servicios.

El indicador alcanzado confirma que, durante noviembre de 2025, la Práctica de Habilitación de Cambios fue gestionada de manera eficiente, cumpliendo con los lineamientos definidos para la planeación, verificación, evaluación y ejecución de los cambios. Este nivel de desempeño contribuye directamente a la estabilidad operativa de la organización y refuerza la mejora continua de los servicios de TI.

2.1.2.3. Práctica Gestión de Activos

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

Las principales actividades desarrolladas fueron:

- **Seguimiento a la gestión de activos**

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

de siniestro con el fin de asegurar el cumplimiento de los tiempos establecidos y mantener la disponibilidad de los recursos tecnológicos..

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

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

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:

- **Asignación Grupo Resoluotor**

De acuerdo con la necesidad de la operación, se asignó el grupo resolutor SOC al servicio Soporte Microinformática para realizar el proceso de devolución de equipos ya que se debe crear el caso indicando el hostname del equipo a inactivar y ser escalado al SOC.

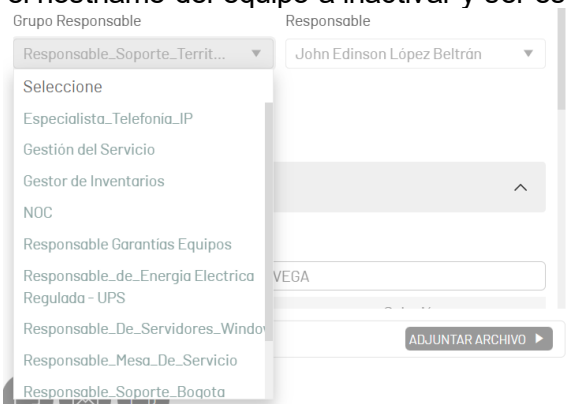


Ilustración 2 asignación grupo resolutor

Creación Categoría Incidente Mayor

Se crea la categoría Reportar una falla.Incidente Mayor agregada a todos los servicios la cual será utilizada únicamente para los incidentes mayores teniendo en cuenta automatización realizada para el reporte de dichos incidentes.

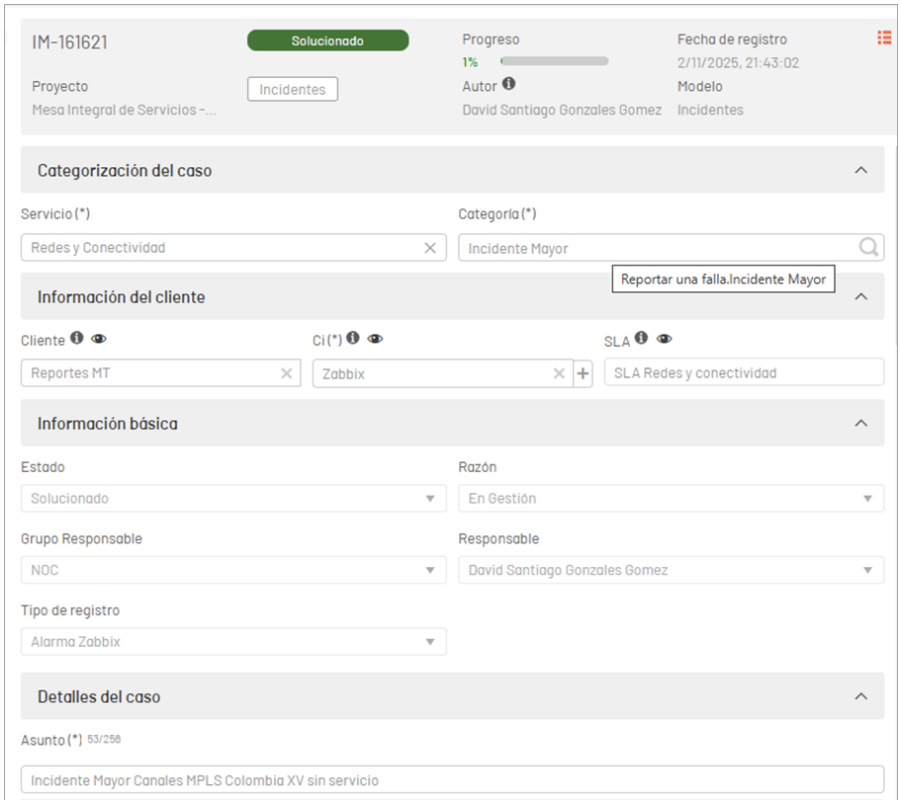


Ilustración 3 creación categoría incidente mayor

Configuración Tarea Actualización de Usuarios VIP

Con relación a la actualización de usuarios VIP, se solicitó la Configuración Tarea - Actualización Usuarios VIP Aranda con el fin de mantener actualizado el listado de usuarios en la herramienta de gestión, así mismo se socializó con el equipo de mesa de servicios.

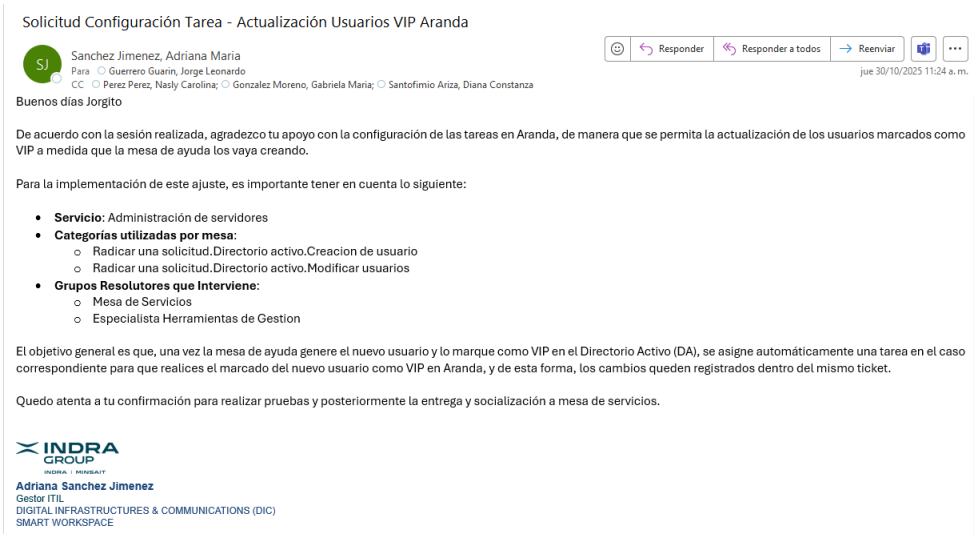


Ilustración 4 Actualización usuarios VIP

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 noviembre
Porcentaje de cumplimiento de la actualización del Catálogo	CPS=(TCG/TCE) *100 CPS: Cumplimiento en la prestación de los servicios TCE: Total de casos escalados (Recibidos) (Modificación, Agregar o Desactivar el servicio). TCG: Total de casos gestionados (Solucionados) (Modificación, Agregar o Desactivar el silencio).	90%	Mensual	CPS= (1/1)*100 EF= 100%

Tabla 4 KPI Práctica Catálogo de Servicios

2.1.2.5. Práctica de Problemas

Dar a conocer las actividades de la Práctica de Problemas correspondientes al periodo del 1 al 30 de noviembre 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 3 1	Error conocido Solución Temporal Solución definitiva
MINTRABGD01A - Gestor documental	1	Investigación y Diagnóstico
Office 365	1	Error conocido
Página web	1	Solución definitiva - cierre
servicio de relay en el ISS	1	Solución Temporal
SISINFO	1	Solución Temporal
Telefonía	1	Solución definitiva - cierre
UPS Manizales	1	Solución Temporal
Total	13	

Tabla 5 Consolidado problemas identificados

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

Avances: Se realizó la instalación de los componentes de FileNet, se realizaron pruebas unitarias hacia la base de datos las cuales fueron satisfactorias. Se revisaron los logs de websphere para verificar errores o fallos en el despliegue de las conexiones jdbc y excepciones del sistema. Se validó el acceso a la consola administrativa de content engine (ACCE) para visualizar los objetos de los repositorios.

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

Durante el período del informe, se registraron 734 incidentes, este volumen incluye:

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

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

Estado	Cantidad
Cerrado	710
Suspendido	12
Solucionado	10
En proceso	2
Total general	**734**

Tabla 6 Estados Incidentes

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

Tipo de incidente	Total	Observación
Reportar una falla.Alarma Zabbix.Router	237	Incidentes generados en el servicio de redes y conectividad por afectaciones en infraestructura del proveedor.
Reportar una falla.Falla impresora.No imprime	97	Novedades por atasco de papel en el mecanismo de alimentación.
Reportar una falla.Alarma Zabbix.Starlink	97	Intermitencias presentadas por: condiciones climáticas adversas (tormentas, nubes densas), obstrucciones físicas (techos, árboles), fluctuaciones eléctricas y ajustes en la cobertura satelital en regiones específicas.
Reportar una falla.Alarma Zabbix.FortiGate	94	Incidentes generados en el servicio de impresión: desconexión de impresoras por falta de comunicación con el servidor tras cambio de contraseña, alertas por tamaño de papel incorrecto, cancelación de documentos por cupos de impresión agotados, finalización de saldos, cables de red desconectados, entre otros.
Reportar una falla.Gestor Documental.Falla radicacion	20	Errores por conexión en puertos incorrectos, cambios de IP por bloqueo, patch cord desconectado, cambios de contraseña, red del proveedor con fallas, tarjeta inalámbrica inhabilitada, y problemas con controladores.

Reportar una falla.Alarma Zabbix.UPS	19	El 72% de las novedades de UPS corresponde a que la novedad se originó por un alertamiento en el servicio “Internet Columbus”, afectando la Sede Central durante un periodo aproximado de 18 minutos. Esta situación impactó la disponibilidad de los equipos Access Point (AP), Switch y UPS en dicha sede. La novedad se registró a las 00:26 a.m De acuerdo con la revisión efectuada junto al equipo de redes, la causa corresponde a una intermitencia temporal, por lo cual no fue posible escalar al proveedor en el momento de la alerta. Durante el transcurso del día se ha realizado seguimiento, confirmando que el servicio se encuentra actualmente operativo y estable.
Reportar una falla.Falla impresora.Atasco	18	Novedades con el correo: claves incorrectas, cuentas bloqueadas o deshabilitadas, errores de sincronización, falta de espacio, límites de envío, problemas en la descarga de archivos, cierre inesperado del cliente y lentitud en el navegador.
Reportar una falla.Alarma Zabbix.Servidor Windows	15	Incidentes generados en el servicio de impresión: desconexión de impresoras por falta de comunicación con el servidor tras cambio de contraseña, alertas por tamaño de papel incorrecto, cancelación de documentos por cupos de impresión agotados, finalización de saldos, cables de red desconectados, entre otros.
Reportar una falla.Gestor Documental.Lentitud gestor	14	El 96% de los casos corresponde a errores en la aplicación del gestor documental. Se destacan reprocesos, relanzamientos y sobrecarga del sistema debido al desconocimiento de los flujos por parte de los usuarios.
Reportar una falla.Equipo de computo.Falla - Error conexión a red	13	Novedades presentadas debido a contraseñas que caducan, desconexión de red Wifi, renovación de dirección IP. ETC.

Tabla 7 Top 10 Incidentes

- **Casos Suspendidos**

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

Grupo Resolutor	Noviembre
Especialista Redes	6
NOC	5
Responsable_de_Energia Electrica Regulada - UPS	2
Responsable_Soporte_Bogota	1
Total general	**14**

Tabla 8 Incidentes Suspendidos

Del total de casos en backlog (suspendido y en proceso), solo se registra 14 tickets en gestión por parte de los grupos resolutores tales como Redes y Conectividad (6), NOC (5), Responsable_de_Energia Electrica Regulada – UPS (2) y soporte Bogotá (1).

Del total de casos en backlog (suspendido y en proceso), solo se registra 14 tickets en gestión por parte de los grupos resolutores como Redes y Conectividad (6), NOC
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:

Incidente Aranda	Estado Ticket Aranda	Asunto	Causa Raíz	Acciones Realizadas para restablecer el servicio	Usuarios Afectados	Fecha/Hora inicio	Fecha/Hora Fin	Tiempo de Indisponibilidad
IM-163278	Cerrado	Incidente Mayor Novedad Soporte Impresión	o La causa raíz se logró identificar a nivel de SO por medio de un bug generado en el aumento donde el servidor tomo el aumento de forma correcta pero los servicios quedaron en un estado inestable.	o Como primera acción se realiza revisión de los servicios a nivel de SO luego del aumento de performance de la MV con apoyo del equipo de nube privada. o Reinicio de los servicios y revisión de logs a nivel de servicios de aplicación de PaperCUT o Como medida para tomar el cambio se reinició el servidor y se validó de manera correcta cada uno de los servicios que usan los binarios de PaperCUT.	10% de usuarios de acuerdo con actualización de la nueva interfaz	10/11/2025 7:00	10/11/2025 12:25	5 h 25 min
IM-163707	Cerrado	Incidente Mayor Novedad con Impresión en el papercut	o Multiversionamiento de drivers de impresoras RICOH	o Reinicio de la cola de impresión a raíz de incompatibilidad de drivers multi versión. o Estandarización de dos drivers entre PCL6 y PS. o Errores de sincronización con el cambio de controladores o Reinicio de la cola de impresión y espera de tiempos para resincronización con el nuevo driver, sin embargo, en algunos casos si comunicación toco forzarla de forma manual	General	11/11/2025 9:45	11/11/2025 11:00	1 H 45 min
IM-163223	Cerrado	Incidente Mayor Novedad Internet Zona Norte	En comunicación con ETB nos confirma que se observaba la fibra afectada por podas realizadas.	Los técnicos asignados realizaron el correctivo de fibra correspondiente, solucionando así la falla.	RInternet_ETB_Santa_Marta RInternet_ETB_Riohacha Router_Fundacion Router_Fonseca Router_Plato Router_Cienaga	10/11/2025 8:50	10/11/2025 9:53	1h 3m
IM-161621	Cerrado	Incidente Mayor Canales MPLS Colombia XV sin servicio	Corte de fibra por vandalismo	Dando seguimiento a los casos 25868322, 25868320, los cuales se vieron afectados por una falla de alto impacto. Nos permitimos informarle que la falla de alto impacto ha sido solucionada exitosamente, y se ha logrado recuperar la operatividad de los servicios. Resumen: Le compartimos el siguiente reporte técnico correspondiente a la atención en terreno: Se realiza validación de la caja de empalme en la Carrera 55A con Calle 170. Se ubica el daño en la siguiente dirección: Dirección: Calle 170 con	Inspecciones a nivel nacional	1/11/2025 21:41	3/11/2025 20:50	1d 23h 9m

				Carrera 55A Coordenadas: 4.753247150959328, -74.0554390846945 Cable afectado: 71248 Capacidad: 144 hilos Causa del daño: Vandalismo Se preparan puntas para realizar la reparación de la fibra óptica. Se han fusionado los hilos requeridos, quedando operativas las dos interfaces reportadas. Faltan por fusionar los hilos 23 y 53. Los hilos 23 y 53 ya fueron fusionados, y se continúa con el proceso de fusión de los demás hilos. Se observan interfaces operativas.				
IM-167562	Cerrado	Incidente Mayor Alertamiento Masivo Inspecciones	Validando con el equipo de redes y el proveedor de telecomunicaciones, se identificaron dos causas principales. En primera instancia, se presentó un corte de fibra a 33 metros, lo que ocasionó una renegociación del protocolo de enrutamiento BGP.	Validando con el equipo de redes y el proveedor de telecomunicaciones, se identificaron dos causas principales. En primera instancia, se presentó un corte de fibra a 33 metros, lo que ocasionó una renegociación del protocolo de enrutamiento BGP. Esto generó la pérdida de la ruta hacia la IP de Zabbix, motivo por el cual no era posible alcanzarla, a pesar de que los canales de internet se mantenían operativos. Una vez restablecida la fibra, el protocolo BGP se normalizó y se recuperó el enrutamiento, permitiendo el funcionamiento habitual del monitoreo en la operación.	No se presentó afectación a los usuarios, se identificó novedad con el monitoreo de inspecciones a nivel nacional.	25/11/2025 15:26	26/11/2025 14:41	23h 15m
IM-164105	Cerrado	INCIDENTE MAYOR - Alertamientos sede central Zabbix.	Intermitencia en el servicio de internet de Columbus	Se procede con la validación del momento exacto en que se presentó la alarma, la cual se originó por un alertamiento en el servicio "Internet Columbus", afectando la Sede Central durante un periodo aproximado de 18 minutos. Esta situación impactó la disponibilidad de los equipos Access Point (AP), Switch y UPS en dicha sede. La novedad se registró a las 00:26 a.m. y, según las validaciones realizadas con el equipo NOC, el evento no fue visualizado en el tablero de monitoreo Zabbix. De acuerdo con la revisión efectuada junto al equipo de redes, la causa corresponde a una intermitencia temporal, por lo cual no fue posible escalar al proveedor en el momento de la alerta. Durante el transcurso del	Sede Central	12/11/2025 0:26	12/11/2025 0:44	18 Min

				día se ha realizado seguimiento, confirmando que el servicio se encuentra actualmente operativo y estable.				

Tabla 9 Incidentes Mayores

- **Otras Actividades**

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

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

Nombre	Descripción / Fórmula	Meta	Periodicidad	Resultado noviembre
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=732/734*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= 1/720*100 RRP= 0,10%

Tabla 10 Medición de KPIs

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

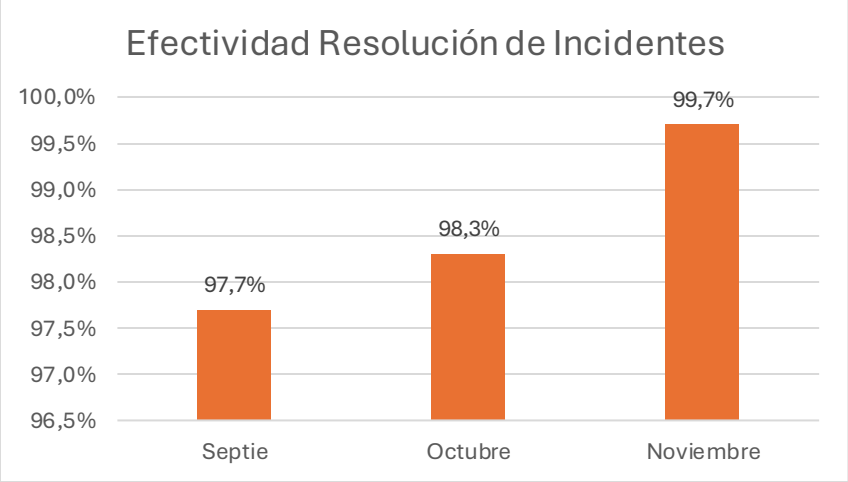


Ilustración 5 Efectividad de resolución de incidentes

Durante los últimos 3 meses, la efectividad en la resolución de incidentes se mantuvo por encima del indicador de cumplimiento del 80%, con los siguientes resultados:

- Septiembre: 97.7%
- Octubre: 98,2%
- Noviembre: 99,7%

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

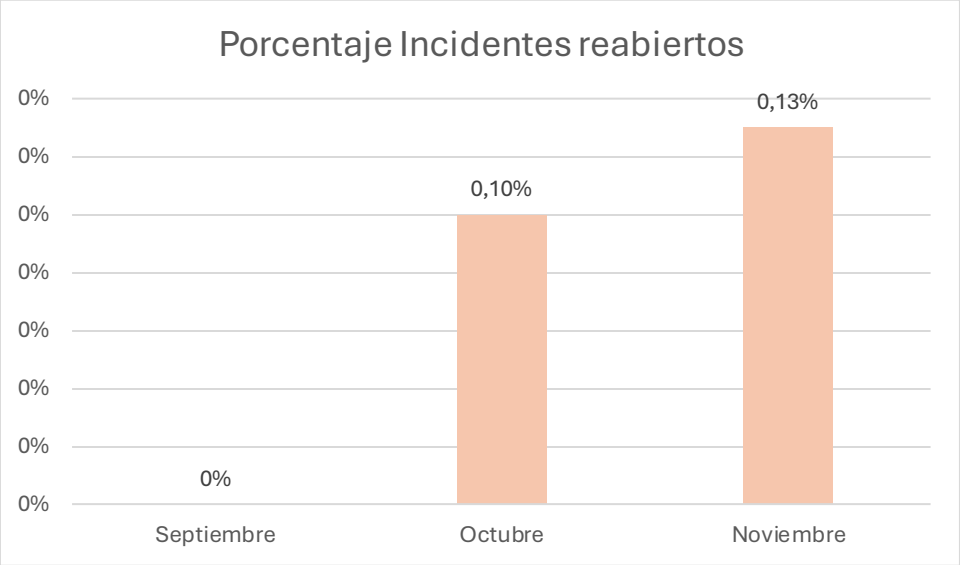


Ilustración 6 Porcentaje de incidentes abiertos

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

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

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 noviembre 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 5946 casos tipo requerimiento quedando en los siguientes estados:

Estado	Casos
Cerrado	5831
Solucionado	17
Suspendido	79
En proceso	16
Anulado	3

Tabla 11 Estados de Requerimientos

- Durante el mes, se presentaron 3 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 octubre al periodo actual.

Grupo Responsable	Octubre	Noviembre
Especialista Aplicaciones .Net	2	1
Especialista Herramientas de Gestion	0	0
Especialista Nube Privada	1	1
Especialista Nube Publica	0	0
Especialista Redes	0	2
Especialista_Telefonía_IP	0	0
SOC	5	3
Especialistas_IBM	0	3
Responsable Garantías Equipos	7	9
Responsable_De_Servidores_Windows	4	1
Responsable_Mesa_De_Servicio	19	16
Responsable_Soporte_Bogota	17	10
Responsable_Soporte_Impresoras	20	15
Gestor de Inventarios	1	2
Responsable_Soporte_Territoriales	18	14
Responsable_de_EER - UPS	0	1
Especialista Base de datos	0	1
Total por Periodo	**94**	**79**

Tabla 12 Seguimiento del Backlog Suspendidos

En el inicio del período, se identificaron 94 casos suspendidos correspondientes al backlog del mes de octubre de 2025. Se realizaron seguimientos semanales de las solicitudes en estado abierto, logrando la solución de 93 casos a través de la herramienta de Gestión Aranda de los anteriores periodos. Para el cierre del mes, se encuentran pendientes 79 casos en el mes de noviembre, 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.Instalacion - configuración	1078
Radicar una solicitud. Impresora. Aumentó de cuota	577
Radicar una solicitud. Impresora. Cargue de papel en impresora	559
Radicar una solicitud. Alarma Zabbix.Impresora	286
Radicar una solicitud. Impresora. Asesoría - Consulta	192
Radicar una solicitud. Directorio activo. Cambiar contraseña	169
Radicar una solicitud. Equipó de cómputo. Configuración	127
Radicar una solicitud. Impresora. Cambió Toner	123
Radicar una solicitud. Correo Electronico.Asesoria - Consulta	122
Radicar una solicitud. Equipó de cómputo. Actualización BIOS	119

Tabla 13 Top 10 de Solicitudes

- De acuerdo con el TOP 10 de solicitudes, se evidencia que las categorías con mayores solicitudes son del servicio de Impresión con las categorías de instalación y configuración con 1078 tickets, Aumento de cuota de impresión con 577 tickets y Cargue de papel en impresora 559 tickets.
- Se realizó seguimiento a requerimientos en backlog, enviando correos a los especialistas para la documentación y cierre de casos pendientes.
- Desde la Práctica de ITIL se realizan auditorias de casos en los que se evidencian oportunidades de mejora, compartidas por correo a los especialistas a quienes se les hace retroalimentación, con base en las novedades encontradas en cada ticket.

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

Nombre	Descripción / Fórmula	Meta	Periodicidad	Resultado del Periodo
Porcentaje de efectividad en resolución de Requerimientos de servicio.	**EF=(RFS/RFR) *100**	80%	Mensual	**EF=** 5935/5943 *100
	EF: Efectividad en solución de Requerimientos.			
	RFS: Requerimientos solucionados que cumplen el ANS en el período.			**EF= 99.87%**
	RFR: Requerimientos registradas en el período.			
Porcentaje de Requerimientos Reabiertos en el Periodo	**RRP:** Porcentaje de casos Reabiertos en el periodo.	<2%	Mensual	**RRP=** 8/5848*100
	RFR: Requerimientos Reabiertos en el período.			**RRP= 0,136%**
	RFS: Requerimientos solucionadas en el período.			

Tabla 14 Detalle de KIP Practica de Requerimientos

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

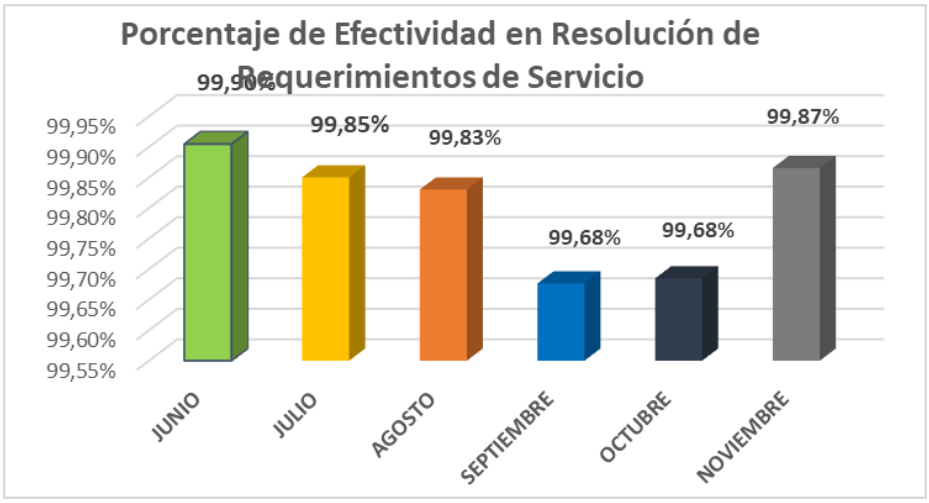


Ilustración 7 KPI Efectividad de Resolución de Requerimientos de Servicio

Durante el periodo, se evidencia el cumplimiento del 99.87% aumenta efectividad de la solución de los requerimientos a comparación de los anteriores periodos, los cuales se verifica de 5943 casos registrados en los diferentes canales oficinales de la Mesa de Servicio que fueron solucionados, 5935 casos cumplieron con los tiempos del ANS para dar una respuesta efectiva al usuario y 8 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.

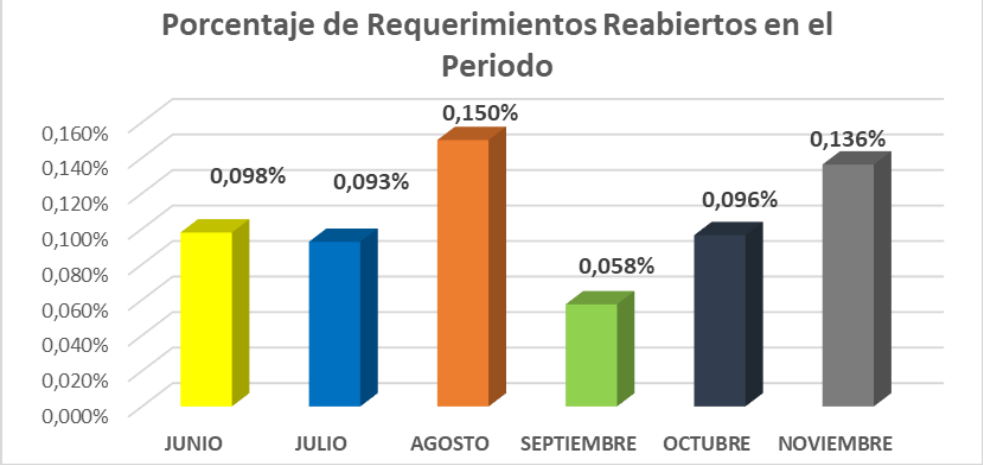


Ilustración 8 Requerimientos de Reabiertos en el periodo

Durante el periodo, se realizó el seguimiento de los requerimientos reabiertos por los usuarios, se ha evidenciado durante los últimos meses se había presentado disminución de reaperturas, pero para noviembre aumentaron casos de reaperturas por errores en la documentación y se reabre el caso por parte de los servicios TIC, por lo tanto, se precederá a realizar retroalimentación a los grupos responsables.
Para noviembre se presentaron 8 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-161830	Radicar una solicitud. Ofimatica.Asesoria Excel	Responsable Soporte Bogotá	Se comunica la usuaria indicando que no le abren los archivos de Excel el lunes 03/11/2025	Se brindo soporte en su puesto de trabajo a la funcionaria el 03/11/2025 sobre la solicitud de asesoría de archivos en Excel, lo cual el 04/11/2025 se documentó el caso en la herramienta, al enviar la notificación de la solución, la funcionaria no recordaba que la habían prestado servicio el 03/11/2025 y reabrió el caso. Por lo cual se realiza revisión e indica al Soporte en Sitio que debe gestionar los casos y documentarlos en las fechas establecidas al momento de su reapertura.
RF-163177	Radicar una solicitud.Navegadores. Asesoria - Consulta	Responsable Mesa de Servicio	Se envía correo por parte del funcionario, el cual indica presentan problemas de internet porque realizaron un mantenimiento al poste y cortaron la fibra de internet de la sede	Se indica que la solicitud informada en el correo electrónico se está gestionando por el área encargada con el caso IM-163170, por lo tanto, al ver esta respuesta no está de acuerdo al cierre del caso RF-163177 porque se sigue presentando la falla en el canal internet y sin impresión de la sede. En el caso IM-163170, se brindó la respuesta y realizó el respectivo soporte y solución al caso. Por lo anterior, se indica al Agente de MDS, se debe ser claro con el usuario para evitar confusiones frente a la solución del caso.
RF-163341	Radicar una solicitud. Escaner.Instalacion - Configuración	Responsable Soporte Impresoras	Usuario indica que no puede utilizar la impresora porque genera error para escanear	Se indica en la solicitud la siguiente respuesta frente al caso : " Buen día, usuario cuenta con saldo para imprimir, a nivel de escáner no hay necesidad de tener saldo, pero si realizar la validación de los parámetros para que tome ambas caras de las hojas. Por lo anterior, se evidencia que no corresponde a la solicitud del usuario, por lo cual se reabre el caso por parte del usuario, ya que al momento de escanear más de 5 hojas la impresora bota el error que no es posible enviar el correo por el tamaño del archivo, por lo anterior se envía al soporte en sitio a la revisión de la impresora, he indica que ya se puede escanear los documento y se cierra el caso.
RF-163718	Radicar una solicitud. Gestor documental. Asignar Radicado TYS	Especialistas IBM	Usuaria solicita revisar la causa por la cual no se puede descargar el PDF de Gestor Documental con el Radicado 05EE2025310300000059298	Se solicita revisar la descarga de un PDF de Gestor Documental, por lo que el especialista de IBM informo que se realizó la verificación correspondiente y se confirma que el documento inicialmente se encontraba con errores debido a caracteres especiales que tenía en el nombre (%) se realiza la corrección del documento y ya está activo para continuar con el proceso. Al verificar la respuesta, se evidencia por parte de la usuaria, se sigue presentando el error al descargar y reabre el caso. Por lo anterior el especialista adjunta el archivo solicitado y solicita volver a realizar la consulta, saliendo y entrando nuevamente a la aplicación, lo cual es efectivo y se cierra el caso.
RF-164012	Radicar una solicitud. Vídeo Beam.Prestamo	Responsable Soporte Bogotá	Solicitan el préstamo del video beam para una reunión en el auditorio, por lo cual se debe instalar y tener todo listo para la sesión.	Se realizó préstamo, una vez devuelto, se retorna dispositivo al piso 2, por lo cual se soluciona el caso, pero por error del Soporte Sitio al documentar, se reabre para realizar la documentación faltante. Por lo anterior, se procedió a realizar la retroalimentación al Soporte en Sitio.
RF-165094	Radicar una solicitud. Impresora.Instalacion - Configuración	Responsable Soporte Territoriales	Se solicita la configuración de la impresora RICOH por actualización de software de impresión.	Se realiza la verificación de la instalación del nuevo controlador para las impresoras de Facatativá y se instala a todas las impresoras de la Territorial Cundinamarca y las pruebas de impresión son satisfactorias y se soluciona el caso.

RF-165651	Radicar una solicitud. Antivirus. Habilitación Puertos USB	SOC	Se solicita realizar la apertura de unos puertos bidireccionalmente entre el Datacenter de Bogotá y el de Cali.	Por parte del Grupo responsable indica que se realizó lo siguiente: 1. Se crean las políticas en el Vdom DMZ desde el ID 45 hasta el ID 50, que permite la conexión entre el origen y destino solicitado. 2. Se crean las políticas en el Vdom DMZ desde el ID 190 hasta el ID 197, que permite la conexión entre el origen y destino solicitado. Por lo anterior, se dio por solucionado el caso, pero por error del Grupo responsable de Soporte se reabrió el caso, al momento de documentarlo y se realiza la retroalimentación frente a lo ocurrido.
RF-166058	Radicar una solicitud. Ofimatica.Asesoria - Consulta	Responsable Soporte Territoriales	Solicita el desbloqueo del correo electrónico, ya que no es posible ingresar con su usuario y contraseña	De acuerdo con la validación del caso, se evidencia la contraseña se encuentra vencida desde el 03/05/2025, por lo tanto se solucionó el caso por equivocación, por lo tanto se revisa desde la Coordinación de MDS, se procede a volver abrir el caso para poder hacer el restablecimiento de la contraseña al usuario pero en diferentes días hábiles se intentó contactarlo, lo cual no fue posible la comunicación para el restablecimiento de la contraseña y se cierra el caso con la situación presentada del contacto no efectivo.

Tabla 15 Casos reabiertos

2.1.2.8. Práctica de Eventos

Para el mes de noviembre, 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 1240 casos escalados mediante la herramienta de gestión de los cuales 493 alarmas fueron gestionadas por el NOC, los casos restantes corresponden a casos generados por incidentes masivos que se relacionaron a los mismos o casos creados por los diferentes CI que hacen parte de una misma sede

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

  - Cambios en nombres e IP de Host de impresión.
  - Inhabilitación de monitoreo para equipos apagados desde infraestructura.
  - Creación de monitoreo para host de redes.
  - Creación de dependencias para nuevos hosts recibidos.
  - Categorización por sede, tipo y ubicación para los nuevos hosts.
  - Optimización de la automatización de creación de mantenimientos, mejoras de la seguridad, los parámetros, personalización de nombres, timeout.
  - Mejora en la generación del informe de disponibilidad reduciendo tiempos de ejecución.
  - Modificación reportes de cambios agregando los nuevos campos adicionales.
  - Mantenimiento infraestructura Aranda para optimización en el rendimiento de las herramientas.

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

  - Se realizó seguimiento a casos en backlog
  - Se realizó seguimiento de alarmas diarias en Zabbix y se envía reporte diario con apoyo del equipo NOC

- Solicitud de mantenimiento de sedes en las que los funcionarios apagan los equipos y/o se ausentan de las mismas
- Solicitud de Mantenimientos de acuerdo con RFC aprobados.

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 noviembre
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= (481/493)*100 EF= 97%

Tabla 16 KPI Práctica de Eventos

- **Informe Operación NOC**

La labor del equipo del Centro de Diagnóstico y Operaciones (CDO) permitió identificar y gestionar oportunamente un total de 493 incidentes, lo cual evidencia una alta capacidad operativa y de respuesta ante eventos críticos.

Los Routers fueron el componente con mayor incidencia, concentrándose 240 casos (49% del total). Esto está asociado a factores como la inestabilidad de la red eléctrica en zonas remotas o condiciones ambientales adversas.

Para este mes se evidencia una disminución en los casos reportados por Antenas Starlink, los cuales se encuentran en el tercer lugar, representando 97 (20% del total) de los casos. Se evidencia que estas antenas son mayormente afectadas por temas eléctricos en las sedes, de igual forma una intervención humana con el apagado de los equipos.

Los dispositivos FortiGate representaron el 19% de los casos (95 incidentes), eventos causados por falla en la energía comercial, apagado de equipos por parte de los funcionarios e intermitencias en el servicio en horario no hábil. En los eventos que se presentaron en horario no hábil no se logró determinar la causa raíz. A comparación de meses anteriores se ha visto una mejoría en la operación de los FortiGate.

Los servidores Windows en cuarto lugar representados 30 (6% del total) de los incidentes, evidenciando este mes una disminución del 2% en comparación con el mes anterior, aunque, son considerablemente altos en comparación con los Servidores Linux con solo 6 casos, representando el 1% del total de los casos.

Los Access Point ocupan el 5to lugar con un 3% (13 casos) del total de los incidentes, cifra la cual es similar en comparación con los meses anteriores ya que en este aumento solo un caso.

Los dispositivos UPS, Switches y canal internet en conjunto reflejan una baja incidencia del 2% (12) del total de los casos, lo cual muestra una baja incidencia en fallas relacionadas a estos equipos.

Redes y Conectividad

Routers: Desde el centro de operaciones NOC durante el mes de noviembre se gestionaron 240 incidentes relacionados con equipos de red Routers en diferentes sedes a nivel nacional, los cuales representaron el 49% de los casos.

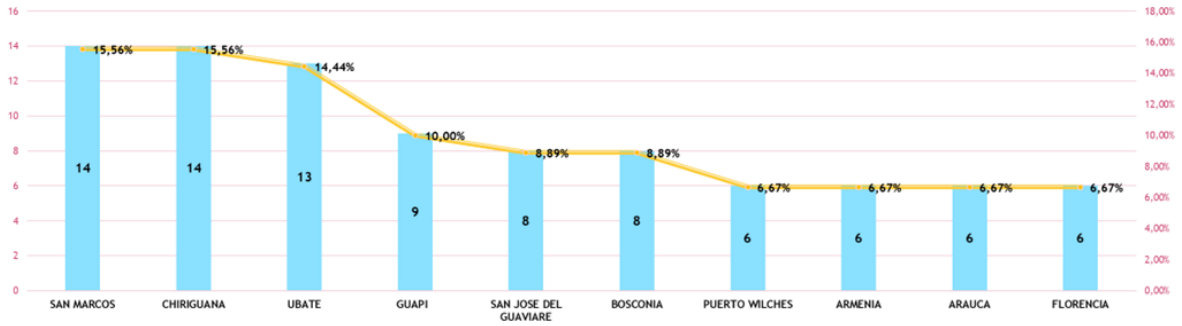


Ilustración 9 Top de incidentes por sedes

Para este mes se evidencia que las sedes San Marcos y Chiriguaná se consolidan como las sedes del TOP 10 con mayor número de incidentes, registrando 14 casos cada una, representando en conjunto el 31,12%) del total de los casos para esta categoría. La causa predominante en todos ellos es la desconexión o apagado físico de equipos por parte de los funcionarios al finalizar su jornada laboral, lo que genera alarmas en Zabbix fuera del horario hábil.

Ubaté ocupa el segundo lugar con 13 casos (14,44%) corresponden en su mayoría (5 de los 13 casos) a fallas en la red de proveedor de UM, 3 de los casos por intermitencias o lentitud en la red, 2 casos por apagado de equipos en sede por parte de los funcionarios y 3 casos por falla de energía eléctrica. Se evidencia que durante el mes de noviembre esta sede presento una intermitencia reiterada en la red del proveedor la cual fue solucionada, sin embargo, en los últimos dos meses se ha evidenciado que la intermitencia a persistido en esta sede.

Guapi ocupa el tercer lugar con 9 casos de los cuales 7 son por falla de energía eléctrica y 2 por Intermitencia/Lentitud en la red.

San José del Guaviare y Bosconia se posiciona en el cuarto lugar del TOP 10 con 8 casos cada una. La causa principal de los incidentes en San José del Guaviare para este mes está dividida en dos, por un lado 4 casos con proveedor y 4 casos por falla de energía eléctrica. Por otro lado, Bosconia presento causa principal 5 casos por falla de energía, 2 casos por Desconexión/apagado Físico de Equipos en Sede y 1 caso por Intermitencia/Lentitud en la red. Esta diversidad de causas sugiere que también existen factores internos en la sede (como falta de mecanismos de respaldo eléctrico) que contribuyan significativamente a la prevención de alarmas.

Las sedes de Puerto Wilches, Armenia, Arauca y Florencia, las cuatro con 6 casos cada una relacionada a Routers. En Puerto Wilches 5 de los 6 incidentes se relacionan a Falla Energía Eléctrica y el restante a Desconexión/apagado Físico de Equipos en Sede. Armenia registro 6 casos relacionados, 3 por Intermitencia/Lentitud en la red, 1 por falla en red de proveedor y 2 por falla de energía eléctrica. Arauca registro 6 casos de los cuales 5 fueron por falla de energía y el restante por Intermitencia/Lentitud en la red. Florencia registro 6 casos de los cuales 4 por falla de energía y los dos restantes Falla en Red de Proveedor. Esto refuerza la necesidad crítica de implementar sistemas de respaldo energético (UPS) en las sedes para mitigar la recurrencia de alarmas y garantizar la continuidad del servicio en las zonas que presentan esta falla reiterativa.

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

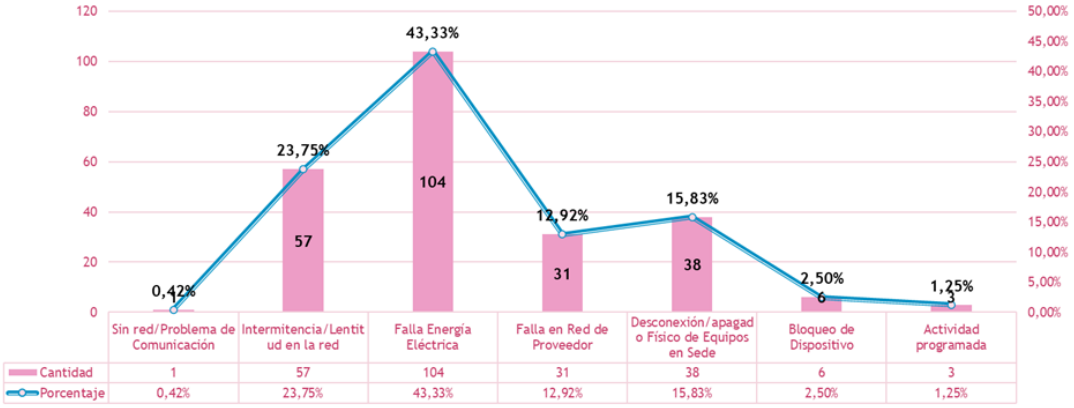


Ilustración 10 Top de incidentes por sedes

Se evidencia que la causa principal del total de eventos para la categoría de Routers es por Falla Energía Eléctrica ocupando el 43,33% y seguido por la falla en Intermitencia/Lentitud en la red y este último con un 23,75% del total de los casos para esta categoría.

Las fallas por energía eléctrica representan el 43,33% de los casos (104), afecta principalmente a zonas remotas o rurales como Guapi, Arauca, Bosconia, Puerto Wilches, San José del Guaviare, Florencia, Copey, entre otras, donde la red eléctrica es inestable o está sujeta a cortes constantes.
El 23,75% (57) de los casos están asociados a Intermitencia/Lentitud en la red, este tipo de incidencias se concentra en regiones con interrupciones del servicio de energía o en la red de datos de proveedor, sin embargo, estas se han registrado en su mayoría en horario no hábil y las cuales no han durado más de 20 a 30 minutos activas. Las sedes con mayor número de eventos por esta causa son Yopal, Villavicencio, Ubaté, Málaga y Armenia.

El 15,83% (38) de los casos están relacionados a desconexión apagado físico de equipos en sede, siendo San Marcos la que registra mayor cantidad de eventos con 14, seguida de Chiriguana con 12 registros, los cuales son ocasionados porque los funcionarios apagan los equipos al salir de turno con el fin de prevenir la afectación de los equipos por picos altos en el servicio de energía.

El 12,92% (31) de los casos están relacionados a Falla en Red de Proveedor, siendo Ubaté la sede con mayor número de eventos registrados (5) por esta causa y seguido por San

José del Guaviare con 4 casos. Estos registran todos en estado cerrado por rupturas en la fibra y solucionados por personal del equipo de empalmaría en terreno.

El 4,17% (10) de los casos es por bloqueo de dispositivo, actividad programada y Sin red/Problema de Comunicación suman en conjunto este porcentaje, siendo bloqueo de dispositivo la mayor causa con 6 (2.50%) eventos registrados, seguido de actividad programada con 3 eventos (1.25%) y por último Sin red/Problema de Comunicación con 1 evento (0,42%). En varios casos, el bloqueo ocurre tras eventos eléctricos o fluctuaciones de red, lo que sugiere que los dispositivos carecen de mecanismos de autorrecuperación robustos.

Switches

Durante el mes de noviembre se generaron 5 casos referentes a Switches en la herramienta de monitoreo Zabbix en diferentes sedes, los cuales representan el 1% del total de los casos, donde se evidencia una baja de 5 casos en comparación con el mes pasado.
Se evidencia que, de los 5 eventos registrados sobre Switches, las sedes con eventos fueron Bogotá sede central, Mocoa, Sincelejo y Cali.

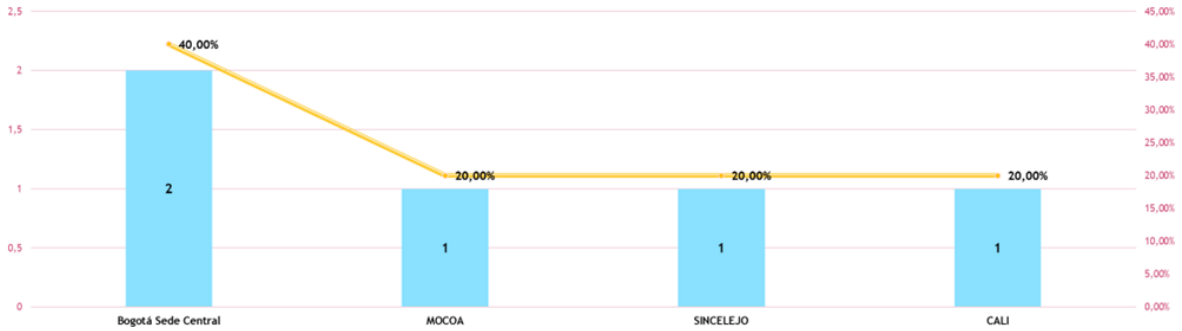


Ilustración 11 eventos por sedes routers

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

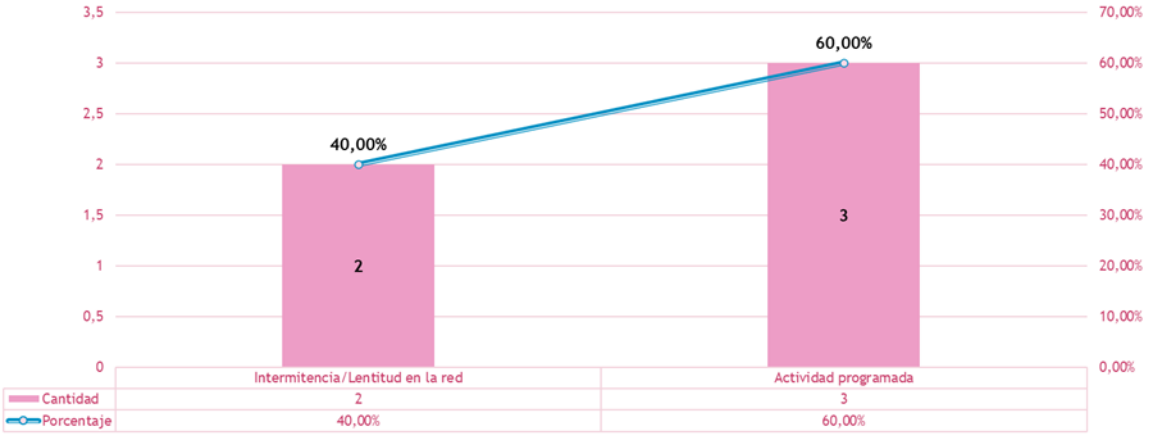


Ilustración 12 Top de causas por sedes switches

Se listan 2 diferentes causas para la categoría de Switches registradas durante el periodo del mes de noviembre.

3 de los 5 casos (60%) están directamente relacionados con actividad programada en la que se vieron afectadas y se registraron dos eventos para Bogotá sede central y una para Cali, de las cuales las 3 fueron por un bloqueo en el FW y el cual fue atendido por el equipo del SOC quienes realizaron el respectivo ajuste.

Los 2 casos restantes (40%) se atribuyen a intermitencia o lentitud en la red, ya que estas alarmas estuvieron activas por un lapso corto y menor a 20 minutos. Estos eventos se presentaron 1 en Sincelejo y 1 Mocoa donde el servicio de energía es inestable según lo informado por el personal en sitio.

Access Point

Desde el Centro de Operaciones (NOC), durante el mes de noviembre se gestionaron 13 incidentes asociados a equipos de red WLAN – Access Point en distintas sedes a nivel nacional, los cuales representan el 3% del total de casos reportados. Estos eventos fueron abordados dentro de los niveles de servicio establecidos, sin afectación crítica a la operación general de la red.

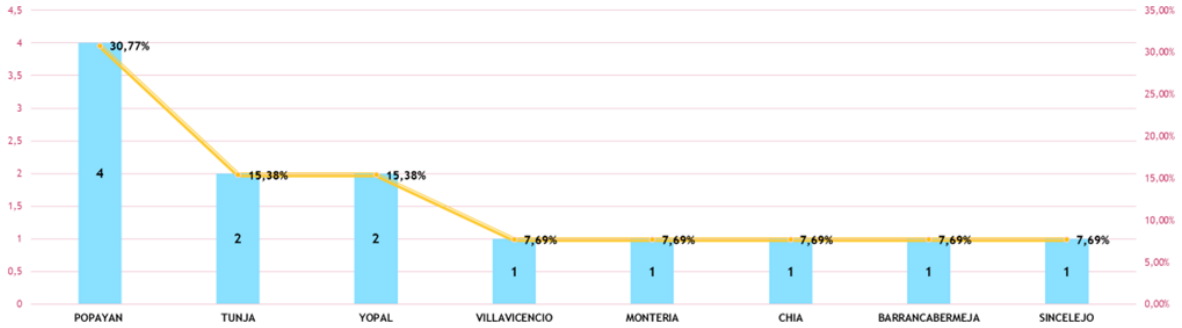


Ilustración 13 Top de eventos por sedes Access Point

Durante el mes de noviembre se evidencia que la sede con mayor número de eventos relacionados con Access Point es Popayán, con 4 casos que representa el 30,77% del total de los casos, conservando el primer lugar en el TOP. Causa predominante: actividad programada con 3 de los 4 casos y el restante por falla de energía.

Le sigue Tunja y Yopal con 2 casos cada una, representando el 30.76% en conjunto, Causa: los 2 casos de Tunja por falla de energía y los 2 casos de Yopal por Intermitencia/Lentitud en la red.

Las sedes Villavicencio, Montería, Chía, Barrancabermeja y Sincelejo reportan 1 caso cada una, que sumados en conjunto representan el 38,45% del total de los casos para esta categoría. Sincelejo, Chía y Barrancabermeja registraron eventos por Intermitencia/Lentitud en la red, mientras que Villavicencio y Montería registraron eventos por Bloqueo de Dispositivo, resueltos mediante reinicio físico.

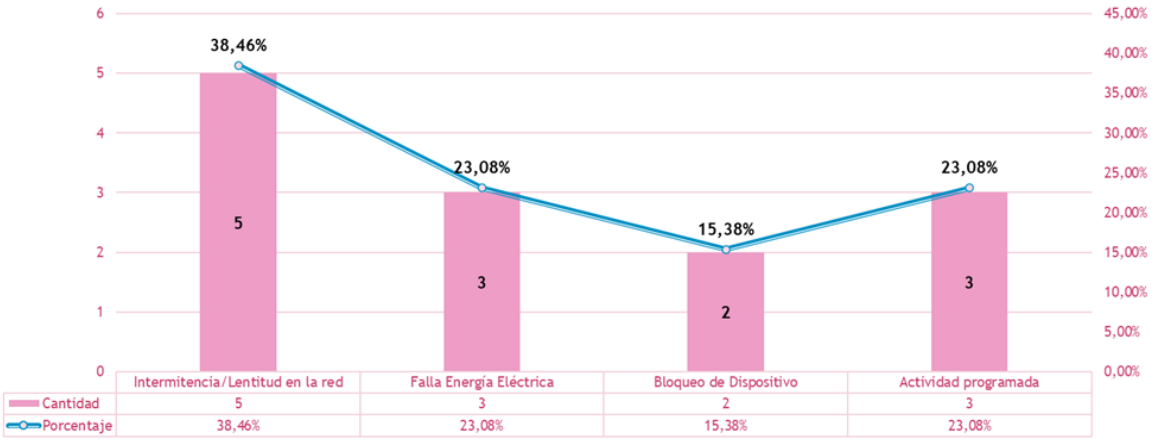


Ilustración 14 15Top de causas por sedes Access point

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

El 38,46% de los incidentes en APs (5 de 13) están directamente relacionados con Intermitencia/Lentitud en la red y el 23,08% (3 de 13) fallas eléctricas.

El 23,08% de los casos (3 de 13) corresponden a actividad programada, ya que el dispositivo se movió de lugar. Por otro lado, se tienen dos eventos por bloqueo de dispositivo, uno de la sede Villavicencio el cual se ajusta cableado y sube la alarma y el caso restante en la sede de Montería también por bloqueo de dispositivo el cual se soluciona reiniciando el dispositivo.

Starlink

Durante el mes de noviembre se gestionaron 97 incidentes relacionados con equipos de red Starlink en diferentes sedes a nivel nacional, los cuales representan el 20% del total de los casos.

Las sedes que puntean con mayor número de eventos por Desconexión/apagado Físico de Equipos en Sede son: Sabana Larga con 17 casos, Puerto Carreño con 16 casos, Puerto Lopez con 11 casos y Curumani con 10 casos. En estas sedes los funcionarios por falta de mecanismos de protección ante picos de energía prefieren realizar el apagado de los dispositivos.

Las sedes con mayor número de eventos por Falla Energía Eléctrica son Puerto Carreño con 6 casos, Bahía Solano con 5 casos, Rio Sucio con 5 casos. Lo que evidencia vulnerabilidad en la infraestructura energética local. Se recomienda evaluar la implementación de sistemas de respaldo energético (UPS, estabilizadores) para mitigar estos eventos.

Mitú es la sede con mayor número de eventos registrados por Intermitencia/Lentitud en la red ya que registra 4 eventos, evidenciando una inactividad del servicio recurrente en comparación con las demás sedes durante el mes por la misma categoría.

Bahia Solano registra un evento por falla en la red proveedor y el cual registra en estado cerrado.

Durante el mes de noviembre se pudo observar que la falla en dichos puntos con este dispositivo Starlink se debió a efectos climáticos y por energía eléctrica, lo que ocasiono constantes caídas en este servicio y esto causa mucha intermitencia en los puntos que manejan esta tecnología.

Hay casos que se evidenciaron durante el horario no hábil y, por lo tanto, no se determinaron las causas reales de las alarmas, debido a que estas subieron a los pocos minutos; estas fallas se atribuyen a intermitencias causadas por malas condiciones climáticas que del mismo modo afectan el servicio de energía.
Las sedes que puntean con mayor número de eventos por Desconexión/apagado Físico de Equipos en Sede son: Sabana Larga con 17 casos, Puerto Carreño con 16 casos, Puerto Lopez con 11 casos y Curumani con 10 casos. En estas sedes los funcionarios por falta de mecanismos de protección ante picos de energía prefieren realizar el apagado de los dispositivos.

Las sedes con mayor número de eventos por Falla Energía Eléctrica son Puerto Carreño con 6 casos, Bahía Solano con 5 casos, Rio Sucio con 5 casos.
Mitú es la sede con mayor número de eventos registrados por Intermitencia/Lentitud en la red ya que registra 4 eventos, evidenciando una inactividad del servicio recurrente en comparación con las demás sedes durante el mes por la misma categoría.
Bahia Solano registra un evento por falla en la red proveedor y el cual registra en estado cerrado.
Durante el mes de noviembre se pudo observar que la falla en dichos puntos con este dispositivo Starlink se debió a efectos climáticos y por energía eléctrica, lo que ocasiono constantes caídas en este servicio y esto causa mucha intermitencia en los puntos que manejan esta tecnología.

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

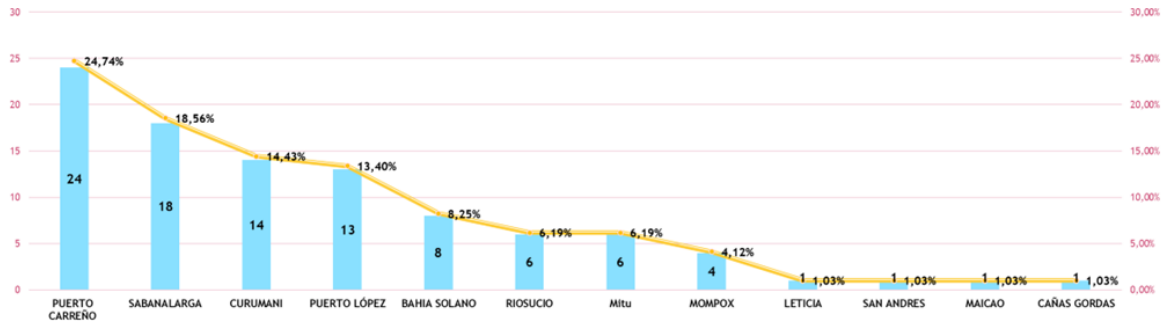


Ilustración 16 Top de eventos por sedes Starlink

Para el mes de noviembre el TOP 10 de las sedes con mayor número de eventos generados para la categoría de Starlink fueron Puerto Carreño con 24 eventos, representando un 24,74%, la cual puntea en primer lugar. Sabana Larga con 18 casos representando 18,56 de los casos. Curumani con 14 casos, representando el 14,43% de los casos. Puerto López con 13 casos, lo cual representa el 13,40% de los casos. Bahía Solano con 8 casos, representando el 8,25% de los casos. Rio Sucio y Mitú suman en conjunto 12 casos, representando el 12,38% de los casos. Mompox con 4 casos, representando el 4,12% de los casos. Por otro lado, se tienen las sedes con muy bajo índice de eventos durante el mes como son Leticia, San Andrés, Maicao y Cañas Gordas que suman en conjunto 4 casos, representando el 4,12% de los casos.

Las fallas Desconexión/apagado Físico de Equipos en Sede son la causa predominante con 57 casos en la mayoría de las sedes del TOP de equipos Starlink, representando el 58,76% del total de los casos para esta categoría, lo que resalta la necesidad de mejorar la infraestructura local o implementar soluciones autónomas.

Sin embargo, en este mes Puerto Carreño puntea con mayor número de eventos (16 casos) relacionados con Desconexión/apagado Físico de Equipos en Sede, esto por temas de prevención por fluctuaciones constantes en el servicio de energía, seguido por Falla Energía Eléctrica (6 casos) y por último,2 casos por Intermitencia/Lentitud en la red estas ocasionadas por interrupción en el servicio durante pocos minutos sin diagnostico en sitio. Por lo cual se recomienda contemplar la posibilidad de sistemas de respaldos robustos.

Por otro lado, tenemos dos sedes como Mitú y Cañas Gordas que reportan en el TOP por actividad programada. En la sede Mitú hubo un traslado, mientras que en Cañas Gordas la funcionaria estuvo fuera del sitio por un tiempo.



Ilustración 17 Top de causas por sedes Starlink

Las sedes que puntean con mayor número de eventos por Desconexión/apagado Físico de Equipos en Sede son: Sabana Larga con 17 casos, Puerto Carreño con 16 casos, Puerto

Lopez con 11 casos y Curumani con 10 casos. En estas sedes los funcionarios por falta de mecanismos de protección ante picos de energía prefieren realizar el apagado de los dispositivos.

Las sedes con mayor número de eventos por Falla Energía Eléctrica son Puerto Carreño con 6 casos, Bahía Solano con 5 casos, Rio Sucio con 5 casos. Lo que evidencia vulnerabilidad en la infraestructura energética local. Se recomienda evaluar la implementación de sistemas de respaldo energético (UPS, estabilizadores) para mitigar estos eventos.

Mitú es la sede con mayor número de eventos registrados por Intermitencia/Lentitud en la red ya que registra 4 eventos, evidenciando una inactividad del servicio recurrente en comparación con las demás sedes durante el mes por la misma categoría.

Bahia Solano registra un evento por falla en la red proveedor y el cual registra en estado cerrado.

Durante el mes de noviembre se pudo observar que la falla en dichos puntos con este dispositivo Starlink se debió a efectos climáticos y por energía eléctrica, lo que ocasiono constantes caídas en este servicio y esto causa mucha intermitencia en los puntos que manejan esta tecnología.

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

Fortigate

Durante noviembre se gestionaron 95 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 tercer lugar.

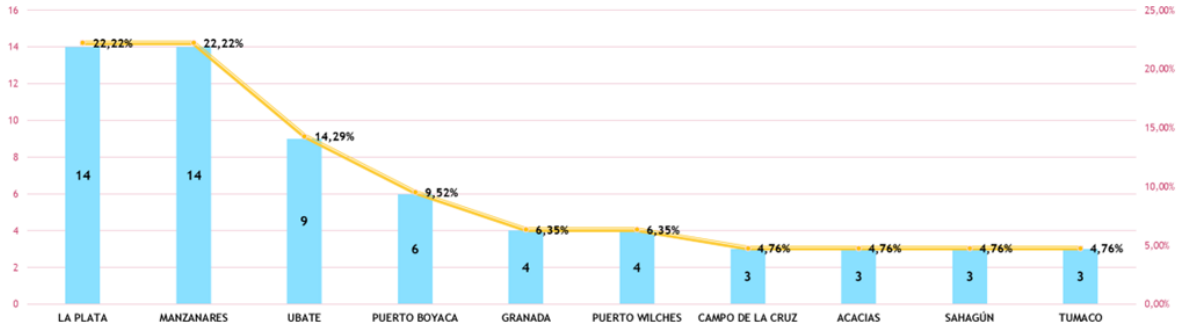


Ilustración 18 Top de incidentes por sedes fortigate

Durante el mes de noviembre se registraron 43 casos que fueron escalados y gestionados con proveedor ETB y TIGO de los cuales quedan 41 (95%) que registran en estado solucionado o cerrado y 2 (5%) en estado suspendido o en espera de RFO.
Durante el mes de noviembre se registraron 43 casos que fueron escalados y gestionados con proveedor ETB y TIGO de los cuales quedan 41 (95%) que registran en estado solucionado o cerrado y 2 (5%) en estado suspendido o en espera de RFO.
Durante el análisis del comportamiento de la red SD-WAN en el mes de noviembre, se identificó una mayor frecuencia de afectación en las sedes de La Plata la cual pasa al primer lugar con 22,22% (14) y al igual empata con Manzanares, manteniendo su lugar en los últimos 2 meses consecutivamente, con un 22,22% (14), seguido por Ubaté con un 14,29% (9), Ambas sedes (La Plata y Manzanares) presentan una alta tasa de eventos críticos asociados a desconexión/apagado de equipos, mientras que Ubaté registra 5 eventos por Intermitencia/Lentitud en la red y 4 eventos por falla de energía eléctrica, factores que afectan directamente la disponibilidad de los enlaces SD-WAN.

Por otro lado, Puerto Boyacá con un 9,52% (6 casos) 4 por falla de energía y 2 por Intermitencia/Lentitud en la red. Granada y Puerto Wilches por su parte presentan sumados 8 casos, representando el 12,7% del total de los casos generados durante el mes siendo falla de energía (4 casos) la causa más frecuente y como segunda causa (3 casos) por Intermitencia/Lentitud en la red y el caso restante por Desconexión/apagado Físico de Equipos en Sede.

Las sedes restantes del TOP como Campo de la Cruz, Acacias, Sahagún y Tumaco suman en conjunto 12 casos (19,04%) de los cuales 8 fueron categorizados como falla de energía eléctrica, 2 categorizados por Intermitencia/Lentitud en la red, 1 por falla en red de proveedor y 1 por Desconexión/apagado Físico de Equipos en Sede.

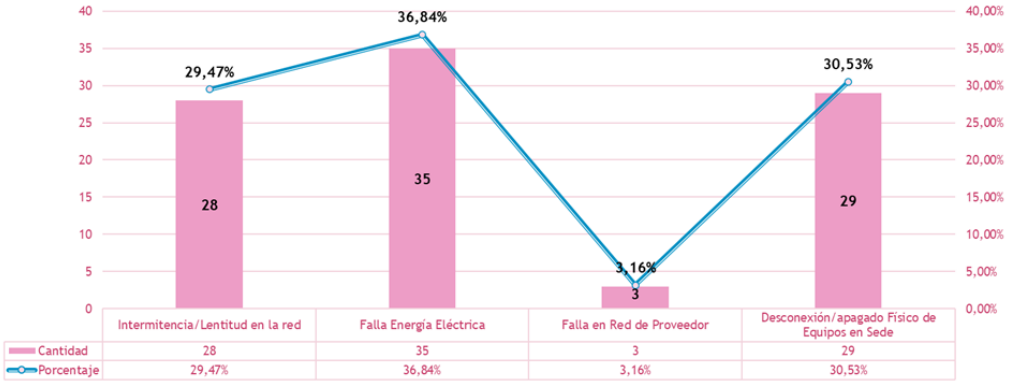


Ilustración 19 Top de causas por sedes fortigate

Durante el mes de noviembre, los dispositivos SD-WAN presentaron una tasa alta en cuanto a la causa de Falla Energía Eléctrica con 35 eventos registrados, representados con el 36,84% de total de los casos para esta categoría. Estas ocasionadas por condiciones climáticas adversas, validadas por el soporte en sitio y algunas fuera de horario hábil.

Un 30,53% (29 casos) de las alarmas correspondieron a Desconexión/apagado Físico de Equipos en Sede que se atribuyen al apagado de los equipos por parte de los funcionarios al salir de labores para evitar daños por picos altos en la energía.

Un 29,47% (28 casos) de los eventos registrados durante el mes a Intermitencia/Lentitud en la red que se atribuyen a interrupciones iguales o menores a 30 y 20 minutos de duración en horario hábil y otros en horario no hábil.

Por otro lado, el 3,16% (3) de los eventos registrados durante el mes se atribuyeron a Falla en Red de Proveedor por fallas y daños en su infraestructura y en la infraestructura del proveedor de UM.

Casos Escalados a Proveedor de Telecomunicaciones

Durante el mes de noviembre se registraron 43 casos que fueron escalados y gestionados con proveedor ETB y TIGO de los cuales quedan 41 (95%) que registran en estado solucionado o cerrado y 2 (5%) en estado suspendido o en espera de RFO.

Servicios Centrales

Servidores Windows

Durante noviembre, se gestionaron 30 incidentes asociados a servidores Windows, equivalentes al 6% del total de casos registrados durante el mes.

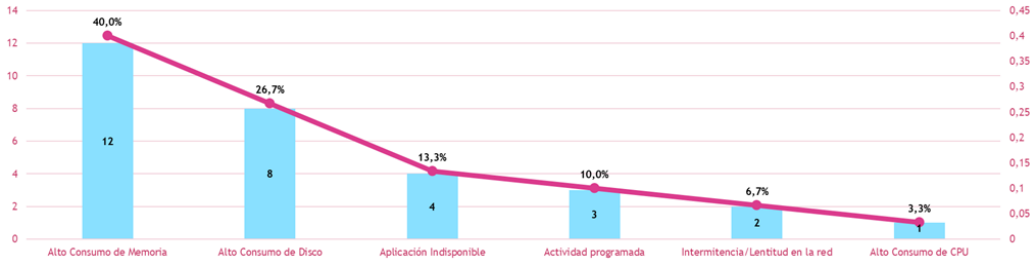


Ilustración 20 Top de eventos Windows

El alto consumo de memoria es el principal causante de eventos en el sistema, representando el 40% del total de incidentes. Para este mes el consumo en disco baja a segundo lugar después de varios meses encabezando la gráfica, con un 26,7%; aplicación indisponible con 4 casos ocupa el tercer lugar, representando el 13,3%, seguido ocupando el cuarto lugar esta actividad programada representa el 10%, el cual se evidencia que disminuyo a la mitad en comparación con meses anteriores.

Otros factores como consumo de CPU y lentitud en la red representan el 10% de los casos, por lo tanto, enfocar las acciones correctivas en las causas principales permitirá lograr una reducción significativa en la ocurrencia de incidentes y un mejoramiento clave en la estabilidad operativa del sistema.

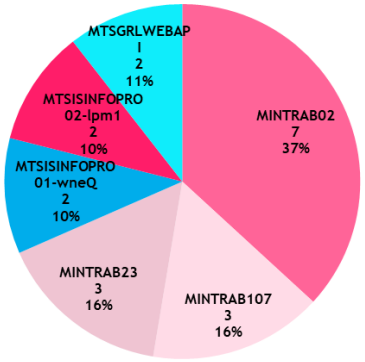


Ilustración 21 Top de servidores Windows

El servidor MINTRABO2 para este mes representan el 37% (7 casos) del total de los casos para esta categoría, se reporta que en su mayoría los casos están relacionados a consumo de memoria; los servidores MINTRAB107 y MINTRAB23 tienen la misma participación en la gráfica ocupando el segundo lugar con un 16%, se evidencia que sus casos están relacionados a consumo de memoria y disco principalmente. El resto de los servidores tienen una participación menor del 10%.
Se evidencia que, de los 30 eventos registrados durante el mes de noviembre, quedan 29 eventos en estado cerrado y solucionado, 1 en estado suspendido y escalados al especialista a cargo. Lo cual refleja una efectiva y oportuna gestión por parte de los especialistas con los eventos reportados, reflejando un porcentaje del 97% de gestión de los casos.
Se realiza el respetivo seguimiento a los casos que se encuentra abiertos y se resuma que:

- Caso en Aranda RF-168695, está relacionado al servidor MTSGRLWEBAPI por alto consumo de disco, este caso se encuentra en suspendido y a espera de validaciones por parte del especialista, no cuenta con actualización.

Servidores Linux

Durante noviembre, el Centro de Operaciones de Red (NOC) gestionó 6 incidentes asociados a servidores Linux, equivalentes al 1% del total de casos registrados en el mes.

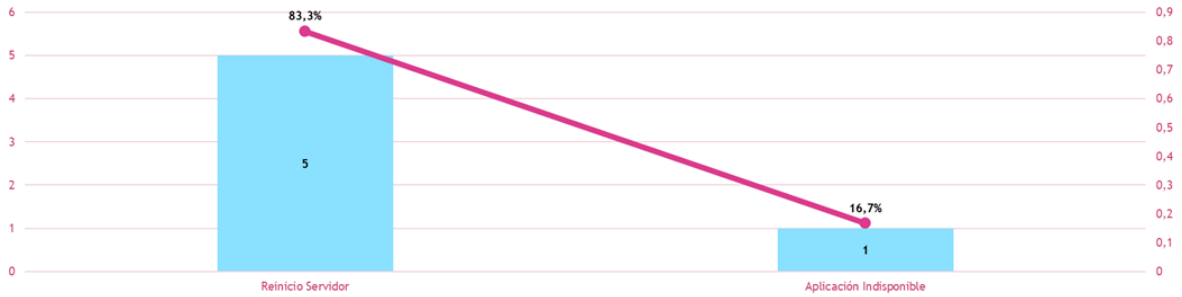


Ilustración 22 Top de causas eventos linux

Las causas principales de los eventos registrados muestran que la gran mayoría están asociadas a factores conocidos y potencialmente controlables. El reinicio del servidor representando un 83% y aplicación indisponible representando el 16% del total.

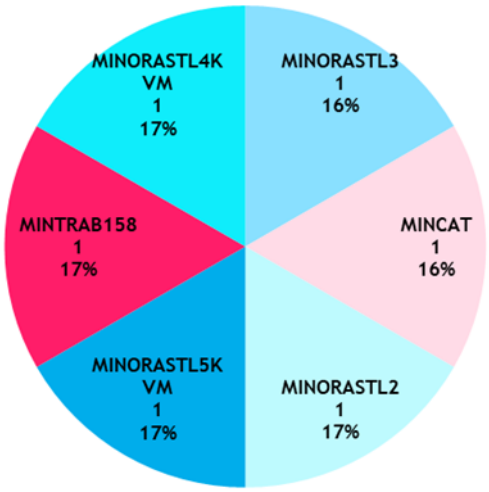
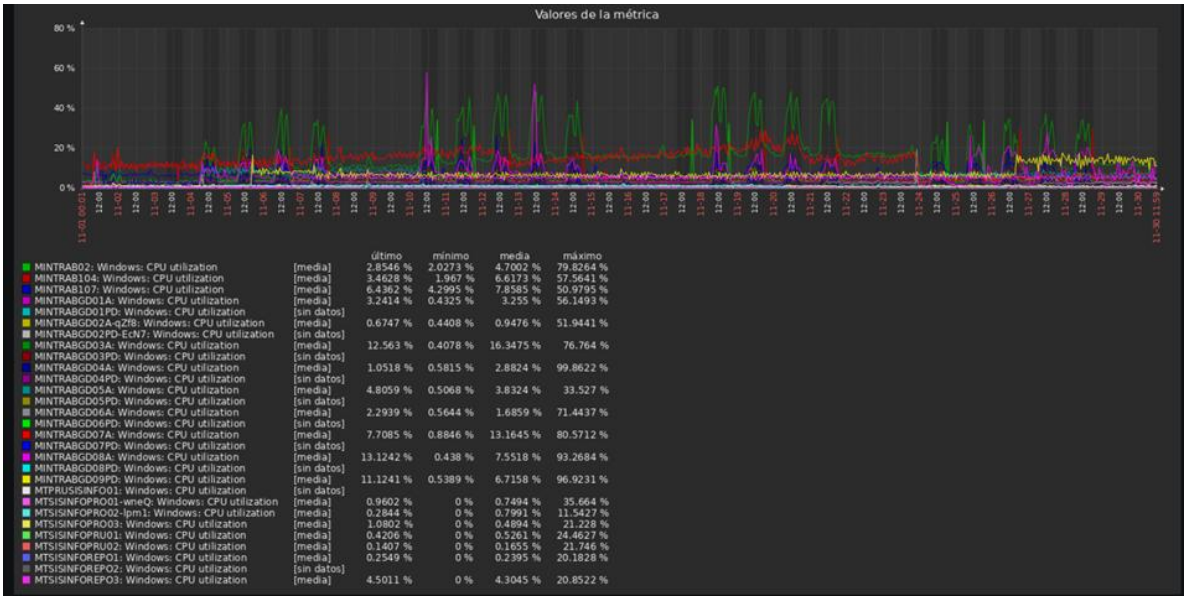


Ilustración 23 Top de servidores linux

Para este mes se observa que los 6 casos reportados tienen un servidor diferente relacionado, por lo tanto, cada servidor tiene la misma ocupación en la gráfica. Todos los servidores presentaron reinicios para noviembre menos el servidor MINTRAB158 el cual reporta indisponibilidad, sin embargo, no se documenta el motivo.

Gráficas de CPU zabbix de todo el mes sobre servidores

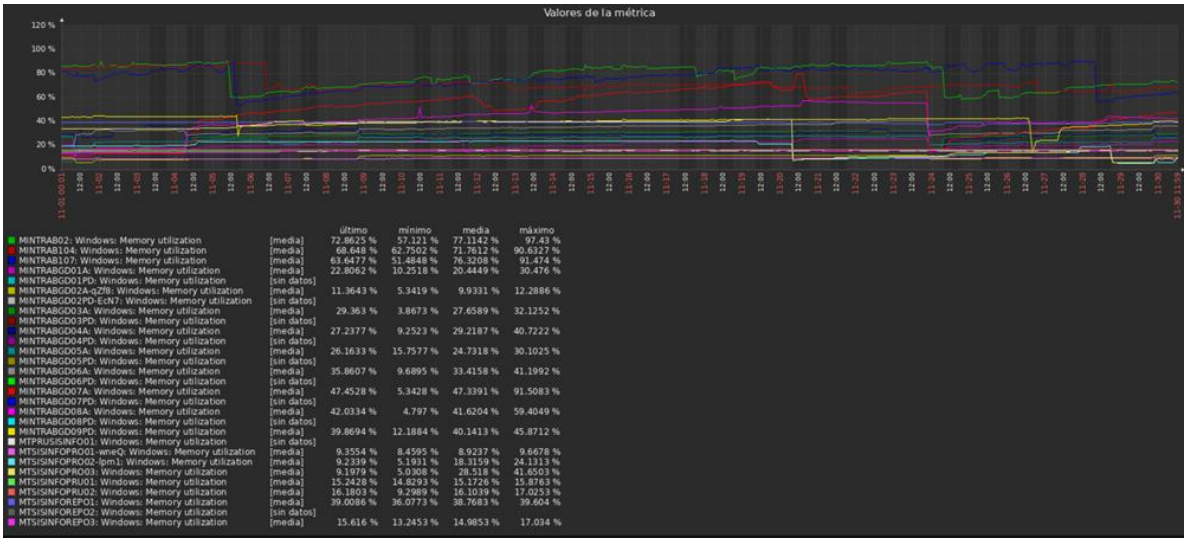


A continuación, se relaciona el TOP 5 de los servidores que por media tuvieron más utilización de recursos de CPU durante el mes.

CPU

MINTRABGD03A 16.3475%
MINTRABGD07A 13.1645%
MINTRAB107 7.8585%
MINTRABGD08A 7.5518%
MINTRABGD09PD 6.7158%

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

MINTRAB02 77.1142%
MINTRAB107 76.3208%
MINTRAB104 71.7612%
MINTRABGD07A 47.3391%
MINTRABGD08A 41.6204%

Datacenter (Cali - Bogotá)

Durante el mes de noviembre se evidencia 1 evento relacionado al CXV-SWCORE1-RAT42-U44-8360, sin embargo, según la documentación suministrada por el Ing en Redes, se menciona que no se genera afectación en los servicios dado que la alerta se originó por bloqueo de ICMP en el firewall lo que ocasionó que el zabbix no pudiera monitorear los equipos, se realizó ajuste con el grupo del SOC y con apoyo del proveedor solventando la alerta.

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 noviembre de 2025.

Servidores

Cantidad de dispositivos	Disponibilidad consolidada
118	99,93%

Tabla 17 Consolidado disponibilidad de servidores

Directorio Activo

Cantidad de dispositivos	Disponibilidad consolidada
3	100,00%

Tabla 18 Consolidado disponibilidad de Directorio Activo

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

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

Tabla 19 Desagregado de Disponibilidad Directorio Activo

Datacenter Principal

Cantidad de dispositivos	Disponibilidad consolidada
8	100,00%

Tabla 20 Consolidado disponibilidad de equipos Datacenter principal

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

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

CXV-FG-600F-SDWAN-HUB02	100,00%

Tabla 21 Desagregado de Disponibilidad Datacenter Principal

Datacenter Alterno

Cantidad de dispositivos	Disponibilidad consolidada
4	100%

Tabla 22 Consolidado disponibilidad de equipos Datacenter alterno

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

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

Tabla 23 Desagregado Disponibilidad de equipos Datacenter alterno

Redes y conectividad

Cantidad de dispositivos	Disponibilidad consolidada
522	96,14%

Tabla 24 Consolidado disponibilidad de equipos redes y conectividad

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

Seguridad

Cantidad de dispositivos	Disponibilidad consolidada
6	100,00%

Tabla 25 Consolidado disponibilidad de equipos de seguridad

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

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

Tabla 26 Disponibilidad de equipos Seguridad de la Información

Telefonía

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

Tabla 27 Consolidado disponibilidad de equipos de telefonía

Antivirus

Cantidad de dispositivos	Disponibilidad consolidada
1	100%

Tabla 28 Consolidado disponibilidad de plataforma antivirus

Actividades de la Practica de Disponibilidad:

- Seguimiento a los resultados de los cambios presentados en el CAB por partes de especialistas que afecten la disponibilidad del servicio.
- 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 25 han sido ejecutadas durante el 2025 por los servicios de los servicios Conectividad, Seguridad de la Información y Telefonía IP, se encuentran ejecutadas y aprobadas en los CAB.

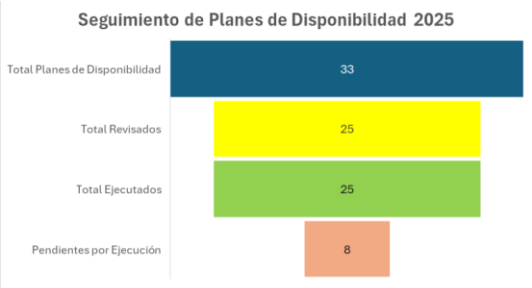


Ilustración 24 Seguimiento Pruebas de Disponibilidad

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 noviembre de 2025.

Actividades en curso:

Revisión de los RFC ejecutados durante el periodo, para los cuales (27) cambios fueron aprobados su cierre, ya que cuentan con las evidencias completas de los planes de Pruebas Previas y Posteriores, al corte del 30/11/2025se encuentra (9) casos abiertos (en proceso

de revisión o en implementación) a la espera de entrega de las evidencias por parte los especialistas.

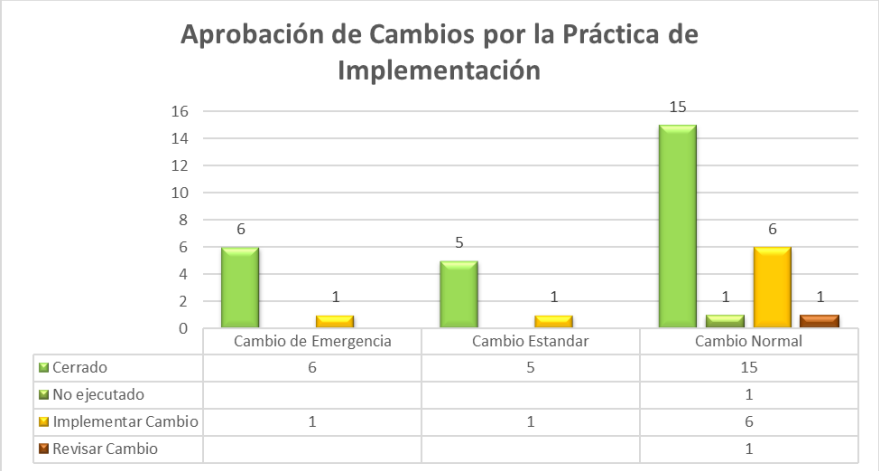


Ilustración 25 Seguimiento Práctica Implementación

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

Seguimiento 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 noviembre, 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 noviembre, en el Ministerio del trabajo a la MDS ingresaron 295 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	161	161	161	0	0	0
COL - mintrabajo-Impresora	53	53	53	0	0	0
COL - Mintrabajo-Gestor-documental	47	47	47	0	0	0
COL - Mintrabajo-office365	34	34	34	0	0	0
TOTAL	295	295	295	0	0	0

Tabla 29 Llamadas Atendida por la Mesa de Servicio

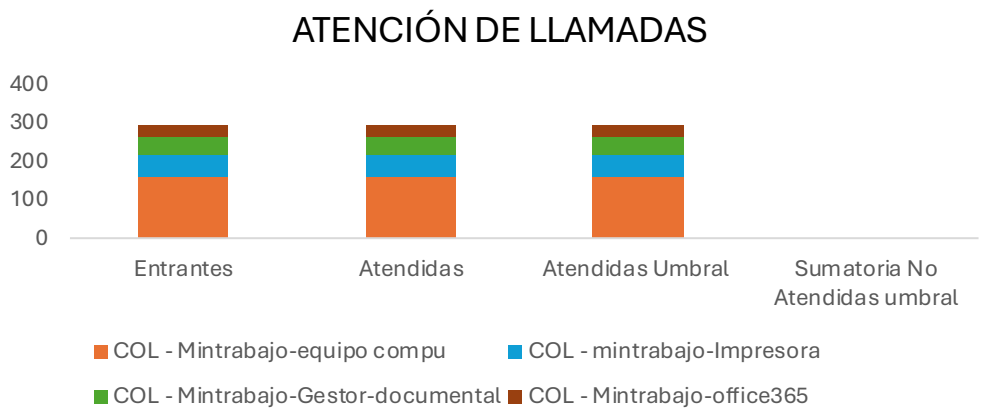


Ilustración 26 Llamadas Atendidas

El servicio más solicitado a través de la atención de llamadas es: Equipo de cómputo con 161 llamadas entrantes, se atendieron 295 solicitudes.

- **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_noviembre* pestaña *categoría.*

- **Análisis de Casos Anulados por Servicio**

Para este periodo se tiene 3 casos anulados de los siguientes servicios:

CASOS ANULADOS	TOTAL
Creación de Servicio	3
Total general	**3**

Tabla 30 Casos anulados por Servicio

- **Creación de Servicio:** se tiene casos 3 de Solicitudes de Mantenimientos de Equipos Colombia XV.

En comparación del mes anterior se evidenció una disminución del 66,66%, que corresponde a 6 casos.

- **Análisis de Casos Suspendidos por Servicio**

Para el periodo del mes de noviembre, se dio una disminución de casos suspendidos del 9,90% que corresponde a 10 casos para un total de este mes de 91 casos de los siguientes servicios:

CASOS SUSPENDIDOS	TOTAL
Soporte Microinformática	53
Administración de servidores	9
Redes y Conectividad	9
Seguridad informática	8

Energía Eléctrica Regulada - UPS	6
Aplicaciones Especializadas	5
Administración de Bases de Datos	1
Total general	**91**

Tabla 31 Casos Suspendidos por Servicio

- **Soporte Microinformática:** 53 casos suspendidos debido a que se ha solicitado información complementaria a los usuarios o están pendientes por disponibilidad del usuario: Cambio Tóner con 11 casos, Backup, Asesoría – Consulta y Solicitud Backup, con 6 casos cada categoría, Equipo Escritorio , Configuración , Devolución de equipo (portátil o PC) 5 casos cada categoría, Equipo Periférico , Asignación de equipo (portátil o PC) y Equipo Portátil con 2 casos cada categoría Mantenimiento preventivo , Cambio de unidad de imagen e Instalación - Configuración con 1 caso cada categoría.
- **Administración de servidores**: 9 casos suspendidos por: Inactivar usuario con 6 casos, Servidor Windows, Configuración, Configuración MFA con 1 caso de cada categoría.

- **Redes y Conectividad:** 9 casos suspendidos debido a: Router con 4 casos, Sin servicio 1 caso, degradación, Starlink , equipos conectividad internet y asesoría consulta con 1 caso de cada categoría.

- **Seguridad informática:** 8 casos suspendidos: Configuración consola 3 casos, Validación Habilitación Puertos USB, permitir accesos 2 casos de cada categoría y Análisis de Malware con 1 caso.

- **Energía Eléctrica Regulada – UPS:** 6 casos suspendidos debido a: UPS 5 casos y Modo By Pass 1 caso.
  .
- **Aplicaciones Especializadas:** 5 casos suspendidos debido a: depuración bandeja 2 casos, asignación modificación-roles, relanzamiento y asesoría-consulta 1 caso de cada categoría.

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

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

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

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

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

Requerimientos solucionados por Soporte en sitio Bogotá: en el mes de noviembre quedaron 7 requerimientos discriminados de la siguiente manera:

REQUERIMIENTOS SOLUCIONADOS POR SOPORTE EN SITIO	TOTAL
Cargue de papel en impresora	2
Accesos por fuerza bruta	1
Prestamo	1
Actualización Bios	1
Cambiar contraseña	1
Instalar - Configurar	1
Total general	**7**

Tabla 32 Requerimientos Solucionados por Soporte en Sitio



Ilustración 27 Requerimientos Solucionados por Soporte en Sitio

Requerimientos solucionados por Soportes Territoriales: Para el mes de noviembre quedaron 4 casos en estado solucionado de las territoriales.

REQUERIMIENTOS SOLUCIONADOS POR TERRITORIALES	TOTAL
Cargue de papel en impresora	2
Instalación - Configuración	1
Asesoría - Consulta	1
Total, general	**4**

Tabla 33 Requerimientos Solucionados por Territoriales



Ilustración 28 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 noviembre se cerraron 1000 casos, discriminados así: Asesoría – Consulta con 308 casos, Aumento de cuota con 307, ,Cambiar contraseña con 146 casos, Creación de usuario 63 casos, cambio de grupo 34 casos, Inactivar usuario con 19 casos, Habilitar usuario, Backup 18 casos cada categoría, Lentitud gestor con 32 casos y Cambio de grupo con 25 casos cada Categoría, instalación y configuración VPN con 11 casos, Configuración 8 casos.

En comparación del mes anterior se nota un aumento de casos cerrados por la mesa de un 17.8% que es equivalente a 178 casos.

CERRADOS POR LA MESA DE SERVICIOS	TOTAL
Asesoría - Consulta	308
Aumento de cuota	307
Cambiar contraseña	146
Creación de usuario	63
Cambio de grupo	34
Inactivar usuario	19
Habilitar usuario	18
Backup	18
Instalación y configuración VPN	11
Configuración	8
Lentitud gestor	6
Instalación - Configuración	5
Configuración MFA	4
Falla radicación	4
Asignación de licencia	4
Soporte Aplicaciones Office 365	3
Relanzamiento	3
Traslado - Movimiento	3

Asignación de equipo (portátil o PC)	3
Validación Habilitación Puertos USB	3
Reportar Solicitud/Falla	3
Préstamo	2
Envío y recepción de correos	2
Asignación - Modificación Roles	2
Solicitud Backup	2
Depuración Bandeja	2
Solicitud instalación	2
Falla Funcional	2
Desbloquear usuario	2
No imprime	2
Análisis Equipo de Computo	1
Modificar usuarios	1
Conectar a red Mintrabajo	1
Asignación de permisos	1
Falla Cargue página web	1
Mantenimiento preventivo	1
No funciona	1
Accesos por fuerza bruta	1
Análisis de evento	1
Total general	**1000**

Tabla 34 Casos Cerrados por la Mesa de Servicios

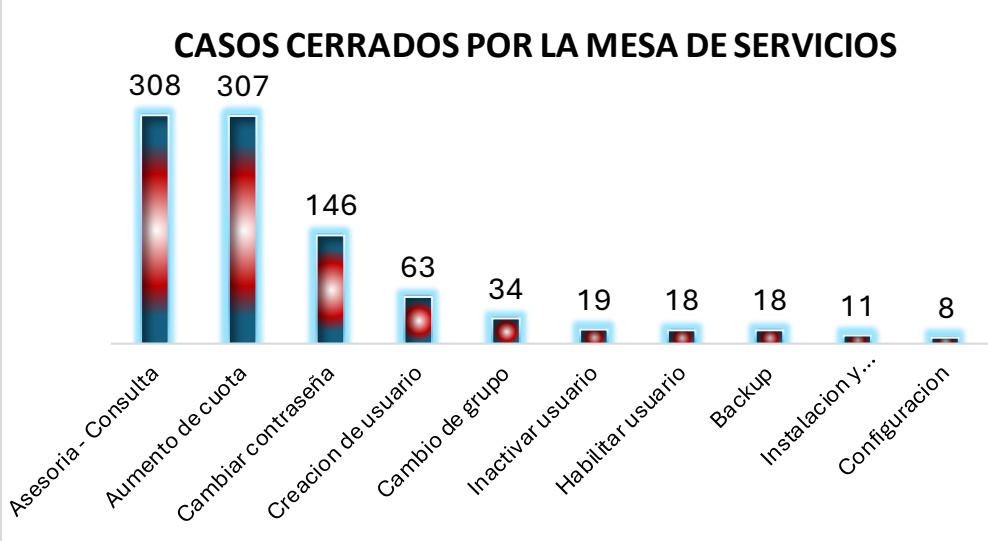


Ilustración 29 Requerimientos Solucionados por Territoriales

Casos Cerrados por Soporte en Sitio: Se indica el top 10 de Requerimientos cerrados por soporte en sitio, para el mes de noviembre se cerraron 1512 casos discriminados así: Instalación - Configuración con 400 casos, Cargue de papel en impresora con 335 casos, Asesoría - Consulta con 179 casos, Configuración con 136 casos, No imprime 67, Préstamo 49 casos, Soporte Aplicaciones Office 365 con 33 casos, Asignación de equipo (portátil o PC) , Solicitud Backup 22 casos de cada categoría y Devolución de equipo (portátil o PC)

21 casos, a comparación con el mes anterior se tiene una disminución del 17,91% que corresponde a 330 casos.

CERRADOS POR SOPORTE EN SITIO	TOTAL
Instalación - Configuración	400
Cargue de papel en impresora	335
Asesoría - Consulta	179
Configuración	136
No imprime	67
Préstamo	49
Soporte Aplicaciones Office 365	33
Asignación de equipo (portátil o PC)	22
Solicitud Backup	22
Devolución de equipo (portátil o PC)	21
Actualización Bios	20
Instalación y configuración VPN	19
Conectar a red Mintrabajo	17
Borrado seguro Portátil	16
Asesoría PDF	15
Cambiar contraseña	14
Cambio Tóner	11
Asesoría Excel	11
Aumento de cuota	11
Atasco	10
Asesoría Word	10
Instalación-Desinstalación	10
Eliminar Hostname	9
Conectar a red Invitados	9
Envío y recepción de correos	7
Validación Habilitación Puertos USB	6
Falla - Error conexión a red	5
Traslado - Movimiento	5
Mantenimiento preventivo	4
Análisis de Malware	3
Crear Backups	3
Falla - error	3
Instalación - Configuración	3
Lentitud - Bloqueo	2
Instalar - Configurar	2
Asignar Radicado TYS	2
Configuración de PST	2
Falla Aplicaciones Office 365	2
Borrado seguro PC	1
Asesoría Power Point	1
Administración de equipos	1
Revisar correo malicioso	1
Solicitud instalación	1
Solicitud depuración carpeta	1
Aprovisionamiento	1
Actualización	1
Falla Funcional	1
Equipo Periférico	1

Falla Aplicativo	1
Análisis Equipo de Computo	1
Configuración MFA	1
Falla	1
Solicitud de cambio	1
Falla Excel	1
Análisis de Correos	1
Total general	**1512**

Tabla 35 Casos Cerrados por Soporte en Sitio

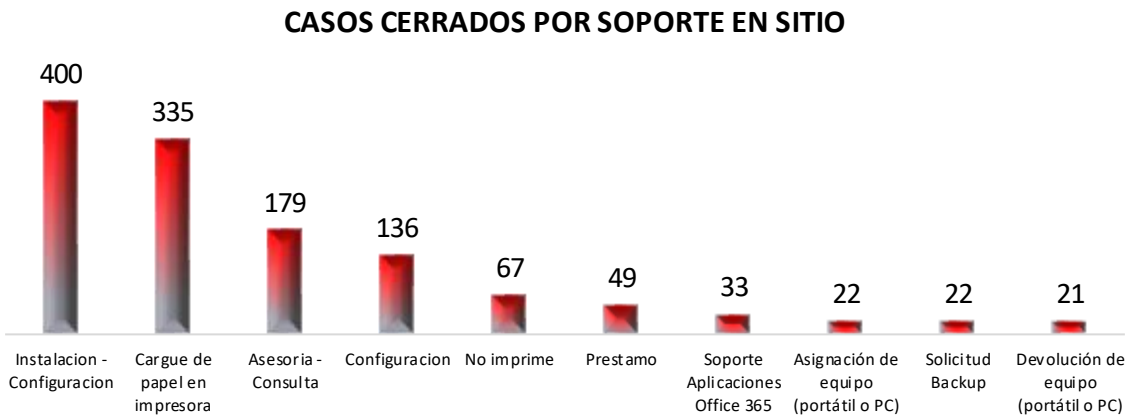


Ilustración 30 Casos Cerrados por Soporte en Sitio

Casos Cerrados por soporte en sitio Territoriales: Se indica el top 10 de Requerimientos cerrados por soporte en Territorio, para el mes de noviembre se cerraron 2110 casos discriminados así: , Instalación - Configuración con 749 casos, Asesoría – Consulta con 304 casos, Cargue de papel en impresora con 207 casos, Actualización BIOS con 98 casos, , Mantenimiento preventivo con 97 casos, Configuración con 95 casos, Asesoría PDF con 83 casos, Asesoría Excel con 61 casos, Soporte Aplicaciones Office 365 con 36 casos, Asesoría Word con 35 casos.

CERRADOS POR TERRITORIALES	TOTAL
Instalación - Configuración	749
asesoría - Consulta	304
Cargue de papel en impresora	207
Actualización Bios	98
Mantenimiento preventivo	97
Configuración	95
Asesoría PDF	83
Asesoría Excel	61
Soporte Aplicaciones Office 365	36
Asesoría Word	35
Copia de información	33
Instalación-Desinstalación	28
No imprime	25
préstamo	22
Validación Habilitación Puertos USB	19

Asignación de equipo (portátil o PC)	18
Instalación	18
Solicitud instalación	18
Instalación y configuración VPN	16
Cambio tóner	15
Actualización	13
Aumento de cuota	12
Conectar a red Mintrabajo	9
Atasco	8
Falla - Error conexión a red	8
Solicitud Backup	7
Traslado - Movimiento	6
Borrado seguro PC	6
Lentitud	5
Cambiar contraseña	5
Devolución de equipo (portátil o PC)	5
Revisar correo malicioso	5
asesoría Power Point	3
Impresora	3
Falla PDF	2
No enciende	2
Solicitud de cambio	2
Falla Word	2
Instalación - configuración	2
Análisis de Malware	2
Asesoría en ZIP	2
Sin servicio	2
Instalar - Configurar	2
Office 365	1
Falla al cargar archivos	1
Equipo Conectividad internet	1
Permitir acceso	1
Asignar Radicado TYS	1
Falla - error	1
Desinstalación	1
Escaneo de activo	1
No Escanea	1
Lentitud gestor	1
Análisis de Correos	1
Backup	1
Falla aplicación	1
Falla Excel	1
Habilitar usuario	1
Reportar Solicitud/Falla	1
Informes y Reportes	1
Análisis de evento	1
Error sincronización	1
Configuración MFA	1
Total general	**2110**

Tabla 36 Top 10 Casos Cerrados por Soportes Territoriales

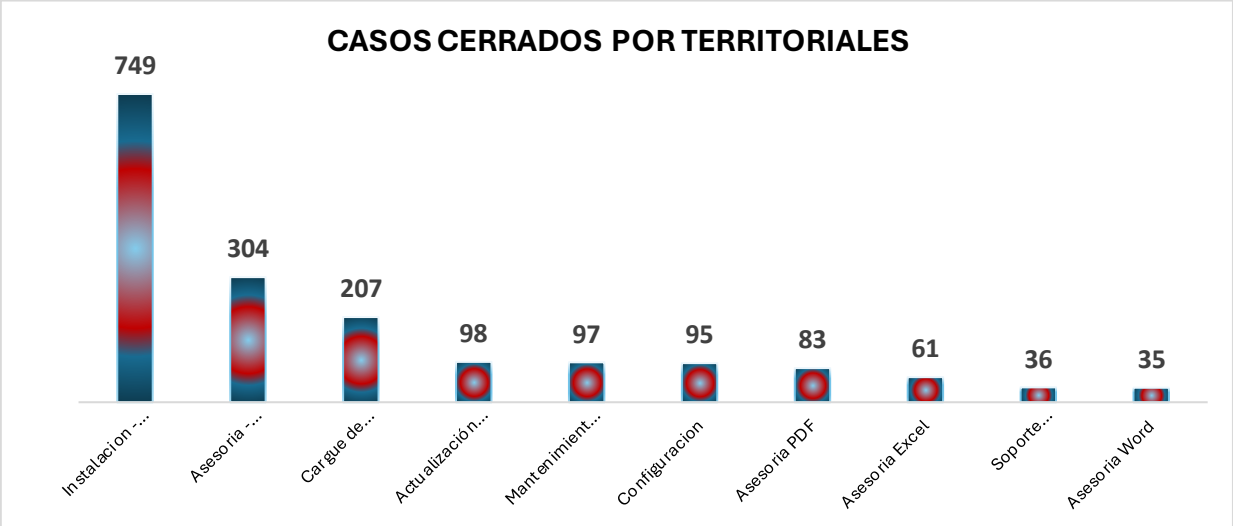


Ilustración 31 Casos Cerrados por Territoriales

- **Casos Atendidos a Usuarios VIPS**

Durante este periodo se crearon 1531 solicitudes para ser atendidas por soporte en sitio, de estas solicitudes se evidenciaron 35 casos creados para VIPS los cuales fueron atendidos y solucionados dentro de los ANS establecidos por la entidad, discriminados a continuación por tipo de caso:

TIPO DE CASO_VIPS	CUMPLIMIENTO	NO_CUMPLE	TOTAL
Incidents	1	0	1
Requerimiento	34	0	34
Total general	**35**	**0**	**35**

Tabla 37 Casos Atendidos usuarios VIPs

Se atendieron 1496 solicitudes para el resto de los usuarios discriminados así:

TIPO DE CASO-NO-VIPS	CUMPLIMIENTO	NO_CUMPLE	TOTAL
Incidentes	100	0	100
Requerimientos	1396	0	1396
Total general	**1496**	**0**	**1496**

Tabla 38 Casos Atendidos usuarios

- **Medio de Ingreso de Casos**

Durante el período ingresaron a la mesa de servicio 6707 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	3361
Correo SoporteMT	2058
Alarma Zabbix	978
Telefónico	283
Alarma Fortisiem	21
Portal Auto-Gestión	5
Case Creator Mesa de Servicios	1
Total general	**6707**

Tabla 39 Medios de Ingreso de Casos

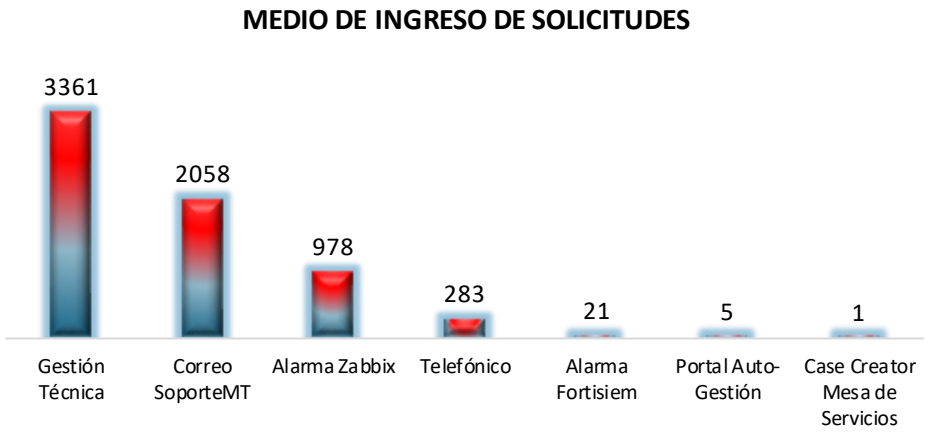


Ilustración 32 *Medio de ingreso solicitudes*

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

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

Durante el mes de noviembre 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.

Se continua con la actualización de Bios de los Equipos, en operación de la unión temporal.

Se realiza actualización de interfaz de las impresoras, se continua con el despliegue en sedes territoriales e inspecciones de trabajo.

Se inician los mantenimientos de las impresoras tanto en sede central como en las territoriales, con un avance del 10%, está actividad se continuara para el mes de diciembre.

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

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

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

Visita a 10 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 en 2132 casos, dentro de los que se destacan: Instalaciones - Configuraciones sobre aplicaciones de la línea base de software, Asesorías – Consultas, Cargues de Papel en las impresoras de las diferentes Sedes, Actualización de BIOS, Mantenimiento de Impresoras, Asesorías en PDF, Soporte a Aplicaciones 365 y Asesoría Word

Organización de cables de red y apoyo en la instalación de antenas starlink requeridas por los especialistas de redes y conectividad en las sedes Territoriales y las Inspecciones a cargo de los Soportes en sitio.

Se termina el proceso de actualización de la interfaz de las impresoras que se encuentran en las direcciones terririales de acuerdo con los lineamientos a nivel nacional.

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

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

Para el período se realizaron las siguientes visitas:

Mes	Territorial	Sede	Servicio	Descripción	Caso
Nov-25	Cauca	Popayan	Instalación de AP	Se realizan las labores correspondientes por parte del aliado para reubicación del AP logrando dar solución a los inconvenientes que se tenían con el equipo, los dos Access point dispuestos en la sede se dejaron operativos.	N/A
Nov-25	Vaupés	Mitu	Desmontar antena Stalink,traslado de compuatdores y RACK	El aliado hace presencia en la sede, atiende las siguientes acciones: -Realiza retiro de la antena Starlink ubicada en la azotea de la sede -Realiza desinstalación de dos equipos rack peueños y cámaras de grabación en sitio. -Se realiza desinstalación y embalaje de 3 equipos completos de escritorio Lenovo, 1 impresora marca Ricoh y 1 impresora marca HP	N/A
Nov-25	Norte de Santander	Los Patios	Actualización BIOS	Instalación y configuración de Impresora	RF-164919

Nov-25	Vaupés	Mitú	Instalar antena Starlink	Actualización de la BIOS en el equipo de la Inspección	N/A
Nov-25	San Andres	San Andres	Revisión de Internet, actualización de la impresora	Se coordina visita a la sede por parte del aliado para: -Revisión del correcto funcionamiento del Internet y la navegabilidad de los equipos de cómputo de la sede. -Apoyo para la actualización de la impresora de manera remota desde Bogotá y actualización del driver de la misma, con pruebas desde el PC de los usuarios. -Actualización de la BIOS de los equipos requeridos. -Reinstaalción de Agente Aranda en equipos de cómputo	N/A
Nov-25	Cauca	Santander de Quilichao	Mantenimiento de impresoras y revisión de equipos de cómputo	Se requiere desplazamiento de soporte en sitio para realizar el mantenimiento de la impresora y la revisión de equipos de cómputo para garantizar su correcto funcionamiento.	RF-167285
Nov-25	Caquetá	Florencia	Instalación antena Starlink	Se realiza instalación de antena Starlink como contingencia del servicio de conectividad cuando se presentan novedades con los enlaces de fibra de la DT.	N/A
Nov-25	Santander	Barbosa	Revisión de Internet, actualización de la impresora	Se coordina visita a la sede por parte del personal de Soporte en Sitio con el propósito de validar el funcionamiento del Internet, así como la verificación de la nueva interface en las impresoras y la instalación del nuevo driver disponible en el servidor	RF-168087 RF-168092 RF-168440 RF-168446
Nov-25	Boyacá	Chiquinquirá	Mantenimiento de impresoras y revisión de equipos de cómputo	Se realiza desplazamiento de soporte en sitio para realizar el mantenimiento de la impresora y la revisión de equipos de cómputo para garantizar su correcto funcionamiento.	RF-168997 RF-169003 RF-169004 RF-169005
Nov-25	Apartadó	Turbo	Mantenimiento de impresoras y revisión de equipos de cómputo	Se realiza desplazamiento de soporte en sitio para realizar el mantenimiento de la impresora y la revisión de equipos de cómputo para garantizar su correcto funcionamiento.	RF-168553 RF-168554

Tabla 40 Visitas a Sedes sin Soporte

- Medición ANS Mesa de Servicios

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

Área	Nombre del Indicador	Resultado	Meta
Mesa de Servicio	Tiempo de atención de solicitudes por soporte en sitio	100,00%	95,00%
	Tiempo de solución de incidentes por soporte en sitio	98,75%	90,00%
	Tiempo de solución de requerimientos por soporte en sitio	99,86%	90,00%

Área	Nombre del Indicador	Resultado	Meta
	Tiempo de respuesta de la mesa de servicio	100,00%	85,00%
	Abandono de llamadas	0,00%	Máximo 8,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 41 Medición de ANS Mesa de servicios

3 LINEA DE SERVICIOS CENTRALES

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

3.1 Datacenter Principal

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

Se observó un comportamiento de crecimiento la asignación de licencias de Office 365 reportados a través de ARANDA, donde se realizó la atención de 100 requerimientos asociados a esta categoría del servicio de Windows, así como la creación, modificación de usuarios que reduce su reporte a 9 casos para el mes de noviembre. De la mano de asignación de licencias se atendieron 51 requerimientos, obteniendo un incremento considerable con respecto a los meses anteriores, con respecto a los casos asociados a configuración de MFA se mantiene en 10 casos adicionales de apoyo en configuraciones del servicio de Office 365. Las categorías restantes asociadas al servicio de Windows se mantienen con un reporte bajo reflejando la estabilidad del servicio de cara a usuario final. Dentro de las labores de administración se encuentran actividades tales como revisar regularmente la base de datos de usuarios para identificar cuantas inactivas, duplicadas o desactualizadas, y proceder con su eliminación o actualización según sea necesario.

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

Es importante que la entidad remita bimestral o trimestralmente informes relacionados con la desvinculación de funcionarios y contratistas para realizar las actividades de actualización y liberación de licenciamiento de Office 365. También es importante precisar que es requerido el listado de nombres oficiales de todas las dependencias de la entidad, esto con el fin de estructurar un plan de calidad de la información del directorio activo y que se alinee con los nombramientos estipulados por la entidad. Actualmente se está trabajando con la Oficina de Tecnologías de la Información para fortalecer este punto en específico e

implementar un plan de calidad de la información de Directorio activo. Actualmente se está a espera del envío de la información de manera formal por parte de la entidad, pero se ha trabajado de manera articulada con la Oficina de Tecnologías de la Información, para fortalecer este ítem dentro de la entidad. Es importante que esta actividad se priorice para el mes de diciembre y enero debido a la desvinculación de contratistas de la entidad por cierre de gestión.

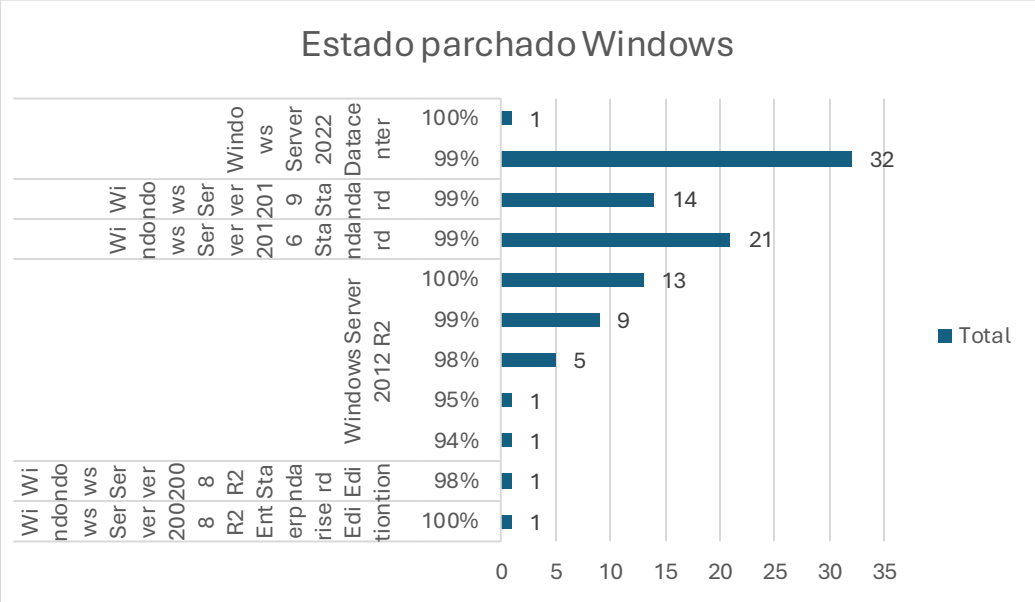


Ilustración 33 Cumplimiento WSUS

La interacción de los requerimientos de servicio asociados al equipo de trabajo de Windows está relacionada en su gran mayoría a asesoría y consultas que generan los funcionarios con respecto al funcionamiento de los servicios de Office 365 a los cuales tienen acceso, seguido por los casos en donde se requiere de algún tipo de configuración sobre sus cuentas, shared mailbox o servicios a los que acceden. Se ha reducido la solicitud de generación de backups significativamente con respecto a meses anteriores y es un comportamiento habitual en el reporte mensual de este tipo de casos. Se ha incrementado el reporte de asignación de licencias por creación de cuentas de servicio por parte de las áreas.

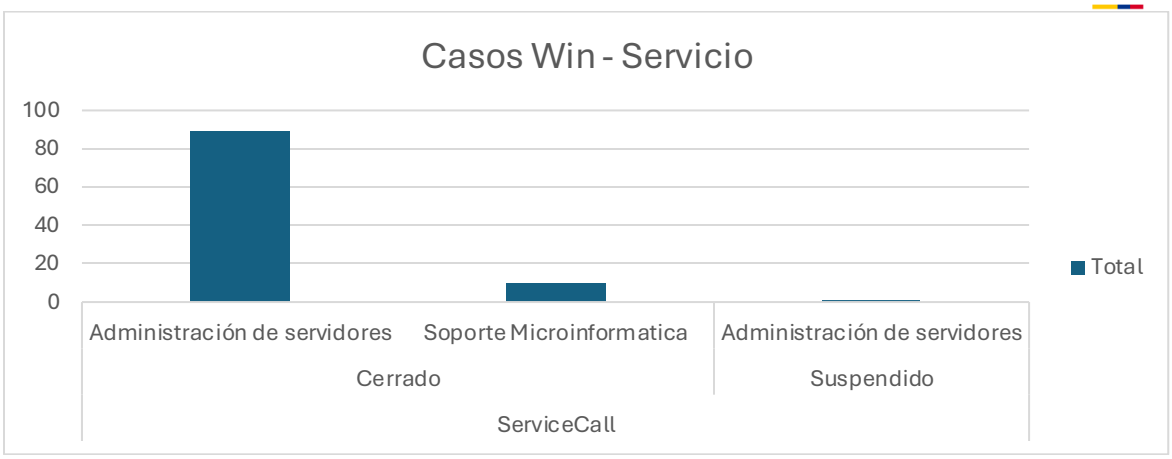


Ilustración 34 Casos Win Servicio

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.

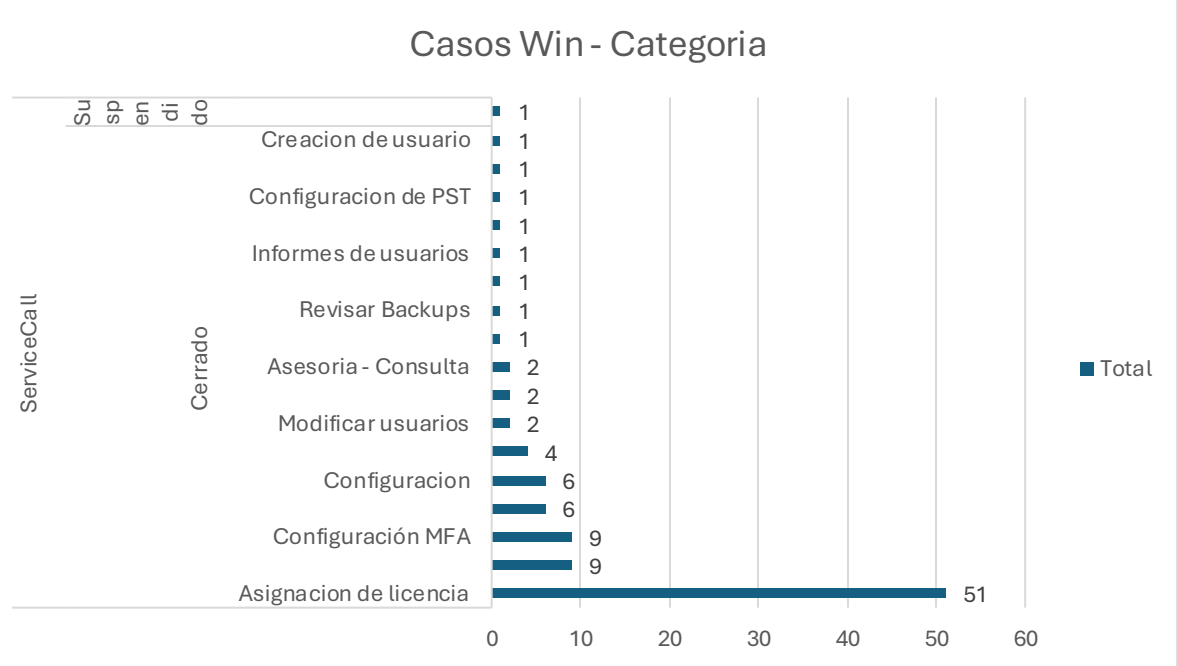


Ilustración 35 Estado final de los casos Windows

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

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

Tabla 42 Capacidades contractuales

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

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

Tabla 43 Capacidades contractuales

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

Total MinT (Con servidores para desaprovisionar + ambientes de pruebas)	
Descripción Características	Total
vCPU	742
RAM	3.1 TB
Almacenamiento	132 TB
Numero de Servidores	106

Tabla 44 Consumo de capacidad con servidores para desaprovisionar + ambientes de pruebas)

Total MinT (Sin servidores para desaprovisionar con ambientes de pruebas)	
Descripción - características	Total
vCPU	700
RAM	2.9 TB
Almacenamiento	129 TB
Numero de Servidores	101

Tabla 45 Consumo de capacidad Sin servidores para desaprovisionar con ambientes de pruebas

Total MinT (Sin servidores para desaprovisionar sin ambientes de pruebas)	
Descripción - características	Total
vCPU	556
RAM	2.3 TB
Almacenamiento	113 TB
Numero de Servidores	76

Tabla 46 Consumo de capacidad Sin servidores para desaprovisionar sin ambientes de pruebas

Total MinT (Servidores Pruebas y Desarrollo)	
Descripción - características	Total
vCPU	144
RAM	573 GB
Almacenamiento	16 TB
Numero de Servidores	28

Tabla 47 Consumo de capacidad Servidores Pruebas y Desarrollo

vCPU Ficha: **854** a vCPU consumida: **700 (81.9%)**
Memoria Ficha: **3.3 TB** a Memoria consumida: **2.9 TB (87.8%)**
Almacenamiento Ficha: **156 TB** a Almacenamiento consumido: **129 TB (82.9%)**
Número de Servidores Ficha: **106** a Numero de Servidores disponibles: **101**

Se realizó validación de los datos, realizando exclusión de la información asociada a las capacidades consumidas por parte de los servidores de servicios de la operación, es decir máquinas aprovisionadas para operar un servicio y que no hicieron parte de la virtualización de la nube privada de la entidad, aun así realizando esta exclusión, la entidad se encuentra en un escenario de consumos dentro de lo acordado en la ficha en los ítems de vCPU y RAM y almacenamiento aumento ligeramente sus consumos, teniendo en cuenta que se están excluyendo los servidores asociados al servicio de Backup los cuales deben validarse en conjunto con la entidad para considerar o no excluir estos consumos de capacidades de almacenamiento, ya que incluyéndolos dentro de la revisión, nuevamente entraría el ítem de almacenamiento superando la capacidad contratada. Es importante mencionar que la entidad cuenta con 10 Servidores de pruebas nuevos asociados a nuevas aplicaciones y existe una redundancia de servidores del servicio SIAS, ya que se aprovisionaron los 3 nuevos servidores de pruebas para este servicio, pero no se encuentran en uso actualmente, por lo cual en cuanto se realice el cambio de los servidores antiguos a los nuevos, se reducirán las capacidades consumidas, así como el servidor creado de manera temporal para el Asessment realizado para aplicaciones a migrar hacía Azure. De igual forma se restan las capacidades de estos servidores al no estar en escenario productivo o pruebas.

	vCPUs	RAM - TB	Capacidad Disco
Consumos	**700**	**2.9 TB**	**129 TB**

Tabla 48 Consumo de capacidad actual

Es importante mencionar que, en el proceso de redimensionamiento de la nube privada de la entidad, los ambientes de pruebas son los que están creciendo de manera continua (nuevos aprovisionamientos), por lo cual se debe entrar a revisar procesos de reducción de capacidades de estos entornos. De igual forma se han reducido capacidades y desaprovisionado servidores para reducir los consumos sin afectar la disponibilidad de servicios productivos. En el escenario actual, la entidad tiene capacidad de crecimiento o ampliación de capacidades de los servicios ya aprovisionados. Se está en proceso de revisión para reducción de capacidades de servidores de aplicación como SISINFO por asignación de capacidades en RAM elevadas en contra parte con sus consumos.

También se expone que el servidor MINTRAB60 que cumple su rol como File Server principal, ha sufrido diferentes intervenciones de ampliación de capacidades de disco

virtual, teniendo en cuenta que este servicio a crecido exponencialmente, se está trabajando en una política de retención de backups de usuario final, ya que estos backups están consumiendo una cantidad importante de almacenamiento en el file server y a largo plazo se puede convertir en una actividad y/o tarea demandante de almacenamiento y de tareas operativas que puede convertirse en una solución no sostenible dadas las capacidades de almacenamiento contratadas. Se está realizando depuración de los backups de PST ya entregados a usuario final con el fin de optimizar cargas de almacenamiento en el File Server.

Nube Pública

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

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

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

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

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

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

Responsabilidades

Cada miembro de la organización debe:

- *Gestionar el acceso de acuerdo con los principios de esta política: Los administradores de sistemas y recursos son responsables de asegurarse de que los privilegios de acceso se asignen correctamente y se ajusten a las necesidades laborales de los usuarios.*
- *Solicitar cambios de privilegios a través de los canales adecuados: Cualquier solicitud para otorgar, modificar o eliminar privilegios debe ser canalizada a través del proceso formal de gestión de accesos de la organización.*
- *Reportar accesos sospechosos o actividades inusuales: Todos los usuarios deben estar atentos a comportamientos inusuales y reportarlos inmediatamente al departamento de seguridad o administración de sistemas.*
- *Seguridad: La seguridad de los sistemas y la protección de la información son fundamentales para el éxito y la continuidad de la organización. La implementación efectiva del principio de privilegio de acceso mínimo contribuye a la mitigación de los riesgos de seguridad, tales como:*
- *Prevención de brechas de seguridad: Limitar el acceso de los usuarios solo a los recursos necesarios reduce significativamente la probabilidad de que un atacante pueda obtener acceso a información sensible en caso de que una cuenta de usuario sea comprometida.*
- *Auditoría y trazabilidad: Al aplicar el principio de privilegio mínimo, es más fácil realizar auditorías y seguimientos de las actividades de los usuarios. Si un incidente de seguridad ocurre, la trazabilidad de accesos y actividades será más clara y se podrá tomar acción correctiva rápidamente.*

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

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

- Aprovisionamiento de Appliance de Azure Migrate.
- Creación de Grupo de Recursos en el Tenant de la entidad en la Suscripción de Empleo.
- Creación de Componentes de Azure Migrate en el tenant.
- Sincronización de On Premises con Azure a través del Appliance.
- Tracking de información de las apicaciones a intervenir.

- Generación de logs exportados desde el appliance para revisión y estudio del equipo de GoToCloud.

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

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

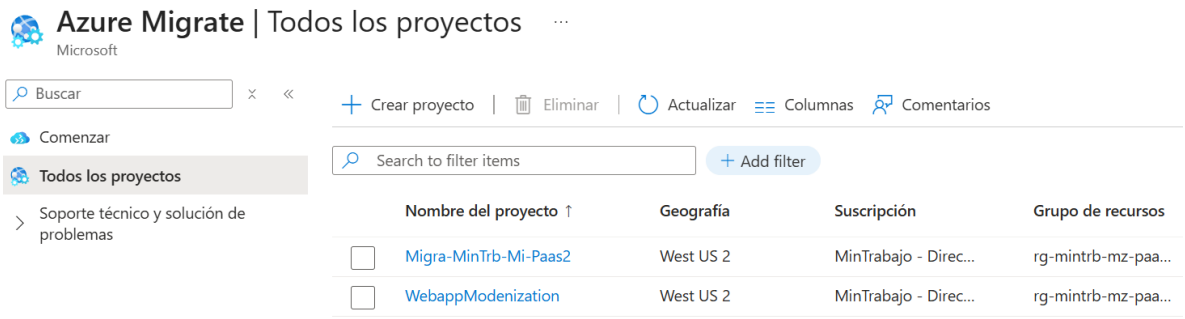


Ilustración 36 Azure Migrate

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

- Atenciones: la actualización desde el origen de datos 01/06/2024
- Capacitaciones y cieti: la actualización desde el origen de datos 01/05/2026
- 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. Así como el proceso de migración del ChatBot de la entidad alineado con el framework de arquitectura. Se realiza creación de la máquina virtual para el proyecto de interoperabilidad institucional en Azure, para la configuración por parte de la AND del componente de XROAD. Se está a espera de agendamiento de sesión técnica para instalación del componente de XROAD dentro de las maquinas virtuales. AND manifiesta que previamente requiere enviar un checklist a la entidad para validar que todos los prerrequisitos están acordes antes de iniciar la instalación.

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

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.

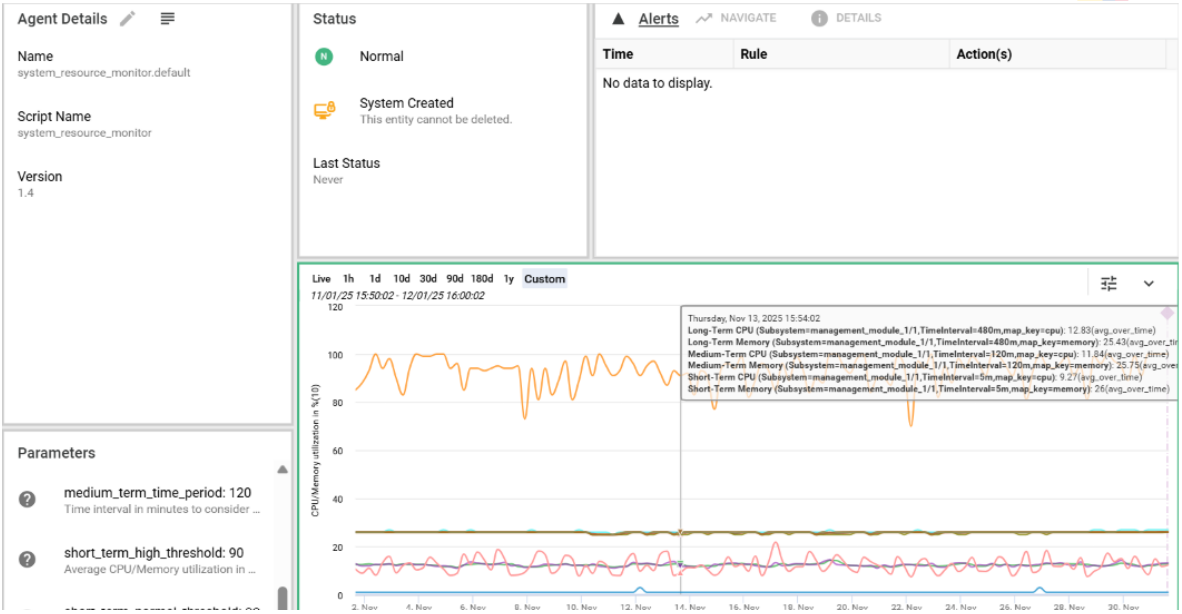


Ilustración 37 Comportamiento SWCORE Datacenter Colombia XV

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

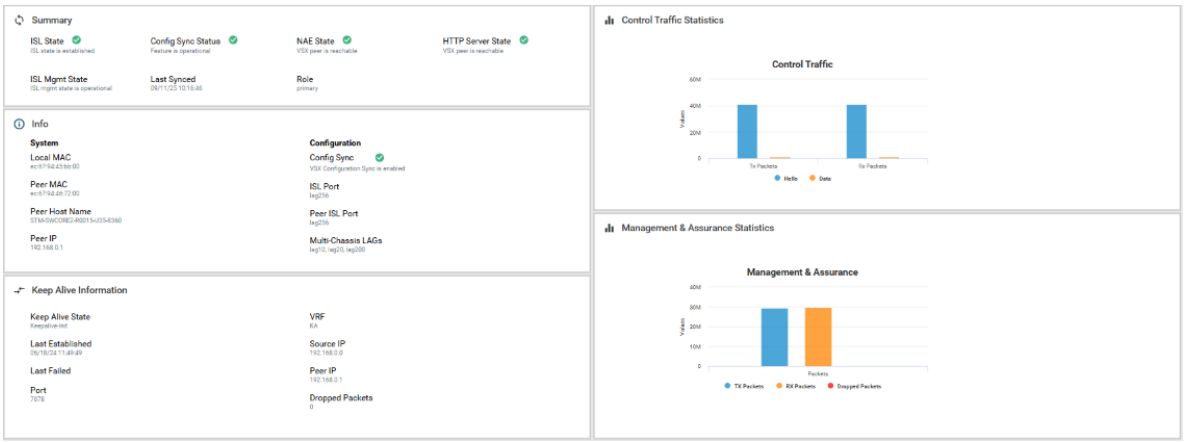


Ilustración 38 Sincronización HA de los Switch Core

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 430 Mbps y 480 Mbps de salida. El tráfico se ha mantenido con el mismo comportamiento de consumo de los últimos meses.

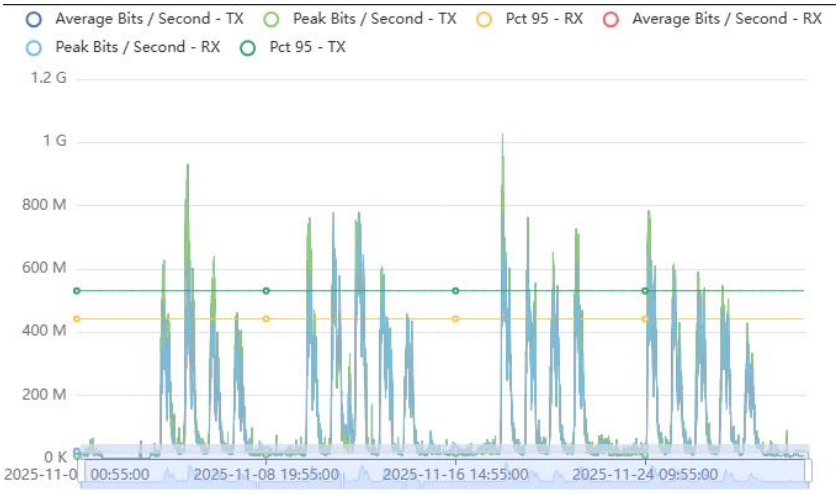


Ilustración 39 Grafica de consumo canal Internet Datacenter

Durante el mes de noviembre 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:

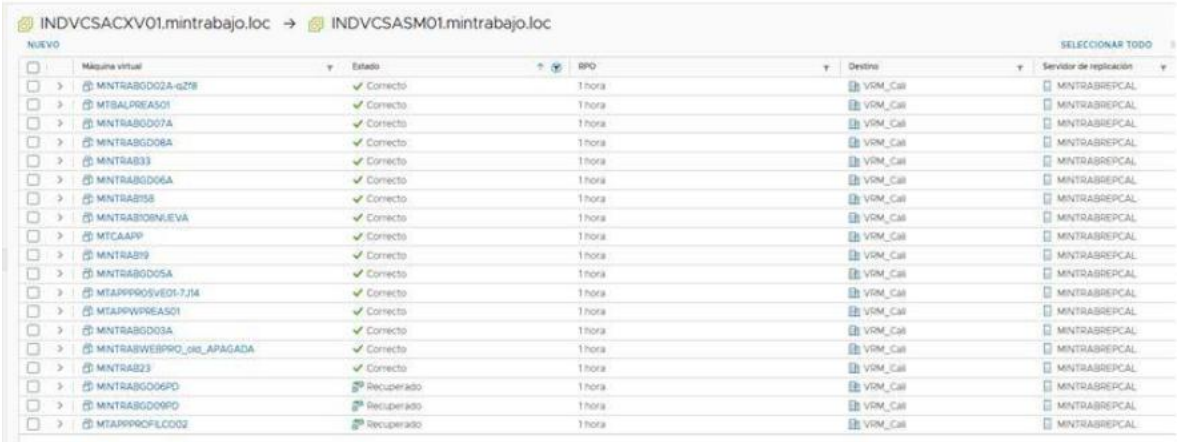


Ilustración 40 Captura de imagen máquinas virtuales

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

Actualmente se culminó con los ajustes de segmentación de red para preparar el escenario de pruebas para el último trimestre del año de cara a las aplicaciones .NET de acuerdo con lo socializado con la entidad. Las IP fueron asignadas durante el mes de noviembre para realizar las pruebas DRP definidas para el año 2025. De acuerdo con lo anterior, se iniciaron las configuraciones de prueba para replicación de las bases de datos de aplicaciones .NET alojadas en motor MSSQL Server a través de log shipping con una frecuencia de envío de logs cada 15 minutos. Esta prueba se ejecutará las primeras semanas de diciembre y se documentará de acuerdo a lo establecido.

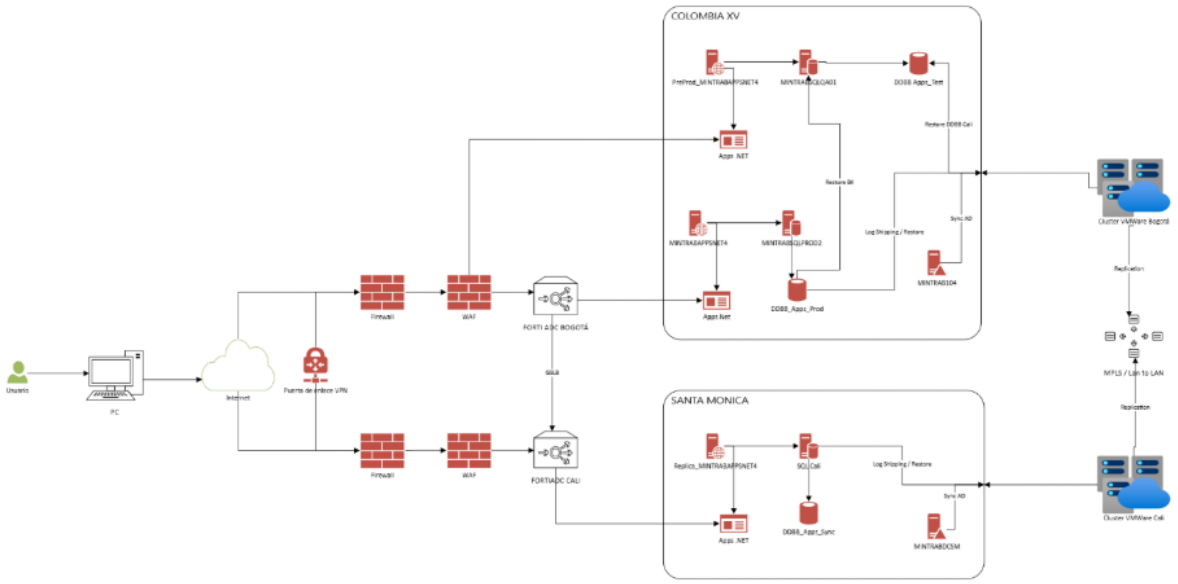


Ilustración 41 Escenario de pruebas Aplicaciones y AD

A nivel de comunicaciones en DC alterno, se observa que la conexión del LAN to LAN entre los dos Datacenter funcionó correctamente, de esta forma se garantizó la conexión entre estos. Se relaciona el comportamiento de tráfico Entre cada extremo de la conexión, donde se observa que se mantuvo activo con bajo tráfico durante el mes. Se observa que se tuvo un pico máximo de 13 Mbps.



Ilustración 42 Extremo DC Bogotá

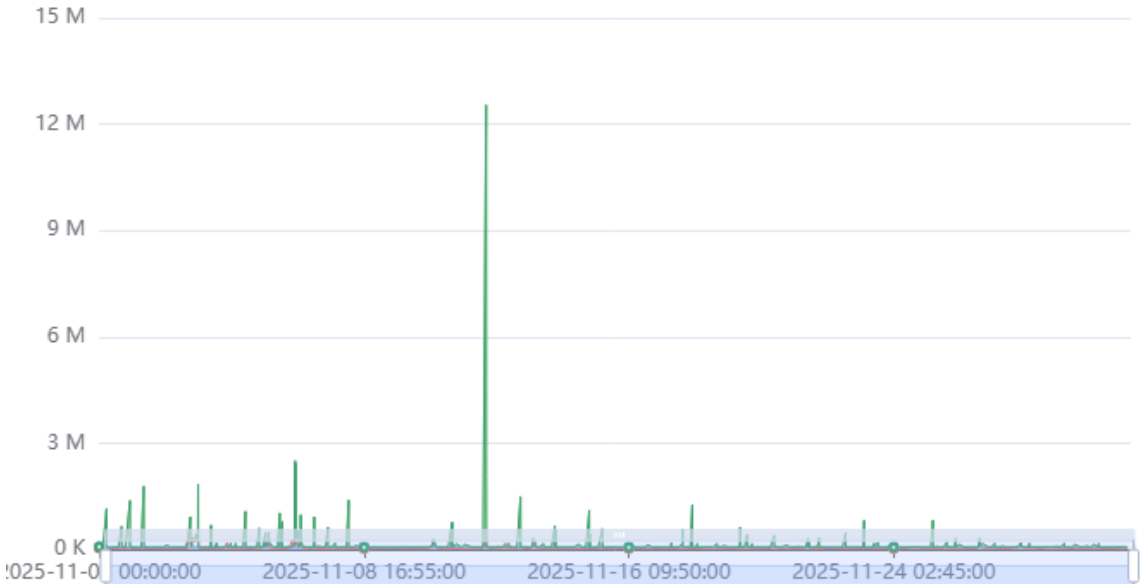


Ilustración 43 Extremo DC Cali

El canal de Internet de datacenter alterno se encuentra operativo, se observa que el canal tiene poco tráfico ya que el tráfico general se usa el canal ubicado en DC Principal. Se observa un pico máximo de 380Mbps.

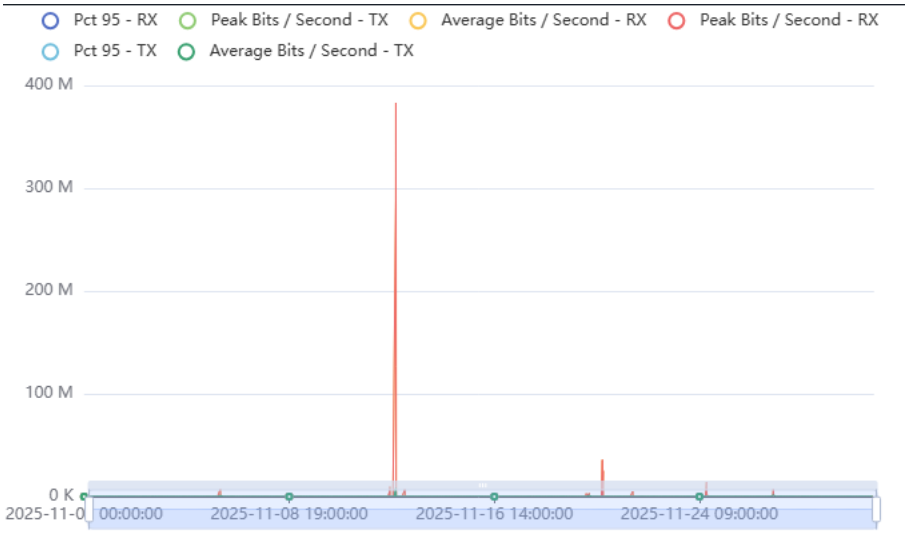


Ilustración 44 Estado canal de Internet DC Cali

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



Ilustración 45 Estado SWCORE Datacenter alterno

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

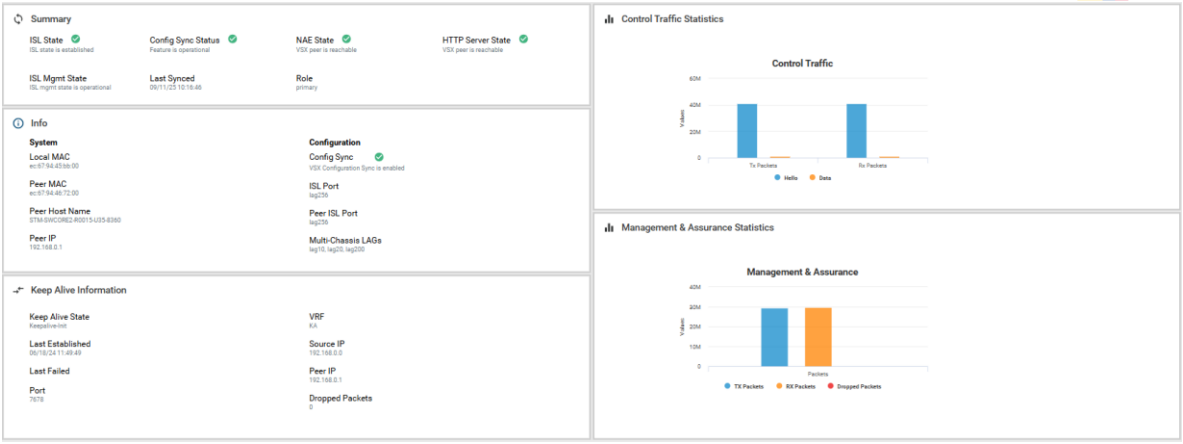


Ilustración 46 Estado HA SWCORE Datacenter alterno

Se verifica el canal MPLS de datacenter alterno, el cual se observa que se ha mantenido activo durante el mes de noviembre, no se presentaron reportes de caídas de servicio. El tráfico en este canal es bajo debido a que es el correspondiente al canal del centro alterno. Se observa que se tiene un promedio de entrada de 54 Kbps y de salida de 53 Kbps.

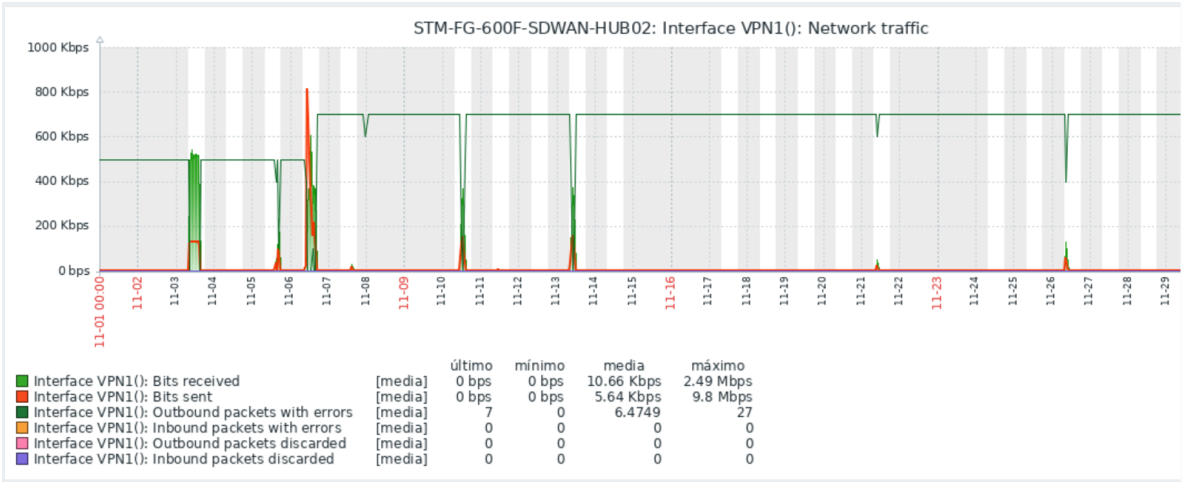


Ilustración 47 Consumo canal MPLS DC Alterno

Se verifica estado del equipo, donde se observa que presenta un uptime de 34 semanas con 5 días.

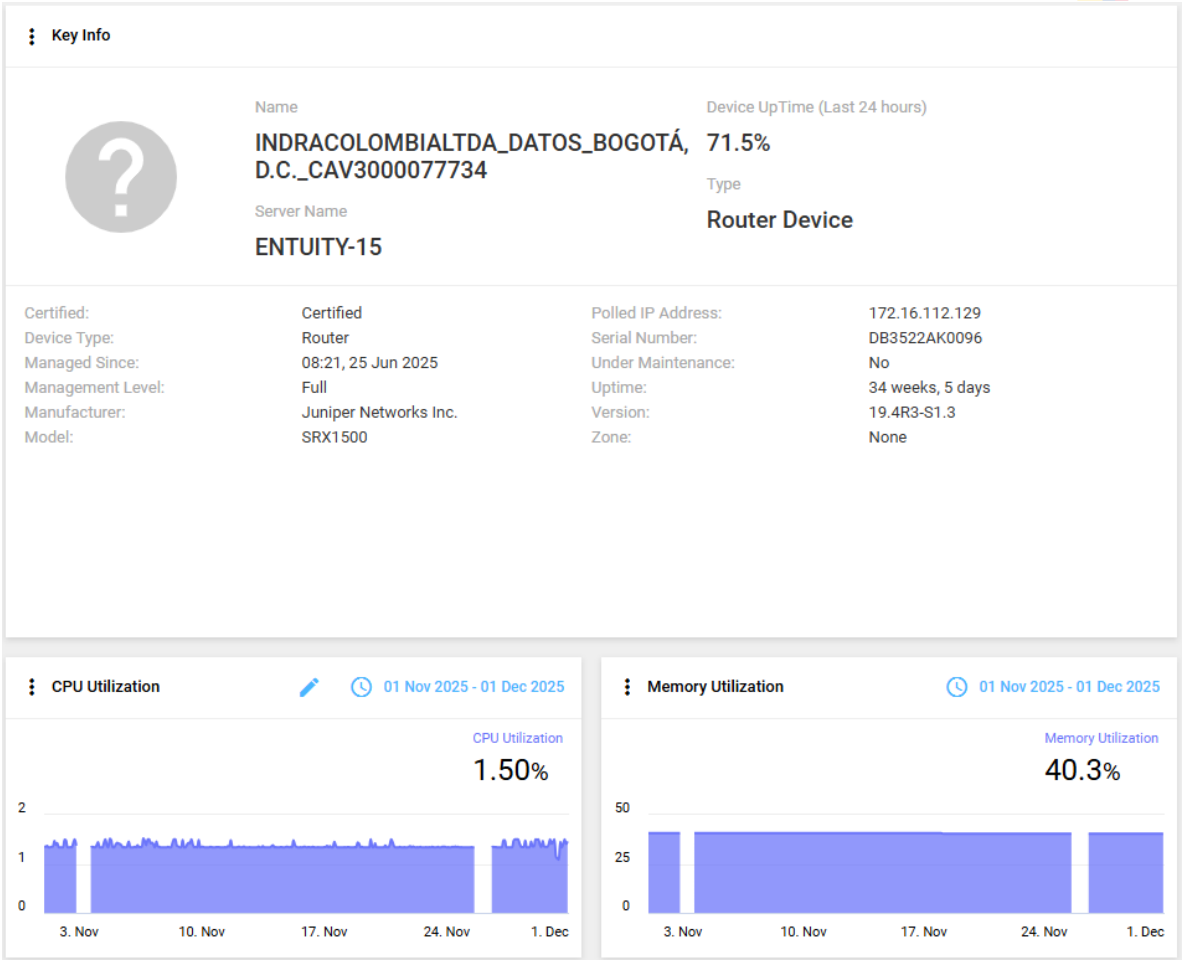


Ilustración 48 Estado Router MPLS DC Alterno

3.1.2 Procesamiento, Almacenamiento y Respaldo

- Servidores Windows e Infraestructura Virtualizada

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

Se continúa con la ejecución del plan de backups en donde se generan respaldos completos de todas las máquinas virtuales críticas alojadas en VMWare, este plan de backup en la actualidad se ejecuta los viernes en la noche generando un backup full de la semana de cada máquina y su almacenamiento, garantizando un punto de retorno semanal en caso de contingencia o incidencia crítica, durante los procesos de afinamiento se ha identificado la criticidad y propuestas de planes de backups totales e incrementales para estas. En donde

se identificaron máquinas que, por su criticidad y servicios alojados, ameritan un plan de Backup incremental diario, ya sea de discos, base de datos o máquina virtual completa, dependiendo del escenario y el tipo de máquina virtual. A este plan de Backups se han añadido servidores que han sufrido intervenciones técnicas con finalidad de adecuar la infraestructura virtualizada y depurar máquinas virtuales que no se encuentran en uso por parte de la entidad, pero sí que consumen capacidades que pueden ser aprovechadas por los entornos productivos.

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

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

Se dio visibilidad de esta situación para realizar las maniobras técnicas correspondientes de manera coordinada con el proveedor de este software a la entidad durante el mes de julio de 2024 se realizó esta sesión, en donde se identifican los servidores productivos como parte del escenario de virtualización de la entidad y que su proceso de migración a nuevos servidores de aplicación puede surtirse de la mano del área funcional. Actualmente se está a espera que el área funcional nuevamente permita un espacio de socialización para lograr entender el paradigma de consulta y validar que es posible migrar bajo una modalidad más simple y dejar la dependencia de esta infraestructura en estado de obsolescencia. Para el servidor MINTRAB13, el cual aloja una copia histórica del anterior aplicativo y base de datos de nómina de la entidad, el proveedor nos confirma que no tiene administración y ningún tipo de gestión sobre el recurso y la información que esta aloja. La entidad confirma tener acceso de consulta a una base de datos y solo es consultada por demanda, pero no está asociada a ningún sistema de información productivo.

Es importante mencionar que el estado sobre la documentación de esta base de datos y el sistema de información que alojaba anteriormente es crítico ya que la entidad no cuenta con documentación, la empresa que desarrollo el aplicativo dejo de existir hace unos años y el desarrollador que tenía contacto con la entidad, desafortunadamente falleció previo al inicio del contrato de la UT.

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

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

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

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

Sin embargo durante estos procesos de mitigación, se han encontrado escenarios en donde el alcance contractual y técnico del equipo de trabajo, no permite realizar una mitigación total de las vulnerabilidades encontradas, sobre todo para el escenario de aplicaciones especializadas, por lo cual se consolidarán aquellas vulnerabilidades que por su naturaleza no pueden ser mitigadas con las actividades que se han propuesto y se han venido ejecutando, por lo cual se realizará una socialización y posterior entrega de aceptación del riesgo por parte de la entidad, ya que dentro de los escenarios encontrados, se observan obsolescencia de versiones de componentes que interoperan y permiten hacer funcional una aplicación que al intentar actualizarlos, indica que el código de la aplicación se encuentra en un grado de obsolescencia y de uso de paradigmas de programación que ya no son soportados, por lo cual algunas de estas aplicaciones deben pasar por un proceso de re factorización total del código, que la entidad debe validar internamente, ya que esta actividad implica desarrollo de software de toda la aplicación y esto no se encuentra contemplado dentro de las actividades de mitigación de vulnerabilidades ni dentro del alcance contractual del servicio.

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

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

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

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

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

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

En estos servidores de archivos, se refleja la información de diferentes áreas, hemos identificado lo siguiente:

- Se aloja información de diferentes áreas y dependencias sin una estructura organizacional definida.
- Únicamente existen carpetas relacionadas con tópicos en específico o áreas en concreto, pero no una estructura relacional.
- No se observa un estándar de nombramiento para las carpetas, archivos u organización, así como una ausencia de cuotas para controlar la capacidad de almacenamiento por área o carpeta.
- Usuarios con privilegios de asignación de permisos, es decir no existe una centralización en la administración de este servicio.
- Aunque existe un plan de backup incremental de la información, donde se ejecutan backups de la información o discos virtuales donde se aloja la información, estos backups se ejecutan diariamente en horario nocturno, por ende, si un usuario elimina un archivo, carpeta o fichero durante el transcurso del día, no hay garantía de recuperación de la información eliminada o manipulada por los usuarios de la entidad que posean este tipo de permiso.
- Se han encontrado backups de información personal de funcionarios y contratistas dentro del servidor de archivos, así como archivos multimedia, como fotos, videos y música.
- Se han encontrado archivos con extensiones .exe, desconociendo su origen y abriendo una brecha de seguridad importante, teniendo en cuenta que, si surgen incidencias de seguridad de la información, vulneraciones de seguridad, infección de archivos con virus o malware, este sería un canal en donde los usuarios podrían exponer este tipo de archivos que puedan tener esta vulnerabilidad.
- No existe un estándar de nombramiento de carpetas o archivos electrónicos visible en el file server o servidor de archivos, generando inconvenientes en la integridad de la información allí alojada. Es importante tener en cuenta, que Microsoft posee un límite de caracteres para nombramiento de carpetas y archivos, así como unas

limitantes en los caracteres introducidos en los nombres, si este estándar no es cumplido, en los procesos de backup o copiado de la información, se podría perder acceso a la misma, debido a que la ruta se vuelve tan extensa que la propia solución de Microsoft no le permite acceder a la misma.

- La entidad ha aplazado las actividades relacionadas con File Server hasta Julio 2025. Hasta el momento no se ha obtenido retroalimentación por parte de la entidad.
- Se comparte informe de estado actual a la entidad, tanto a la nueva Jefatura de la Oficina de Tecnologías de la Información como el nuevo Coordinador de Soporte informático.
- Se está a espera de retroalimentación de la documentación de File Server compartida y de la estrategia propuesta para la migración hacia un nuevo entorno.
- La no migración de este tipo de recursos así como la no actualización, pone en riesgo la implementación de DRP para este servicio en específico.

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

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

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

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

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

- Actualización MINTRAB25: La maquina fue migrada a Windows 2022 y fue separada la base de datos en un servidor independiente, se están realizando pruebas de conectividad de la aplicación. A la fecha la aplicación está estabilizada

y solo restaría la validación del área funcional y el visto bueno para apagado y reemplazar el servidor.

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

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

3.1.3 Aplicaciones Especializadas

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

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

Se observaron escenarios en donde se identifican aplicaciones que por su arquitectura y uso de componentes deprecados como versiones anteriores de Framework, sistema operativo entre otros componentes, no permiten una migración transparente a un OS con soporte vigente, por lo cual hay que explorar cada escenario para las aplicaciones con un énfasis .Net para realizar los procesos de separación y adecuación de cada aplicativo, se dará visibilidad de las aplicaciones impactadas y alojadas en el server MINTRAB23 para concretar sesiones con áreas funcionales y estructura un plan de trabajo de afinamiento y transición a sistemas operativos y componentes .Net más actualizados. Estos procesos de afinamiento permitirán un mejor rendimiento sobre las aplicaciones de la entidad, una mejora en su performance y la alineación con buenas prácticas y modelos de arquitectura que permiten una mejor administración, soporte y monitoreo de estas. Estas aplicaciones han sido migradas a nuevos entornos 2022 y algunas han sido desaprovisionadas por solicitud de las áreas funcionales y la OTIC.

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

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

Se propuso la independización del aplicativo SIRITI del servidor MINTRAB23 el cual aloja más de 40 aplicativos, lo cual podría indicar un inconveniente a la hora de gestionar controles de cambios ya que el despliegue de paquetes podría afectar el funcionamiento de otra aplicación que coexista en este entorno, esto debido a que cada aplicación fue desarrollada con diferentes prácticas y arquitecturas que a la hora de aprovisionarse en un solo entorno, podría provocar inconvenientes de cara al despliegue de controles de cambios para cada aplicación.

Tras este ejercicio la aplicación ya se encuentra migrada y lista para salir a producción en un servidor totalmente independiente y sin coexistencia de otras aplicaciones en su mismo entorno, lo cual permite un mejor funcionamiento del componente GeoServer.

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

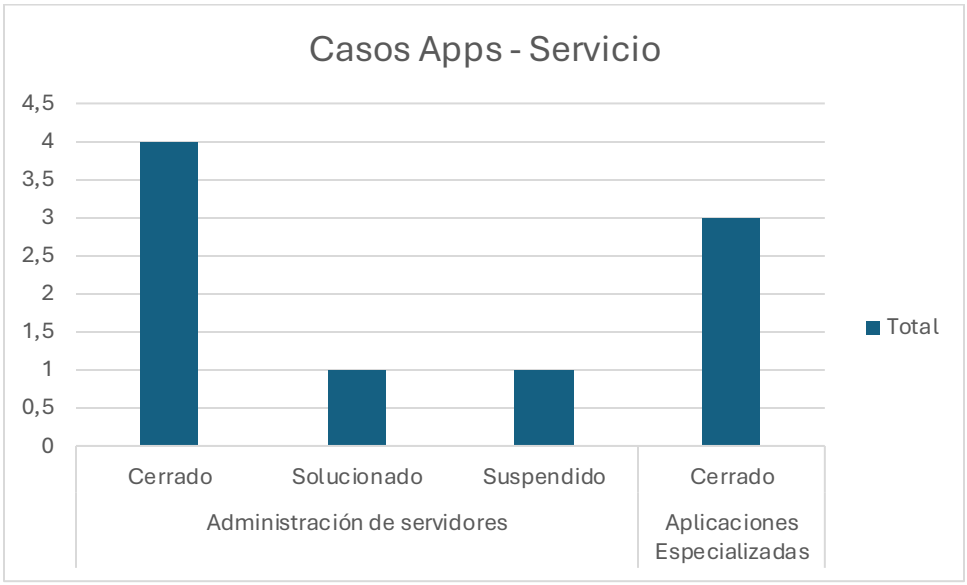


Ilustración 49 Casos App Servicio

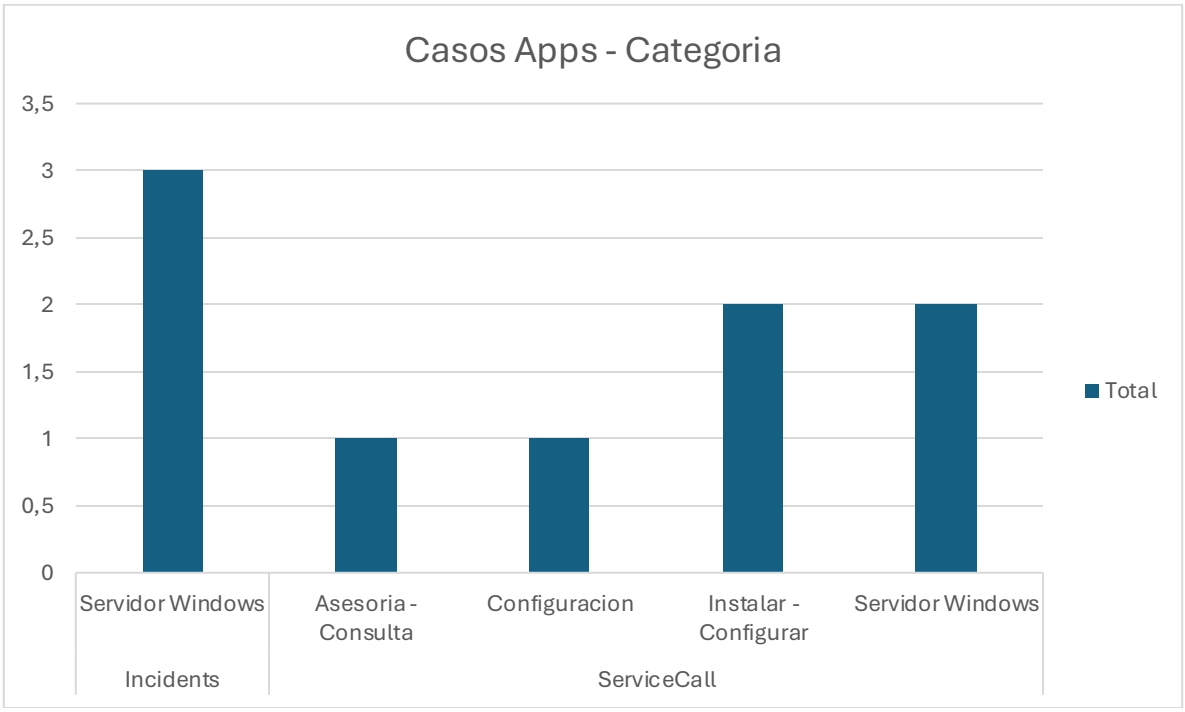


Ilustración 50 Casos App Categoría

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

Escenario SIAS:
Pendientes:

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

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.

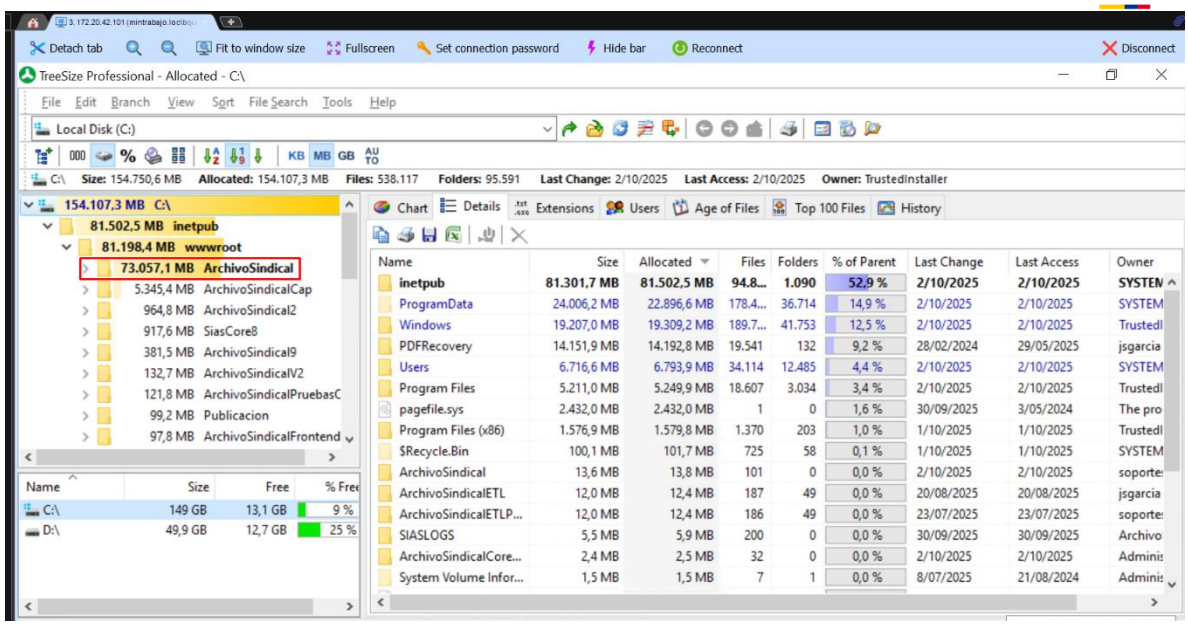


Ilustración 51 Tamaño Archivo Sindical

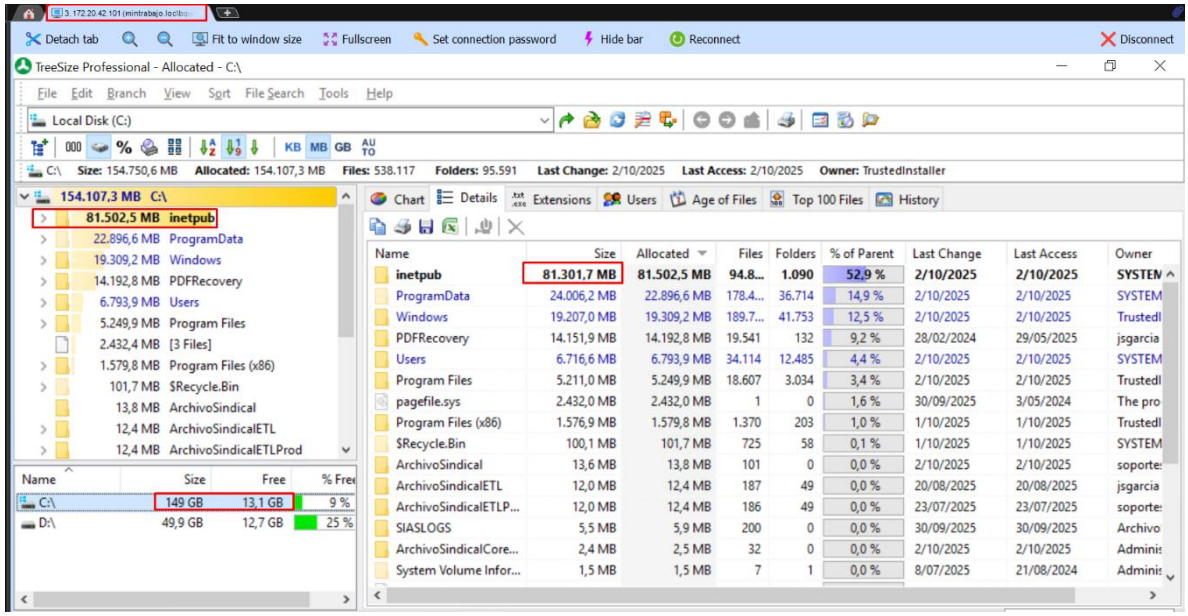


Ilustración 52 Tamaño IIS

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.
  - Se crea micrositio para alojar los documentos de la red ormet y se está espera de aprobación funcional por parte del área de empleo.

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

Migración Aplicaciones .NET

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

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

También es importante para nosotros como proveedor de servicios tecnológicos abrir estos espacios con las áreas funcionales de manera independiente, porque abre las puertas a una comunicación más fluida como administradores técnicos de los repositorios de estas aplicaciones, ya que permite mantener un canal de comunicación directo, actualización de fichas de servicio e identificar los actores necesarios para socializaciones con las gestiones ITIL, por ende es importante establecer estos canales de comunicación directos no solo

para las pruebas de migración, sino también para conocer a detalle la dinámica de las áreas con los sistemas de información y articular la gestión realizada desde las gestiones ITIL con cada área responsable de cada aplicativo que se traduce en un CI dentro de la herramienta de gestión ARANDA.

En el marco de la migración de aplicaciones .NET, se observan que algunas aplicaciones están marcadas como productivas, pero actualmente no están operativas, se debe contemplar si realmente se encuentran en uso por parte de la entidad para realizar la migración del componente NET, DDBB SQL y Sistema Operativo o si de lo contrario debe generarse un backup, pero no continuar con la migración de estas aplicaciones. Las aplicaciones pendientes de aprobación y a las cuales se hace referencia en el presente correo para realizar pruebas y migración a un entorno de Windows Server 2022 son:

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

De acuerdo con el contexto anterior se informa que las aplicaciones especializadas migradas a satisfacción a nivel de base de datos a entorno SQL Server 2022 son las siguientes:

- Tmigrante
- FTrutec
- Biblioteca Virtual de trabajo
- Calculadora Laboral
- Censo Sindical
- Centro de entrenamiento
- Conjovenes
- Contratos
- Estado Joven
- FTrue
- Saber hacer vale
- Subsistema de formación para el trabajo
- Ftalentos empleo

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

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

Se sostiene reunión con área de nómina y su proveedor y comparten las nuevas capacidades para dar continuidad al proceso de migración de la aplicación de nómina. Las máquinas virtuales fueron aprovisionadas de manera satisfactoria y se está a espera de configuración conjunta con el proveedor de la aplicación.

Se programa sesión para el 15 de diciembre de 2025 con el fin de socializar con las áreas funcionales la independización de aplicaciones, el impacto técnico y a nivel de seguridad de este cambio y que tengan visibilidad de la propuesta para el cambio que se espera realizar durante la vigencia del presente contrato.

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

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

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

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

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

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

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

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

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

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

una sesión técnica/funcional que tendría como objetivo presentar el estado final del despliegue, validar que el sistema se encuentra disponible en el ambiente de pruebas, y dejar constancia de los pendientes identificados durante la instalación. Esta sesión también permitirá oficializar la transferencia del sistema para su validación y uso por parte del equipo del Ministerio.

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

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

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

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

caso Microsoft, que recomienda el desarrollo y la actualización de las aplicaciones a los versionamientos mencionados.

  - El estado actual de .NET Framework 4.7 por parte de Microsoft es el siguiente:
  - Solamente recibe actualizaciones o parches de seguridad hasta 2027 como máximo.
  - Tiene soporte limitado por parte de fabricante (Microsoft)
  - Se recomienda migrar a .NET 4.8 o .NET 6/8

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

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

- Aspectos técnicos: ya fueron gestionados todos los ítems que pueden depender del Grupo de Soporte Informático y el equipo de servicios centrales de la UT.
  - Ya se configuró todo el entorno de servidores y base de datos para pruebas.

- Se actualizó la imagen institucional del sistema. o Se ejecutaron los scripts de creación de roles. o Se realizó configuración con Active Directory.
- Se suministraron usuarios administradores para creación de usuarios.

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

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

Migración Portal Web

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

- Se realizó la migración de forma exitosa a versión 7.3 sin afectación del servicio o corrupción de información
- Envío de Información/Ajustes por parte del equipo de Empleo sobre los tableros de FILCO publicados en el ambiente de pruebas de la página web de la entidad para que los cambios puedan aplicarse en el marco de la migración y puedan salir a producción con la nueva versión del portal. Se sostiene reunión a espera de formalización de los ajustes requeridos
- La entidad se encuentra en validación para creación de un equipo de experiencia de usuario 100% Ministerio del trabajo.
- La revisión de links rotos sigue en cabeza de la entidad.
- Actualmente se encuentra en fase de pruebas el versionamiento de LifeRay 7.3, Tomcat y versión de Oracle DB 19c.
- Se ejecuta paso a producción de las últimas versiones mencionadas en julio de 2025 de manera satisfactoria y sin errores en su despliegue.
- En etapa de pruebas para versión 7.4.
- Se esta apoyando el desarrollo de un nuevo Organigrama para publicación en el portal. En validación de plantillas.
- Se están apoyando procesos de creación y templates para nuevos micrositios, así como actualización de la imagen institucional en todo el portal.
- Se programa migración de versión para mediados de diciembre de 2025, finalizando con todas las actualizaciones de versión del portal.

GESTOR DOCUMENTAL

A nivel de mantenimientos del gestor documental se realizaron actividades técnicas de mantenimiento en el marco de proceso de afinamiento y optimización, esto de acuerdo con

la solicitud de ejecución por parte de la entidad, se plasman como evidencia los siguientes procedimientos:

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

Plataforma – Aplicaciones

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

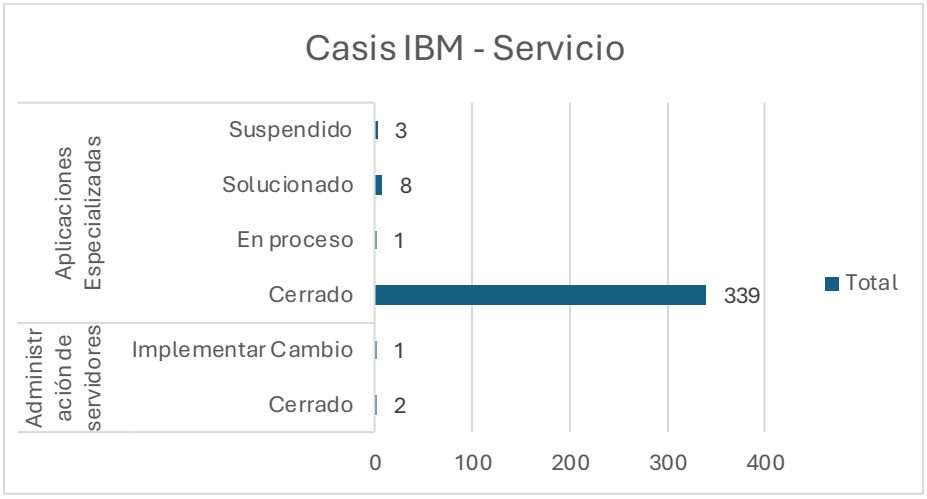


Ilustración 53 Casos *IBM Servicio*

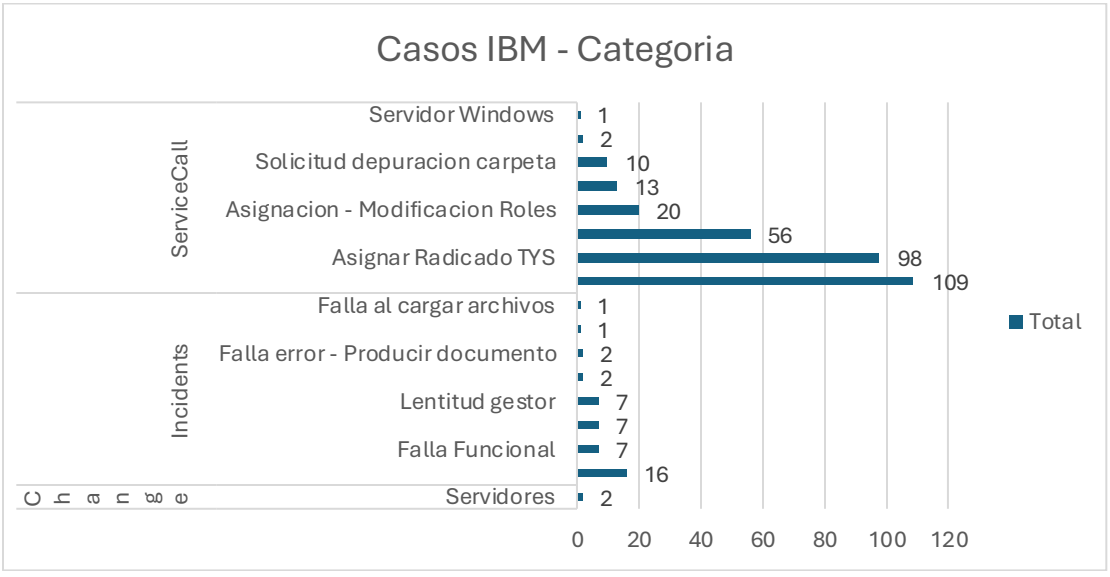


Ilustración 54 Casos IBM - categoría

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 (109 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 (98 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 (56 casos) Eliminación de casos activos una vez el proceso de documentos ha sido transferido al módulo de Instrumentos Archivísticos, conforme al ciclo de vida documental.
- Radicar una solicitud - Asesoría/Consulta (13 casos) Consultas relacionadas con procesos del Gestor Documental en las que los usuarios reportan errores durante la radicación o al intentar subir documentos, lo cual impide completar correctamente la solicitud.
- Falla radicación (16 casos): Requerimientos a fallas en los procesos de radicación, errores asociados a este proceso, ya sea por mal procedimiento, problemas en conectividad, falta de roles para ejecución de actividades o temas aislados que se tratan de manera diferencial.

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

Se realiza cambio de inactivación del campo referido de acuerdo a lo solicitado por el área funcional generando el siguiente comunicado: Por medio de la presente, informamos que, a partir del **lunes 1 de diciembre de 2025**, la sección **"Radicados Referidos"** ha sido deshabilitada en todas las pantallas del proceso del gestor documental.
Esta medida obedece a la necesidad de garantizar la integridad y la precisión de los datos en los informes de gestión a nivel documental. Se identificó que la referenciación de radicados afectaba la trazabilidad y la consolidación de reportes.
La deshabilitación tiene como finalidad fundamental estandarizar y formalizar los procedimientos de cierre de peticiones. A partir de ahora, todas las áreas de negocio del Ministerio.

De acuerdo con la serie de sesiones sostenidas con el equipo IBM y el Ministerio del Trabajo, se remiten las capacidades mínimas para el aprovisionamiento de un ambiente de pruebas en condiciones para la entidad, ya que actualmente el escenario de licenciamiento no permite el aprovisionamiento de este entorno.

El objetivo de esta arquitectura es asegurar la capacidad para:

- Simular escenarios de pruebas de carga.
- Realizar pruebas exhaustivas de actualizaciones de los diferentes componentes.
- Soporte de alta transaccionalidad y balanceo.

Maquinas Gestor Desarrollo - Pruebas				
Rol Servidor	Cores por Server	Tipo de licenciamiento	PVCs por Core / PVU's por Core	total
WASND	6	PVU	70	420
WASND	6	PVU	70	420
BUS - AppConnect	6	PVU	70	420
ODM	4	PVC	5	20
DATACAP	5	PVC	5	25
DATACAP	5	PVC	5	25
BAW	6	PVC	5	30
BAW	6	PVC	5	30
Filenet FRONT	7	PVC	5	35
Filenet BACK	7	PVC	5	35

Total PVU's	1260
Total PVC's	200

Es importante mencionar que así como se requieren licenciamiento para el aprovisionamiento de la capa de aplicación, también deben validarse la disponibilidad de licenciamiento de base de datos, ya que actualmente la totalidad de licencias de DDBB Oracle, se encuentran asignadas a las bases de datos del portal web, gestor documental, nomina y SISINFO.

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

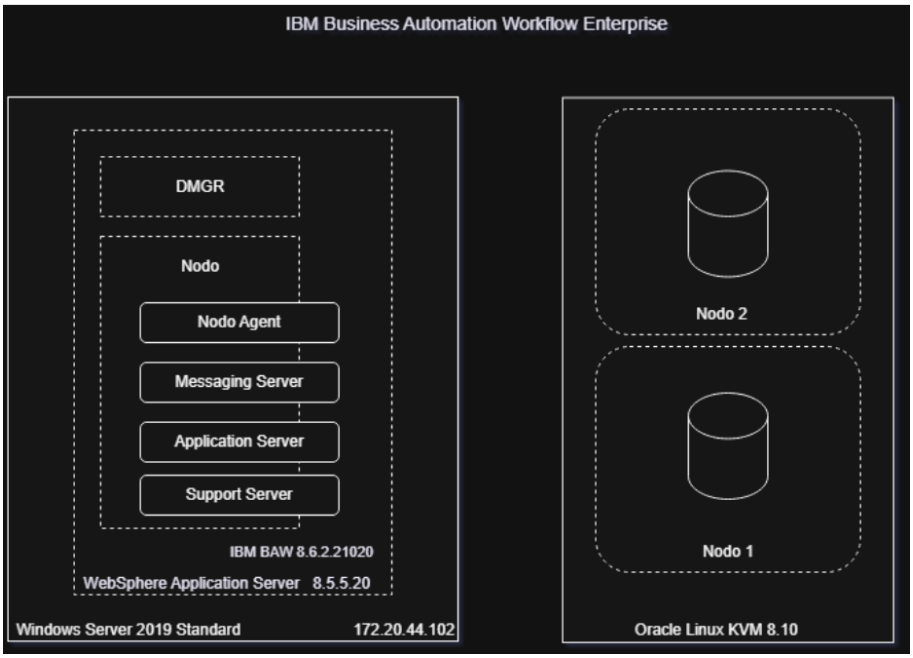


Ilustración 55 Diagrama BP

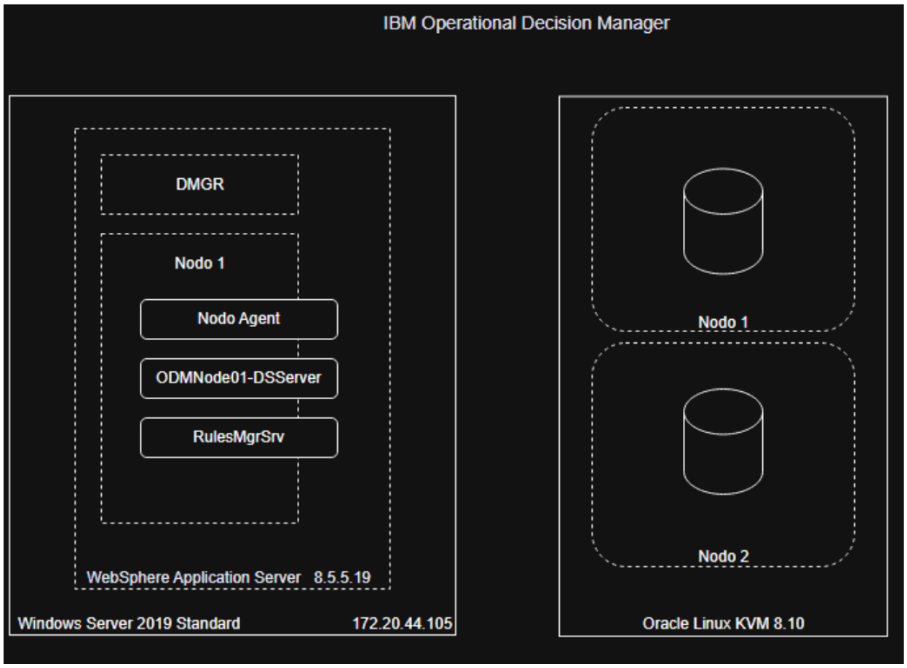


Ilustración *56* Diagrama ODM

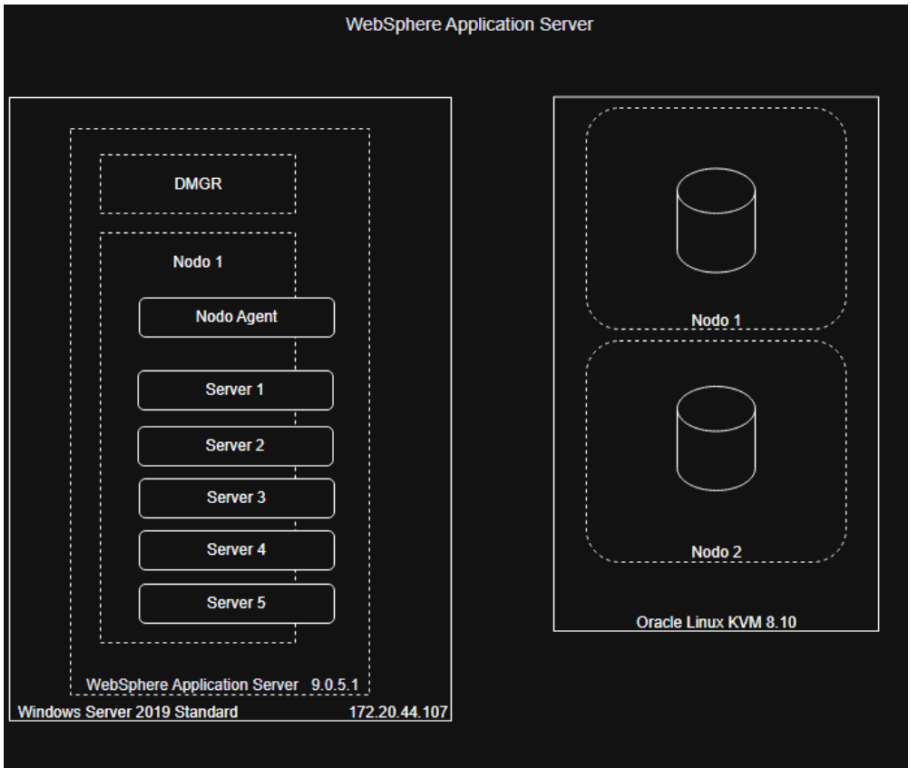


Ilustración 57 Diagrama WASND

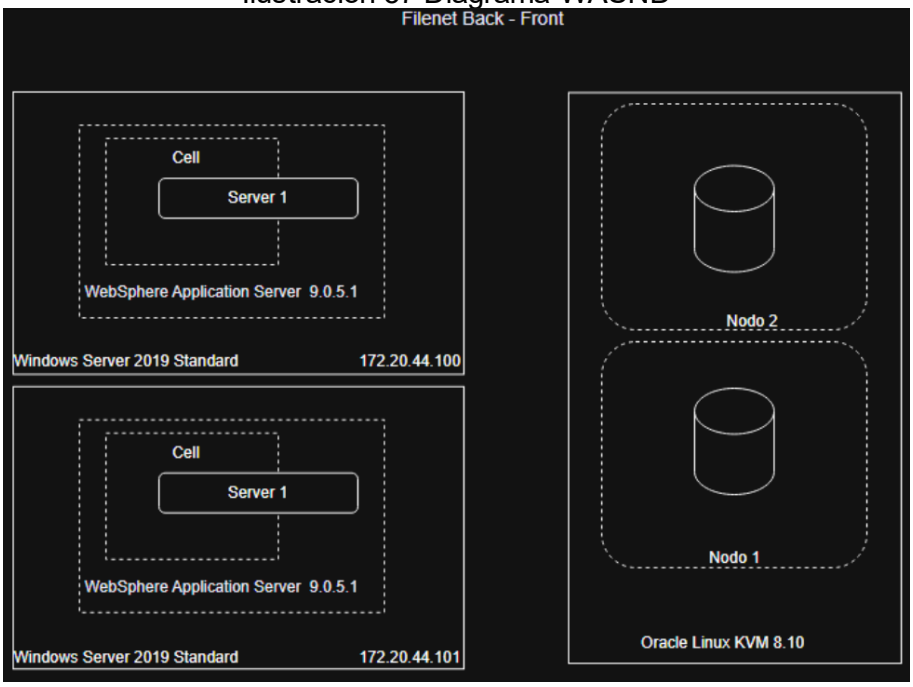


Ilustración 58 Diagrama FileNet Front

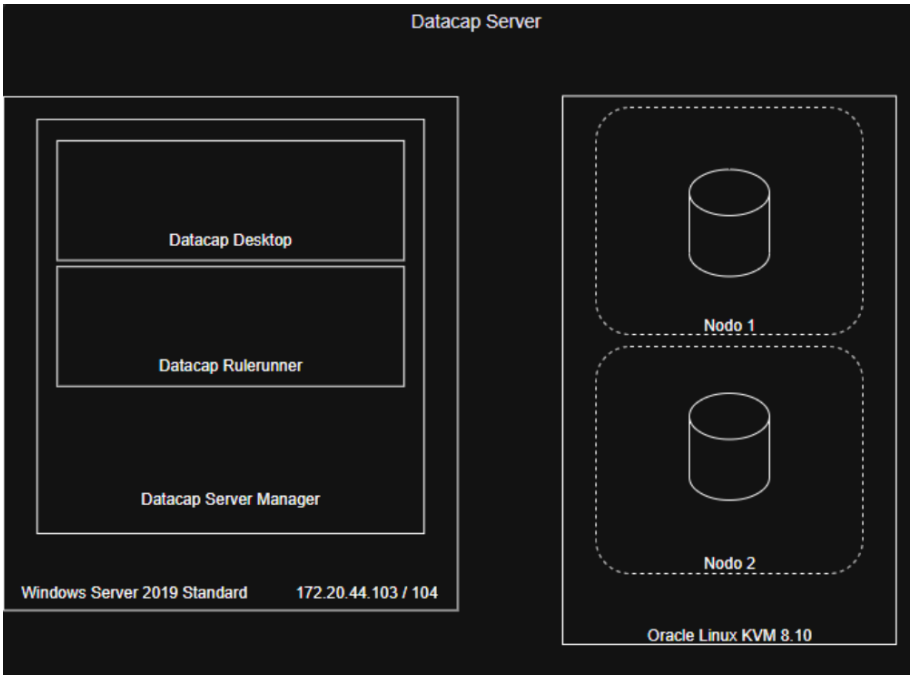


Ilustración 59 Diagrama Datacap

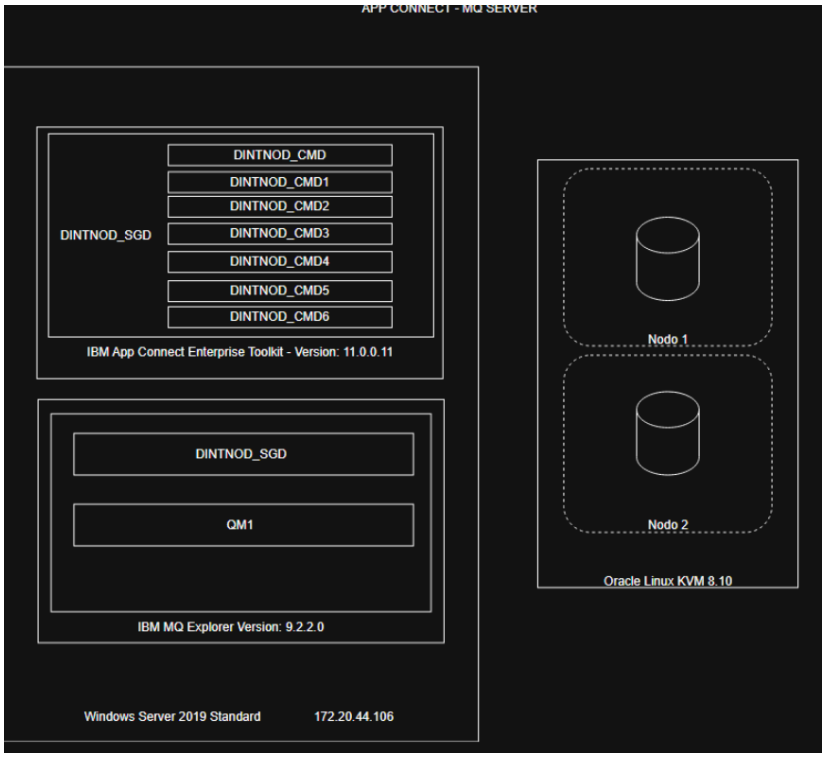


Ilustración 60 Diagrama App Connect

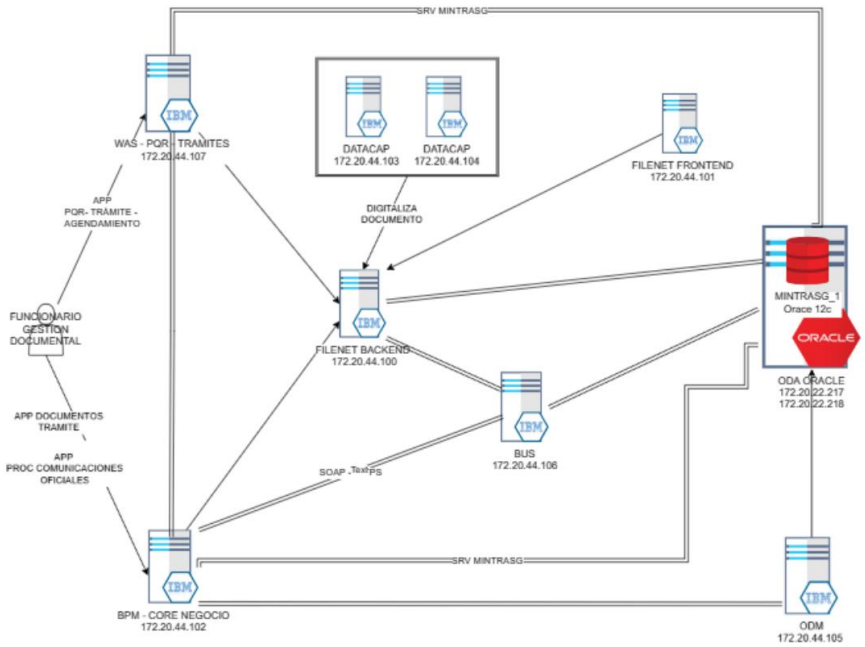


Ilustración 61 Arquitectura Gestor Documental

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 62 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 63 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
70	D55WJLL	IBM WebSphere Application Server Network Deployment Processor Value Unit (PVU) License + SW Subscription & Support 12 Months	29-Nov-2024 - 30-Nov-2025

www.rational.com/licensing

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 64 IBM Licenciamiento

Mes	Suma de Total Instancias
Enero 2025	111854
Febrero 2025	149070
Marzo 2025	148829
Abril 2025	135756
Mayo 2025	154121
Junio 2025	137472
Julio 2025	78502
Agosto 2025	92786
Septiembre 2025	164424
Octubre 2025	74524
Noviembre 2025	123254
Total acumulado	**1.370.592**

Tabla 49 Suma Instancias

Mes	Suma de Total Documentos
Enero 2025	149454
Febrero 2025	183729
Marzo 2025	193697
Abril 2025	180888
Mayo 2025	204354
Junio 2025	178790

Julio 2025	201882
Agosto 2025	190074
Septiembre 2025	208044
Octubre 2025	178349
Noviembre 2025	170835
Total acumulado	**2.037.596**

Tabla 50 Total Docs

Mes	Suma de Total radicados
Enero 2025	59197
Febrero 2025	70194
Marzo 2025	72317
Abril 2025	64370
Mayo 2025	73694
Junio 2025	63934
Julio 2025	79429
Agosto 2025	66811
Septiembre 2025	73473
Octubre 2025	66160
Noviembre 2025	58977
Total, acumulado	**748.556**

Tabla 51 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 52 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:

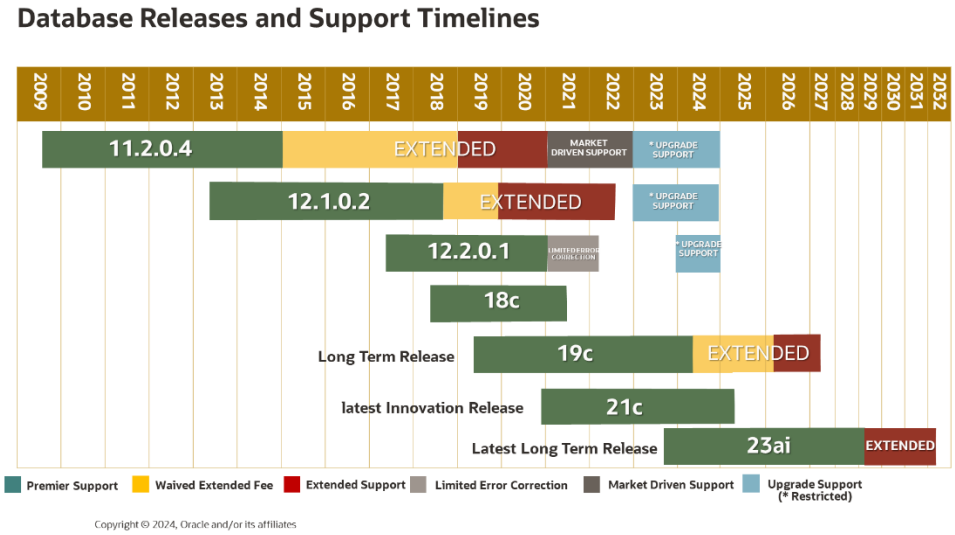


Ilustración 65 Estado Bases de Datos

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 53 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

INST_NAME	IP	SERVER_NAME	AMBIENTE	Version_Motor	S.O	MEMORIA GB	CPU	STORAGE ASIG GB	STORAGE USED GB	STORAGE FREE GB
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 54 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 55 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 66 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 67 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 68 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 69 Estadísticas Pool compartido

Tamaño base de datos MINSTRASG:

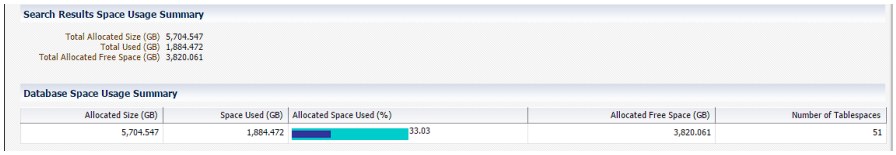


Ilustración 70 Tamaño DDBB

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 71 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

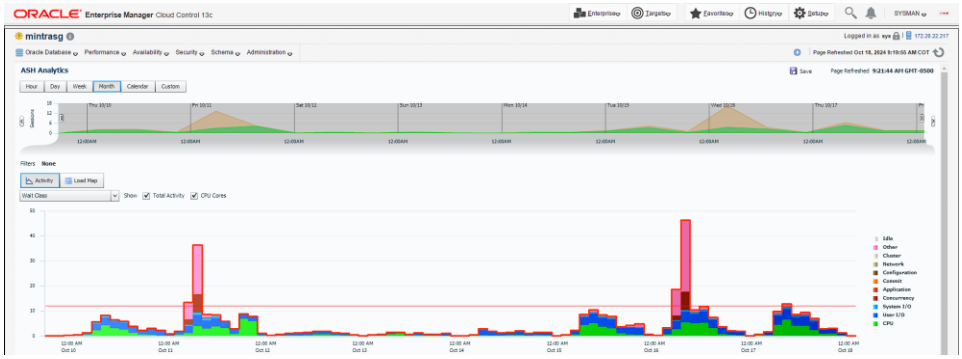


Ilustración 72 Rendimiento DDBB

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 73 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 74 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 75 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 76 Estadística Shared Pool

Tamaño base de datos DBMINTRA:

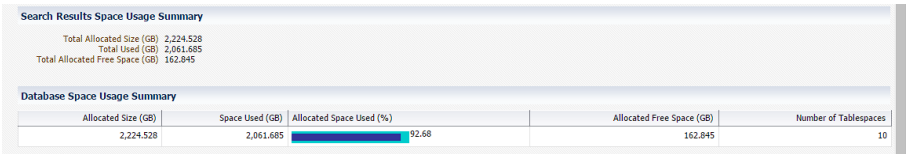


Ilustración 77 Tamaño DDBB DBMINTRA

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 78 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

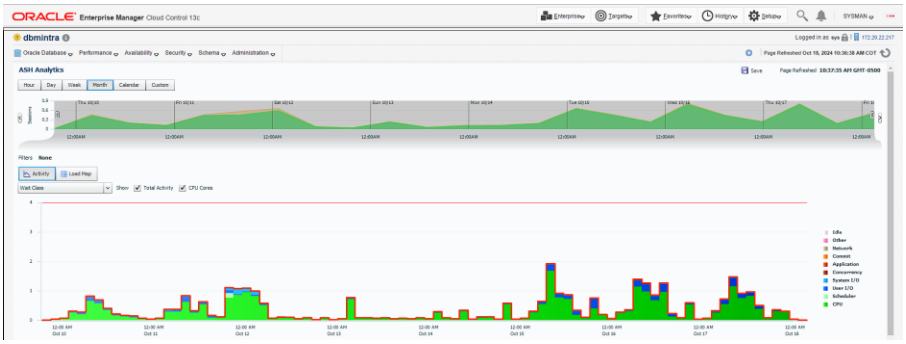


Ilustración 79 Rendimiento DDBB MINTRASG

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 80 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 81 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 82 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 83 Estadísticas Shared Pool

Tamaño base de datos PLIFERAY:

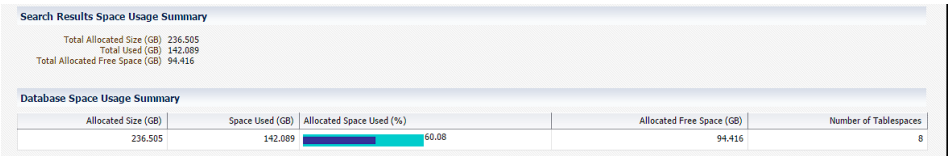


Ilustración 84 Tamaño DDBB PLifeRay

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 85 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

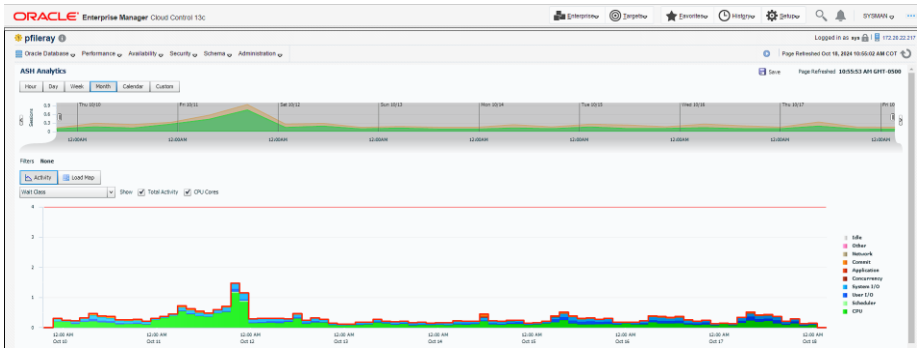


Ilustración 86 Rendimiento DDBB PlifeRay

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 87 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 88 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 89 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 90 Estadística Shared Pool

Tamaño base de datos SIGEP:

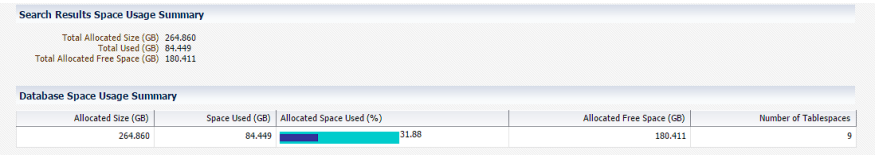


Ilustración 91 Tamaño DDBB SIGEP

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 92 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

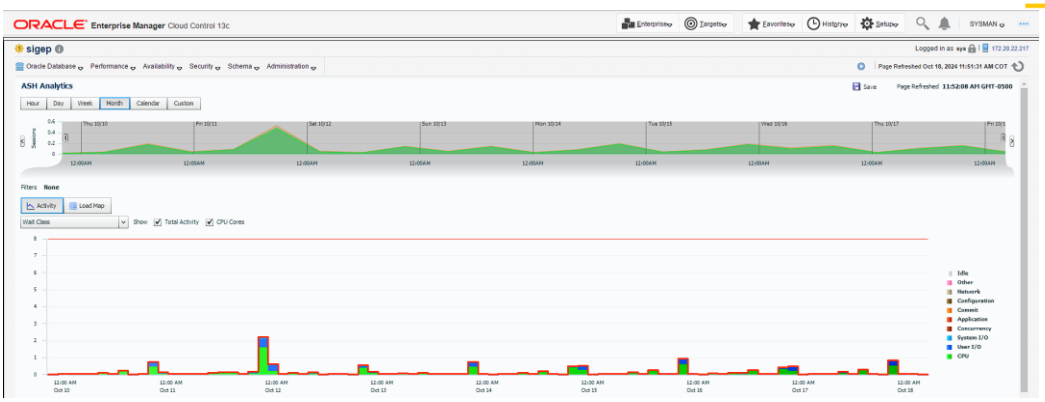


Ilustración 93 Rendimiento DDBB SIGEP

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 94 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 95 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 96 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 97 Estadística Shared Pool

Tamaño base de datos DBSIMPC:

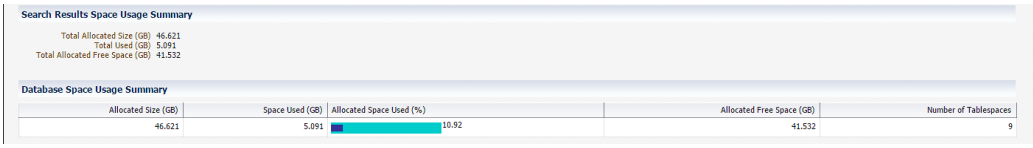


Ilustración 98 Tamaño DDBB SIMPC

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 99 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

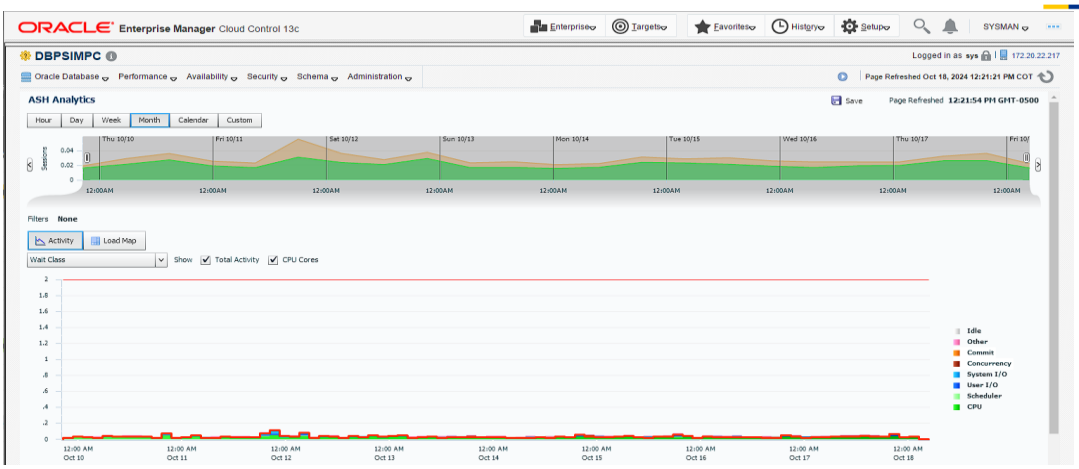


Ilustración 100 Rendimiento DDBB

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 101 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 102 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 103 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 104 Estadística Shared Pool

Tamaño base de datos MINTRASD:

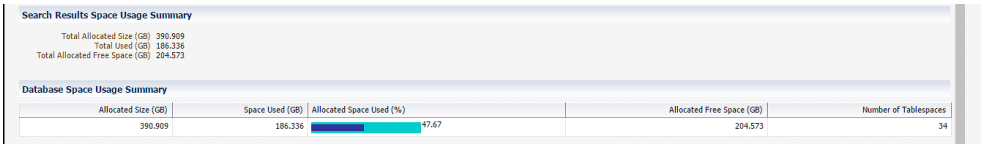


Ilustración 105 Tamaño DDBB MINTRASD

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

Tamaño de esquemas de base de datos:

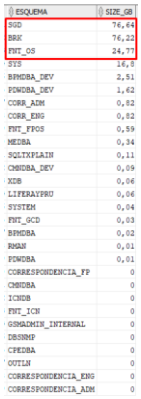


Ilustración 106 Tamaño Esquemas

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

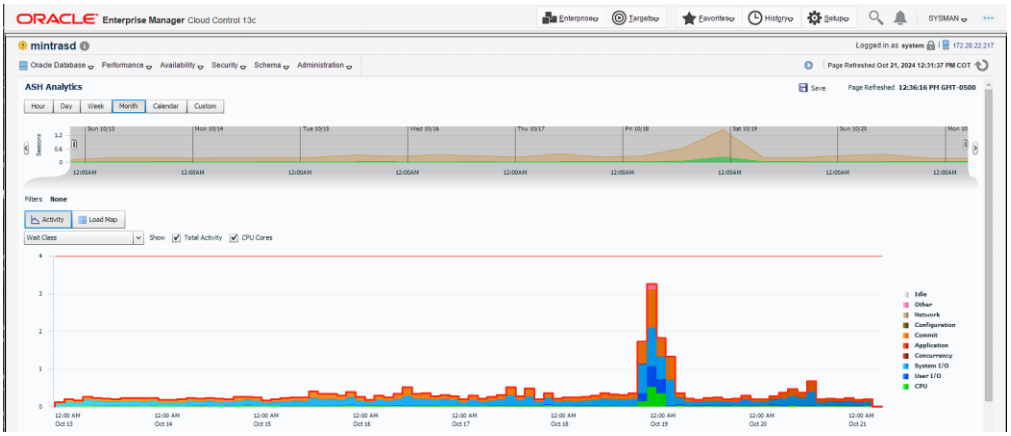


Ilustración 107 Rendimiento MINTRASD

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 108 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 109 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 110 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 111 Estadística Shared Pool

Tamaño base de datos MINTRASD:

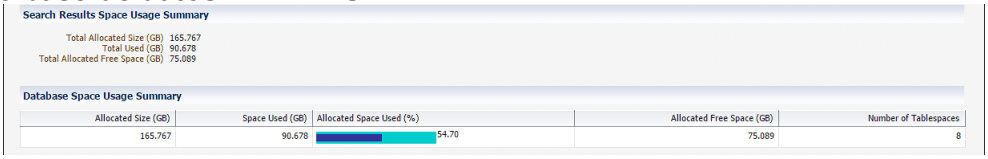


Ilustración 112 Tamaño DDBB

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
NEWIVCMI	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 113 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

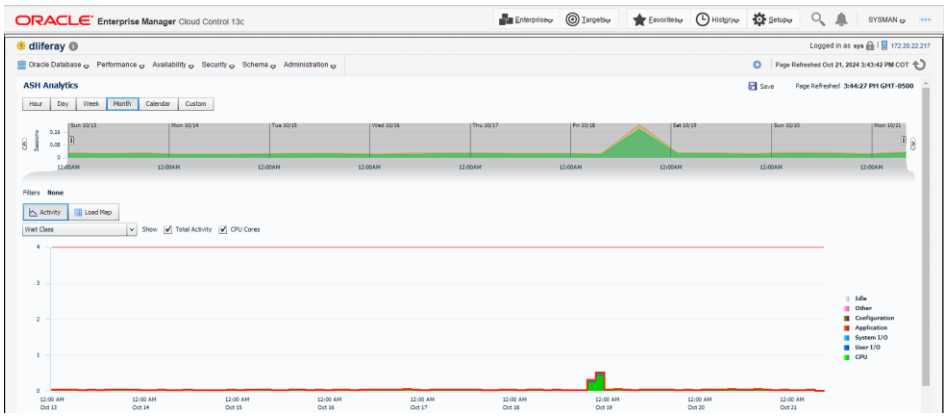


Ilustración 114 Rendimiento DDBB

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 115 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 116 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 117 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 118 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 119 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 120 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

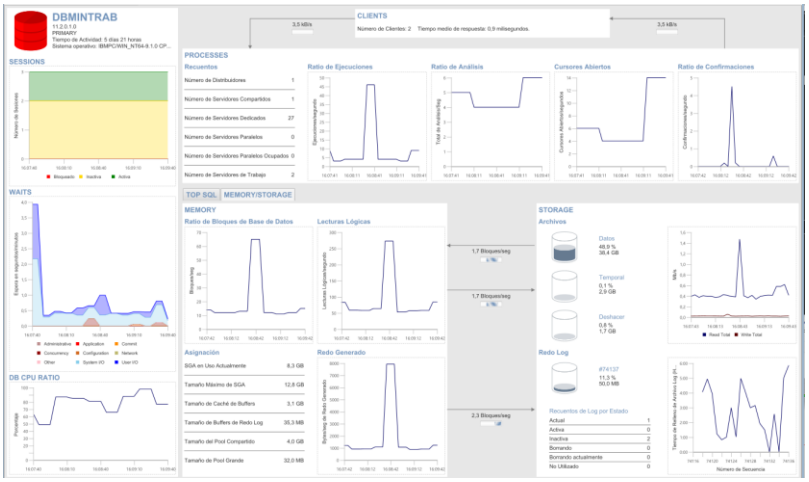


Ilustración 121 Rendimiento DDBB

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 122 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 123 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 124 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 125 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 126 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

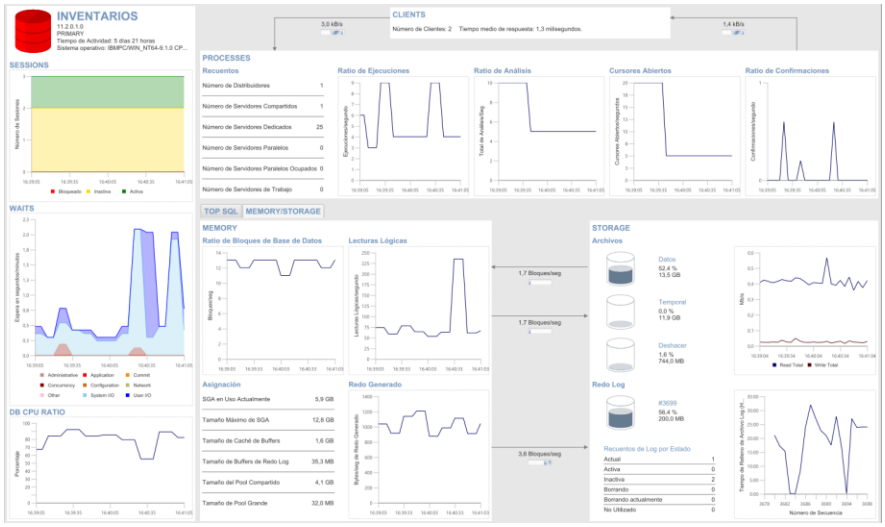


Ilustración 127 Comportamiento DDBB

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

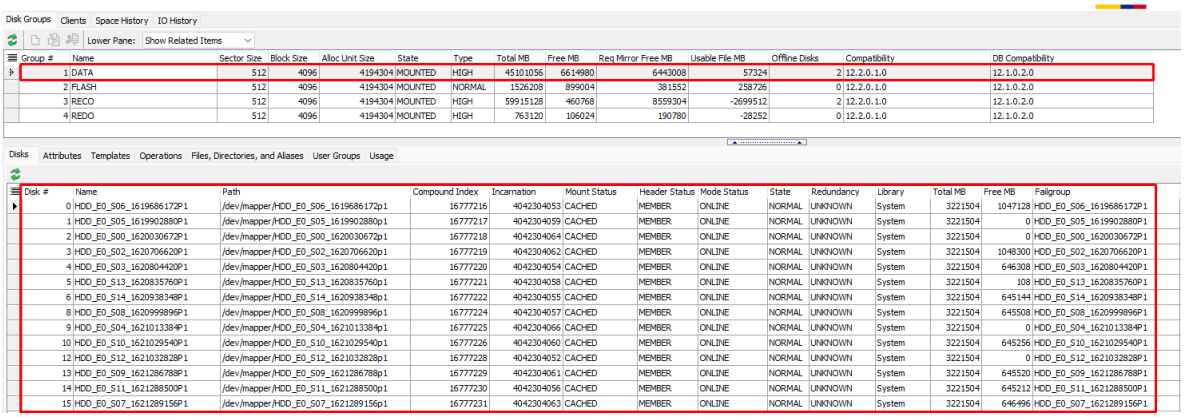
4.1 Almacenamiento General ASM:

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 128 Almacenamiento ASM

DISKGROUP DATA:



Disk Groups | Clients | Space History | IO History

Lower Pane: Show Related Items

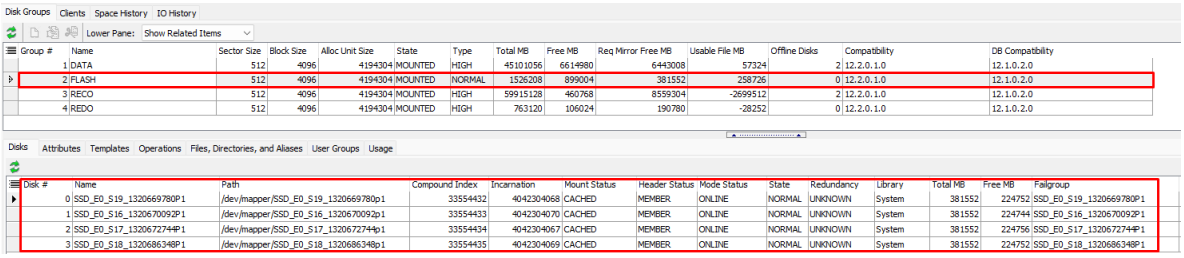
Group #	Name	Sector Size	Block Size	Alloc Unit Size	State	Type	Total MB	Free MB	Req Mirror Free MB	Usable File MB	Offline Disks	Compatibility	DB Compatibility
1	DATA	512	4096	4194304	MOUNTED	HIGH	45101056	6614980	6443008	57324	2	12.2.0.1.0	12.1.0.2.0
2	FLASH	512	4096	4194304	MOUNTED	NORMAL	1526208	899004	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 129 DiskGroup Data

DISKGROUP FLASH:



Disk Groups | Clients | Space History | IO History

Lower Pane: Show Related Items

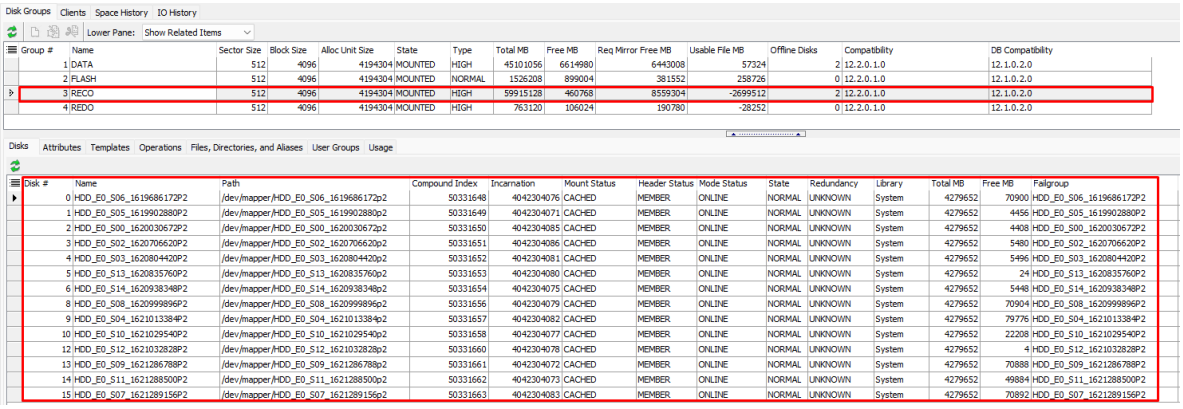
Group #	Name	Sector Size	Block Size	Alloc Unit Size	State	Type	Total MB	Free MB	Req Mirror Free MB	Usable File MB	Offline Disks	Compatibility	DB Compatibility
1	DATA	512	4096	4194304	MOUNTED	HIGH	45101056	6614980	6443008	57324	2	12.2.0.1.0	12.1.0.2.0
2	FLASH	512	4096	4194304	MOUNTED	NORMAL	1526208	899004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

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

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

Ilustración 130 DiskGroup Flash

DISKGROUP RECO:



Disk Groups | Clients | Space History | IO History

Lower Pane: Show Related Items

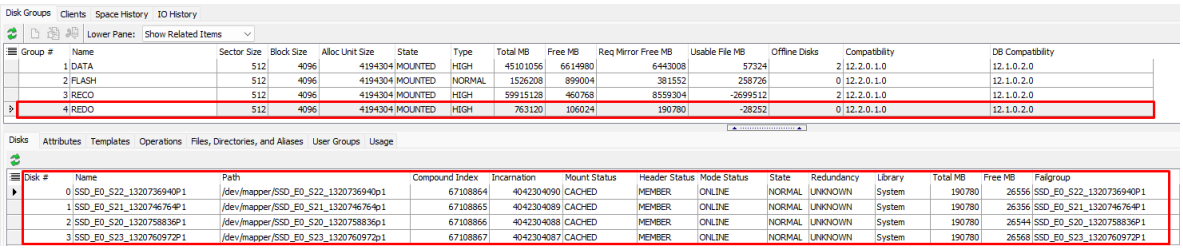
Group #	Name	Sector Size	Block Size	Alloc Unit Size	State	Type	Total MB	Free MB	Req Mirror Free MB	Usable File MB	Offline Disks	Compatibility	DB Compatibility
1	DATA	512	4096	4194304	MOUNTED	HIGH	45101056	6614980	6443008	57324	2	12.2.0.1.0	12.1.0.2.0
2	FLASH	512	4096	4194304	MOUNTED	NORMAL	1526208	899004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

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

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

Ilustración 131 DiskGroup Reco

DISKGROUP REDO:



Disk Groups | Clients | Space History | IO History

Lower Pane: Show Related Items

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

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

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

Ilustración 132 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 133 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 noviembre 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.

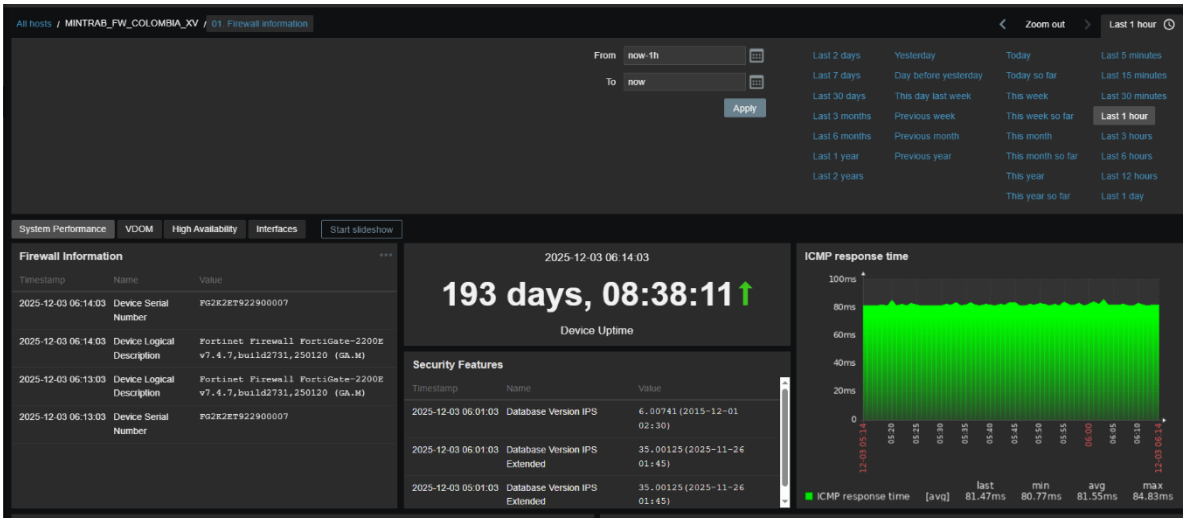


Ilustración *134* Firewall de nueva generación.

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 noviembre. 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 2 TB y 12 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	13 de noviembre, 25 de noviembre y 27 de noviembre: 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	8 de noviembre y 15-17 de noviembre: 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 56 Tendencia de uso de ancho de banda

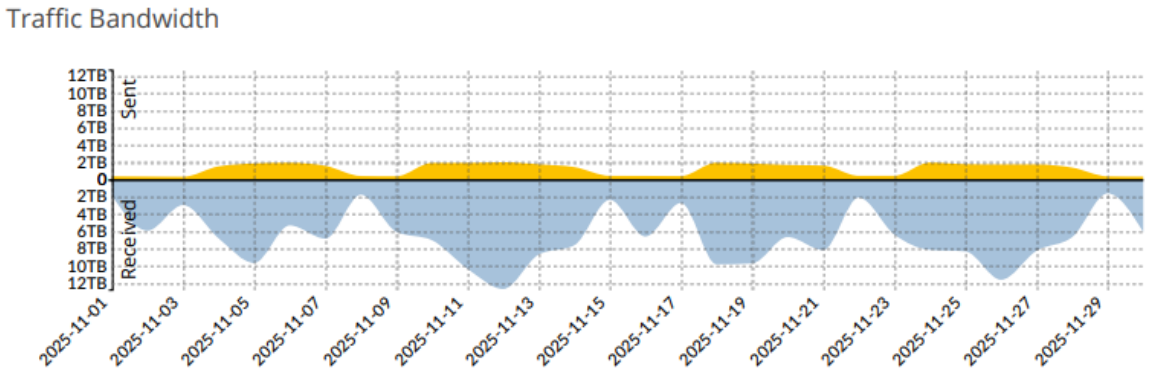


Ilustración 135 Comportamiento ancho de banda

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 noviembre. 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	**70.55 TB**	Tráfico extremadamente alto, servidor de almacenamiento, backup (MINTRABCKEXEC.mintrabajo.loc).
2	Mduarteo	**5.60 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	**5.35 TB**	IP interna — podría corresponder a servidor de aplicaciones o gestión. Revisar patrón de uso.
4	172.20.44.102	**4.21 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 57 usuarios con mayor consumo de ancho de banda

Top Users by Bandwidth

#	User(or IP)	Bytes	Sent	Received
1	172.20.22.251			70.55 TB
2	mduarteo			5.60 TB
3	172.28.28.38			5.35 TB
4	172.20.44.102			4.21 TB
5	172.20.22.27			2.43 TB
6	172.16.68.28			1.53 TB
7	172.20.44.106			1.16 TB
8	172.20.22.32			894.08 GB
9	10.200.1.35			886.67 GB
10	172.16.5.37			731.11 GB

Ilustración 136 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 noviembre 2025 del Ministerio de Trabajo, donde se listan los usuarios o direcciones IP que generaron el mayor número de sesiones de red durante el periodo.

Top Users by Sessions

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

Ilustración 137 Top de usuarios por números de sesiones

Análisis Top Users by Sessions

N°	Usuario/IP	Sesiones	Observaciones
1	**172.25.0.5**	**198.834.571**	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**	**72.139.7.50**	Usuario con actividad muy elevada. Puede estar vinculado a gestion de alguna plataforma(Mireya Duarte Osma)
3	**172.20.22.234**	**26.176.1.11**	Servidor interno asociado a un controlador de dominio.
4	**FORTINET**	**21.216.6.77**	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 58 Top de usuarios por sesiones

Top Applications by Bandwidth

La imagen corresponde al apartado “Top Applications by Bandwidth” del informe perimetral de noviembre 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			69.96 TB
2	HTTPS			31.29 TB
3	SMB			30.82 TB
4	TCP/445			15.72 TB
5	SYSLOG			7.40 TB
6	TCP/1521			6.75 TB
7	HTTP			6.45 TB
8	Microsoft.365.Portal			6.14 TB
9	Microsoft.SharePoint			5.04 TB
10	SSL			4.78 TB

Ilustración 138 Top de aplicaciones

Aplicación	Tamaño	Descripción
TCP/902	69.96 TB	Puerto comúnmente usado para VMware ESXi (administración de máquinas virtuales). Indica alto volumen de sincronización o replicación de entornos virtualizados.
2. HTTPS	31.29 TB	Tráfico web cifrado — servicios cloud, correo, portales institucionales. Representa la base del tráfico corporativo seguro.
3. SMB (Server Message Block)	30.82 TB	Protocolo de compartición de archivos en red. Muestra alto uso de repositorios compartidos internos.
4. TCP/445	15.72 TB	Asociado también a SMB y autenticación Windows (Active Directory). Indica intenso intercambio de archivos y autenticaciones.
5. SYSLOG	7.40 TB	Transmisión de logs desde dispositivos hacia el FortiAnalyzer o SIEM. Tráfico esperado y saludable para monitoreo de seguridad.
6. TCP/1521	6.75 TB	Puerto usado por Oracle Database. Indica consultas o réplicas intensivas en bases de datos institucionales.
7. HTTP	6.45 TB	Tráfico no cifrado. Nivel bajo comparado con HTTPS, lo que refleja correcta adopción de canales seguros.
8. Microsoft.Portal	6.14 TB	Tráfico asociado a la autenticación y uso de portales de Microsoft 365.
9. Microsoft.SharePoint	4.78 TB	Uso activo de bibliotecas documentales internas y colaboraciónen línea.

Tabla 59 Top de aplicaciones

Top 15 Authenticated Logins by VPN Connections

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

Authenticated Logins

#	User	Type	First Used	Total Number of Connections	Total Duration Connected(HH:MM:SS)
1	contaccenter	ssl-tunnel	2025-11-01 00:06:58	134	197:06:28
2	eyreyes	ssl-tunnel	2025-11-03 01:29:54	106	137:17:12
3	jmaestre	ssl-tunnel	2025-11-04 07:12:50	100	132:56:38
4	RMURCIA	ssl-tunnel	2025-11-02 21:05:32	98	148:31:26
5	aorozcoca	ssl-tunnel	2025-11-05 20:25:32	85	118:49:38
6	bcasas	ssl-tunnel	2025-11-02 14:22:04	85	75:50:26
7	dfdiazd@noc_indra	ssl-tunnel	2025-11-01 00:00:06	77	555:34:59
8	yjordan	ssl-tunnel	2025-11-01 00:04:10	74	188:42:42
9	cjimenez	ssl-tunnel	2025-11-03 16:43:50	70	75:13:02
10	jespinosam	ssl-tunnel	2025-11-04 11:55:06	63	200:06:27
11	ablanco	ssl-tunnel	2025-11-01 17:49:39	60	85:43:39
12	tecnicoamirl	ssl-tunnel	2025-11-05 10:04:52	58	138:02:01
13	mcarrascal	ssl-tunnel	2025-11-03 15:19:40	55	40:01:16
14	eortizfa	ssl-tunnel	2025-11-04 12:47:12	53	112:43:50
15	yrcifuentes	ssl-tunnel	2025-11-01 07:59:45	51	285:44:36

Ilustración 139 Top de Autenticación

Indicador	Descripción
Tipo de conexión	Todas las sesiones se realizaron mediante **SSL-Tunnel**, lo que indica que los usuarios accedieron a la red institucional a través de la **VPN segura de FortiGate**.
Usuarios más activos	**dfdiazd@noc_indra (555:34:59 h), yrciFuentes (285:44:36 h), jfortun (200:06:27 h), contaccenter (197:06:28 h), yjordan (188:42:42 h).** Estos usuarios mantienen sesiones prolongadas, indicando labores de monitoreo continuo o soporte crítico.
Mayor duración total	**El usuario con mayor tiempo acumulado es dfdiazd@noc_indra con 555 horas (~23 días) de conexión activa, reflejando un uso permanente asociado a operaciones del SOC o mesas de soporte 24/7.**
Mayor cantidad de conexiones	**Los usuarios con mayor número de sesiones iniciadas son: contaccenter (134), eyreyes (106), jmaestre (100), RMURCIA (98), aorozcoca (85), bcasas (85). Este patrón corresponde a reconexiones frecuentes típicas de personal operativo.**
Duraciones elevadas (>200 h)	**Usuarios con actividad superior a 200 horas: dfdiazd@noc_indra, yrciFuentes, jfortun. Requieren revisión para verificar legitimidad y necesidad operativa.**

Duraciones medias (100 h–190 h)	**Usuarios con uso estable y recurrente: contaccenter, eyreyes, jmaestre, RMURCIA, aorozcoca, yjordan, eortizfa (112 h). Indican trabajo remoto habitual o roles operativos.**
Duraciones bajas (<100 h)	**Usuarios con actividad puntual: **bcasas (75 h), ablanco (85 h), tecnicoamirl (58 sesiones/138 h)**, mcdarrascsl (40 h). Representan accesos ocasionales o de soporte específico. *Nota: tecnicoamirl tiene pocas conexiones pero alta duración acumulada.**

Tabla 60 Consolidado de indicadores

Failed Login Attempts by User

Esta imagen corresponde al apartado “Failed Login Attempts” del informe perimetral de noviembre 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	841
2	admin	ssl-web	403
3	support	ssl-web	298
4	test	ssl-web	283
5	User	ssl-web	252
6	sales	ssl-web	244
7	printer	ssl-web	238
8	scan	ssl-web	154
9	training	ssl-web	154
10	cradmin	ssl-web	140

Ilustración 140 sesiones fallidas

Análisis
Durante noviembre 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 noviembre de 2025, se generaron 100 eventos analizados, los cuales fueron limpiados de algún tipo de amenazas

Scan Statistics - Last 4 Weeks

Inputs	*Pending*	*Processing*	Malicious	High Risk	Medium Risk	Low Risk	Clean	Other	Total
Device	*0*	*0*	0	0	0	0	100	0	*100*
Adapter	*0*	*0*	0	0	0	0	0	0	*0*
On Demand	*0*	*0*	0	0	0	0	0	0	*0*
Network Share	*0*	*0*	0	0	0	0	0	0	*0*
Sniffer	*0*	*0*	0	0	0	0	0	0	*0*
URL	*0*	*0*	0	0	0	0	0	0	*0*
All Sources	*0*	*0*	0	0	0	0	100	0	*100*

File Scan - Last 4 Weeks

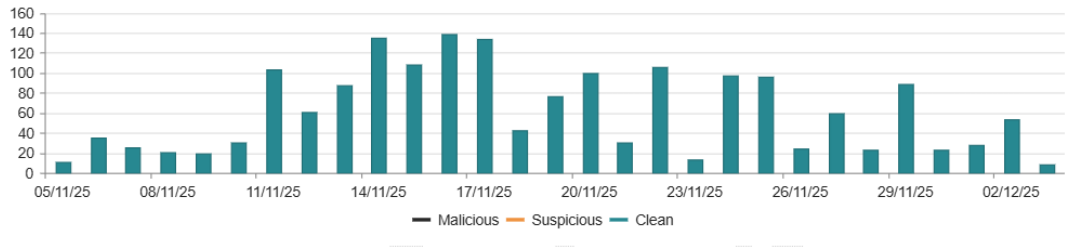


Ilustración 141 Reporte mensual noviembre

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

Perfomance

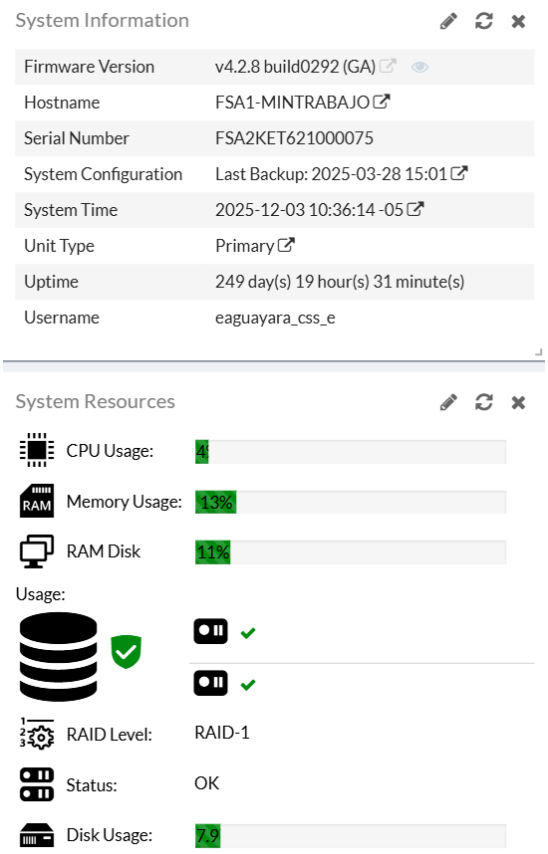


Ilustración 142 Captura de pantalla perfomance

Licencia Sandbox

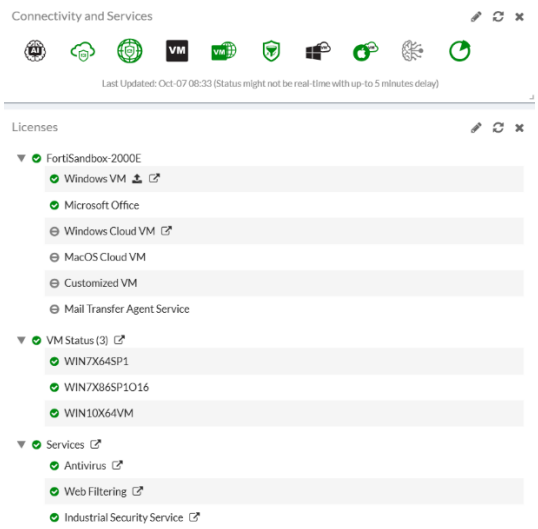


Ilustración 143 licencia sandbox

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

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

3.1.6.3.1 Casos de uso Fortisiem

Desempeño (performance)

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

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

Ilustración 144 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 145 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.

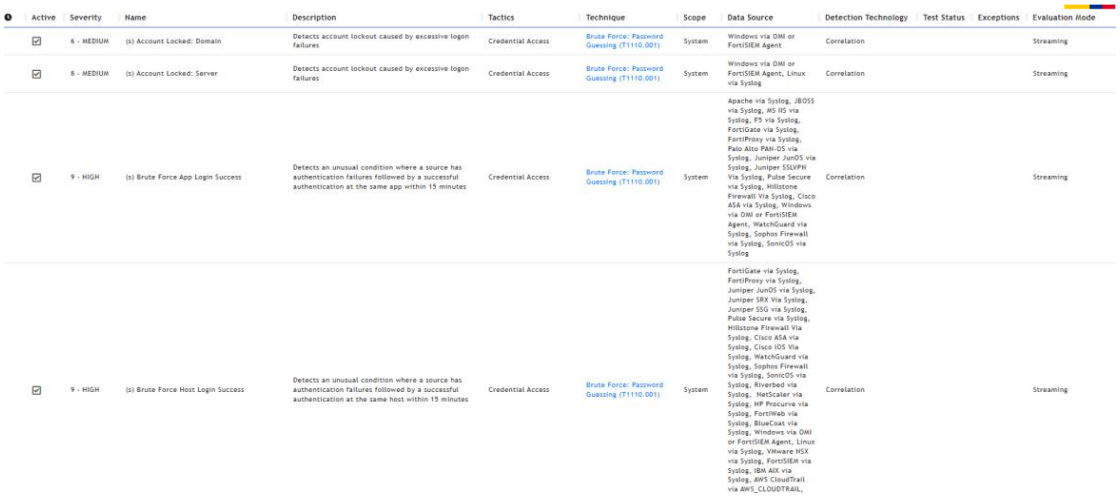
Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☐	4 - LOW	(s) Auto Service Stopped	Detects that an automatically running service stopped. Currently this works for windows servers and is detected via WMI.	Impact	Service Stop (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 146 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:

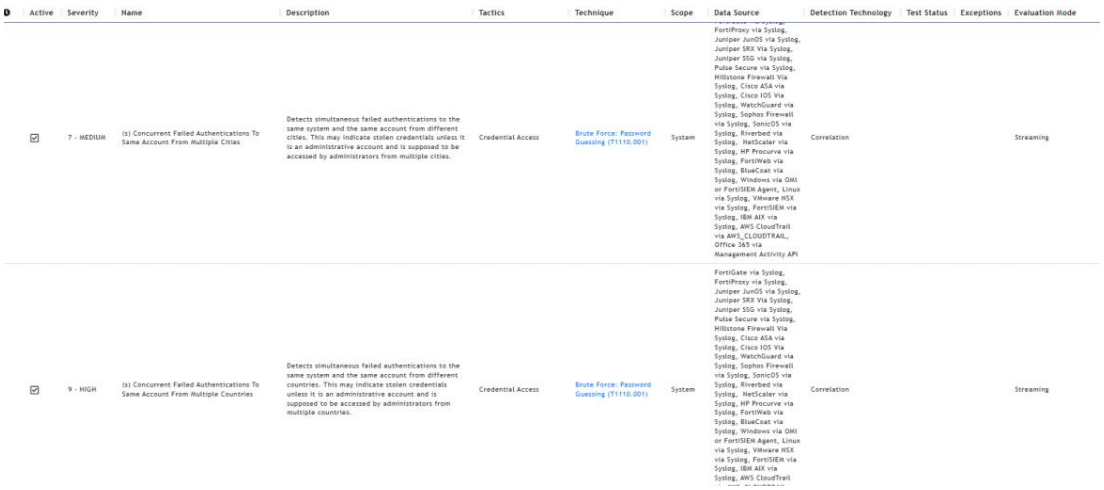
Los casos de uso de seguridad de autenticación en el FortiSIEM se centran en garantizar la integridad y la autenticidad de las credenciales de usuario en todos los dispositivos que tienen instalado el agente. Se muestran los casos Autenticación configurados para el ministerio de trabajo:



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 147 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 148 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 149 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 noviembre se registraron:

- 30.074 ataques web bloqueados por el perímetro.
- Intentos de acceso VPN no autorizados (sin intrusiones).

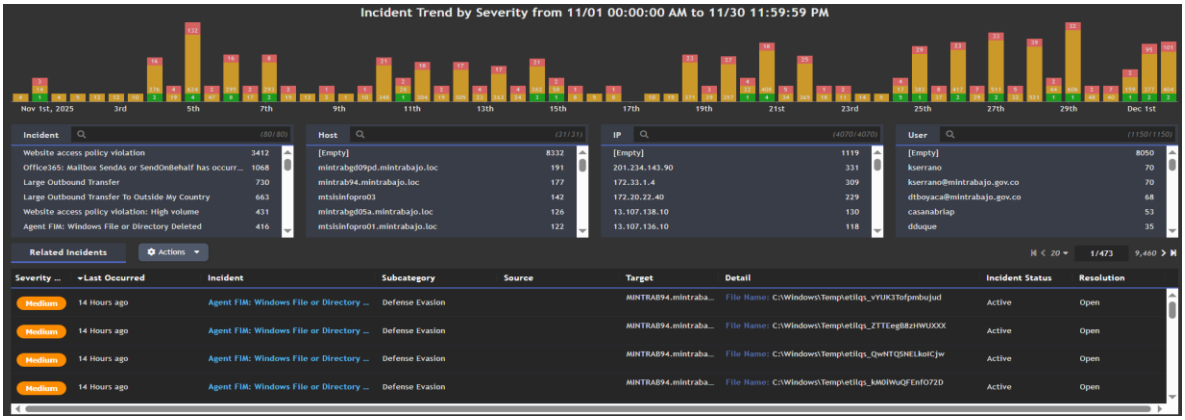


Ilustración 150 Detalle de incidentes

Análisis de incidentes

Tipo de incidente	Descripción	Volumen	Observaciones
Ataques web permitidos	Patrones conocidos (SQLi, Path Traversal)	22,427	Actividad intensa desde Internet
Violaciones de política web	Navegación no permitida	3,816	Requiere reforzar políticas internas
VPN fallida desde el extranjero	Intentos desde IP no autorizadas	1,95	Posibles ataques automatizados
Fallos múltiples VPN	Errores repetitivos de autenticación	1,927	Relacionado con fuerza bruta o fallos de usuario
Actividad Office365	Envíos desde buzones compartidos	1,13	Actividad válida pero sensible
Transferencias de gran volumen	Excesivo tráfico saliente	750	Posible fuga o carga de archivos

Tabla 61 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 noviembre. Ofrece información valiosa sobre los patrones de disponibilidad de servidores en lo relacionado con la última fecha de reinicio. A continuación, se presentan los hallazgos más relevantes:
Los servidores con mayor tiempo de disponibilidad continua en los últimos 30 días sin presentar eventos son:

Hallazgos relevantes:

- Servidores como MINTRAB03 y MINTRAB94 presentan más de 35 días de operación sin interrupciones.
- La latencia promedio es de 1 ms, indicando estabilidad total.
- Muestra un entorno estable y confiable, apto para soportar las operaciones institucionales.

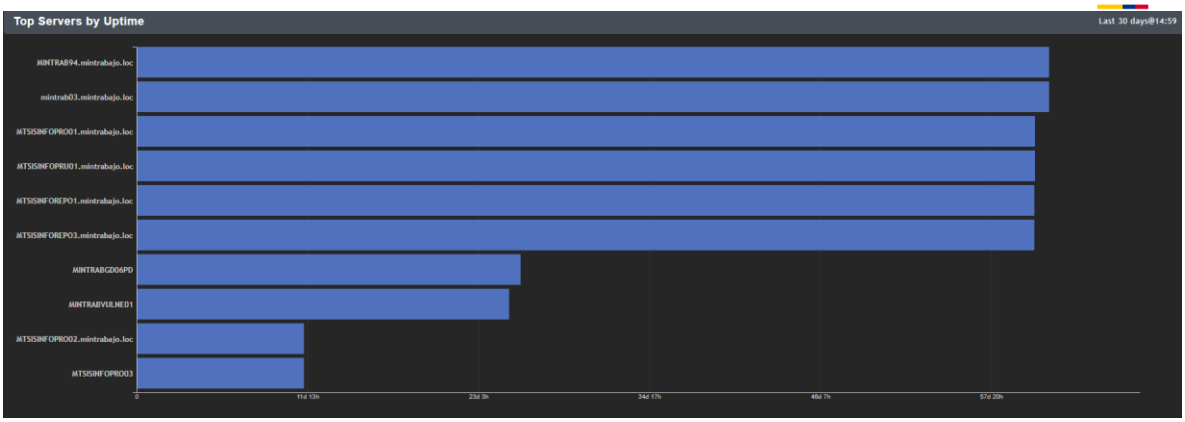


Ilustración 151 Detalle servidores

3.1.6.4.7 Top Aplicaciones por Bandwidth

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

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

Consumo predominante:

- SSL/HTTPS: 68.38 TB
- SSL: 53.07 TB

El tráfico revela un uso intensivo de:

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

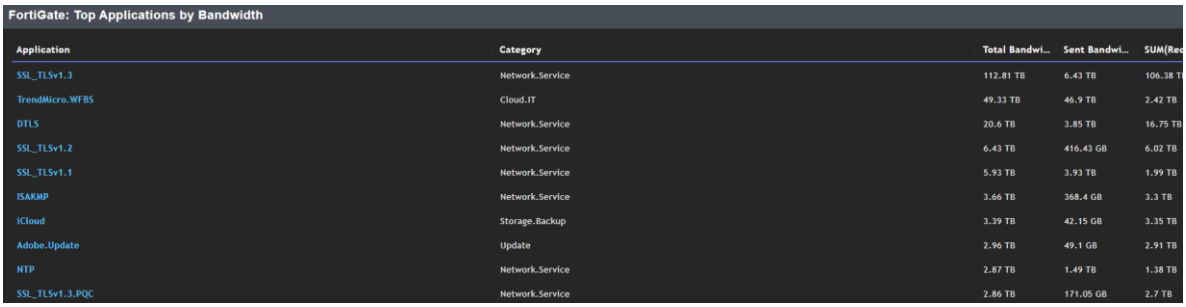


Ilustración 152 Detalle fortigate

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

Conclusiones

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

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

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

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

Durante el mes de noviembre, el WAF del Ministerio del Trabajo registró un volumen elevado de intentos de ataque, con patrones consistentes de explotación, divulgación de información y consultas sospechosas dirigidas a aplicaciones públicas institucionales.

El reporte confirma que el WAF está bloqueando correctamente los principales vectores identificados, sin evidencias de compromiso exitoso durante el periodo evaluado.

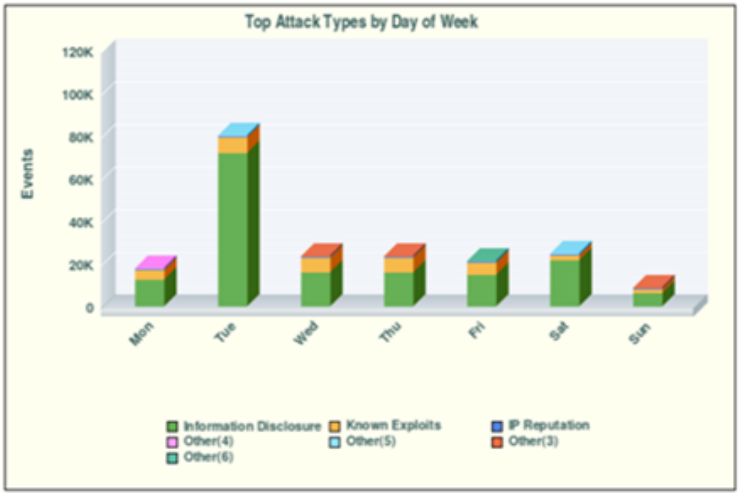


Ilustración 153 Top attack types

Análisis

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

Tipo de ataque

3.1.5.5 Solución de Anti-DDoS

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

Top Attacked SPPs

SPP	Direction	Drops	Events
PAGINA_MINTRABAJO	Outbound	394	27
GESTOR_DOC_MINT	Outbound	30	2

Ilustración 154 Top de ataques

Análisis Detallado:

PAGINA_MINTRABAJO también muestra un número considerable de intentos salientes bloqueados (27), lo que sugiere riesgo en aplicaciones web institucionales.

3.1.6.5.1 Login Fallidos

Durante el mes de noviembre, 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 noviembre 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-165763	18/11/2025 17:27	FortiSIEM Alert: TLP:RED - Mintrabajo - Traffic to Emerging Threat IP List	SOC	Seguridad Informática
RF-161800	4/11/2025 8:41	Habilitar acceso Pagina Web por el día de hoy 4/11/2025	SOC	Agregar a sitios permitidos
RF-167685	26/11/2025 7:04	Sitio fuera de Servicio	SOC	Agregar a sitios permitidos
RF-166384	20/11/2025 11:31	MINTRABAJO TLP:RED// TI – ShinySp1d3r - Nueva Amenaza de Ransomware-as-a-Service.	SOC	Crear politica
RF-166745	21/11/2025 10:35	Solicitud enrutamiento segmento wifi VISITANTES	SOC	Permitir acceso
RF-162889	7/11/2025 10:51	Solicitud Sesión de Pruebas SOC - Gestión Vulnerabilidades	SOC	Reportes Seguridad Informática
RF-168406	28/11/2025 7:25	RV: Proveído Ejecutivo: Conformidad con el Estatuto Procesal de Ejecución Integral EPEI-900/A	SOC	Revisar correo malicioso
RF-161938	4/11/2025 14:30	RV: CAUSA PROCESAL / ACTO EJECUTIVO RDO. 02803 2025 1082	SOC	Revisar correo malicioso
RF-162847	7/11/2025 10:04	RV: CONFIRMACION DE SOLICITUD A COMPARECER ANTE JUZGADO QUINTO PROMISCUO DEL SECTOR JUDICIAL DE BOGOTA	SOC	Revisar correo malicioso
RF-163004	7/11/2025 14:48	solicitud verificacion	SOC	Revisar correo malicioso
RF-164744	13/11/2025 11:31	RV: Demanda en su contra - Comunicación electrónica Radicado 11001-40-08-2025-29741	SOC	Revisar correo malicioso
RF-165190	14/11/2025 13:59	Posible correo sospechoso.	SOC	Revisar correo malicioso
RF-166276	20/11/2025 9:06	RE: Verificación obligatoria - Evite la suspensión de su cuenta.	SOC	Revisar correo malicioso
RF-166725	21/11/2025 9:58	Revisión de correo presunto pishing	SOC	Revisar correo malicioso

RF-167089	24/11/2025 10:40	El Requerimiento No. RF-165540 se le ha solucionado	SOC	Revisar correo malicioso
RF-167176	24/11/2025 14:19	Revisión de correo	SOC	Revisar correo malicioso
RF-167523	25/11/2025 14:20	Correo sospechoso	SOC	Revisar correo malicioso
RF-168136	27/11/2025 11:25	RV: COMUNICADO FORMAL DE PROCESO EN CURSO EN PLATAFORMA CIUDADANA	SOC	Revisar correo malicioso
RF-168164	27/11/2025 13:24	RV: Notificación nuevo comentario PQRSD 14632 - Solicitud entre autoridades	SOC	Revisar correo malicioso
RF-168165	27/11/2025 13:30	RV: Notificación cambio estado PQRSD 14632 - Solicitud entre autoridades	SOC	Revisar correo malicioso
RF-168166	27/11/2025 13:30	RV: 🎉 A Blue Week chegou com os maiores descontos do ano!	SOC	Revisar correo malicioso
RF-168167	27/11/2025 13:31	RV: Nuevo documento del proyecto: 27/11/2025	SOC	Revisar correo malicioso
RF-165626	18/11/2025 14:11	SOLICITUD VALIDACION APLICACIONES	SOC	Análisis vulnerabilidades
RF-165921	19/11/2025 10:18	Vulnerabilidad Crítica Detectada en FortiWeb Alerta TLP:CLEAR COLCERT AL-20251118	SOC	Análisis vulnerabilidades
RF-168404	28/11/2025 7:25	CORREO MALICIOSO	SOC	Análisis de Correos
RF-161964	4/11/2025 15:10	RE: Admisión Acción de Tutela Rad. 2025 001518	SOC	Análisis de Correos
RF-161967	4/11/2025 15:11	RE: JUZGADO 12 PENAL DE CIRCUITO, APERCIBIMIENTO DE DEMANDA	SOC	Análisis de Correos
RF-162154	5/11/2025 9:01	RV: DOCUMENTO COPIA CONSULTA JUDICIAL POR INCUMPLIMIENTO	SOC	Análisis de Correos
RF-163702	11/11/2025 10:11	RV: PROCESOS DISCIPLINARIO EN SU CONTRA REVISAR ARCHIVO CON LA INFORMACIÓN COMPLETA	SOC	Análisis de Correos
RF-166501	20/11/2025 15:25	Re: Demanda en su contra - Radicado 11001-31-09-2025-51402	SOC	Análisis de Correos
RF-167270	24/11/2025 16:22	Solicitud de revisión de información potencialmente sospechosa "Documento disponible en demanda en su contra y proceso de cobro coactivo"	SOC	Análisis de Correos
RF-162095	5/11/2025 5:22	FortiSIEM Alert: TLP:RED - Mintrabajo - Malware Alert Trend Micro	SOC	Análisis de Malware
RF-162538	6/11/2025 11:59	FortiSIEM Alert: TLP:RED - Mintrabajo - Office365: Suspicious File Type Uploaded	SOC	Análisis de Malware
RF-163374	10/11/2025 12:54	Escaneo de posible URL sospechosa de phishing	SOC	Análisis de Malware
RF-165889	19/11/2025 9:32	FortiSIEM Alert: TLP:RED - Mintrabajo - Malware Alert Trend Micro	SOC	Análisis de Malware
RF-161872	4/11/2025 11:05	FortiSIEM Alert: TLP:RED - Mintrabajo - Command interpreter in Windows cmd or powershell	SOC	Análisis de evento
RF-161878	4/11/2025 11:12	FortiSIEM Alert: TLP:RED - Mintrabajo - Command interpreter in Windows cmd or powershell	SOC	Análisis de evento
RF-165149	14/11/2025 11:46	FortiSIEM Alert: TLP:RED - Mintrabajo - Office365: Success Login Outside Colombia	SOC	Análisis de evento
RF-167776	26/11/2025 10:27	FortiSIEM Alert: TLP:RED - Mintrabajo - Traffic to Emerging Threat IP List	SOC	Análisis de evento
RF-167778	26/11/2025 10:29	FortiSIEM Alert: TLP:RED - Mintrabajo - Traffic to Emerging Threat IP List	SOC	Análisis de evento
RF-165173	14/11/2025 13:15	SOLICITUD VALIDACION VIDEO	SOC	Analisis de archivo
RF-168575	28/11/2025 14:37	Borrar hostname BOPLRICO de la consola de Antivirus.	SOC	Configuracion consola
RF-168477	28/11/2025 10:11	Borrar hostname BOPJGUTIERREZG de consola Antivirus.	SOC	Configuracion consola

RF-168452	28/11/2025 9:15	Borrar hostname BOPLRUBIOV de consola Antivirus.	SOC	Configuracion consola
RF-168339	27/11/2025 17:55	Eliminar hostname bopmpmedinar de la consola de Antivirus.	SOC	Configuracion consola
RF-168332	27/11/2025 17:09	Borrar hostname bopmzuluagar de la consola del antivirus.	SOC	Configuracion consola
RF-161925	4/11/2025 14:01	Borrar hostname BOPMPMORENO de consola trendmicro	SOC	Configuracion consola
RF-166762	21/11/2025 11:16	MINTRABAJO TLP:RED // Boletín Lite // TI - Botnet Tsundere; infraestructura de comando y control oculta a través de la red Ethereum.	SOC	Configuracion consola
RF-167071	24/11/2025 10:09	Solicitud de Licencia para desinstalar Antivirus	SOC	Configuracion consola
RF-167527	25/11/2025 14:36	Solicitud de Licencia para desinstalar Antivirus	SOC	Configuracion consola
RF-166070	19/11/2025 13:58	Eliminar hostname BOPJMONTESDEOCA de la consola de trendmicro	SOC	Instalacion
RF-166248	20/11/2025 8:03	Eliminar hostname BOPAGONZALEZ de la consola de trendmicro.	SOC	Instalacion

Tabla 62 Reporte de requerimientos noviembre

3.1.5.7 Análisis de riesgo

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

- **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 63 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 64 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 65 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:

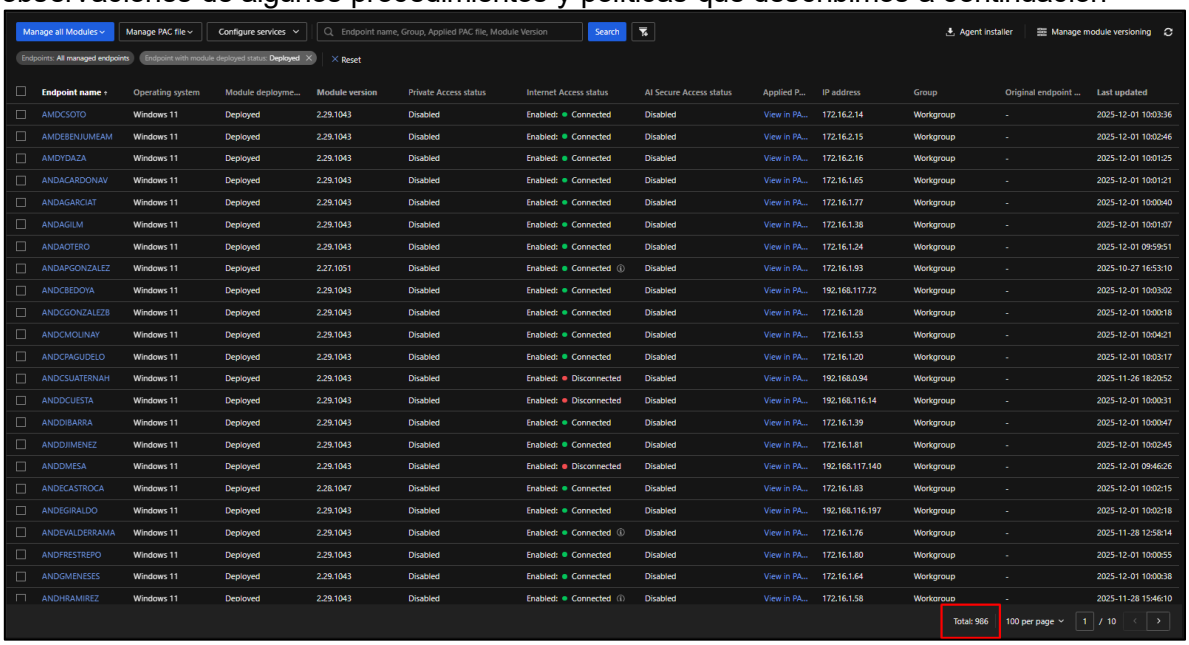
- Se están aplicando parches y actualizaciones de seguridad en la infraestructura de TI.
- Se realizó revisión periódica (semanal) de la matriz de vulnerabilidades y su priorización.
- Se realiza

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



Políticas y procedimientos

Actualmente, el servicio de Zero Trust Network Access (ZTNA) se encuentra en proceso de ajuste y optimización de las reglas de acceso a Internet. A la fecha, se han desplegado 986 agentes funcionales en las distintas Direcciones Territoriales (DTs), lo cual ha permitido establecer una capa adicional de protección frente a amenazas cibernéticas y prevenir posibles fugas de información. Esta implementación fortalece significativamente los mecanismos de control de acceso y seguridad en los equipos de la entidad

Boletines Seguridad

27/11/2025 – MINTRABAJO
Boletín // TI - Boletín Lite // TI - Vulnerabilidad en Microsoft Teams Expone a Usuarios a Malware y Phishing
Riesgo: Ataques selectivos contra infraestructuras críticas.

21/11/2025 – MINTRABAJO
Boletín Lite // TI - Boletín Lite // TI - Botnet Tsundere; infraestructura de comando y control oculta a través de la red Ethereum.

Riesgo: Botnet Tsundere usa blockchain y Node.js para operar modular, resiliente y altamente evasivo.

20/11/2025 – MINTRABAJO
Boletín // ShinySp1d3r - Nueva Amenaza de Ransomware-as-a-Service.
Riesgo: ShinySp1d3r es una nueva operación de ransomware-como-servicio desarrollada por actores vinculados a ShinyHunters, que incorpora un cifrador propio y funciones avanzadas para evadir registros del sistema, cerrar procesos y dificultar la recuperación de datos. Su diseño contempla propagación dentro de redes, eliminación de copias de seguridad y compatibilidad con entornos Windows, Linux y ESXi, posicionándose como una plataforma RaaS emergente con capacidades técnicas en rápida evolución

23/11/2025 – MINTRABAJO
Charla de Riego de Ciberseguridad

El ingeniero Edwin Walteros impartió una conferencia dirigida a todos los usuarios del Ministerio del Trabajo, en la cual se abordaron los principales riesgos de ciberseguridad que afectan tanto a los funcionarios como a la entidad. La sesión obtuvo una excelente calificación por parte de los asistentes, destacando la calidad de los contenidos y la claridad en la exposición.

3.1.6 Licenciamiento

A continuación, se presenta la información del licenciamiento:

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

Tabla 66 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	100,00%	99,70%
DC-5	Tiempo de solución de incidentes asociado a los servicios de aplicaciones especializadas	100,00%	90,00%
DC-6	Tiempo de solución de requerimientos asociado a los servicios de aplicaciones especializadas	100,00%	90,00%
DC-7	Continuidad y disponibilidad de los servicios de directorio activo	100,00%	99,60%
DC-8	Continuidad y disponibilidad de los servicios de seguridad informática	100,00%	99,90%

DC-9	Tiempo de solución de incidentes asociado a los servicios de administración, soporte y monitoreo	99,49%	90,00%
DC-10	Tiempo de solución de requerimientos asociado a los servicios de administración, soporte y monitoreo	99,98%	90,00%
DC-11	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 67 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 68 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 noviembre, no se observan caídas del canal, se tiene un consumo promedio de entrada de 33.26Mbps y 100.39 Mbps de salida.

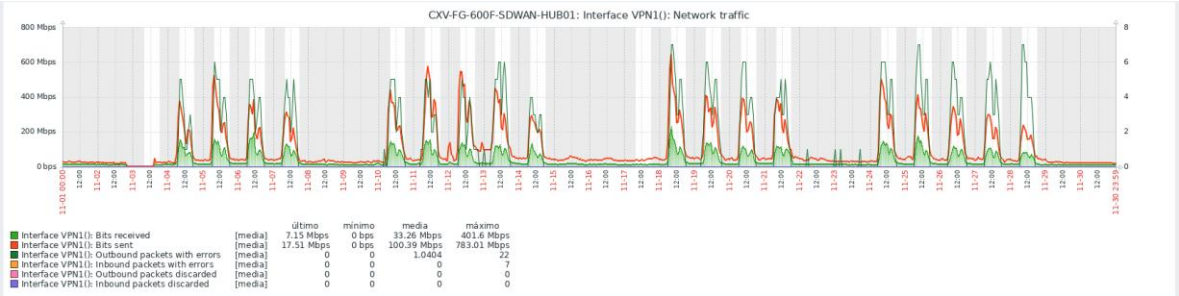


Ilustración 155 Consumo canal MPLS DC Principal

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

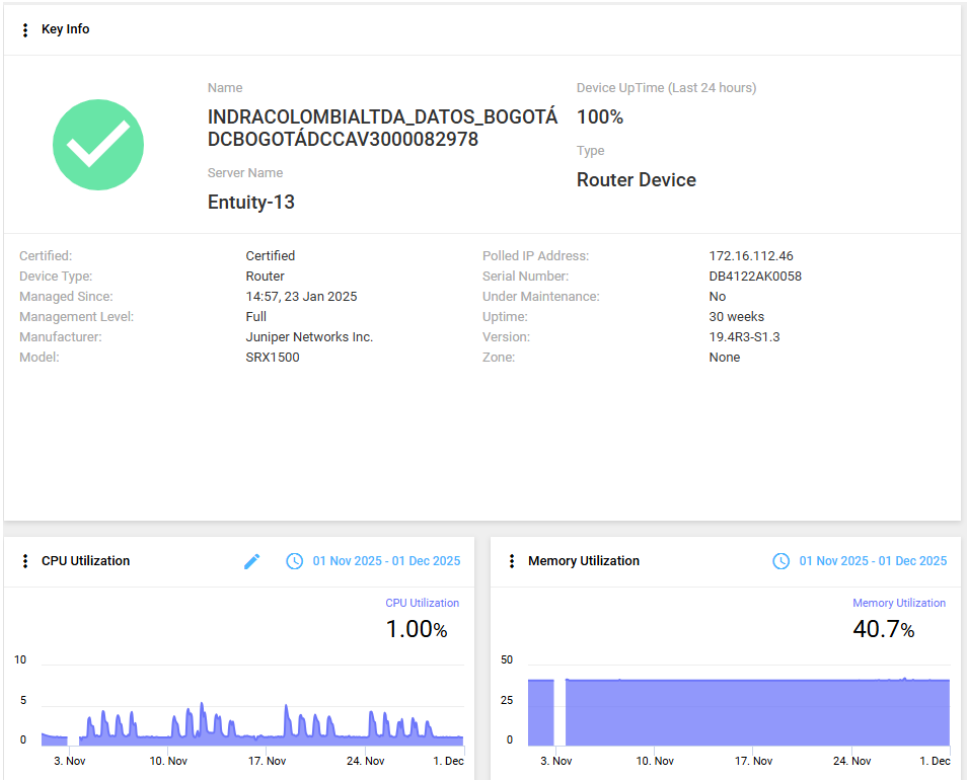


Ilustración 156 Estado Router MPLS DC Principal

3.3.1.1 Incidentes de Conectividad

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

Dirección territorial	Disponibilidad de la Sede	Caso Asociado
Caucasia	97,33%	IM-161621
Cisneros	97,33%	IM-161621
Guarne	97,33%	IM-161621
Santa Rosa	97,33%	IM-161621
Yarumal	97,33%	IM-161621
Tame	97,33%	IM-161621
Baranoa	97,33%	IM-161621
Carmen De Bolívar	97,33%	IM-161621
Magangué	97,33%	IM-161621
Chiquinquirá	97,33%	IM-161621
Duitama	97,33%	IM-161621
Guateque	97,33%	IM-161621
Soata	97,33%	IM-161621
Sogamoso	97,33%	IM-161621
La Dorada	97,33%	IM-161621
Manzanares	97,33%	IM-161621
Salamina	97,33%	IM-161621
El Doncello	97,33%	IM-161621
Paz De Ariporo	97,33%	IM-161621
Guapi	97,33%	IM-161621
Santander De Quilichao	97,33%	IM-161621
Bosconia	97,33%	IM-161621
Chiriguaná	97,33%	IM-161621
El Copey	97,33%	IM-161621
La Jagua De Ibirico	97,33%	IM-161621

Riosucio	97,33%	IM-161621
Istmina	97,33%	IM-161621
Cerete	97,33%	IM-161621
Lorica	97,33%	IM-161621
Montelíbano	97,33%	IM-161621
Planeta Rica	97,33%	IM-161621
Sahagún	97,33%	IM-161621
Chía	97,33%	IM-161621
Girardot	97,33%	IM-161621
Tocancipá	87,83%	IM-165788
Ubaté	82,53%	IM-166270
Villeta	97,33%	IM-161621
Fonseca	97,33%	IM-161621
Garzón	97,33%	IM-161621
Pitalito	97,33%	IM-161621
Ciénaga	97,33%	IM-161621
Fundación	97,33%	IM-161621
Plato	97,33%	IM-161621
Granada	97,33%	IM-161621
Puerto Gaitán	86,85%	IM-162097
Ipiales	97,33%	IM-161621
Tumaco	97,33%	IM-161621
Tuquerres	97,33%	IM-161621
Los Patios	97,33%	IM-161621
Salazar De Las Palmas	97,33%	IM-161621
San Juan Bautista De Chinácota	97,33%	IM-161621
Puerto Asís	97,33%	IM-161621
Orito	97,33%	IM-161621
Dosquebradas	97,33%	IM-161621
La Virginia	97,33%	IM-161621
Santa Rosa De Cabal	97,33%	IM-161621
Puerto Wilches	97,33%	IM-161621
Sabana De Torres	97,33%	IM-161621
San Vicente Chucurí	97,33%	IM-161621
Socorro	97,33%	IM-161621
Vélez	97,33%	IM-161621
Tolú	97,33%	IM-161621
Espinal	97,33%	IM-161621
Mariquita	99,35%	IM-163368
Turbo	97,33%	IM-161621
Buga	97,33%	IM-161621
Cartago	97,33%	IM-161621
Palmira	97,33%	IM-161621
Roldanillo	97,33%	IM-161621
Sevilla	97,33%	IM-161621
Tuluá	97,33%	IM-161621
Sede Territorial Florencia	94,99%	IM-163107
Sede Territorial Bucaramanga	99,44%	IM-166313

Tabla 69 Incidentes de conectividad

3.3.1.2 Topología Actual

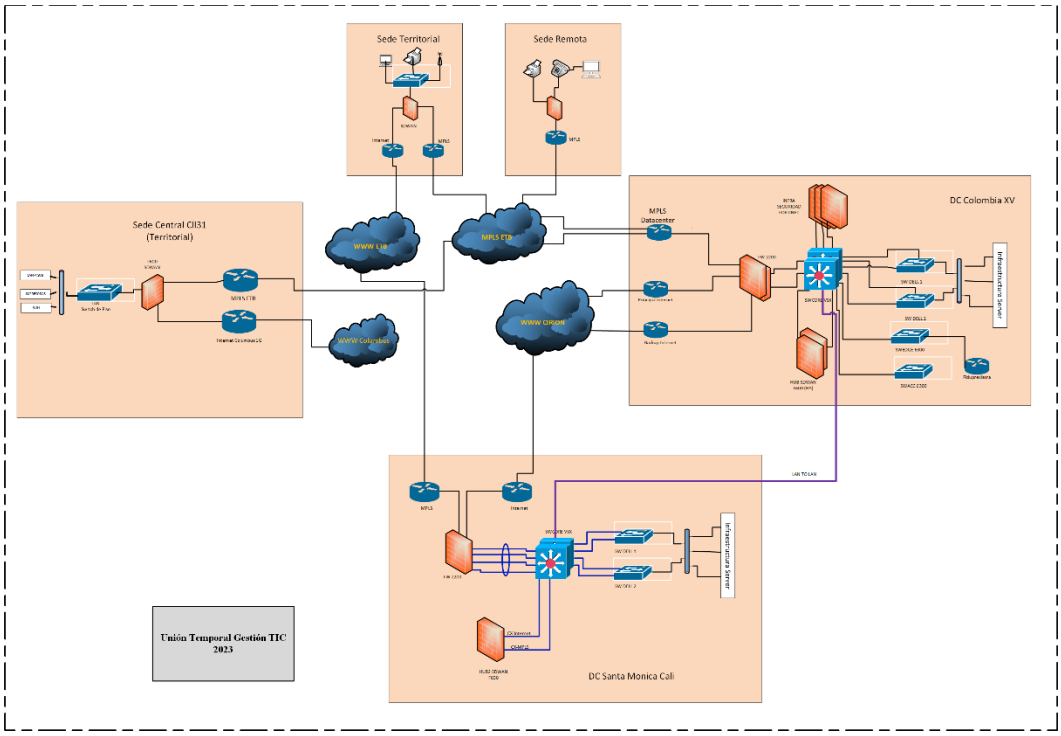


Ilustración 157 Topología actualizada

3.3.2 Canales SDWAN e Internet Dedicado

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

A nivel SDWAN se tienen los equipos registrados en la plataforma Fortimanager, desde donde se observa el estado de los equipos de las sedes territoriales e inspecciones, al igual que el estado de los túneles SDWAN establecidos contra el HUB SDWAN en Datacenter, se tienen 152 equipos registrados en esta plataforma.

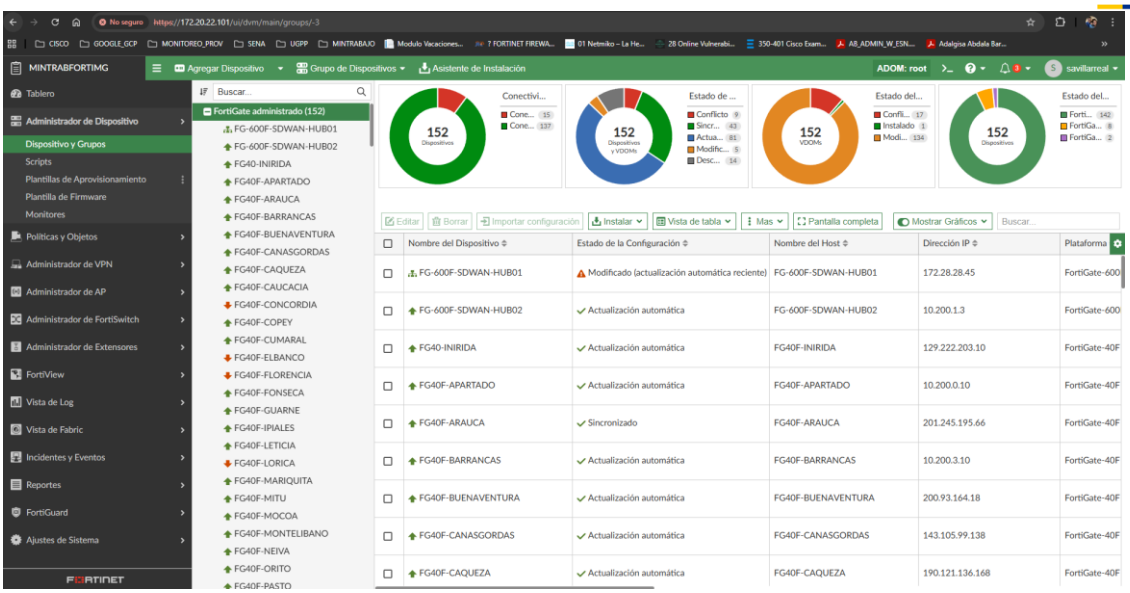


Ilustración 158 Interface Fortimanager

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 186.42 Mbps de consumo con un máximo de 1.37 Gbps, este canal es de 2GB, con el tráfico generado se observa que no presentó saturación durante el mes

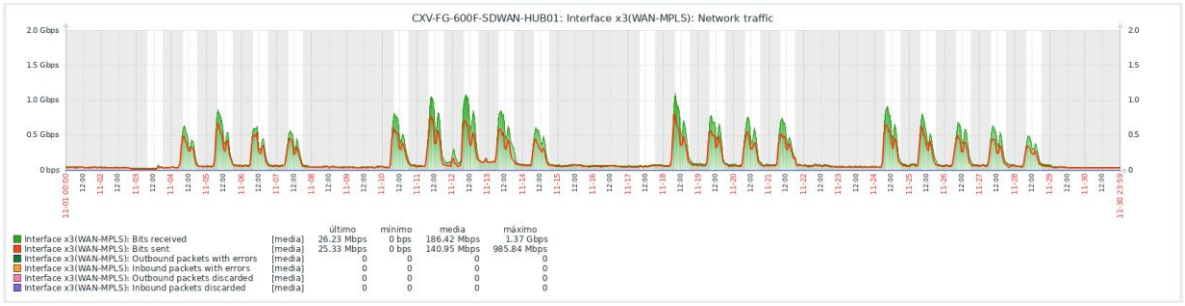


Ilustración 159 Interface MPLS HUB SDWAN

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 63.49Mbps de consumo en el mes donde se tuvo un máximo de 797.91 Mbps. Este canal es de 1GB, con el tráfico generado en el mes, no se presentó saturación.

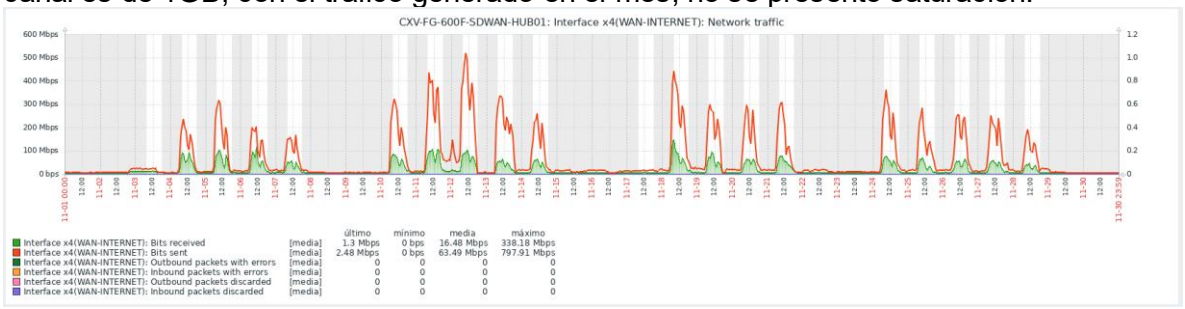


Ilustración 160 Interface Internet HUB SDWAN

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

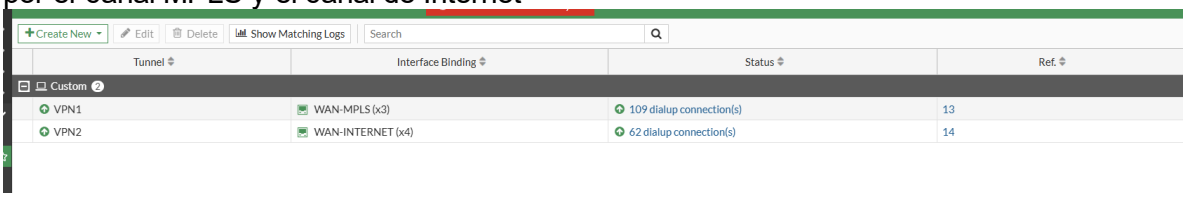


Ilustración 161 VPN SDWAN establecidas

El comportamiento del HUB SDWAN en cuanto a memoria y CPU, se observa que no ha tenido alto procesamiento, se observa un pico máximo de 21% de utilización de memoria y 9% de CPU, el equipo ha trabajado de forma estable sin presentar picos que causen algún bloqueo o algún reinicio de este.

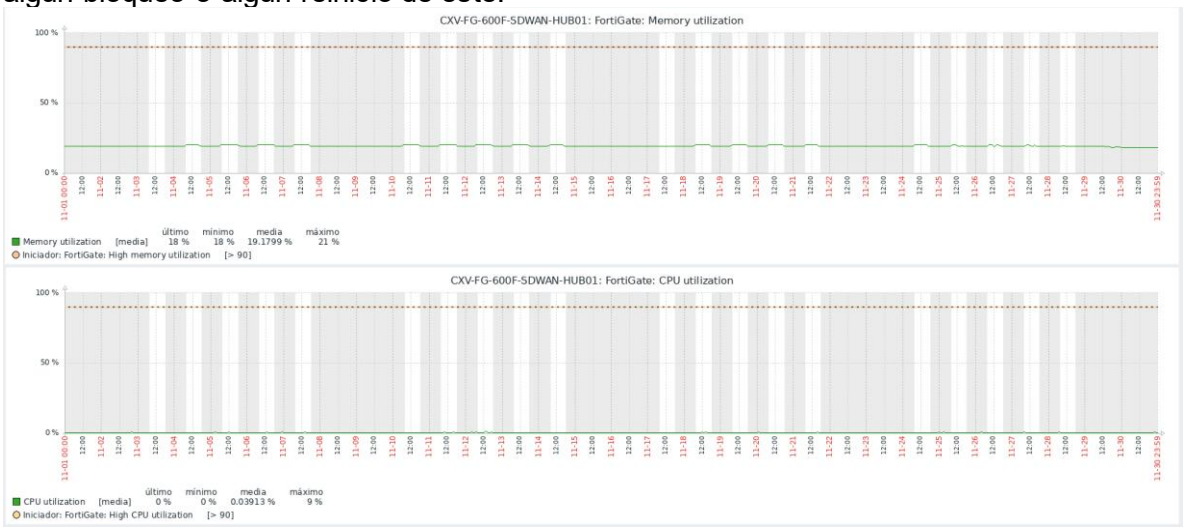


Ilustración 162 Estado HUB SDWAN Datacenter

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.

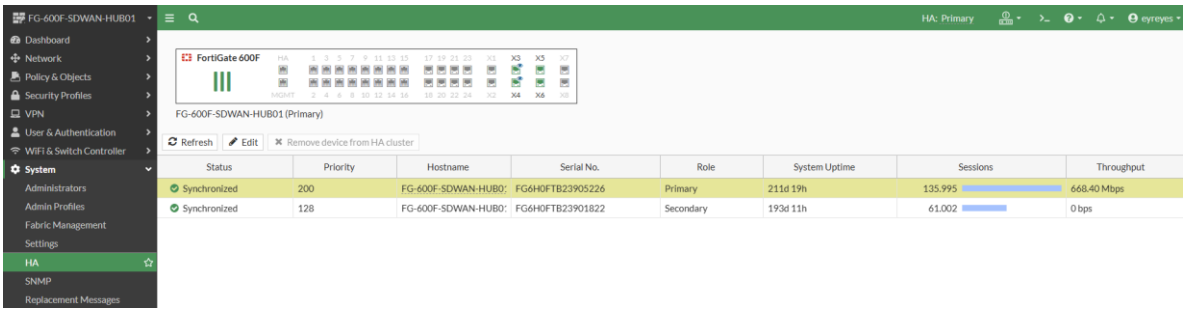


Ilustración 163 Estado HA HUB Sdwan

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

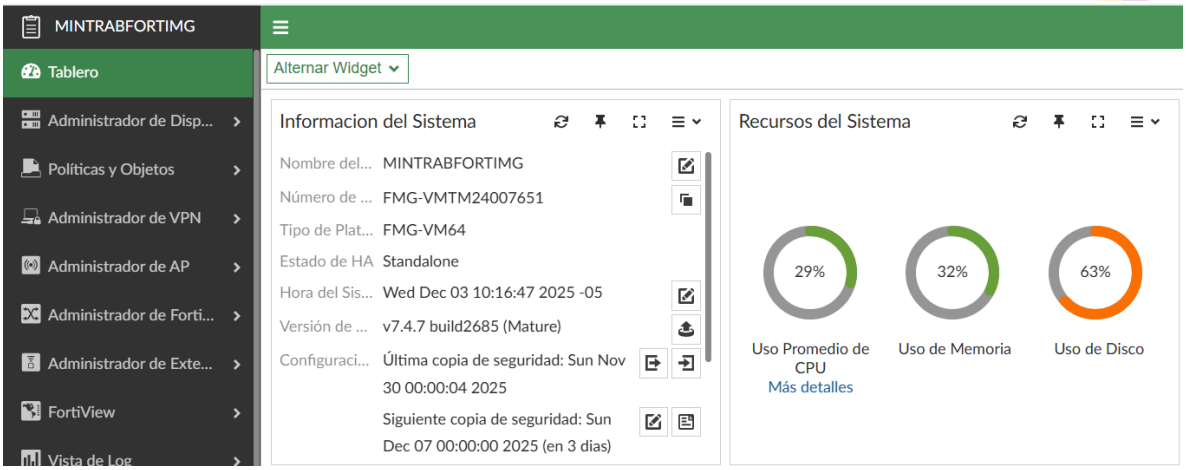


Ilustración 164 Recursos Fortimanager

Otras novedades del servicio:

Durante el mes de noviembre se realizaron las siguientes actividades:

- Se activó canal de internet en la inspección de Campo de la Cruz con el proveedor Tigo UNE.
- Se trabajo con el SOC en la mitigación de vulnerabilidades sobre el protocolo ICMP.
- Se activó servicio de internet a través de modem 4G en Inspección Patía.
- Se reservo IP y asigno ancho de banda para evento auditorio piso 5.
- Se gestionó revisión y mantenimiento de UPSs en sede central.

Medición de ANS Conectividad WAN e Internet

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

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

Tabla 70 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 Noviembre:

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

Dirección Territorial	% de Disponibilidad	Caso Asociado	% Penalidad	Valor Penalidad un enlace
Caucasia	97,33%	IM-161621	3%	$ 9.240
Cisneros	97,33%	IM-161621	3%	$ 9.240
Guarne	97,33%	IM-161621	3%	$ 9.240
Santa Rosa	97,33%	IM-161621	3%	$ 9.240
Yarumal	97,33%	IM-161621	3%	$ 9.240
Tame	97,33%	IM-161621	3%	$ 9.240
Baranoa	97,33%	IM-161621	3%	$ 9.240
Carmen De Bolívar	97,33%	IM-161621	3%	$ 9.240
Magangué	97,33%	IM-161621	3%	$ 9.240
Chiquinquirá	97,33%	IM-161621	3%	$ 9.240
Duitama	97,33%	IM-161621	3%	$ 9.240
Guateque	97,33%	IM-161621	3%	$ 9.240
Soata	97,33%	IM-161621	3%	$ 9.240
Sogamoso	97,33%	IM-161621	3%	$ 9.240
La Dorada	97,33%	IM-161621	3%	$ 9.240
Manzanares	97,33%	IM-161621	3%	$ 9.240
Salamina	97,33%	IM-161621	3%	$ 9.240
El Doncello	97,33%	IM-161621	3%	$ 5.544
Paz De Ariporo	97,33%	IM-161621	3%	$ 9.240
Guapi	97,33%	IM-161621	3%	$ 9.240
Santander De Quilichao	97,33%	IM-161621	3%	$ 23.101
Bosconia	97,33%	IM-161621	3%	$ 9.240
Chiriguaná	97,33%	IM-161621	3%	$ 9.240
El Copey	97,33%	IM-161621	3%	$ 9.240
La Jagua De Ibirico	97,33%	IM-161621	3%	$ 9.240
Riosucio	97,33%	IM-161621	3%	$ 9.240
Istmina	97,33%	IM-161621	3%	$ 9.240
Cerete	97,33%	IM-161621	3%	$ 9.240
Lorica	97,33%	IM-161621	3%	$ 9.240
Montelíbano	97,33%	IM-161621	3%	$ 9.240
Planeta Rica	97,33%	IM-161621	3%	$ 9.240
Sahagún	97,33%	IM-161621	3%	$ 9.240
Chía	97,33%	IM-161621	3%	$ 9.240
Girardot	97,33%	IM-161621	3%	$ 9.240
Tocancipá	87,83%	IM-165788	10%	$ 30.801
Ubaté	82,53%	IM-166270	20%	$ 61.603
Villeta	97,33%	IM-161621	3%	$ 9.240
Fonseca	97,33%	IM-161621	3%	$ 9.240
Garzón	97,33%	IM-161621	3%	$ 9.240
Pitalito	97,33%	IM-161621	3%	$ 9.240
Ciénaga	97,33%	IM-161621	3%	$ 9.240
Fundación	97,33%	IM-161621	3%	$ 9.240
Plato	97,33%	IM-161621	3%	$ 9.240
Granada	97,33%	IM-161621	3%	$ 9.240
Puerto Gaitán	86,85%	IM-162097	10%	$ 30.801
Ipiales	97,33%	IM-161621	3%	$ 9.240

Tumaco	97,33%	IM-161621	3%	$ 9.240
Tuquerres	97,33%	IM-161621	3%	$ 9.240
Los Patios	97,33%	IM-161621	3%	$ 9.240
Salazar De Las Palmas	97,33%	IM-161621	3%	$ 9.240
San Juan Bautista De Chinácota	97,33%	IM-161621	3%	$ 9.240
Puerto Asís	97,33%	IM-161621	3%	$ 9.240
Orito	97,33%	IM-161621	3%	$ 9.240
Dosquebradas	97,33%	IM-161621	3%	$ 9.240
La Virginia	97,33%	IM-161621	3%	$ 9.240
Santa Rosa De Cabal	97,33%	IM-161621	3%	$ 9.240
Puerto Wilches	97,33%	IM-161621	3%	$ 9.240
Sabana De Torres	97,33%	IM-161621	3%	$ 9.240
San Vicente Chucurí	97,33%	IM-161621	3%	$ 9.240
Socorro	97,33%	IM-161621	3%	$ 9.240
Vélez	97,33%	IM-161621	3%	$ 9.240
Tolú	97,33%	IM-161621	3%	$ 9.240
Espinal	97,33%	IM-161621	3%	$ 9.240
Mariquita	99,35%	IM-163368	3%	$ 9.240
Turbo	97,33%	IM-161621	3%	$ 9.240
Buga	97,33%	IM-161621	3%	$ 9.240
Cartago	97,33%	IM-161621	3%	$ 9.240
Palmira	97,33%	IM-161621	3%	$ 9.240
Roldanillo	97,33%	IM-161621	3%	$ 9.240
Sevilla	97,33%	IM-161621	3%	$ 9.240
Tuluá	97,33%	IM-161621	3%	$ 9.240
Total				**$ 761.720**

Tabla 71 Desagregado sedes con novedad un solo enlace

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

Dirección Territorial	% de Disponibilidad	Caso Asociado	% PENALIDAD	Valor Penalidad doble enlace
Sede Territorial Florencia	94,99%	IM-163107	10%	$ 81.261
Sede Territorial Bucaramanga	99,44%	IM-166313	3%	$ 60.946
Total				**$ 142.207**

Tabla 72 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. Así mismo, 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 73 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 NOVIEMBRE		
SEDE	**TIPO DE ELEMENTO**	**CANTIDAD**
Nivel Central	Portátil	7
DT Huila	Portátil	1
DT Meta	Portátil	1
DT Valle del Cauca	Portátil	2
DT Atlántico	Portátil	1
TOTAL		**12**

Tabla 74 Cantidades de equipos asignados nivel nacional

DEVOLUCION DE EQUIPOS NOVIEMBRE		
SEDE	**TIPO DE ELEMENTO**	**CANTIDAD**
DT Bogotá	Escritorio	1
DT Sucre	Escritorio	1
DT Sucre	Portátil	1
Insp.Soacha	Escritorio	1
Nivel Central	Portátil	18
TOTAL		**22**

Tabla 75 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 noviembre, se reportó un total de 20 casos de garantía a corte del periodo. A continuación, se detallan los estados asociados a estos casos:

Estado de caso	Cantidad
Cerrado	10
Proceso	1
Suspendido	9
Total	20

Tabla 76 Estado de casos de garantía.

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

ANS	Cerrado	Proceso	Suspendido	Total
CUMPLE	10	1	9	20
Total	10	1	9	20

Tabla 77 ANS casos de garantía.

Fecha de Reporte	Serial	Parte	Falla	Sede	No. Caso	Estado
4/11/2025	HC3BBKYN	Diadema	No funciona el audio	Nivel central	RF-161877	Cerrado
4/11/2025	HC3BBLN3	Diadema	No funciona el auricular izquierdo	Manizales	RF-161936	Cerrado
5/11/2025	HC3BBMXV	Diadema	Falla en sonido	Nivel central	RF-162292	Cerrado
6/11/2025	HC3BBN8B	Diadema	Presenta falla en audio	Nivel central	RF-162592	Cerrado
11/11/2025	HC3BBKWQ	Diadema	No funciona el auricular	Norte de Santander	RF-163700	Cerrado
11/11/2025	HC3BBL6S	Diadema	No se escucha	Nivel central	RF-163786	Cerrado
11/11/2025	HC3BBMVN	Diadema	Presenta daño en audio y micrófono	Nivel central	RF-163920	Cerrado
13/11/2025	HC3BBNAP	Diadema	Falla en los auriculares	Sucre	RF-164820	Cerrado
19/11/2025	HC3BBL4Z	Diadema	Presenta corto en el cable	Boyacá	RF-166094	Cerrado
27/11/2025	HC3BBLKL	Diadema	No tiene audio	Nivel central	RF-168135	Cerrado
27/11/2025	AVLC3C7A20C	Teclado	Algunas teclas se pegan	Nivel central	RF-168154	En proceso
13/11/2025	AVLC3C5A2T4	Teclado	Las teclas se sienten excesivamente rígidas al presionarlas	Bahía Solano Choco	RF-164672	Suspendido
13/11/2025	AVLC39SAJJ0	Mouse	Clic derecho queda pegado	Bahía Solano Choco	RF-164689	Suspendido
13/11/2025	VNAA64RN	Monitor	presenta falla en los pixeles de pantalla. Se	Istmina/choco	RF-164704	Suspendido
18/11/2025	MJ0LS5RW	Escritorio	No da imagen	Florencia	RF-165529	Suspendido
20/11/2025	PW0A3CHT	Portátil	No carga	Antioquia	RF-166319	Suspendido
20/11/2025	PW0A3CK9	Portátil	No funciona el Touchpad	Nivel central	RF-166457	Suspendido
24/11/2025	VNAA622P	Monitor	Imagen distorsionada durante el funcionamiento	Buenaventura	RF-167322	Suspendido
24/11/2025	VNAA64D3	Monitor	Imagen distorsionada durante el funcionamiento	Palmira	RF-167323	Suspendido
26/11/2025	VNAA62F0	Monitor	Pixeles muertos	Istmina/choco	RF-167816	Suspendido

Tabla 78 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 a accidentes o mal uso por parte del usuario final. 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	Asegurada realiza reposición de equipo	PRG_2025_3256134
Bernardo Ardila Fernández	PW09Z34H	DT Cesar	Golpes en esquinas	Reportado ante aseguradora	PRG_2025_4160592
Galia Lena Álvarez Hernández	PW0A3CHL	Nivel Central	Golpes en esquinas	Pendiente informe técnico para reporte ante aseguradora	
Ana Mireya Escobar Tierradentro	MJ0S5TW	DT Cauca	No enciende	Pendiente reposición del equipo	PRG_2025_1766918
Lacides 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 Córdoba	Golpes en esquinas	Reportado ante aseguradora	PRG_2025_4160302
William Ricardo Álvarez Gómez	PW0A3CK3	Nivel Central	Hurto	Aseguradora realiza reposición de equipo	PRG_2025_3861658
Miguel Ángel Izquierdo Hospital	PW0A3BFT	Nivel Central	Falla en puerto de carga por objeto	Reportado ante aseguradora	PRG_2025_4159804
Amber Duran Lozano	PW0A3BJM	Nivel Central	Reporta varias grietas en el equipo portátil	Se envía documentación para tramite con aseguradora	PRG_2025-4611910

Tabla 79 Equipos en siniestro

- **Instalaciones de Equipos y Entrega a Usuarios Finales:**

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

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

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

TIPO DE EQUIPO	CANTIDAD INSTALADA
Portátil	980
Escritorio	1142
Total	2122

Tabla 80 *Parque Computacional Instalado*

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 noviembre se gestionaron devoluciones de elementos asociados a novedades de funcionarios, tales como retiros, traslados, jubilaciones, entre otros.

DEVOLUCION DE EQUIPOS NOVIEMBRE		
SEDE	TIPO DE ELEMENTO	CANTIDAD
DT BOGOTA	ESCRITORIO	1
DT SUCRE	ESCRITORIO	1
DT SUCRE	PORTATIL	1
INSP.SOACHA	ESCRITORIO	1
NIVEL CENTRAL	PORTATIL	18
TOTAL		22

Tabla 81 Devolución de equipos

CANTIDAD DE EQUIPOS		
LUGAR	PORTATIL	ESCRITORIO
ALMACEN	140	30
OPERACIÓN	980	1142
TOTAL	1120	1172

Tabla 82 cantidad de equipos

4.1.1 Equipos de Escritorio

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

- Se registraron en Aranda un total de 20 solicitudes tipificadas así:
  - Incidentes – 0 casos
  - Requerimientos – 20 casos

- Al corte de mes quedaron en estado:
  - Cerrado – 10 casos.
  - Suspendido - 9 casos.
  - En Proceso – 1 caso.

- 19 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	19
Total, general	20

Tabla 83 Solicitudes de Equipos Usuario Final – Según Grupo Responsable

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

Tipificación / Categoría	Cantidad de Solicitudes
Incidentes	**0**
Requerimientos	**20**
Equipo Periférico	13
Equipo Escritorio	5
Equipo Portátil	2
Total	20

Tabla 84 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	100,00%	90,00%
EUF-2	Cumplimiento en la entrega del informe	100,00%	100,00%

Tabla 85 Medición ANS Equipos de Usuario Final

4.2 Conectividad LAN y WLAN

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

- Se realizó gestión en la revisión y solución de alertas sobre dispositivos como Access Point con la colaboración de los soportes en sitio.
- Se realizó gestión y seguimiento a alertas sobres canales de comunicación para lograr el restablecimiento del servicio por parte del proveedor de conectividad.
- Se activó canal de internet en la inspección de Campo de la Cruz con el proveedor Tigo UNE.
- Se trabajo con el SOC en la mitigación de vulnerabilidades sobre el protocolo ICMP.
- Se reservo IP y asigno ancho de banda para evento auditorio piso 5.
- Se tiene pendiente 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.
- **Red WiFi gratis para la gente**: Para las Direcciones Territoriales y Oficinas Especiales, se tiene habilitada la red inalámbrica Zona WiFi gratis, este servicio de WIFI gratis para la gente se presta a través de un portal cautivo, el cual ya se encuentra disponible en las sedes del Ministerio que cuentan con servicio de WLAN. Con el fin de hacer la divulgación correspondiente que incluye la señalización informativa de la red; durante noviembre de 2025 se hizo entrega de la señalética en Nivel Central y se empezó a distribuir en las sedes, estos avisos están alineados con los requisitos de MINTIC para las zonas de acceso público y gratuito de internet inalámbrico bajo la resolución 3436 de 2017 la cual deben cumplir todas las entidades públicas del orden nacional. Desde el 26/11/2025 se empiezan a recibir en las sedes para instalación gestionada por cada territorial, se notifica al equipo de soporte para que conozcan el alcance de la UT.

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

- Los especialistas gestionaron un total de 19 solicitudes escaladas a través de la herramienta Aranda. Al corte del mes, 14 casos quedaron en estado Cerrado, 1 en estado No ejecutado y 4 en estado Suspendido. los casos obedecen a cambios de actualización de dispositivos, revisión y pruebas de red en canales de internet, revisión de alerta en dispositivos de red, habilitar puntos de red.

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

Categoría	Cantidad de solicitudes
Equipo Conectividad Internet	4
Switch	3

Sin servicio	3
Actualización de Software	2
FortiGate	2

Tabla 86 Top 5 de categorías en el Servicio de conectividad LAN-WLAN



Ilustración 165 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 87 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 88 Distribución y Cantidades de Switch 48 puertos

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

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

4.2.5 Puntos de Acceso

Se encuentran operativos y en monitoreo los siguientes equipos:

Dirección Territorial	Población y/o ciudad de ubicación	Cantidad Access Points
Territorial Antioquia	MEDELLIN	4
Territorial Arauca	ARAUCA	1
Territorial Atlántico	BARRANQUILLA	3
OE Barrancabermeja	BARRANCABERMEJA	2
Calle 32	BOGOTA	4
Territorial Bolívar	Cartagena	2
Territorial Boyacá	TUNJA	2
Territorial Caldas	MANIZALEZ	2
Territorial Caquetá	FLORENCIA	1
Territorial Casanare	YOPAL	2
Territorial Cauca	POPAYAN	2
Territorial Cesar	VALLEDUPAR	2
Territorial Chocó	QUIBDÓ	2
Territorial Córdoba	MONTERIA	2
Territorial Cundinamarca	FACATATIVÁ	2
Territorial Guajira	RIOHACHA	2
Territorial Huila	NEIVA	0
Territorial Magdalena	SANTA MARTA	2
Territorial Meta	VILLAVICENCIO	3
Territorial Nariño	PASTO	2
Territorial Norte de Santander	CÚCUTA	3
Territorial Putumayo	MOCOA	1
Territorial Quindío	ARMENIA	3
Territorial Risaralda	PEREIRA	2
Territorial Santander	BUCARAMANGA	1
Territorial Sucre	SINCELEJO	2
Territorial Tolima	IBAGUÉ	3*
OE Urabá Apartadó	APARTADÓ	2
Territorial Valle	CALI	4
OE Buenaventura	BUENAVENTURA	1
Sede Nivel Central	BOGOTA	47
	Total	**111**

Tabla 89 Distribución de puntos de acceso

Territorial Norte de Santander - Cúcuta: El AP fue enviado e instalado en la DT Santander / Bucaramanga
Calle 32: 5 Access Point se desinstaló por cierre de oficina y se instaló en sede central.
Territorial Tolima -Ibagué: En la sede permitieron la instalación de 3 AP y 1 equipo restante se encontraba en Stock. El 11/06/2025 se gestionó la recolección del AP disponible y se envió a sede Central.

- Medición de ANS LAN y WLAN

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

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

Tabla 90 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 91 Equipos gama media

(*) Novedades en la instalación de teléfonos

Nivel Central disponibilidad de 3 teléfonos, a espera de asignación por demanda por parte de la entidad

4.3.2 Teléfono Gama Baja

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

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

Dirección territorial	Población y/o ciudad de ubicación	Cantidad teléfonos Gama Baja	Novedad
ANTIOQUIA	AMAGA	1	Cerrada se envió teléfono a Medellín
CASANARE	MONTERREY	1	Cerrada
CAUCA	BOLIVAR	1	Cerrada
CORDOBA	TIERRA ALTA	1	Cerrada
QUINDIO	QUIMBAYA	1	Cerrada
QUINDIO	CALARCA	1	Cerrada
SUCRE	MAJAGUAL	1	Cerrada
TOLIMA	CASA DE JUSTICIA (IBAGUÉ)	1	Cerrada
Total		**8(*)**	

Tabla 92 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 93 Consolidado de teléfonos gama baja

Adicionalmente el servicio de Telefonía IP incluye:

4.3.3 Troncales SIP

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

4.3.4 No Aplica

4.3.5 No Aplica

4.3.6 Módems 4G – Con plan de 50 Gbps

A continuación, se mencionan los equipos en operación en Nivel Central y DT para el servicio de MIFI y los equipos disponibles para asignación según novedades o solicitudes del ministerio.

Sede	Cantidad
Asignados Nivel Central y DT	25
Disponibles para asignación	5
Total	30

Tabla 94 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 noviembre de 2025, se presentaron las siguientes novedades sobre el servicio:

- Operatividad sobre la grabación de llamadas en la mesa de servicios.
- Configuración de permisos de llamadas a celular, larga distancia nacional, local a coordinadores e implementación de licenciamiento correspondiente al Addon Phone System a nivel nacional.
- Se tienen teléfonos hardphone disponibles para aprovisionamiento al usuario final a nivel nacional, se relacionan en este informe las cantidades disponibles según cada referencia.
- Se continúa el monitoreo sobre las troncales para las opciones 2 y 0 configuradas en el IVR para atención al ciudadano con el nuevo aliado BPM.
- Durante el mes en curso se realizó el proceso de configuración y aprovisionamiento de extensión y asignación de licencia de Teams Phone Standard en el tenant de Microsoft Teams para un usuario solicitado. Los cambios fueron aplicados exitosamente. Se adjuntaron manuales de soporte y configuración para referencia. Estado actual: Todos los usuarios se encuentran activos – casos RF-166285.

- Asignación de Licencias – Extensiones

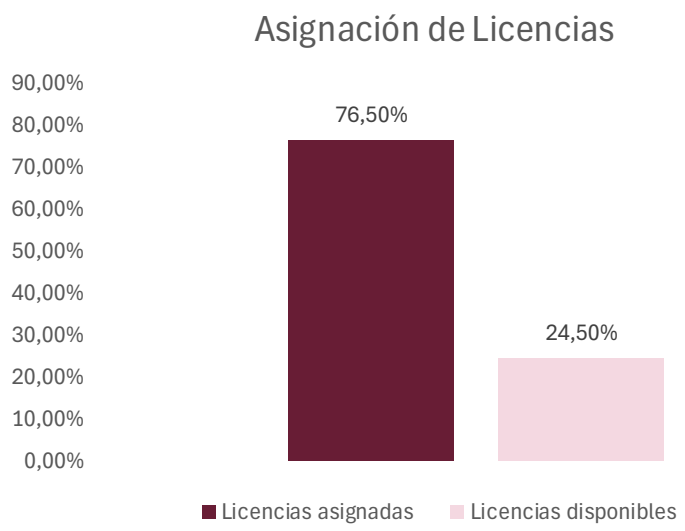


Ilustración 166 Asignación de licencias

Durante el mes en gestión, se han asignado un total de 465 extensiones a nivel nacional. Actualmente, permanecen disponibles 135 extensiones.

- Estadísticas de Tráfico

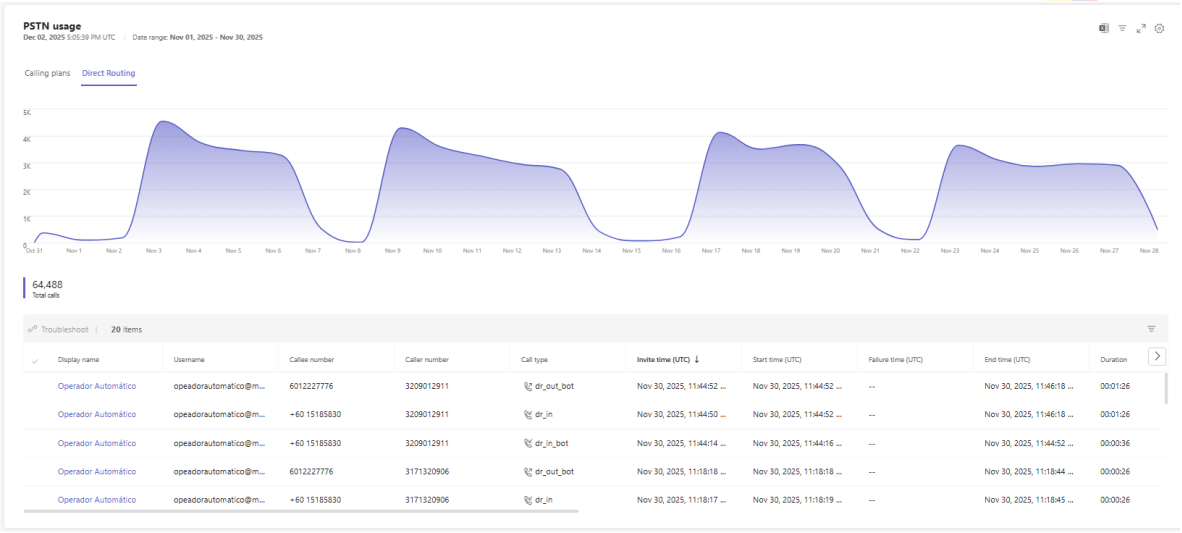


Ilustración 167 Comportamiento de tráfico

En la gráfica anterior se visualizan las tendencias de uso del servicio, en el periodo correspondiente al mes de noviembre de 2025, donde se atendieron un total de 64,448 llamadas.

Servicio	Minutos Disponibles	Minutos Utilizados
Locales	Ilimitados	632.14
Celular	1000	915.12
Nacional	Ilimitados	512.31
Internacional	700	4.41
Total		2063.98

Tabla 95 Minutos, consumos

- Consumo de llamadas LDN (Larga Distancia Nacional)

Con respecto a las llamadas realizadas a destinos larga distancia nacional en el mes de noviembre de 2025, se identifica que se realizaron llamadas con una duración total de 512.31 minutos.

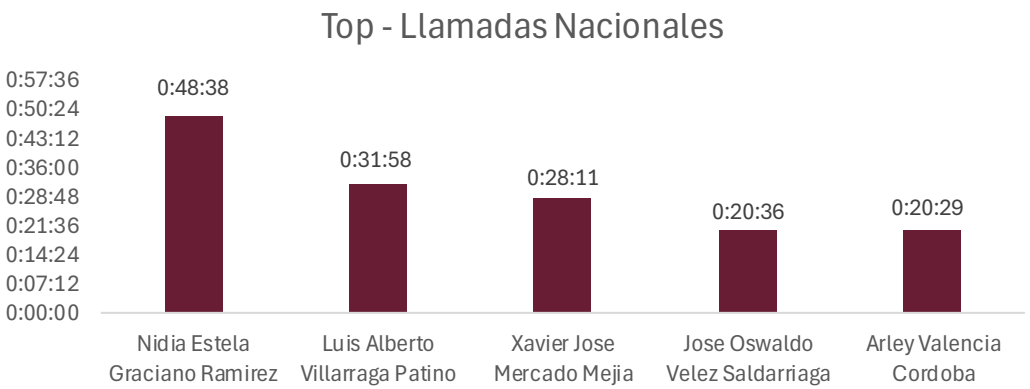


Ilustración 168 Top llamadas nacionales

N°	Usuario	Área	Tiempo llamadas
1	Nidia Estela Graciano Ramirez	Riesgos laborales Antioquia	0:48:38
2	Luis Alberto Villarraga Patino	Dirección de riesgos laborales Bogotá	0:31:58
3	Xavier Jose Mercado Mejia	Grupo De Atencion Al Ciudadano Y Tramites Antioquia	0:28:11
4	Jose Oswaldo Velez Saldarriaga	Grupo de Atencion Al Ciudadano Y Tramites Antioquia	0:20:36
5	Arley Valencia Cordoba	Oficina especial de uraba - Apartado	0:20:29

Tabla 96 Top 5 consumo de llamadas

- Consumo de llamadas LDI (Larga Distancia Internacional)

Con respecto a las llamadas internacionales en el mes de noviembre 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 169 llamada internacional de prueba

Como se puede observar en el grafico anterior, se evidencia que, en el mes de noviembre 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	0:04:41

Tabla 97 Top 5 llamadas LDI

- Consumo de llamadas destinos celulares

Con respecto a las llamadas realizadas a celular en el mes de noviembre de 2025, se identifica que se realizaron llamadas con una duración total de 915.12 minutos.

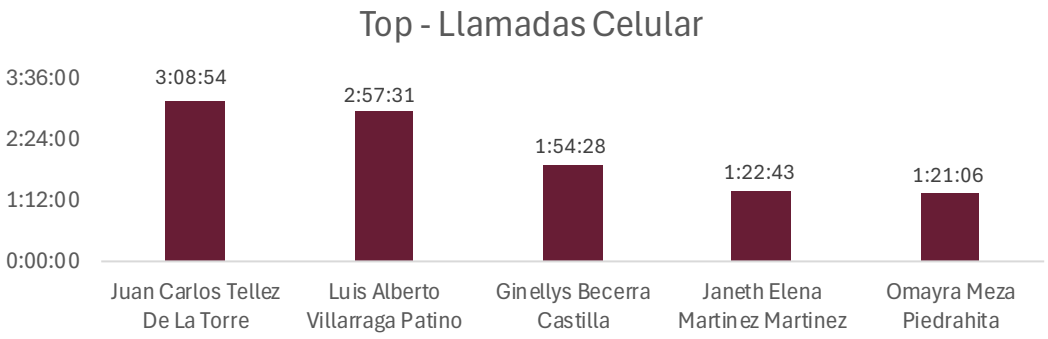


Ilustración 170 Top Celular

N°	Usuario	Área	Tiempo llamadas
1	Juan Carlos Tellez De La Torre	Grupo interno de trabajo para las victimas y equidad laboral - Bogotá	3:08:54
2	Luis Alberto Villarraga Patino	Dirección de riesgos laborales Bogotá	2:57:31
3	Ginellys Becerra Castilla	Comunicaciones GEEG Bogotá	1:54:28
4	Janeth Elena Martinez Martinez	Grupo Interno De Trabajo De Central De Cuentas - Bogotá	1:22:43
5	Omayra Meza Piedrahita	Oficina asesora jurídica Bogotá	1:21:06

Tabla 98 Top 5 llamadas Celular

- Consumo de llamadas locales

Con respecto a las llamadas realizadas a destinos locales en el mes de noviembre de 2025, se identifica que se realizaron llamadas con una duración total de 632.14 minutos.

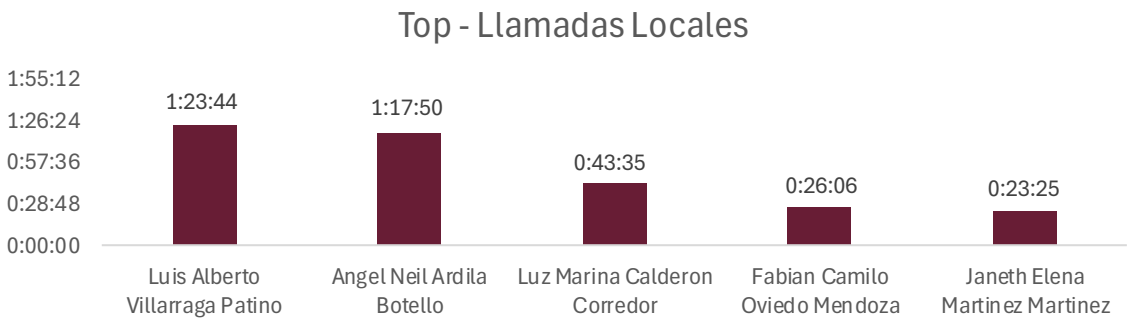


Ilustración 171 Top Local

N°	Usuario	Área	Tiempo llamadas
1	Luis Alberto Villarraga Patino	Dirección de riesgos laborales Bogotá	1:23:44
2	Angel Neil Ardila Botello	Grupo de Atención al ciudadano Bogotá	1:17:50
3	Luz Marina Calderon Corredor	Grupo interno de nómina e incapacidades Bogotá	0:43:35

4	Fabian Camilo Oviedo Mendoza	Oficina asesora jurídica Bogotá	0:26:06
5	Janeth Elena Martinez Martinez	Subdirección administrativa y financiera Bogotá	0:23:25

Tabla 99 Top 5 llamadas locales

- Capacitaciones y divulgaciones

En el mes de noviembre no se realizó proceso de capacitación y/o divulgaciones.

- Mejores Prácticas

Se adelantarán procesos de capacitación y divulgación sobre el uso de la nueva herramienta de telefonía. Paralelamente, avanza la liberación de licencias a nivel nacional 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 172 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

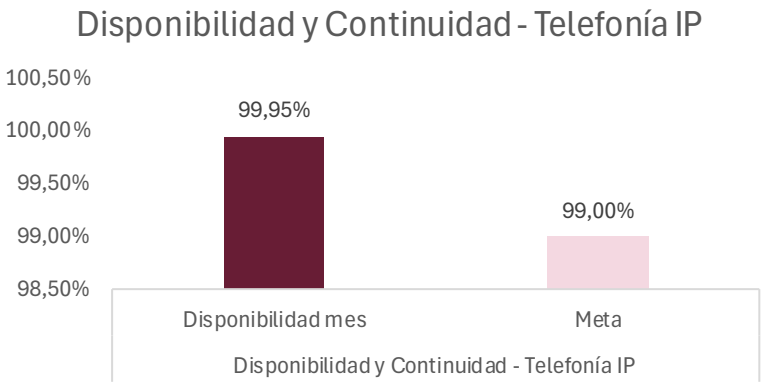


Ilustración 173 Disponibilidad y Continuidad TOIP

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

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

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

Tabla 100 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 101 Inventario de UPS – 10kVA

4.4.2 UPS 15 kVA

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

Ruta Repositorio MinTrabajo: 3. INFORME UT GESTION TIC 2023 - ENTREGA LINEA DE SERVICIO EER UPS.pdf

4.4.3 UPS 20 kVA

SEDE	POBLACIÓN Y/O CIUDAD	UBICACIÓN EN LA SEDE	MARCA	REFERENCIA UPS	NUMERO DE SERIE UPS
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 23	ABLEREX	KRONOS UL20D	TD8004CC80020

SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 22	ABLEREX	KRONOS UL20D	TD2110B2M0006
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 21	ABLEREX	KRONOS UL20D	TD8004CC80001
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 20	ABLEREX	KRONOS UL20D	TD8004CC80025
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 19	ABLEREX	KRONOS UL20D	TD8004CC80023
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 18	ABLEREX	KRONOS UL20D	TD8004CC80012
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 17	ABLEREX	KRONOS UL20D	TD2110B2M0004
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 10	ABLEREX	KRONOS UL20D	TD9121BAS0008
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 9	ABLEREX	KRONOS UL20D	TD8004CC80015
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 8	ABLEREX	KRONOS UL20D	TD8004CC80003
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 5	ABLEREX	KRONOS UL20D	TD8004CC80002
TERRITORIAL SANTANDER	BUCARAMANGA	Cuarto técnico piso 2	ABLEREX	KRONOS-UL20D	TD8004CC80018
TERRITORIAL ANTIOQUIA	MEDELLÍN	cuarto técnico primer piso	ABLEREX	KRONOS-UL20D	TD4007C740004
OE BARRANCABERMEJA	BARRANCABERMEJA	Cuarto técnico primer piso	ABLEREX	KRONOS-UL20D	TD8004CC80004

Tabla 102 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.

No se tienen novedades durante el período del informe con respecto al escalamiento que se realizó en febrero 2025, referente a la novedad con la UPS en la territorial de Santander (Bucaramanga) propiedad de la UT, ya que se encontró que hay picos de voltaje de entrada con valores de 135V, se requiere hacer validación con la empresa proveedora de energía ya que de lo contrario sería necesario adquirir un regulador de voltaje para corregir las alertas que está presentando la UPS.

No se tienen novedades durante el período del informe con respecto al escalamiento de la UPS de la OE Apartadó (propiedad del ministerio), ya que el personal de soporte en sitio reitera que se vienen presentando eventos sobre el equipo, el apoyo que brinda actualmente nuestro técnico es generar el reinicio correspondiente, pero en ocasiones algunos usuarios de la sede no comprenden que se encuentra fuera de nuestro alcance su reparación y atención. A espera de recibir 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.

- **Mantenimiento Preventivo de UPS**

Se coordina lo correspondiente para dar inicio en noviembre 2025 al mantenimiento preventivo de las UPS en Nivel Central, se gestionan recursos y personal para atención el 01 de noviembre 2025. Llega personal de la UT a la sede pero no se encuentra el personal por parte del ministerio para acompañamiento, ni se cuenta con ticket habilitado para ASD para la apertura de los centros de cableado. Se confirma visita fallida.

El 8/11/2025 se coordina nuevamente el inicio de la actividad, se realiza mantenimiento de las UPS en Nivel Central de los pisos 20, 21, 22, 23, 24 entre las 7:00am y las 5:30pm.

El 26 y 27 de noviembre a partir de las 6:00pm se continúan las actividades y se logra atender las UPS de los pisos 3, 5, 8, 9, 10, 17, 18, 19, 25.

Se están consolidando las actas de atención en el repositorio dado por la entidad para el contrato.

Ruta Repositorio MinTrabajo: Mantenimientos_Preventivos_2025

- 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 103 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 104 Inventario de impresoras para el servicio

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

- Para el mes de noviembre, el responsable del servicio gestionó un total de 684 solicitudes escaladas a través de Aranda. Al corte del mes, 671 casos quedaron en estado Cerrado/Solucionado, 13 en estado Suspendido (los casos suspendidos se deben a cambio de toners 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 67% 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 realizó la asignación de cuotas de clics de impresión de usuarios finales bajo el caso Aranda RF-161791; allí se relaciona el listado total de usuarios con el aprovisionamiento.
- Se llevó a cabo la actualización de la interfaz de usuario en las impresoras Ricoh IM430F de las Direcciones Territoriales e Inspecciones a nivel nacional completando un total de 149 impresoras actualizadas, esta actividad continúa en curso para el siguiente período.
- Adicionalmente, se realizó la actualización del controlador de impresión en todos los equipos, migrando de la versión 4.38 a 4.43, con el fin de mitigar vulnerabilidades, mejorar la estabilidad y optimizar la configuración de impresión en los equipos de los funcionarios.
- El 7/11/2025 bajo RFC de emergencia se gestiona el aumento de performance del servidor mintrabimp (impresión), ya que se requería una ampliación de vCPU y memora RAM para mejorar el procesamiento.
- Mantenimientos Preventivos: Se inicia la atención de mantenimientos preventivos de las impresoras Ricoh a nivel nacional. A corte del período se han atendido 16 sedes de territorio, actividad se continuará en el siguiente periodo.
- El 14/11/2025 se realiza la delegación por parte del administrador del servicio de impresión al personal de MDS la actividad de asignación por demanda de cuotas de impresión, se incluyeron las siguientes actividades:
  - Acceso controlado al PaperCut
  - Generación de manual con el paso a paso de la actividad.
  - Habilitación de permiso de acceso para los usuarios del personal de MDS
  - Sesión de transferencia de conocimiento, entrega de manual y confirmación de accesos al portal

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

Nombre de la impresora	Ubicación	Nombre de Usuario	Nombre Completo	Blanco y negro
ricohpiso19a	Bogotá Sede Central	pnustes	Patricia Celestial Nustes Barrera	4.855
ricoh-bmanga-ofc305	Bucaramanga	lberbeo	Laura Daniela Berbeo Ardila	2.776
ricohpiso5a	Bogotá Sede Central	cjunco	Carlos Julio Junco Arenas	2.458
ricoh-bmanga-ofc305	Bucaramanga	ybeltran	Yerson Daniel Beltran Martinez	2.324
ricoh-cali-piso4	Cali	gparra	Gabriel Parra Trujillo	2.298
ricoh-ibague-radicacion	Ibagué	mnavarrog	Maria Alejandra Navarro Garcia	1.962
ricohpiso23b	Bogotá Sede Central	ldleal	Luz Dary Leal Cotamo	1.866
ricoh-cali-piso2-atc	Cali	llondono	Leydy Johanna Londono Ramos	1.769
ricoh-cali-piso2-atc	Cali	mquinonesp	Mildreth Quinonez Peinado	1.745
ricoh-apartado-piso2-c	Apartado	tllanes	Tatiana Llanes Ibarguen	1.705

Tabla 105 Consumo de impresiones por usuario - Impresoras B/N

Clisc por Usuarios.xlsx

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

Nombre de la impresora	Ubicación	Blanco y negro
ricoh-bmanga-ofc305	Bucaramanga	16337
ricohpiso5a	Bogotá Sede Central	13147
ricohpiso23b	Bogotá Sede Central	11620
ricohpiso19a	Bogotá Sede Central	11449
ricoh-cali-piso4	Cali	11313
ricoh-cali-piso3	Cali	9516
ricohpiso12a	Bogotá Sede Central	8866
ricohcl32-rcc	Bogotá Calle 32	8842
ricoh-cali-piso2-atc	Cali	8744
ricohpiso9a	Bogotá Sede Central	8159

Tabla 106Top 10 de impresoras con mayor uso

Impresoras con mayor uso.xlsx

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

Nombre de la impresora	Ubicación	Nombre de Usuario	Nombre Completo	Color
ricohpiso25c	Bogotá Sede Central	mserrano	Malliber Serrano Nieto	1152
ricohpiso25c	Bogotá Sede Central	bhernandez	Bibiana Hernandez Hernandez	303
ricohpiso25c	Bogotá Sede Central	ymedinag	Yeisson Medina Gonzalez	208

Tabla 107 Top usuarios impresión a color



Impresora 25C.xlsx

En la siguiente tabla se muestra el Top de oficinas con mayor volumen de impresión:

Oficina	Color	Blanco y negro	Doble Cara	Páginas simples	Total, Páginas	Trabajos realizados	Promedio de Páginas por trabajo
Nivel Central	1670	128839	93112	37397	130509	36631	3582,6
D.T. Valle del Cauca	0	42157	30422	11735	42157	12372	431,6
D.T. Santander	0	28544	20056	8488	28544	8813	365,6
D.T. Antioquia	0	23579	16610	6969	23579	7728	357,7
D.T. Tolima	0	15427	10664	4763	15427	4199	217
D.T. Bogotá	0	13439	8546	4893	13439	4583	239,2
D.T. Norte de Santander	0	12342	8008	4334	12342	4284	287
D.T. Cundinamarca	0	11031	6334	4697	11031	3355	189,5
D.T. Córdoba	0	10029	6076	3953	10029	3287	186,3
D.T. Atlántico	0	9273	5706	3567	9273	3112	281,6

Tabla 108 Top oficinas



Oficinas Impresión.xlsx

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

Impresora	Ubicación	Copias
ricoh-medellin-piso1	Medellín	58568
RICOHCALLE32-GAU-B	Bogotá cll32	56041
RICOHCALLE32-RCC	Bogotá cll32	46894
ricohpiso5b	Bogotá sede central	42400
ricoh-bmanga-ofc205	Bucaramanga	33021
ricoh-cali-piso4	Cali	32217
RICOHCALLE32-GAU-A	Bogotá cll32	25519
RICOH-BMANGA-OFC305	Bucaramanga	24848
ricoh-monteria-piso2	montería	22199
ricohpiso9a	Bogotá sede central	21487

Tabla 109 Top 10 impresoras más usadas del servicio de fotocopiado

Copias impresora.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
gparra	Gabriel Parra Trujillo	ADJUST	2303	10
keguis	Karen Alejandra Eguis Cifuentes	ADJUST	1200	8
dmontenegro	Diana Maria Montenegro Baltazar	ADJUST	1494	7
jadiaz	Javier Diaz Marroquin	ADJUST	1498	7
mmorenoma	Maria Camila Moreno Mayuza	ADJUST	1396	6
ybeltran	Yerson Daniel Beltran Martinez	ADJUST	2434	6
ymedina	Yanneth Medina Lopez	ADJUST	1318	6
esantana	Edgar Manuel Santana Castro	ADJUST	1317	5
evaron	Elvy Yadira Varon Reyes	ADJUST	1981	5
jmejiab	Jacqueline Mejia Botello	ADJUST	1353	5

Tabla 110 Ampliación de cuota de impresión

Asignación de saldo.xlsx

- Despacho de papel, tóner y unidades a nivel nacional

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

	sep-25		oct-25		nov-25	
	Resmas Carta	Resmas Oficio	Resmas Carta	Resmas Oficio	Resmas Carta	Resmas Oficio
Total, Resmas	454	74	441	220	432	255
Total, Cajas por Tamaño	45,4	7,4	44,1	22	43,2	25,5
Total, Cajas Enviadas	**52,8**		**66,1**		**68,7**	

Tabla 111 Despacho de papel a sedes del Ministerio del Trabajo

Durante el período, se despacharon a sedes del ministerio un total de 22 toners para impresora B/N IM430F, 2 unidades de imagen y 4 unidades fusoras.

4.6.1 No aplica

4.6.2 Multifuncional B/N rango medio – Cargo fijo mensual

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

Tabla 112 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 113 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 noviembre de 2025:

MES	DETALLE	CANTIDAD
Noviembre	Multifuncional blanco y negro rango medio - Clic de impresión tóner y papel carta	**502.396**
	TOTAL	**502.396**

Tabla 114 Clics de impresión de noviembre 2025 – Multifuncional B/N

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

Mes 2025	Septiembre	Octubre	Noviembre
Cantidad de clics consumidos	571.449	553.658	502.396

Tabla 115 Tendencia de consumo de clics B/N

El consumo mensual establecido para el servicio es de **450.000** clics de impresión en B/N a nivel nacional; para el período del informe se presentó un consumo de **438.317** clics de impresión (esto incluye **4.526** de la impresora de contratos piso 8) y **64.079** de fotocopias para un total de **502.396** para este servicio, superando el estimado del mes por **52.396.**

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 noviembre de 2025:

MES	DETALLE	CANTIDAD
Noviembre	Impresora color rango medio - Cargo fijo mensual - Clic de impresión tóner y papel carta	1.677

TOTAL	1.677

Tabla 116 Clics de Impresión de noviembre 2025 – Impresora Color

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

Mes 2025	Septiembre	Octubre	Noviembre
Cantidad de clics consumidos	2.297	1.602	1.677

Tabla 117 Tendencia de consumo de clics color

El consumo mensual establecido para el servicio por la entidad es de **1.500** clics de impresión en color para el único equipo de este tipo ubicado en Nivel Central; para el período del informe se presentó un consumo de **1.677** clics para este servicio, superando el estimado del mes por **177**.

- 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 118 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 noviembre 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.

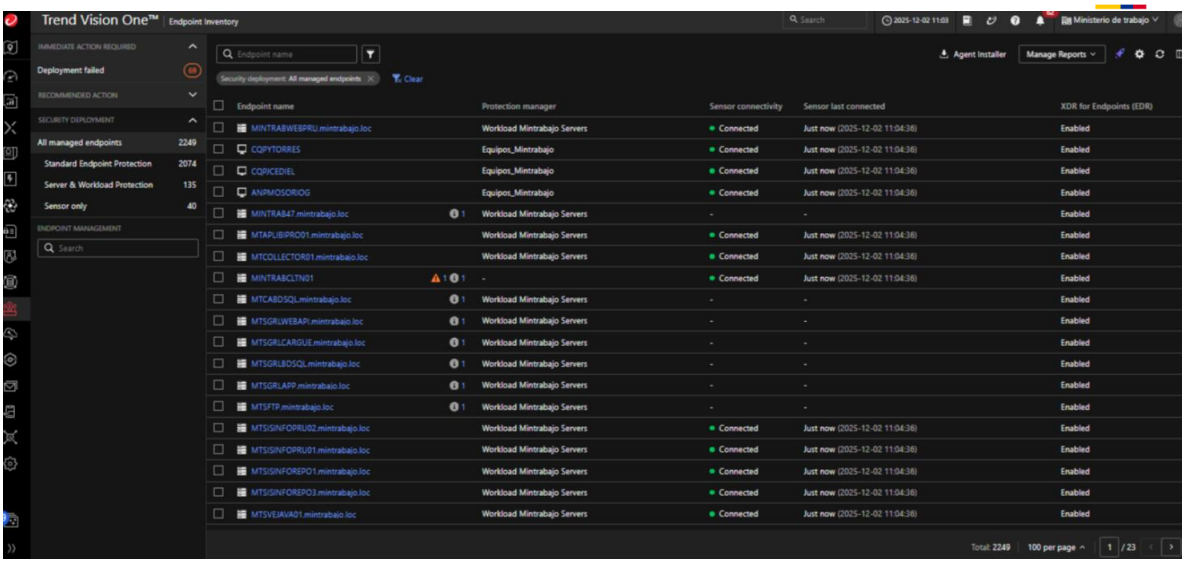


Ilustración 174 Equipos consola antivirus

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 (2074) de Mintrabajo, se cuenta con 2255 licencias, se tienen disponibles 88.

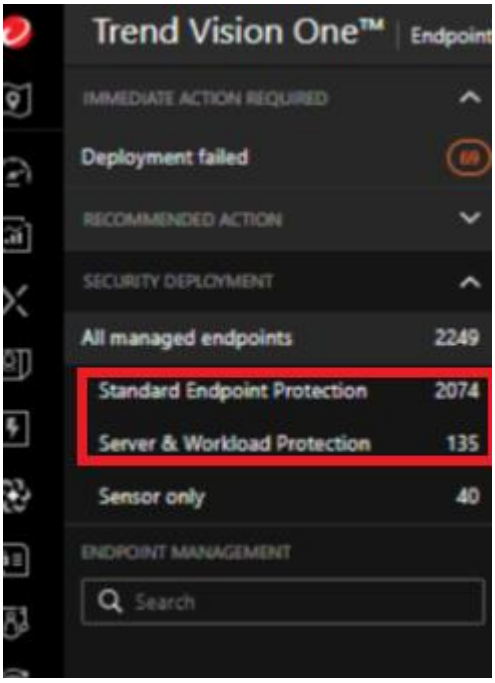


Ilustración 175 Gestión consola antivirus – equipos usuario final

4.7.3 Top 10 Virus Detectados

Durante el mes analizado, los eventos detectados por la plataforma TrendMicro se detectaron un total de 4859 eventos, lo que permite evaluar el grado de riesgo asociado a cada actividad observada en los Endpoint, estos fueron controlados por la herramienta haciendo con algunos de ellos el bloqueo, de otros la eliminación, y también enviando a cuarentena:

Análisis de los Datos:

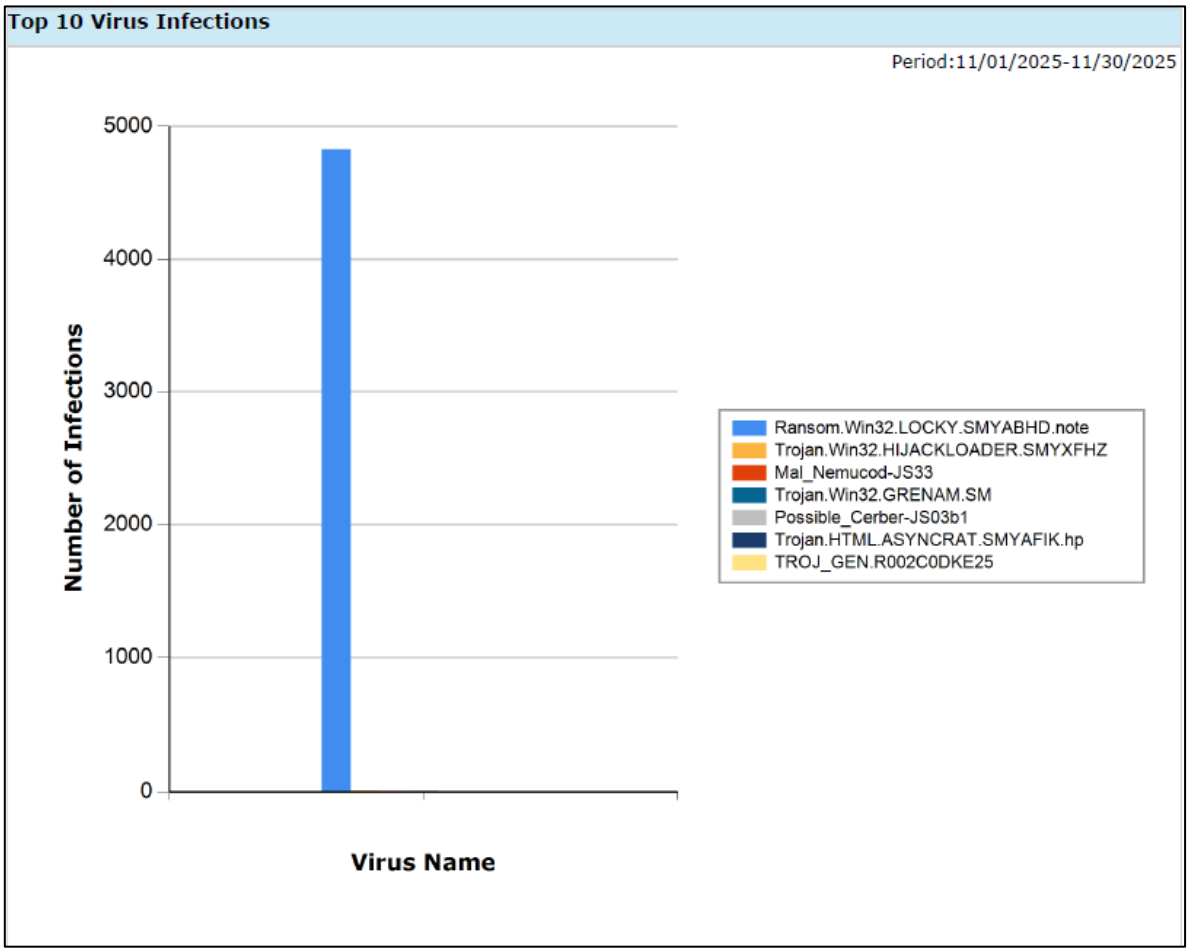


Ilustración 176 Top 10 virus detectado

Top 10 Virus Infections		
Virus Name	# of Infections	Detected By
Ransom.Win32.LOCKY.SMYABHD.note	4,827	Desktop (4,827)
Trojan.Win32.HIJACKLOADER.SMYXFHZ	10	Desktop (10)
Mal_Nemucod-JS33	8	Desktop (8)
Trojan.Win32.GRENAM.SM	7	Desktop (7)
Possible_Cerber-JS03b1	3	Desktop (3)
Trojan.HTML.ASYNCRAT.SMYAFIK.hp	3	Desktop (3)
TROJ_GEN.R002C0DKE25	1	Desktop (1)

Tabla 119 Descripción de virus

- Ransom.Win32.LOCKY.SMYABHD.note es un tipo de malware que cifra los archivos de la víctima y pide un rescate (ransom) para devolver el acceso, también indica el sistema operativo en que puede ejecutarse 32 o 64 bits. Estas 4860 detecciones fueron encontradas el 05 de noviembre en el host BODYQUINTERO, razón por la cual ese mismo día el host fue aislado y se solicitó su correspondiente validación con mesa de servicio.

- Trojan.Win32.HIJACKLOADER.SMYXF: Es un troyano diseñado para cargar y ejecutar otros tipos de malware en el equipo comprometido, permitiendo que atacantes instalen herramientas adicionales como stealers, ransomware o backdoors. Indica compatibilidad con sistemas Windows de 32 y 64 bits. Estas detecciones fueron registradas en los siguientes equipos:
  - BODGSANDOVAL
  - GUDACAICEDO
  - BODFROJASC
  - BOPJRUIZQ
  - BODNLEIVA

  La consola de trendmicro tomo acciones sobre los equipos y los archivos asociados fueron limpiados.

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

- Trojan.Win32.GRENAM.SM: Es un troyano que modifica o reemplaza archivos legítimos del sistema para evadir la detección y garantizar persistencia en Windows. Puede abrir puertas traseras, permitir control remoto o descargar más malware. Esta detección genera riesgo de manipulación no autorizada del sistema, la herramienta tomo acciones y limpio los archivos implicados.

- Possible_Cerber-JS03b1: Hace referencia a una posible variante del ransomware Cerber distribuida a través de archivos JavaScript. Este tipo de amenaza suele iniciar la cadena de infección descargando el payload principal encargado del cifrado. Aunque se clasifica como “possible”, la detección requiere atención inmediata, ya que este ransomware es conocido por cifrar documentos y exigir pago en criptomonedas. El host afectado fue revisado para descartar actividad adicional, sin embargo, la herramienta tomo acciones eliminando los archivos asociados a la amenaza

- Trojan.HTML.ASYNCRAT.SMYAFIK.hp: Se trata de un archivo HTML malicioso asociado al RAT AsyncRAT, una herramienta de acceso remoto usada por atacantes para tomar control del equipo, robar información, registrar teclas y descargar más componentes dañinos. Esta variante está diseñada para ejecutarse a través de contenido web. Por la naturaleza de la amenaza, se procedió con la verificación del host, la herramienta tomo acciones eliminando los archivos asociados a este tipo de amenaza

- TROJ_GEN.R002C0DKE25: Es una detección genérica de troyano que indica que el archivo presenta comportamientos o patrones característicos de malware, aunque no pertenezca a una familia específica. Este tipo de alertas se genera cuando el motor identifica código sospechoso con potencial de causar daño, ejecutar acciones no autorizadas o comprometer el sistema. la herramienta tomo acciones limpiando los archivos asociados a este tipo de amenaza

TOP 5 EQUIPOS

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

Product Entity/Endpoint	Cantidad	Virus/Malware
BODYQUINTERO	4860	Ransom.Win32.LOCKY.SMYABHD.note
BOPDZARATE	5	Trojan.HTML.ASYNCRAT.SMYAFIK.hp
HUDIRAMIREZF	4	Trojan.HTML.ASYNCRAT.SMYAFIK.hp
HUPGGARCIAO	4	Backdoor.Win64.REMCOS.YXFIJZ
BOPLRIVEROSM	3	TSPY.Win32.TRX.XXPE50F13031

Tabla 120 *Top 5 Equipos*

BODYQUINTERO

Las 4860 detecciones en el equipo se deben por Ransom.Win32.LOCKY.SMYABHD.note es un tipo de malware que cifra los archivos de la víctima y pide un rescate (ransom) para devolver el acceso, también indica el sistema operativo en que puede ejecutarse 32 o 64 bits. Estas 4860 detecciones fueron encontradas el día 21 de octubre en el host

BODYQUINTERO y son escaladas bajo el RF-159034, razón por la cual ese mismo día el host fue aislado y se solicitó su correspondiente validación con mesa de servicio.

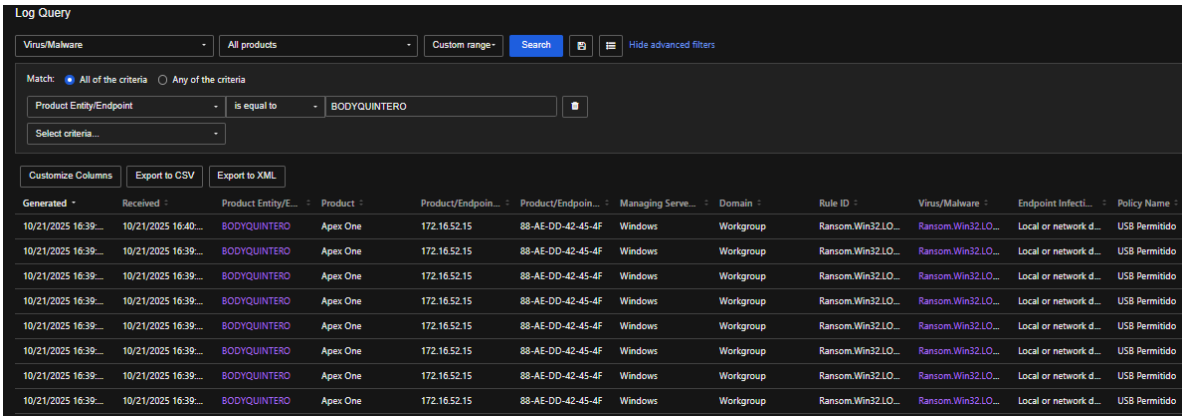


Ilustración 177 HUPGGARCIAO

BOPDZARATE

Las 5 detecciones 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

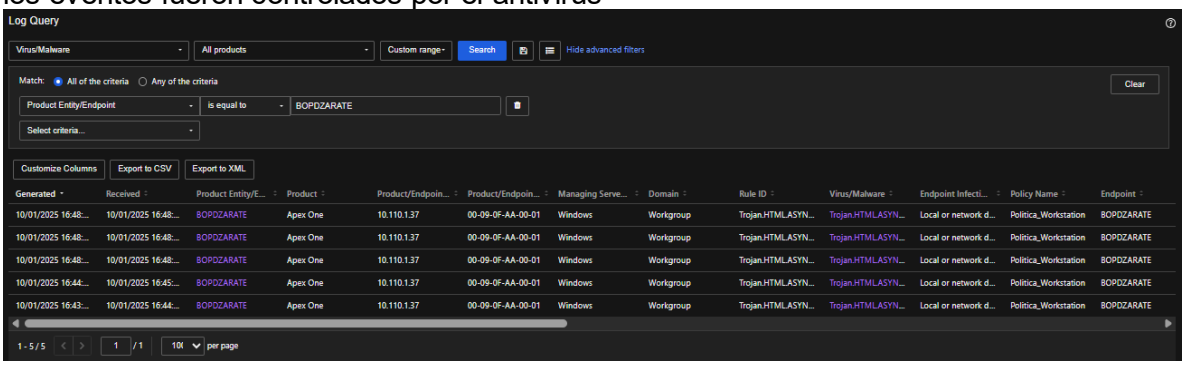
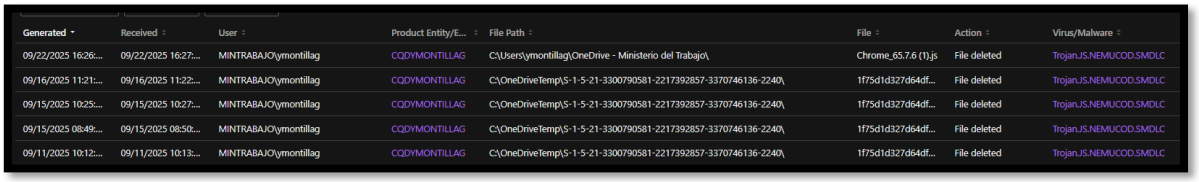


Ilustración 178 BOPDZARATE

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 *179 CQDYMONTILLAG*

HUDIRAMIREZF

Las 4 detecciones en el equipo se deben 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

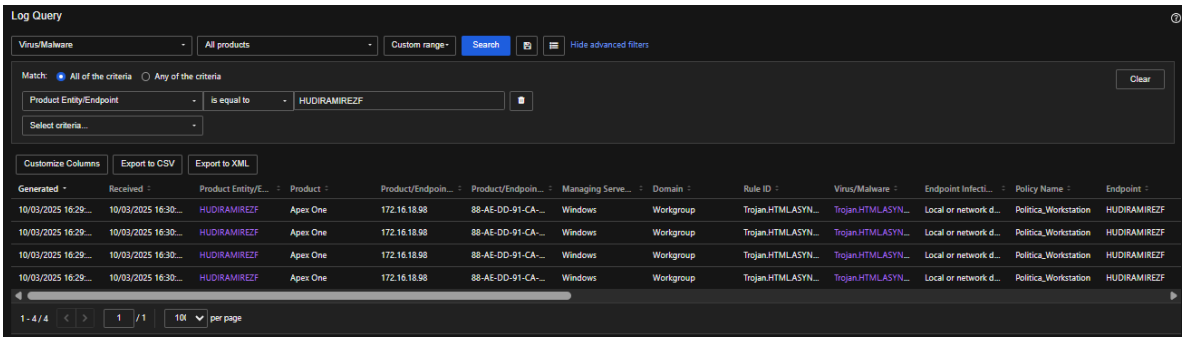


Ilustración 180 BOPLSALAMANCAP

HUPGGARCIAO

La detección en el equipo se debe por Backdoor.Win64.REMCOS.YXFIJZ Esta detección corresponde a 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. También presenta 1 detección por TROJ_GEN.R002C0DIU25 este indica la presencia de un troyano genérico. En este caso, “TROJ” significa que se trata de un troyano, un tipo de

malware diseñado para realizar acciones maliciosas sin el consentimiento del usuario; “GEN” señala que es una detección genérica.

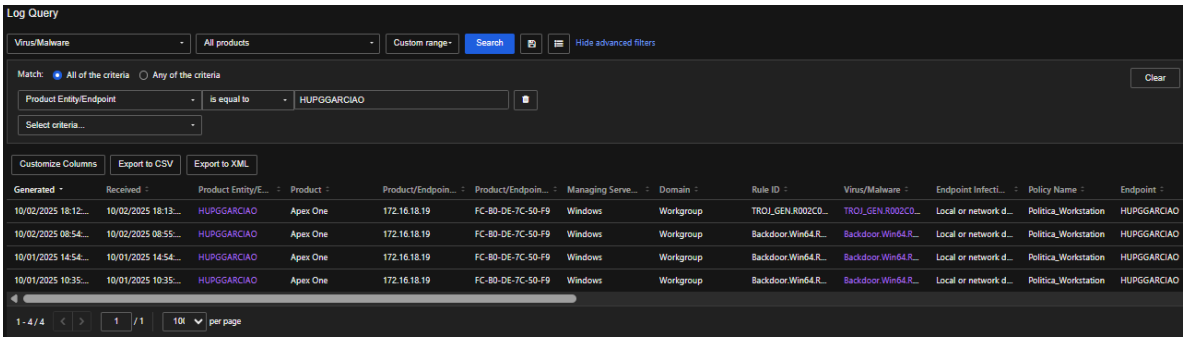


Ilustración 181 CNDDQUEVEDO

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.

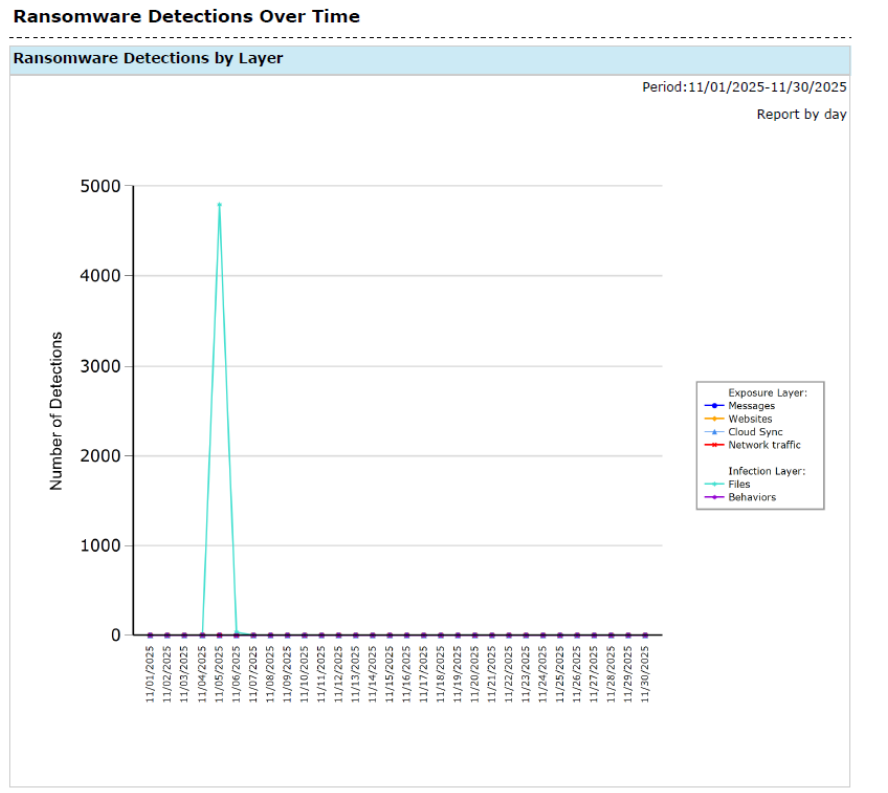


Ilustración 182 Eventos Ransomware

En el mes de noviembre 2025, se presentaron eventos 4827 eventos escalados por detección de malware Ransomware, estas detenciones se realizaron en el host

BODYQUINTERO el día 5 de noviembre, el equipo es aislado por parte del equipo AV y finalmente verificado por soporte en sitio, quien eliminan archivos potencialmente maliciosos, temporales y demás el evento finaliza con el RF- 166898..

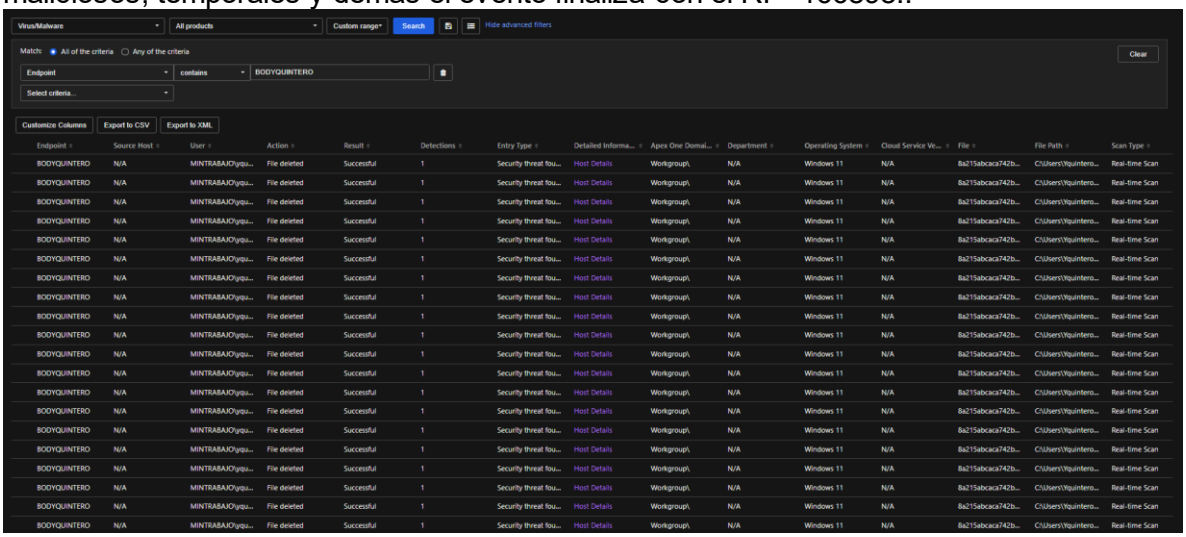


Ilustración 183 captura eventos ransonware

4.7.4 Servicio de Vulnerabilidades

A continuación, se muestra un resumen de los resultados, actividades y procesos relacionados al servicio de gestión de vulnerabilidades, que han sido llevadas a cabo durante el mes de noviembre 2025 sobre la infraestructura tecnológica registrada del Ministerio de Trabajo, con el objetivo de identificar los hallazgos a nivel de vulnerabilidades que pueden alterar el nivel de exposición cibernética del negocio.

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

Se informó al Ministerio de trabajo y equipo infraestructura que se procede con la primera fase de la **Prueba de Vulnerabilidades** del **segundo semestre 2025** para el proyecto Ministerio del Trabajo, de acuerdo con el cronograma de ejecución propuesto.

Plan de acción y remediación de vulnerabilidades
Priorización: Priorizar las vulnerabilidades críticas y de alta severidad para su remediación inmediata. Automatización: Considerar el uso de herramientas de gestión de parches automatizadas para agilizar el proceso en cual se está implementado un WSUS.
Validación: Realizar pruebas exhaustivas antes de implementar parches en entornos de producción.

4.7.4.1 Inventario y licenciamiento

El inventario de activos registrado en la herramienta Tenable Nessus Professional se basa en la 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 301 activos de TI.

En noviembre se alcanzó un registro de 301 activos de TI (98 %) de la línea base documentada en la herramienta.

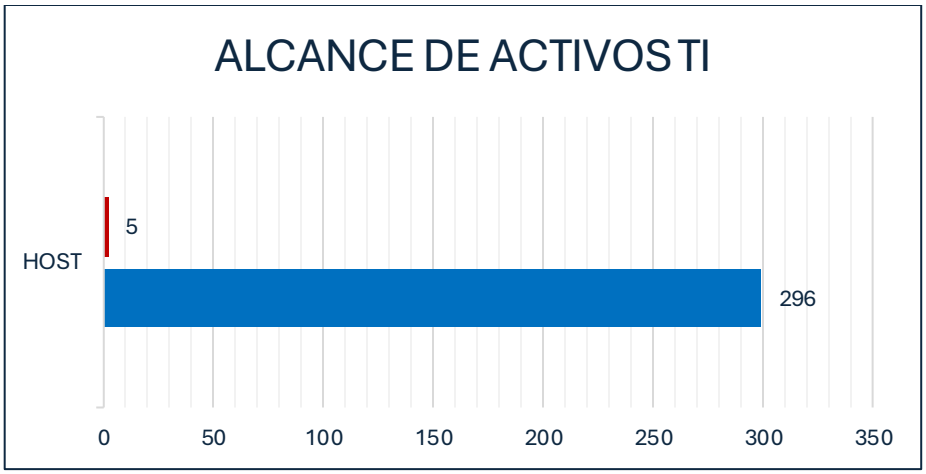


Ilustración 184 *Gestión consola Nessus*

4.7.4.2 Escaneos programados

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

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

Name	Scan Type	Schedule	Last Scanned
2025 SEMANAL II - WINDOWS DESKTOP	Vulnerability	Weekly on Sat at 12:30 AM	November 29 at 12:31 ...
2025 SEMANAL II - NETWORKING	Vulnerability	Weekly on Sat at 8:00 PM	November 29 at 8:31 PM
2025 SEMANAL II - FORTISIEM	Vulnerability	Weekly on Sat at 9:00 PM	November 29 at 9:38 PM
2025 SEMANAL II - VMWARE	Vulnerability	Weekly on Sat at 10:00 PM	November 29 at 10:10 ...
2025 SEMANAL II - LINUX	Vulnerability	Weekly on Sat at 11:00 PM	November 29 at 11:42 ...
2025 SEMANAL II - NO AUTH	Vulnerability	Weekly on Sun at 3:30 AM	November 30 at 3:40 AM
2025 SEMANAL II - WINDOWS SERVER	Vulnerability	Weekly on Sun at 9:00 PM	November 30 at 11:35 ...

Ilustración 185 *Escaneos programados*

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

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

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

4.7.4.3 TOP 10 – Vulnerabilidades más explotables

Al cierre de noviembre del 2025, el activo TI con la mayor cantidad de vulnerabilidades identificadas corresponde al host (172.20.22.42), con un total de 99 hallazgos, corresponde a un servidor Rocky Linux release 8.10 (Green Obsidian) y la mayoría de las vulnerabilidades están asociadas a actualizaciones de seguridad para la librería OpenSSL..

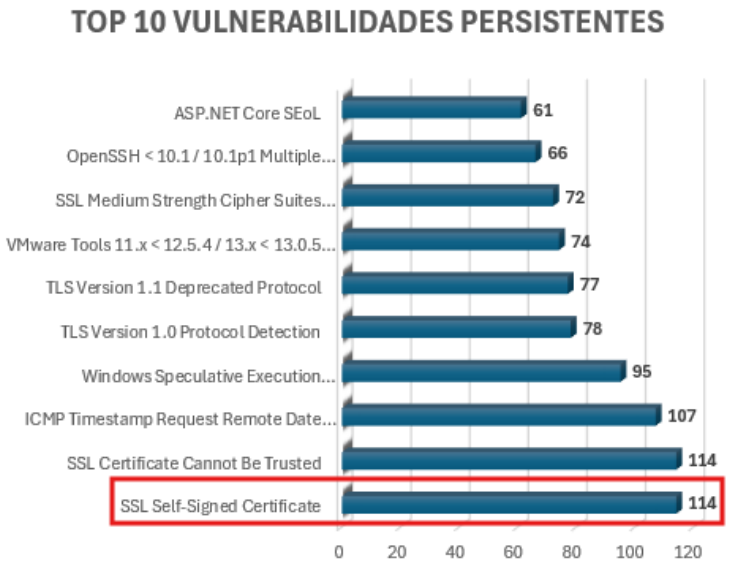


Ilustración 186 TOP 10 - Activos más explotables

Al cierre de noviembre del 2025, la vulnerabilidad identificada con la mayor cantidad de persistencias corresponde a (SSL Self-Signed Certificate), con un total de 114 hallazgos, esta vulnerabilidad puede ser un falso positivo debido a que aparece cuando se identifica un servicio que está utilizando un certificado auto firmado, es decir, que no fue emitido por certificadoras públicas, por lo que generalmente se acepta el riesgo de esta debido a que los certificados auto firmados son muy usados en servicios internos con el fin de ahorrar costes..

4.7.4.4 Estrategia de remediación y/o mitigación

La estrategia de remediación de vulnerabilidades implementada en MINTRABAJO consiste en priorizar las vulnerabilidades según la criticidad; y definir fechas contempladas para cerrarlas. Por lo que las fechas corresponden a:

- Vulnerabilidades Criticas: sobre estas vulnerabilidades se enfocará la mayoría de los esfuerzos para una rápida mitigación.
- Vulnerabilidades Altas – Se trabajarán en conjunto con la vulnerabilidad críticas, pero estas tendrán una menor criticidad en la mitigación.
- Vulnerabilidades Medias y bajas – Estas vulnerabilidades se trabajar a un periodo más amplio debido a que no tienen un impacto critico o alto en la operación.

Para cumplir con la estrategia de remediación, se programan sesiones semanales con el equipo resolutor (Windows, Linux y Oracle) con el objetivo de validar los avances en la remediación. Sin embargo, dado que estas fechas son planificadas, es posible que algunas vulnerabilidades se extiendan más allá de lo previsto. En estos casos, se documentarán las vulnerabilidades extendidas junto con una justificación detallada del retraso.

4.7.4.5 Resumen de mitigación efectuada

A continuación, se contrasta un resumen de las actividades relacionas con la gestión de vulnerabilidades correspondientes al Snapshot del semestre 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 noviembre del 2025, se remediaron un total de 591 vulnerabilidades, de las cuales, 167 fueron de severidad crítica, 151 de severidad alta, 186 de severidad media y 87 de severidad baja. Por otro lado, con relación a indicadores semestrales, se gestionaron un total de 1.722 vulnerabilidades TI, de las cuales, 402 fueron de severidad crítica, 290 de severidad alta, 631 de severidad media y 399 de severidad baja.

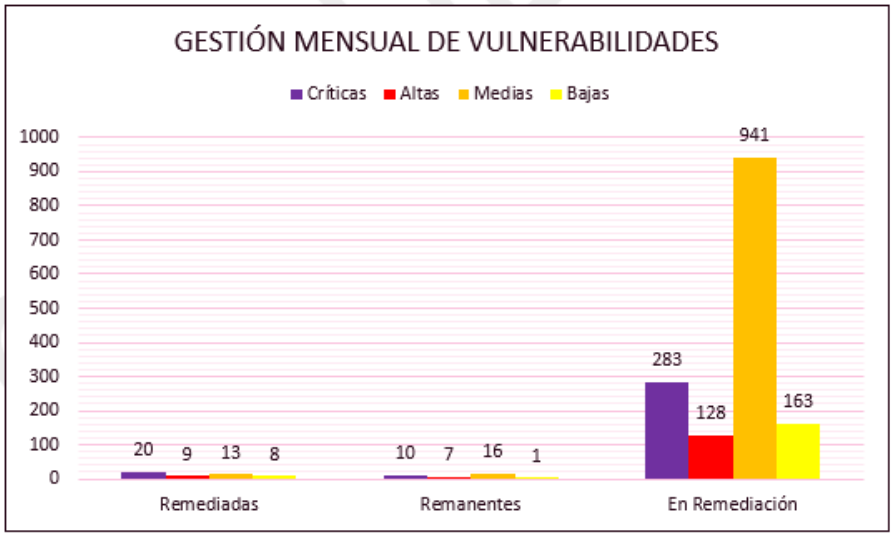
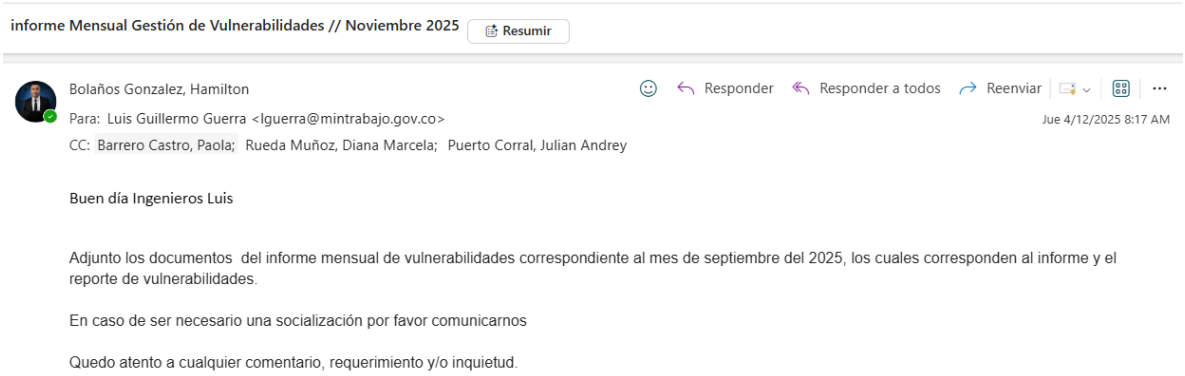


Ilustración 187 Vulnerabilidades gestionadas vs en remediación

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

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


informe Mensual Gestión de Vulnerabilidades // Noviembre 2025 Resumir

Bolaños Gonzalez, Hamilton Responder Responder a todos Reenviar

Para: Luis Guillermo Guerra <lguerra@mintrabajo.gov.co> Jue 4/12/2025 8:17 AM

CC: Barrero Castro, Paola; Rueda Muñoz, Diana Marcela; Puerto Corral, Julian Andrey

Buen día Ingenieros Luis

Adjunto los documentos del informe mensual de vulnerabilidades correspondiente al mes de septiembre del 2025, los cuales corresponden al informe y el reporte de vulnerabilidades.

En caso de ser necesario una socialización por favor comunicarnos

Quedo atento a cualquier comentario, requerimiento y/o inquietud.

Ilustración 188 captura envío de correo gestión de vulnerabilidades

4.7.4.6 Prueba de Vulnerabilidades Semestre II 2025
Se notifica que se procede con la primera fase de la Prueba de Vulnerabilidades del segundo semestre 2025 para el proyecto Ministerio del Trabajo, de acuerdo con el cronograma de ejecución propuesto.

FASE	RIESGO	RESPONSABLE	PROGRESO	INICIO MM-DD-YYYY	DÍAS
Levantamiento de información requerida	Riesgo medio	Daniel Castillo	0%	10/27/2025	5
Planeación de la prueba	Riesgo medio	Daniel Castillo	0%	11/03/2025	5
Ejecución y diagnóstico	Riesgo alto	Daniel Castillo	0%	11/10/2025	5
Documentación de hallazgos	Riesgo medio	Daniel Castillo	0%	11/17/2025	10
Presentación de los resultados	Riesgo bajo	Daniel Castillo	0%	12/01/2025	5

Ilustración 189 Cronograma Ethical Hacking

Esta primera fase corresponde a la definición del alcance de la actividad, es decir, la actualización de la línea base de activos registrados en la herramienta del Nessus Professional.

- Medición de ANS Antivirus

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

ID	Indicadores	Resultado	Meta
AV-1	Cobertura de antivirus	99,51%	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 121 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 noviembre, se realizó la evaluación cuantitativa de la muestra de 259 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	4	99,7%
2. Asunto	4	99,7%
3. Descripción	5	99,6%
4. Prioridad	0	100,0%
5. Categoría	14	99,0%
6. Escalamiento	0	100,0%
7. Solución	9	99,4%
8. Estado del Caso	0	100,0%
9. Justificación Estado del Caso	0	100,0%
10. Periodicidad de seguimientos	2	99,9%
11. Elemento CI	2	99,9%
12. Ortografía y redacción	24	98,3%

13. Cumplimiento de ANS	2	99,9%

Tabla 122 Errores cometidos

Se identificaron 66 errores con un porcentaje de cumplimiento consolidado de 95,30%.
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 24 novedades de ortografía y redacción, 14 de categoría y 9 de solución de ANS.

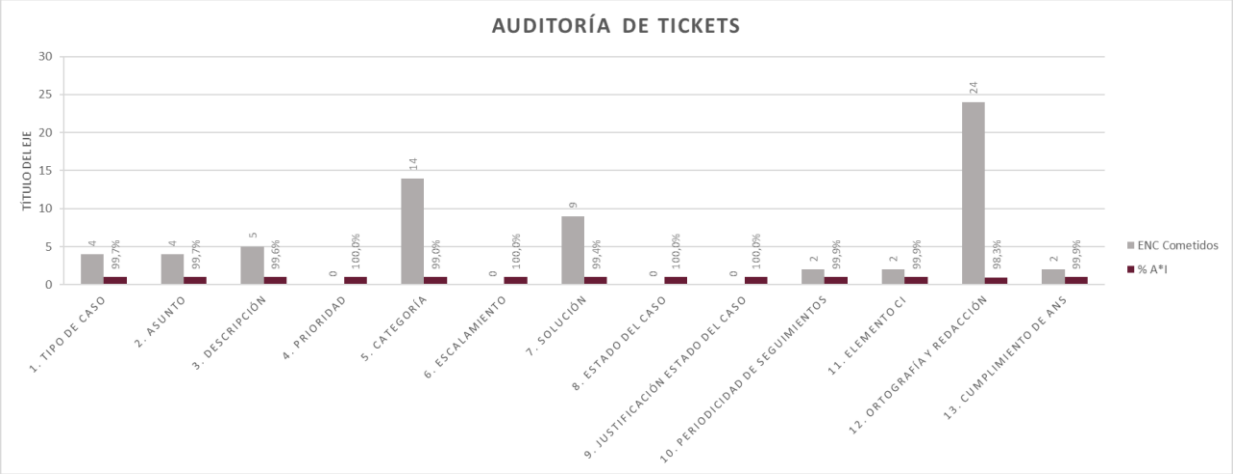


Ilustración 190 Resultados auditoria de casos

5.2 Evaluación de calidad de llamadas

En el mes de noviembre de 2025, se realizó la evaluación cuantitativa de la muestra de las llamadas presentadas con una duración mayor a 1:30 minutos
Para el cálculo de llamadas, se evalúan por cada caso, los criterios definidos, obteniendo el siguiente resultado:

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

	PEC		
#	Practica medida	Q errores	Frec
1	Protocolo de bienvenida y presentacion	0	100%

2	Identificación/captura de datos del usuario	0	100%
3	Comunicación del mensaje de espera	0	100%
4	Comunicación ID solicitud	0	100%
5	Confirmación de satisfacción/encuesta	0	100%

Tabla 123 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 noviembre de 2025. Este apartado contiene información relevante sobre las acciones de mejora identificadas por los Servicios TIC durante el 2025.

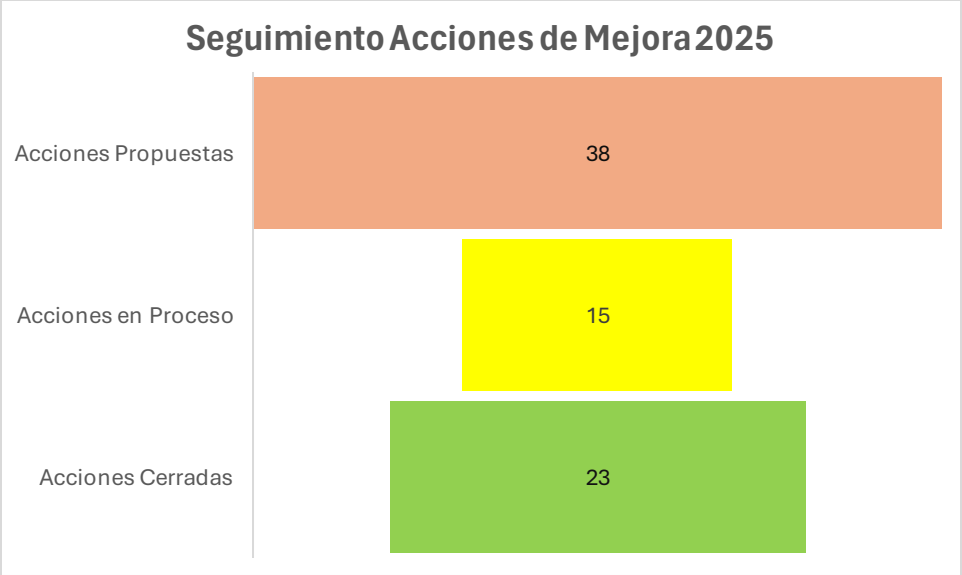


Ilustración 191 Seguimiento Práctica Mejora

En el anterior gráfico, se evidencia que de las 38 acciones de mejora identificadas, 15 acciones se encuentran en proceso y cerradas 23 acciones de mejora, lo cual se cuenta con un cumplimiento de ejecución del cuarto trimestre del 60,53% de los diferentes servicios TIC y Gestiones ITIL al corte del 30 de noviembre de 2025.

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 124 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:

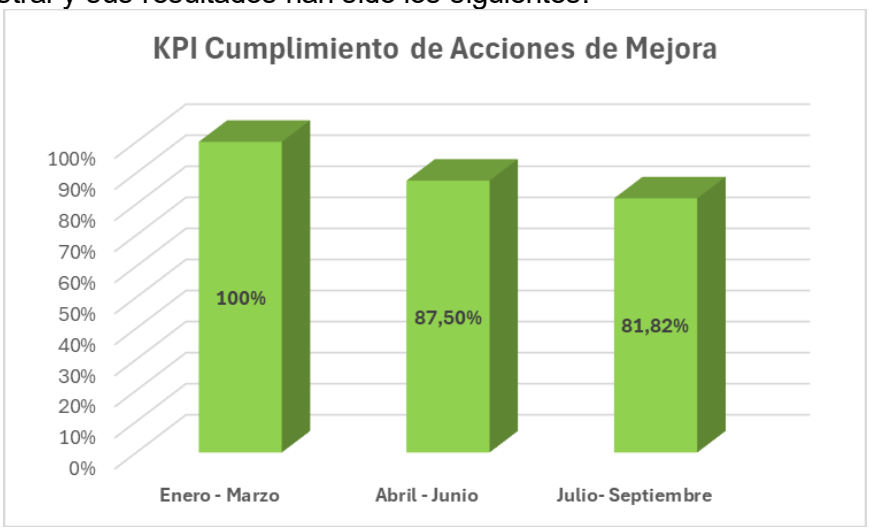


Ilustración 192 Resultado de Cumplimiento AM

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 2 acciones pendiente de fin de ejecución, se encuentra previstas para cierre durante el 4 trimestre del 2025, el cual se realizará el seguimiento y calculo en el mes de diciembre de 2025.

6 GESTION DE RIESGOS

A continuación, se indica el seguimiento a los riesgos identificados para los servicios prestados:

SERVICIO/ PRÁCTICA	NOMBRE	DESCRIPCIÓN	¿MATERIALIZADO?	ACCIONES PARA REALIZAR
Todos	Posibilidad de incumplimiento de obligaciones contractuales	Posibilidad de incumplimiento de obligaciones contractuales relacionadas con cumplimiento, responsabilidad de empleados, proveedores o terceros	NO	Las pólizas se encuentran vigentes
Todos	Incumplimiento en los ANS establecidos en el contrato	Incumplimiento en los ANS establecidos en el contrato	SI	En el periodo se presentaron incumplimiento de 2 ANS relacionados con el servicio de conectividad y se aplicaron las penalizaciones correspondientes
Todos	Ausencia del personal asignado	Ausencia del personal, encargado de gestionar, administrar y operar los servicios.	NO	El personal asignado estuvo disponible durante el periodo.
Todos	Imposibilidad de acceso a la Herramienta de Gestión Aranda	Falla de acceso a la herramienta de gestión.	NO	La herramienta de gestión ha estado disponible

Eventos/ servicio de monitoreo	Imposibilidad acceso a Herramienta monitoreo (Zabbix)	Falla de acceso a la herramienta de monitoreo	NO	La herramienta de gestión ha estado disponible
Mesa de servicios	Problemas de funcionalidad en la cuenta de soportemt@mintrabajo.gov.co.	Falla en el acceso y/o sincronización del correo soportemt@mintrabajo.gov.c o	NO	El correo electrónico institucional ha estado disponible
Mesa de servicios	Imposibilidad de contacto por la línea telefónica de la mesa de servicios	Falla en el ingreso de las llamadas a la mesa de servicios	NO	La línea telefónica ha estado disponible
Mesa de servicios	Desborde de solicitudes (vía correo electrónico y/o llamadas) en la Mesa de Servicios	Aumento eventual de la cantidad de solicitudes que supera la capacidad de atención de los Agentes de la Mesa de servicios	NO	No se ha presentado desborde de solicitudes
Mesa de servicios	Riesgo de seguridad de la información que comprometan la confidencialidad, integridad o disponibilidad de la información.	Posibilidad de uso indebido de la cuenta genérica del cliente, asignada para la Mesa de servicios	NO	No se ha presentado dicha situación.
Soporte en sitio	Incumplimiento de los compromisos pactados por atención de actividades urgentes - no planeadas	Solicitud de realización de actividades urgentes no planeadas que afectan la prestación del servicio de acuerdo con lo planeado	NO	No se ha presentado dicha situación.
Todas las prácticas	Deficiencias en la adopción de las prácticas de ITIL	Resistencia a la adopción de las prácticas de ITIL por las partes interesadas	NO	Se proporcionó capacitación a los involucrados
Práctica de Activos	Posibilidad de pérdida de inventario	La pérdida de inventario se produce cuando las cantidades reales del inventario son inferiores a las registradas en el módulo de gestión	NO	Se realizó seguimiento con el equipo de trabajo para revisar los compromisos de la práctica
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 125 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 color	177	$107.775
	Subtotal	$4.051.687

Tabla 126 Bolsa de Recursos

8 MEDICIÓN DE ACUERDOS DE NIVEL DE SERVICIO

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

Efectuar la medición de los ANS mensualmente.

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

Área	Nombre Indicador	Resultado	Meta
Mesa de Servicio	Tiempo de atención de solicitudes por soporte en sitio	100,00%	95,00%
	Tiempo de solución de incidentes por soporte en sitio	98,75%	90,00%
	Tiempo de solución de requerimientos por soporte en sitio	99,86%	90,00%
	Tiempo de respuesta de la mesa de servicio	100,00%	85,00%
	Abandono de llamadas	0,00%	Máximo 8,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Equipos de usuario final	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
ANTIVIRUS	Cobertura de antivirus	99,51%	95,00%
	Continuidad y disponibilidad de la plataforma	100,00%	98,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
LAN y WLAN	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Energía Regulada	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Datacenter	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Continuidad y disponibilidad del datacenter principal	100,00%	99.95%
	Continuidad y disponibilidad del datacenter alterno	100,00%	99,60%
	Continuidad y disponibilidad de la plataforma de procesamiento, almacenamiento y respaldo	100,00%	99,70%
	Tiempo de solución de incidentes asociado a los servicios de aplicaciones especializadas	100,00%	90,00%
	Tiempo de solución de requerimientos asociado a los servicios de aplicaciones especializadas	100,00%	90,00%
	Continuidad y disponibilidad de los servicios de directorio activo	100,00%	99,60%
	Continuidad y disponibilidad de los servicios de seguridad informática	100,00%	99,90%
	Tiempo de solución de incidentes asociado a los servicios de administración, soporte y monitoreo	99,49%	90,00%
	Tiempo de solución de requerimientos asociado a los servicios de administración, soporte y monitoreo	99,56%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Nube pública	Continuidad y disponibilidad de la nube pública	100,00%	99,90%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Outsourcing de impresión	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Telefonía IP	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Continuidad y disponibilidad de los servicios de telefonía IP	99,95%	99,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Conectividad WAN e Internet	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Continuidad y disponibilidad del servicio de WAN en sedes nacionales con un solo enlace	(*)	99,60%

	Continuidad y disponibilidad del servicio de WAN en sedes nacionales con doble enlace (principal MPLS + secundario Internet dedicado)	(*)	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 127 Medición de Acuerdos de Niveles de Servicio noviembre 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 noviembre
- detalle_llamadas_recibidas_(01.11.2025-30.11.2025)
- Datos_Mintrabajo_noviembre

FIN DEL DOCUMENTO