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

Marzo de 2025

DOCUMENTO/ ARCHIVO	
Código:	**Informe Gestión - Unión Temporal Gestión TIC 2023**
Nombre Archivo:	**Informe Gestión - Unión Temporal Gestión TIC 2023 – Marzo 2025**
Fecha:	7/04/2025
Versión:	1

REGISTRO DE CAMBIOS			
Versión	**Páginas**	**Fecha Modificación**	**Motivo del cambio**
1	202	07/04/2025	Elaboración del documento

CONTROL DE DOCUMENTOS			
Versión	**PREPARADO**	**REVISADO**	**APROBADO**
1	**Equipo de Operación del Proyecto**	Paola Barrero Castro **Gestor ITIL Senior**	Diana Marcela Rueda **Gerente de Proyecto**

Índice

Introducción 12
Objetivo 12
Alcance 12
Definición de Siglas y Expresiones Técnicas 12
1 GERENCIA Y/O ADMINISTRACIÓN 14
2 LÍNEA DE GESTIÓN DE SERVICIOS 14
2.1. Gestión del Servicio 14
2.1.2. Prácticas ITIL 4 21
2.1.2.1. Práctica Acuerdos Niveles de Servicio (ANS) 21
2.1.2.2. Práctica Habilitación de Cambios 21
2.1.2.3. Práctica Activos 23
2.1.2.4. Práctica Catálogo de servicios 25
2.1.2.5. Práctica de Problemas 26
2.1.2.6. Práctica de Incidentes 27
2.1.2.7. Práctica de Requerimientos 30
2.1.2.8. Práctica de Eventos 32
2.1.2.9. Práctica de Disponibilidad 44
2.1.2.10. Práctica de Implementación 46
2.2. Mesa de Servicios y Soporte en Sitio 47
3. LINEA DE SERVICIOS CENTRALES 63
3.1. Datacenter 64
3.1.1. Datacenter Principal 64
3.1.2. Datacenter Alterno y DRP 77
3.1.3. Procesamiento, Almacenamiento y Respaldo 80
3.1.4. Aplicaciones Especializadas 90
3.1.5. **No aplica** 139
3.1.6. Seguridad Informática 139
3.1.6.1. Firewalls de nueva generación 139
3.1.6.2. Sandbox – Amenazas día 0 144
3.1.6.3. SIEM - Solución de correlación de eventos de seguridad, disponibilidad y recursos 146
3.1.6.4. WAF - Servicio de tipo “Firewall de Aplicaciones Web” 152
3.1.6.5. Solución de Anti-DDoS 153
3.1.7. Licenciamiento 156
3.1.8. Administración, soporte y monitoreo 156
3.2. No aplica 157
3.3. Conectividad WAN, SDWAN e Internet 157

3.3.1. Canales WAN 157
3.3.1.1. Incidentes de Conectividad 158
3.3.1.2. Topología Actual 159
3.3.2. Canales SDWAN e Internet Dedicado 159
4. LINEA DE SERVICIOS EN SEDE 165
4.1. Equipos de Cómputo de usuario final 165
4.1.1. Equipos de Escritorio 166
4.1.2. Equipos Portátiles 166
4.2. Conectividad LAN y WLAN 167
4.2.1. Switch CORE Sede Principal 168
4.2.2. Switch para conexiones perimetrales (EDGE) en sede principal 168
4.2.3. Switch de acceso 24 puertos 168
4.2.4. Switch de acceso 48 puertos 169
4.2.5. Puntos de Acceso 170
4.3. Telefonía IP 171
4.3.1. Teléfono Gama Media 171
4.3.2. Teléfono Gama Baja 171
4.3.3. Troncales SIP 172
4.3.4. No Aplica 172
4.3.5. No Aplica 172
4.3.6. Módems 4G – Con plan de 50 Gbps 172
4.4. Energía Regulada UPS 178
4.4.1. UPS 10 kVA 178
4.4.2. UPS 15 kVA 179
4.4.3. UPS 20 kVA 179
4.5. No aplica 180
4.6. Outsourcing de Impresión 180
4.6.1. No aplica 182
4.6.2. Multifuncional B/N rango medio – Cargo fijo mensual 182
4.6.3. Impresora Color rango medio – Cargo fijo mensual 182
4.6.4. No aplica 182
4.6.5. Multifuncional B/N rango medio – Clic de impresión 182
4.6.6. Impresora Color rango medio – Clic de impresión 183
4.7. Antivirus 185
4.7.1. Instalaciones de antivirus en servidores 185
4.7.2. Instalación de antivirus PCs usuarios final 185
4.7.3. Top 10 spyware 186

4.7.4. Top 10 Virus Detectados 187
4.7.5. Servicio de Vulnerabilidades 188
4.7.5.1. Inventario y licenciamiento 189
4.7.5.2. Escaneos programados 189
4.7.5.3. TOP 10 – Vulnerabilidades más explotables 190
4.7.5.4. Estrategia de remediación y/o mitigación 191
4.7.5.5. Resumen de mitigación efectuada 191
4.7.5.6. Ethical Hacking Primer semestre 2025 192
5. GESTIÓN DE CALIDAD DE INFORMACIÓN 193
5.1 Metodología calidad documental de casos 193
5.2 Evaluación calidad documental de casos 194
5.3 Metodología de calidad de llamadas 195
5.4 Evaluación de calidad de llamadas 197
6. GESTION DE RIESGOS 198
7. BOLSA DE RECURSOS 201
8. MEDICIÓN DE ACUERDOS DE NIVEL DE SERVICIO 201
9. ANEXOS 202

Índice de Tablas

Tabla 1 Atención de solicitudes por grupo de especialistas 16
Tabla 2 Lista de chequeo de retiro Nivel Central 19
Tabla 3 Consolidado de elementos y cantidades – Nivel Central 19
Tabla 4 Tipificación de cambios 21
Tabla 5 Distribución de equipos por ubicación y tipo de equipo 24
Tabla 6 Distribución de Agentes Aranda activos a nivel nacional 25
Tabla 7 Tipo de registro de tickets en Aranda 25
Tabla 8 Categorías Cambios 26
Tabla 9 Novedad Matriz de Escalamiento 26
Tabla 10 Listados Incidentes 27
Tabla 11 Top 10 Categorías Incidentes 27
Tabla 12 Incidentes Mayores Registrados 28
Tabla 13 KPI Práctica de Incidentes 29
Tabla 14 Causas Reaperturas 30
Tabla 15 Causas Reaperturas 30
Tabla 16 Top 10 Categorías Requerimientos 30
Tabla 17 Casos reabiertos 31
Tabla 19 Detalle de KIP Practica de Requerimientos 31
Tabla 19 Consolidado disponibilidad de servidores 44
Tabla 20 Consolidada disponibilidad de Directorio Activo 44
Tabla 21 Desagregado de Disponibilidad Directorio Activo 44
Tabla 22 Consolidado disponibilidad de equipos Datacenter principal 44
Tabla 23 Desagregado de Disponibilidad Datacenter Principal 45
Tabla 24 Consolidado disponibilidad de equipos Datacenter alterno 45
Tabla 25 Desagregado Disponibilidad de equipos Datacenter alterno 45
Tabla 26 Consolidado disponibilidad de equipos redes y conectividad 45
Tabla 27 Consolidado disponibilidad de equipos de seguridad 45
Tabla 28 Disponibilidad de equipos Seguridad de la Información 46
Tabla 29 Consolidado disponibilidad de equipos de telefonía 46

Tabla 30 Consolidado disponibilidad de plataforma antivirus 46
Tabla 31 Atención de Llamadas 47
Tabla 32 Top 10 administración de servidores 48
Tabla 33 Top 10 redes y conectividad 48
Tabla 34 Top 10 seguridad informática 49
Tabla 35 Top Telefonía IP 49
Tabla 36 Top 10 soporte aplicaciones 49
Tabla 37 Top 10 soporte microinformática 50
Tabla 38 Casos Anulados por Servicio 50
Tabla 39 Casos Suspendidos por Servicio 50
Tabla 40 Casos solucionados mesa de servicios 51
Tabla 41 Casos solucionados soporte en sitio 52
Tabla 42 Incidentes solucionados por Soporte Territoriales 52
Tabla 43 Requerimientos solucionados por Mesa de Servicios 53
Tabla 44 Requerimientos solucionados por Soporte en sitio 53
Tabla 45 Requerimientos solucionados por Soportes Territoriales 54
Tabla 46 Casos cerrados por la mesa de servicios 56
Tabla 47 Casos cerrados por soporte en sitio 57
Tabla 48 Casos cerrados por Territoriales 60
Tabla 50 Casos usuarios VIP 60
Tabla 51 Casos usuarios Regulares 60
Tabla 52 Medio de ingreso de casos 61
Tabla 53 Visitas en sedes sin Soporte en Sitio 63
Tabla 54 Consolidado de Visitas en sedes sin Soporte en Sitio 63
Tabla 55 Medición ANS Mesa de Servicios 63
Tabla 56 capacidades de acuerdo con las fichas técnicas 67
Tabla 57 Capacidades consumidas (Sin servidores de backup) 69
Tabla 58 Capacidades SI – IVC 84
Tabla 59 Almacenamiento asignado - SI – IVC 85
Tabla 60 Migración actividades .NET 101
Tabla 62 Dimensionamiento Servers IBM - Virtualización Optima 114
Tabla 63 Apps & DDBB Oracle 118
Tabla 64 Escenario de Capacidades Oracle - Estado de consumo Actual 119
Tabla 65 Escenario de Capacidades Oracle - Total de recursos empleados 119
Tabla 66 *Top tráfico de aplicaciones* 142
Tabla.67 Listado de incidentes atendidos 153
Tabla.68 Listado de requerimientos atendidos 155
Tabla.69 Ejecución de archivos maliciosos 155
Tabla.70 Vulnerabilidades en la infraestructura 155
Tabla.71 Ataque de Phishing dirigidos 155
Tabla 72 Licenciamiento 156
Tabla 73 Medición ANS Datacenter 157
Tabla 74 Medición ANS Nube Pública 157
Tabla 75 Novedades servicio de internet 158
Tabla 76 Sedes configuradas en marzo 2025 163
Tabla *77* Medición de ANS Conectividad WAN e Internet 163
Tabla 78 Desagregado sedes con novedad un solo enlace 163
Tabla 79 Desagregado sedes con novedad doble enlace 164
Tabla 80 Cantidades de equipos a distribuir a nivel nacional 165
Tabla 81 Estado de casos de garantía. 165
Tabla 82 ANS casos de garantía. 165
Tabla 83 ANS Equipos en siniestro 166
Tabla 84 *Avance instalación de equipos* 166
Tabla 85 Solicitudes de Equipos Usuario Final – Según Grupo Responsable 167
Tabla 86 Solicitudes de Equipos Usuario Final – Según Tipificación y Categoría 167
Tabla 87 Medición ANS Equipos de Usuario Final 167

Tabla 88 Top 5 de categorías en el Servicio de conectividad LAN-WLAN 168
Tabla 89 Distribución y Cantidades de switch 24 puertos 169
Tabla 90 Distribución y Cantidades de Switch 48 puertos 170
Tabla 91 Distribución de puntos de acceso 170
Tabla 92 Medición ANS LAN y WLAN 171
Tabla 93 Equipos gama media 171
Tabla 94 Sedes cerradas 172
Tabla 95 Consolidado de teléfonos gama baja 172
Tabla 96 Consolidado equipos MIFI 172
Tabla 97 Minutos, consumos 174
Tabla 98 Top 5 llamadas LDN 174
Tabla 99 Top 5 llamadas LDI 175
Tabla 100 Top 5 llamadas Celular 176
Tabla 101 Top 5 llamadas locales 176
Tabla 102. Capacitaciones y divulgaciones 176
Tabla 103 Medición ANS Telefonía IP 177
Tabla 104 Inventario de UPS – 10kVA 178
Tabla 105 Inventario de UPS – 20Kva 180
Tabla 106 Medición ANS Energía Eléctrica UPS 180
Tabla 107 Consumo de impresiones por usuario - Impresoras B/N 181
Tabla 108 Top 10 de impresoras con mayor uso 181
Tabla 109 Top oficinas 182
Tabla 110 Cargo mensual multifuncional rango medio 182
Tabla 111 Cargo mensual impresora color 182
Tabla 112 Clics de Impresión de marzo 2025 – Multifuncional B/N 182
*Tabla 113 T*endencia de consumo de clics B/N 182
Tabla 114 Top 10 impresoras más usadas del servicio de fotocopiado 183
Tabla 115 Clics de Impresión de marzo 2025 – Impresora Color 183
Tabla 116 tendencia de consumo de clics color 183
Tabla 117 Ampliación de cuota de impresión 184
Tabla 118 Despacho de papel a sedes del Ministerio del Trabajo 184
Tabla 119 Medición ANS Outsourcing de Impresión 185
Tabla 120 Top spayware 187
Tabla 121 Top 10 virus detectados 188
Tabla 122 Total de vulnerabilidades 190
Tabla 123 TOP 10 - Activos más explotables 191
Tabla 124 Medición de ANS Antivirus 193
Tabla 125 Criterios y parámetros calidad documental casos 194
Tabla 126 Errores cometidos 194
Tabla 127 PRECISIÓN ERROR NO CRÍTICO – PENC 196
Tabla 128 Criterios y parámetros calidad de llamadas 196
Tabla 129 Calificación Calidad llamadas 197
Tabla 130 Resultado de criterios y parámetros - Calidad de llamadas 197
Tabla 131 Seguimiento a riesgos 200
Tabla 132 Bolsa de Recursos 201
Tabla 133 Medición de Acuerdos de Niveles de Servicio marzo 2025 202

Índice de Ilustraciones

Ilustración 1 Volumetría de casos en el período 15
Ilustración 2 Socialización Árbol de Categorías 25
Ilustración 3 KPI Efectividad de Resolución de Incidentes de Servicio 29
Ilustración 4 KPI Incidentes de Reabiertos en el periodo 29
Ilustración 5 KPI Efectividad de Resolución de Requerimientos de Servicio 32
Ilustración 6 KPI Requerimientos de Reabiertos en el periodo 32

Ilustración 7 Cantidad de Incidentes por Tipo 33
Ilustración 8 Número de eventos de Access Point por CI 34
Ilustración 9 Causas de alertamiento Access Point 34
Ilustración 10 TOP 5 sedes alertados por AP 35
Ilustración 11 Servidores alertados por plataforma 35
Ilustración 12 Servidores Linux Afectados 35
Ilustración 13 Servidores Windows 36
Ilustración 14 Causas de alertamientos (Servidores) 36
Ilustración 15 Casos solucionados vs casos suspendidos (Servidores) 37
Ilustración 16 Switches alarmados por sede 37
Ilustración 17 Casos solucionados vs suspendidos (Switch) 38
Ilustración 18 Causas de incidentes (Switches) 38
Ilustración 19 TOP 10 Routers alarmados por sede 38
Ilustración 20 Causas de alertamiento (Routers) 39
Ilustración 21 Total Alarmas Starlink 39
Ilustración 22 Alertamientos por sede Starlink 40
Ilustración 23 Causas de incidente Dispositivos Starlink 40
Ilustración 24 SD WAN fortigate 41
Ilustración 25 Grafica de CPU 43
Ilustración 26 Grafica de memoria Zabbix 43
Ilustración 27 Atención de Llamadas 47
Ilustración 28 Casos solucionados mesa de servicios 51
Ilustración 29 Casos solucionados soporte en sitio 52
Ilustración 30 Incidentes Solucionados por Soportes Territoriales 52
Ilustración 31 Requerimientos Solucionados por la Mesa de Servicios 53
Ilustración 32 Requerimientos Solucionados por Soporte en sitio 54
Ilustración 33 Requerimientos solucionados por Soportes Territoriales 55
Ilustración 34 Casos cerrados por la mesa de servicios 56
Ilustración 35 Casos cerrados por Soporte en Sitio 58
Ilustración 36 Casos cerrados por Territoriales 60
Ilustración 37 Modo de Ingreso de Solicitudes 61
Ilustración *38* Cumplimiento WSUS 65
Ilustración 39 Estado final de los casos Windows 65
Ilustración 40 Casos por categorías Windows 66
Ilustración 41 Estado final de los casos Nube privada 66
Ilustración 42 Casos por categoría Nube privada y pública 67
Ilustración 43 Infra total + servidores de pruebas + servidores a desaprovisionar 67
Ilustración 44 Infra total producción + servidores de pruebas de la entidad 68
Ilustración 45 Infra total sin servidores de pruebas 68
Ilustración 46 Capacidades consumidas por entornos de pruebas 68
Ilustración 47 Estado File Server Mintrab60 69
Ilustración 48 Proyección de Modelo de Suscripción 70
Ilustración 49 Modelo de Tenant bajo arquitectura 70
Ilustración 50 Comportamiento SWCORE Datacenter Colombia XV 76
Ilustración 51. Grafica de consumo canal Internet Datacenter 76
Ilustración 52 Diagrama Interoperabilidad Bogotá CXV 77
Ilustración 53 VM Replicadas a través de site recovery 78
Ilustración 54 Diagrama de Replicación CXV - Santa Mónica 78
Ilustración 55 Grafica de consumo LanToLan extremo Cali 79
Ilustración 56 Grafica de consumo LanToLan extremo Bogotá 79
Ilustración 57 Estado SWCORE Datacenter alterno 80
Ilustración 58 Detalle servidor 86
Ilustración 60 Hardware solicitado 87
Ilustración 61 Componentes Moodle nuevo 88
Ilustración *62* Estado final de casos – Aplicaciones Especializadas 94
Ilustración 63 categorías Apps 94

Ilustración 64 Estado pre-ventana 104
Ilustración 65 Generación de Backups DDBB 104
Ilustración 66 Validación Tablas DDBB 105
Ilustración 67 Validación Tablas DDBB 105
Ilustración 68 Validación Tablas DDBB 105
Ilustración 69 Validación Tablas DDBB 106
Ilustración 70 Validación Tablas DDBB 106
Ilustración 71 Validación Tablas DDBB 106
Ilustración 72 validación Tablas DDBB 107
Ilustración 73 Verificación Registros 107
Ilustración 74 Verificación Registros 107
Ilustración 75 Verificación Registros tras ejecución de procesos 108
Ilustración 76 Validación de estado de tablas tras ejecución de procesos 108
Ilustración 77 Estado de instancias DDDB 108
Ilustración 78 Eliminación de instancias 109
Ilustración 79 Disminución de instancias tras ejecución de proceso 109
Ilustración 80 Estado del servidor - pre-desfragmentación 109
Ilustración 81 Ejecución desfragmentación 110
Ilustración 82 Ejecución desfragmentación 110
Ilustración 83 Ejecución desfragmentación 110
Ilustración 84 Reconstrucción de Índices 111
Ilustración 85 Validación de tamaños de tablas 111
Ilustración 86 Validación de tamaños de tablas 111
Ilustración 87 Validación de tamaños de tablas 112
Ilustración 88 Validación de tamaños de tablas 112
Ilustración 89 Validación de tamaños de tablas 112
Ilustración 90 Validación de tamaños de tablas 113
Ilustración 91 Validación de tamaños de tablas 113
Ilustración 92 Ejecución de estadísticas de validación 113
Ilustración 93 Distribución de licencias Oracle 115
Ilustración 94 Licencias ambientes 115
Ilustración 95 Estado final casos GD 115
Ilustración 96 categoría DDBB 116
Ilustración 97 casos DDBB 117
Ilustración *98* Estado Bases de Datos 118
Ilustración 99 Información base de datos – Servidor 120
Ilustración 100 Estadísticas CPU 120
Ilustración 101 Estadísticas Memoria 120
Ilustración 102 Estadísticas Pool compartido 120
Ilustración 103 Tamaño DDBB 120
Ilustración 104 Tamaño Esquema DDBB 121
Ilustración 105 Rendimiento DDBB 121
Ilustración 106 DDBB por Server 121
Ilustración 107 Host e Instancia CPU 122
Ilustración 108 Estadísticas Memoria 122
Ilustración 109 Estadística Shared Pool 122
Ilustración 110 Tamaño DDBB DBMINTRA 122
Ilustración 111 Tamaño Esquema DDBB 123
Ilustración 112 Rendimiento DDBB MINTRASG 123
Ilustración 113 Información DDBB PLIFERAY 123
Ilustración 114 Host e Instancia CPU 124
Ilustración 115 Estadísticas Memoria 124
Ilustración 116 Estadísticas Shared Pool 124
Ilustración 117 Tamaño DDBB PLifeRay 124
Ilustración 118 Tamaño Esquemas DDBB 124
Ilustración 119 Rendimiento DDBB PlifeRay 125

Ilustración 120 Información DDBB SIGEP 125
Ilustración 121 Estadística Host e Instancia 125
Ilustración 122 Estadística Memoria 126
Ilustración 123 Estadística Shared Pool 126
Ilustración 124 Tamaño DDBB SIGEP 126
Ilustración 125 Tamaño Esquema DDBB 126
Ilustración 126 Rendimiento DDBB SIGEP 127
Ilustración 127 Información DDBB DBSIMPC 127
Ilustración 128 Estadística CPU 127
Ilustración 129 Estadística Memoria 128
Ilustración 130 Estadística Shared Pool 128
Ilustración 131 Tamaño DDBB SIMPC 128
Ilustración 132 Tamaño Esquema DDBB 128
Ilustración 133 Rendimiento DDBB 129
Ilustración 134 Información servidor DBBB 129
Ilustración 135 Host e Instancia CPU 129
Ilustración 136 Estadística memoria 130
Ilustración 137 Estadística Shared Pool 130
Ilustración 138 Tamaño DDBB MINTRASD 130
Ilustración 139 Tamaño Esquemas 130
Ilustración 140 Rendimiento MINTRASD 131
Ilustración 141 Información Server DDBB 131
Ilustración 142 Host e Instancia CPU 131
Ilustración 143 Estadística Memoria 132
Ilustración 144 Estadística Shared Pool 132
Ilustración 145 Tamaño DDBB 132
Ilustración 146 Tamaño DDBB 132
Ilustración 147 Rendimiento DDBB 133
Ilustración 148 Información Server DDBB 133
Ilustración 149 Host e Instancia CPU 134
Ilustración 150 Estadística Memoria 134
Ilustración 151 Estadística Shared Pool 134
Ilustración 152 Tamaño DDBB 134
Ilustración 153 Tamaño Esquemas DDBB 135
Ilustración 154 Rendimiento DDBB 135
Ilustración 155 Información Server DDBB 136
Ilustración 156 Estadística CPU 136
Ilustración 157 Estadística Memoria 136
Ilustración 158 Estadística Shared Pool 136
Ilustración 159 Tamaño Esquemas DDBB 137
Ilustración 160 Comportamiento DDBB 137
Ilustración 161 Almacenamiento ASM 138
Ilustración 162 DiskGroup Data 138
Ilustración 163 DiskGroup Flash 138
Ilustración 164 DiskGroup Reco 139
Ilustración 165 DiskGroup Redo 139
Ilustración 166 Licenciamiento adicional componente IBM 139
Ilustración167 Disponibilidad firewall 140
Ilustración168 Comportamiento ancho de banda 140
Ilustración 169 Reporte consumo ancho de banda 141
Ilustración170 Top de usuarios 141
Ilustración 171 Top tráfico de aplicaciones 142
Ilustración 172 Top 15 Authenticated Logins by VPN Connections 143
Ilustración 173 Failed Login Attempts by User 143
Ilustración 174 estadísticas de escaneo 144
Ilustración 175 performance 145

Ilustración 176 Licenciamiento 146
Ilustración 177 Casos de uso 147
Ilustración 178 Disponibilidad 147
Ilustración 179 Autenticación de seguridad 149
Ilustración 180 Violación de políticas 150
Ilustración 181 Incidentes 150
Ilustración 182 Disponibilidad de servidores- Seguridad 151
Ilustración 183 Desempeño CPU 152
Ilustración 184 Top attack types 152
Ilustración 185 Top de ataques 153
Ilustración 186 Login fallidos 153
Ilustración *187*. Grafica de consumo canal MPLS Datacenter 158
Ilustración 188 Uptime del equipo MPLS Datacenter 158
Ilustración 189. Topología actualizada 159
Ilustración 190. Interface Fortimanager 160
Ilustración 191. Interface MPLS HUB SDWAN 160
Ilustración 192 Interface Internet HUB SDWAN 161
Ilustración 193. VPN SDWAN establecidas 161
Ilustración 194. Estado HUB SDWAN Datacenter 162
Ilustración 195. Recursos Fortimanager 162
Ilustración 196 Estado de casos Redes y Conectividad 168
Ilustración 197. Licencias y extensiones 173
Ilustración 198 Estadística de tráfico 173
Ilustración 199 Top LDN 174
Ilustración 200 *Top LDI* 175
Ilustración 201 Top Celular 175
Ilustración 202 Top Local 176
Ilustración *203 Requerimientos por garantía* 177
Ilustración 204 *Disponibilidad y Continuidad TOIP* 177
Ilustración 205 Equipos consola antivirus 185
Ilustración 206 Gestión consola antivirus – equipos usuario final 186
Ilustración 207 Top *infección virus* 188
Ilustración 208 Gestión consola Nessus 189
Ilustración 209 Vulnerabilidades gestionadas vs en remediación 192
Ilustración 210 Criterios calidad documental casos 193
Ilustración 211 Resultados auditoria de casos 195
Ilustración 212 Precisión error no Critico de llamadas 195
Ilustración 213 Precisión error Critico de llamadas 195
Ilustración 214 Resultados llamadas PENC 198
Ilustración 215 Resultados llamadas PEC 198

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 marzo de 2025

Alcance

A continuación, se mencionan los componentes sobre los cuales se presenta el cumplimiento de las obligaciones:

GERENCIA Y/O ADMINISTRACION
- Gerencia y/o administración

LINEA DE GESTION DE SERVICIOS
- Gestión del Servicio
- Herramienta de gestión ITSM
- Prácticas Itil 4
- Mesa de Servicio y Soporte en Sitio

LINEA DE SERVICIOS CENTRALES
- DATACENTER
  - Datacenter principal
  - Datacenter Alterno y DRP
  - Procesamiento, almacenamiento y respaldo
  - Aplicaciones especializadas
  - Seguridad informática
  - Licenciamiento
  - Administración, soporte y monitoreo
- CONECTIVIDAD WAN, SD-WAN E INTERNET

LINEA DE SERVICIOS EN SEDE
- Equipos de cómputo de usuario final
- Conectividad WLAN y Red LAN
- Telefonía IP
- Energía regulada UPS
- Outsourcing de Impresión
- Antivirus

MEDICIÓN DE ACUERDOS DE NIVEL DE SERVICIO
BOLSA DE RECURSOS

Definición de Siglas y Expresiones Técnicas

ANS: Acuerdos de Nivel de Servicio.
DRP: Disaster Recovery Plan - Plan de Recuperación ante Desastres
DT: Dirección Territorial.
IM: Incidentes.

ITSM: Information Technology Service Management - Gestión de servicios de TI
OE: Oficina Especial.
RF: Peticiones o Requerimientos de Servicio.
LAN: Local Area Network - Red de Área Local
MDS: Mesa de Servicio
NOC: Network Operations Center - Centro de Operaciones de Red.
SD-WAN: Software Defined Wide Area Network - Red de Área Extensa Definida por Software.
SOC: Security Operations Center - Centro de Operaciones de Seguridad.
SS: Soporte en Sitio
UPS: Uninterruptable Power Supply - Sistema de Alimentación Ininterrumpida.
UT: Unión Temporal Gestión TIC 2023.
WAF: Web Application Firewall - Firewall de aplicaciones Web.
WLAN: Wireless Local Area Network - Red de Área Local Inalámbrica.

Acción de Mejora: Acción que identifica una actividad, aspecto u oportunidad que pueda mejorarse en un servicio o proceso y al ejecutarse aporta valor a la operación.
Procedimientos: Son los documentos que describen la secuencia ordenada de acciones que concurren en la realización de una función específica, tanto técnica, administrativa, como de gestión.
Proceso: Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados.
Acuerdos de Niveles de Servicios (ANS): Acuerdo entre un proveedor de Servicios de TI el cliente, describe el Servicio de TI, documenta las Metas de Niveles de Servicio y específica las responsabilidades del Proveedor de Servicios de TI y del Cliente.
Contacto: Interacción entre el usuario y la Mesa de Servicios para solicitar alguno de sus servicios (incidentes, consultas, interacciones de servicio), este puede ser llevado a través de cualquiera de los canales ofrecidos.
Interacción: Término utilizado en la herramienta de gestión que sirve para identificar las peticiones creadas y resueltas durante la atención del primer nivel y que son generados por una petición de servicio de los usuarios.
Incidente: Una interrupción no planificada de un Servicio de TI, una reducción en su calidad o una falla que ha impactado su prestación. En la herramienta de gestión se usa este término para los incidentes que han sido escalados por el primer nivel de atención y son identificados con las letras IM.
Incidente Mayor: Cualquier evento identificado con prioridad crítica.
Problema: Incidentes repetitivos o de gran impacto, del cual no se conoce las causas que lo originan.
Peticiones: Solicitud que realizan los usuarios para los servicios TIC y son representados por la letra (RF).
Soporte Primer Nivel: Corresponde a los grupos de la mesa de servicios que brindan soporte por vía telefónica, correo electrónico, portal web, chat y a las personas que brindan el soporte en sitio en cada una de las sedes del contrato y los grupos de soporte especializados de cada servicio de TI.
Nivel Especializado: Soporte especializado de solución de peticiones de servicios TIC.
Usuario: Es la persona que utiliza o trabaja con algún dispositivo provisto por el Contratista o que utiliza el servicio de TI definido dentro el alcance del contrato.

1 GERENCIA Y/O ADMINISTRACIÓN

Durante el mes objeto del presente informe en gestión no se adelantó ningún modificatorio.

2 LÍNEA DE GESTIÓN DE SERVICIOS

2.1. Gestión del Servicio

Durante el período del informe, desde la Gestión de Servicios se apoyaron las siguientes actividades:

a. Divulgación de comunicados a través de Soporte MT:

El equipo de Gestores ITIL y procesos apoyaron la operación de los servicios con la elaboración, recepción de VoBo por parte de la supervisión del contrato 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.
- En el marco de las estrategias de uso y apropiación del servicio de Outsourcing de Impresión se generan piezas con orientaciones para fortalecer la política de cero papel y el uso adecuado de clics asignados y limitar el uso de consumibles.



¡INFORMACIÓN
IMPORTANTE SERVIC

- Publicación de mensaje de entrega de bienes relacionada con el paz y salvo de elementos tecnológicos.



¡INFORMACION
IMPORTANTE DEVOL

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

- Apoyo para la actualización del banner de la Pagina Web con el PBX del ministerio, la pieza ya fue aprobada pero no se ha actualizado en el sitio.
- El 13 de marzo 2025 se envia a la Coordinación del Grupo de Soporte Informático la propuesta del contenido sugerido para la intranet relacionada con el Grupo de Soporte Informático. A espera de observaciones y la coordinación del espacio con la Oficina de Comunicaciones para ampliar el tema.



Propuesta de
información para Intra

b. Traslados y novedades de sedes:

- **Traslado Inspección de trabajo Acacías (Meta):** El 22 de noviembre el Ministerio realizó traslado de la inspección de Acacías sin notificación a la UT, se asistió a la sede para instalación de equipos de usuario final, se solicitó formalmente el traslado del canal al proveedor de conectividad, se despachó e instaló antena Satelital Starlink como

contingencia para la conexión a Internet. La sede no cuenta con cableado estructurado para la conexión LAN, por lo que se realiza visita para Site Survey y cotización de estos servicios al Ministerio del trabajo. Durante el mes de marzo 2025 se tuvo VoBo de la Coordinación del Grupo de Soporte Informático a la oferta realizada y se agenda la instalación de los puntos para el 7 de abril 2025.

- **Traslado Inspección de trabajo Tumaco (Nariño):** El 25 de noviembre el Ministerio realizó traslado de la inspección de Tumaco sin notificación a la UT, asistió a la sede para instalación de equipos de usuario final, se solicitó formalmente el traslado del canal al proveedor de conectividad, se despachó e instaló antena Satelital Starlink como contingencia para la conexión a Internet. La sede no cuenta con cableado estructurado para la conexión LAN, por lo que se realiza visita para Site Survey y cotización de estos servicios al Ministerio del trabajo. Durante el mes de marzo 2025 se tuvo VoBo de la Coordinación del Grupo de Soporte Informático a la oferta realizada y se agenda la instalación de los puntos para el 7 de abril 2025.

c. Matriz de escalamiento de la MDS

El 28 de marzo 2025 se remite actualización de la Matriz de Escalamiento de la MDS con las siguientes novedades:

- Se actualiza nombre de especialista de aplicaciones .Net
- Se realiza actualización del nuevo soporte de Mocoa Robinson Lasso
- Se realiza actualización del nuevo soporte de piso 22 sede central Yerik Stevens Castro Grosso

d. Volumetría de Solicitudes Gestionadas:

En el mes de marzo 2025 se registraron en la herramienta ITSM 7929 casos, 5282 requerimientos de servicio, 2633 incidentes y 13 cambios, se registró 1 problema (tipificado por error durante la gestión del mes). 20 casos fueron anulados por la MDS.

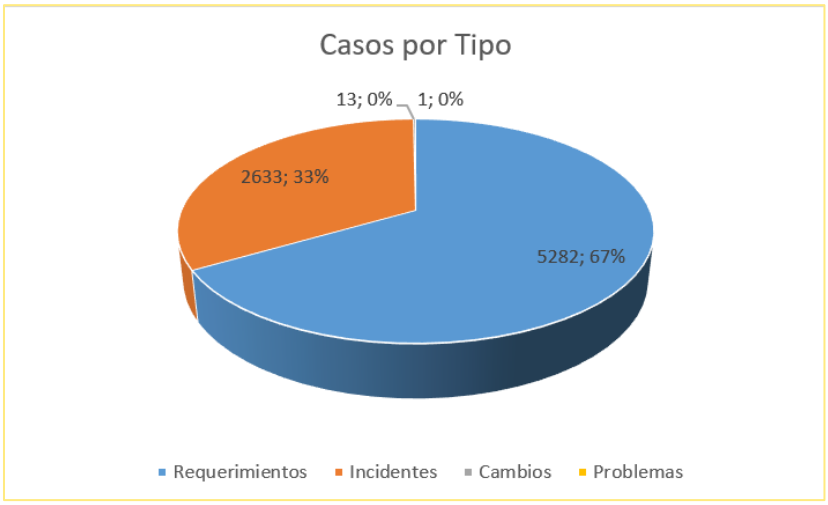


Ilustración 1 Volumetría de casos en el período

Gestión por parte de los grupos de especialistas: A continuación, se presenta la distribución de esta volumetría según los grupos de especialistas:

Grupo Responsable	Cantidad de casos gestionados	Porcentaje de casos gestionados (%)
Responsable_Soporte_Territoriales	2326	29,34

Grupo Responsable	Cantidad de casos gestionados	Porcentaje de casos gestionados (%)
NOC	1637	20,65
Responsable_Soporte_Bogota	1128	14,23
Responsable_Mesa_De_Servicio	1079	13,61
Responsable_Soporte_Impresoras	891	11,24
Especialistas_IBM	429	5,41
Responsable_De_Servidores_Windows	133	1,68
SOC	59	0,74
Especialista Nube Privada	55	0,69
Especialista Herramientas de Gestion	36	0,45
Especialista Base de datos	34	0,43
Especialista_Telefonía_IP	29	0,37
Especialista Redes	18	0,23
Especialista Aplicaciones .Net	17	0,21
Responsable Garantías Equipos	14	0,18
Gestión del Servicio	13	0,16
Especialista Aplicaciones JAVA	10	0,13
Especialista Nube Publica	8	0,10
Almacenamiento y Backups	4	0,05
CAB Servicios en Sede	3	0,04
CAB Servicios Centrales	2	0,03
Gestor de Inventarios	2	0,03
Liferay	2	0,03
Total general	**7929**	**100,00**

Tabla 1 Atención de solicitudes por grupo de especialistas

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

Se presenta a la Coordinación del Grupo de Soporte informático el plan de trabajo de documentos propuestos para publicación de la SVE el cual fue aprobado para envío a la Oficina Asesora de Planeación. Así mismo, se realiza sesión de presentación de los documentos a la coordinación y el 27 de marzo 2025 se remiten las guías para el iniciar el proceso de publicación en la SVE.


RE_ Plan de trabajo documentos SIG Acue


RE_ Plan de trabajo documentos SIG Acue


RE_ Plan de trabajo documentos SIG Acue

f. Sesiones con el equipo de trabajo

Se desarrollaron las siguientes sesiones con el equipo de trabajo:

- Todos los días se realiza sesión vía Microsoft Teams con el personal de Soporte en Sitio de Territorio para conocer las novedades de las DT, OE e Inspecciones soportadas y gestionar en caso de que se requieran los escalamientos necesarios para asegurar la prestación de los servicios de TI.
- Socialización de la Práctica de Requerimientos al personal de Soporte en Sitio vía Microsoft Teams el 6 de marzo.
- Reiteración de los lineamientos de la Práctica de Implementación vía correo electrónico a todo el equipo de especialistas y responsables de servicios. Esto se realizó el 17 de marzo.

- Socialización de la Practica de Habilitación de Cambios y Práctica de Implementación el 28 de marzo 2025 al Grupo de IVC, se realiza a través de Microsoft Teams y envío de correo electrónico a todos los interesados.
- Se realizan sesiones sobre el despliegue del agente ZTNA a personal de Soporte Técnico Nivel 2.
- Socialización de la Practica de Habilitación de Cambios y Práctica de Implementación el 31 de marzo 2025 al grupo que administra SIRITI (Henry Yamid Villanueva), se realiza a través de Microsoft Teams y envío de correo electrónico a todos los interesados.

g. Recolección de residuos electrónicos y RAEEs

El 31/03/2025 se realiza recolección de residuos electrónicos y RAEEs en Nivel Central, se comparte a continuación los datos principales de la lista de chequeo del transporte por parte de SUMA Desarrollo Ambiental.

FECHA DE GENERACIÓN	FECHA DE CESIÓN	RESIDUO GENERADO	Población y/o ciudad de ubicación	Dirección territorial - Sede	Clasificación decreto 4741 de 2005	CANTIDAD [Kg]
9/01/2025	31/03/2025	Unidades de Tambor Impresoras- RAEE	Bogotá Cll 32	Sede Cll 32	A1180	**2**
8/01/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
8/01/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
13/01/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
13/01/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
13/01/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá Cll 32	Sede Cll 32	Y12	**2**
16/01/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
16/01/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
16/01/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
20/01/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
20/01/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
20/01/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
28/01/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
29/01/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
30/01/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
7/02/2025	31/03/2025	Disco Duro - RAEE	Bogotá central	Sede Nivel Central	A1180	**1**
7/02/2025	31/03/2025	Memorias USB - RAEE	Bogotá central	Sede Nivel Central	A1180	**3**
14/02/2025	31/03/2025	Diademas Lenovo - RAEE	Bogotá central	Sede Nivel Central	A1180	**21**
26/02/2025	31/03/2025	Cables- RAEE	Bogotá central	Sede Nivel Central	A1180	**15**

FECHA DE GENERACIÓN	FECHA DE CESIÓN	RESIDUO GENERADO	Población y/o ciudad de ubicación	Dirección territorial - Sede	Clasificación decreto 4741 de 2005	CANTIDAD [Kg]
14/02/2025	31/03/2025	Mouse - RAEE	Bogotá central	Sede Nivel Central	A1180	**1**
7/02/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
18/02/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
18/02/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
24/02/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
21/03/2025	31/03/2025	Unidad Fusora Impresoras- RAEE	Bogotá Cll 32	Sede Cll 32	A1180	**1**
24/02/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá Cll 32	Sede Cll 32	Y12	**2**
25/02/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
28/02/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
28/02/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
4/03/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
4/03/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
4/03/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
4/03/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá Cll 32	Sede Cll 32	Y12	**1**
4/03/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
6/03/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
5/02/2025	31/03/2025	Unidad Fusora Impresoras- RAEE	Bogotá central	Sede Nivel Central	A1180	**1**
20/02/2025	31/03/2025	Unidades de Tambor Impresoras- RAEE	Bogotá central	Sede Nivel Central	A1180	**1**
17/03/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
18/03/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
19/03/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
25/03/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
25/03/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
26/03/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**

FECHA DE GENERACIÓN	FECHA DE CESIÓN	RESIDUO GENERADO	Población y/o ciudad de ubicación	Dirección territorial - Sede	Clasificación decreto 4741 de 2005	CANTIDAD [Kg]
27/03/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**
28/03/2025	31/03/2025	Cartuchos y tóner de impresoras de oficina	Bogotá central	Sede Nivel Central	Y12	**1**

Tabla 2 Lista de chequeo de retiro Nivel Central

A continuación se incluye la consolidación de los residuos y cantidades entregados:

Sede	Tipo de Residuo	Cantidad
Sede Central Bogotá	Cable VGA- RAEE	1
Sede Central Bogotá	Cartuchos y tóner de impresoras de oficina	106
Sede Central Bogotá	Disco Duro - RAEE	1
Sede Central Bogotá	Memorias USB - RAEE	3
Sede Central Bogotá	Mouse - RAEE	1
Sede Central Bogotá	Unidad Fusora Impresoras- RAEE	2
Sede Central Bogotá	Unidades de Tambor Impresoras- RAEE	4
Sede Central Bogotá	Cable rj45- RAEE	15

Tabla 3 Consolidado de elementos y cantidades – Nivel Central

h. Reporte información de residuos tecnológicos y suministro de resmas de papel

Debido a corte de Q1 de 2025, se realiza envío al Ministerio del Trabajo del reporte de residuos tecnológicos y suministro de resmas de papel entregados por la UT.

- Relación de resmas entregadas a nivel nacional.
- Relación de consumo de papel cargado en impresoras en Nivel Central.
- Clics de impresión a nivel nacional discriminado por mes para cada impresora.
- Instructivo de recolección y Manejo de residuos especiales del proyecto.
- Reporte de la cantidad de residuos tecnológicos de enero a marzo de 2025.
- Certificado de recolección de Nivel Central del 31/03/2025 con su respectiva verificación de la lista de chequeo del transporte por parte de SUMA Ambiental.
- Certificación de capacitación en transporte de mercancías peligrosas de SUMA Desarrollo Ambiental.



i. Otras actividades

- Gestión, seguimiento y consolidación de las evidencias para las visitas a Direcciones Territoriales e Inspecciones de Trabajo que no cuentan con personal de Soporte en Sitio dedicado. En el apartado de MDS y SS se incluye la relación detallada de estas actividades.

- Previa aprobación de la Coordinación del Grupo de Soporte Informático, se gestiona la recuperación del inventario de elementos tecnológicos de la inspección ya que la misma no cuenta con mobiliario para su instalación y se tenían en almacenamiento de la Casa de Justicia del municipio. El 6 de marzo 2025 se reciben todos los elementos en Nivel Central de Bogotá, son recibidos y se actualiza su estado por parte del Administrador de Inventarios.



RE_ Novedad
Inspección El Bagre.m

- El 13 de marzo se envía a la Coordinación del Grupo de Soporte Informático la propuesta de Encuesta de percepción del personal de Soporte en Sitio Territorial (en Forms) y una pieza para recordar la matriz de escalamiento por si se presentan novedades con el personal. A espera de retroalimentación.



Encuesta de
percepción de soporte

- El 15 de marzo se gestiona personal de soporte en sitio de Nivel Central para actividad de apagado controlado de racks en el Edificio WTC por actividad de mantenimiento preventivo eléctrico programado por ASD. Se hizo apagado de racks a primera hora, encendido en horas de la tarde una vez ASD confirmó finalización y pruebas de servicios, reportando normalidad. Se registra la actividad con el caso Aranda RF-92496.

- El 31 de marzo 2025 se comparte a la Coordinación del Grupo de Soporte Informático las cantidades de kits periféricos USB propiedad del ministerio que están asignados y disponibles en las DT donde se tiene personal dedicado de la UT.



RE_ solicitud de
información .msg

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

- Se generó y entregó informe con las novedades de las UPS propiedad del Ministerio del trabajo, cableado eléctrico y puntos de red para presentar al Grupo de Recursos Físicos con el propósito que sean subsanadas estas novedades en pro de una buena prestación de los servicios de TI. Para el período del informe, la coordinación del Grupo de Soporte Informático solicita consolidado de los compromisos y los responsables, se genera listado y se comparten los avances a cargo de la UT.

2.1.1. Herramienta de Gestión ITSM

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

- Creación de categorías adicionales para integración con el Fortisiem (Herramienta SOC).
- Optimización de reportes de sabana de casos general reduciendo el consumo de recursos.
- Se integró el fortisiem con Aranda para la creación automática de casos a partir de los correos enviados por el fortisiem (está en etapa piloto).
- Actualización de ASMS a su última versión.
- Habilitación de API de Zabbix para uso desde PowerBI.
- Atención de solicitudes de Administración Herramienta Zabbix por demanda, ajuste de nombres de nodos, inclusión de equipos de seguridad en monitoreo, programación de estado

de mantenimiento para sedes con novedades por parte de usuario final, en línea con la gestión de eventos.
- Pruebas de funcionalidad de la nueva versión de Zabbix para migración a nueva infraestructura.
- Implementación funcionalidad de control remoto desde ADM.
- Modificación tableros para monitoreo de la infraestructura de la página web de la entidad.

2.1.2. Prácticas ITIL 4

En el marco de la adopción de las prácticas ITIL, durante el mes de marzo de 2025, la UT trabajó en el fortalecimiento y madurez de los lineamientos definidos para cada una de las prácticas que apoyan la operación de los servicios presentados a la entidad.

2.1.2.1. Práctica Acuerdos Niveles de Servicio (ANS)

Dar a conocer las actividades de la Práctica Acuerdos Niveles de Servicios correspondientes al periodo del 1 al 31 de marzo de 2025. Este apartado contiene información relevante sobre actividades realizadas y novedades presentadas.

- **Seguimiento y control de ANS**

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

2.1.2.2. Práctica Habilitación de Cambios

Dar a conocer las actividades de la Práctica Habilitación de Cambios correspondientes al periodo del 1 al 31 de marzo de 2025. Este apartado contiene información relevante sobre actividades realizadas y novedades presentadas.

- **Tipificación de los cambios**

Durante el mes de marzo de 2025 se gestionaron 13 tickets tipificados como Cambios, clasificados en las siguientes categorías:

CATEGORÍAS	NÚMERO DE CASOS	PORCENTAJE (%)
Aplicaciones Especializadas. SICIP	1	8%
Herramientas de Gestión. Aranda	1	8%
Aplicaciones Especializadas. Portal Web	2	17%
Administración de servidores. Servidores	3	25%
Administración de Bases de Datos.Servidor de base de datos	6	46%
Total general	**13**	**100%**

Tabla 4 Tipificación de cambios

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

- **Relación casos registrados**

A continuación, se presenta la relación de casos registrados del 1 al 31 de marzo de 2025, en total se crearon 13 tickets de los cuales se gestionaron 6 como cambios de normales, 6 cambios estándar y 1 cambio de emergencia, los cuales se describen a continuación:



Sesion_HC_Mar_2025.
xlsx

- **Cambios por estado**

Al corte del 31 de marzo, doce (12) casos quedaron *estado Cerrado* y un (1) caso en estado implementar cambio, esto debido a que se debió reprogramar ya que en las pruebas se estableció la conexión entre el MINRAC-SCAN y el servidor MTCABDSQL pero en la instalación del ODBC no se estable la conexión hacia la BBDD de Gestor Documental. Por tal motivo se ejecutará el 3 de abril de 2025.

- **Medición Indicador Porcentaje de Cambios Exitosos**

En el proceso de actualización de la Guía de la Práctica de Habilitación de Cambios, 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 Marzo
Porcentaje de cambios exitosos.	**PCE = (NCE/TCI)*100** Donde: **PCE:** Precisión Cambios Exitosos **NCE:** Numero de Cambios Exitosos **TCI:** Total de Cambios implementados	80%	Mensual	**PCE=11/12***100 **PCE= 91,66%**

La **meta** para este indicador es alcanzar un **80%** de cambios exitosos, y el **resultado de marzo** es **91,66%**, lo cual es **superior a la meta**. Esto indica que el proceso de implementación de cambios fue efectivo, logrando un alto porcentaje de éxito. Este resultado refleja que, de los 12 cambios que se intentaron implementar, 11 fueron exitosos, lo que sugiere un proceso bien gestionado en cuanto a la ejecución de cambios.

- **Actualización de la guía y formato Práctica habilitación de cambios para su inclusión en la SVE**

Durante el periodo correspondiente, se llevó a cabo la actualización de la Guía y el Formato de la práctica de habilitación de cambios con el fin de mejorar los procesos y asegurar que se alineen adecuadamente con los requisitos establecidos para su inclusión en la SVE (Sistema de Gestión de Eventos). Las modificaciones se detallan a continuación:

- **Guía Práctica para la Habilitación de Cambios V2:**

Entradas y Salidas de la Práctica: Se añadieron las entradas y salidas relevantes dentro de la práctica, lo que permite una mayor claridad sobre los puntos de inicio y finalización del proceso de habilitación de cambios.

Indicador de la Práctica: Se incorporó un nuevo indicador que facilitará el seguimiento y evaluación de la práctica, permitiendo medir su efectividad y asegurar el cumplimiento de los estándares de calidad.

Modificación en los Lineamientos del PRE CAB: Los lineamientos relacionados con el PRE CAB (Pre-Cambio de Aprobación de Cambios) fueron ajustados para optimizar el flujo y la toma de decisiones, buscando mejorar la eficiencia y la alineación con los procedimientos ministeriales.

- **Formato de Solicitud de Cambios (RFC) V2:**

Inclusión de los CI en Lista Desplegable: Ahora se pueden seleccionar los CI (Componentes de Infraestructura) relevantes a través de una lista desplegable, lo que mejora la usabilidad y precisión en la solicitud de cambios.

Servicios en Lista Desplegable: Se añadieron los servicios correspondientes en una lista desplegable para facilitar la selección de estos y mejorar la estructura de las solicitudes.

Categorías en Lista Desplegable: Se actualizó el formato con una lista desplegable para las categorías de cambio, lo que permite una clasificación más ordenada y ágil de las solicitudes.

De manera adicional, la Oficina Asesora de Planeación realizó una revisión de estos documentos, con el objetivo de garantizar que cumplan con los requisitos y procedimientos internos establecidos. Estos fueron enviados para su aprobación final por parte de la Coordinación del Grupo de Soporte Informático en la SVE, lo que permitirá su implementación formal y su inclusión en el sistema.

- **Socialización Práctica habilitación de cambios e implementación a las dependencias de la Entidad**

Durante los días 6, 28 y 31 de marzo se llevó a cabo la socialización de la práctica de habilitación de cambios en diversas dependencias de la entidad, específicamente dirigida a la Dirección de Pensiones, la IVC y la Subdirección de Protección Laboral. Esta actividad tuvo como objetivo principal garantizar el cumplimiento de los lineamientos establecidos en los procedimientos del Ministerio, con el fin de asegurar una transición eficiente y alineada con las normativas vigentes.

El proceso de socialización permitió a los participantes comprender de manera detallada las implicaciones de los cambios a implementar, así como las acciones necesarias para adaptarse a los nuevos procedimientos. Además, se proporcionaron herramientas y recursos clave para asegurar que la implementación se realice de manera efectiva, asegurando que las dependencias de la entidad puedan llevar a cabo sus funciones de manera óptima.

A través de estas jornadas, se busca no solo informar a los equipos sobre los cambios, sino también fomentar la colaboración entre las distintas áreas, garantizando que todos los actores involucrados estén plenamente capacitados y alineados con los objetivos del Ministerio. Esta socialización constituye un paso fundamental para el cumplimiento de las normativas y el fortalecimiento de las capacidades operativas dentro de la entidad.



Práctica_Habilitación_Cambios.pptx

2.1.2.3. Práctica Activos

Durante el mes de marzo de 2025, la Práctica de Activos ha llevado a cabo una serie de acciones estratégicas orientadas a asegurar el funcionamiento óptimo y la disponibilidad continua de los servicios dentro de la entidad. Estas acciones han sido fundamentales para mantener la operatividad

de la infraestructura tecnológica y asegurar que todos los recursos se gestionen de manera eficiente, alineados con las mejores prácticas de gestión de activos. A continuación, se detallan las principales actividades ejecutadas durante este periodo:

- **Presentación Gestión Garantías Supervisión y Coordinación Grupo Soporte Informático**

Con el objetivo de proporcionar una visión integral de los procesos implicados en la gestión de garantías, así como de los procedimientos necesarios para abordar los siniestros relacionados con los equipos y servicios tecnológicos el 18 de marzo se llevó a cabo la presentación del flujo de garantías y siniestros ante la Supervisión y la Coordinación del Grupo de Soporte Informático.

Durante la presentación, se detallaron las etapas clave del proceso de gestión de garantías, incluyendo la coordinación con los fabricantes. Se hizo hincapié en la importancia de mantener una comunicación fluida entre los involucrados, para garantizar que todas las incidencias se resuelvan de manera eficiente y dentro de los plazos establecidos.

En cuanto al manejo de siniestros, se explicó el protocolo a seguir en caso de daños o pérdidas de equipos bajo garantía, resaltando las acciones necesarias para la correcta documentación y seguimiento de los incidentes, así como la intervención de los equipos técnicos para evaluar los daños y determinar las posibles soluciones, ya sea reparación o reemplazo de los equipos afectados.

Esta presentación también fue una oportunidad para que plantear preguntas, compartir inquietudes y sugerir mejoras en los procesos, creando un espacio para la retroalimentación constructiva.

En resumen, el objetivo principal de esta reunión fue establecer una comprensión común de los procedimientos y asegurar la correcta implementación de las políticas de gestión de garantías y siniestros, alineando a todo el equipo con las mejores prácticas para garantizar un servicio de soporte técnico de calidad.

Gestión de Garantias.pptx

- **Actualización de información de la CMDB**

Durante el periodo se realizaron procedimientos de rutina de actualización de inventario de equipos y la sincronización de esta información con su correspondiente elemento de configuración CI en la CMDB acordes con la dinámica y actividad propias de los equipos de cómputo.

- **Gestión de inventarios**

Se presenta a continuación, la relación general de equipos por tipo y distribución geográfica en inventario Aranda a la fecha de corte del informe.

Sede/Tipo Equipo	Inventario
Sede Central- DT Bogotá	**651**
DESKTOP	138
PORTATIL	513
Territoriales	**1330**
DESKTOP	971
PORTATIL	359
Total	**1981**

Tabla 5 Distribución de equipos por ubicación y tipo de equipo

- **Aranda – Agentes instalados**

Se presenta a continuación, la relación general de los equipos con instalación del agente Aranda a nivel nacional

PRODUCTO	Distribución Ubicación			Agentes por Ubicación		
	Central	Nacional	Total	Central	Nacional	Total
AGENTE ARANDA	651	1330	1981	32,86%	67,14%	100,00%

Tabla 6 Distribución de Agentes Aranda activos a nivel nacional

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:

- **Ajuste Tipo de Registro Aranda:** Se realizó actualización en los tipos de registro de los casos en la herramienta de gestión. Esta modificación define claramente el tipo de registro que debe utilizarse en cada situación, brindando mayor claridad a los grupos resolutores sobre cómo proceder al momento de crear un caso:

Tipo de Registro	Aplica para
Alarmas Zabbix	NOC, alarmas generadas desde la herramienta de monitoreo
Case Creator Mesa	Creación Tickets Automáticos Mesa de Servicios
Correo Soporte MT	Correos gestionados por Mesa de Servicios
Gestión Técnica	Casos generados por Soporte en Sitio, Especialistas, Líderes, Gestión ITIL
Telefónico	Atención telefónica mesa
Portal Auto-Gestión	Casos creados únicamente por usuarios mediante el Portal de Autoservicio

Tabla 7 Tipo de registro de tickets en Aranda

- **Envío de árbol de categorías:** Se realizó la socialización del árbol de categorías, de acuerdo con los ajustes implementados en Aranda, mediante correo electrónico dirigido a todo el equipo de trabajo.

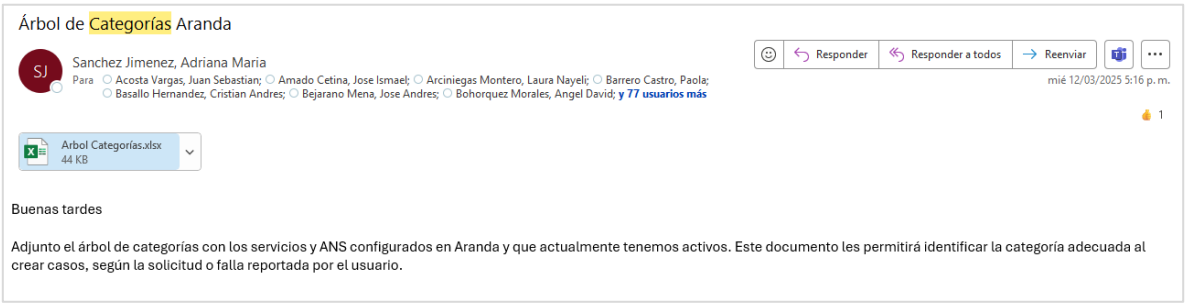


Ilustración 2 Socialización Árbol de Categorías

- **Revisión y Ajuste Categorías de Cambios:** En conjunto con la gestora de cambios y especialistas, se revisó árbol de categorías de la práctica de cambio y se realizaron ajustes quedando de la siguiente manera**:**

Servicio	Jerarquía	Tipo Caso
Administración de Bases de Datos	Radicar un cambio.Servidor de base de datos	Cambio
Administración de servidores	Radicar un cambio.File Server	Cambio

Servicio	Jerarquía	Tipo Caso
Administración de servidores	Radicar un cambio.Directorio Activo	Cambio
Administración de servidores	Radicar un cambio.Servidores	Cambio
Aplicaciones Especializadas	Radicar un cambio.Cobro Coactivo	Cambio
Aplicaciones Especializadas	Radicar un cambio.Gestor documental	Cambio
Aplicaciones Especializadas	Radicar un cambio.SISINFO	Cambio
Aplicaciones Especializadas	Radicar un cambio.SIAS	Cambio
Aplicaciones Especializadas	Radicar un cambio.SIRITI	Cambio
Aplicaciones Especializadas	Radicar un cambio.RUTEC	Cambio
Aplicaciones Especializadas	Radicar un cambio.SFT	Cambio
Aplicaciones Especializadas	Radicar un cambio.Portal Web	Cambio
Energía Eléctrica Regulada - UPS	Radicar un cambio.UPS	Cambio
Herramientas de Gestión	Radicar un cambio.Aranda	Cambio
Herramientas de Gestión	Radicar un cambio.Zabbix	Cambio
Redes y Conectividad	Radicar un cambio. servicio LAN.Switch Sede central	Cambio
Redes y Conectividad	Radicar un cambio. servicio WLAN.Access point Sede Central	Cambio
Redes y Conectividad	Radicar un cambio. servicio WLAN.Access point Dirección Territorial	Cambio
Redes y Conectividad	Radicar un cambio. servicio LAN.Switch Dirección Territorial	Cambio
Redes y Conectividad	Radicar un cambio. servicio LAN.Actualización de Software	Cambio
Redes y Conectividad	Radicar un cambio. servicio WLAN.Actualización de Software	Cambio
Seguridad informatica	Radicar un cambio.SIEM	Cambio
Seguridad informatica	Radicar un cambio.Sandbox	Cambio
Seguridad informatica	Radicar un cambio.Firewall de aplicaciones Web - WAF	Cambio
Seguridad informatica	Radicar un cambio.Firewall	Cambio
Soporte Microinformatica	Radicar un cambio.Impresión	Cambio
Telefonía IP	Radicar un cambio.Infraestructura de telefonia	Cambio

Tabla 8 Categorías Cambios

- **Actualización Matriz de Escalamiento**

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

Fecha de envío matriz	Novedades reportadas
17/03/2025	Se actualiza nombre de especialista de aplicaciones .Net
17/03/2025	Se realiza actualización del nuevo soporte de Mocoa Robinson Lasso
28/03/2025	Se realiza actualización del nuevo soporte de piso 22 sede central Yerik Stevens Castro Grosso

Tabla 9 Novedad Matriz de Escalamiento

2.1.2.5. Práctica de Problemas

Dar a conocer las actividades de la Práctica de Problemas correspondientes al periodo del 1 al 31 de marzo 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. Durante el mes de marzo se creó un caso tipo problema por error en la tipificación durante el registro del caso.

2.1.2.6. Práctica de Incidentes

Dar a conocer las actividades de la Práctica de Incidentes correspondientes al periodo del 1 al 31 de marzo de 2025. Este apartado contiene información relevante sobre los incidentes generados en el periodo de medición, las actividades realizadas y novedades presentadas. En total se registraron 2659 casos tipo incidente quedando en los siguientes estados:

Estado	Cantidad
Cerrado	2417
Solucionado	158
Suspendido	50
Anulado	20
Registrar	3
Reabierto	3
En proceso	2
Total general	2653

Tabla 10 Listados Incidentes

Los casos anulados corresponden a 20 casos que fueron creados por la herramienta de gestión mediante la función case Creator, estos son casos generados por reglas ya definidas que generaron novedad en el momento de la asignación. Dicha novedad fue escalada al administrador de herramientas para su revisión.

- A cierre del mes de marzo, quedaron 50 casos en estado suspendido de los cuales 35 tickets quedaron asignados al equipo NOC, 8 a Telefonía IP, 3 a Especialistas IBM, 2 al equipo de soporte en sitio, 1 a mesa de servicios y 1 a nube privada.

De los casos generados como incidentes, a continuación, se relaciona el top 10 de las categorías con mayor novedad:

Categorización	Cantidad
Reportar una falla.Alarma Zabbix.Router	496
Reportar una falla.Alarma Zabbix.FortiGate	419
Reportar una falla.Alarma Zabbix.Starlink	403
Reportar una falla.Falla impresora.Zabbix	244
Reportar una falla.Alarma Zabbix.Impresora	120
Reportar una falla.Alarma Zabbix.AP	116
Reportar una falla.Alarma Zabbix.Servidor Windows	104
Reportar una falla.Falla impresora.No imprime	86
Reportar una falla.Alarma Zabbix.Switch	83
Reportar una falla.Gestor Documental.Falla Funcional	55

Tabla 11 Top 10 Categorías Incidentes

- Con relación a las novedades por alarma Zabbix, estas corresponden a las alarmas generadas desde la herramienta de monitoreo las cuales son gestionadas por los equipos correspondientes y según CI afectado, algunos de los router e impresoras son alarmados por apagado de los equipos por parte de los usuarios una vez culminan su jornada. También se envió notificación informando la importancia de no apagar los equipos. Los demás casos son gestionados por el proveedor de telecomunicaciones.
- Las novedades por categoría “Reportar una falla. Falla impresora.No imprime” son debido a casos que se generan por algunas sedes en las que los funcionarios apagan las impresoras

al finalizar labores, teniendo en cuenta esto, se solicitó el ajuste en Zabbix para que el monitoreo se realice en horario hábil entre las 8 y 4 pm. Adicional, se ha evidenciado que varias de estas alarmas son por novedades con la conectividad a internet, fallas del fluido eléctrico, cumplimiento con la cuota de impresión o novedades con la conexión las cuales son gestionados por el equipo de soporte en sitio en el momento en el que se presenta la novedad.

- Con relación a la categoría “Reportar una falla.Gestor Documental.Falla Funcional” son debido a la lentitud en el aplicativo por un alto impacto y consumo de transacciones.

De los incidentes generados, se registraron 4 incidentes mayores los cuales se muestran a continuación:

Ticket Arada	SERVICIO AFECTADO	NOVEDAD	CAUSA RAÍZ	ESTADO ARANDA	FECHA INICIO	FECHA FIN
IM-85714	**Telefonía**	Falla al llamar a la mesa de ayuda (601) 5185830 ext 1080	Falla masiva en el entorno de Microsoft Teams	Cerrado	3/03/2025	3/03/2025
IM-85835	**Internet**	Falla Canal Principal de Internet	Corte de Fibra en la caja de empalme	Cerrado	3/03/2025	4/03/2025
IM-95972	**Internet**	Sin Internet Zona Occidental	Ventana de mantenimiento de emergencia por parte del proveedor	Cerrado	30/03/2025	30/03/2025
IM-96056	**Scanner**	No llega documento escaneado al correo	Contraseña buzón Relay	Cerrado	31/03/2025	31/03/2025

Tabla 12 Incidentes Mayores Registrados

- Se realizó seguimiento a incidentes en backlog, enviando correos a los especialistas para la documentación y cierre de tickets pendientes de gestión. Adicional, se realizó contacto mediante Teams solicitando celeridad en la gestión y cierre de casos.
- Desde la gestión ITIL se realizan auditorias de casos en los que se ha evidenciado oportunidades de mejora, las cuales son compartidas mediante correo a los especialistas a quienes se les realiza retroalimentación vía Teams, con base a las novedades encontradas en cada ticket.

En el proceso de actualización de la Guía Operacional de la Práctica de Incidentes, 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 Marzo
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=2608**/2653*100 **EF= 98,3%**
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= 3**/2653*100 **RRP= 0,11%**

Tabla 13 KPI Práctica de Incidentes

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

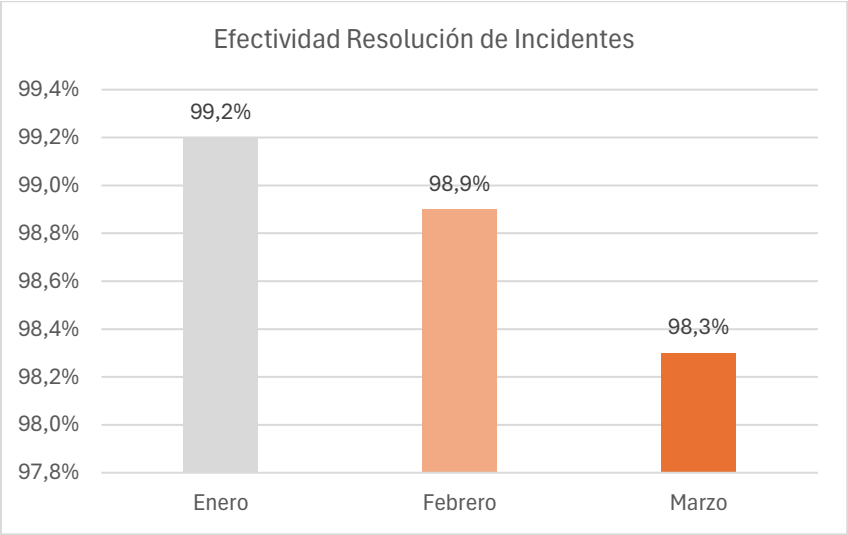


Ilustración 3 KPI Efectividad de Resolución de Incidentes de Servicio

En marzo se evidenciaron 45 casos que no cumplieron el ANS, de estos casos que presentan incumplimiento, se validaron con cada responsable y se realizó el feedback correspondiente, varios de estos se debieron a error en categorización.

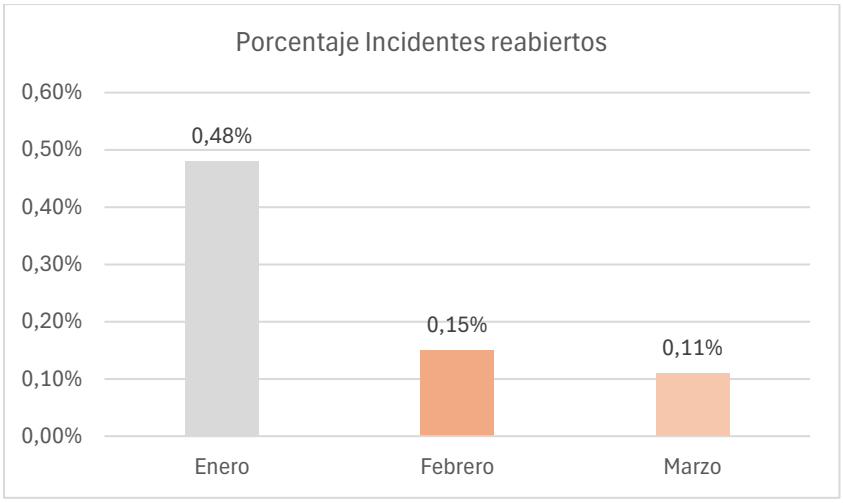


Ilustración 4 KPI Incidentes de Reabiertos en el periodo

En cuanto a los incidentes reabiertos, en marzo se presentaron 3 reaperturas en el equipo NOC, al validar, estos corresponden a alarmas que aun aparecían en Zabbix, pero al validar en sede, el servicio estaba operativo. A continuación, se relaciona mayor detalle:

Caso	Descripción de la solicitud	Grupo responsable	Causa	Atención al caso
IM-77475	Falla Servicio Internet Dedicado en Mariquita //// CAV3000077611	NOC	Caso reabierto dado que la alarma se había solventado, pero horas después se volvió a presentar, motivo por el cual se dio manejo con el mismo caso	El caso continúa en gestión por parte del proveedor de telecomunicaciones, escalado con caso 22878080

Caso	Descripción de la solicitud	Grupo responsable	Causa	Atención al caso
IM-96002	Falla Servicio Internet Dedicado en Ubaté //// CAV3000077724	NOC	Caso reabierto dado la alarma se había solventado, pero horas después se volvió a presentar, motivo por el cual se dio manejo con el mismo caso	Se procede a cerrar el caso ya que el alertamiento generado en la herramienta Zabbix está en estado solucionado, adicional a ello se validó soporte en sitio indicando que el servicio se alertó debido a una falla momentánea de servicio de energía pero que en estos momentos el servicio se encuentra operativo.
IM-94689	Falla Servicio Internet Dedicado en San José del Guaviare //// ID00082715	NOC	Caso reabierto dado la alarma se había solventado, pero horas después se volvió a presentar, motivo por el cual se dio manejo con el mismo caso	El caso continúa en gestión por parte del proveedor de telecomunicaciones, escalado con caso 22769275

Tabla 14 Causas Reaperturas

2.1.2.7. Práctica de Requerimientos

Dar a conocer las actividades de la Práctica de Requerimientos correspondientes al periodo del 1 al 31 de marzo 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 5282 casos tipo requerimiento quedando en los siguientes estados:

Estado	Cantidad
Cerrado	4886
Solucionado	297
Suspendido	87
En proceso	12
Total General	**5282**

Tabla 15 Causas Reaperturas

- No se presentaron casos en estado anulado en el periodo.

De los casos generados como requerimientos, a continuación, se relaciona el top 10 de las categorías con mayor solicitud:

Categoría	Cantidad
Asesoría - Consulta	1577
Aumento de cuota	462
Solicitud Papel	365
Instalación - Configuración	345
Configuración	259
Creación de usuario	244
Asignar Radicado TYS	143
Cambiar contraseña	140
Asignación - Modificación Roles	122
Préstamo	104

Tabla 16 Top 10 Categorías Requerimientos

- Se realizó seguimiento a requerimientos en backlog, enviando correos a los especialistas para la documentación y cierre de tickets pendientes.
- Desde la Práctica de ITIL se realizan auditorias de casos en los que se evidencian oportunidades de mejora, compartidas por correo a los especialistas a quienes se les hace retroalimentación, con base en las novedades encontradas en cada ticket.
- Se realizó capacitación de refuerzo Practica de Requerimientos y seguimiento de casos reabiertos a grupo de Soporte en Sitio Territorial.

- Se realizó el seguimiento de los requerimientos reabiertos por los usuarios, por lo tanto, para marzo se reportó 6 solicitudes de reapertura y actualmente se encuentra cerrada. A continuación, se relaciona el estado del caso por requerimiento y grupo responsable:

Requerimiento	Descripción de la Solicitud	Grupo Responsable	Causa	Atención al Caso
RF-85700	Radicar una solicitud.Gestor documental.Asignacion - Modificacion Roles	Especialistas_IBM	El usuario solicitar apoyo para hacer cambios en el gestor documental, así como la creación del grupo de riesgos laborales y la unificación de PIVC con RCC	Se documenta una solución de otro caso por parte de los especialista, por lo tanto se reabre para la corrección de la documentación.
RF-85729	Radicar una solicitud.Solicitud informacion.Asesoria - Consulta	Responsable_Mesa_De_Servicio	El usario indica que registro el RF-84007 para verificar superfil que estan llegando radicados de otras territoriales,lo cual el ultimo caso registrado, se documenta como solucionado porque se encuentra gestionando con otro numero del caso y el usuario no esta conforme con la solución.	Se verifica por parte del espcialista del caso, se le indica el caso RF-84007 se encuentra realizando la validación de los perfiles del Gestor con la Supervisión del contrato.
RF-85906	Radicar una solicitud.Gestor documental.Depuración Bandeja	Especialistas_IBM	Usuario solicita eliminar unos radicados del Gestor Documental, lo cual se realiza pero le siguen apareciendo en la aplicación, por lo tanto se procede a reabir el caso para su solución.	Se verifica nuevamente y se eliminan los radicados solicitados por parte del Usuario y se procede al cierre de la solicitud.
RF-86728	Radicar una solicitud.Servidor Backups.Crear Backups	Especialista Nube Privada	Solicito un Backup RUTEC, el cual se realizo y el funcionario indico en la encuesta de satisfacción que no estaba de acuerdo con la solución.	Por parte del especialista se vuelve a documentar por medio correo electronico la solución del caso y no se recibio mas comentarios por parte del usuario.
RF-94744	Radicar una solicitud.Correo Electronico.Configuracion	Responsable_Soporte_Bogota	Se solicito soporte de inicio de sesión de teams pero al momento documentar la espera del usuario el soporte lo registro como solucionado.	Al verificar el soporte en sitio por error en el estado reabre el caso y procede a documentar la Gestión realizada.
RF-94926	Radicar una solicitud.VPN cliente.Modificacion VPN	SOC	Se solicita modificar la politica ID 242, la cual se realiza el proceso solo para el trafico de Latinoamérica y Estados unidos hacia el FortiADC por el servicio DNS.	Se verifica el caso, el cual fue reabierto por error del especialista de Ciberseguridad.

Tabla 17 Casos reabiertos

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

Nombre	Descripción / Fórmula	Meta	Periodicidad	Resultado del Periodo
Porcentaje de efectividad en resolución de Requerimientos de servicio.	**EF=(RFS/RFR) *100** **EF:** Efectividad en solución de Requerimientos. **RFS:** Requerimientos solucionados que cumplen el ANS en el período. **RFR:** Requerimientos registradas en el período.	80%	Mensual	**EF=** 5274/5282*100 **EF= 99.85%**
Porcentaje de Requerimientos Reabiertos en el Periodo	**RRP:** Porcentaje de casos Reabiertos en el periodo. **RFR:** Requerimientos Reabiertos en el período. **RFS:** Requerimientos solucionadas en el período.	<2%	Mensual	**RRP=** 6/5183*100 **RRP= 0.116%**

Tabla 18 Detalle de KIP Practica de Requerimientos

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

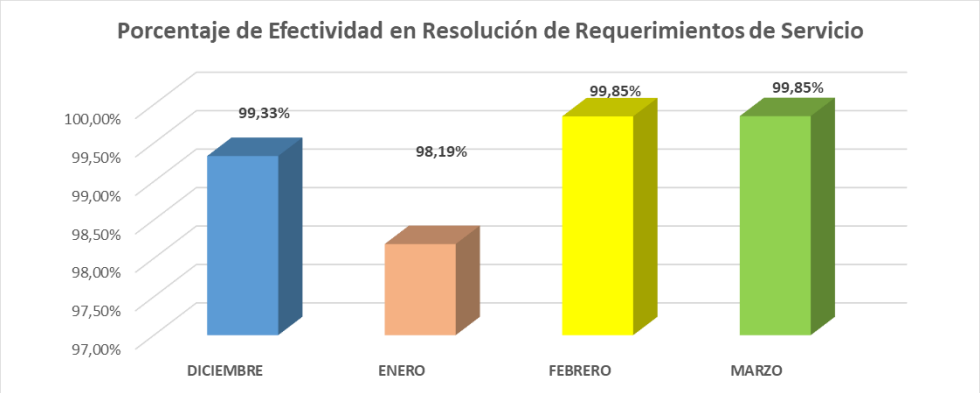


Ilustración 5 KPI Efectividad de Resolución de Requerimientos de Servicio

Durante el periodo, se evidencia el cumplimiento del 99.85% en efectividad de la solución de los requerimientos, los cuales se verifica de 5282 casos registrados en los diferentes canales oficinales de la Mesa de Servicio fueron solucionados 5274 casos.

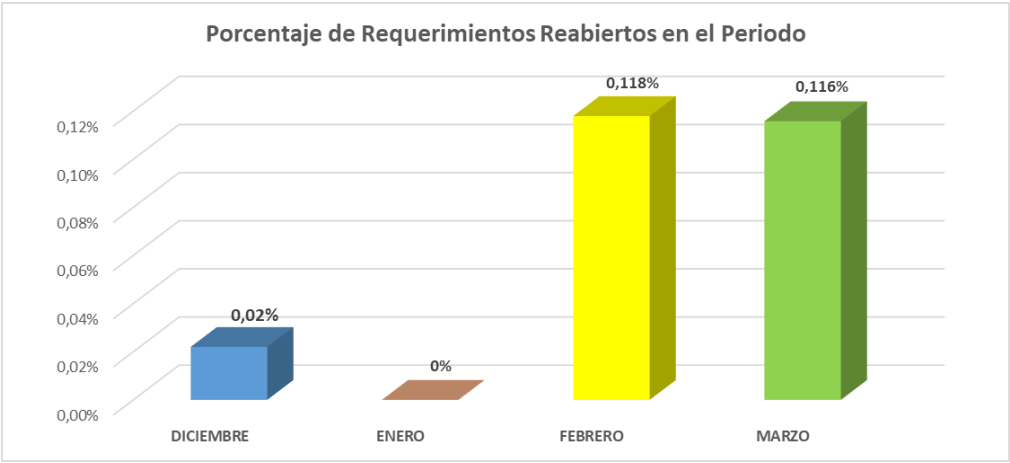


Ilustración 6 KPI Requerimientos de Reabiertos en el periodo

Durante el periodo, se realizó el seguimiento de los requerimientos reabiertos por los usuarios, se ha evidenciado durante los últimos meses una disminución de reaperturas, lo cual para este mes se presentaron 6 casos reabiertos (3 casos fueron reabiertos porque los usuarios no están satisfechos con las soluciones brindadas por la Mesa de Servicios y sus especialistas) y los restantes fueron por errores de documentación o registro del estado por parte del grupo resolutor del caso. Así mismo, se retroalimentará a los especialistas sobre el proceso de atención de casos reabiertos y la correcta documentación de los casos.

2.1.2.8. Práctica de Eventos

Para el mes de marzo, 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 2079 tickets escalados mediante la herramienta de gestión de los cuales 1270 alarmas fueron gestionadas por el NOC, los casos restantes corresponden a tickets 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**

- ✓ Creación de host tipo Starlink
- ✓ Configuración Case Creator SOC
- ✓ Creación MPLS satelital ETB
- ✓ Creación de host tipo SDWAM
- ✓ Actualización de routers de las sedes
- ✓ Ajustes en IP de impresoras y actualización de inventario
- ✓ Creación de mantenimientos programados a sedes
- ✓ Ajustes de campos adicionales en herramienta ITSM de automatización de bitácora NOC
- ✓ Ajuste de reporte de bitácora NOC según necesidades de la operación

Actividades realizadas desde la Gestión de Eventos:

- ✓ Se realizó seguimiento a casos en backlog, asignados al grupo soporte NOC de los cuales, se realiza feedback por correo y vía teams según novedad detectada
- ✓ Se realizó seguimiento de alarmas diarias en Zabbix y se envía reporte diario a la supervisión del contrato del estado y gestión realizada por parte de los responsables.
- ✓ Validación y seguimiento de la automatización correspondiente de la matriz NOC en Aranda
- ✓ Durante el mes de marzo, se identificaron novedades en cuanto al monitoreo de soporte impresión, se realizó el cruce de inventario y con apoyo del líder de herramientas, se realizó ajuste en la herramienta Zabbix

- **Informe Operación NOC**

En lo corrido del mes el equipo CDO gestionó en total **1270** incidentes, los cuales se distribuyen en diversos grupos de CI que detallamos a continuación: Router 424 (33%), servidores Windows 92 (7%), servidores Linux 35 (3%), Access Point 23 (2%), Switches 19 (1%), UPS 1 (0%), Canal Internet 11(1%), incidentes por afectación masiva 3 (1%), Starlink 435 (34%) y Fortigate 230 (18%)

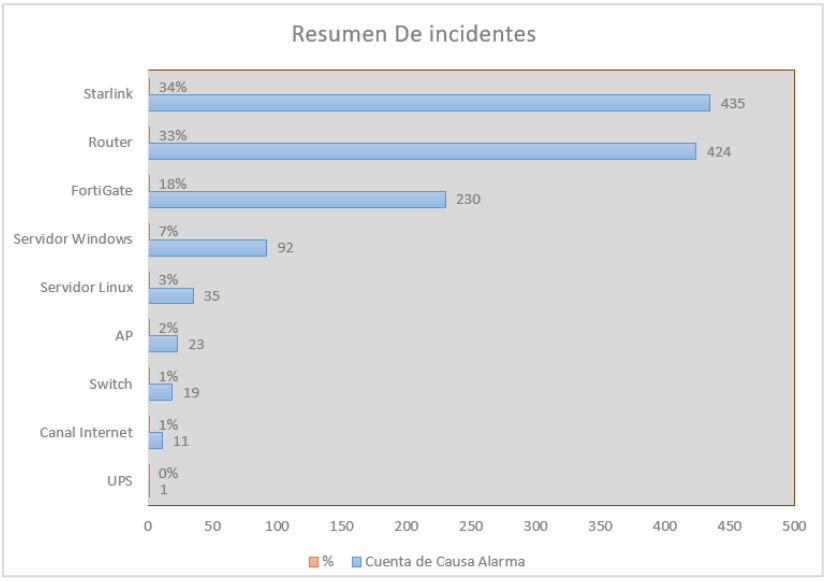


Ilustración 7 Cantidad de Incidentes por Tipo

Access Point

Desde el centro de operaciones NOC durante el mes de marzo se escalaron 23 incidentes relacionados con equipos de red WLAN Access Point en diferentes sedes a nivel nacional.

- Se evidencia que en la sede Choco se presenta mayor recurrencia de incidentes con los dispositivos Wifi; correspondiente al 30% de los eventos de esta categoría generando 23

casos padre de los 116 totales manejados por parte del NOC en cuanto a dispositivos AP refiere.

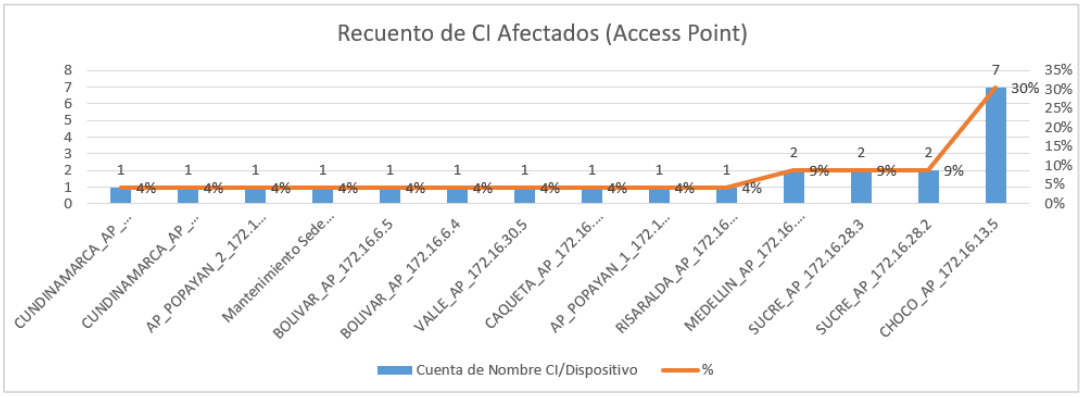


Ilustración 8 Número de eventos de Access Point por CI

- Para el mes de marzo se solucionaron con éxito la totalidad de los 23 casos padre generados en Aranda para gestión de alarmas proactivas por Access Point, es decir el 100% de los casos quedan resueltos.
- Los 93 casos restantes que se generaron por Access Point, fueron relacionados a casos padres como casos hijos y de estos quedan 4 en estado suspendido y relacionados al caso IM-95972 por falla masiva en zona occidental y el cual aún se encuentra en validaciones por parte del proveedor ETB.
- De los 23 alertamientos por Access Point 15(65%) fueron por causa de intermitencia de red, 2 (9%) por dispositivo apagado, 5 (22%) por indisponibilidad y 1 (4%) y por actividad programada.
- Se evidencia que el 65% de las alertas registradas por APs fueron por causa de intermitencia de red, siendo esta la mayor causa de indisponibilidad para la categoría.
- Se evidencia tendencia a presentar mayor número de incidencias en cuanto a dispositivos de red inalámbrica en la sede Manizales; esto debido a que en esa sede se realizaron actividades programadas las cuales generaron alertamientos sobre el CI CALDAS_AP_172.16.8.5.

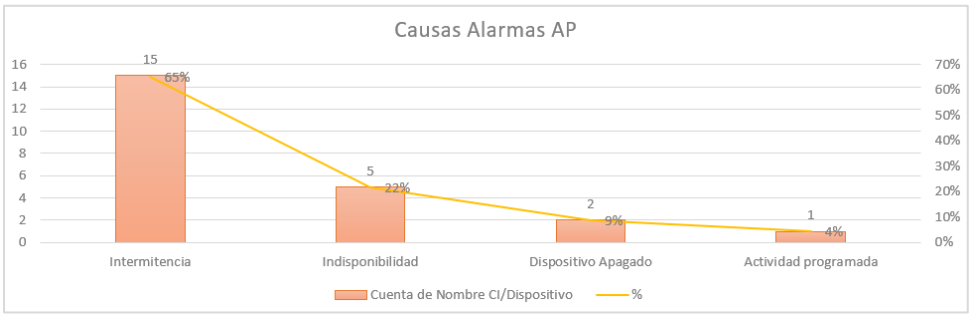


Ilustración 9 Causas de alertamiento Access Point

- Sede de Choco con 7 alertas en total, en las validaciones realizadas se evidencia que corresponde a intermitencias e inactividad en los AP para un total del **30%** del total de los casos generados para esta categoría.

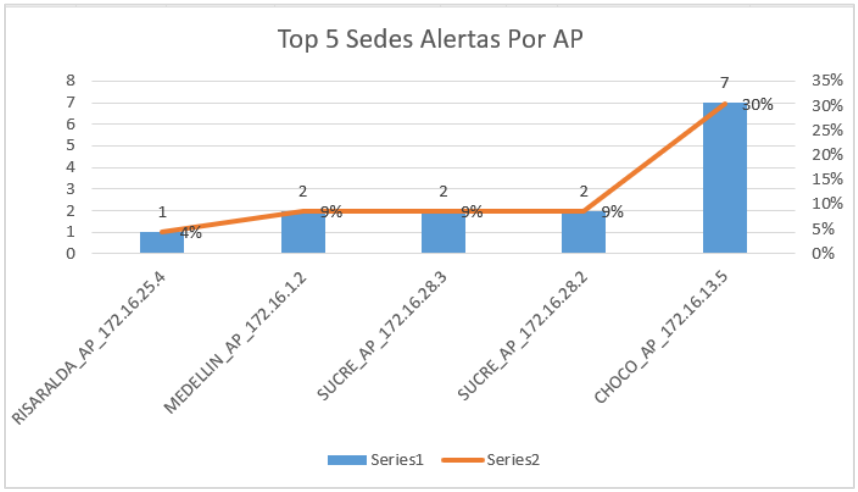


Ilustración 10 TOP 5 sedes alertados por AP

Servidores

Por parte del grupo NOC en el mes de marzo, se evidenciaron un total de 127 alarmas presentadas sobre servidores mostradas a continuación:

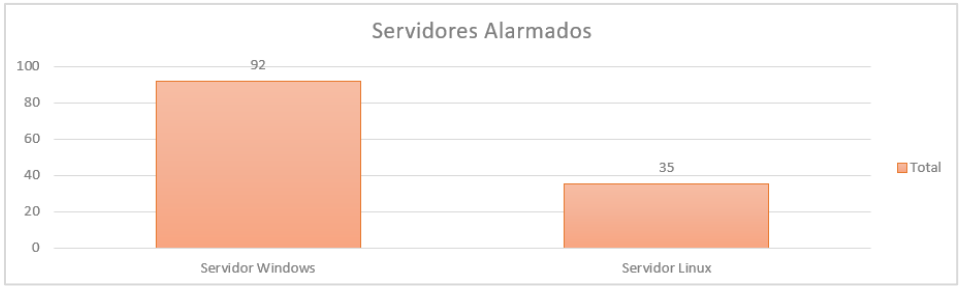


Ilustración 11 Servidores alertados por plataforma

- De acuerdo con las validaciones realizadas por parte del NOC, de las 127 alarmas que se presentaron durante el mes de marzo referentes a servidores, 92 pertenecen a plataformas Windows y 35 a plataformas Linux.

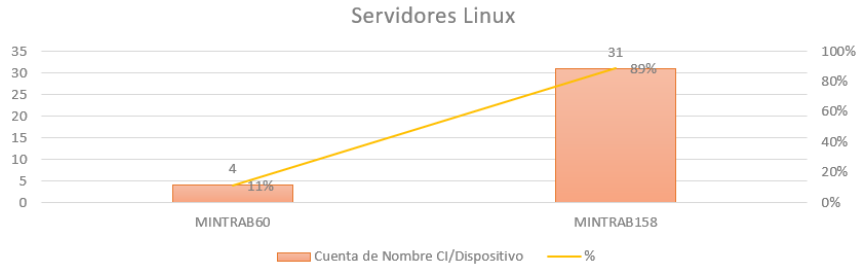


Ilustración 12 Servidores Linux Afectados

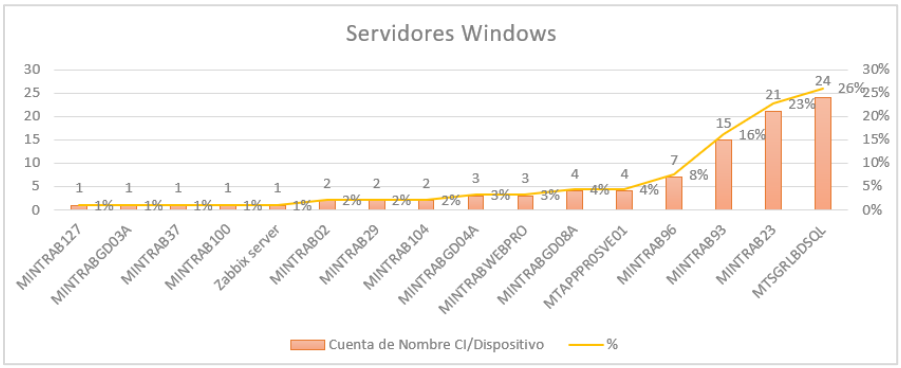


Ilustración 13 Servidores Windows

- De acuerdo con las validaciones realizadas por parte del NOC, de las alertas generadas para plataforma Windows se evidencia un servidor con una cantidad de alarmas recurrentes; siendo el servidor MTSGRLBDSQL el que mayor cantidad de alarmas genero (24), la mayoría de estas alarmas se debieron a elevado uso de recursos e intermitencias y según lo informado por el especialista tuvo que cerrar la sesión de algunos usuarios en estado desconectados y escala el tema al área correspondiente.
- En plataformas Linux el servidor con mayor porcentaje de alertamientos es MINTRAB158 con el 89% del total de alarmas generadas para servidores (31 alarmas de las cuales todas son recurrentes debido a un proceso de backup que se realiza entre las 5am y 6 am) (este servidor es recurrente en informes pasados).
- La mayor cantidad de casos están especialmente relacionados con intermitencia, alto consumo de memoria e indisponibilidad. Esto se debe a un volumen de operaciones significativamente mayor o posibles problemas recurrentes en la infraestructura y baja capacidad de recursos en dichas maquinas.
- Para las 127 alertas presentadas en el mes de marzo el equipo NOC realizó gestión de cada una junto a los especialistas a cargo.
- Para servidores a lo largo del mes de marzo se presentaron incidentes debido a diversas causas de alertamiento dentro de las cuales se listan, intermitencia, alto consumo de memoria, alto consumo de CPU, indisponibilidad y actividad programada:

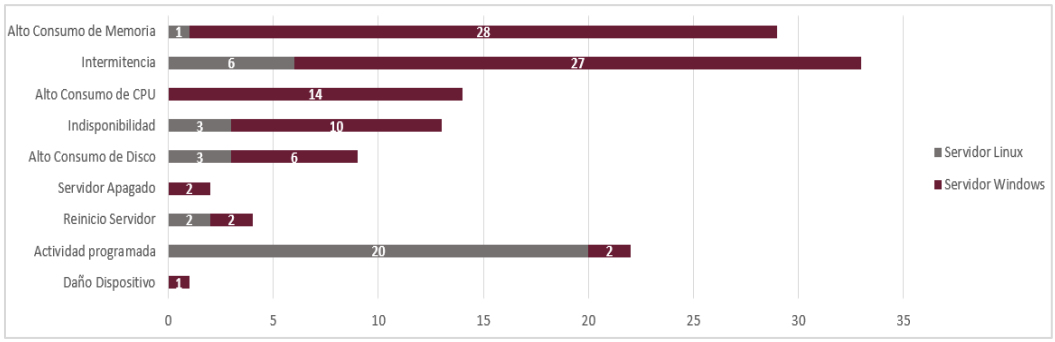


Ilustración 14 Causas de alertamientos (Servidores)

- Entre el TOP4 de los servidores con más alarmas presentadas durante el mes de marzo sobresalen el MTSGRLBDSQL y el MINTRAB23 relacionados a Windows y relacionados a Linux el MINTRAB158 y MINTRAB60.

- Para el mes de marzo el NOC gestiono en conjunto con los especialistas un total de 127 casos referentes a servidores tanto Windows como Linux, se cumplió a cabalidad con el escalamiento de los 127 casos generados en Aranda y de estos listan como solucionados 20, cerrados 105, suspendido 1 y 1 en proceso.
- El caso que se mantiene en estado suspendido corresponde al IM-86194 del servidor MTAPPPR0SVE01 el cual se encuentra en gestión por parte del especialista.
- El siguiente caso se mantiene en proceso, IM-93892 correspondiente al servidor MINTRABWEBPRO el cual está a espera que finalice la actividad programada que se venía realizando. A continuación, se relacionan el porcentaje de tickets por cada estado.

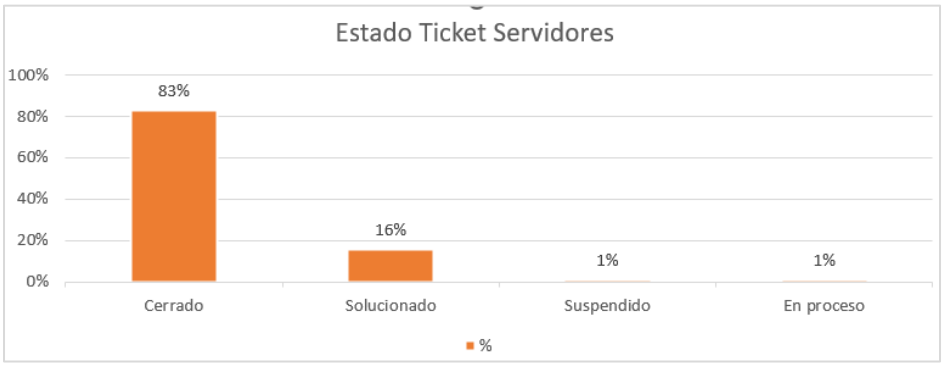


Ilustración 15 Casos solucionados vs casos suspendidos (Servidores)

Switches

Por parte del grupo NOC en el mes de marzo, se evidenciaron un total de 19 alarmas presentadas sobre Switches de las distintas sedes mostradas a continuación:

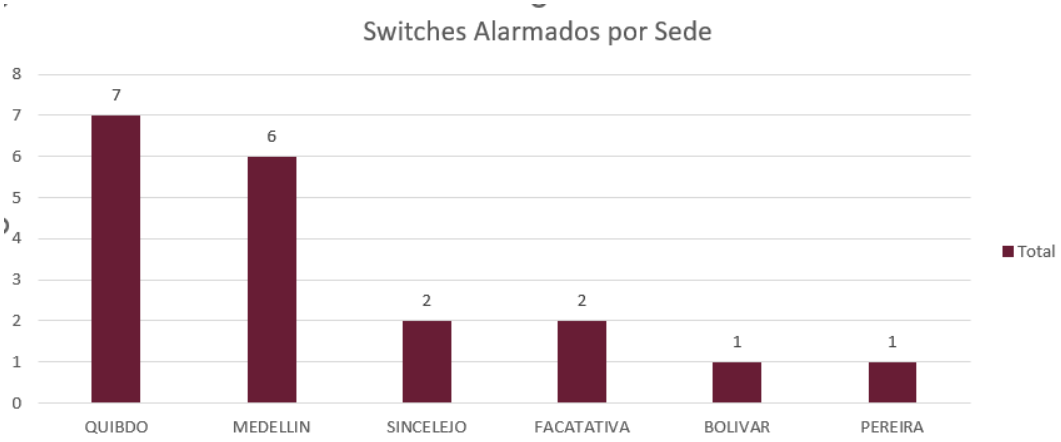


Ilustración 16 Switches alarmados por sede

- Durante el mes de marzo se generaron 19 casos referentes a Switches en la herramienta de monitoreo Zabbix. En total por dispositivos Switch se generaron 83 alarmas, es decir que los 64 casos restantes fueron relacionados y gestionados bajo casos padre, estos distribuidos por diferentes sedes a nivel nacional.

- La sede Quibdó presento la mayor cantidad de casos, especialmente relacionados con problemas de energía comercial en la zona.

- 9 de los casos para el mes de marzo referidas a Switch con un 47%, son relacionados con temas de intermitencia, mientras que los demás se debieron a dispositivo apagado, indisponibilidad y fallas de energía.
- Con base a la información registrada se solucionó en totalidad los casos generados por incidentes con dispositivos de red Switch.

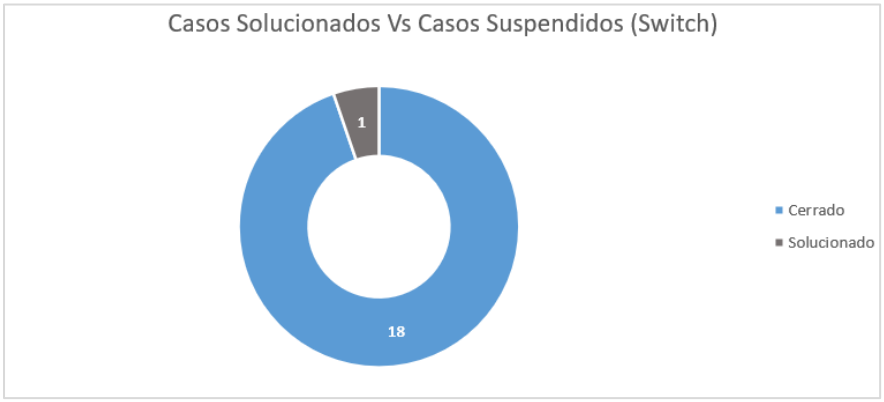


Ilustración 17 Casos solucionados vs suspendidos (Switch)

- Se evidencia que la mayor recurrencia de alertamiento es debido a intermitencia de red (9 casos) con el 47% de los incidentes generados a lo largo del mes de marzo.

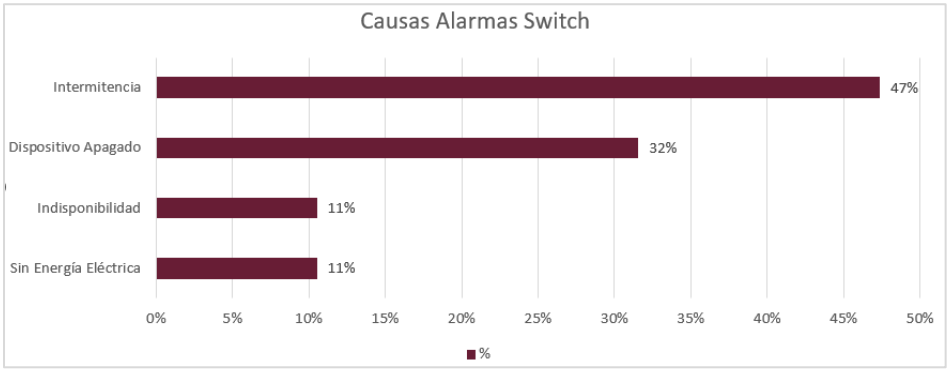


Ilustración 18 Causas de incidentes (Switches)

Routers

Por parte del grupo NOC en el mes de marzo, se evidenciaron un total de 424 alarmas presentadas sobre Routers de las distintas sedes, se muestran a continuación el top 10 de eventos. Donde se observa que las sedes que mayor cantidad de eventos generaron fueron Ubaté y Puerto Gaitán.

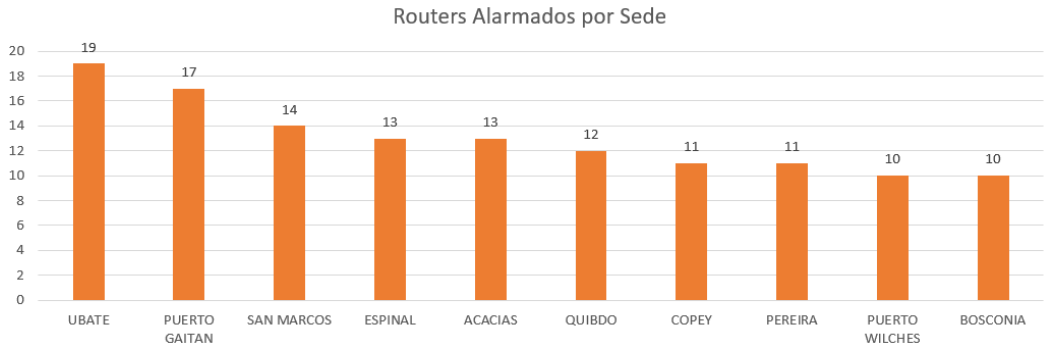


Ilustración 19 TOP 10 Routers alarmados por sede

- Se listan 8 diferentes causas de incidentes para Routers: intermitencia, sin energía eléctrica, indisponibilidad, dispositivo apagado, falla en red de proveedor, actividad programada, reinicio servidor, corte de fibra.

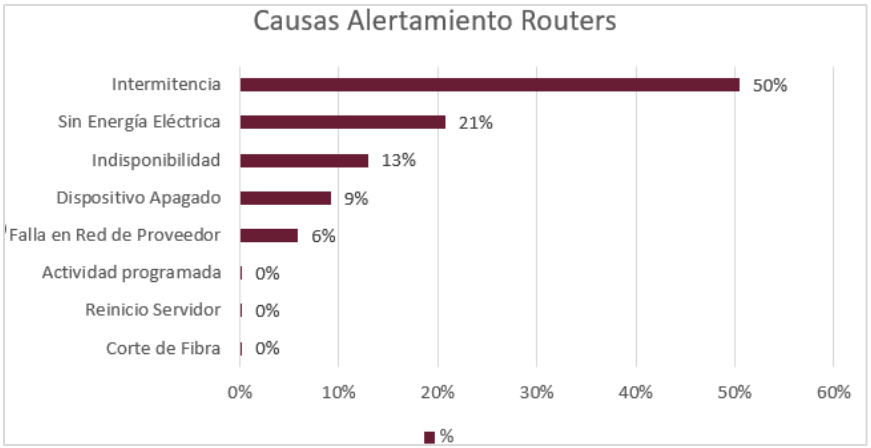


Ilustración 20 Causas de alertamiento (Routers)

- Se evidencia que la mayor causa por la que se evidencian alarmas es por intermitencia que corresponde al 50% del total de los casos.

Starlink

En lo corrido del año anterior y el presente 2025 se han instalado servicios de internet satelital mediante antenas Starlink en sedes donde la cobertura del proveedor de red es limitada con el fin de funcionar como un respaldo.

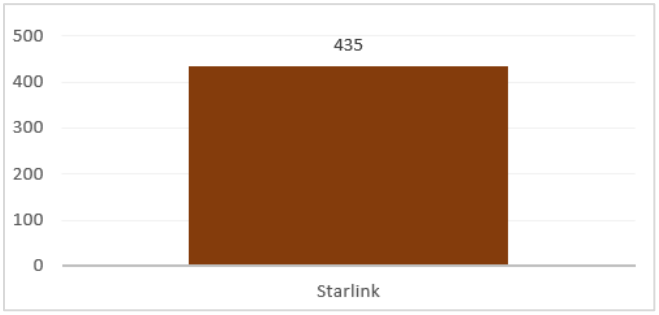


Ilustración 21 Total Alarmas Starlink

- Para el mes de marzo se generaron 435 alarmas correspondientes a servicios de Starlink (internet satelital) afectando las siguientes sedes:

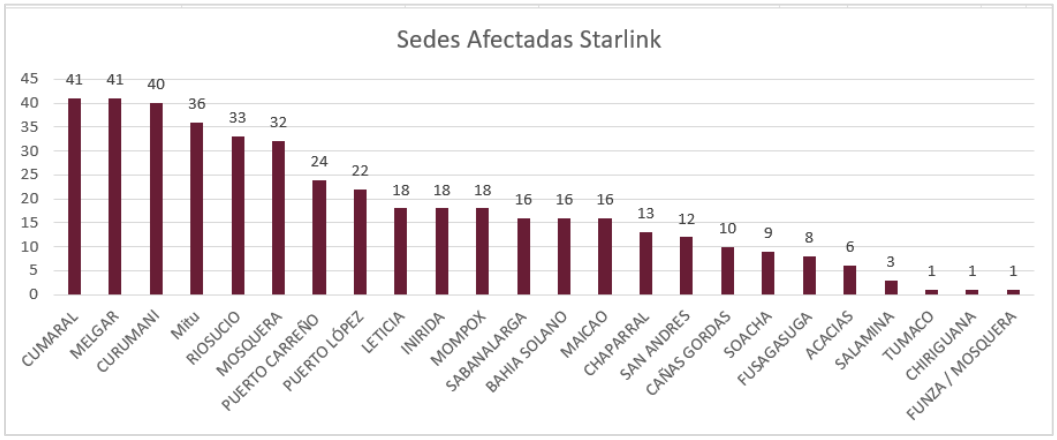


Ilustración 22 Alertamientos por sede Starlink

- Se evidencia mayor recurrencia de caída del servicio de internet satelital en sede Cumaral y Melgar, estas sedes presentan problemas con intermitencias y constantes fallas de energía por temas climáticos y el servicio en la zona es deficiente.
- Para incidentes con antenas starlink se realizan validaciones de primer nivel con equipo de soporte en sitio, una vez realizadas las validaciones se adjunta al ticket las evidencias mediante el servicio “Redes y Conectividad” y se escala al equipo de redes quienes notifican la novedad al equipo responsable APICOM.
- Durante el mes de marzo se pudo observar que la falla en dichos puntos con este dispositivo Starlink se debió a efectos climáticos y por energía eléctrica, lo que ocasionó constantes caídas en este servicio.
- 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 pueden atribuir a intermitencias causadas por malas condiciones climáticas que del mismo modo afectan el servicio de energía.
- En otros casos en que se presentaron alarmas con el servicio de Starlink se pudo indagar que fueron por causa de energía eléctrica ya que los funcionarios apagan los dispositivos por prevención a picos altos en la energía. A continuación, se relacionan las causas que generaron alarmas en las starlink.

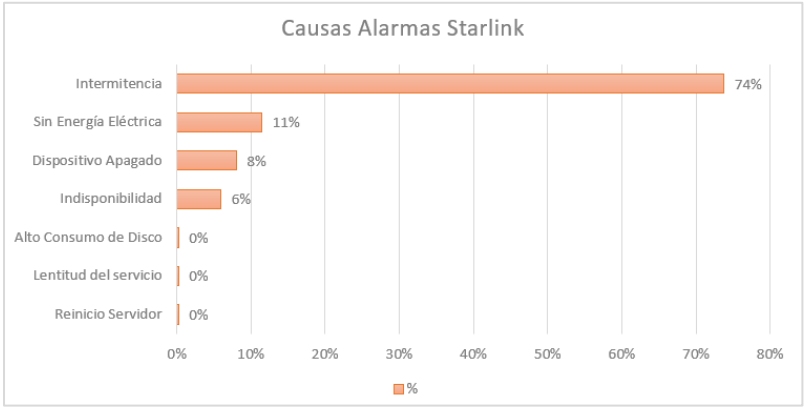


Ilustración 23 Causas de incidente Dispositivos Starlink

SD-WAN

Esta sección detalla los incidentes que el NOC atendió para la gestión proactiva de SD-WAN en el mes de marzo.

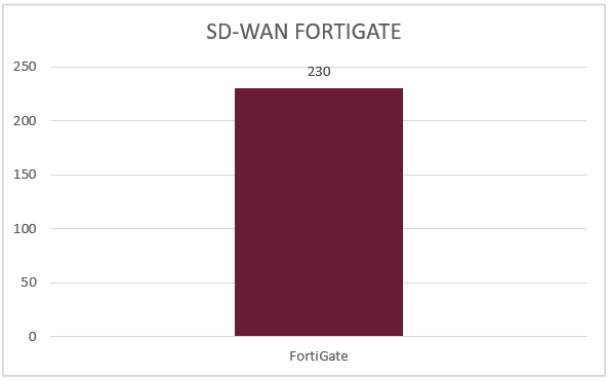


Ilustración 24 SD WAN fortigate

- Para el mes de marzo se generaron 230 alarmas correspondientes a servicios de SD WAN fortigate
- La mayor causa de las alarmas generadas durante el mes de marzo por SD-WAN fueron por intermitencias que no superan en su mayoría los 15 minutos y estas se les atribuyen a fallas en el servicio por temas climáticos.
- La segunda causa de las alarmas por SD-WAN según lo registrado fueron por dispositivo apagado ya que los funcionarios apagan los dispositivos por prevención en horario no hábil.
- Por último, la tercera causa de los alertamientos por SD-WAN fueron por falla en el servicio de energía por temas climáticos en las distintas zonas, confirmadas por los soportes en sitio.

Revisión de incidentes con proveedor para el mes de marzo.

Las siguientes sedes presentaron novedades en la herramienta de monitoreo.

- Se generaron para el mes de marzo 47 tickets con proveedor, de los cuales 40 fueron solucionados, como resultado el 85% de los casos gestionados y en estado solucionado.
- Durante el mes de marzo se presentaron 3 incidentes masivos debido a fallas de red y escaladas con proveedor de los cuales todos ya están solucionados.
- De los 47 casos escalados a proveedor aún quedan 7 en validación y a espera que ETB de solución y el reporte final para dar cierre en Aranda. Estos continúan en seguimiento diario.

Causas de fallas escaladas con proveedor.

- Se evidencian las causas que falla de red con proveedor, dentro de las cuales predomina falla de red debido a infraestructura del mismo proveedor.
- Durante el mes de marzo se reportan con proveedor 47 incidentes referentes a fallas en red de proveedor que denotan afectación en diferentes sedes a nivel nacional.
- Se evidencian 26 incidentes provocados por falla en red del proveedor prolongadas, dichos incidentes generan indisponibilidades de manera masiva al servicio en mayor o menor impacto.

Relación de fallas masivas

Cada afectación masiva es escalada al proveedor de servicio, los números de casos generados con proveedor se anexan a los casos generados en Aranda realizando seguimiento diario según el reporte realizado:

- **Falla Masiva Zona Occidente País - IM-95972 (30/03/2025 8:11):** Se procede a cerrar el caso ya que los alertamientos presentados en la herramienta de Zabbix están en estado solventado, adicional a ello se validó con proveedor ETB indicando que el servicio se encuentra operativo, se adjunta evidencias de la operatividad del servicio y cierre del caso de ETB.

Tiempo de indisponibilidad: No especificado.
Sedes afectadas: Zona occidente país

- **Falla Masiva Zona Norte País - IM-85916 (4/03/2025 1:49):** Se procede a cerrar el caso ya que la falla masiva presentada fue solucionada por parte de Proveedor ETB se adjunta correo del proceso que realizo el proveedor de ETB para la solución a dicha falla masiva en el que indican que realizan empalme por parte del área de correctivo de fibra y de este modo queda solucionada la falla.

  Tiempo de indisponibilidad: No especificado.

  Sedes afectadas:

- Router_Cartagena
- Router_Barbosa
- Router_Puerto_Wilches
- Router_Patia
- Router_Los_Patios.

- **Falla Masiva Zona Oriente País - IM- 86710 (5/03/2025 23:15):** Se procede a cerrar el caso ya que los alertamientos presentes en la herramienta de Zabbix están en estado solventado, adicional a ello se validó con Proveedor ETB indicando que los servicios de RInternet están nuevamente operativos y sin intermitencias como lo informo Julio García.

  Tiempo de indisponibilidad: No especificado.

  Sedes afectadas:

- Router_Puerto_Berrio
- RInternet_ETB_Medellin
- RInternet_ETB_Sincelejo
- RInternet_ETB_Monteria
- RInternet_ETB_Apartado.

Casos escalados al proveedor en estado suspendido

- Para el mes de marzo se evidencia 7 casos en Aranda que quedan en estado suspendido y reabierto, con caso a proveedor. Se está a la espera de nuevos avances y en su defecto solución de las fallas reportadas en el menor tiempo posible. Con apoyo del equipo de redes y seguimiento diario realizado por el equipo NOC, se solicita prioridad en la atención de los casos escalados.

- 2 de los 7 casos que quedan aún abiertos y escalados con proveedor, están en Aranda en estado reabierto ya que por error humano se habían cerrado, sin embargo, estos continua en gestión.

Graficas de CPU Zabbix de todo el mes sobre servidores

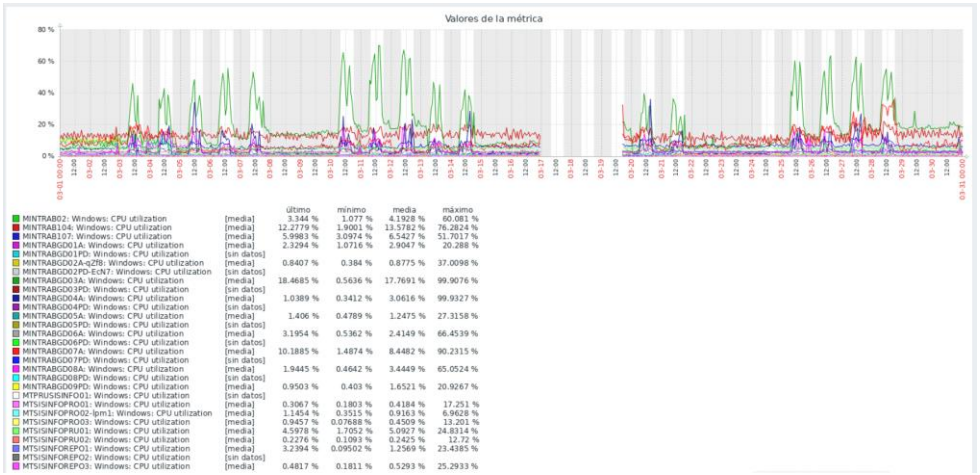


Ilustración 25 Grafica de CPU

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

CPU

1. MINTRABGD03A 17,7691%
2. MINTRAB104 13.5782%
3. MINTRABGD07A 8.4482%
4. MINTRAB107 6.5427%
5. MITSISINFOPRU01 5,0927%

Grafica de MEMORIA Zabbix de todo el mes sobre servidores

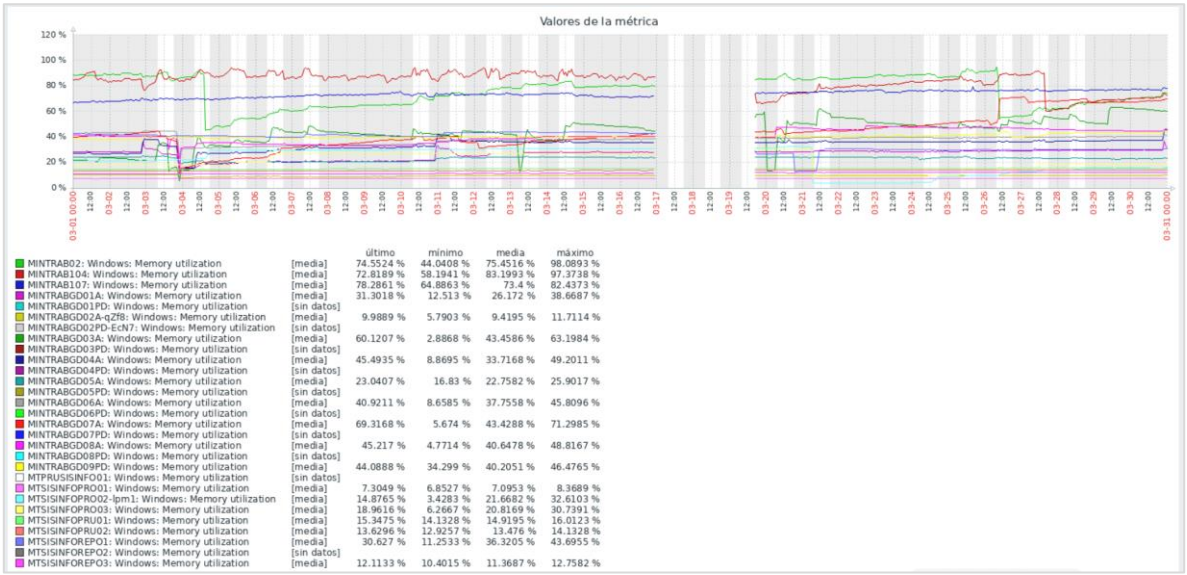


Ilustración 26 Grafica de memoria Zabbix

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

MEMORIA

1. MINTRAB104 83,1993%
2. MINTRAB02 75,4516%
3. MINTRABGD03A 43,4586%
4. MINTRABGD07A 43.4288%
5. MINTRABGD08A 40.6478%

El consumo generado sobre el top 10 de servidores sobre las gráficas de referencia, hacen alusión a los servidores que alojan los servicios de Directorio activo para toda la entidad y los servidores de gestor documental, sumando los consumos de la aplicación SISINFO.

Es importante precisar, que estos consumos son de acuerdo con la transaccionalidad y la operación normal de la entidad, teniendo en cuenta el tipo de servicios que alojan estos servidores, por lo cual los consumos están dentro de la capa de procesamiento asignada para cada servicio y acorde a los licenciamientos adquiridos por parte de la entidad. No se dimensiona crecimiento de estas máquinas debido a que están dentro del comportamiento adecuado, los topes son consumos dentro de la holgura de crecimiento de esta VM

2.1.2.9. Práctica de Disponibilidad

Dentro del marco de la práctica de la disponibilidad del servicio se está trabajando en los procesos y las herramientas que permitan cumplir con los objetivos de disponibilidad definidos en la práctica. A continuación, se muestra la información correspondiente a la disponibilidad de los servicios para el periodo del 1 al 31 de marzo de 2025. Las novedades de dichos dispositivos se gestionan a través del monitoreo del NOC.

Servidores

Cantidad de dispositivos	Disponibilidad consolidada
103	100%

Tabla 19 Consolidado disponibilidad de servidores

No se presentaron alarmas en el umbral de monitoreo a los servidores durante el periodo.

Directorio Activo

Cantidad de dispositivos	Disponibilidad consolidada
3	100%

Tabla 20 Consolidada disponibilidad de Directorio Activo

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

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

Tabla 21 Desagregado de Disponibilidad Directorio Activo

Datacenter Principal

Cantidad de dispositivos	Disponibilidad consolidada
8	100%

Tabla 22 Consolidado disponibilidad de equipos Datacenter principal

Los siguientes equipos se encuentran el Datacenter Principal, los cuales no presentan indisponibilidad del servicio durante el periodo.

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

Tabla 23 Desagregado de Disponibilidad Datacenter Principal

Datacenter Alterno

Cantidad de dispositivos	Disponibilidad consolidada
5	*100%*

Tabla 24 Consolidado disponibilidad de equipos Datacenter alterno

Los siguientes equipos se encuentran el Datacenter alterno, los cuales no presentan indisponibilidad del servicio durante el periodo.

Equipo	Disponibilidad
STM-FG-600F-SDWAN-HUB02	100,00%
STM-SWCORE1-R0015-U37-8360	100,00%
STM-SWCORE2-R0015-U35-8360	100,00%
STM-SWDELL1-R0015-U41-S4148T	100,00%
STM-SWDELL2-R0015-U42-S4148T	100,00%

Tabla 25 Desagregado Disponibilidad de equipos Datacenter alterno

Redes y conectividad

Cantidad de dispositivos	Disponibilidad consolidada
368	*99,96%*

Tabla 26 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%

Tabla 27 Consolidado disponibilidad de equipos de seguridad

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

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

Tabla 28 Disponibilidad de equipos Seguridad de la Información

Telefonía

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

Tabla 29 Consolidado disponibilidad de equipos de telefonía

Antivirus

Cantidad de dispositivos	Disponibilidad consolidada
1	100%

Tabla 30 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 elaboraron y revisaron los planes de disponibilidad de los servicios de Conectividad, LAN y WLAN.
- Se realizo la verificación de la documentación de los resultados de las pruebas de alta disponibilidad WAF de seguridad de la información con el RFC-78613.
- Seguimiento al calendario de pruebas de alta disponibilidad de los servicios.

2.1.2.10. Práctica de Implementación

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

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

Actividades en curso:

- Seguimiento a los resultados de los cambios presentados en el CAB por partes de especialistas durante el periodo.
- Se realiza una socialización a los especialistas de infraestructura y servicios de la operación 17 de marzo sobre los lineamientos de la práctica de implementación y la automatización de la aprobación de las Pruebas Previas y Posteriores en la herramienta de gestión Aranda.
- Durante los días 28 y 31 de marzo se llevó a cabo la socialización de la práctica de implementación en diversas dependencias de la entidad, específicamente dirigida a IVC y la Subdirección de Protección Laboral. Esta actividad tuvo como objetivo principal garantizar

el cumplimiento de los lineamientos establecidos de la Practica de Habilitación de cambio con su integración con la Practica de implementación, con el fin de dar a conocer el formato de evidencias de Pruebas Previas y Posteriores.

- Revisión y seguimiento a los 11 cambios ejecutados durante el periodo con el fin revisar y verificar la correcta documentación de las evidencias de los planes de Pruebas Previas y Posteriores de cada RFC.



Seguimiento de cambios Implementac

2.2. Mesa de Servicios y Soporte en Sitio

A continuación, se relaciona la gestión desarrollada en el transcurso del mes de marzo, 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 marzo, en el Ministerio del trabajo a la MDS ingresaron 320 llamadas de usuarios finales para solicitar servicios de Soporte Tecnológico, a continuación, se discrimina donde se clasificaron según el servicio solicitado:

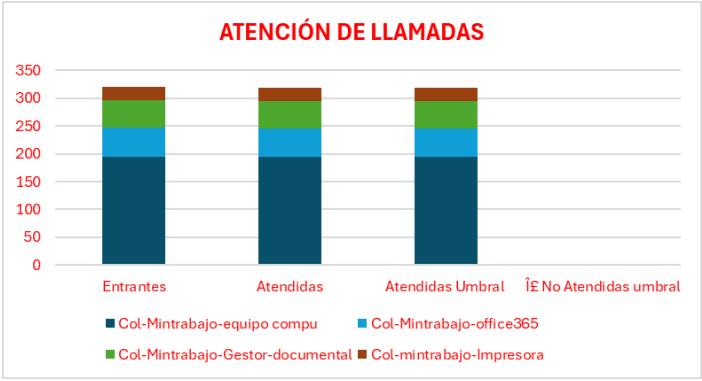


Ilustración 27 Atención de Llamadas

Servicio	Entrantes	Atendidas	Atendidas Umbral	No Atendidas umbral
Col-Mintrabajo-equipo compu	195	195	195	0
Col-Mintrabajo-office365	52	52	52	0
Col-Mintrabajo-Gestor-documental	49	49	49	0
Col-mintrabajo-Impresora	24	24	24	0
TOTAL	320	320	320	0

Tabla 31 Atención de Llamadas

El servicio más solicitado a través de la atención de llamadas es: *Equipo de cómputo* con 195 llamadas entrantes, se atendieron 320 solicitudes.

- **Casos Registrados por Categoría de Servicio**

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

Top 10 de Solicitud de Administración de servidores: Los casos más representativos están asociados a la gestión de marzo solo se tiene 6 categorías: Directorio Activo con 525 casos corresponde al 66,79%, Alarma Zabbix *con* 143 casos, corresponde al 18,19%, Correo Electrónico con 71 casos que corresponden al 9,03%, Servidores 23 casos que corresponden al 2,93%, File Server 22 casos, que corresponden al 2,80%, Servidores Backups 2 casos que corresponden al 0,25% para un total de 877 casos.

ADMINSTRACION DE SERVIDORES	TOTAL
Directorio Activo	525
Alarma Zabbix	143
Correo Electronico	71
Servidores	23
File Server	22
Servidor Backups	2
Total general	**786**

Tabla 32 Top 10 administración de servidores

Top 10 de Redes y Conectividad: para el mes de marzo se tiene 6 categorías más representativos de redes y conectividad que corresponden a las siguientes categorías: Alarmas Zabbix 1523 que corresponden al 97,88%, Internet con 17 casos que corresponden al 1,09%, LAN con 12 casos, corresponde al 0,77%, WLAN con 2 casos, corresponde al 0,13%, servicio LAN con 1 caso, corresponde al 0,06% y Enlace Sedes (Mlps) con 1 caso, corresponde al 0,06%, para un total de 1556 casos.

REDES Y CONECTIVIDAD	TOTAL
Alarma Zabbix	1523
Internet	17
LAN	12
WLAN	2
servicio LAN	1
Enlace Sedes (Mlps)	1
Total general	**1556**

Tabla 33 Top 10 redes y conectividad

Top 10 de Seguridad Informática: durante el mes de marzo, los caso más representativos de seguridad informática que corresponden a las siguientes categorías: Firewall con 32 casos que corresponde al 49,23%, Servicios SOC con 11 caso que corresponde al 16,92%, Seguridad de la Información con 4 casos que corresponde al 6,15%, Servicio SOC con 3 casos que corresponde cada uno al 4.62%, VPN cliente, SIEM, Reportes, Alarma Zabbix, y Soporte Antivirus con 2 casos que corresponde al 3,08%, VPN Site to Site, Manejo inadecuado de datos, Ataques al portal Web, Vulnerabilidades y Ingenieria Social , con 1 caso que corresponde al 1,54% del total de 65 casos.

SEGURIDAD INFORMATICA	TOTAL
Firewall	32
Servicios SOC	11
Seguridad de la Información	4
Servicio SOC	3
VPN cliente	2
SIEM	2
Reportes	2
Alarma Zabbix	2
Soporte Antivirus	2

VPN Site to Site	1
Manejo inadecuado de datos	1
Ataques al portal Web	1
Vulnerabilidades	1
Ingeniería Social	1
Total general	**65**

Tabla 34 Top 10 seguridad informática

Top 10 de Telefonía IP: Durante este periodo se gestionaron 29 casos de Telefonía IP que corresponden a: Softphone con 21 casos corresponde al 72,41%, Servicios con 8 casos corresponde al 27,59%.

TELEFONIA IP	TOTAL
Softphone	21
Servicios	8
Total general	**29**

Tabla 35 Top Telefonía IP

Top 10 de Aplicaciones Especializadas: Para el mes de marzo se tienen los casos más representativos de la gestión de soportes de aplicaciones que corresponden a las siguientes categorías: Gestor Documental con 461 casos que corresponde al 95.45%, Servidor de aplicaciones con 15 casos que corresponden al 3,11%, SICIP con 3 casos que corresponde al 0,62%, Datacap con2 casos que corresponde al 0,21%, SIRITI con 1 casos que corresponden al 0,21% y Sisinfo con 1 casos que corresponden al 0,21%, para un total de 483 casos.

APLICACIONES ESPECIALIZADAS	TOTAL
Gestor Documental	461
Servidor de aplicaciones	15
SICIP	3
Datacap	2
SIRITI	1
Sisinfo	1
Total general	**483**

Tabla 36 Top 10 soporte aplicaciones

Top 10 de Soporte Microinformática: Los casos más representativos de la gestión de **soporte microinformática** que corresponden a las siguientes categorías: Impresora 1246 casos corresponde al 25,63%, Equipo de cómputo con 547 casos corresponden al 11,25%, Ofimática con 514 casos que representa el 10,57%, Falla impresora con 373 que representan el 7,67%, Solicitud información con 353 casos que representan el 7,26%, Correo Electrónico con 337 casos que representan el 6,93%, Antivirus con 239 casos que representan el 4,92%, Software Adicional con 219 casos que representan el 4,51%, Navegadores con 184 casos que representan el 3,79%, Alarma Zabbix con 120 casos que representan el 2,47% un total de casos 4861.

SOPORTE MICROINFROMATICA	TOTAL
Impresora	1246
Equipo de computo	547
Ofimática	514
Falla impresora	373
Solicitud información	353
Correo Electrónico	337
Antivirus	239

Software Adicional	219
Navegadores	184
Alarma Zabbix	120
One Drive	111
Escáner	105
Microsoft Teams	104
Video Beam	94
Televisor - Monitor industrial	89
VPN	69
Aplicaciones Office 365	47
Unidad de CD	44
Teléfono IP	28
Garantía	16
Monitor Pc	13
Mouse - Teclado - Base - Diadema	9
Total general	**4861**

Tabla 37 Top 10 soporte microinformática

- **Análisis de Casos Anulados por Servicio**

Para este periodo se tiene 20 casos anulados de los siguientes servicios:

CASOS ANULADOS	TOTAL
Herramientas de Gestión	19
Redes y Conectividad	1
Total general	**20**

Tabla 38 Casos Anulados por Servicio

Herramientas de Gestión: se tiene19 casos, anulados por duplicidad Monitoreo desde zabbix.
Redes y Conectividad: se tiene 1 caso por duplicidad Monitoreo desde zabbix

- **Análisis de Casos Suspendidos por Servicio**

Para el periodo del mes de marzo, quedaron en estado suspendidos 145 casos de los siguientes servicios:

CASOS SUSPENDIDOS	TOTAL
Soporte Microinformática	49
Redes y Conectividad	45
Administración de servidores	16
Aplicaciones Especializadas	15
Telefonía IP	13
Seguridad informática	6
Herramientas de Gestión	1
Total general	**145**

Tabla 39 Casos Suspendidos por Servicio

Soporte Microinformática: 49 casos suspendidos debido a que se ha solicitado información complementaria a los usuarios por: Cambio Toner 12; con 7 casos las categorías: Solicitud Backup, Asesoría - Consulta y Equipo Periférico, Instalación - Configuración con 6 casos, Configuración con

4 casos; Equipo Portátil con 2 casos, con 1 caso Falla – error, Préstamo, Asignación de equipo (portátil o PC) y Error sincronización.

Redes y Conectividad: 45 casos suspendidos debido a: Alarma de Zabbix en router 43 casos, Internet sin servicio con 1 caso, WLAN con 1 caso**.**

Administración de servidores: 16 casos suspendidos por: Directorio Activo con 11 casos, con 2 casos tenemos: servidores y correo electrónico, con 1 caso tenemos alarmas de zabbix.

Aplicaciones Especializadas: 15 casos suspendidos debido a que se ha solicitado información complementaria a los usuarios: Gestor Documental con 10 casos, con 5 casos de Servidor de Aplicaciones.

Telefonía IP: 13 casos suspendidos de: Softphone 8 y Servicios 5.

Seguridad informática: 6 casos suspendidos debido a que se ha solicitado información complementaria a los usuarios: Permisos de accesos con 2 casos, con 1 caso de están las categorías de Análisis de evento, Verificar conexión VPN, Accesos por fuerza bruta, Reportes Seguridad Informática.

Herramientas de Gestión: 1 caso suspendidos de Creacion/Modificación/Elimacion Funcionalidades Aranda.

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

Incidentes solucionados por la Mesa de Servicios: Para este periodo quedaron 2 incidentes en estado solucionado.

MESA_DE_SERVICIO	TOTAL
Falla Funcional	1
Falla Aplicativo	1
Total general	**2**

Tabla 40 Casos solucionados mesa de servicios

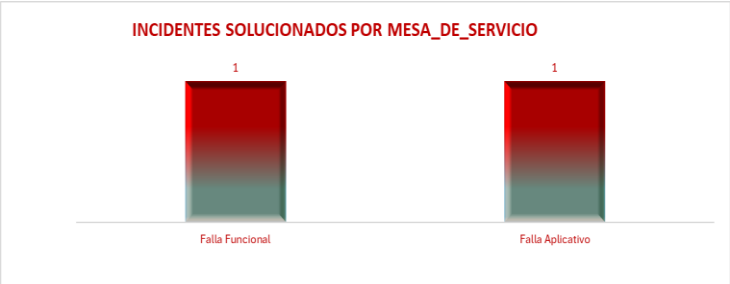


Ilustración 28 Casos solucionados mesa de servicios

Incidentes solucionados por Soporte en sitio: Para este periodo quedaron 9 incidentes en estado solucionado.

SOPORTE_EN _SITIO	TOTAL
Falla - error	2
Falla Word	1
No escanea	1
No enciende	1
No imprime	1
Falla - Error conexión a red	1
Envio y recepción de correos	1

Falla Aplicativo	1
Total general	**9**

Tabla 41 Casos solucionados soporte en sitio

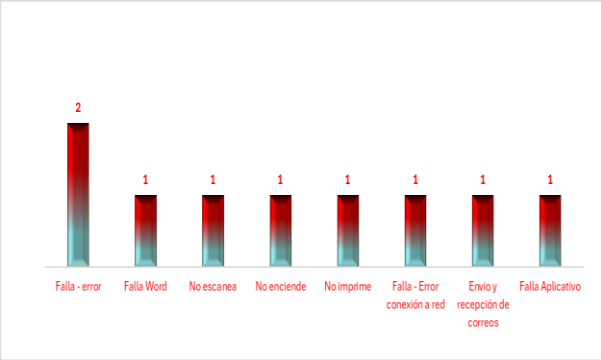


Ilustración 29 Casos solucionados soporte en sitio

Incidentes solucionados por Soporte Territoriales: para el mes de marzo quedaron estado solucionado 15 casos, discriminados de la siguiente manera.

SOPORTE_TERRITORIAL	TOTAL
Zabbix	4
Falla Funcional	2
Envio y recepción de correos	2
Lentitud - Bloqueo	1
No escanea	1
No imprime	1
Falla - error	1
Falla Aplicaciones Office 365	1
Falla - Error conexión a red	1
Falla Cargue pagina web	1
Total general	**15**

Tabla 42 Incidentes solucionados por Soporte Territoriales

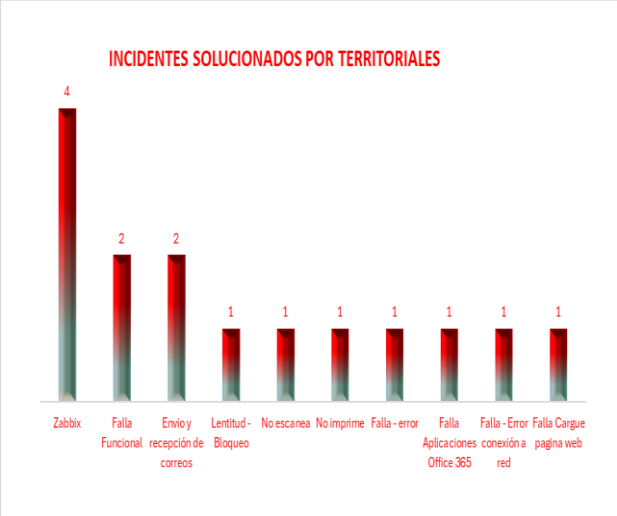


Ilustración 30 Incidentes Solucionados por Soportes Territoriales

Requerimientos solucionados por la Mesa de Servicios: Para el mes de marzo quedaron 43 requerimientos discriminados de la siguiente manera:

REQUERIMIENTOS SOLUCIONADOS MESA_DE_SERVICIOS	TOTAL
Asesoria - Consulta	24
Creacion de usuario	8
Cambiar contraseña	7
Cambio de grupo	2
Depuración Bandeja	1
Modificar usuarios	1
Total general	**43**

Tabla 43 Requerimientos solucionados por Mesa de Servicios

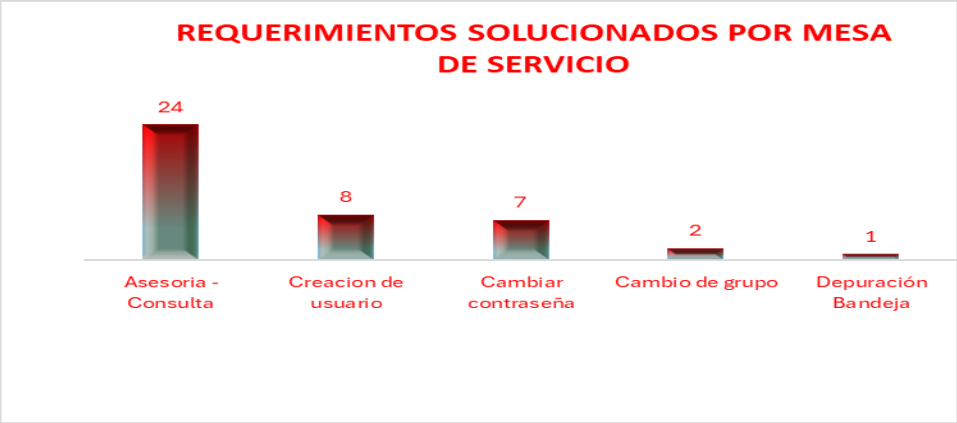


Ilustración 31 Requerimientos Solucionados por la Mesa de Servicios

Requerimientos solucionados por Soporte en sitio Bogotá: en el mes de marzo quedaron 47 requerimientos discriminados de la siguiente manera:

REQUERIMIENTOS SOLUCIONADOS POR SOPORTE EN SITIO	TOTAL
Asesoria - Consulta	17
Instalacion - Configuracion	7
Prestamo	6
Solicitud Papel	4
Asignación de equipo (portátil o PC)	4
Asesoria Excel	3
Configuracion	2
Asesoria PDF	1
Soporte Aplicaciones Office 365	1
Asesoria Word	1
Solicitud instalacion	1
Total general	**47**

Tabla 44 Requerimientos solucionados por Soporte en sitio



Ilustración 32 Requerimientos Solucionados por Soporte en sitio

Requerimientos solucionados por Soportes Territoriales: Para el mes de marzo se solucionaron 111 requerimientos discriminados de la siguiente manera:

REQUERIMIENTOS SOLUCIONADOS POR TERRITORIALES	TOTAL
Asesoria - Consulta	29
Instalacion	13
Configuracion	11
Copia de informacion	10
Solicitud Papel	7
Instalacion - Configuracion	7
Asesoria Consulta	6
Traslado - Movimiento	4
Mantenimiento preventivo	3
Asignación de equipo (portátil o PC)	3
Prestamo	2
Aumento de cuota	2
Conectar a red Mintrabajo	2
Backup	2
Devolución de equipo (portátil o PC)	2
Asesoria Word	2
Instalacion y configuracion VPN	1
Borrado seguro PC	1
Asesoria Excel	1
Solicitud Backup	1
Cambio Toner	1
Solicitud instalacion	1
Total general	**111**

Tabla 45 Requerimientos solucionados por Soportes Territoriales



Ilustración 33 Requerimientos solucionados por Soportes Territoriales

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

Casos Cerrados por la Mesa de Servicios: Se indica el top de 10 de Requerimientos cerrados por la mesa de servicios, para el mes de marzo se cerraron 986 casos, discriminados así: Asesoría – Consulta con 467 casos, Creación de usuario con 233 casos, Cambiar contraseña 132, Cambio de grupo con 45 casos, Inactivar usuario y Habilitar usuario con 23 casos cada uno, Crear usuario con 12 casos, Configuración con 9 casos, Modificar usuarios con 7 casos, Instalación y configuración VPN con 6 casos.

CERRADOS POR LA MESA DE SERVICIOS	TOTAL
Asesoria - Consulta	467
Creacion de usuario	233
Cambiar contraseña	132
Cambio de grupo	45
Inactivar usuario	23
Habilitar usuario	23
Crear usuario	12
Configuracion	9
Modificar usuarios	7
Instalacion y configuracion VPN	6
Asignacion de licencia	6
Falla Funcional	5
Solicitud Backup	2
Permitir acceso	2
Asignacion - Modificacion Roles	2
Falla aplicación	2
Informes y Reportes Asesoria Word	2 2
Envio y recepción de correos	1
Aumento de cuota	1

Falla radicacion	1
Asignar Radicado TYS	1
Agregar a sitios permitidos	1
Falla - error	1
Total general	**986**

Tabla 46 Casos cerrados por la mesa de servicios

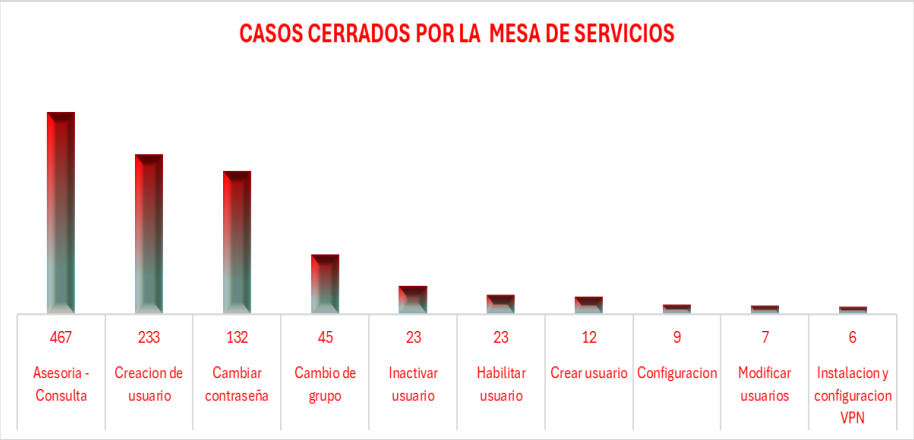


Ilustración 34 Casos cerrados por la mesa de servicios

Casos Cerrados por Soporte en Sitio: Se indica el top 10 de Requerimientos cerrados por soporte en sitio, para el mes de marzo se cerraron 1044 casos discriminados así: Asesoría - Consulta con 312 casos, Solicitud Papel con 104 casos, Instalación - Configuración con 86 casos, Configuración con 68 casos, Préstamo con 62 casos, Falla - error con 40 casos, No imprime con 31 casos, Soporte Aplicaciones Office 365 con 23 casos, Asesoría Word con 22 casos, Asesoría Excel con 21 casos.

CERRADOS POR SOPORTE EN SITIO	TOTAL
Asesoría - Consulta	312
Solicitud Papel	104
Instalación - Configuración	86
Configuración	68
Préstamo	62
Falla - error	40
No imprime	31
Soporte Aplicaciones Office 365	23
Asesoría Word	22
Asesoría Excel	21
Asesoría Consulta	19
Asesoría PDF	19
Instalación y configuración VPN	19
Aumento de cuota	16
Solicitud Backup	15
Asignación de equipo (portátil o PC)	15
Envió y recepción de correos	14
Falla Cargue página web	13
Instalación - Configuración	12

Conectar a red Mintrabajo	12
Devolución de equipo (portátil o PC)	11
Solicitud instalación	11
Cambio Toner	10
Falla aplicación	9
Atasco	8
Borrado seguro Portátil	8
Traslado - Movimiento	7
Copia de información	7
Falla Aplicaciones Office 365	4
No enciende	4
Degradación	4
Falla - Error conexión a red	4
Instalación	4
Backup	3
Conectar a red Invitados	3
Configuración de PST	3
Préstamo Equipo (portátil o PC)	3
Falla Excel	3
Falla Word	2
Falla PDF	2
Daño Físico	2
Falla punto de red	1
Cambiar contraseña	1
Falla- Error	1
Lentitud - Bloqueo	1
Mantenimiento preventivo	1
No escanea	1
Equipo Portátil	1
No conecta	1
Error sincronización	1
Total general	**1044**

Tabla 47 Casos cerrados por soporte en sitio



Ilustración 35 Casos cerrados por Soporte en Sitio

Casos Cerrados por soporte en sitio Territoriales: Se indica el top de 10 de Requerimientos cerrados por soporte en sitio territoriales se cerraron un total de 2173 casos, los requerimientos discriminados a continuación: Asesoría - Consulta 667 casos, Instalación - Configuración con 229 casos, Solicitud Papel con 177 casos, Configuración con 141, Solicitud instalación 111 casos, Asesoría Excel con 70 casos, Asesoría PDF con 58 casos, Asesoría Word con 53 casos, No imprime con 49 casos y Soporte Aplicaciones Office 365 con 44casos.

CASOS CERRADOS POR SOPORTE TERRITORIAL	TOTAL
Asesoria - Consulta	667
Instalacion - Configuracion	229
Solicitud Papel	177
Configuracion	141
Solicitud instalacion	111
Asesoria Excel	70
Asesoria PDF	58
Asesoria Word	53
No imprime	49
Soporte Aplicaciones Office 365	44
Aumento de cuota	42
Falla - Error conexión a red	38
Asesoria Consulta	36
Traslado - Movimiento	31
Prestamo	30
Envio y recepción de correos	28
Atasco	26
Falla - error	26
Conectar a red Mintrabajo	25
Instalacion y configuracion VPN	24
Falla Cargue pagina web	19
Solicitud Backup	18
Cambio Toner	18

Mantenimiento preventivo	16
Copia de informacion	16
Zabbix	13
Instalación - Configuracion	11
Impresora	10
Borrado seguro Portátil	9
Asignación de equipo (portátil o PC)	9
Falla aplicación	8
Asesoria en ZIP	8
No escanea	8
Error sincronizacion	6
Lentitud - Bloqueo	6
Devolución de equipo (portátil o PC)	6
Falla Aplicaciones Office 365	6
Falla de sistema operativo	6
No enciende	5
Borrado seguro PC	5
Backup	5
Falla Aplicativo	4
Bloqueo Navegador	4
Asesoria Power Point	4
Asignar Pin	4
Falla Word	4
Falla Excel	4
Falla General	3
Falla PDF	3
Conectar a red Invitados	2
Falla punto de red	2
Falla- Error	2
Sin servicio	2
Falla error - Producir documento	2
Préstamo Equipo (portátil o PC)	2
No conecta	1
Equipo Escritorio	1
Falla del lector	1
Impresión deficiente	1
No permite ingresar datos	1
Caida	1
Falla al cargar archivos	1
Error de aplicación	1
Solicitud de cambio	1
Configuracion de Switch	1
No navega	1

Implementacion Switch	1
Falla	1
Falla Funcional	1
Habilitar punto de red	1
Revision estado del canal	1
Falla radicacion	1
Instalar - Configurar	1
Total general	**2173**

Tabla 48 Casos cerrados por Territoriales

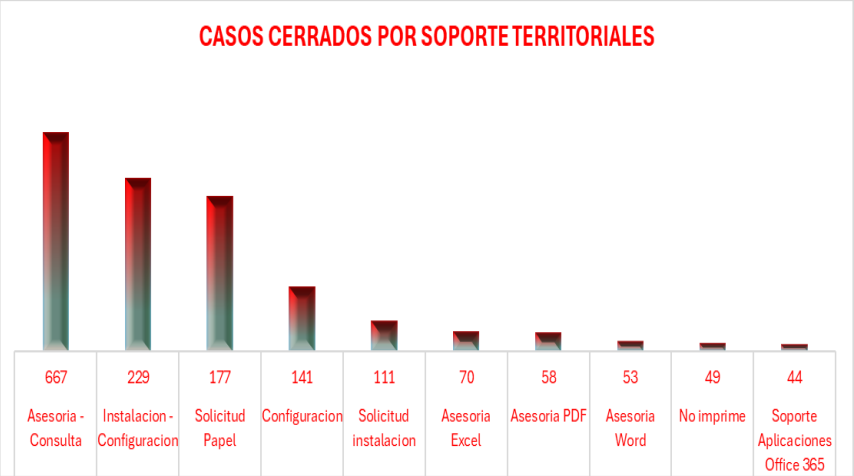


Ilustración 36 Casos cerrados por Territoriales

- **Casos Atendidos a Usuarios VIP**

Duran este periodo se crearon 1126 solicitudes para ser atendidas por soporte en sitio, de estas solicitudes se evidencio 128 casos creados para VIPs todo cumpliendo los ANS establecidos por la entidad, discriminados a continuación por tipo de caso:

TIPO DE CASO_VIPS	CUMPLIMIENTO	TOTAL
Incidentes	17	17
Requerimiento	111	111
Total general	**128**	**128**

Tabla 49 Casos usuarios VIP

Se atendieron 998 solicitudes para el resto de los usuarios discriminados así:

TIPO DE CASO-NO-VIPS	CUMPLIMIENTO	TOTAL
Incidentes	140	141
Requerimientos	858	858
Total general	**998**	**998**

Tabla 50 Casos usuarios Regulares

- **Medio de Ingreso de Casos**

Durante el mes de marzo ingresaron a la mesa de servicio 2544 casos a través de los diferentes medios que se tiene habitados para la atención de solicitudes, como son correo, telefonía, web,

alarma de zabbix, casos creados de forma automática por la herramienta y creación masiva para temas específicos:

MEDIO DE INGRESO DE CASOS	TOTAL
Alarma Zabbix	2079
Telefónico	287
Correo	61
Web	60
Gestión	57
Total general	**2544**

Tabla 51 Medio de ingreso de casos

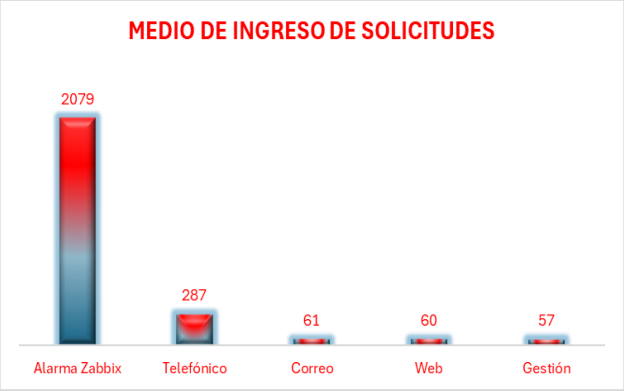


Ilustración 37 Modo de Ingreso de Solicitudes

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

Durante el mes de marzo de 2025, Se continuó realizando las clínicas de llamadas con los agentes de mesa de servicios realizando la retroalimentación en línea de los hallazgos y acciones de mejora para cada una de las situaciones presentadas.

Se modificó la herramienta de gestión para el estado *Solución* creando la razón *' Contacto no efectivo con el usuario'* para controlar los casos en los que se ha buscado contacto con el usuario para solicitar información para atender su requerimiento, se tiene como lineamiento realizar 3 intentos, si no se logra contacto se procede al cierre de caso con la razón establecida. Esta modificación será implementada durante el mes de abril.

Se realizó la estandarización del agente de Aranda versión 9.21 en los equipos dados por la Unión Temporal al Ministerio del Trabajo.

Se realizó la estandarización del agente del Antivirus versión 14.01.43.20 a todo el parque computacional del Ministerio del trabajo

Se realizó actualización de inventario y de plano por cada uno de los pisos de la sede central y calle 32.

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

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

Organización de cables de red de los racks y apoyo en la instalación de antenas starlink requeridas.

Inventario actualizado de los elementos presentes en los cuartos de comunicaciones de las sedes territoriales, que pertenecen al Ministerio.

Visitas a **10** inspecciones donde no se cuenta con personal dedicado para solucionar los casos que se requieren ser atendidos.

De los **2173** casos atendidos se destacan las asesorías -consultas, las configuraciones e instalaciones, el continuo suministro de papel en los equipos multifuncionales y las asesorías en Ofimática, entre otras

Actualización en ZTNA para validar acceso a las URLs y páginas recurrentes que apoyan las labores del Ministerio.
Seguimiento a la solución del cambio de idioma de Outlook Web a nivel país hasta su resolución.

- **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 a 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:

Fecha de visita	Dirección Territorial	Sede	Actividad ejecutada para dar solución	Caso Aranda / Proveedor
Marzo 2025	Popayán	Bordo	Se valida cruce de cableado de red mal conectado, se corrige y permite restablecer conexión a la red, usuarios: Mario Villada, Liliana Ledezma	86896 86277
Marzo 2025	Cali	Buga	Se reemplaza regleta eléctrica, se conectan componentes y se confirma que están funcionales, trabajan con normalidad y se realiza la organización de cableado en el swich	RF-90314
Marzo 2025	Cali	Tuluá	Se procede con la organización deL cableado dejandolos bien dispuestos para evitar accidentes o posibles desconexiones, también para evitar que los funcionarios manipulen estos elementos	RF-93902
Marzo 2025	Manizales	Anserma	Se realiza visita técnica a inspección de Anserma para la revisión de activos tecnológicos por el traslado de urgencia a una oficina provisional.	RF-93169
Marzo 2025	Facatativá	Soacha	Se inicia sesión con el usuario de la funcionaria en el teléfono. Se verifica que la cuenta de TEAMS esté vinculada correctamente con los permisos necesarios y al mismo se procede a realizar una llamada	RF-93452

			telefónica de prueba donde se evidencia correcta comunicación tanto por el auricular como por el altavoz.	
Marzo 2025	Yopal	Paz Ariporo	Se verifica la necesidad de instalar y configurar Fortinet y el Firewall con ayuda remota del Especialista, se validan servicios instalados y operativos	RF-95073
Marzo 2025	Vichada	Puerto Carreño	Organización del cableado del Rack y adecuación de un punto de red	N/A
Marzo	Magdalena	Ciénaga	Se revisa estado físico y funcional del equipo que entrega el funcionario, se realiza el backup requerido, el borrado seguro y la disposición segura del equipo de computo	RF-88906

Tabla 52 Visitas en sedes sin Soporte en Sitio

En la siguiente tabla se relaciona el acumulado de visitas atendidas por la UT para el último trimestre de la fase de operación del servicio de soporte:

Mes/Año	Cantidad visitas Ejecutadas Mes	Total Visitas Contractuales
Enero 2025	15	8
Febrero 2025	11	8
Marzo2025	8	8
Total general	**34**	**24**

Tabla 53 Consolidado de Visitas en sedes sin Soporte en Sitio

• Medición ANS Mesa de Servicios

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

ID	Indicadores	Resultado	Meta
MDS 1	Tiempo de atención de solicitudes por soporte en sitio	99,09%	95,00%
MDS 2	Tiempo de solución de incidentes por soporte en sitio	100,00%	90,00%
MDS 3	Tiempo de solución de requerimientos por soporte en sitio	100,00%	90,00%
MDS 4	Tiempo de respuesta de la mesa de servicio	100,00%	85,00%
MDS 5	Abandono de llamadas	0%	Máximo el 8%
MDS 6	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 54 Medición ANS Mesa de Servicios

3. LINEA DE SERVICIOS CENTRALES

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

3.1. Datacenter

3.1.1. Datacenter Principal

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

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

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

Con esta actividad se realizó despliegue de gran parte de los servidores de Windows 2012 – 2016 -2019 – 2022 realizando instalación de los KB más recientes, mitigando la falta de instalación de actualizaciones de sistema operativo sobre los servidores de entorno de pruebas de manera adecuada. Asociada a esta actividad se postularon como cambio estándar aquellos RFC identificadas para despliegue de actualizaciones de Windows Server 2012-2016-2019-2022. Se toma una muestra de 100 máquinas virtuales sobre cumplimiento de acuerdo con las estadísticas arrojadas por el WSUS y a nivel de cumplimiento de descarga e instalación de actualizaciones se encuentra en un 98% de cumplimiento, esto atado a la mitigación de vulnerabilidades asociada a la instalación de estas actualizaciones.

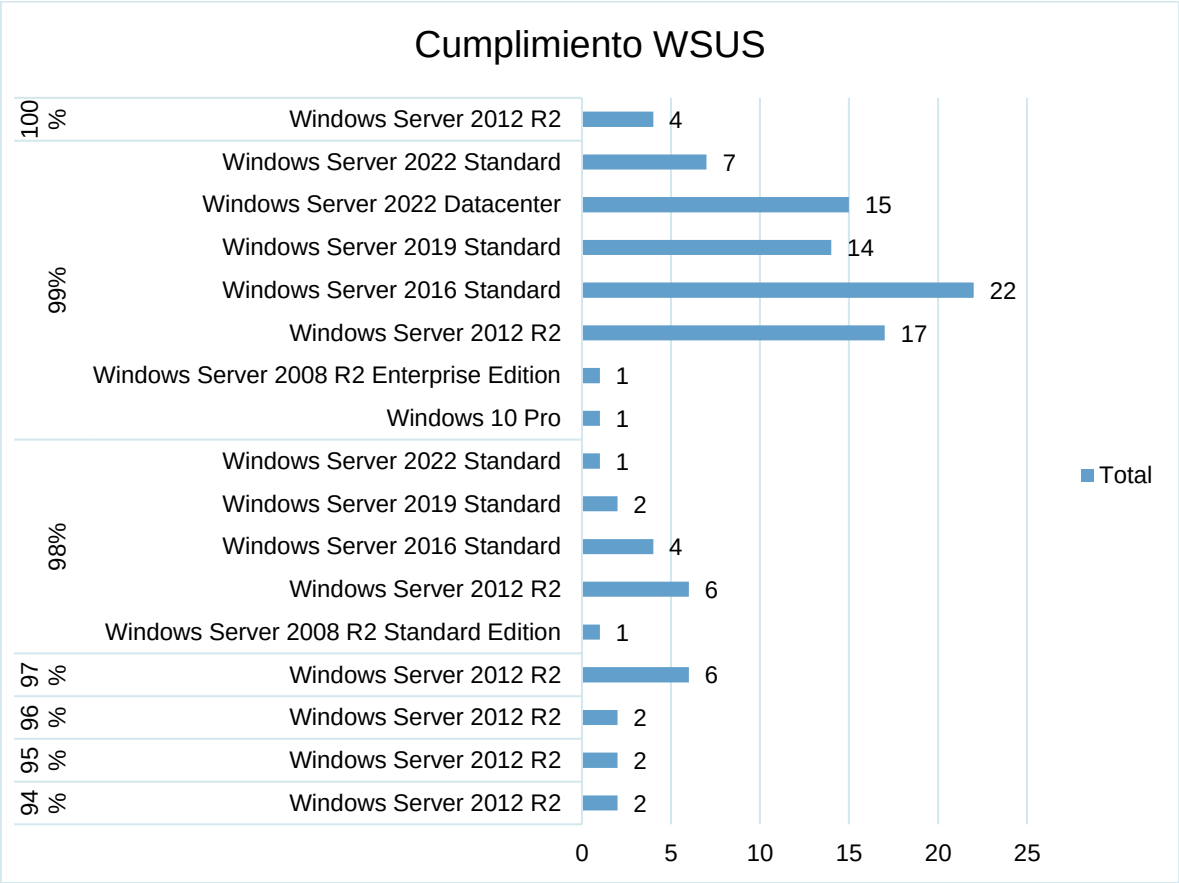


Ilustración *38* Cumplimiento WSUS

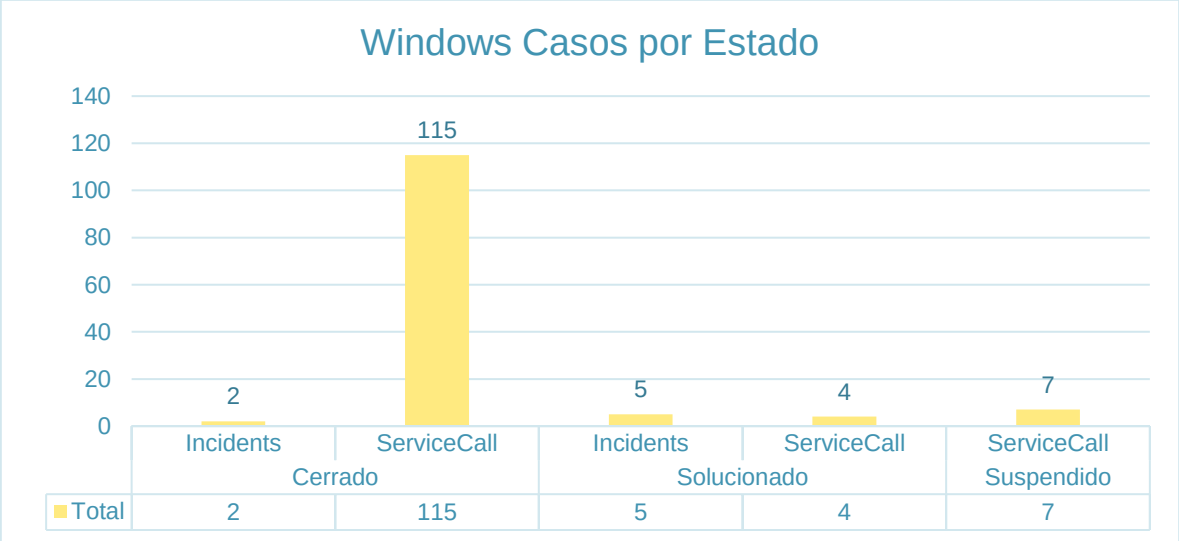


Ilustración 39 Estado final de los casos Windows

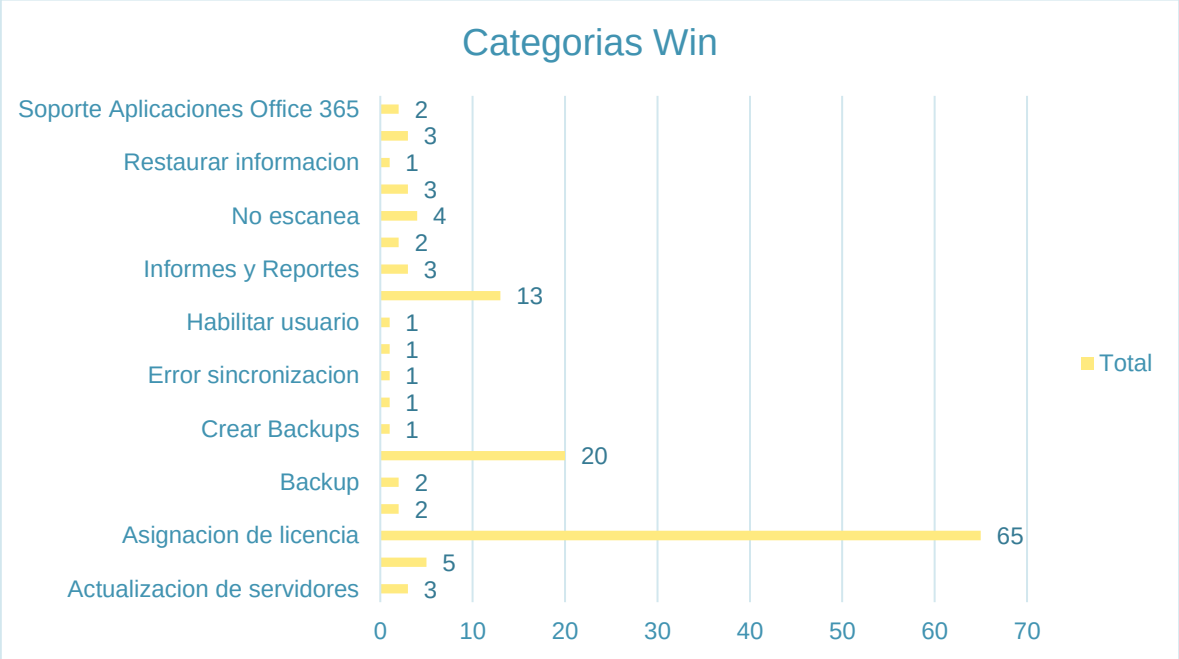


Ilustración 40 Casos por categorías Windows

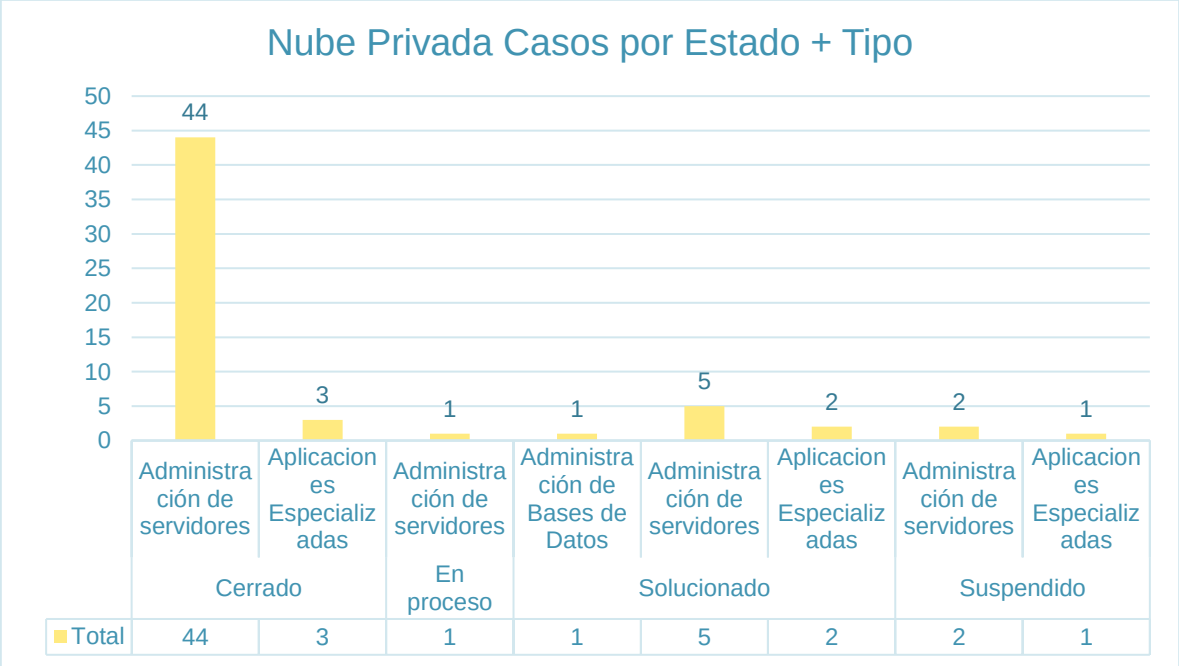


Ilustración 41 Estado final de los casos Nube privada

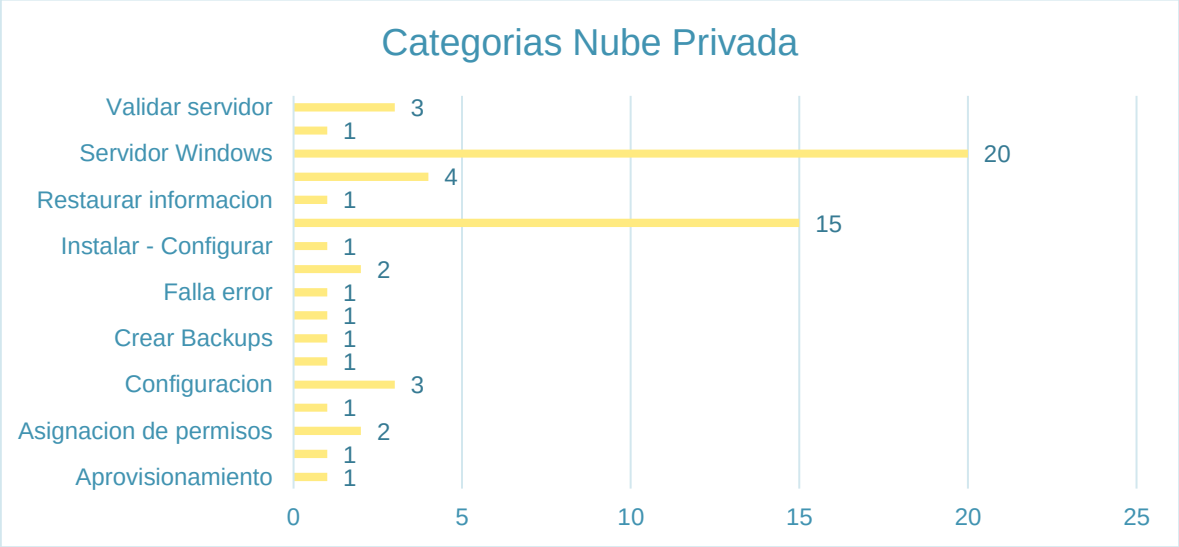


Ilustración 42 Casos por categoría Nube privada y pública

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

Descripción / Características	Mínimo requerido
Capacidad VCP	657 vCPUs en sitio de producción.
Capacidad Memoria Virtual	2637 GB de memoria virtual en sitio de producción
Capacidad de Almacenamiento	120 TB usables en sitio de producción
Numero Servidores	106 servidores

Tabla 55 capacidades de acuerdo con las fichas técnicas

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

Total MinT (Con servidores para desaprovisionar + ambientes de pruebas)	
Descripción Características	Total
vCPU	790
RAM	3,4 TB
Almacenamiento	140 TB
Numero de Servidores	106

Ilustración 43 Infra total + servidores de pruebas + servidores a desaprovisionar

Total MinT (Sin servidores para desaprovisionar con ambientes de pruebas)	
Descripción - características	Total
vCPU	654
RAM	3 TB
Almacenamiento	134 TB
Numero de Servidores	89

Ilustración 44 Infra total producción + servidores de pruebas de la entidad

Total MinT (Sin servidores para desaprovisionar sin ambientes de pruebas)	
Descripción - características	Total
vCPU	559
RAM	2.5 TB
Almacenamiento	120 TB
Numero de Servidores	73

Ilustración 45 Infra total sin servidores de pruebas

Total MinT (Servidores Pruebas y Desarrollo)	
Descripción - características	Total
vCPU	95
RAM	425 GB
Almacenamiento	13 TB
Numero de Servidores	16

Ilustración 46 Capacidades consumidas por entornos de pruebas

vCPU Ficha: **657** a vCPU consumida: **654**
Memoria Ficha: **2.6 TB** a Memoria consumida: **3 TB**
Almacenamiento Ficha: **120 TB** a Almacenamiento consumido: **134 TB**
Número de Servidores Ficha: **106** a Numero de Servidores disponibles: **89**

Se realizó validación de los datos, realizando exclusión de la información asociada a las capacidades consumidas por parte de los servidores de servicios de la operación, es decir máquinas aprovisionadas para operar un servicio y que no hicieron parte de la virtualización de la nube privada de la entidad, aun así realizando esta exclusión, la entidad se encuentra en un escenario de consumos por encima de los definido en la ficha en los ítems de vCPU y RAM, el almacenamiento disminuyó considerablemente sus consumos, teniendo en cuenta que se están excluyendo los servidores asociados al servicio de Backup los cuales deben validarse en conjunto con la entidad para considerar o no excluir estos consumos de

capacidades de almacenamiento, ya que incluyéndolos dentro de la revisión, nuevamente entraría el ítem de almacenamiento superando la capacidad contratada.

	vCPUs	RAM - TB	Capacidad Disco
Consumos	**654**	**3 TB**	**134 TB**

Tabla 56 Capacidades consumidas (Sin servidores de backup)

Pero es importante mencionar que, en el proceso de redimensionamiento de la nube privada de la entidad, los ambientes de pruebas son los que están consumiendo las capacidades que están superando los ítems de RAM y Almacenamiento, por lo cual se debe entrar a revisar procesos de reducción de capacidades de estos entornos. También se expone que el servidor MINTRAB60 que cumple su rol como File Server principal, ha sufrido diferentes intervenciones de ampliación de capacidades de disco virtual, teniendo en cuenta que este servicio a crecido exponencialmente:

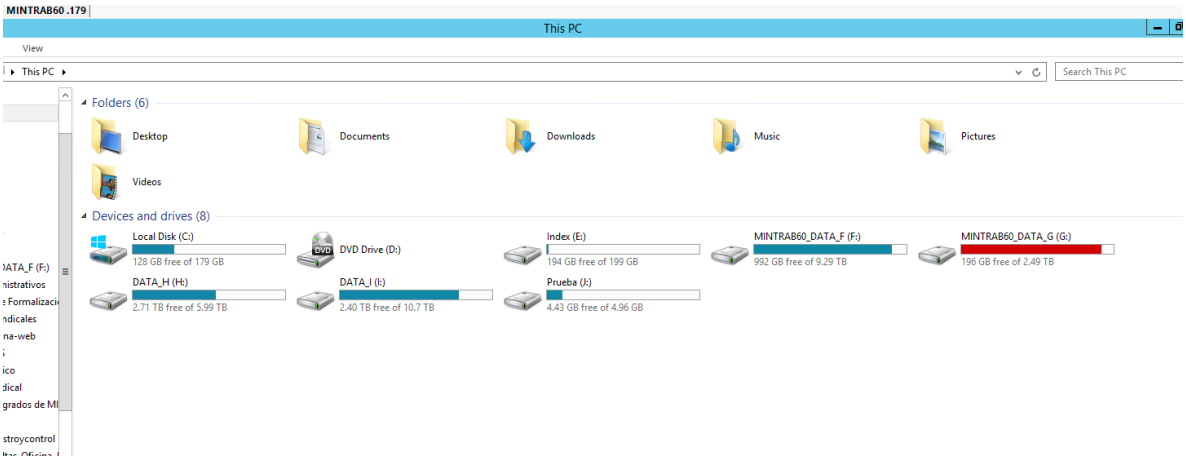


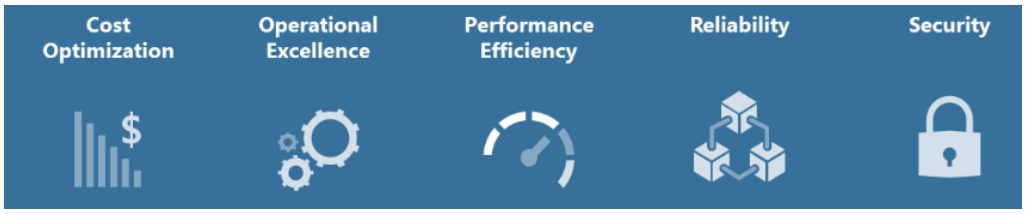
Ilustración 47 Estado File Server Mintrab60

Nube Pública

Se realizó socialización de los escenarios de Arquitectura en Nube publica Azure y la interacción hacia los componentes que permiten el funcionamiento de tableros Power BI y componente de ciencia de datos. En este ejercicio de arquitectura, se enfatizó en la estructura actual, como se encuentra el tenant a nivel de componente de infraestructura como servicio en nube y la interacción contra otros componentes de aplicación, ya sea en la misma nube pública, como conexiones hacía On Premises. Se definen los escenarios en donde se plantean cambios o mejoras sobre las propias implementaciones del Ministerio en el marco de la implementación de buenas prácticas para la gestión y administración de estos componentes.

Se validaron temas relacionados con el monitoreo de estos componentes a través de Azure Monitor, componentes que podrían postularse para des aprovisionamiento, estado de cada suscripción a nivel de arquitectura como de consumo de créditos, recomendaciones a nivel de cumplimiento de políticas establecidas por Azure, nombramiento de recursos y grupos de recursos, entre otras apreciaciones plasmadas en el documento de Línea base del servicio de Nube pública. Se indica la implementación de Well Architected Framework, el cual está diseñado para proveer los lineamientos de alto nivel con las mejores Prácticas

para ayudar a mantener las aplicaciones confiables, seguras, con alto rendimiento, gestión del costo, y la excelencia operativa de los recursos de nube.



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

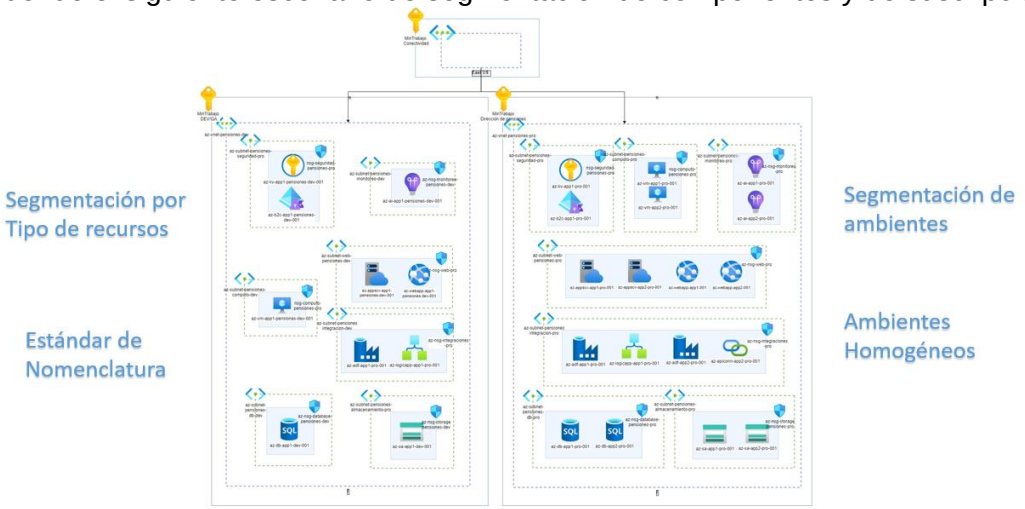


Ilustración 48 Proyección de Modelo de Suscripción

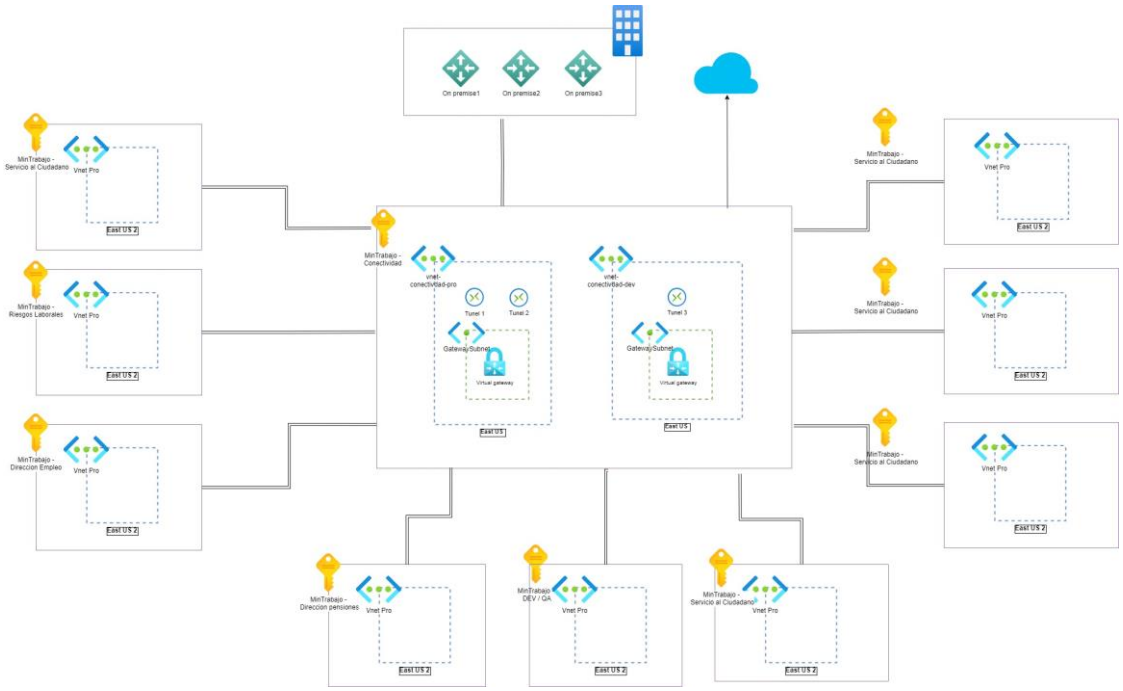


Ilustración 49 Modelo de Tenant bajo arquitectura

Se formaliza acta de recepción del sistema SICIP con la siguiente información:

El grupo de Soporte Informático define como documentos mínimos de recepción de un sistema de información aprovisionado, desarrollado y desplegado a través de un desarrollo in House o desarrollo externo en plataformas de nube privada o pública los siguientes ítems, los cuales permiten al grupo de Soporte Informático de la Subdirección Administrativa y financiera, ejercer las respectivas funciones de Administración, soporte y monitoreo de cualquier aplicativo que sea entregado de manera formal cumpliendo las respectivas condiciones anteriormente descritas.

- Documento de Arquitectura de Solución y de Software del Sistema de Información desarrollado y/o aplicativo, alcance del sistema de información y/o aplicativo (descripción jerárquica, diagrama de módulos, descripción individual de módulos, dependencias externas, licenciamiento y certificados digitales necesarios).
- Diagrama de arquitectura e interoperabilidad y diagramas de ambientes de pruebas, desarrollo, preproducción con otros sistemas de información y/o aplicativos.
- Documento de arquitectura de la base de datos y diseño de modelo de datos.
- Documento de Especificación de Historias de Usuario o Documento de Especificación de Casos de Uso Requisitos funcionales.
- Manual de despliegue del sistema de información y/o aplicativo.
- Manuales técnicos y de Operación de las funcionalidades del sistema de información y/o aplicativo. • Manuales de usuario.
- Procedimientos de instalación y prueba
- Registro de pruebas unitarias ejecutadas (proyectos internos)
- Registro de pruebas de QA ejecutadas (proyectos externos)
- Plan Maestro de Pruebas
- Informes de seguimiento a la ejecución de los casos de prueba.
- Actas de aceptación de los casos de uso y de la suite de pruebas.
- Informe de Pruebas No Funcionales (de rendimiento, carga y estrés, vulnerabilidad, inyección de código y seguridad)
- Informe de Corrección de vulnerabilidades (Si Aplica)
- Certificado del Registro de Derechos Patrimoniales del sistema de información
- Ficha Técnica Software y Licencias para el registro del sistema en el sistema contable
- Formato de requerimiento de cambio RFC remitido a la Mesa de Servicios para el paso a producción

Para el escenario del sistema de información SICIP se realiza recepción de los siguientes documentos:

- Documento técnico versión final
- Documento requerimientos funcionales
- Documento metodología de desarrollo
- Documento de recomendaciones y buenas prácticas para el mantenimiento del sistema
- Documento de puesta en operación de ambiente de producción y pruebas
- Documento de Código fuente
- Certificado de derechos de autor
- Acta de recibo a satisfacción
- Manual de usuario Administrador
- Manual de Usuario final

Dentro del documento técnico versión final se hace alusión a los siguientes Ítems: - Arquitectura de la solución - Arquitectura de referencia conceptual - Arquitectura de Solución en Nube Publica - Privilegios necesarios - Bases de datos de aplicación - Diagrama Entidad relación - Diccionario de datos - Tablas - Vistas - Procedimientos almacenados - Front End & BackEnd de la Aplicación - Arquitectura de servidores - Librerías y componentes utilizados - Informes de herramientas utilizadas - Conexiones de datos - Ubicación y construcción de reportes - Aplicaciones Lógicas – Logic Apps - Credenciales de inicio de sesión - Instrucción de Instalación y/o Despliegue - Prerrequisitos tecnológicos - Conexiones o interoperabilidad con otros sistemas - Despliegue o Instalación del Sistema - Código Fuente - Instrucciones de Instalación Local BackEnd - Instrucciones de Instalación local Front End - Instrucciones Despliegue BackEnd - Instrucciones Despliegue FrontEnd Con lo anterior se da viabilidad y aceptación de la documentación recepcionada por parte de las áreas funcionales y presentada como parte de la entrega formal del Sistema de Información SICIP al grupo de Soporte Informático para Administración, soporte y monitoreo del estado actual del aplicativo.

Es importante mencionar que este aplicativo, durante las sesiones de empalme con el proveedor quien desarrollo este aplicativo, se pudo observar algunos ítems que no quedaron descritos dentro de la documentación entregada por el proveedor y desde el grupo de Soporte Informático es importante dejarlos definidos dentro del acta de aceptación ya que hacen referencia al estado del sistema de información, la experiencia de usuario y la interacción del sistema de información con otros aplicativos del Ministerio del Trabajo y la forma en que interopera. - Formularios poco amigables con el usuario final: se observan formularios que no permiten la visualización adecuada de la información del aplicativo, lo cual implica para el usuario final, aplicar el Zoom nativo del navegador por el cual accede al sistema de información para poder visualizar de una forma más nítida los datos arrojados por los formularios consultas o los reportes generados a través del aplicativo. Esto agrega una acción adicional para el usuario que debería brindar la propia herramienta, la plantilla por defecto debería aplicar los principios responsive, que permite adecuar los formularios y la información de estos. - Consultas lentas y despliegue de información: El usuario final del aplicativo SICIP al realizar una consulta dentro del sistema de información, presenta una lentitud significativa en la búsqueda y despliegue de los datos en los formularios para cualquier rol del aplicativo, Esto degrada la experiencia de usuario ya que ralentiza las funciones y actividades inherentes a su cargo debido a la lentitud que genera el sistema de información.

Esto ocurre tanto en búsquedas dentro de la base de datos nativas para el sistema de información en MSSQL Server como en búsquedas externas hacia otros componentes tecnológicos de otros sistemas de información y aplicativos del Ministerio del trabajo. - Ausencia de Indización de las tablas: Durante el empalme del servicio de SQL Server y bases de datos se observó que no se contempló durante el aprovisionamiento de las bases de datos de SQL Server la configuración de la indización de las tablas, esto optimiza las consultas realizadas hacia la base de datos, especialmente cuando una consulta es realizada hacia una tabla muy grande y se requiere información en un formulario del sistema de información. - Usuarios para Aplicación y Bases de datos SQL: Se observa que el aplicativo durante su etapa de configuración, mantenía un solo usuario para todo el despliegue del aplicativo, tanto para la capa de aplicación como para la capa de reportaría y base de datos, lo cual no es una buena práctica, se sugiere mantener cuentas de servicio para cada capa del aplicativo con credenciales individuales y segmentadas para cada especialista y servicio. Esto debe ajustarse en entornos de pruebas y producción con el fin de realizar la implementación de la buena práctica a nivel de administración de los servicios

que permiten operar de manera adecuada el sistema de información SICIP. - Logic Apps / App Service: No se observan redundancia de los Logics Apps en ambiente de pruebas QA del sistema de información lo cual podría generar problemas de alta disponibilidad de estos componentes dentro del grupo de recursos de la nube publica de la entidad.

Key Vaults y Secrets: Se observa que los secrets se encuentran vencidos y no se efectuó renovación desde la cuenta que se generaron estos componentes, por lo cual, al realizar el llamado de estos registros, genera error ya que esta está haciendo llamado de un recurso con fecha de expiración pasada. Esta renovación debió haberse efectuado antes de la entrega formal al área funcional, con el fin de no presentar problemas dentro del sistema de información. - Dentro de la documentación técnica se observan credenciales de usuarios administradores o propietarios de servicios en nube publica de acuerdo con la ODI Política de Gestión de Contraseñas del Ministerio del Trabajo ítems 2.5.7 y 2.5.8 indica: “El administrador de cada sistema es responsable de asegurar que las contraseñas que se transmitan a través de redes públicas estén protegidas contra acceso no autorizado mientras se encuentren en tránsito, para este caso se recomienda sean cifradas.” “El usuario es responsable de asegurar la privacidad de las contraseñas asignadas para acceder a los sistemas de información.” Por ende, toda Contraseña, independientemente de su origen o su propósito, debe ser compartida en un medio seguro y cifrado para garantizar la seguridad de acceso. Así como definir el propósito de estas credenciales.

Se creó estructura de entrega formal de suscripciones para Ministerio del Trabajo:

En aras de continuar brindado cumplimiento al contrato No. 574 de 2023 celebrado entre el Ministerio del Trabajo y la Unión Temporal Gestión TIC 2023, el Grupo Interno de Trabajo de Soporte Informático de la Subdirección Administrativa y Financiera y la Unión Temporal Gestión TIC 2023, se encargará de proporcionar cobertura para que los servicios requeridos estén enfocados en la administración, soporte y monitoreo de la infraestructura total de TI en los datacenters, la infraestructura que se aprovisione a través de la nube pública, así como la solución de conectividad WAN e internet que forman parte de este proceso. Esto contribuirá a mantener un flujo de trabajo eficiente.

En este contexto, solicitamos amablemente realizar la entrega de la suscripción a nube pública. Esta entrega enmarca la siguiente información:

- Inventario de componentes que estén aprovisionados en la suscripción
- Documento de Arquitectura de Solución y de Software del Sistema de Información desarrollado y/o aplicativo, alcance del sistema de información y/o aplicativo (descripción jerárquica, diagrama de módulos, descripción individual de módulos, dependencias externas, licenciamiento y certificados digitales necesarios).
- Diagrama de arquitectura e interoperabilidad y diagramas de ambientes de pruebas, desarrollo, preproducción con otros sistemas de información y/o aplicativos.
- Documento de arquitectura de la base de datos y diseño de modelo de datos.
- Documento de Especificación de Historias de Usuario o Documento de Especificación de Casos de Uso Requisitos funcionales.
- Manual de despliegue del sistema de información y/o aplicativo.
- Manuales técnicos y de Operación de las funcionalidades del sistema de información y/o aplicativo.
- Manuales de usuario.
- Procedimientos de instalación y prueba

- Registro de pruebas unitarias ejecutadas (proyectos internos)
- Registro de pruebas de QA ejecutadas (proyectos externos)
- Plan Maestro de Pruebas
- Informes de seguimiento a la ejecución de los casos de prueba.
- Actas de aceptación de los casos de uso y de la suite de pruebas.
- Informe de Pruebas No Funcionales (de rendimiento, carga y estrés, vulnerabilidad, inyección de código y seguridad)
- Informe de Corrección de vulnerabilidades (Si Aplica)
- Certificado del Registro de Derechos Patrimoniales del sistema de información
- Ficha Técnica Software y Licencias para el registro del sistema en el sistema contable
- Formato de requerimiento de cambio RFC remitido a la Mesa de Servicios para el paso a producción

Cabe señalar que la administración de los recursos de los componentes mencionados continuará siendo responsabilidad del área, en este caso, la Dirección de Pensiones y Otras Prestaciones.

Se hace envío de borrador de política de Privilegio de acceso mínimo:

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.*

A nivel de equipos de red en Datacenter, se observa que funcionaron correctamente, no se presentaron caídas ni bloqueos sobre el equipo, se relaciona grafica de comportamiento del equipo.

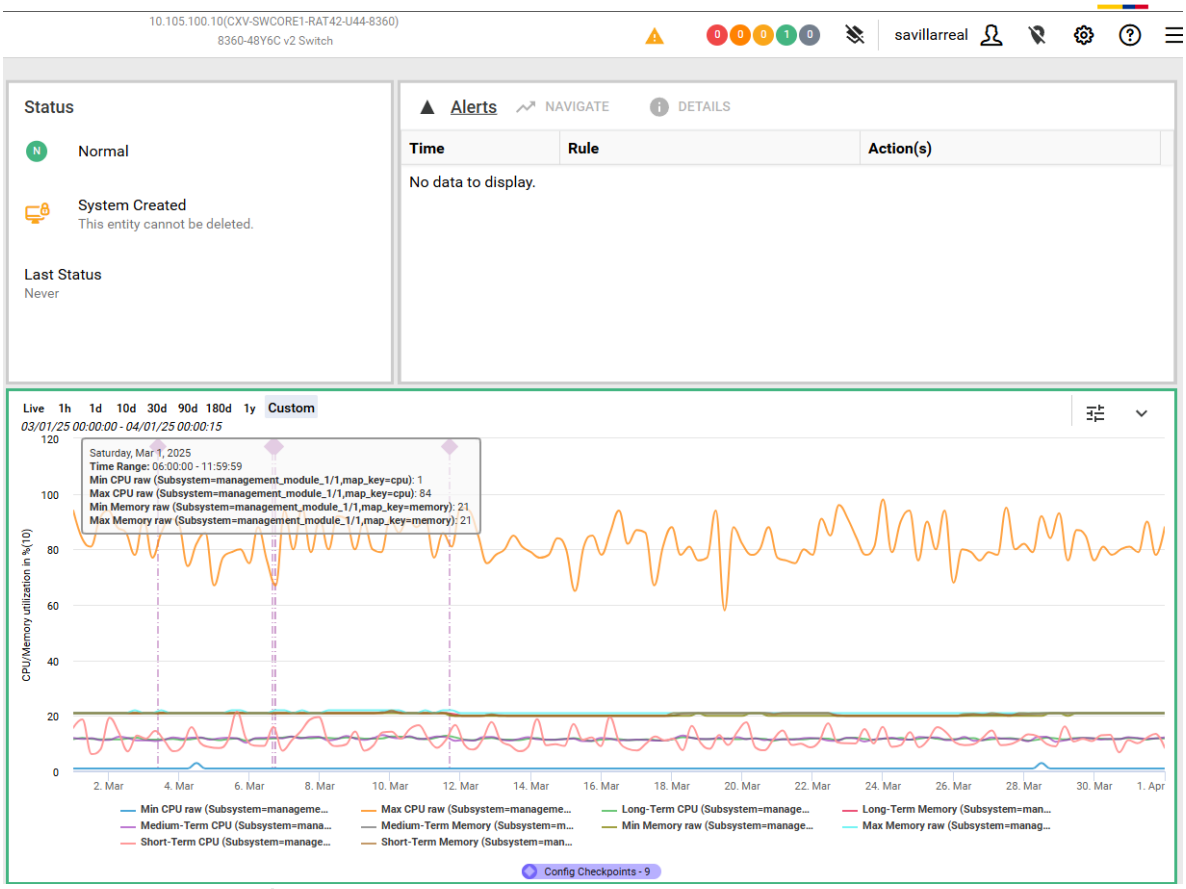


Ilustración 50 Comportamiento SWCORE Datacenter Colombia XV

El canal centralizado de Internet en Datacenter se mantuvo estable, la navegación de todas las sedes se ve reflejado en este canal. Se relaciona gráfica de comportamiento del canal de Internet en Datacenter, donde se observa que no se tuvieron caídas de servicio. El consumo promedio fue de 346.27 Mbps de recepción y 421.87 Mbps de transmisión.

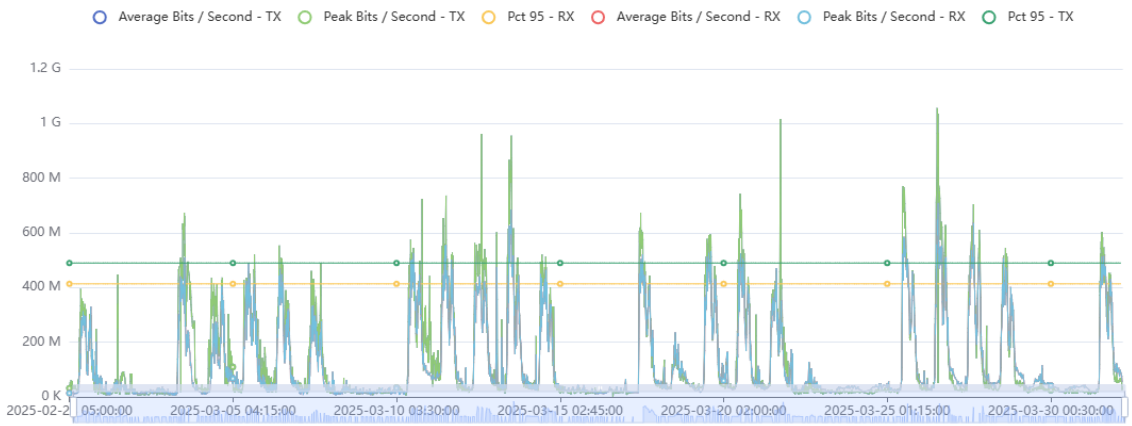


Ilustración 51. Grafica de consumo canal Internet Datacenter

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

3.1.2. Datacenter Alterno y DRP

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

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

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

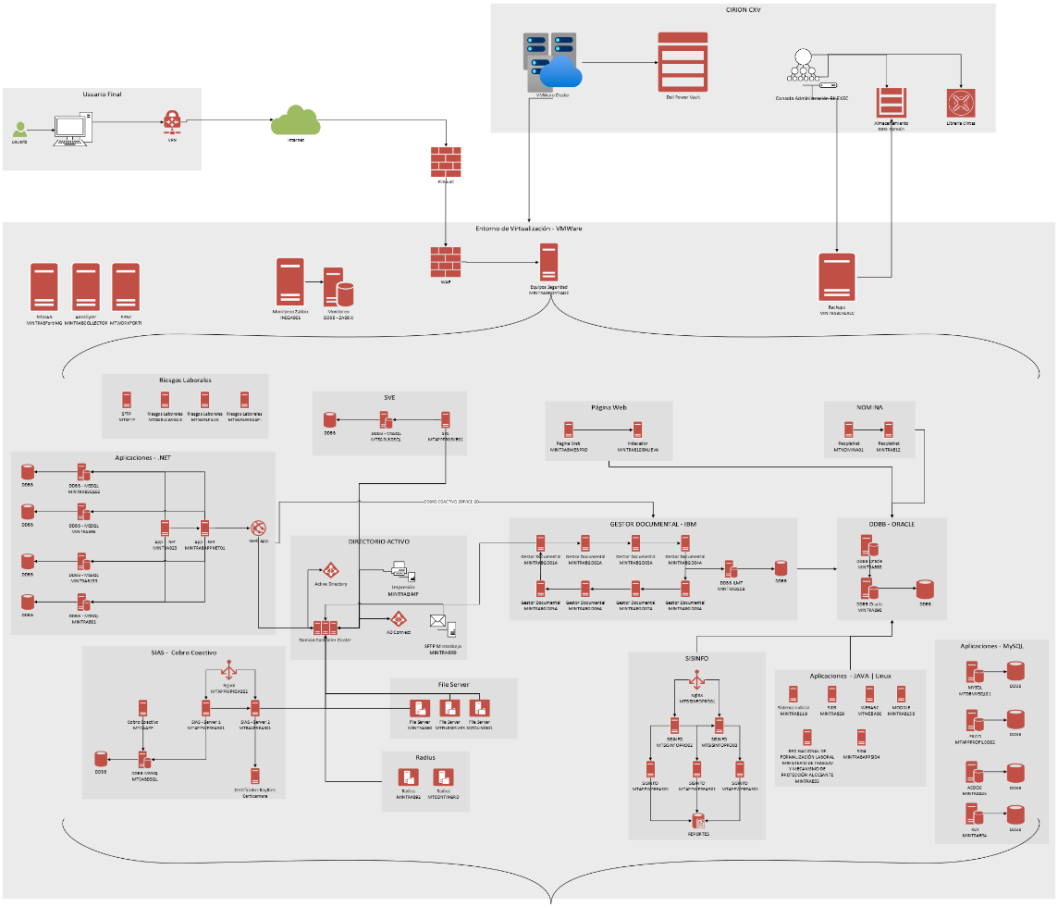


Ilustración 52 Diagrama Interoperabilidad Bogotá CXV

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

INDVCSACXV01.mintrabajo.loc → INDVCSASM01.mintrabajo.loc

NEW

Virtual Machine	Status	RPO
MINTRAB108NUEVA	OK	1 hour
MINTRAB158	OK	1 hour
MINTRAB19	Initial Sync	1 hour
MINTRAB23	OK	1 hour
MINTRAB33	OK	1 hour
MINTRAB94	OK	1 hour
MINTRABFORTIADC_CALI	Recovered	1 hour
MINTRABGD08A	OK	1 hour
MINTRABWEBPRO	OK	1 hour
MTAPPPROSVE01-7J14	OK	1 hour
MTAPPPROFILCO02	OK	1 hour
MTAPPWPREAS01	OK	1 hour
MTAPPWPREAS02	OK	1 hour
MTBALPREAS01	OK	1 hour
MTCAAPP	OK	1 hour

Ilustración 53 VM Replicadas a través de site recovery

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

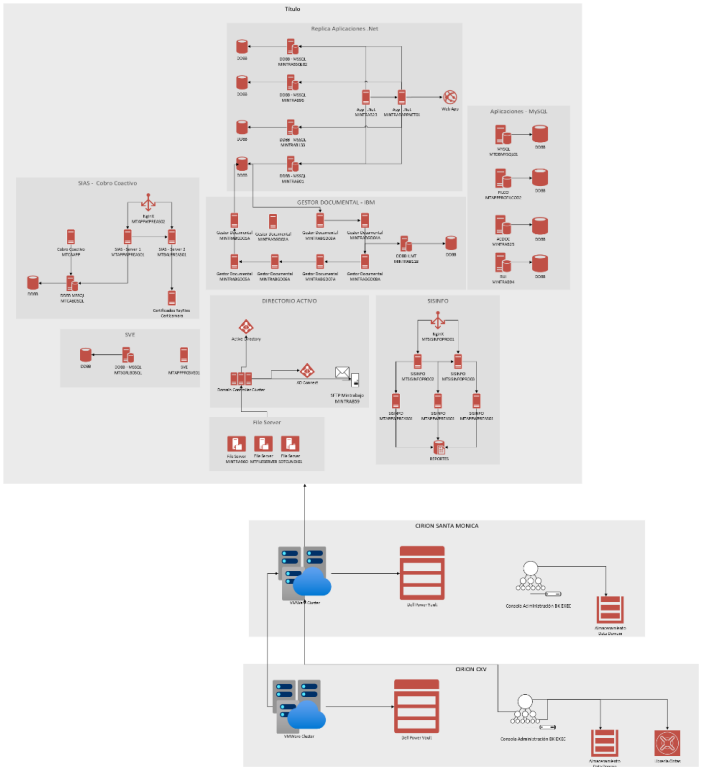


Ilustración 54 Diagrama de Replicación CXV - Santa Mónica

La conexión del LAN to LAN entre los dos Datacenter funcionó correctamente, de esta forma se garantizó la conexión entre los Datacenter. Se relacionan las gráficas de consumo en extremo, Datacenter Santa Mónica. Se observa un consumo promedio de 14.36 Mbps de transmisión y 310 Kbps de recepción.

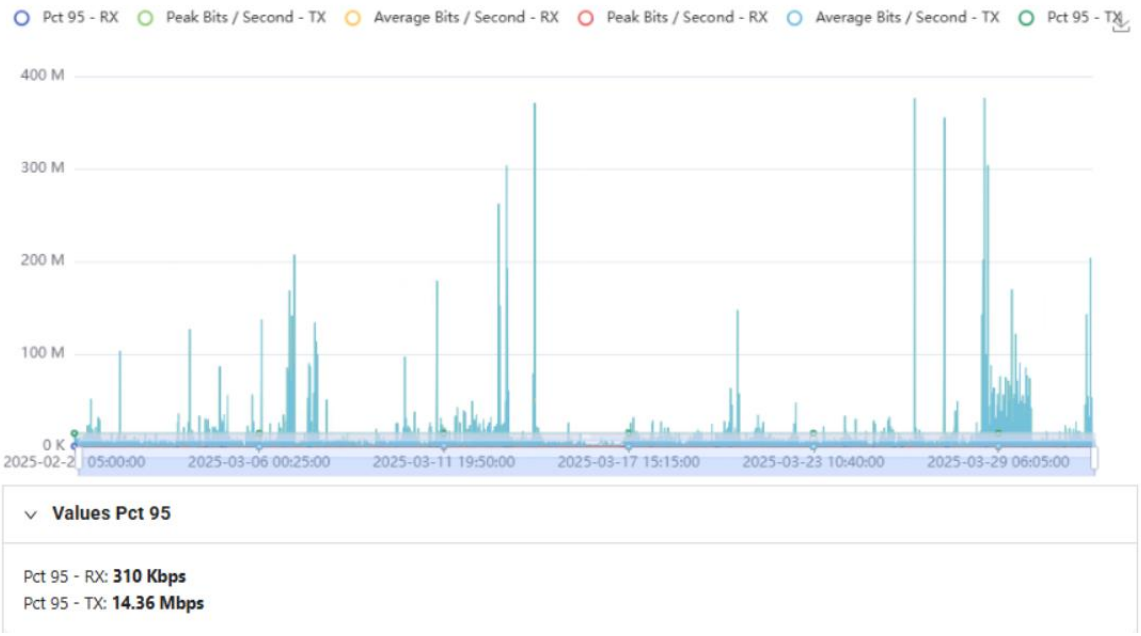


Ilustración 55 Grafica de consumo LanToLan extremo Cali

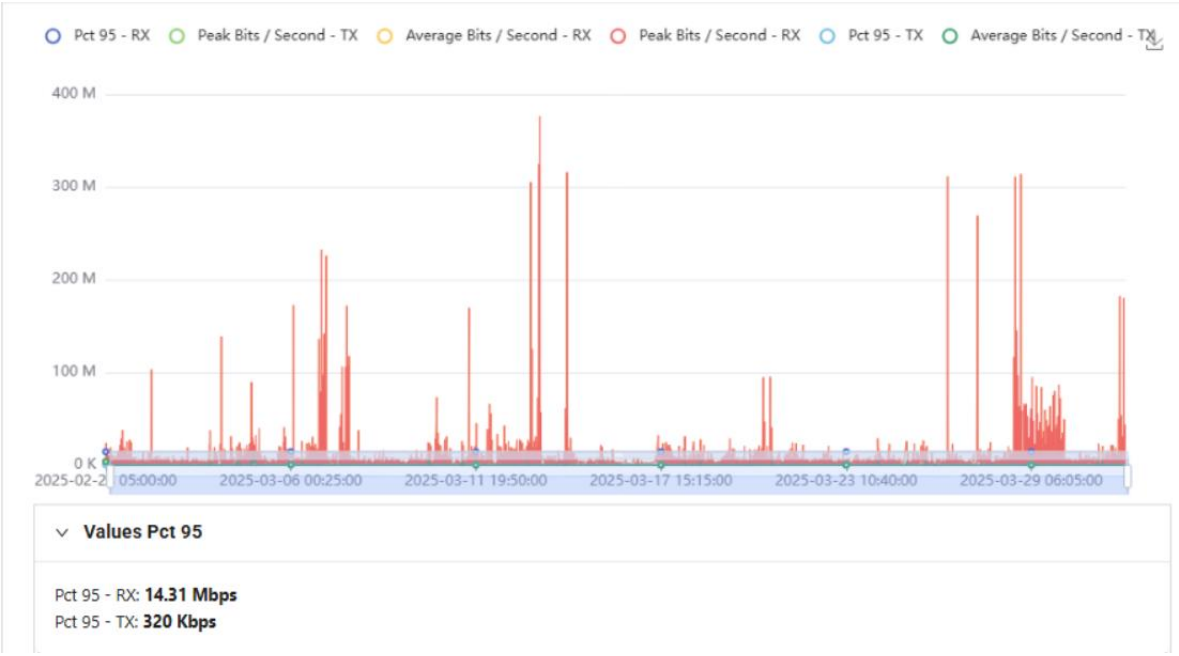


Ilustración 56 Grafica de consumo LanToLan extremo Bogotá

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

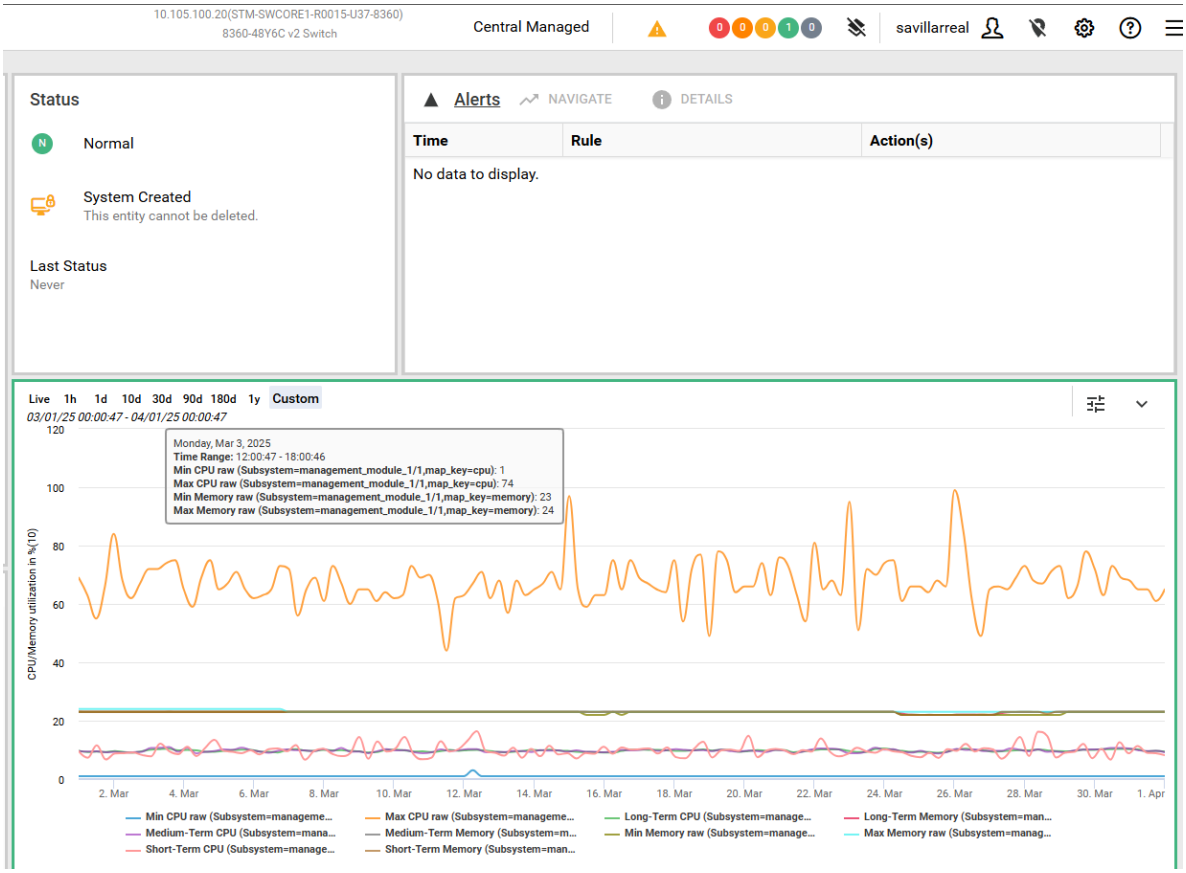


Ilustración 57 Estado SWCORE Datacenter alterno

3.1.3. Procesamiento, Almacenamiento y Respaldo

- **Servidores Windows e Infraestructura Virtualizada**

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

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

añadido servidores que han sufrido intervenciones técnicas con finalidad de adecuar la infraestructura virtualizada y depurar máquinas virtuales que no se encuentran en uso por parte de la entidad, pero sí que consumen capacidades que pueden ser aprovechadas por los entornos productivos.

Es importante mencionar que el escenario de arquitectura de la entidad actual ha permitido como operador de servicios tecnológicos, identificar diversas acciones de mejora que se han venido ejecutando de manera transversal desde el inicio del contrato, pero es importante dar visibilidad de los escenarios observados. Durante los procesos de afinamiento y egreso de equipos no productivos en Datacenter se logra visualizar componentes en estado sensible que podrían poner en riesgo la disponibilidad de servicios críticos como lo es el sistema de información 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 se realiza esta sesión, en donde se identifican los servidores productivos como parte del escenario de virtualización de la entidad y que su proceso de migración a nuevos servidores de aplicación puede surtirse de la mano del área funcional. Para el servidor MINTRAB13, el cual aloja una copia histórica del anterior aplicativo y base de datos de nómina de la entidad, el proveedor nos confirma que no tiene administración y ningún tipo de gestión sobre el recurso y la información que esta aloja. La entidad confirma tener acceso de consulta a una base de datos y solo es consultada por demanda, pero no está asociada a ningún sistema de información productivo.

Por lo cual, desde el equipo de trabajo de la UT, se están estudiando diferentes alternativas para migrar este recurso a un entorno de virtualización seguro, de manera provisional se continuará con el servidor físico operativo, teniendo en cuenta que a la entidad ya se le presentaron las vulnerabilidades y riesgos que corre al conservar este servidor, sumada la ausencia de documentación de este servidor a nivel técnico funcional.

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.

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 iniciando con 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 consolidaran 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.

Con apoyo del equipo de nube privada se adelantó la instalación de agentes SIEM en diferentes máquinas atadas a las actividades realizadas por el SOC de escaneo e identificación de vulnerabilidades. Así como actualización de antivirus y agentes de este para máquinas que hacen parte del inventario definitivo de nube privada. Se realizó aprovisionamiento de cuentas de servicio para servidores Windows como Linux para escaneo autenticado y poder tener información de vulnerabilidades registradas en cada servidor de manera más específica y real.

Dentro de las actividades de optimización de la infraestructura virtualizada, específicamente para servidores de archivos (file server) se realizó cambio del sistema operativo que alojaba el servidor de archivos MINTRAB19 el cual se encontraba en un entorno de sistema operativo obsoleto y por su criticidad se realizó esta intervención con el fin de poder garantizar una disponibilidad de este recurso en un entorno soportado y que permita actualizaciones a nivel de OS y su administración sea más sencilla para el equipo técnico. Este cambio no significó un traumatismo para usuario final a nivel de accesibilidad de la información y del recurso mapeado como unidad de red. Este cambio es un primer escenario para una futura actualización y centralización de los servidores de archivos de la entidad.

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.

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.

A nivel de capacidades de las máquinas virtuales asignadas a la dirección de IVC, se realiza un ejercicio de la mano del equipo de la dirección, identificando las máquinas virtuales que están en desuso por versionamiento deprecado por parte de los sistemas de información. Capacidades que pueden ser asignadas a otros recursos como lo son aprovisionamientos nuevos de sistemas de información o en su defecto ampliación de capacidades de sistemas de información que lo requieran por demanda.

La totalidad de almacenamiento consumido por estos servidores es de 4.07 TB distribuidos en 35 discos virtuales asignados a 17 máquinas virtuales.

Servicio	vCPUs	RAM	Discos	Capacidad Discos en MB	Capacidad GB	IP Servidor
SISINFO	20	40.960	1	129.748	129,7 GB	172.20.22.181
SISINFO	12	65.536	3	215.040	215 GB	172.20.44.30
SISINFO	32	131.072	3	215.040	215 GB	172.20.44.31
SISINFO	32	131.072	3	215.040	329,0 GB	172.20.44.32
SISINFO	12	65.536	3	215.040	329,0 GB	172.20.42.33
SISINFO	16	65.536	3	215.040	329,0 GB	172.20.42.34
SISINFO	16	65.536	2	184.320	229,3 GB	172.20.44.33
SISINFO	16	65.536	2	184.320	229,3 GB	172.20.44.34
SISINFO	8	32.768	2	163.840	229,8 GB	172.20.44.35
RUTRAPORT	8	32.768	1	512.000	129,0 GB	172.20.22.122
RUTRAPORT	8	32.768	1	512.000	129,0 GB	172.20.22.121
SIAS	8	16.384	2	204.800	229,8 GB	172.20.42.101
SIAS	8	16.384	1	102.400	129,4 GB	172.20.42.102
SIAS	8	12.288	2	153.600	229,6 GB	172.20.42.103
SIAS	8	16.384	2	199.680	229,6 GB	172.20.42.100
SIAS	8	32.768	1	256.000	129,0 GB	172.20.42.104
FILE SERVER DT BOGOTA CUNDISSIT	24	12.288	3	287.143	287,1 GB	172.20.22.13

Tabla 57 Capacidades SI – IVC

VM	NOMBRE DISCO	CAPACIDAD MB	CAPACIDAD GB
MTPRUSISINFO01	C:\	129.748	129,7 GB
MTSISINFOPRO01-wneQ	C:\	102.400	102,4 GB
MTSISINFOPRO01-wneQ	D:\	102.400	102,4 GB
MTSISINFOPRO01-wneQ	P:\	10.240	10,2 GB
MTSISINFOPRO02-lpm1	C:\	102.400	102,4 GB
MTSISINFOPRO02-lpm1	D:\	102.400	102,4 GB
MTSISINFOPRO02-lpm1	P:\	10.240	10,2 GB
MTSISINFOPRO03	C:\	102.400	102,4 GB
MTSISINFOPRO03	D:\	102.400	102,4 GB
MTSISINFOPRO03	P:\	10.240	10,2 GB
MTSISINFOPRU01	C:\	102.400	102,4 GB
MTSISINFOPRU01	D:\	102.400	102,4 GB
MTSISINFOPRU01	P:\	10.240	10,2 GB
MTSISINFOPRU02	C:\	102.400	102,4 GB
MTSISINFOPRU02	D:\	102.400	102,4 GB
MTSISINFOPRU02	P:\	10.240	10,2 GB
MTSISINFOREPO1	C:\	81.920	81,9 GB
MTSISINFOREPO1		102.400	102,4 GB
MTSISINFOREPO2	C:\	81.920	81,9 GB
MTSISINFOREPO2		102.400	102,4 GB
MTSISINFOREPO3	C:\	81.920	81,9 GB
MTSISINFOREPO3		81.920	81,9 GB
MINTRABRUTRABACK	C:\	512.000	512,0 GB
MINTRABRUTRAFRONT	C:\	512.000	512,0 GB
MTAPPWPREAS01	C:\	153.600	153,6 GB
MTAPPWPREAS01	D:\	51.200	51,2 GB
MTAPPWPREAS02	C:\	102.400	102,4 GB
MTAPPWPREAS03	C:\	102.400	102,4 GB
MTAPPWPREAS03		51.200	51,2 GB
MTBALPREAS01	C:\	148.480	148,4 GB
MTBALPREAS01		51.200	51,2 GB
MTINFRAPREAS01	C:\	256.000	256,0 GB
SDTCUNDI01	F:\, C:\, D:\	287.143	287,1 GB

Tabla 58 Almacenamiento asignado - SI – IVC

Tras esta revisión, se informa a la Subdirección de IVC lo siguiente:

Actualmente el servidor mencionado MTINFRAPREAS01 con IP 172.20.42.104 cuenta con un almacenamiento de 250 GB en la partición o disco virtual C: cómo se puede observar en la siguiente imagen:

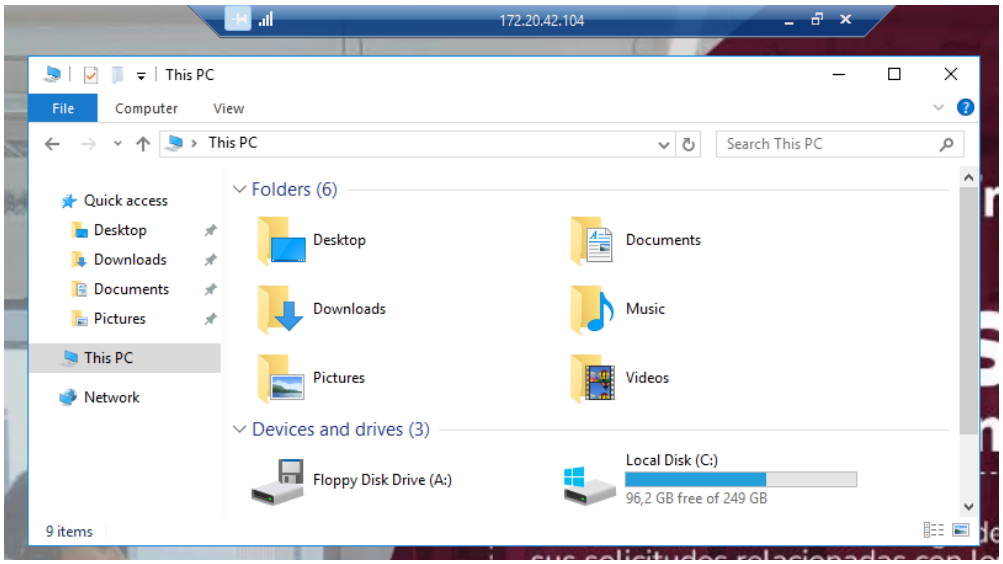


Ilustración 58 Detalle servidor

De acuerdo con lo anterior observamos que el disco en mención cuenta con un consumo del 61.6% del almacenamiento asignado contando con un 38.4% del almacenamiento libre para el uso del área, este almacenamiento no ha crecido exponencialmente en los últimos dos meses y no hemos identificado un comportamiento que justifique el crecimiento del 20% adicional de este almacenamiento, esto en el marco de la gestión de capacidades de la nube privada de la entidad de manera adecuada. Adicionalmente observamos que, aunque se liberaron capacidades de los servidores indicados por el Ing. Omar Coronado, estas capacidades serán empleadas para el aprovisionamiento de los servidores de RUTRAPORT en entorno productivo.

En esta gráfica podemos observar el consumo de almacenamiento desde el mes de noviembre, se visualiza que se ha mantenidos sobre 98-96 GB libres desde inicios de diciembre de 2024:
(Importante tener en cuenta que se observan 2GB adicionales (98 GB en vez de 96 como se muestra en la captura de arriba) por el factor de conversión binaria de Windows para los almacenamientos 1024 MB = 1 GiB)

Adicionalmente. nos permitimos informar que las máquinas que el Ing. Omar Coronado nos aprobó para desaprovisionar, se encuentran ubicadas en un Data Store diferente al de la máquina MTINFRAPREAS01 (Data Store: almacén de datos que permite guardar discos virtuales y máquinas virtuales dentro de un entorno de nube privada) por ende la asignación de recursos no depende estrictamente de liberar las capacidades asignadas a una máquina virtual, sino también del repositorio en donde se encuentren las máquinas virtuales. En este caso las máquinas de SISINFO des aprovisionadas, no se encuentran en el mismo repositorio en donde se encuentra la máquina de SIAS en mención.

En caso de que se requiera estrictamente el crecimiento de este disco virtual, se debe justificar debidamente para que esta asignación de capacidades de almacenamiento no sea subutilizada y se pueda aprovechar de manera correcta dentro de la nube privada.

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

Infraestructura actual
Servidor Aplicación

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

Servidor DDBB

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

En revisión de la documentación cambia el paradigma actual, el Sistema Operativo que aloja Moodle cambiaría, por lo que debe validarse la pertinencia del cambio de entorno o si se conservara un entorno Linux, pero más actualizado.
Para el escenario de DDBB, si se cambia a los motores de base de datos autorizado (SQL Server - Oracle DBA) no solo debe tenerse en cuenta el licenciamiento requerido para esta DDBB nueva en este entorno si no también la homologación de la DDBB de MySQL al motor que se elija.

Las características de Hardware solicitadas son las siguientes:

Elemento	Requerimiento
Sistema Operativo	Windows Server 2019 o superior
Roles y Características	IIS habilitado, soporte para PHP y bases de datos
CPU	Mínimo 8 núcleos (recomendado 16 núcleos para más de 1000 usuarios concurrentes)
Memoria RAM	Mínimo 16GB (recomendado 32GB para entornos de producción)
Almacenamiento	SSD con al menos 500GB para instalación y datos, escalable según necesidad
Conectividad	Ancho de banda mínimo de 1 Gbps para acceso interno y externo

Ilustración 59 Hardware solicitado

Se observa que es un crecimiento de un 135% de las capacidades actualmente asignadas, sin tener en cuenta que estos servidores actuales no tienen un consumo elevado de las características que tienen asignadas actualmente, por lo que no se justifica técnicamente este crecimiento tan elevado. Con respecto al cambio de sistema Operativo, debe confirmarse si se debe cambiar por obligaciones contractuales del proveedor que va a realizar la migración de versión o si es posible conservarlo en entorno Linux. Al igual que lo mencionado para la capa de base de datos.

Con respecto a las características de los componentes instalados dentro del servidor:

Requerimientos del Servidor

Elemento	Requerimiento
Actualización de Moodle	Moodle 4.5.2
Versión de PHP	Mínimo PHP 8.1.0 (se recomienda PHP 8.3.x)
Extensión PHP Sodium	Obligatoria
Configuración PHP max_input_vars	Debe ser >= 5000
Arquitectura PHP	Solo versiones de 64 bits compatibles

Ilustración 60 Componentes Moodle nuevo

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

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

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

- Manuales técnicos y de Operación de las funcionalidades del sistema de información y/o aplicativo.

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

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

- Servidor Backend
  - Almacenamiento de 2TB → Se requiere se envíe documento de arquitectura donde se pueda visualizar la justificación técnica para la asignación del almacenamiento, si hará uso de un servidor ya aprovisionado o si requiere de un servidor independiente para este fin.
  - Memoria RAM de 256 GB → Se requiere se envíe documento de arquitectura donde se pueda visualizar la justificación técnica para la asignación del almacenamiento, si hará uso de un servidor ya aprovisionado o si requiere de un servidor independiente para este fin. Es importante mencionar que la entidad solo cuenta con 4 servidores con mas de 100 GB de RAM asignadas y están asociados a SISINFO por su carga transaccional, un servidor del gestor documental por su alto consumo de capacidades y un servidor de SQL que aloja
  - Procesador de 16 cores → Se requiere se envíe documento de arquitectura donde se pueda visualizar la justificación técnica para la asignación del almacenamiento, si hará uso de un servidor ya aprovisionado o si requiere de un servidor independiente para este fin. Se debe indicar los vCPU que se requiere asignar ya que es la métrica usada para creación de máquinas virtuales en la nube privada.
  - Windows Server 2022 → Se cuenta con licenciamiento disponible.

- Servidor FronEnd

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

En total la solución envía consumiría las siguientes capacidades:

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

Para contrastar, toda la solución del gestor documental el sistema de información más robusto que tiene el Ministerio a nivel de capacidades, incluidos servidores de pruebas pesan alrededor de 10 TB distribuidos en más de 10 servidores y no llega a consumir 500 GB de RAM, sin contar con las capacidades asignadas para la capa de base de datos, únicamente contabilizando los servidores de aplicación, sin las bases de datos que tienen una carga mucho más elevada. Bajo esta premisa, recomendamos hacer un ejercicio de gestión de capacidades mucho más profundo y detallado, esto con el fin de asignar las capacidades estrictamente necesarias para que el sistema de información pueda funcionar de manera adecuada, con holgura de crecimiento de 15%-20% pero sin subutilizar los recursos contratados por la entidad, ya que este escenario provoca un desbalance en lo contratado por la entidad y no se aprovecharían de manera adecuada las capacidades de la Infraestructura tecnológica de la entidad.

3.1.4. Aplicaciones Especializadas

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

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

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

En el marco de esta validación, se realizó un escaneo de vulnerabilidades a nivel de aplicaciones en donde el equipo de seguridad (SOC) identifica diversas vulnerabilidades asociadas a aplicaciones alojadas en entorno virtualizado (On premises) en servidores de aplicación que poseen obsolescencia tanto a nivel de sistema operativo como a nivel de arquitectura de software. En estos informes se mencionan problemas a nivel de parámetros de seguridad, la falta de credenciales robustas puede exponer la infraestructura a riesgos significativos, tales como accesos no autorizados, ataques de fuerza bruta, y otras amenazas de seguridad. Para mitigar estos riesgos y proteger la información sensible, es crucial que todos los usuarios adopten contraseñas fuertes y seguras. Es importante mencionar que a la fecha aún se está a espera de despliegue y formalización de la mitigación de vulnerabilidades reportadas en el Ethical Hacking, teniendo en cuenta que se han sostenido diversas sesiones, pero no se ha dado un despliegue de la mitigación de las soluciones por parte del equipo de desarrollo de la entidad.

Recomendaciones para Credenciales Robustas:

- **Longitud mínima**:
  - Las contraseñas deben tener al menos 12 caracteres.
- **Combinación de caracteres**:
  - Incluir letras mayúsculas y minúsculas, números y caracteres especiales.
- **Evitar información predecible**:
  - No usar información personal como nombres, fechas de nacimiento, o palabras comunes.
- **Cambio periódico**:
  - Cambiar las contraseñas regularmente, al menos cada 90 días.
- **No reutilizar contraseñas**:
  - No reutilizar contraseñas antiguas o de otras cuentas

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 supervisión 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 dio continuidad a los procesos de duración de logs sobre la máquina que aloja el portal de la entidad, en el marco del afinamiento este servidor fue redimensionado para así tener un almacenamiento un poco más robusto del asignado y así poder tener una holgura en el almacenamiento consumido por los logs de la capa media que esta aloja.

De igual forma se ejecutaron diferentes controles de cambios, relacionados con sistemas de información como lo es SIRITI la cual se ha convertido en una de las aplicaciones que más controles de cambios presenta durante el mes en comparación con las demás aplicaciones en JAVA o componente .Net. Se propuso la independización del aplicativo SIRITI del servidor MINTRAB13 el cual aloja más de 40 aplicativos, lo cual podría indicar un inconveniente a la hora de gestionar controles de cambios ya que el despliegue de paquetes podría afectar el funcionamiento de otra aplicación que coexista en este entorno, esto debido a que cada aplicación fue desarrollada con diferentes prácticas y arquitecturas que a la hora de aprovisionarse en un solo entorno, podría provocar inconvenientes de cara al despliegue de controles de cambios para cada aplicación.

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

En atención a la información referenciada, nos permitimos informar la trazabilidad del proyecto RUTRAPORT:

- La Subdirección de IVC expone su necesidad del aprovisionamiento de un nuevo sistema de información para el cumplimiento de la necesidad de la Subdirección. Esta necesidad fue expresada durante las primeras semanas de mayo 2024.
- El grupo de Soporte Informático tras la formalización por parte del equipo técnico de IVC se realizó el aprovisionamiento de dos servidores para el ambiente de PRUEBAS del sistema RUTRAPORT. Tras el aprovisionamiento de estos dos servidores, se realizó la entrega formal y el acompañamiento para la configuración de la plataforma durante el mes de mayo 2024. Tras la entrega formal la aplicación pasó a fase pruebas de carga y estrés por parte del equipo técnico de IVC para un posterior dimensionamiento de capacidades en nube privada para el ambiente productivo.
- El 13/11/2024 el equipo técnico de IVC remitió las capacidades para ambiente productivo al grupo de soporte informático.
- Se realizó validación de las capacidades de todos los sistemas de información y aplicaciones de IVC el día 27/11/2024, dejando como pendiente, las máquinas

virtuales que debían ser depuradas para aprovisionar RUTRAPORT producción de manera adecuada en la nube privada de la entidad.
- El 3 de diciembre de 2024 el grupo de soporte informático remite correo a IVC con las capacidades para revisión del equipo IVC.
- El 24/12/2024 IVC responde las maquinas que debían ser des aprovisionadas y que podrían aprovecharse para el aprovisionamiento del ambiente productivo.
- Las maquinas referenciadas por IVC fueron apagadas el día 8/01/2025.
- Las máquinas de RUTRAPORT producción se aprovisionaron durante la semana del 13/01/2025 y fueron entregadas la semana del 20/01/2025
- Desde la fecha de entrega se ha venido acompañando el equipo técnico IVC para las configuraciones que ha requerido el área para adecuar el entorno de manera adecuada para salir a producción.

En complemento a la información remitida, me permito detallar los servidores empleados para cada ambiente y las cuentas de servicio asociadas:

- Ambiente de Pruebas
    - MINTRABRUTRABACK - 172.20.22.122
    - MINTRABRUTRAFRONT - 172.20.22.121
- Ambiente de Producción
    - MTRUTRABACKPD - 172.20.22.131
    - MTRUTRAFRONTPD - 172.20.22.130
- Cuentas de Servicio
    - Mintrabajo\rutraport
    - Mintrabajo\rutraprod

A la fecha no se ha presentado inconvenientes en la comunicación entre las áreas y se ha trabajado articuladamente para dar gestión adecuada desde soporte informático y la UT a los requerimientos técnicos expuestos por la Subdirección de IVC

Se observan vulnerabilidades asociadas a instalación de software obsoleto o no permitido dentro de los servidores de aplicación, actualizaciones de seguridad o parches de seguridad liberados por parte Microsoft, versionamiento de componentes que permiten el funcionamiento de la aplicación, pero se encuentran en una versión que posee vulnerabilidades de seguridad y que son mitigadas con su actualización de versión o instalación de parches de mitigación de fabrica directamente.

Dentro del ejercicio realizado, se encontraron componentes de Mozilla Firefox en versión 127.0 la cual es una versión obsoleta del explorador. Así como actualizaciones de seguridad de las capas medias Apache TomCat la cual, se encuentra en un versionamiento fuera de soporte y sin actualizaciones de seguridad. De igual forma, las vulnerabilidades más críticas encontradas estaban asociadas al componente de Microsoft Office 2016 Products la cual arrojaba actualizaciones de seguridad desde 2017 que no habían sido instaladas en los servidores de pruebas y producción del sistema de información SISINFO.

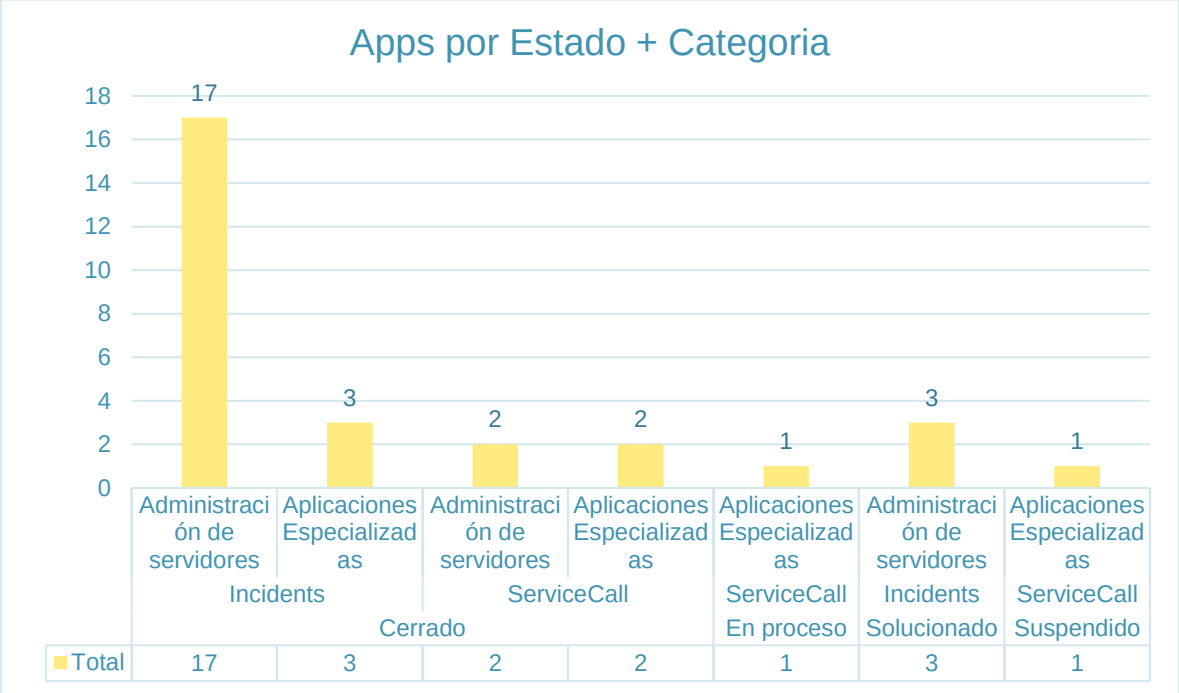


Ilustración *61* Estado final de casos – Aplicaciones Especializadas

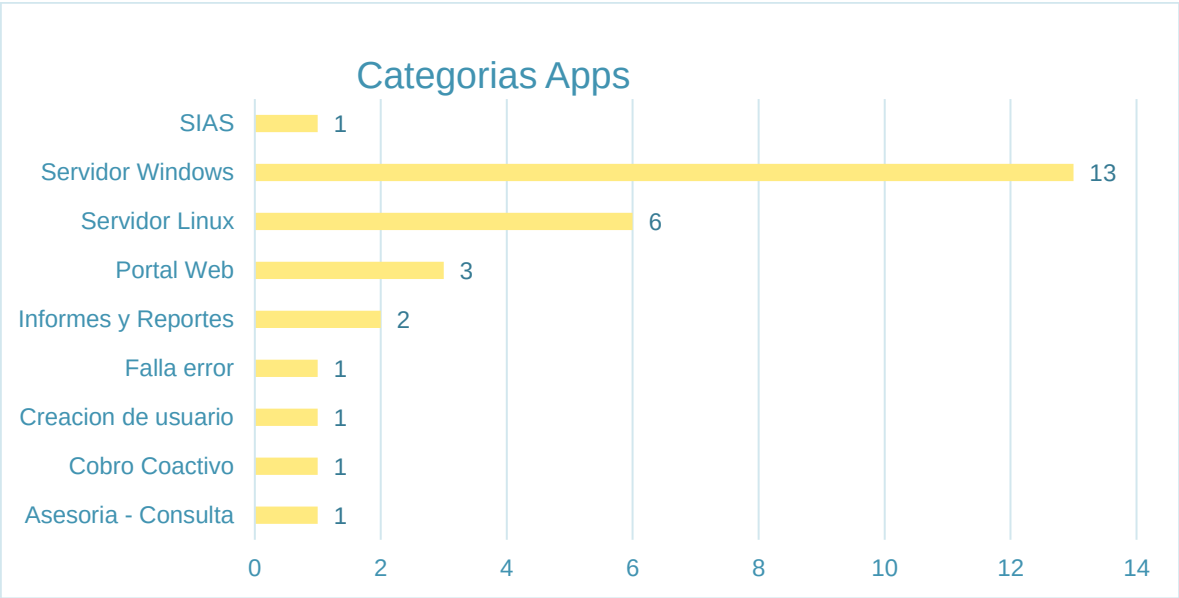


Ilustración 62 categorías Apps

Tras todas estas circunstancias, se realizaron sesiones de seguimiento con el equipo funcional por parte de Ministerio del trabajo, en donde se definieron tres escenarios para los sistemas de información SIAS, RUI, MiGestión y FILCO.

FILCO: Se definieron actividades a corto plazo para poner en disponibilidad la información que requiere el área de Empleo que anteriormente mostraba en FILCO, pero debido al incidente no es posible poner nuevamente en disponibilidad la aplicación.

- El área de empleo se compromete a remitir los links de los tableros de Power BI para que el equipo de Servicio Centrales realice la creación de un micrositio en el portal de la entidad, embebiendo en Frames los reportes para disponibilidad en la pagina Web de la entidad.
- Agendamiento por parte del equipo de Empleo para revisión de los demás componentes DSpace, Postgress y demás que permiten el funcionamiento de SAMPL y FILCO.

RUI: Se definieron actividades a corto plazo para poner en disponibilidad el sistema de información de manera interna estrictamente.

- Se definió flujo para creación de usuarios en el dominio para ingreso por VPN a RUI.
- Se creo perfil de VPN especial para asignación a usuarios de RUI (externos a la entidad).
- El área se compromete a validar el desarrollo y actualización de la aplicación durante la vigencia 2025 en cumplimiento de los estándares de seguridad y desarrollo de software.
- La aplicación ya fue puesta en producción finalizando el mes de marzo tras diversos análisis del equipo SOC, y realizando aprovisionamiento de la Infraestructura necesaria para dar gestión a la solicitud de RUI

SIAS: Un escenario similar al de RUI, en donde la aplicación se deja operativa únicamente dentro de la red del Ministerio del trabajo.

- Se realiza apagado de la máquina de balanceo NGNIX que genero el inconveniente, se deja tráfico centralizado hacia uno de los dos servidores de frontend de SIAS.
- El área se compromete a validar el desarrollo y actualización de la aplicación durante la vigencia 2025 en cumplimiento de los estándares de seguridad y desarrollo de software.
- Se definió flujo para creación de usuarios en el dominio para ingreso por VPN a SIAS por parte de los sindicatos.

Para el escenario de los sistemas de información, tras el contexto anteriormente brindado, se procede a dar el siguiente estado para cada aplicativo:

De manera atenta y en atención a los compromisos adquiridos en las sesiones del:

- 5 de diciembre de 2024 para la aplicación SIAS con la Subdirección IVC
- 17 de diciembre de 2024 para la aplicación FILCO con la Dirección de Empleo
- 20 de diciembre de 2024 para la aplicación RUI de la Oficina de Riesgos Laborales

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

Escenario SIAS:

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

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

Pendientes:

- IVC recopilaría la información de los sindicatos que accederían al sistema para escalar la creación de usuarios VPN que tengan estrictamente acceso a SIAS y a ningún otro recurso tecnológico. Esta información actualmente no ha sido remitida para iniciar con el proceso de creación de usuarios.

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

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

Pendientes:

- El equipo de Empleo tenía como compromiso el envío de los links de cada tablero de Power BI para que el equipo de Servicios Centrales de Soporte informático realizara la creación de un micrositio para embeber en frames los reportes dentro del portal de la entidad. A la fecha no se ha remitido esa información a soporte informático o a la oficina TIC.
- 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.

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

- Poner en disponibilidad la aplicación únicamente dentro de la red interna del Ministerio del trabajo para que los funcionarios y contratistas de riesgos laborales pudieran acceder a la aplicación.
- Se define flujo de creación de usuarios para los intermediarios de la siguiente manera:
    - Recepción de solicitud de creación de usuario en Riesgos Laborales
    - Reenvió de solicitud a la mesa de servicios por parte de riesgos laborales
    - Creación de usuario en directorio activo con el perfil de VPN respectivamente
    - Envío de información (usuario y contraseña) a riesgos laborales en un medio cifrado. Es importante mencionar que esta metodología siempre se ha venido trabajando para la creación de usuarios y envío de información sensible de acuerdo con la ODI Política de Gestión de Contraseñas del Ministerio del Trabajo ítems 2.5.7 y 2.5.8 indica:
        - “El administrador de cada sistema es responsable de asegurar que las contraseñas que se transmitan a través de redes públicas estén protegidas contra acceso no autorizado mientras se encuentren en tránsito, para este caso se recomienda sean cifradas.”
        - “El usuario es responsable de asegurar la privacidad de las contraseñas asignadas para acceder a los sistemas de información.”

        - Por ende, toda Contraseña, independientemente de su origen o su propósito, debe ser compartida en un medio seguro y cifrado para garantizar la seguridad de acceso.
    - Actualmente las actividades de creación de usuario están siendo canalizadas desde Riesgos laborales hacia la mesa de servicios, esta da respuesta tras la creación del usuario y posteriormente riesgos laborales remite el manual de instalación de cliente VPN, sumando los usuarios y contraseñas emitidos en el caso radicado anteriormente.
    - Los ANS de atención de los casos son los mismos ANS de creación de usuario de Ministerio del Trabajo (16 horas).

Actualmente los sistemas de información SIAS y RUI están operativos únicamente desde la red de Ministerio del Trabajo, FILCO se encuentra en indisponibilidad y a espera del envío de la información solicitada de acuerdo con los compromisos adquiridos.

1. **Solicitud de Acceso**
    - La Dirección de Riesgos Laborales enviará un correo electrónico a **Soporte Informático** con el asunto: **"SOLICITUD VPN RUI"**.
    - En el cuerpo del correo se deberá indicar el nombre del usuario al que se le asignará el acceso VPN.
2. **Creación de la VPN**
    - Soporte Informático procesará la solicitud y, en un plazo de **24 horas**, se configurará el acceso VPN para el usuario indicado.
    - Junto con las credenciales de acceso, se proporcionará el procedimiento detallado para la instalación y configuración de la VPN (adjunto al correo de respuesta).
3. **Duración del Acceso**
    - El acceso VPN tendrá una vigencia de **5 días hábiles**.
    - Una vez transcurrido este periodo, la VPN será desactivada automáticamente.
4. **Renovación de Acceso**
    - En caso de requerir nuevamente acceso al aplicativo RUI, se deberá realizar una nueva solicitud enviando un correo a la Mesa de Ayuda siguiendo el mismo procedimiento descrito.

Notas Importantes:

- Asegúrese de proporcionar la información correcta del usuario para evitar demoras en la configuración.
- Consulte el procedimiento adjunto para garantizar la instalación adecuada de la VPN.

Se dio respuesta al Radicado No. **08SI2025310500000001200**

1. *De las más de 60 solicitudes enviadas, solo se han atendido aproximadamente 30, lo que indica una baja tasa de resolución.*

Respuesta: Esto es de acuerdo con el punto #2 debido a que la información de los requerimientos venía incompleta y se retornaba el caso al solicitante para que fuera documentado de manera adecuada y poder dar gestión sobre la solicitud.

2. *En al menos 20 casos, se han devuelto las solicitudes por falta de Información básica para la creación de usuarios (por ejemplo, nombre completo y cédula de la persona). En*

este caso, la Dirección de Riesgos Laborales contacta a los solicitantes para completar la información.

Respuesta: El retorno de estos requerimientos está asociada a que el solicitante no remite la información estrictamente necesaria para la creación del usuario en Active Directory y VPN, por ende, es importante que el solicitante remita toda la información necesaria en cuanto se escale el requerimiento para dar gestión de la solicitud sin reprocesos.

3. *El proceso actual requiere que los intermediarios instalen una VPN en sus equipos y esperan la creación del usuario y contraseña por parte del soporte informático. Este proceso genera demoras y depende de la disponibilidad del personal técnico.*

Respuesta: El grupo de Soporte Informático y la UT no tienen alcance sobre los equipos informáticos fuera del dominio de Ministerio del Trabajo, por ende, es recomendable que cada usuario cuente con un usuario que realice el acompañamiento, durante la sesión se sugirió el acompañamiento técnico de un contratista de Riesgos Laborales, que haría seguimiento a cada solicitud y apoyaría a los intermediarios en la instalación, configuración y conexión al aplicativo.

4. *Las contraseñas se envían comprimidas en formato 7Zip, pero han surgido dificultades debido a que los responsables no cuentan con la herramienta adecuada para descomprimir los archivos.*

Respuesta: se informa que de acuerdo con la ODI Política de Gestión de Contraseñas del Ministerio del Trabajo ítems 2.5.7 y 2.5.8 indica:
“El administrador de cada sistema es responsable de asegurar que las contraseñas que se transmitan a través de redes públicas estén protegidas contra acceso no autorizado mientras se encuentren en tránsito, para este caso se recomienda sean cifradas.”
“El usuario es responsable de asegurar la privacidad de las contraseñas asignadas para acceder a los sistemas de información.”
Por ende, toda Contraseña, independientemente de su origen o su propósito, debe ser compartida en un medio seguro y cifrado para garantizar la seguridad de acceso. Así como definir el propósito de estas credenciales

5. *El "Manual de Conexión VPN" proporcionado por la mesa de ayuda ha generado problemas, ya que no todos los usuarios cuentan con la capacidad técnica para realizar la instalación correctamente, lo que ha obligado al experto en aseguramiento e intermediación de riesgos laborales a ofrecer soporte adicional, lo cual no corresponde a sus funciones.*

Respuesta: Durante la sesión se sugirió el acompañamiento técnico de un contratista de Riesgos Laborales con experticia técnica, que haría seguimiento a cada solicitud y apoyaría a los intermediarios en la instalación, configuración y conexión al aplicativo.

6. *Algunos intermediarios han enfrentado dificultades con la asignación permisos de navegación en la VPN, lo que requiere intervención man que ha venido realizando el experto en aseguramiento para brindar orientación técnica. Este asunto debería estar en cabeza de la mesa. ayuda de soporte informático.*

Respuesta: Durante la sesión se sugirió el acompañamiento técnico de un contratista de Riesgos Laborales con experticia técnica, que haría seguimiento a cada solicitud y apoyaría a los intermediarios en la instalación, configuración y conexión al aplicativo.

7. *En otros casos, los intermediarios no configuran correctamente la IP de la entidad, lo que retrasa el proceso.*

Respuesta: Durante la sesión se sugirió el acompañamiento técnico de un contratista de Riesgos Laborales con experticia técnica, que haría seguimiento a cada solicitud y apoyaría a los intermediarios en la instalación, configuración y conexión al aplicativo.

8. *Las restricciones de seguridad implementadas por las empresas de los intermediarios dificultan el acceso a la plataforma RUI y esto requiere un soporte de mayor nivel.*

Respuesta: El grupo de Soporte informático y la UT no tiene alcance en las políticas y metodologías de seguridad de cada Intermediario, por lo cual no se podría realizar gestión de excepciones en concreto para cada caso en específico, Durante la sesión se indica que el grupo de Riesgos laborales enviaría un consolidado de los usuarios con esta particularidad y la sintomatología y detalle de cada caso (reportado por el intermediario) para realizar la validación respectiva y determinar hasta donde se podría llegar o que alternativas se podrían explorar.

9. *En algunos casos, incluso después de instalar la VPN, los usuarios no pueden conectarse adecuadamente a la plataforma debido a problemas. técnicos fuera del alcance del personal de riesgos laborales.*

Respuesta: Durante la sesión se sugirió el acompañamiento técnico de un contratista de Riesgos Laborales con experticia técnica, que haría seguimiento a cada solicitud y apoyaría a los intermediarios en la instalación, configuración y conexión al aplicativo.

Tras la puesta en marcha del sistema RUI de contingencia, se desestimarán los procedimientos de VPN y los usuarios accederán a la aplicación a través de RUI | Iniciar Sesión

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 adjunta esa información en este correo para ser validada y posteriormente realizar el contacto.

Nombre App	Acceso actual	Funcionario	Observaciones
Biblioteca Virtual de Trabajo	http://app2.mintrabajo.gov.co/Biblioteca	Javier Mauricio Gomez Mantilla	
Centros de entrenamiento	http://app2.mintrabajo.gov.co/centrosentrenamiento/	Carlos Andres Matañana	
Calculadora Laboral	http://app2.mintrabajo.gov.co/CalculadoraLaboral	Ligia Carrero	
Censo Sindical	http://app2.mintrabajo.gov.co/CensoSindical	Maria Jimena Daza	

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

			actualmente esta productiva
Estado joven	http://app2.mintrabajo.gov.co/estadojoven/	Carlos Andres Matañana	
FTRUTEC	http://app2.mintrabajo.gov.co/ftrutec/	Carlos Andres Matañana	

Tabla 59 Migración actividades .NET

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

También es importante para nosotros como proveedor de servicios tecnológicos abrir estos espacios con las áreas funcionales de manera independiente, porque abre las puertas a una comunicación más fluida como administradores técnicos de los repositorios de estas aplicaciones, ya que nos permite mantener un canal de comunicación directo, actualización de fichas de servicio e identificar los actores necesarios para socializaciones con las gestiones ITIL, por ende es importante establecer estos canales de comunicación directos no solo para las pruebas de migración, sino también para conocer a detalle la dinámica de las áreas con los sistemas de información y articular la gestión realizada desde las gestiones ITIL con cada área responsable de cada aplicativo que se traduce en un CI dentro de la herramienta de gestión ARANDA. De igual forma se comunica que la información de plan de trabajo reposa en el SharePoint del contrato, dentro de la carpeta de Aplicaciones de acuerdo con lo solicitado, el plan de trabajo enmarca las actividades globales para la migración de la totalidad de las aplicaciones. Posterior a brindar esta información, se procede con el agendamiento de sesiones con cada área responsable y se programan inicio de pruebas en nuevos entornos las últimas dos semanas de febrero y la primera semana de marzo de 2025. A la fecha no se ha recibido retroalimentación de las pruebas por las área funcionales, es importante dejar claridad que a nivel de infraestructura y configuración, ya se encuentran aprovisionados y listos los entornos, pero no se puede iniciar migración sin VB de la propia entidad.

Migración Portal Web

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

Esto ocurre cuando un usuario quiere ingresar a un sitio privado como es la intranet, el portal hace la petición al servidor LDAP pero no hay acceso.
Como las conexiones configuradas desde el portal responden de forma exitosa, se procede a ejecutar el proceso de importación de usuarios desde el servidor LDAP hacia el servidor del portal. Este proceso se ejecuta en segundo plano y se reportan los usuarios que no se

pueden importar porque no cumplen algún criterio de los campos que no pueden ser null para Liferay, ej: cuentas de servicio, cuentas de usuario que no tiene email, etc.
Con la ejecución del proceso se pueden ver en el log errores de cuentas que no puede importar porque no cumplen con algún criterio.
Se realizaron pruebas con mi usuario y genero error de no cumplir con el criterio de email, así como de otros usuarios que se les solicito probar. Se le solicito al Ing. Elkin Morales que realizara el ajuste a mi cuenta desde el servidor LDAP agregándole mi correo min trabajo para probar y efectivamente una vez actualizada ya no genera error puedo ingresar, pero no tengo permisos sobre la intranet.
Realizado lo anterior se solicitó al usuario del requerimiento validar que efectivamente pueda ingresar a la intranet, se espera su respuesta.
En atención a los compromisos definidos en la sesión del día 26 de febrero de 2025 categorizados de la siguiente forma:

- Se realizo la migración de forma exitosa a versión 7.2 sin afectación del servicio o corrupción de información
- Envío de Información/Ajustes por parte del equipo de Empleo sobre los tableros de FILCO publicados en el ambiente de pruebas de la página web de la entidad para que los cambios puedan aplicarse en el marco de la migración y puedan salir a producción con la nueva versión del portal. Se sostiene reunión a espera de formalización de los ajustes requeridos
- Confirmación del espacio (fecha) con el equipo de empleo que hace uso de DSpace para validar la alternativa de implementación de FileNet para este componente. Sesión que se realizará en abril 2025.
- Confirmación del espacio (fecha) con el equipo de empleo para validar los temas relacionado con migración de componentes STATA a RStudio y Python. No se ha confirmado por parte de Empleo.

- **GESTOR DOCUMENTAL**

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

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

Plataforma - Aplicaciones

- Consultas lentas a los índices sobre los objetos de búsqueda de las tareas que se tiene en el portal de trabajo.
- Lentitud en la carga de información sobre las diferentes pantallas del proceso.
- Tener instancias innecesarias activas de proceso, generan peso a la aplicación ya que tiene toda la información cargada en el cache del servidor.
- No realizar borrado de los Documentos temporales de los File System en los diferentes servidores, se llenarían los espacios de almacenamiento y no permiten carga de más documentos y ejecución correcta de la plataforma.

- El no reinicio de las diferentes instancias del servidor de aplicaciones, ocasiona que se queden hilos pegados y hace que el procesamiento de los servidores físicos, estén en un alto procesamiento, esto genera lentitud y bloqueo de la plataforma.

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

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

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

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

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

Los tamaños de los tablespaces tienden a consumir más espacio antes de los periodos de los mantenimientos, aunque los valores de uso de los tablespaces no están en valores de alerta es necesario mantener valores amplios de estos objetos para periodos de alta demanda transaccional de la aplicación, esto garantiza que las transacciones y procesos del gestor documental puedan ser gestionados óptimamente y garantizando la disponibilidad 100%. Históricamente los tiempos de resolución de solicitudes de la aplicación mejoran considerablemente después de las tareas de mantenimiento, los tiempos pueden mejorar de manera significativa si se realiza los mantenimientos de forma periódica, esto con el fin de mantener la aplicación en todos sus componentes funcionando de la mejor manera para brinda un mejor servicio.

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

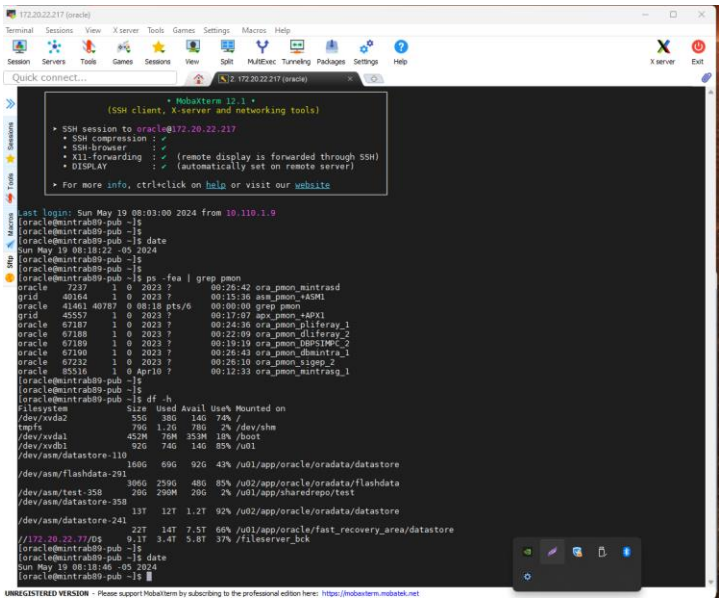


Ilustración 63 Estado pre-ventana

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

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

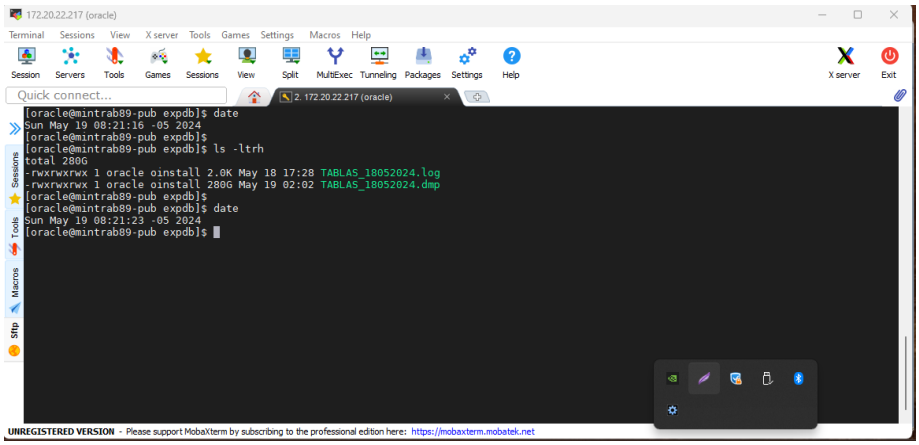


Ilustración 64 Generación de Backups DDBB

Validación tablas:

- **Tabla STORED_SYMBOL_TABLE:**

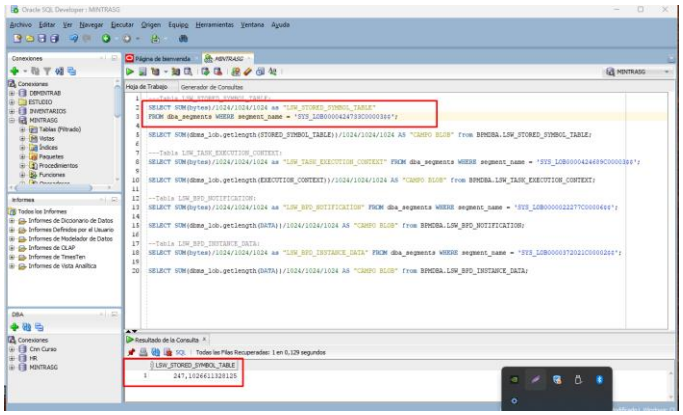


Ilustración 65 Validación Tablas DDBB

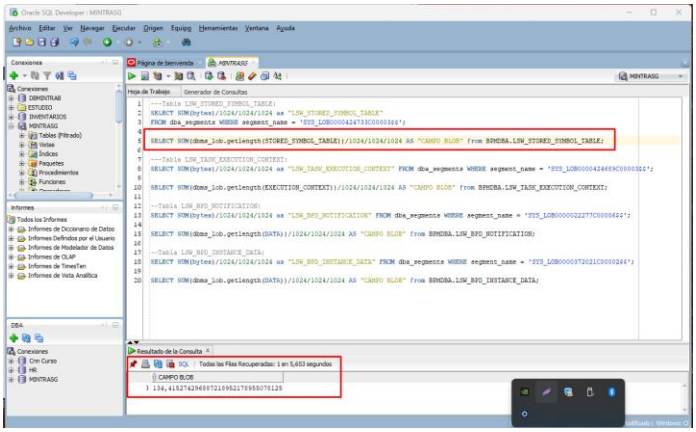


Ilustración 66 Validación Tablas DDBB

- **Tabla LSW_TASK_EXECUTION_CONTEXT:**

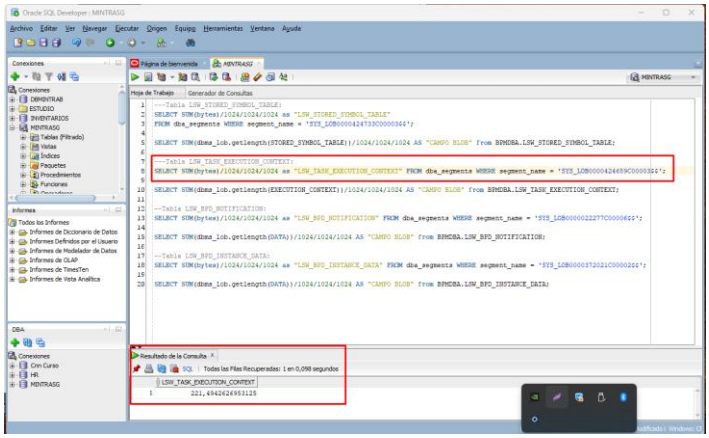


Ilustración 67 Validación Tablas DDBB

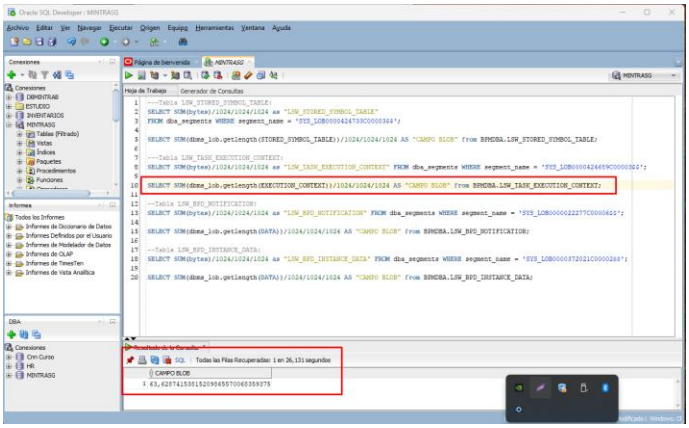


Ilustración 68 Validación Tablas DDBB

- **Tabla LSW_BPD_NOTIFICATION:**

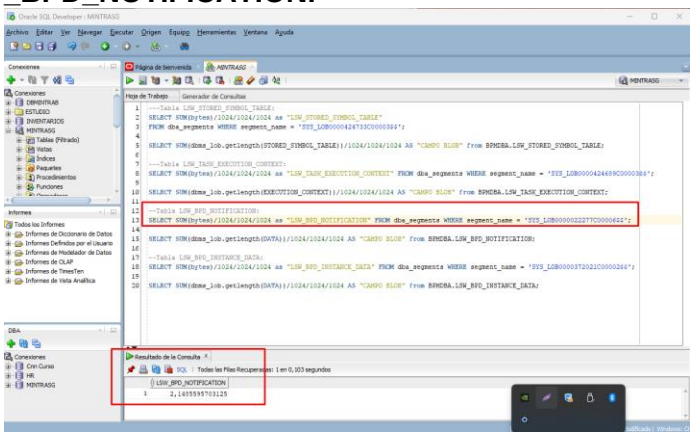


Ilustración 69 Validación Tablas DDBB

- **Tabla LSW_BPD_INSTANCE_DATA:**

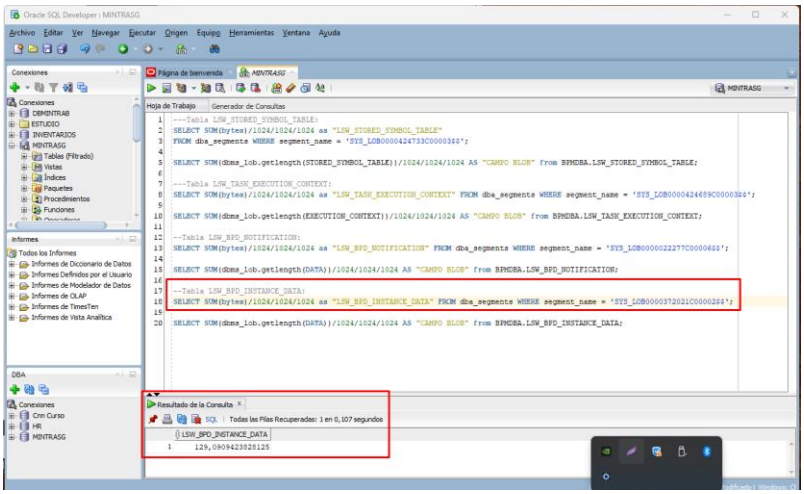


Ilustración 70 Validación Tablas DDBB

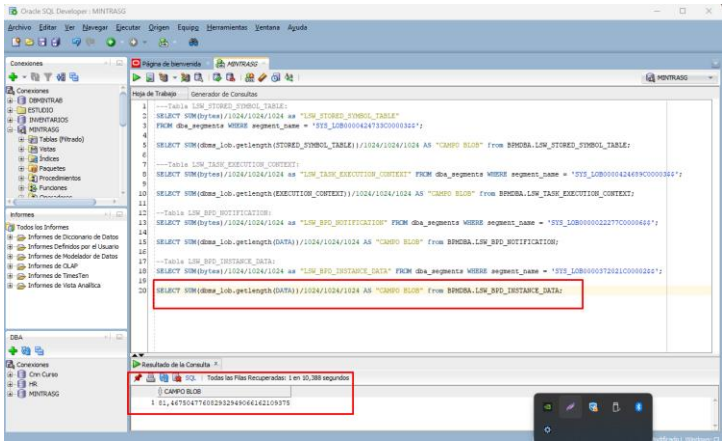


Ilustración 71 validación Tablas DDBB

- **Proceso colocar tablas en cero**

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

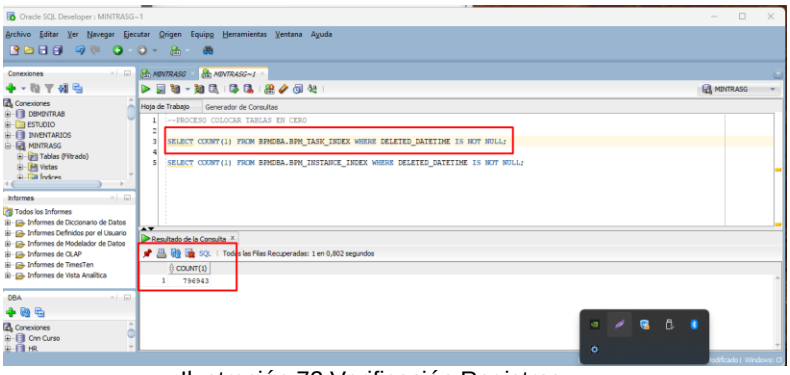


Ilustración 72 Verificación Registros

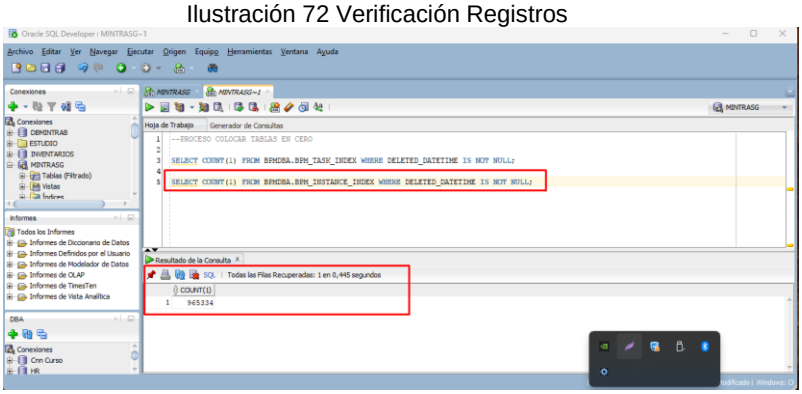


Ilustración 73 Verificación Registros

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

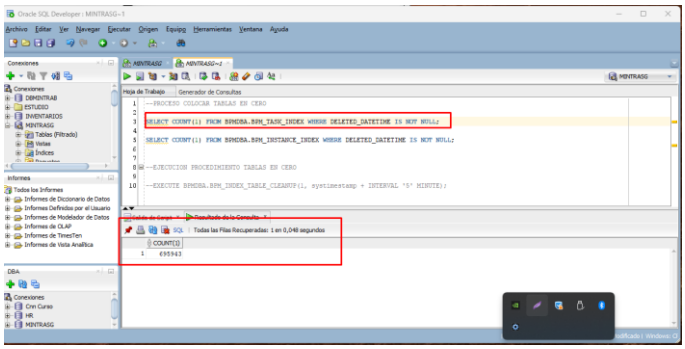


Ilustración 74 Verificación Registros tras ejecución de procesos

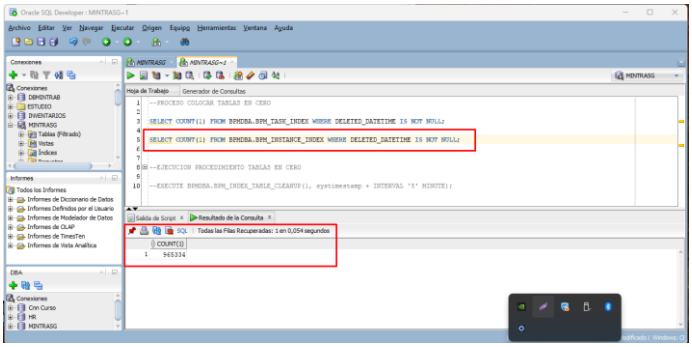


Ilustración 75 Validación de estado de tablas tras ejecución de procesos

- **Validar estatus de las instancias**

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

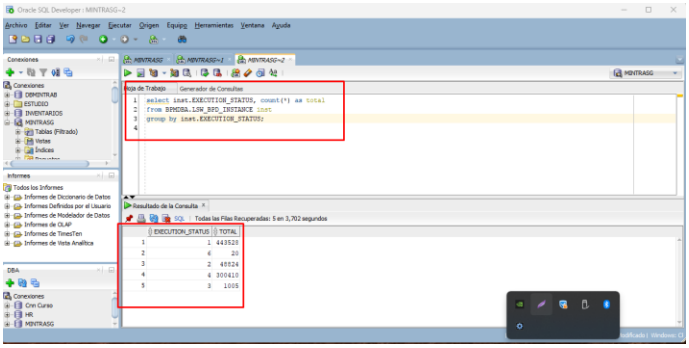


Ilustración 76 Estado de instancias DDDB

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

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

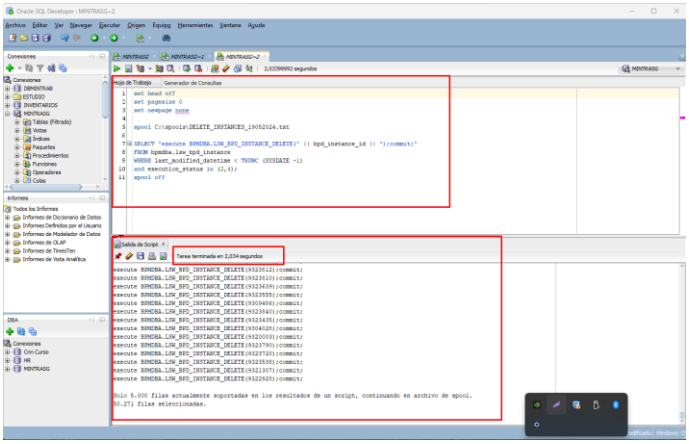


Ilustración 77 Eliminación de instancias

Se ejecutó scripts de eliminación de instancias según consulta anterior:

Validación de las instancias después de haber realizar el borrado

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

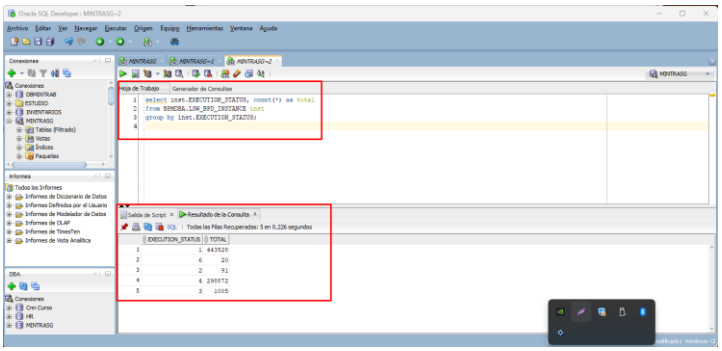


Ilustración 78 Disminución de instancias tras ejecución de proceso

Estado del servidor antes de la desfragmentación de tablas:

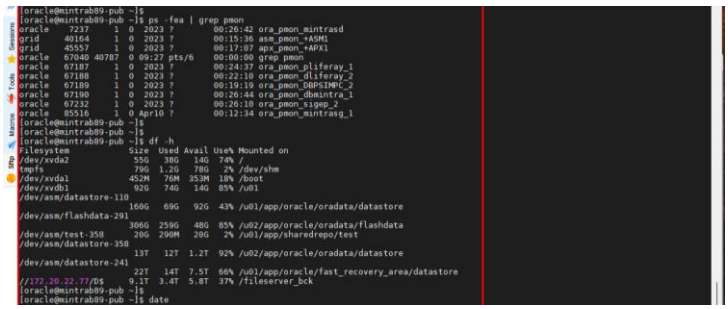


Ilustración 79 Estado del servidor - pre-desfragmentación

Proceso de desfragmentación de tablas del esquema BPMDBA:

BPMDBA.LSW_STORED_SYMBOL_TABLE
BPMDBA.LSW_TASK_EXECUTION_CONTEXT
BPMDBA.LSW_BPD_NOTIFICATION

BPMDBA.LSW_BPD_INSTANCE_DATA
Ejecución de scripts proceso de desfragmentación:

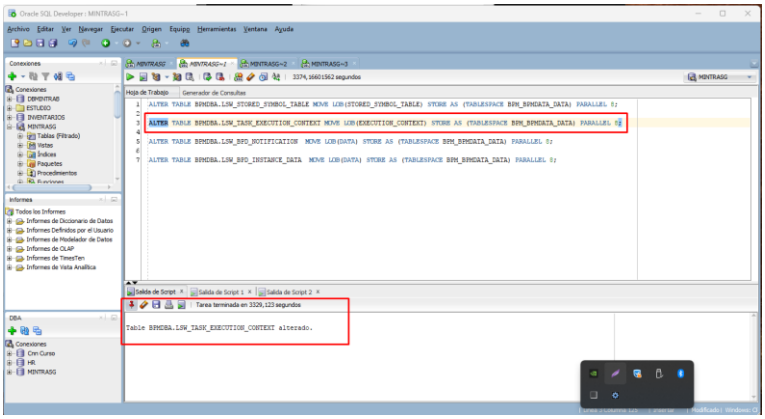


Ilustración 80 Ejecución desfragmentación

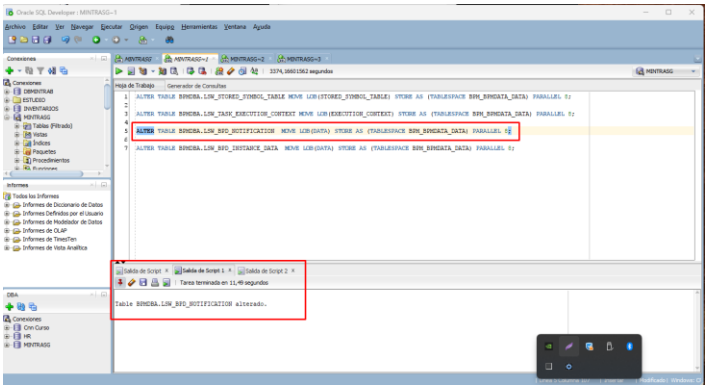


Ilustración 81 Ejecución desfragmentación

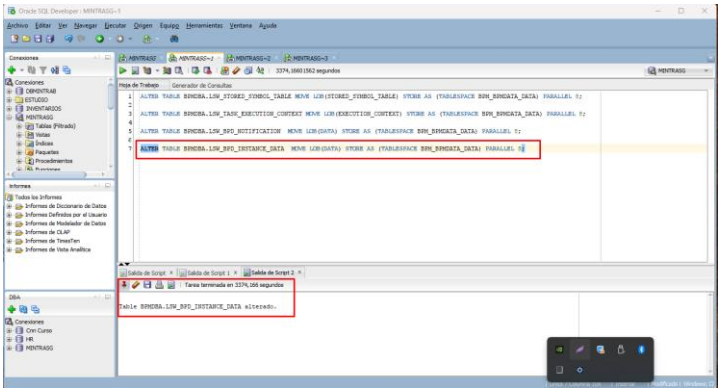


Ilustración 82 Ejecución desfragmentación

- **Reconstrucción de índices:**

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

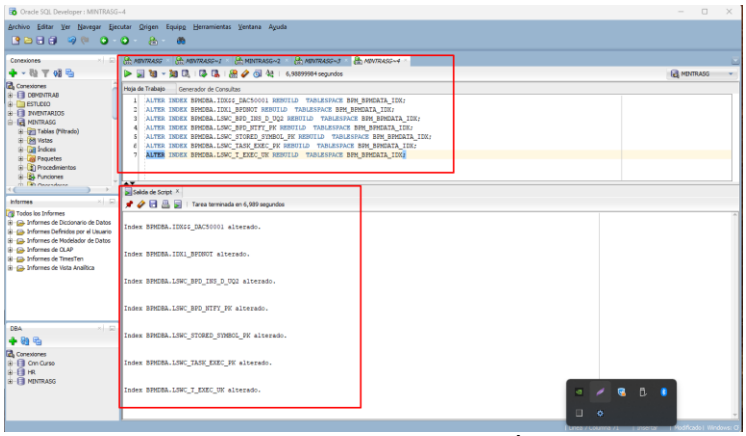


Ilustración 83 Reconstrucción de Índices

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

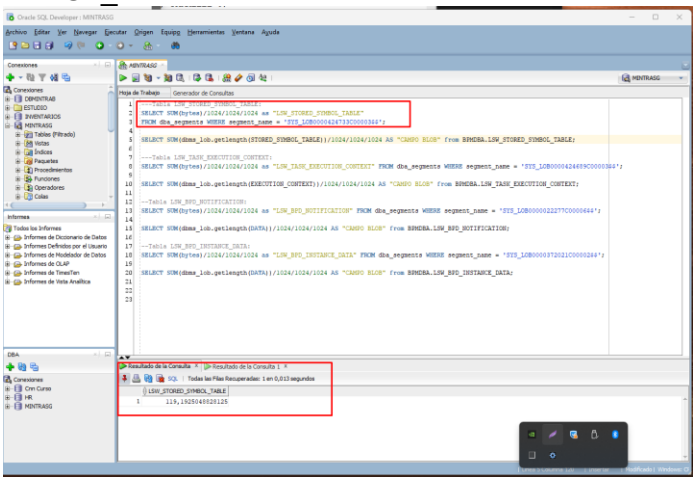


Ilustración 84 Validación de tamaños de tablas

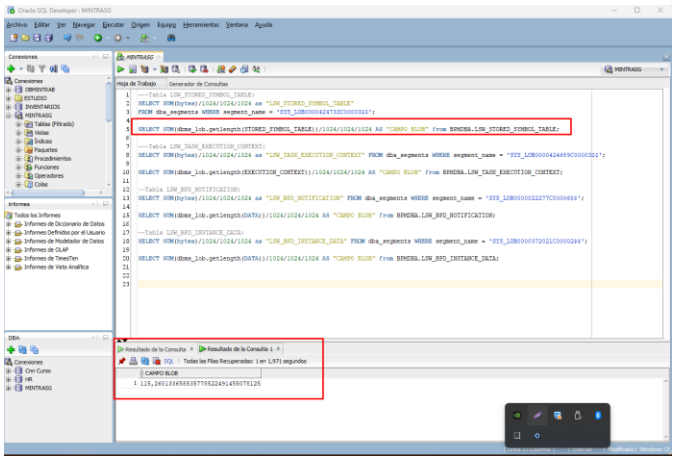


Ilustración 85 Validación de tamaños de tablas

- **Tabla LSW_TASK_EXECUTION_CONTEXT:**

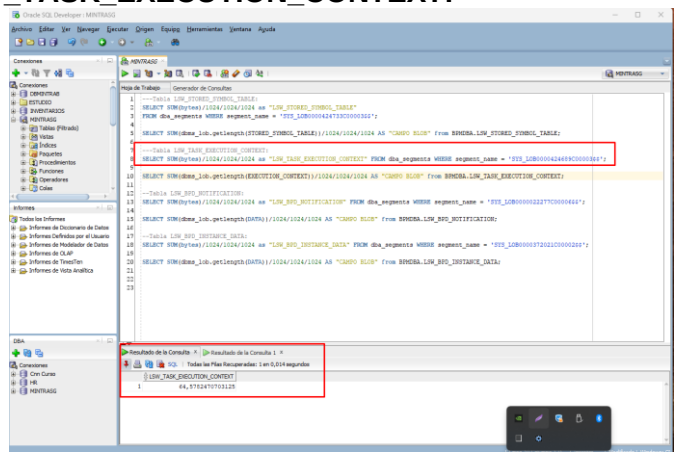


Ilustración 86 Validación de tamaños de tablas

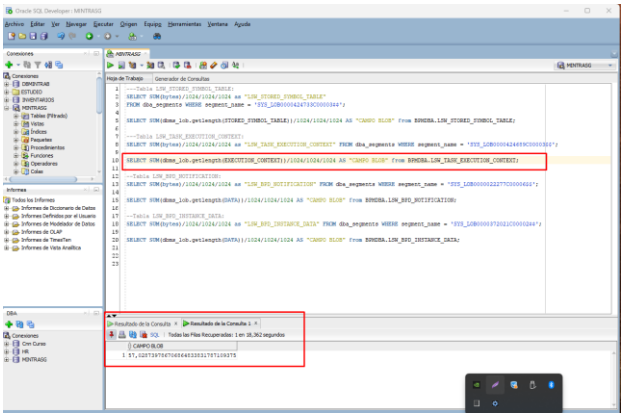


Ilustración 87 Validación de tamaños de tablas

- **Tabla LSW_BPD_NOTIFICATION:**

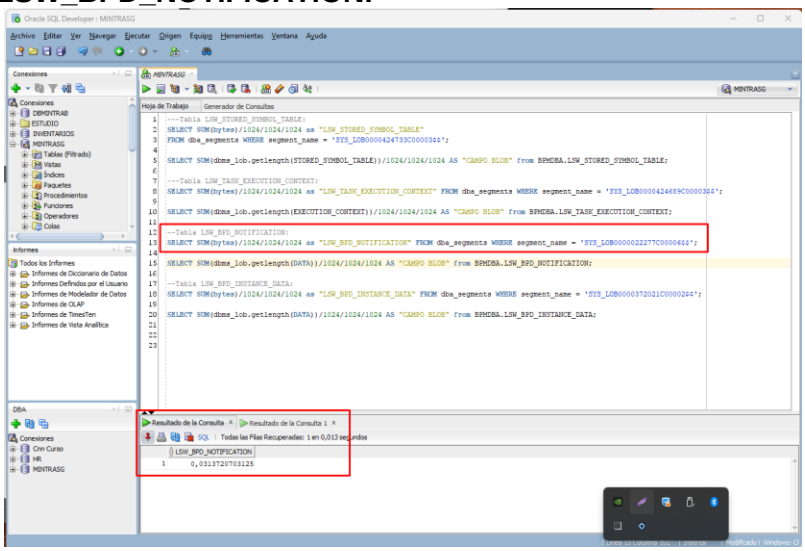


Ilustración 88 Validación de tamaños de tablas

- **Tabla LSW_BPD_INSTANCE_DATA:**

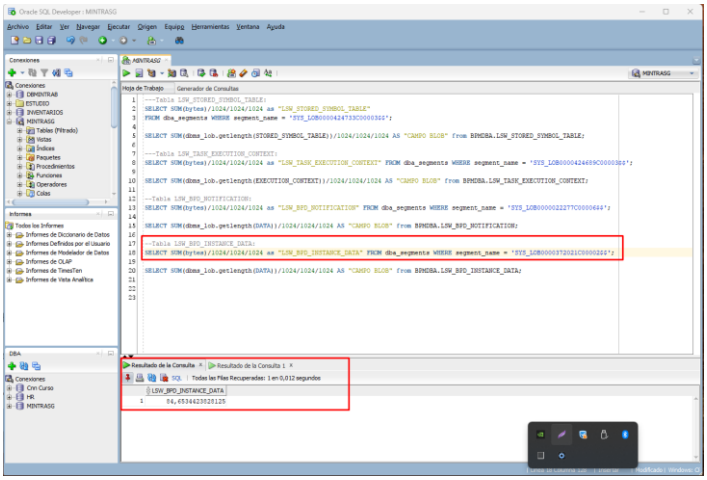


Ilustración 89 Validación de tamaños de tablas

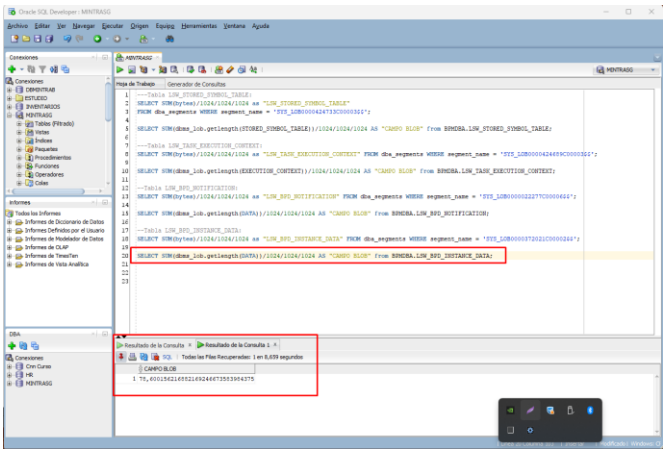


Ilustración 90 Validación de tamaños de tablas

Ejecución de estadísticas sobre las tablas antes desfragmentadas

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

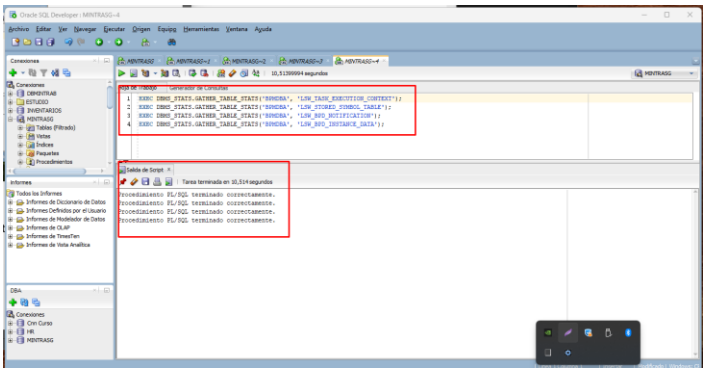


Ilustración 91 Ejecución de estadísticas de validación

Se procedió subir servicios de aplicación, donde se confirmó funcionalidad del sistema.

Se procede a ejecutar estadísticas para que el optimizador de consultas tome decisiones informadas sobre cómo ejecutar las consultas de manera más eficiente. Las estadísticas proporcionan información sobre la distribución de datos, la cardinalidad de las columnas y otros detalles que ayudan al optimizador a generar planes de ejecución más eficientes.
Se procedió a subir servicios de aplicación, donde se confirmó funcionalidad del sistema. El promedio de usuarios conectados al Gestor ha sido de 320 al mismo tiempo. Se presentan las estadísticas de los últimos 3 meses:

Mes	Suma de Total Instancias
Enero 2025	111854
Febrero 2025	149070
Marzo 2025	148829
Total acumulado	**409753**

Mes	Suma de Total Documentos
Enero 2025	149454
Febrero 2025	183729
Marzo 2025	193697
Total acumulado	**527380**

Mes	Suma de Total radicados
Enero 2025	59197
Febrero 2025	70194
Marzo 2025	72317
Total, acumulado	**201708**

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

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

Tabla 60 Dimensionamiento Servers IBM - Virtualización Optima

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

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

Ilustración 92 Distribución de licencias Oracle

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

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

Ilustración 93 Licencias ambientes

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



Ilustración 94 Estado final casos GD

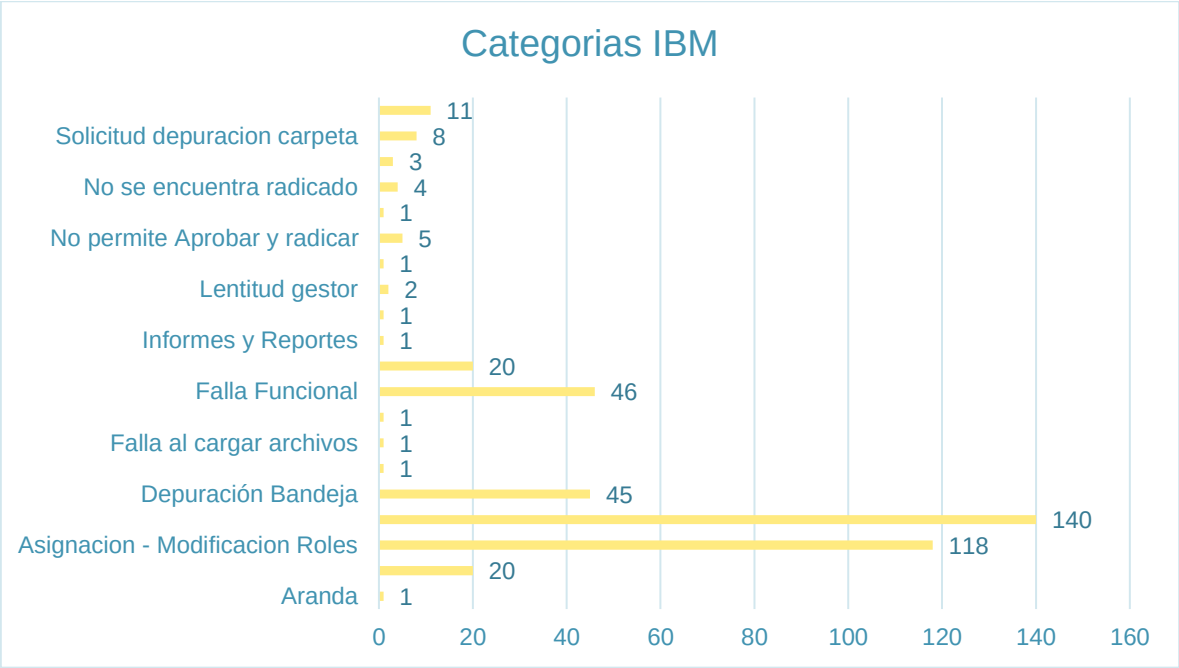


Ilustración 95 categoría DDBB

- **Estado de las Bases de Datos**

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

Se han presentado diferentes controles de cambios para las bases de datos alojadas y soportadas por MSSQL, cambios relacionados con ventanas de mantenimiento, estabilización, Backup, migraciones de versión y de base de datos, reinicios asociados a ventanas de mantenimiento, ejecución de scripts entre otras actividades descritas dentro de cada RFC. Según las acciones de mejora identificadas en cada ventana de mantenimiento, se han construido documentos, topologías e informes asociados a las indisponibilidades (asociadas a ventanas de mantenimiento, procesos de estabilización de proceso de bases de datos y afinamiento de servicio) de los servicios soportados desde bases de datos. Se realizó el cargue de los archivos planos recibidos vía FTP desde el Ministerio de Salud dicha tarea se realizó sobre las tablas que ya están definidas para ser cargadas en la Base de Datos de PILA. Como es de conocimiento del área funcional en el proceso de actualización para la tabla PLANILLA arrojo error, en caso de necesitar alguna modificación o realizar de nuevo el cargue por favor crear un nuevo caso. Se anexa un archivo en Excel llamado Cargue_Tablas_Pila.xlsx con la información de las tablas actualizadas a la fecha, otro archivo llamado LOG_EVENTOS_20240728.txt con el LOG de filas cargadas en cada una de las tablas; además de un archivo llamado SALIDA_TSX_2024-07-29.pdf con imágenes como evidencia de los cargues realizados.

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 supervisión 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 se está listo para dar el paso de migración tanto de OS como de versión de DDBB.

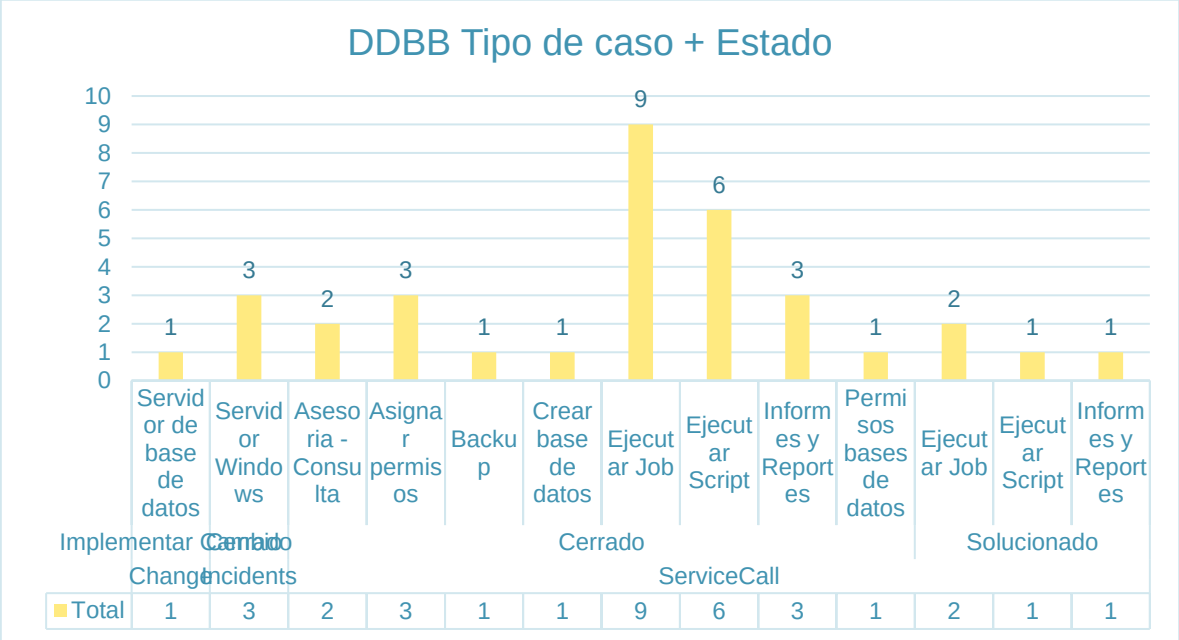


Ilustración 96 casos DDBB

- **Estado de las Bases de Datos – Oracle Gestor Documental**

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

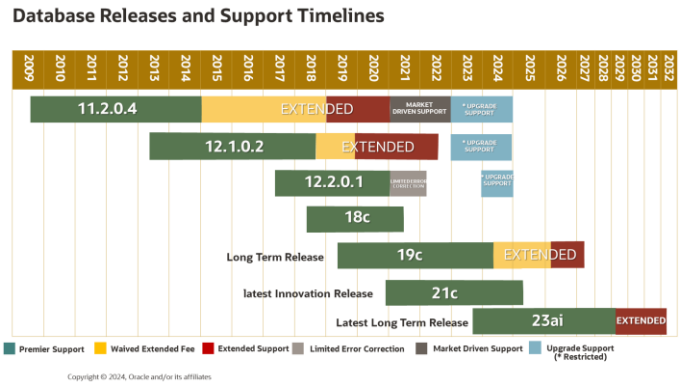


Ilustración *97* Estado Bases de Datos

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 61 Apps & DDBB Oracle

En este apartado la información no es exacta dado que no se cuenta con un soporte donde se especifique que aplicaciones hacen uso de una base de datos o esquemas al detalle, lo que se tiene son las conexiones de servidores de aplicación Weblogic que tienen un apuntamiento sobre bases de datos del ODA x5-2 detalladamente.

Es importante mencionar que, ante un escenario de virtualización, las recomendaciones de fabrica a nivel de asignación de recursos/capacidades están asociadas a las capacidades de la infraestructura que ofrece como fabricante, es decir, las capacidades de un ODA X-10 HA suelen ser las recomendadas para cubrir un escenario de alta disponibilidad y de

crecimiento de servicios. El crecimiento de las capacidades está directamente relacionado con el crecimiento de los componentes Oracle/DDBB de la propia entidad.

De acuerdo con el escenario actual de base de datos, se anexan las capacidades del ODA X-5 aprovisionado por la entidad y el uso de las capacidades para cada componente de DDBB, es decir lo disponible en el hardware de Oracle y el usado por las máquinas virtuales y bases de datos que permiten el funcionamiento actual tanto del gestor documental como de otras aplicaciones que tienen base de datos Oracle:

INST_NAME	IP	SERVER_NAME	AMBIENTE	Version_Motor	S.O	MEMORIA GB	CPU	STORAGE ASIG GB	STORAGE USED GB	STORAGE FREE GB
mintrasg_1	172.20.22.217	mintrab89-pub	PRODUCCION	Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	Oracle Linux 4.9.2-6.2.0.3	40	12	5677	1713	3964
pliferay_1	172.20.22.217	mintrab89-pub	PRODUCCION	Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	Oracle Linux 4.9.2-6.2.0.3	4	2	235	139	95
dbmintra_1	172.20.22.217	mintrab89-pub	PRODUCCION	Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	Oracle Linux 4.9.2-6.2.0.3	8	4	2225	1967	257
DBPSIMPC_2	172.20.22.217	mintrab89-pub	PRODUCCION	Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	Oracle Linux 4.9.2-6.2.0.3	2	2	47	5	42
sigep_2	172.20.22.217	mintrab89-pub	PRODUCCION	Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	Oracle Linux 4.9.2-6.2.0.3	20	8	265	81	184
dliferay_2	172.20.22.217	mintrab89-pub	DESARROLLO	Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	Oracle Linux 4.9.2-6.2.0.3	4	4	151	71	80
mintrasd	172.20.22.217	mintrab89-pub	DESARROLLO	Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	Oracle Linux 4.9.2-6.2.0.3	2	16	390	186	204
dbmintrab	172.20.22.107	mintrab32	PRODUCCION	Oracle Database 11g Enterprice edition Release 11.2.0.1.0	Windows Server 2012 R2	13	10	41	19	22
inventarios	172.20.22.107	mintrab32	PRODUCCION	Oracle Database 11g Enterprice edition Release 11.2.0.1.0	Windows Server 2012 R2	13	10	14	7	7

Tabla 62 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 63 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 98 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 99 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 100 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 101 Estadísticas Pool compartido

Tamaño base de datos MINSTRASG:

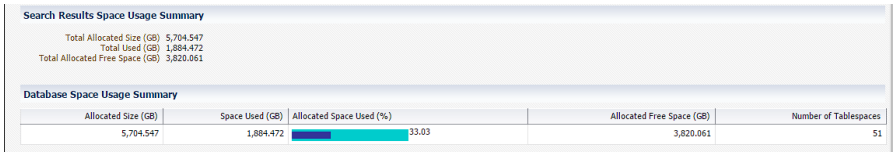


Ilustración 102 Tamaño DDBB

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 103 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

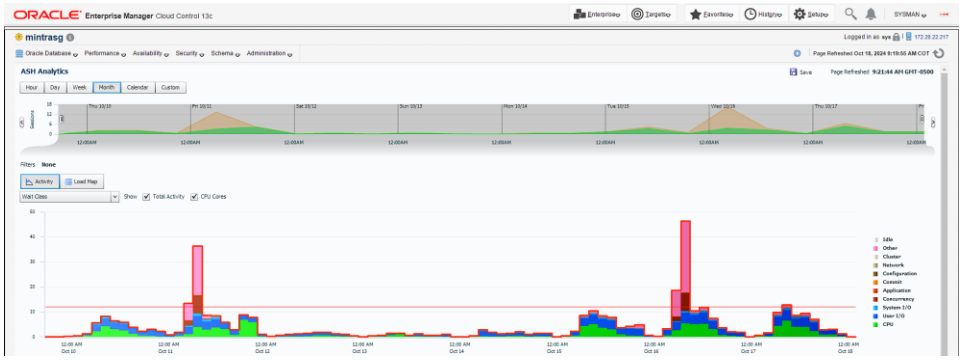


Ilustración 104 Rendimiento DDBB

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 105 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 106 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 107 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 108 Estadística Shared Pool

Tamaño base de datos DBMINTRA:

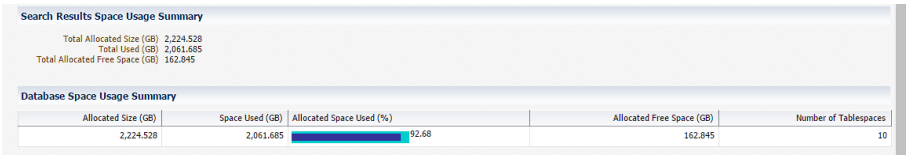


Ilustración 109 Tamaño DDBB DBMINTRA

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 110 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

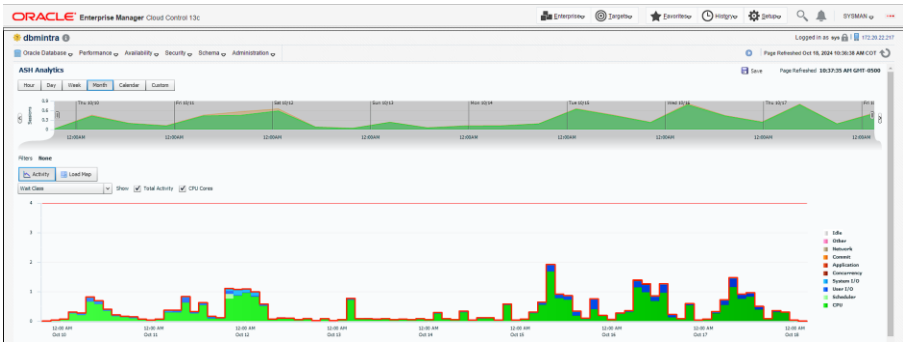


Ilustración 111 Rendimiento DDBB MINTRASG

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 112 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 113 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 114 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 115 Estadísticas Shared Pool

Tamaño base de datos PLIFERAY:

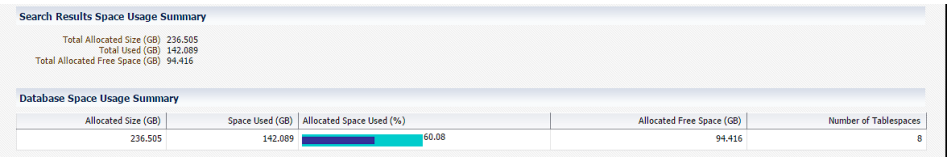


Ilustración 116 Tamaño DDBB PLifeRay

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 117 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

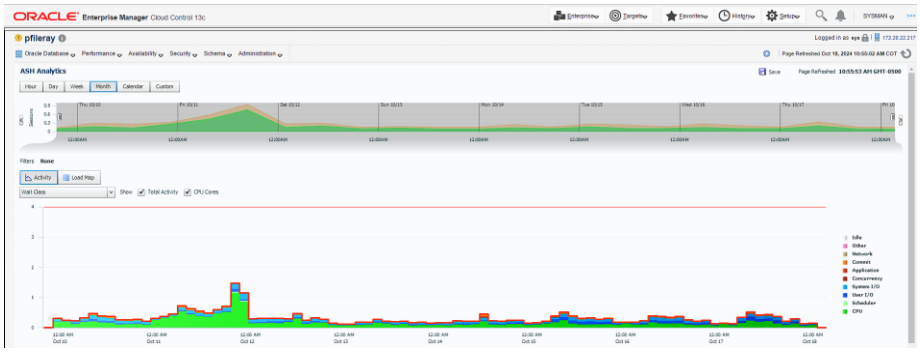


Ilustración 118 Rendimiento DDBB PlifeRay

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 119 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 120 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 121 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 122 Estadística Shared Pool

Tamaño base de datos SIGEP:

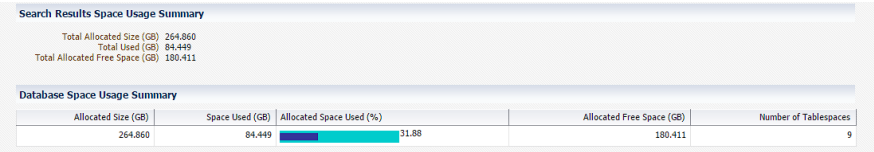


Ilustración 123 Tamaño DDBB SIGEP

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 124 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

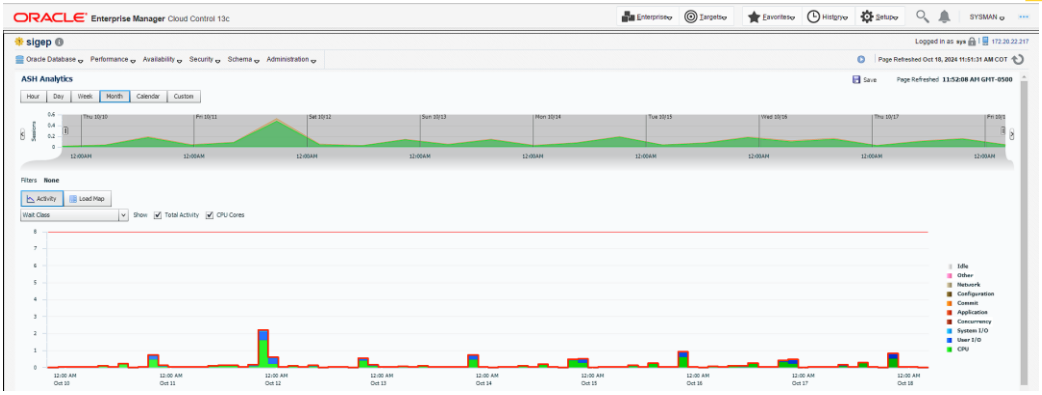


Ilustración 125 Rendimiento DDBB SIGEP

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 126 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 127 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 128 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 129 Estadística Shared Pool

Tamaño base de datos DBSIMPC:

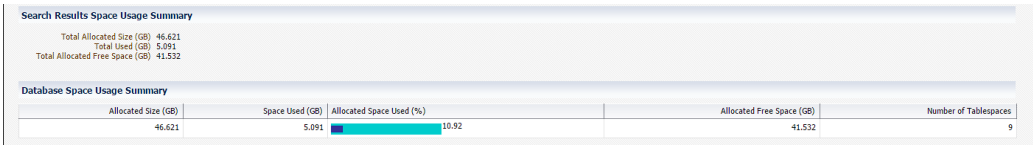


Ilustración 130 Tamaño DDBB SIMPC

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 131 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

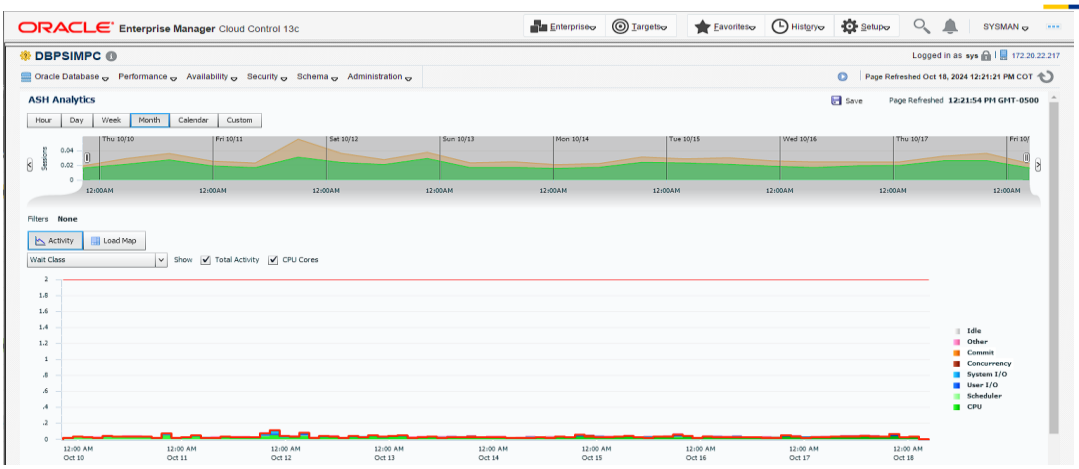


Ilustración 132 Rendimiento DDBB

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 133 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 134 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 135 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 136 Estadística Shared Pool

Tamaño base de datos MINTRASD:

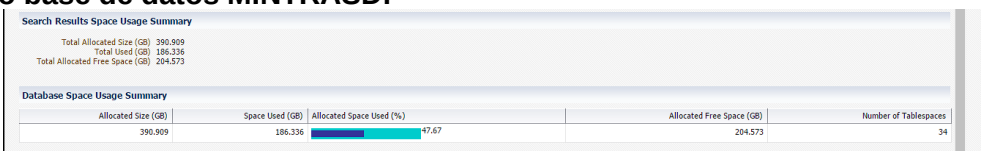


Ilustración 137 Tamaño DDBB MINTRASD

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

Tamaño de esquemas de base de datos:

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

Ilustración 138 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

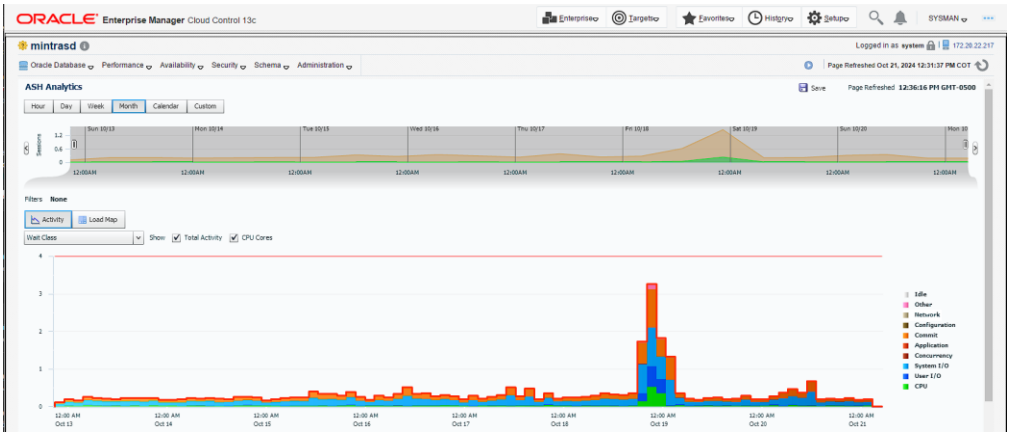


Ilustración 139 Rendimiento MINTRASD

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 140 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 141 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 142 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 143 Estadística Shared Pool

Tamaño base de datos MINTRASD:

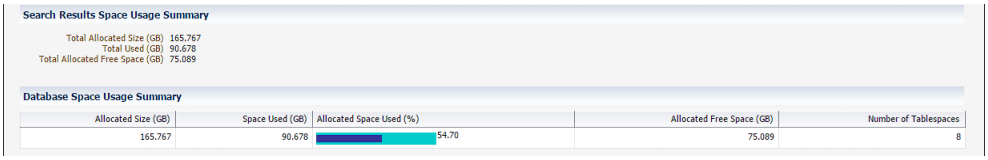


Ilustración 144 Tamaño DDBB

Actualmente la BD MINTRASD tiene parametrizada 165,767 GB a nivel de almacenamiento de los cuales 90,678 GB están en uso y se tiene libre 75,089 GB.

Tamaño de esquemas de base de datos:

ESQUEMA	SIZE_GB
SIMPCPRU	23,3
TLIFERAY	22,55
LIFERAYPRU	22,12
LIFERAYPRO	19,25
SYS	2,5
NEWIVCMT	0,74
AUDSYS	0,15
XDB	0,06
SYSTEM	0,03
WMSYS	0,01
EMPRENDIMIENTOP	0,01
MT_DEFENSA	0
OUTLN	0
DBSNMP	0
GSMADMIN_INTERNAL	0

Ilustración 145 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

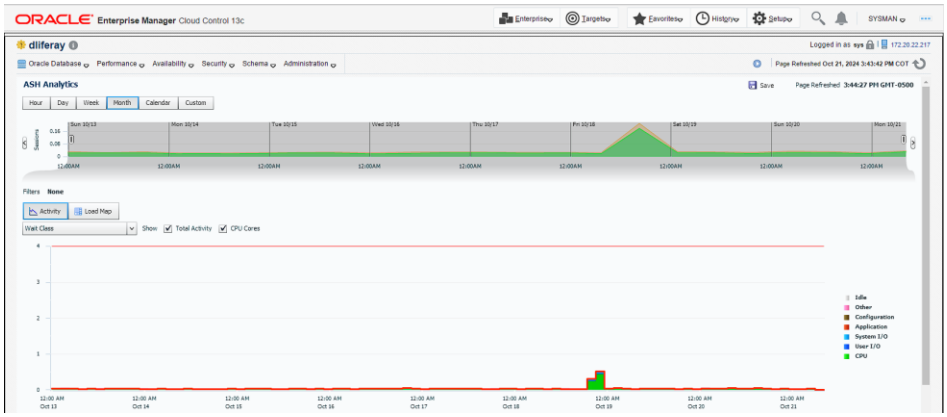


Ilustración 146 Rendimiento DDBB

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 147 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 148 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 149 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 150 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 151 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 152 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

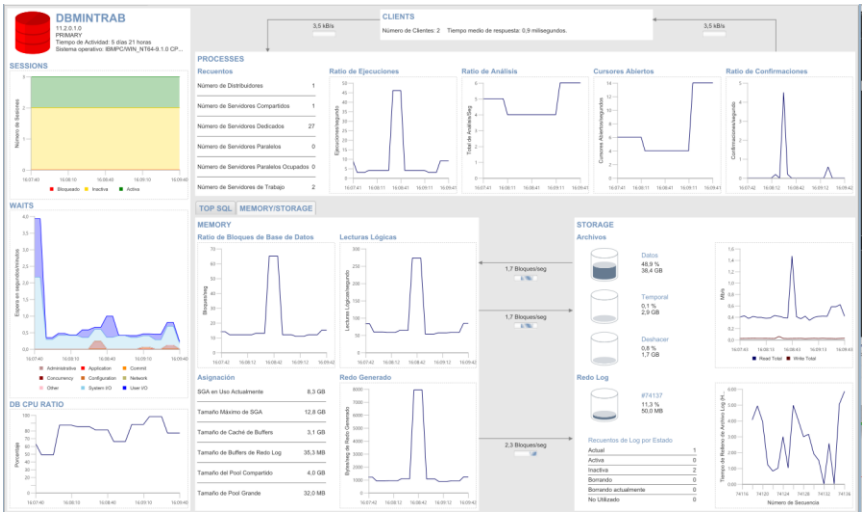


Ilustración 153 Rendimiento DDBB

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 154 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 155 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 156 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 157 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 158 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

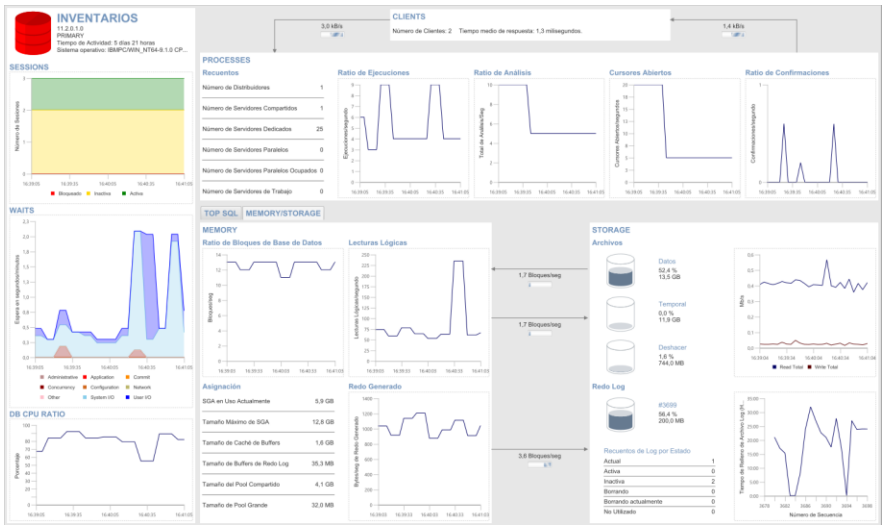


Ilustración 159 Comportamiento DDBB

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

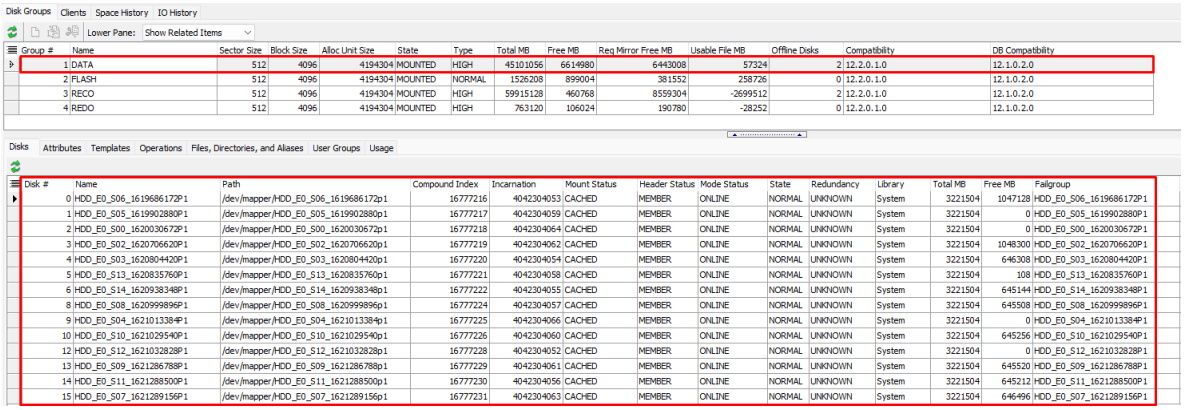
4.1 Almacenamiento General ASM:

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 160 Almacenamiento ASM

DISKGROUP DATA:

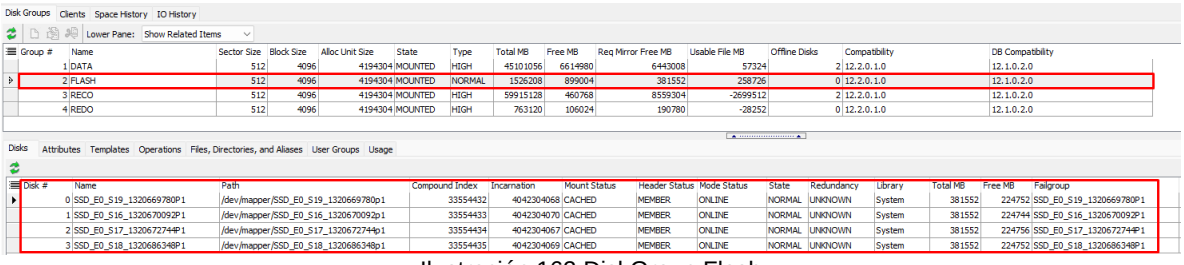


Group #	Name	Sector Size	Block Size	Alloc Unit Size	State	Type	Total MB	Free MB	Req Mirror Free MB	Usable File MB	Offline Disks	Compatibility	DB Compatibility
1	DATA	512	4096	4194304	MOUNTED	HIGH	45101056	6614980	6443008	57324	2	12.2.0.1.0	12.1.0.2.0
2	FLASH	512	4096	4194304	MOUNTED	NORMAL	1526208	899004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

Disk #	Name	Path	Compound Index	Incarnation	Mount Status	Header Status	Mode Status	State	Redundancy	Library	Total MB	Free MB	Failgroup
0	HDD_E0_S06_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 161 DiskGroup Data

DISKGROUP FLASH:



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

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

Ilustración 162 DiskGroup Flash

DISKGROUP RECO:

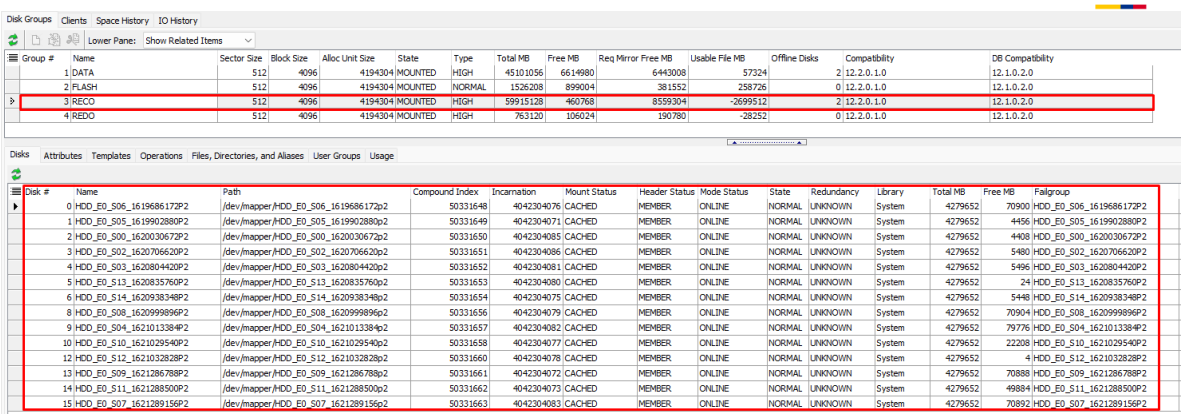


Ilustración 163 DiskGroup Reco

DISKGROUP REDO:

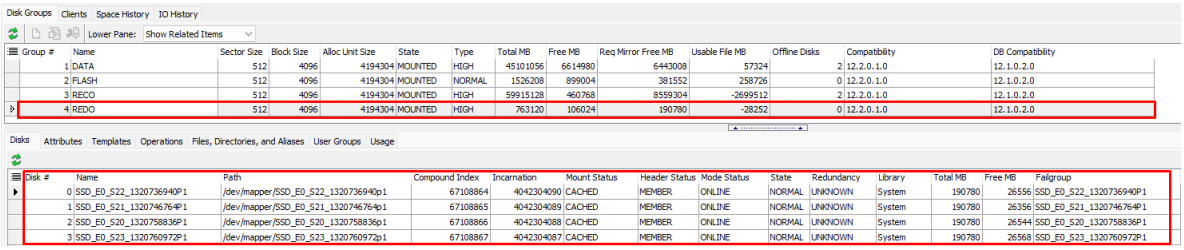


Ilustración 164 DiskGroup Redo

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 165 Licenciamiento adicional componente IBM

3.1.5. **No aplica**

3.1.6. Seguridad Informática

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

3.1.6.1. Firewalls de nueva generación

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

seguridad sólidas para proteger contra amenazas externas, realizando ajustes según las necesidades específicas del Ministerio de Trabajo.

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

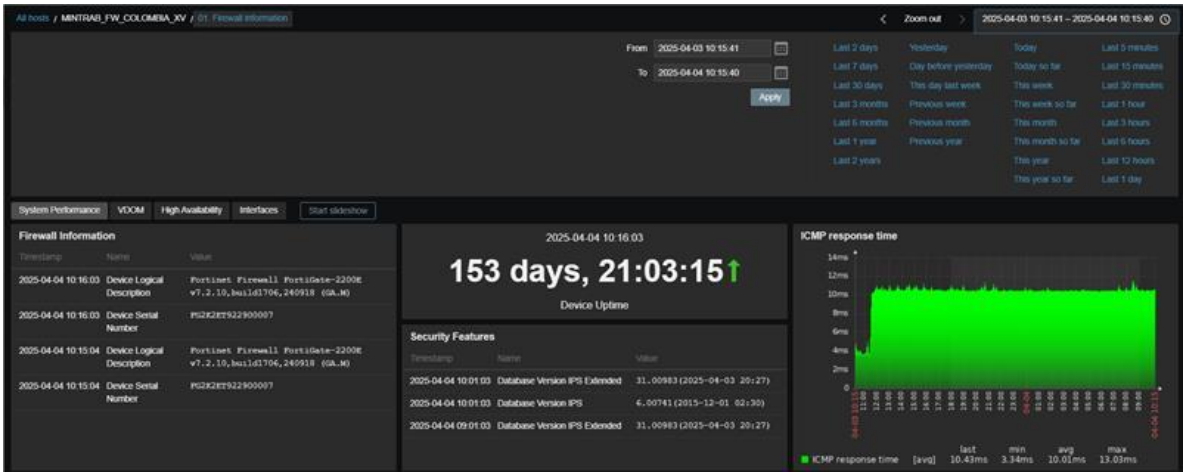


Ilustración166 Disponibilidad firewall

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

Ancho de Banda

Esta imagen presenta un resumen del uso de ancho de banda y el número de sesiones durante el período del mes de marzo. Este análisis del resumen de ancho de banda proporciona una visión clara de los patrones de uso durante el periodo, permitiendo una mejor gestión y planificación de los recursos de red.

Máximo Consumo: El punto más alto del consumo de ancho de banda se aproxima a los 3 TB.

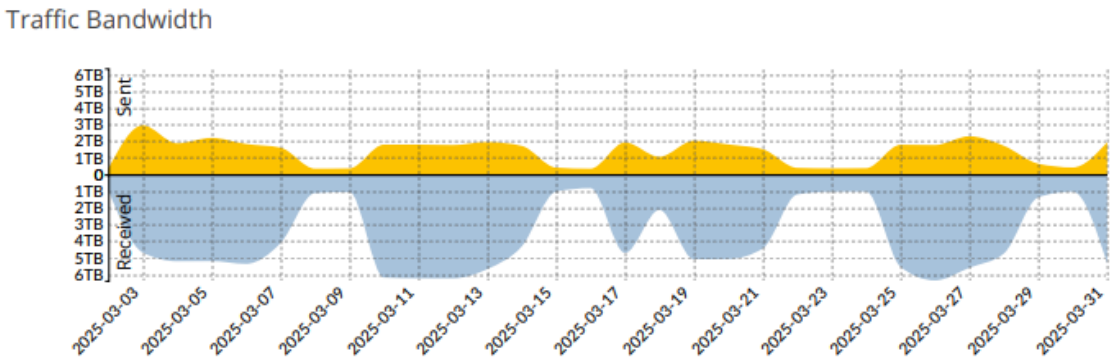


Ilustración167 Comportamiento ancho de banda

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 marzo. La

identificación de los 10 principales usuarios de ancho de banda proporciona información valiosa sobre los patrones de uso de la red y los puntos críticos de congestión.

A continuación, se detallan los hallazgos más relevantes:

Top Users by Bandwidth

#	User(or IP)	Bytes	Sent	Received
1	172.28.28.38			6.02 TB
2	serviciosgestor			5.38 TB
3	172.20.22.32			2.49 TB
4	172.16.64.12			2.43 TB
5	172.20.22.7			2.24 TB
6	172.20.22.179			1.89 TB
7	172.20.22.251			1.86 TB
8	172.24.40.12			1.45 TB
9	172.24.40.15			1,013.55 GB
10	10.200.1.35			851.30 GB

Ilustración 168 Reporte consumo ancho de banda

Top de usuarios por número de sesiones

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

Top Users by Sessions

#	User (or IP)	Sessions
1	172.25.0.5	243,279,973
2	172.20.22.234	45,779,744
3	FORTINET	33,800,517
4	172.20.22.3	24,624,981
5	172.20.22.32	20,306,220
6	172.20.22.40	19,722,697
7	172.20.22.228	13,172,779
8	vulnerabilidadindra	11,886,257
9	172.50.0.2	8,098,623
10	172.50.0.1	8,098,456

Ilustración169 Top de usuarios

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

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

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	HTTPS			38.36 TB
2	SMB			33.32 TB
3	SYSLOG			8.78 TB
4	Microsoft.Portal			6.33 TB
5	TCP/1521			6.27 TB
6	HTTP			5.90 TB
7	Microsoft.SharePoint			4.10 TB
8	HTTPS.BROWSER			3.59 TB
9	Microsoft.Outlook			3.24 TB
10	Microsoft.365.Portal			2.68 TB

Ilustración 170 Top tráfico de aplicaciones

Observación	Descripción
Mayor Uso de Ancho de Banda	- Microsoft Portal 6.33GB, indicando alta actividad colaborativa.
	- **Microsoft** SharePoint 4.00 TB, reflejando la importancia de servicios de red seguros y transferencia de archivos seguros y transferencia de archivos.

Tabla 64 *Top tráfico de aplicaciones*

Categoría de Aplicaciones por Ancho de banda

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

Principales Aplicaciones por Ancho de Tráfico:

- **Colaboración (Collaboration)**:
  Es la categoría con el mayor uso de ancho de banda, alcanzando un total de 9.52 **TB**.
- Las aplicaciones más destacadas en esta categoría son:
  - **Microsoft Portal**: 6.33 TB
  - **Microsoft SharePoint**: 4.10 TB

- **SMB (Server Message Block)** es un **protocolo de red** utilizado para compartir archivos, impresoras y otros recursos entre dispositivos en una red, principalmente en sistemas Windows. También permite la comunicación entre clientes y servidores en redes locales (LAN): 33.32 TB de uso de ancho de banda.

Top 15 Authenticated Logins by VPN Connections

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

Authenticated Logins

#	User	Type	First Used	Total Number of Connections	Total Duration Connected(HH:MM:SS)
1	cjimenez	ssl-tunnel	2025-03-02 15:12:29	131	146:18:04
2	dfdiazd@noc_indra	ssl-tunnel	2025-03-02 00:09:41	120	657:46:56
3	jmaestre	ssl-tunnel	2025-03-03 07:35:45	104	151:53:19
4	ablanco	ssl-tunnel	2025-03-03 06:57:17	103	130:40:13
5	melucumi	ssl-tunnel	2025-03-03 08:26:13	87	101:02:54
6	jmartinezs	ssl-tunnel	2025-03-03 07:35:09	76	129:17:11
7	ewalteros	ssl-tunnel	2025-03-02 00:05:24	72	97:32:00
8	jcalderonf	ssl-tunnel	2025-03-02 16:13:07	72	88:44:26
9	ocardonas	ssl-tunnel	2025-03-03 06:34:54	68	141:07:43
10	jdduque	ssl-tunnel	2025-03-02 00:08:49	68	155:59:28
11	rmurcia	ssl-tunnel	2025-03-02 13:03:34	62	57:31:39
12	eyreyes	ssl-tunnel	2025-03-03 08:27:16	62	185:00:42
13	jespinosam	ssl-tunnel	2025-03-02 00:08:20	60	222:29:22
14	lbricenos	ssl-tunnel	2025-03-03 08:37:05	58	148:06:29
15	cfino	ssl-tunnel	2025-03-02 00:35:18	57	76:12:43

Ilustración 171 Top 15 Authenticated Logins by VPN Connections

Usuarios con Uso Frecuente:

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

Failed Login Attempts by User

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

Failed Login Attempts

#	User	Type	Total Number of Failed Attempts
1	admin	ssl-web	2,015
2	administrator	ssl-web	1,240
3	Admin	ssl-web	588
4	Administrator	ssl-web	298
5	Service	ssl-web	211
6	fortinet	ssl-web	146
7	frontdesk	ssl-web	139
8	print	ssl-web	135
9	itadmin	ssl-web	134
10	scanner	ssl-web	133

Ilustración 172 Failed Login Attempts by User

Intentos Fallidos Significativos:

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

3.1.6.2. Sandbox – Amenazas día 0

El servicio de Sandbox para el Ministerio del Trabajo se utiliza para crear entornos aislados y seguros donde se pueden ejecutar archivos o programas sospechosos para analizar su comportamiento. La función principal del Sandbox es detectar y analizar posibles amenazas de seguridad, como malware o software malicioso, sin comprometer la seguridad del sistema principal. Para el mes de marzo de 2025, se generaron 87 eventos analizados, los cuales fueron limpiados de algún tipo de amenazas

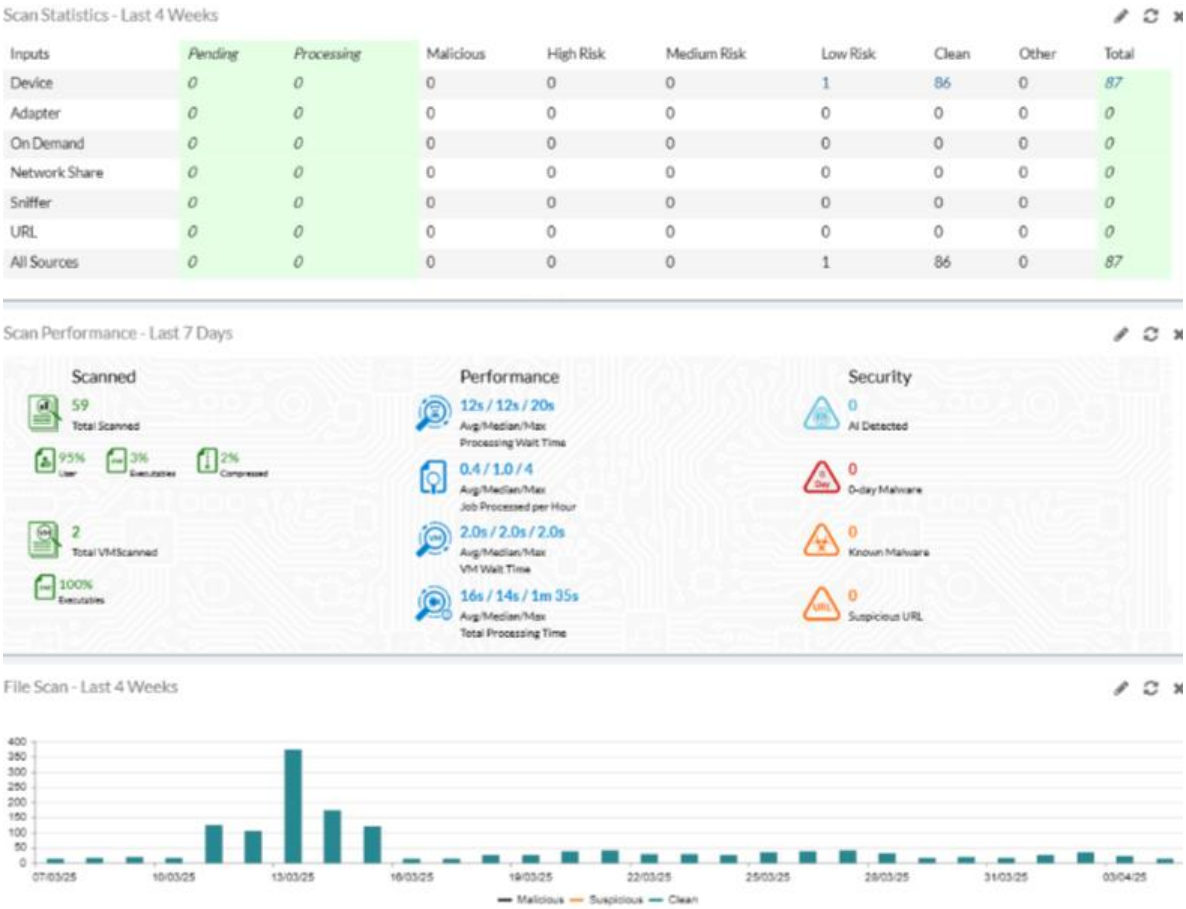


Ilustración 173 estadísticas de escaneo

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

Performance

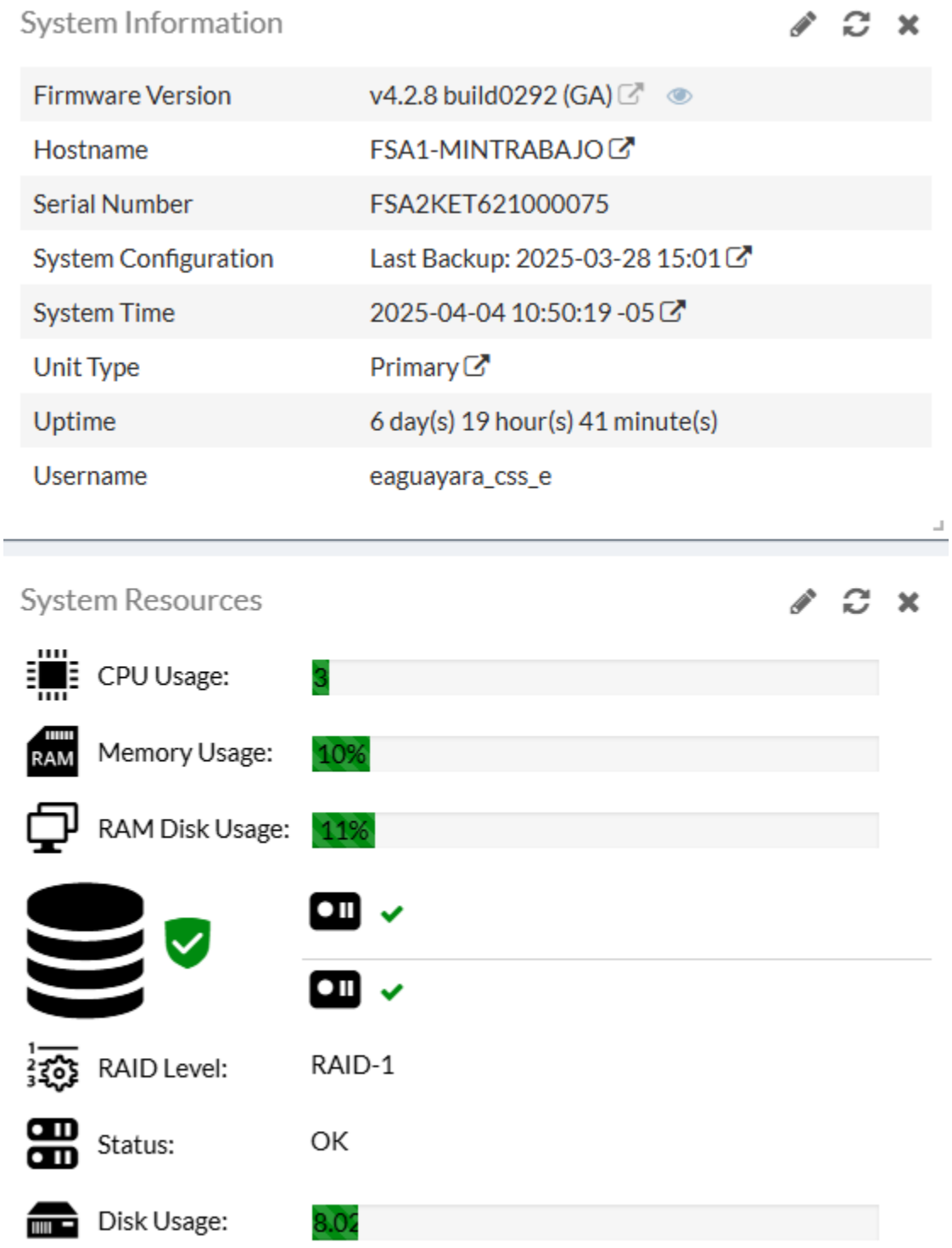


Ilustración 174 performance

Licencia Sandbox

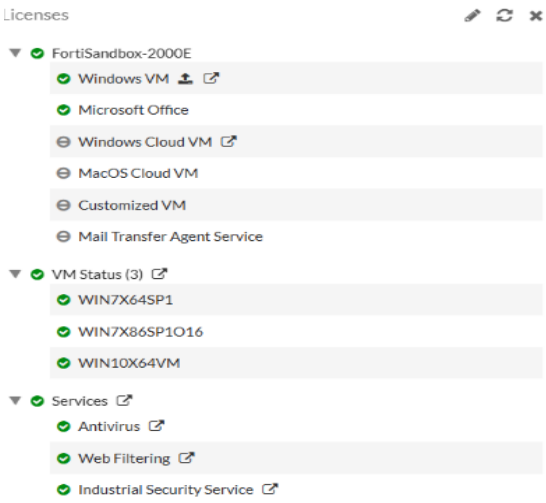


Ilustración 175 Licenciamiento

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

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

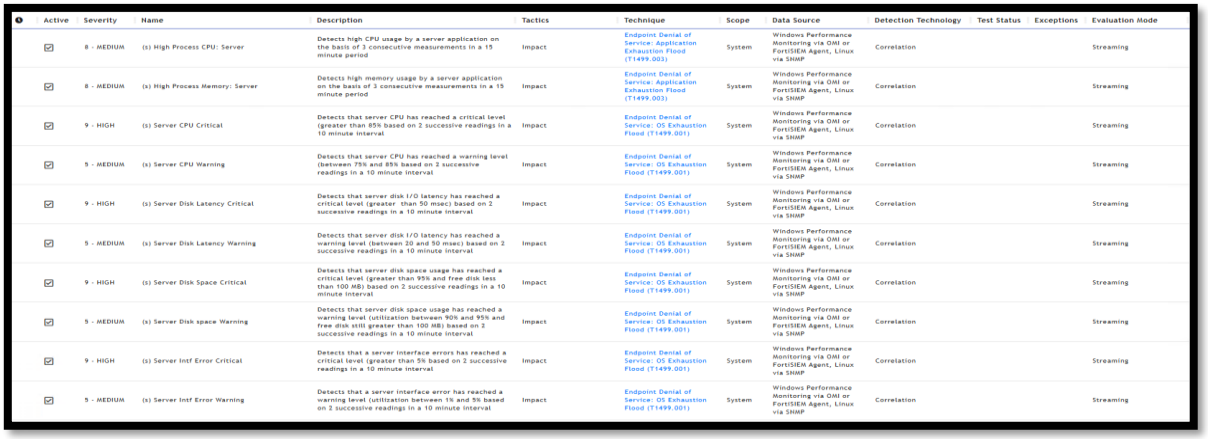
A continuación, se detallan algunos ítems particulares.

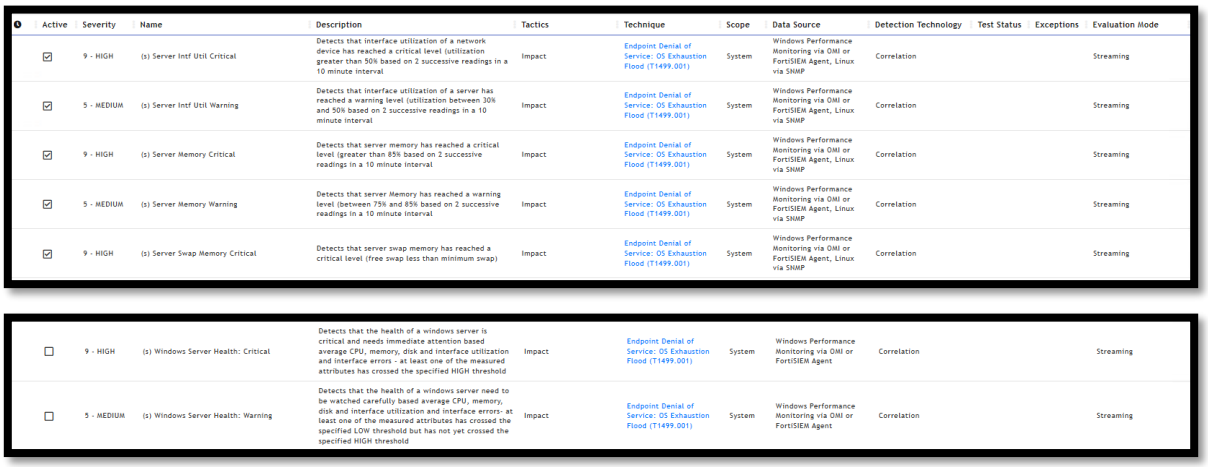
3.1.6.3.1. Casos de uso Fortisiem

Desempeño (performance)

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

A continuación, se detallan algunos ítems particulares:





Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☑	9 - HIGH	(s) Server Intf Util Critical	Detects that interface utilization of a network device has reached a critical level (utilization greater than 50% based on 2 successive readings in a 10 minute interval	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent, Linux via SNMP	Correlation			Streaming
☑	5 - MEDIUM	(s) Server Intf Util Warning	Detects that interface utilization of a server has reached a warning level (utilization between 30% and 50% based on 2 successive readings in a 10 minute interval	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent, Linux via SNMP	Correlation			Streaming
☑	9 - HIGH	(s) Server Memory Critical	Detects that server memory has reached a critical level (greater than 85% based on 2 successive readings in a 10 minute interval	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent, Linux via SNMP	Correlation			Streaming
☑	5 - MEDIUM	(s) Server Memory Warning	Detects that server Memory has reached a warning level (between 75% and 85% based on 2 successive readings in a 10 minute interval	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent, Linux via SNMP	Correlation			Streaming
☑	9 - HIGH	(s) Server Swap Memory Critical	Detects that server swap memory has reached a critical level (free swap less than minimum swap)	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent, Linux via SNMP	Correlation			Streaming
☐	9 - HIGH	(s) Windows Server Health: Critical	Detects that the health of a windows server is critical and needs immediate attention based average CPU, memory, disk and interface utilization and interface errors - at least one of the measured attributes has crossed the specified HIGH threshold	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent	Correlation			Streaming
☐	5 - MEDIUM	(s) Windows Server Health: Warning	Detects that the health of a windows server need to be watched carefully based average CPU, memory, disk and interface utilization and interface errors- at least one of the measured attributes has crossed the specified LOW threshold but has not yet crossed the specified HIGH threshold	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)	System	Windows Performance Monitoring via OMI or FortiSIEM Agent	Correlation			Streaming

Ilustración 176 Casos de uso

3.1.6.3.2. Disponibilidad (Availability)

Los casos de uso de disponibilidad en FortiSIEM están diseñados para garantizar que los sistemas y servicios críticos estén disponibles y funcionando de manera óptima. Se muestran los casos de disponibilidad configurados para el Ministerio de Trabajo:



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

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

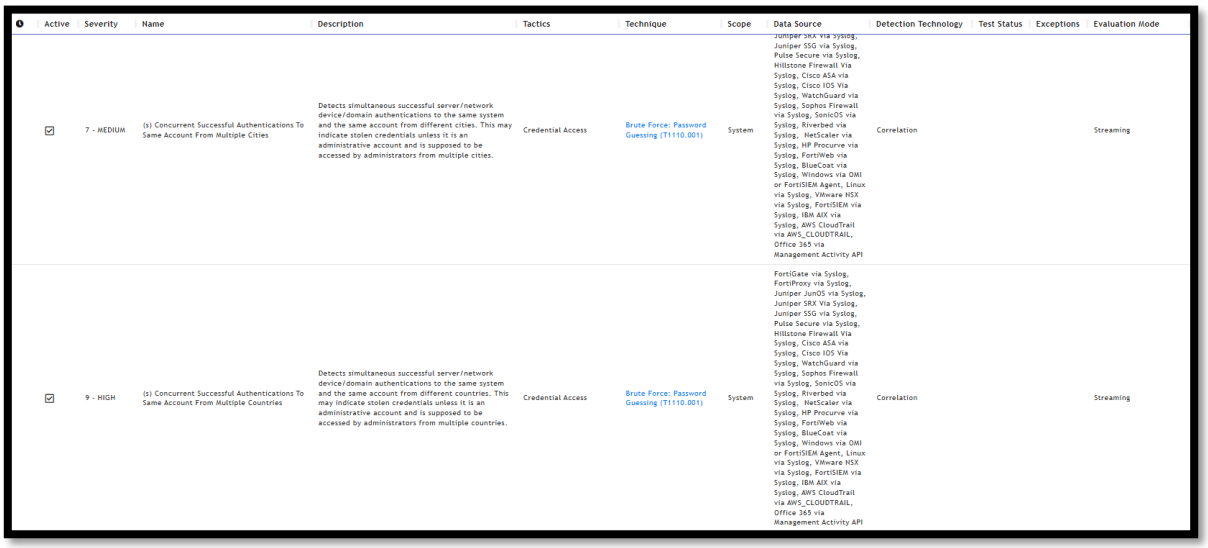
Ilustración 177 Disponibilidad

3.1.6.3.3. Seguridad (Security) Autenticación:

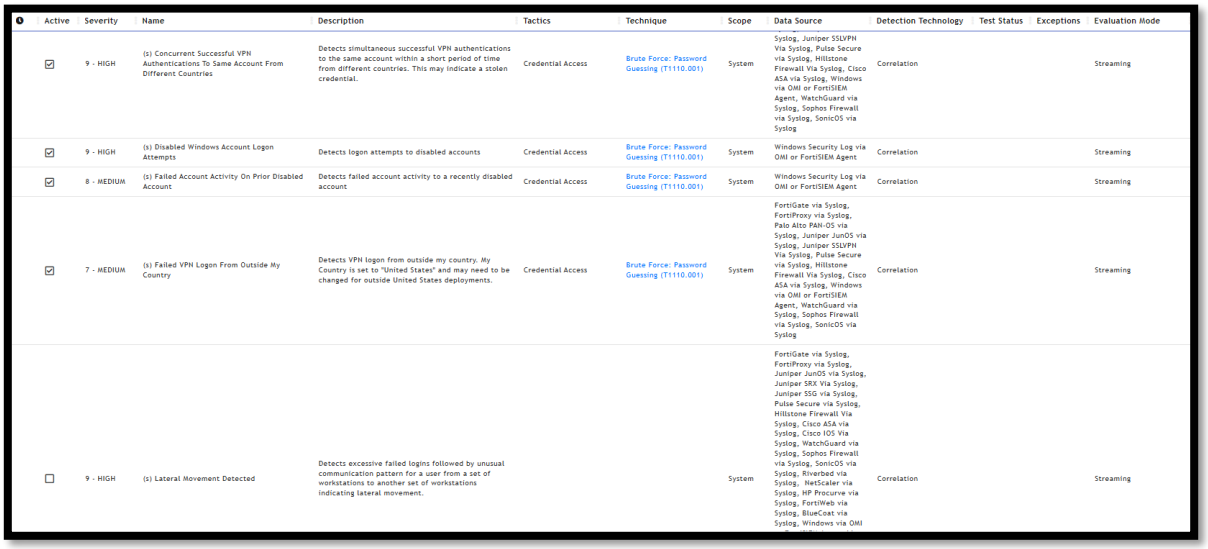
Los casos de uso de seguridad de autenticación en el FortiSIEM se centran en garantizar la integridad y la autenticidad de las credenciales de usuario en todos los dispositivos que tienen instalado el agente. Se muestran los casos Autenticación configurados para el ministerio de trabajo:

Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☑	6 - MEDIUM	(s) Account Locked: Domain	Detects account lockout caused by excessive logon failures	Credential Access	Brute Force: Password Guessing (T1110.001)	System	Windows via OMI or FortiSIEM Agent	Correlation			Streaming
☑	8 - MEDIUM	(s) Account Locked: Server	Detects account lockout caused by excessive logon failures	Credential Access	Brute Force: Password Guessing (T1110.001)	System	Windows via OMI or FortiSIEM Agent, Linux via Syslog	Correlation			Streaming
☑	9 - HIGH	(s) Brute Force App Login Success	Detects an unusual condition where a source has authentication failures followed by a successful authentication at the same app within 15 minutes	Credential Access	Brute Force: Password Guessing (T1110.001)	System	Apache via Syslog, JBOSS via Syslog, MS IIS via Syslog, F5 via Syslog, FortiGate via Syslog, FortiProxy via Syslog, Palo Alto PAN-OS via Syslog, Juniper JunOS via Syslog, Juniper SSLVPN Via Syslog, Pulse Secure via Syslog, Hillstone Firewall Via Syslog, Cisco ASA via Syslog, Windows via OMI or FortiSIEM Agent, WatchGuard via Syslog, Sophos Firewall via Syslog, SonicOS via Syslog	Correlation			Streaming
☑	9 - HIGH	(s) Brute Force Host Login Success	Detects an unusual condition where a source has authentication failures followed by a successful authentication at the same host within 15 minutes	Credential Access	Brute Force: Password Guessing (T1110.001)	System	FortiGate via Syslog, FortiProxy via Syslog, Juniper JunOS via Syslog, Juniper SRX Via Syslog, Juniper SSG via Syslog, Pulse Secure via Syslog, Hillstone Firewall Via Syslog, Cisco ASA via Syslog, Cisco IOS Via Syslog, WatchGuard via Syslog, Sophos Firewall via Syslog, SonicOS via Syslog, Riverbed via Syslog, NetScaler via Syslog, HP Procurve via Syslog, FortiWeb via Syslog, BlueCoat via Syslog, Windows via OMI or FortiSIEM Agent, Linux via Syslog, VMware NSX via Syslog, FortiSIEM via Syslog, IBM AIX via Syslog, AWS CloudTrail via AWS_CLOUDTRAIL, Office 365 via	Correlation			Streaming

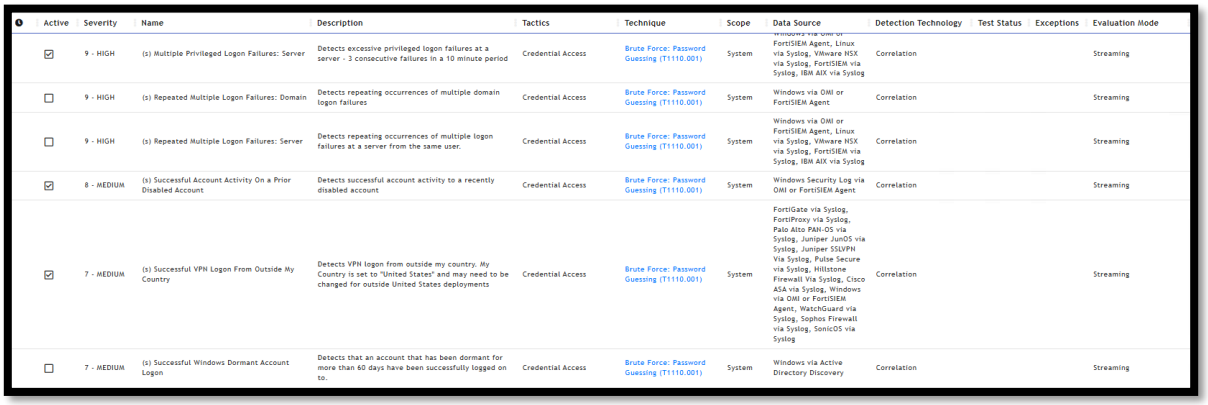
Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☑	7 - MEDIUM	(s) Concurrent Failed Authentications To Same Account From Multiple Cities	Detects simultaneous failed authentications to the same system and the same account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



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



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

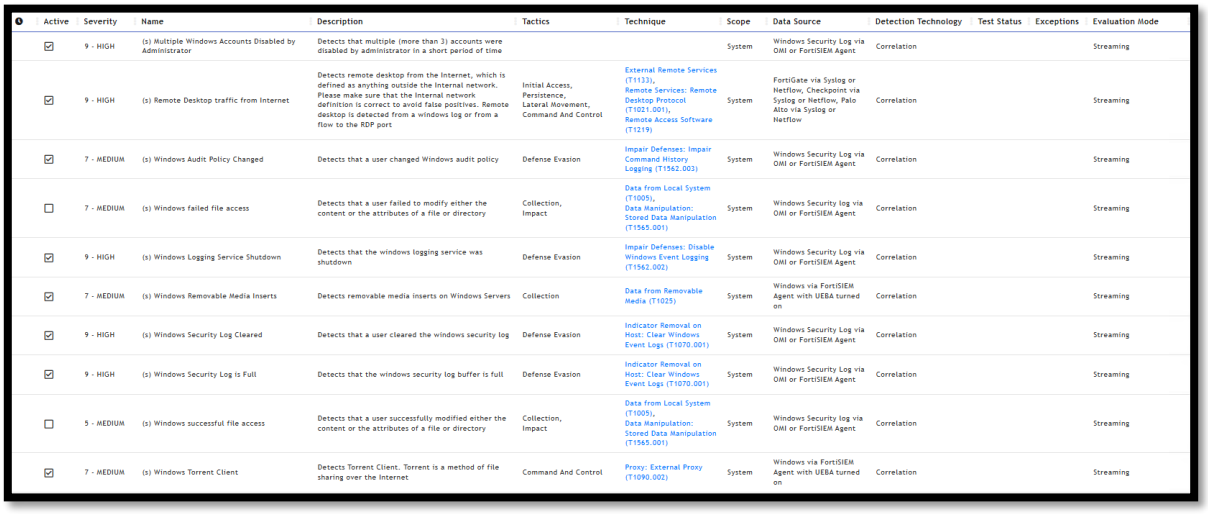


Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☑	9 - HIGH	(s) Multiple Privileged Logon Failures: Server	Detects excessive privileged logon failures at a server - 3 consecutive failures in a 10 minute period	Credential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

Ilustración 178 Autenticación de seguridad

3.1.6.3.4. Violación de políticas (Policy violation)

Los casos de uso de violación de políticas en FortiSIEM se centran en la detección y respuesta ante acciones que violan las políticas de seguridad establecidas en el SIEM de MinTrabajo. Se muestran los casos de políticas de violación configurados para el ministerio de trabajo:



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

Ilustración 179 Violación de políticas

3.1.6.3.5. Overview incidentes

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

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

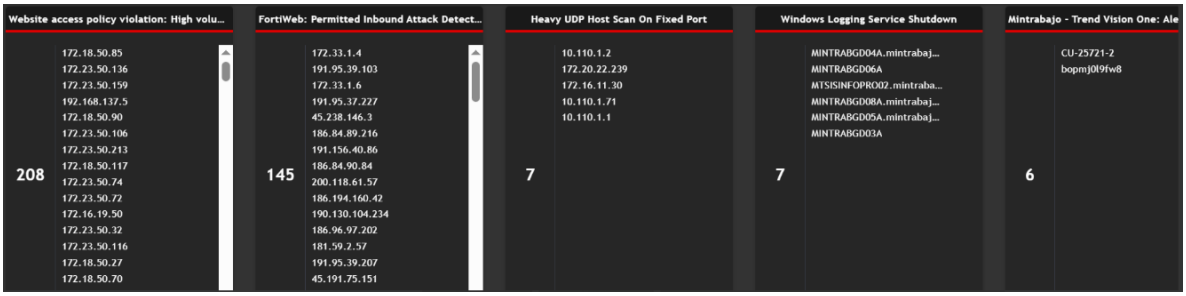


Ilustración 180 Incidentes

Evento	Descripción	Impacto
Website Access Policy Violation (208 eventos)	Accesos a sitios web que violan la política establecida.	Uso indebido de recursos, posible malware o filtración de datos.
FortiWeb: Permitted Inbound Attack Detected (145 eventos)	Tráfico sospechoso entrante detectado por el firewall.	Posible intento de ataque web o exploración de vulnerabilidades.
Heavy UDP Host Scan On Fixed Port (7 eventos)	Escaneo de puertos UDP en la red interna.	Posible movimiento lateral de un atacante o dispositivo comprometido.
Windows Logging Service Shutdown (7 eventos)	Desactivación del servicio de logs en servidores Windows.	Intento de ocultar actividad maliciosa, configuración incorrecta.

Mintrabajo - Trend Vision One: Alertas (6 eventos)	Alertas de seguridad generadas en la plataforma Trend Vision One.	Posible detección de malware o actividades maliciosas.

3.1.6.4.6 Top Disponibilidad de servidores

Esta imagen proporciona un análisis de los servidores monitoreados por FortiSIEM, destacando los 10 servidores que generaron eventos de disponibilidad en términos de seguridad durante el mes de marzo. Ofrece información valiosa sobre los patrones de disponibilidad de servidores. A continuación, se presentan los hallazgos más relevantes:

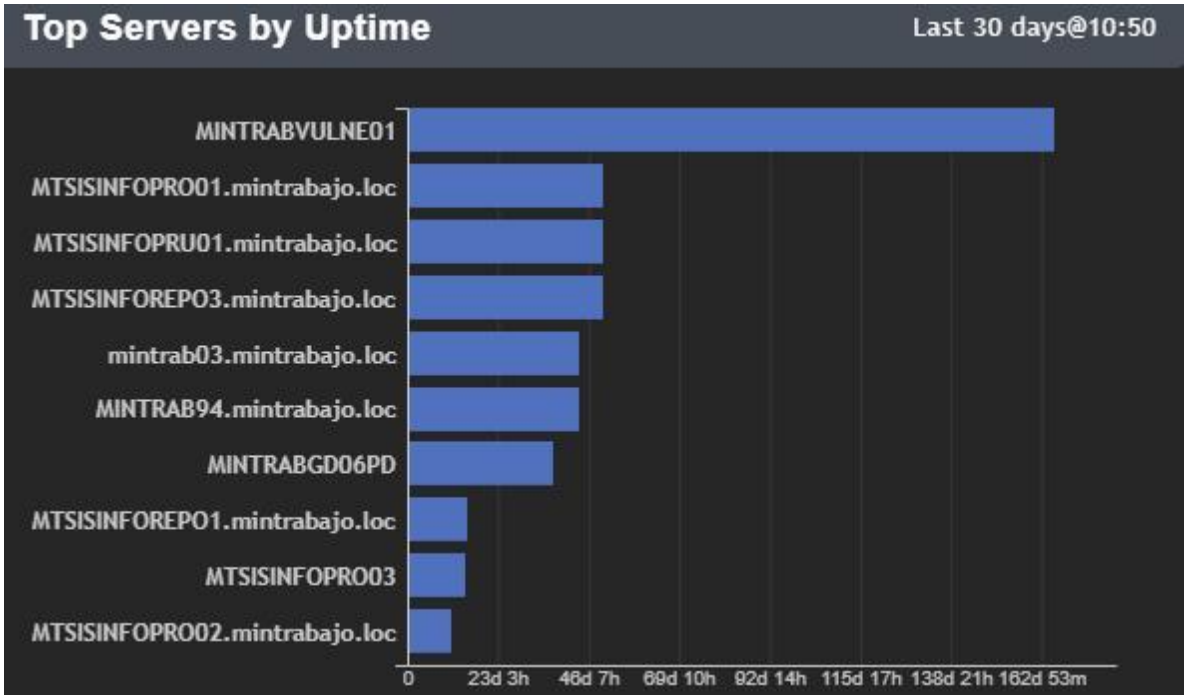


Ilustración 181 Disponibilidad de servidores- Seguridad

3.1.6.4.7 Desempeño CPU, memoria RAM, almacenamiento e interfaces de red durante los últimos 30 días

Durante el período del mes de marzo, se ha realizado un seguimiento detallado del desempeño de los servidores monitoreado por el FortiSIEM en términos de CPU, memoria RAM, almacenamiento e interfaces de red. A continuación, se presenta un resumen de los principales hallazgos en los servidores monitoreados por el FortiSIEM:

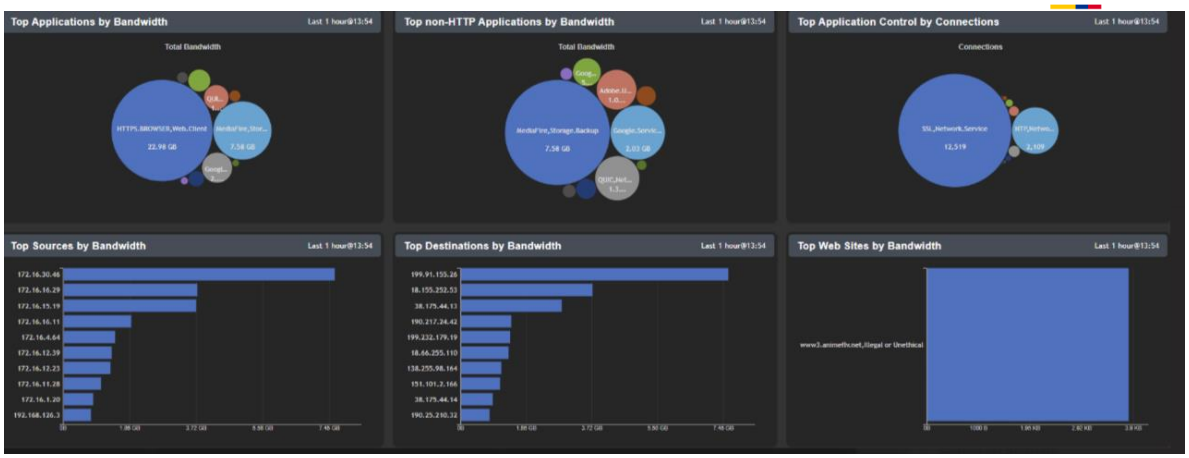


Ilustración 182 Desempeño CPU

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

El gráfico representa los tipos de ataques más comunes por fecha en un período que abarca desde el mes de marzo de 2025. A continuación, se presenta un análisis detallado:

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

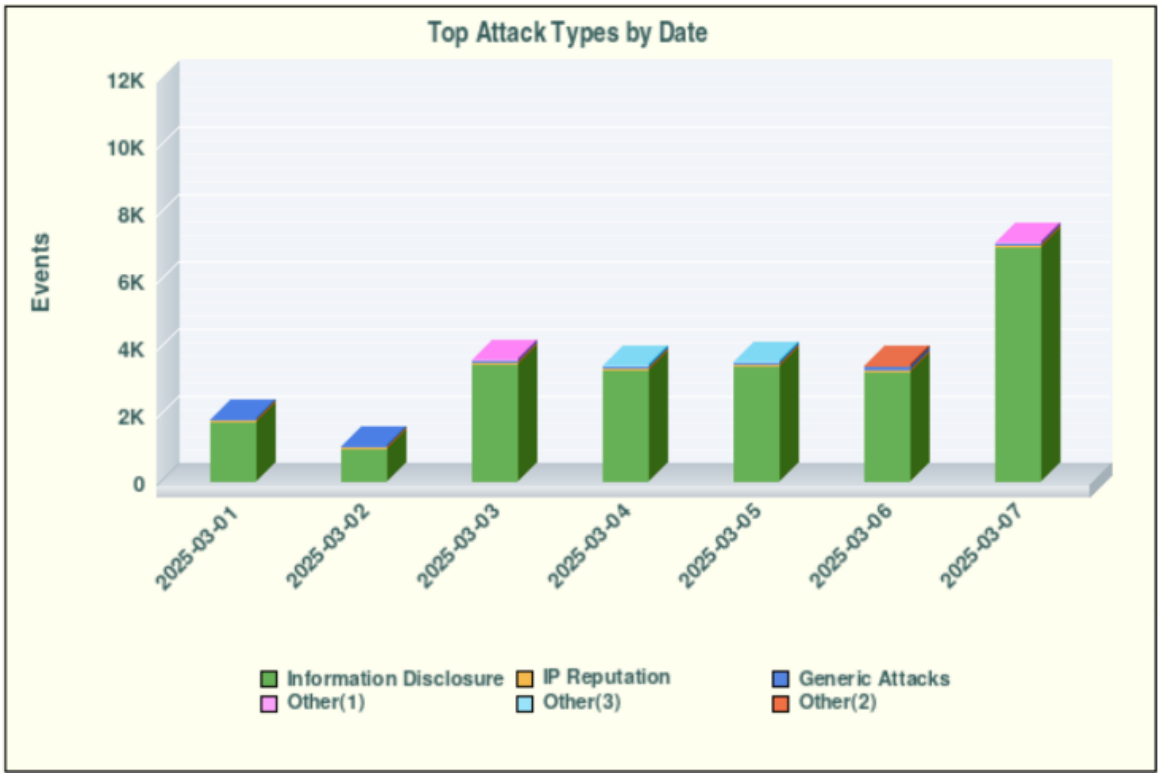


Ilustración 183 Top attack types

3.1.6.5. Solución de Anti-DDoS

Durante el período del mes de marzo, 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 Destinations

IP	SPP	Direction	Drops	Events
201.234.143.91	GESTOR_DOC_MINT	Outbound	14	1

Ilustración 184 Top de ataques

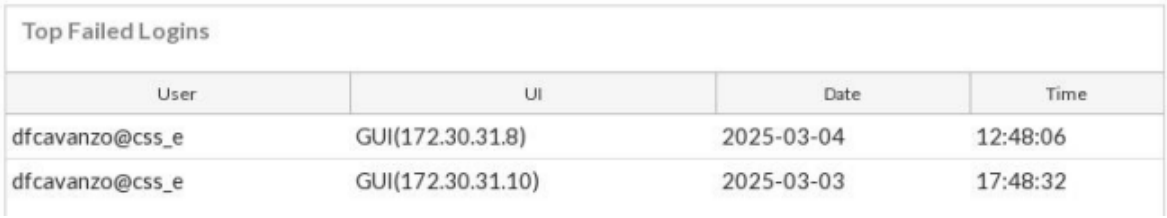
Análisis Detallado:

La imagen muestra un reporte de **Top Attacked Destinations**, lo que indica los destinos más atacados en la red. Aquí están los detalles clave del análisis:

- **IP de Destino:** 201.234.143.91
- Esta dirección IP del sistema atacado, identificado como **"GESTOR_DOC_MINT"**.
- Corresponde al servidor gestión documental del Ministerio.
- **Dirección del tráfico** Outbound: Significa que el tráfico bloqueado fue **saliente**, es decir, desde la red interna hacia un destino externo.

3.1.6.6.2 Login Fallidos

Durante el mes de marzo, se registraron varios eventos de inicio de sesión fallidos, los cuales fueron detectados por nuestra herramienta de seguridad contra ataques de denegación de servicio (DDoS). Es de aclarar que estos intentos de inicios de sesión corresponden a los ingresos que realizaron los especialistas que atienden el servicio. A continuación, se presentan los hallazgos más destacados:



Top Failed Logins

User	UI	Date	Time
dfcavanzo@css_e	GUI(172.30.31.8)	2025-03-04	12:48:06
dfcavanzo@css_e	GUI(172.30.31.10)	2025-03-03	17:48:32

Ilustración 185 Login fallidos

3.1.6.6. Casos atendidos de los servicios de seguridad

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

3.1.6.6.1. Incidentes

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

Caso	Fecha de registro	Asunto	Grupo responsable	Categoría
IM-93716	13/02/2025 11:12:24	Falla Onedrive carpetas compartidas.	SOC	Permitir acceso

Tabla.65 Listado de incidentes atendidos

3.1.6.6.2. Requerimientos

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

Caso	Fecha de registro	Asunto	Grupo responsable	Categoría
RF-86477	5/03/2025 11:16	Creación Caso SOC - Solicitud enrutamiento	SOC	Agregar puertos
RF-86533	5/03/2025 14:21	informe de correo sospechoso	SOC	Revisar correo malicioso
RF-86609	5/03/2025 15:55	RE: Solicitud enrutamiento sedes Remostas SDWAN	SOC	Permitir acceso
RF-86642	5/03/2025 16:45	Revisión de correo sospechoso	SOC	Análisis de Correos
RF-86736	6/03/2025 8:00	RE: Solicitud de espacio par almacenamiento de productos convenios	SOC	Escaneo de activo
RF-86871	6/03/2025 12:06	acceso a internet server 172.25.0.153 172.25.0.154	SOC	Permitir acceso
RF-87079	7/03/2025 9:41	crear regla fopep	SOC	Crear politica
RF-87153	7/03/2025 11:45	Creación Caso SOC - Solicitud Enrutamiento	SOC	Análisis de Herramienta
RF-87616	10/03/2025 12:31	RE: Copia de trámite completado: 20250005998S	SOC	Revisar correo malicioso
RF-87647	10/03/2025 14:16	solicitud de permiso para pagina CISA	SOC	Permitir acceso
RF-87907	11/03/2025 9:56	Solicitud enrutamiento sedes Remostas SDWAN	SOC	Permitir acceso
RF-87910	11/03/2025 10:05	Creación Caso SOC - Solicitud enrutamiento	SOC	Permitir acceso
RF-88042	11/03/2025 15:16	Carlos ernesto trujillo rojas ha compartido "BOGOTA 10 DE MARZO DE 2025" contigo	SOC	Análisis de Correos
RF-88054	11/03/2025 15:36	ERROR REPRODUCCION DE VIDEOS YOUTUBE PORTAL CAPACITACION	SOC	Permitir acceso
RF-88239	12/03/2025 9:15	acceso a internet server 172.25.0.153 172.25.0.154-55	SOC	Permitir acceso
RF-88327	12/03/2025 11:31	RV: PAGINA RUES	SOC	Permitir acceso
RF-88801	13/03/2025 12:21	RV: PROBLEMAS INGRESO RUES	SOC	Permitir acceso
RF-88919	13/03/2025 16:35	Habilitación de puertos	SOC	Agregar puertos
RF-89039	14/03/2025 8:11	Verificación de página	SOC	Reporte conexión de usuario
RF-90178	14/03/2025 11:11	Solicitud enrutamiento sedes Remostas SDWAN	SOC	Permitir acceso
RF-90182	14/03/2025 11:16	MINT // Solicitud enrutamiento sedes Remostas SDWAN	SOC	Permitir acceso
RF-90306	14/03/2025 14:45	HABILITACIÓN DE PÁGINAS	SOC	Permitir acceso
RF-92434	15/03/2025 0:35	[Fortisiem] -- Mintrabajo // [Trend Vision One: Alert Severity 5 to 10 2/7/2024]	SOC	Ajuste o creación de alerta
RF-92771	17/03/2025 12:01	Solicitud enrutamiento segmentos WAN	SOC	Ajustar política
RF-92819	17/03/2025 14:50	RE: Revisión de aplicaciones Web	SOC	Análisis vulnerabilidades
RF-92820	17/03/2025 14:51	RE: Revisión de aplicaciones Web	SOC	Análisis vulnerabilidades
RF-93170	19/03/2025 7:55	Correo sospechoso	SOC	Revisar correo malicioso
RF-93367	19/03/2025 12:45	RV: ¡AVISO! DE ALISTAMIENTO – IMPULSO PROCESAL E INVESTIGACIÓN DE BIENES	SOC	Análisis de Malware
RF-93711	20/03/2025 11:16	Navegación IPs Dispositivos Ministro	SOC	Ataques al portal Web

RF-93809	20/03/2025 14:56	solicitud validación correo sospechoso	SOC	Análisis de Correos
RF-93845	20/03/2025 16:15	CORREO SOSPECHOSO	SOC	Análisis de Correos
RF-93973	21/03/2025 8:41	Solicitud configuración perimetral	SOC	Permitir acceso
RF-94182	21/03/2025 17:25	Habilitación de puertos	SOC	Agregar puertos
RF-94185	21/03/2025 17:41	RV: Habilitación de puertos	SOC	Agregar puerto
RF-94376	25/03/2025 9:41	RE: 100355896255-Cobro coactivo en curso: Medidas de embargo aplicadas-100355896255	SOC	Correo Malicioso (Phishing, Smishing, whaling, otros)

Tabla.66 Listado de requerimientos atendidos

3.1.6.7 Análisis de riesgo

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

- **Ejecución de archivos maliciosos**

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

Tabla.67 Ejecución de archivos maliciosos

- **Vulnerabilidades en la infraestructura**

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

Tabla.68 Vulnerabilidades en la infraestructura

- **Ataques de Phishing dirigidos**

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

Tabla.69 Ataque de Phishing dirigidos

2. Medidas de Mitigación Recomendadas

Control y restricción de archivos ejecutables:

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

Gestión de vulnerabilidades:

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

Prevención y respuesta ante phishing:

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

3.1.6.8 Políticas y procedimiento de seguridad

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

- Implementación del servicio de ZTNA, actualmente en proceso de ajuste y optimización de las reglas de acceso a Internet.

- Se realizo bloqueo de Ioc de malware (31/03/2025) se proceder con el bloqueo de los Indicadores de Compromiso (IoC) en el firewall y Trend Micro, según los detalles proporcionados en los archivos adjuntos.

3.1.7. Licenciamiento

A continuación, se presenta la información del licenciamiento:

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

Tabla 70 Licenciamiento

3.1.8. Administración, soporte y monitoreo

- Servidores

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

- Nube pública

Se validó la infraestructura aprovisionada en Azure, que se encontraba en proceso de monitorear adecuadamente y se configuró un monitoreo sobre las IP públicas de los recursos expuestos y funcionales actualmente, se sostienen sesiones con áreas funcionales y se entrega informe sobre uno de los componentes para que los propietarios de cada suscripción en nube realicen monitoreo sobre la nube a través de Azure Monitor. Dentro del modelo de arquitectura a implementar, se tienen contemplado los componentes de Azure Monitor críticos que deben tenerse en cuenta para tener trazabilidad.

Dentro de la documentación relacionada con Nube publica se agrega un ítem de Monitoreo y se abarcan las recomendaciones y acciones a realizar por parte de la UT y de la entidad a nivel de monitoreo de componentes de nube pública y la información que la herramienta Azure Monitor arroja desde los accesos que posee la UT al Tenant.

- DDBB

Se realizó actualización de la base de datos indicando el nombre del especialista a quien deben reportarse las indisponibilidades y a quien deben llegar los alertamientos automáticos de la herramienta Zabbix, se da visibilidad al NOC de la misma para el escalamiento para evitar asignaciones erradas sobre alertamientos o incidencias presentadas sobre la infraestructura tecnológica y componentes asociados como bases de datos y aplicaciones especializadas. Se está trabajando en la actualización del árbol de categorías del equipo de servicios centrales para el mes de marzo 2025.

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

- Almacenamiento

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

• Medición ANS Datacenter y Nube Pública

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

ID	Indicadores	Resultado	Meta
DC-1	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
DC-2	Continuidad y disponibilidad del datacenter principal	100,00%	99.95%
DC-3	Continuidad y disponibilidad del datacenter alterno	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	100,00%	90,00%
DC-10	Tiempo de solución de requerimientos asociado a los servicios de administración, soporte y monitoreo	100,00%	90,00%
DC-11	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 71 Medición ANS Datacenter

ID	Indicadores	Resultado	Meta
NP-1	Continuidad y disponibilidad de la nube pública	100,00%	99,90%
NP-2	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100%

Tabla 72 Medición ANS Nube Pública

3.2. No aplica

3.3. Conectividad WAN, SDWAN e Internet

3.3.1. Canales WAN

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

Se verifica el canal MPLS central en Datacenter, durante el mes no se presentaron novedades sobre el servicio, se tuvo un promedio 146.32 Mbps de consumo y un poco de 1.04 Gbps, sin afectar la capacidad del canal.

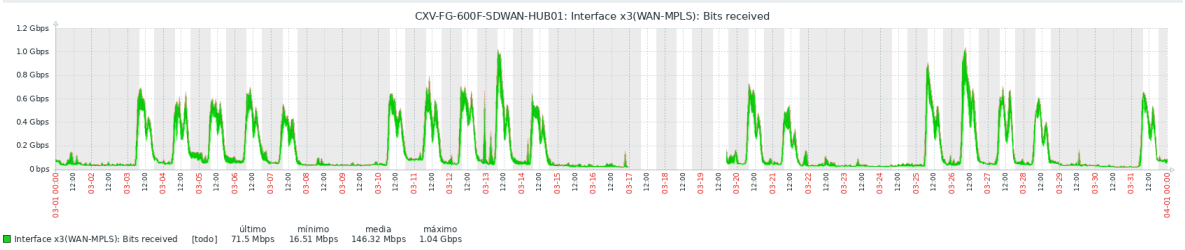


Ilustración *186*. Grafica de consumo canal MPLS Datacenter

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

```
[edit]
etb@INDRA_BOG_K68C169A_D# run show system uptime
Current time: 2025-04-02 16:55:30 COT
Time Source:  LOCAL CLOCK
System booted: 2024-07-25 11:12:28 COT (35w6d 05:43 ago)
Protocols started: 2024-07-25 11:13:28 COT (35w6d 05:42 ago)
Last configured: 2025-01-10 21:30:29 COT (11w4d 19:25 ago) by etb
 4:55PM  up 251 days,  5:43, 4 users, load averages: 0.56, 0.44, 0.36

[edit]
etb@INDRA_BOG_K68C169A_D#
```

Ilustración 187 Uptime del equipo MPLS Datacenter

3.3.1.1. Incidentes de Conectividad

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

Dirección Territorial	Caso Asociado	Disponibilidad
Concordia	IM-85527	98,02%
Puerto Berrio	IM-89131	94,37%
Sede Territorial Barranquilla	IM-95713	99,84%
Campo De La Cruz	IM-95730	77,93%
Sede Territorial Cartagena	IM-85916	99,30%
Sogamoso	IM- 88973	98,59%
Paz De Ariporo	IM-85504	99,58%
Santander De Quilichao	IM-95464	98,19%
Tocancipá	IM-94246	89,96%
Zipaquirá	IM-93766	64,66%
Sede Territorial Cúcuta	IM-88955	98,70%
Socorro	IM-86471	99,45%
Espinal	IM-95983	95,66%
Mariquita	IM-96003	96,38%
Buga	IM-87162	99,43%

Tabla 73 Novedades servicio de internet

3.3.1.2. Topología Actual

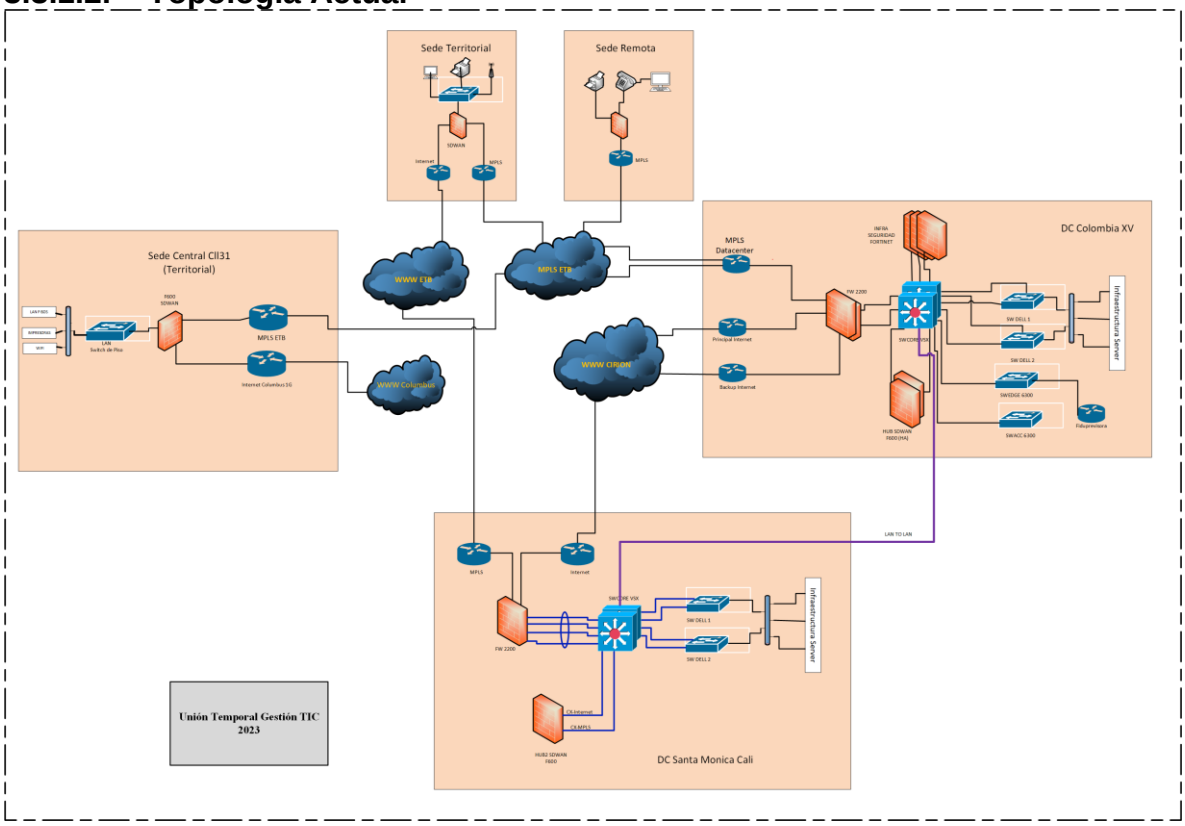


Ilustración 188. Topología actualizada

3.3.2. Canales SDWAN e Internet Dedicado

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

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

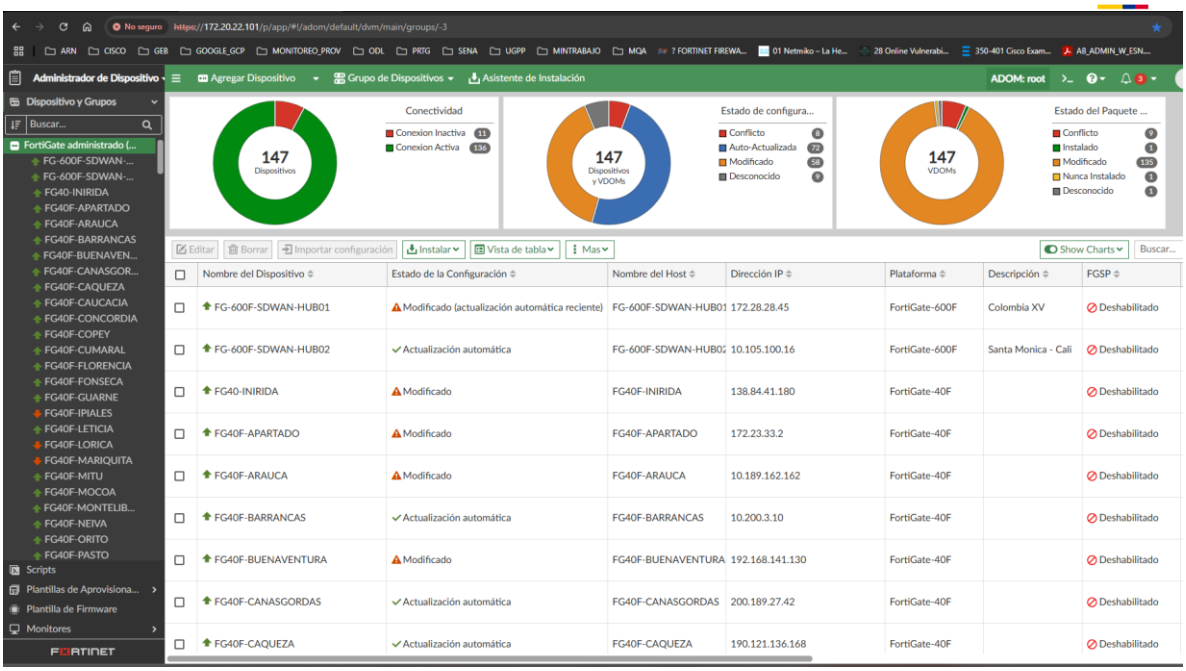


Ilustración 189. Interface Fortimanager

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

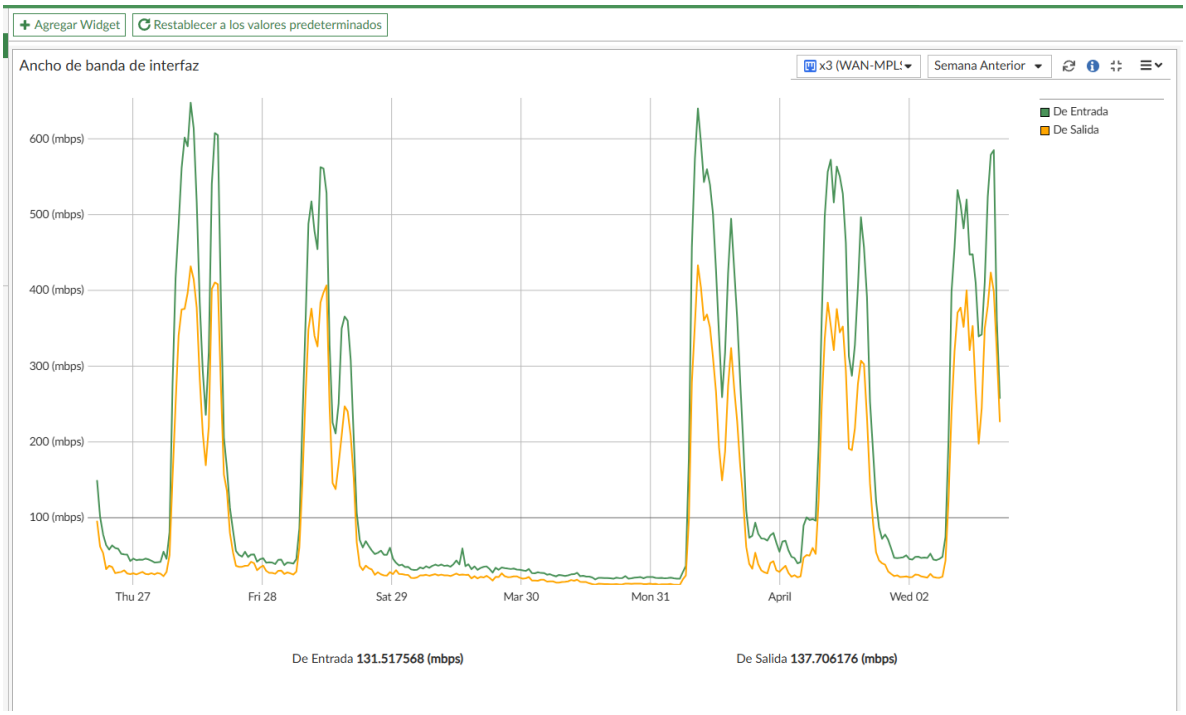


Ilustración 190. Interface MPLS HUB SDWAN

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

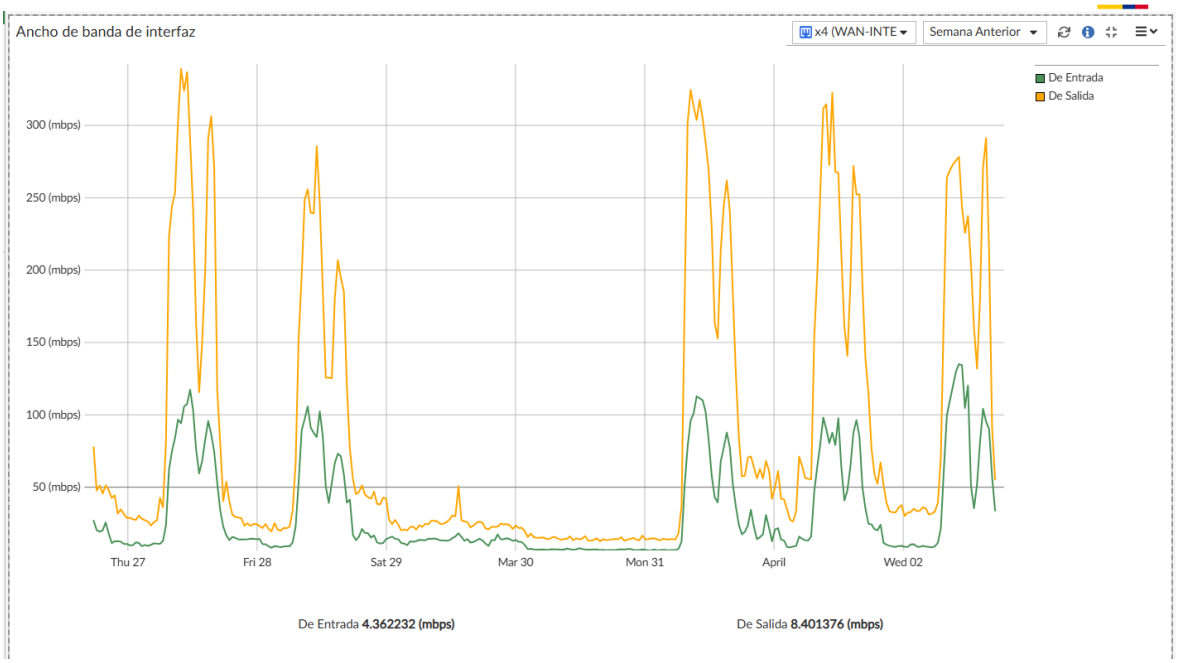
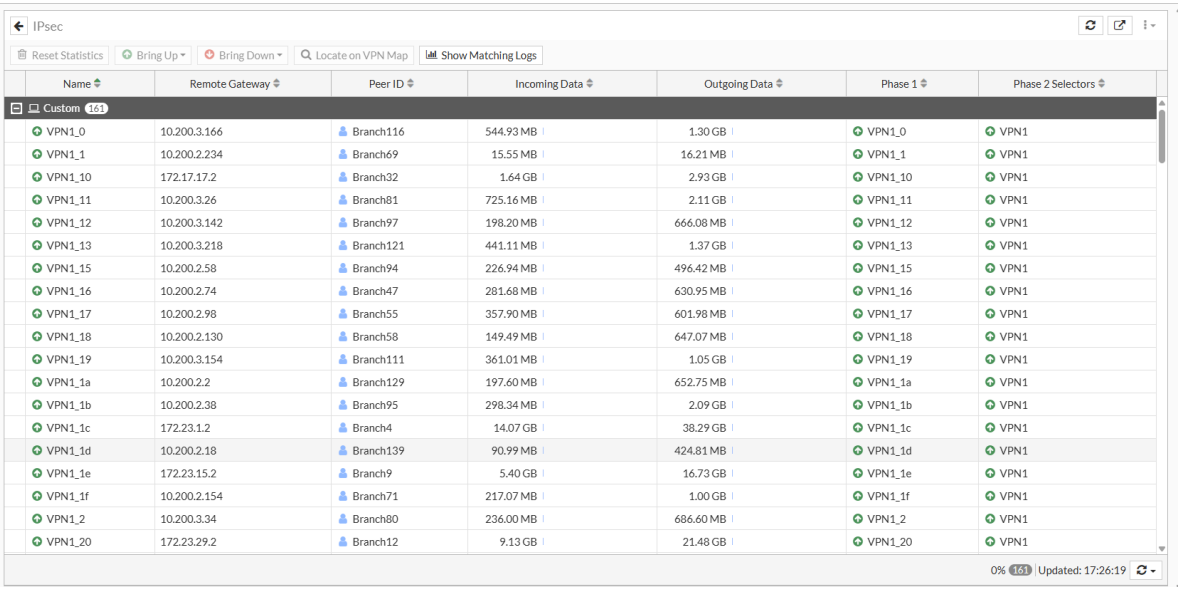


Ilustración 191 Interface Internet HUB SDWAN

Se relaciona las VPNs SDWAN establecidas contra el HUB SDWAN de datacenter, donde se observa el consumo de tráfico que se ha tenido sobre estas.



IPsec

Reset Statistics | Bring Up | Bring Down | Locate on VPN Map | Show Matching Logs

Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Custom 161						
VPN1_0	10.200.3.166	Branch116	544.93 MB	1.30 GB	VPN1_0	VPN1
VPN1_1	10.200.2.234	Branch69	15.55 MB	16.21 MB	VPN1_1	VPN1
VPN1_10	172.17.17.2	Branch32	1.64 GB	2.93 GB	VPN1_10	VPN1
VPN1_11	10.200.3.26	Branch81	725.16 MB	2.11 GB	VPN1_11	VPN1
VPN1_12	10.200.3.142	Branch97	198.20 MB	666.08 MB	VPN1_12	VPN1
VPN1_13	10.200.3.218	Branch121	441.11 MB	1.37 GB	VPN1_13	VPN1
VPN1_15	10.200.2.58	Branch94	226.94 MB	496.42 MB	VPN1_15	VPN1
VPN1_16	10.200.2.74	Branch47	281.68 MB	630.95 MB	VPN1_16	VPN1
VPN1_17	10.200.2.98	Branch55	357.90 MB	601.98 MB	VPN1_17	VPN1
VPN1_18	10.200.2.130	Branch58	149.49 MB	647.07 MB	VPN1_18	VPN1
VPN1_19	10.200.3.154	Branch111	361.01 MB	1.05 GB	VPN1_19	VPN1
VPN1_1a	10.200.2.2	Branch129	197.60 MB	652.75 MB	VPN1_1a	VPN1
VPN1_1b	10.200.2.38	Branch95	298.34 MB	2.09 GB	VPN1_1b	VPN1
VPN1_1c	172.23.1.2	Branch4	14.07 GB	38.29 GB	VPN1_1c	VPN1
VPN1_1d	10.200.2.18	Branch139	90.99 MB	424.81 MB	VPN1_1d	VPN1
VPN1_1e	172.23.15.2	Branch9	5.40 GB	16.73 GB	VPN1_1e	VPN1
VPN1_1f	10.200.2.154	Branch71	217.07 MB	1.00 GB	VPN1_1f	VPN1
VPN1_2	10.200.3.34	Branch80	236.00 MB	686.60 MB	VPN1_2	VPN1
VPN1_20	172.23.29.2	Branch12	9.13 GB	21.48 GB	VPN1_20	VPN1

0% 161 Updated: 17:26:19

Ilustración 192. VPN SDWAN establecidas

En cuanto al comportamiento del HUB SDWAN, se observa que no ha tenido reinicios, y no se presenta alto procesamiento sobre el mismo.

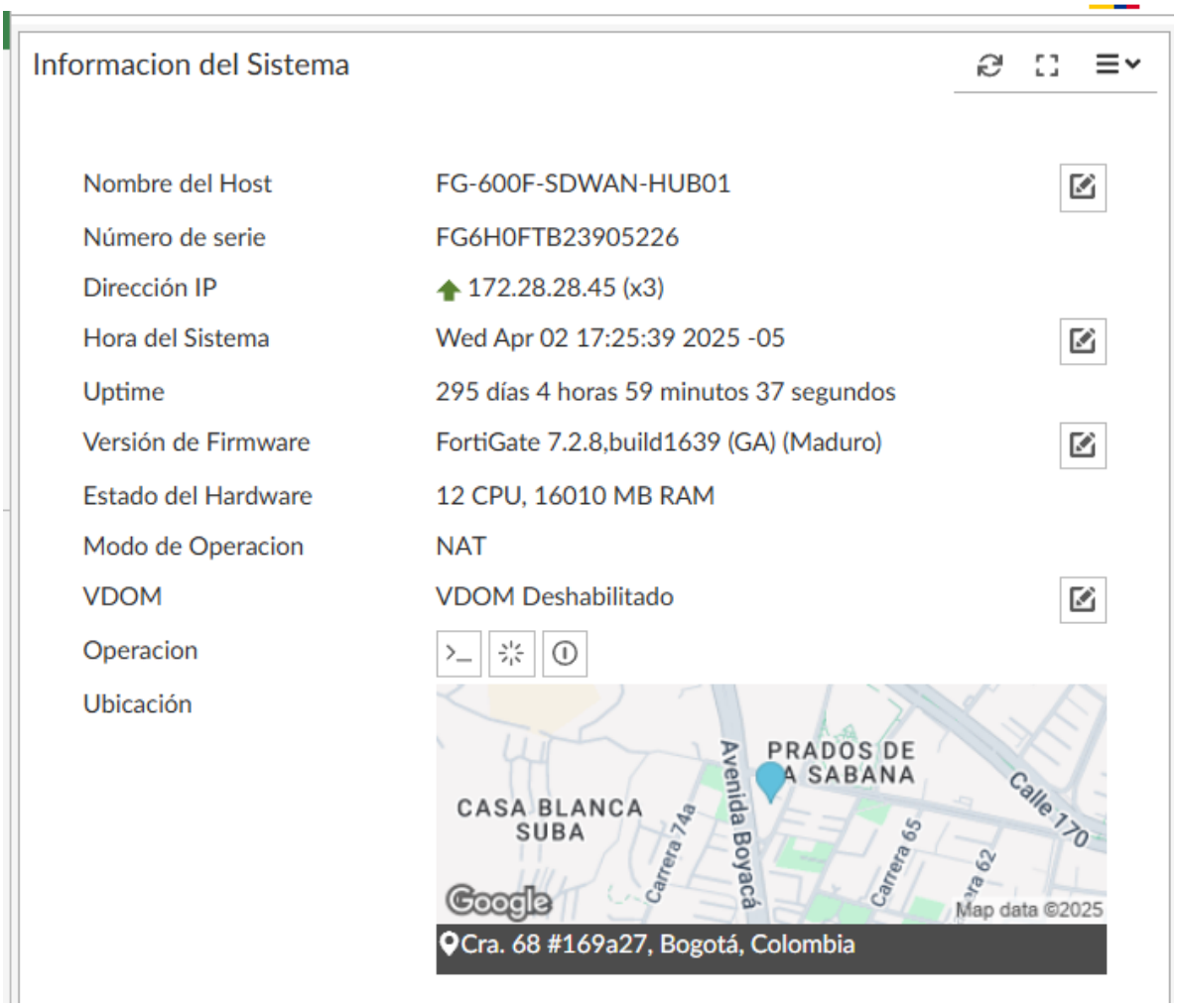


Ilustración 193. Estado HUB SDWAN Datacenter

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

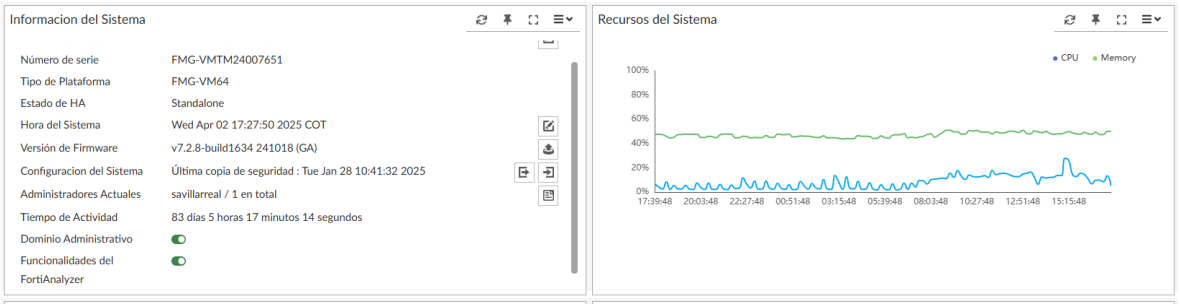


Ilustración 194. Recursos Fortimanager

Actualmente, se está trabajando y cerrando el despliegue de los equipos Fortinet en las sedes remotas, esto con el fin de tener un mayor control sobre la red LAN es estas sedes y que no se contaba con equipo de la administración de la Unión Temporal TIC para dicho fin. De esta forma quedarían asociadas la sedes a la red SDWAN implementada para las sedes territoriales. Durante el mes de marzo se realizó la configuración del equipo Fortinet en 5 sedes, relacionadas en la siguiente tabla.

SEDE	Operativo
Bahía Solano	1
Cáqueza	1
Concordia	1
Garzón	1
Paz de Ariporo	1
Total general	**5**

Tabla 74 Sedes configuradas en marzo 2025

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

(*) De acuerdo con la solicitud de la supervisión del contrato 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 marzo:

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

Dirección Territorial	Caso Asociado	Disponibilidad	% PENALIDAD	Valor Penalidad un enlace
Concordia	IM-85527	98,02%	3%	$ 9.240
puerto Berrio	IM-89131	94,37%	10%	$30.801
Campo De La Cruz	IM-95730	77,93%	50%	$154.007
Sogamoso	IM- 88973	98,59%	3%	$9.240
Paz De Ariporo	IM-85504	99,58%	3%	$ 9.240
Santander De Quilichao	IM-95464	98,19%	3%	$ 23.101
Tocancipá	IM-94246	89,96%	10%	$ 30.801
Zipaquirá	IM-93766	64,66%	100%	$ 308.015
Socorro	IM-86471	99,45%	3%	$ 9.240
Espinal	IM-95983	95,66%	3%	$ 9.240
Mariquita	IM-96003	96,38%	3%	$9.240
Buga	IM-87162	99,43%	3%	$9.240
TOTAL				**$ 611.409**

Tabla 76 Desagregado sedes con novedad un solo enlace

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

Dirección Territorial	Caso Asociado	Disponibilidad	% Penalidad	Valor Penalidad doble enlace
Sede Territorial Barranquilla	IM-95713	99,84%	3%	$60.946
Sede Territorial Cartagena	IM-85487	99,30%	3%	$ 36.567
Sede Territorial Cúcuta	IM-88955	98,70%	3%	$48.757
TOTAL				**$146.270**

Tabla 77 Desagregado sedes con novedad doble enlace

4. LINEA DE SERVICIOS EN SEDE

4.1. Equipos de Cómputo de usuario final

Durante el periodo del informe, la Unión Temporal (UT) realizó el seguimiento a las acciones adelantadas para la devolución de los equipos Dell, propiedad del anterior operador tecnológico. Asimismo, se atendieron las solicitudes de retiro y asignación de equipos de cómputo, y se brindó soporte a las novedades presentadas por el parque computacional Lenovo.

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

Ítem	Cantidad
Computador portátil (morral, guaya y diadema)	1000
Computador escritorio (monitor, CPU, teclado, mouse y diadema)	1172
Computadores portátiles adicionales (puntuables)	120
Total	**2192**

Tabla 78 Cantidades de equipos a distribuir a nivel nacional

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

- **Devolución de equipos Dell:** Se gestionó la devolución de los equipos Dell propiedad del anterior operador tecnológico.
- **Atención de solicitudes de retiro y asignación**: Se atendieron las solicitudes de retiro y asignación de equipos de cómputo según los requerimientos de los usuarios.
- **Soporte a novedades del parque computacional Lenovo:** Se brindó soporte técnico para atender las novedades presentadas en el parque computacional Lenovo.
- **Consolidación de actas de entrega y devolución**: Se consolidaron las actas de entrega y devolución en formato digital, almacenándolas en el repositorio del Nivel Central.

Gestión de Garantías:

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

Estado de caso	Cantidad
Cerrado	4
Suspendido	12
Total	**16**

Tabla 79 Estado de casos de garantía.

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

ANS	Cerrado	Suspendido	Total
CUMPLE	3	12	15
NO CUMPLE	1	0	1
Total	4	12	16

Tabla 80 ANS casos de garantía.

Siniestros:

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

Funcionario	Equipo	DT	Parte afectada	ESTADO
Santodomingo Aguilar Pavel Yasser	PW0A3CDZ	NIVEL CENTRAL	Equipo mojado, le cayó bebida encima del teclado	Reportado a la entidad, a la espera de gestión correspondiente.
Alvarez Hernandez Galia Lena	PW0A3CHL	NIVEL CENTRAL	Equipo con golpes en las esquinas	Reportado a la entidad, está en proceso la definición de la cotización.
Bernardo Ardila Fernandez	PW09Z34H	VALLEDUPAR	El portátil presenta rayones en la parte superior derecha de la pantalla y un leve hundimiento en la parte inferior izquierda de la base, todo esto en la carcasa.	Reportado a la entidad, a la espera de gestión correspondiente.

Tabla 81 ANS Equipos en siniestro

Instalaciones de Equipos y Entrega a Usuarios Finales:

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

Tipo de equipo	Instalados
Portátil	882
Escritorio	1102
Total	1984

Tabla 82 *Avance instalación de equipos*

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

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

4.1.1. Equipos de Escritorio

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

4.1.2. Equipos Portátiles

Durante el presente mes se realizó la gestión y atención de todos los equipos de cómputo portátiles asignados a los usuarios de la entidad tanto en el nivel central como en las sedes territoriales.

- **Reporte de novedades de equipos**

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

- Se registraron en Aranda un total de 16 solicitudes tipificadas así:
  - Incidentes – 0 casos
  - Requerimientos de Servicio – 16 casos.
- Al corte de mes quedaron en estado:
  - Cerrado – 4 casos.
  - Solucionado – 0 casos
  - Suspendido – 11 casos.
  - En Proceso – 1 caso.
- 4 casos corresponden a solicitudes de usuarios VIP y 12 casos corresponden a solicitudes de usuarios estándar.

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

Grupo responsable	Cantidad de solicitudes
Responsable Garantías Equipos	14
Gestor de Inventarios	2
Total general	**16**

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	**16**
Asesoria - Consulta	1
Configuración	1
Instalación - Configuración	1
Asignación de equipo (portátil o PC)	1
Equipo Periférico	7
Equipo Escritorio	2
Equipo Portátil	3
Total general	**16**

Tabla 84 Solicitudes de Equipos Usuario Final – Según Tipificación y Categoría

- **Medición de ANS Equipo de usuario final**

A continuación, el resultado de la medición de los ANS para los equipos de usuario final:

ID	Indicadores	Resultado	Meta
EUF-1	Tiempo de solución de requerimientos de garantía	93.10%	90,00%
EUF-2	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 85 Medición ANS Equipos de Usuario Final

4.2. Conectividad LAN y WLAN

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

- Se dejó instalado, configurado y monitoreado un cuarto Access Point para el piso 20 para mejorar la cobertura.
- Se dejo instalado, configurado y monitoreado el firewall en la inspección de Concordia.
- Se finalizó la implementación del SD-WAN en la inspección de Puerto Boyacá.
- Se dejó instalado, configurado y monitoreado el firewall en la inspección de Cáqueza.
- Se dejó instalado, configurado y monitoreado un Access Point en la oficina del ministro, de igual forma se realizó la reserva de IPs para la navegación de los dispositivos asignados sin restricción en la navegación.
- Se dejó implementado nuevo canal de internet para la territorial de Cartagena con el proveedor Tigo UNE.

A continuación, se relacionan las actividades relevantes para este servicio:

- Para el mes de marzo, los especialistas responsables del servicio gestionaron un total de 18 solicitudes escaladas a través de la herramienta Aranda. Al corte del mes, los 18 casos quedaron en estado Cerrado.

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

Categoría	Cantidad de solicitudes
Sin Servicio	4
Configuraciones Adicionales	3
Starlink	3
Falla Punto de Red	2
Degradación	1

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



Ilustración 195 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

Dirección Territorial	Población y/o ciudad de ubicación	Cantidad switches 24 puertos
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, ANTIOQUIA	1
Territorial Valle	CALI	2

Dirección Territorial	Población y/o ciudad de ubicación	Cantidad switches 48 puertos
OE Buenaventura	BUENAVENTURA	1
Sede Nivel Central	BOGOTA	34*
	Total	**71**

Tabla 88 Distribución y Cantidades de Switch 48 puertos

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

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

4.2.5. Puntos de Acceso

Se encuentran operativos y en monitoreo los siguientes equipos:

Dirección Territorial	Población y/o ciudad de ubicación	Cantidad Access Points
Territorial Antioquia	MEDELLIN	4
Territorial Arauca	ARAUCA	1
Territorial Atlántico	BARRANQUILLA	3
OE Barrancabermeja	BARRANCABERMEJA	2
Calle 32	BOGOTA	4
Territorial Bolívar	Cartagena	2
Territorial Boyacá	TUNJA	2
Territorial Caldas	MANIZALEZ	2
Territorial Caquetá	FLORENCIA	1
Territorial Casanare	YOPAL	2
Territorial Cauca	POPAYAN	2
Territorial Cesar	VALLEDUPAR	2
Territorial Chocó	QUIBDÓ	2
Territorial Córdoba	MONTERIA	2
Territorial Cundinamarca	FACATATIVÁ	2
Territorial Guajira	RIOHACHA	2
Territorial Huila	NEIVA	0
Territorial Magdalena	SANTA MARTA	2
Territorial Meta	VILLAVICENCIO	3
Territorial Nariño	PASTO	2
Territorial Norte de Santander	CÚCUTA	3
Territorial Putumayo	MOCOA	1
Territorial Quindío	ARMENIA	3
Territorial Risaralda	PEREIRA	2
Territorial Santander	BUCARAMANGA	1
Territorial Sucre	SINCELEJO	2
Territorial Tolima	IBAGUÉ	3*
OE Urabá Apartadó	APARTADÓ, ANTIOQUIA	2
Territorial Valle	CALI	4
OE Buenaventura	BUENAVENTURA	1
Sede Nivel Central	BOGOTA	46
	Total	**110**

Tabla 89 Distribución de puntos de acceso

Territorial Bogotá: 1 equipo restante se encuentra en Stock.
Territorial Norte de Santander - Cúcuta: El AP pendiente de instalación fue enviado a Bucaramanga
Territorial Tolima -Ibagué: En la sede permitieron la instalación de 3 AP y 1 equipo restante se encuentra en Stock.

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 4 teléfonos, no han proporcionado el listado de asignación de estas extensiones.

4.3.2. Teléfono Gama Baja

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

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

Dirección territorial	Población y/o ciudad de ubicación	Cantidad teléfonos Gama Baja	Novedad
AMAGA	AMAGA	1	Cerrada se envió teléfono a Medellín
MONTERREY	MONTERREY	1	Cerrada
BOLIVAR	BOLIVAR	1	Cerrada
TIERRA ALTA	TIERRA ALTA	1	Cerrada
TIBU	TIBU	1	Cerrada
QUIMBAYA	QUIMBAYA	1	Cerrada
CALARCA	CALARCA	1	Cerrada

Dirección territorial	Población y/o ciudad de ubicación	Cantidad teléfonos Gama Baja	Novedad
MAJAGUAL	MAJAGUAL	1	Cerrada
CASA DE JUSTICIA (IBAGUE)	CASA DE JUSTICIA (IBAGUÉ)	1	Cerrada
LIBANO	LÍBANO	1	Cerrada
	Total	**9(*)**	

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

Sede	Cantidad
Asignados Sede Central	27
Pendientes definición de usuario por parte de la supervisión para asignación	3
Total	30

Tabla 94 Consolidado equipos MIFI

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

- **Gestión del servicio**

En el mes de marzo de 2025, se presentan las siguientes novedades sobre el servicio:

- Operatividad sobre la grabación de llamadas en la mesa de servicios.

- Configuración de permisos de llamadas a celular, larga distancia nacional, local a coordinadores e implementación de licenciamiento correspondiente al addon Phone System a nivel nacional.
- En proceso aprovisionamiento de equipos a usuario final a nivel nacional, para las sedes pendientes por disponibilidad del usuario del ministerio.
- Se lleva a cabo proceso de reconfiguración sobre las troncales para las opciones 2 y 0 configuradas en el IVR para atención al ciudadano con el nuevo aliado BPM.

- **Asignación de Licencias - Extensiones**

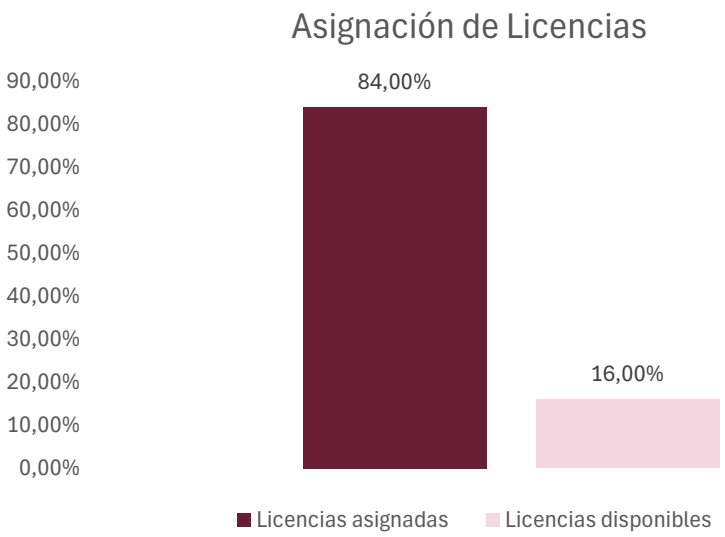


Ilustración 196. Licencias y extensiones

Durante el mes en gestión, se han asignado un total de 1.426 extensiones a nivel nacional. Actualmente, permanecen disponibles 274 extensiones.

- **Estadísticas de Tráfico**

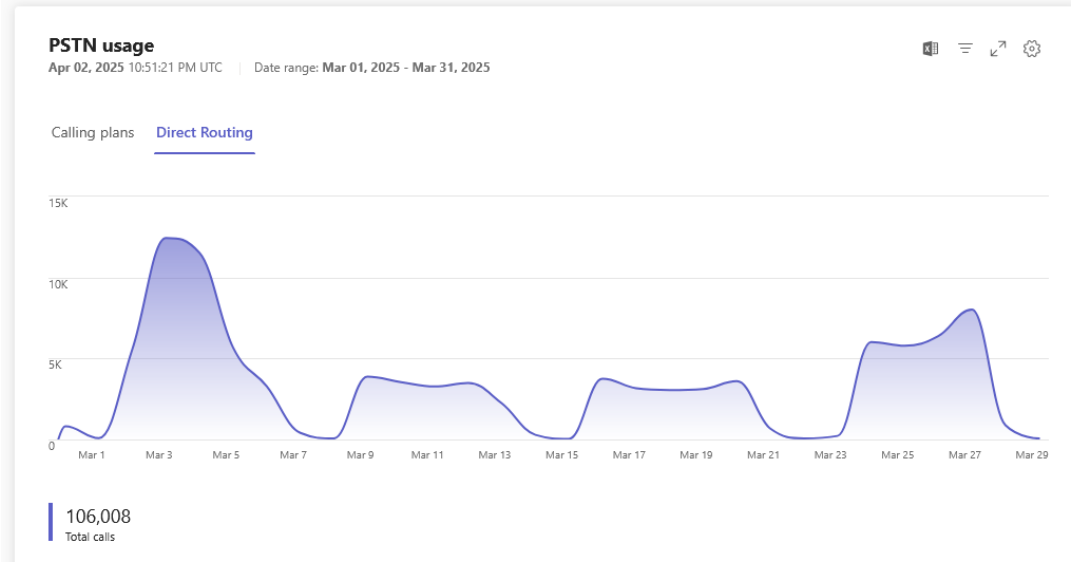


Ilustración 197 Estadística de tráfico

En la gráfica anterior se visualizan las tendencias de uso del servicio, en el periodo correspondiente al mes de marzo de 2025, donde se atendieron un total de 106,008 llamadas.

Servicio	Minutos Disponibles	Minutos Utilizados
Locales	Ilimitados	1187.08
Celular	1000	810.12
Nacional	Ilimitados	324.10
Internacional	700	3.30
Total		2324.6

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 marzo de 2025, se identifica que se realizaron llamadas con una duración total de 324.10 minutos.

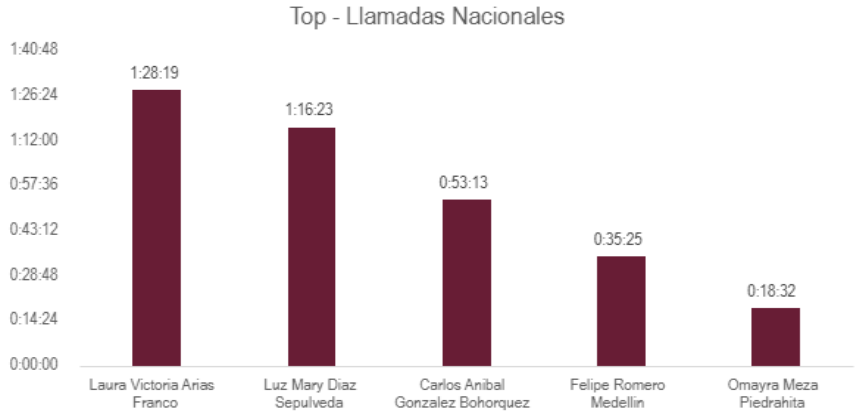


Ilustración 198 Top LDN

N°	Usuario	Área	Tiempo llamadas
1	Laura Victoria Arias Franco	Riesgos Laborales Antioquia	1:28:19
2	Luz Mary Diaz Sepulveda	Grupo de comisiones-DT-Antioquia	1:16:23
3	Carlos Anibal Gonzalez Bohorquez	Grupo de riesgos laborales - DT Antioquia	0:53:13
4	Felipe Romero Medellin	MT_Apli_Sve-Nivel Central	0:35:25
5	Omayra Meza Piedrahita	Oficina Asesora Jurídica	0:18:32

Tabla 96 Top 5 llamadas LDN

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

Con respecto a las llamadas internacionales en el mes de marzo 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 gráfico correspondiente.

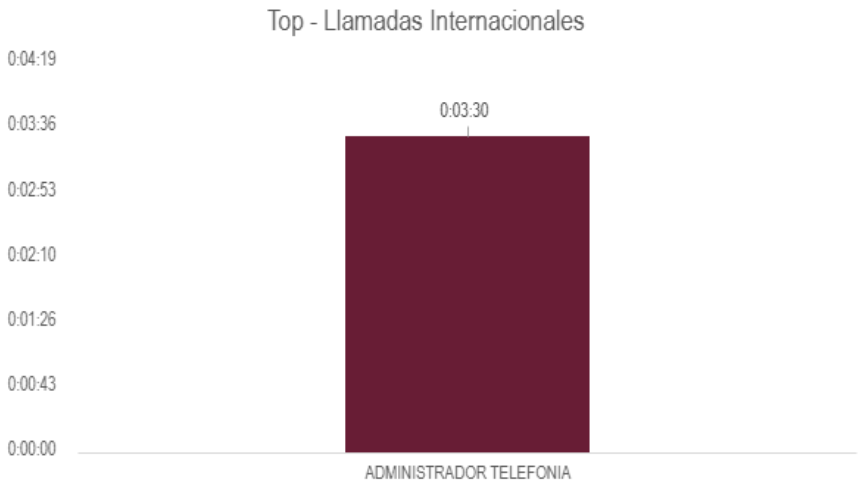


Ilustración 199 *Top LDI*

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

N°	Usuario	Área	Tiempo llamadas
1	ADMINISTRADOR TELEFONIA	UT Gestion TIC 2023	0:03:30

Tabla 97 Top 5 llamadas LDI

- **Consumo de llamadas destinos celulares**

Con respecto a las llamadas realizadas a celular en el mes de marzo de 2025, se identifica que se realizaron llamadas con una duración total de 810.12 minutos.

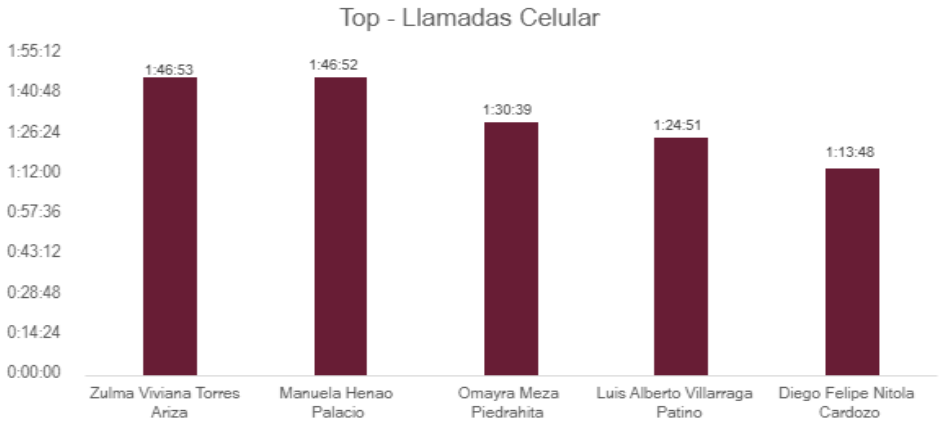


Ilustración 200 Top Celular

N°	Usuario	Área	Tiempo llamadas
1	Zulma Viviana Torres Ariza	Comunicaciones Dt Bogotá	01:46:53
2	Manuela Henao Palacio	Grupo Cobro Coactivo	01:46:52
3	Omayra Meza Piedrahita	Grupo Cobro Coactivo	01:30:39

4	Luis Alberto Villarraga Patino	Análisis y Monitoreo	01:24:51
5	Diego Felipe Nitola Cardozo	DT Boyaca	01:13:48

Tabla 98 Top 5 llamadas Celular

- **Consumo de llamadas locales**

Con respecto a las llamadas realizadas a destinos locales en el mes de marzo de 2025, se identifica que se realizaron llamadas con una duración total de 1187.08 minutos.

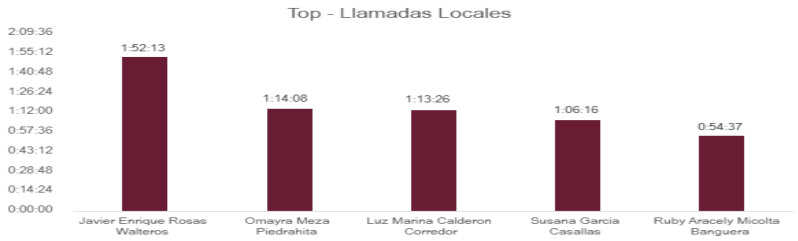


Ilustración 201 Top Local

N°	Usuario	Área	Tiempo llamadas
1	Javier Enrique Rosas Walteros	Grupo de Dirección Antioquia	01:42:13
2	Omayra Meza Piedrahita	Grupo Cobro Coactivo	01:14:08
3	Luz Marina Calderon Corredor	Grupo de comisiones	01:13:26
4	Susana Garcia Casallas	Subdirectora de Talento Humano	01:04:16
5	Ruby Aracely Micolta Banguera	Administración Control y Cargue	00:54:37

Tabla 99 Top 5 llamadas locales

- **Capacitaciones y divulgaciones**

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

Item	Descripción	Fecha
1	Divulgación de manual para uso de servicios de TOIP en Teams generado por medio de los comunicados de soporte MT	Mar-2025

Tabla 100. Capacitaciones y divulgaciones

- **Mejores Prácticas**

Se trabajará en procesos de capacitación y divulgación del uso sobre la nueva herramienta de telefonía. Se encuentra en proceso el avance de liberación de licencias a nivel nacional, de igual manera se continuará validando los backups de las grabaciones sobre las llamadas que ingresan a la mesa de servicios.

- **Medición de ANS – Telefonía IP**

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

TIP-1 Tiempo de solución de requerimientos de garantía

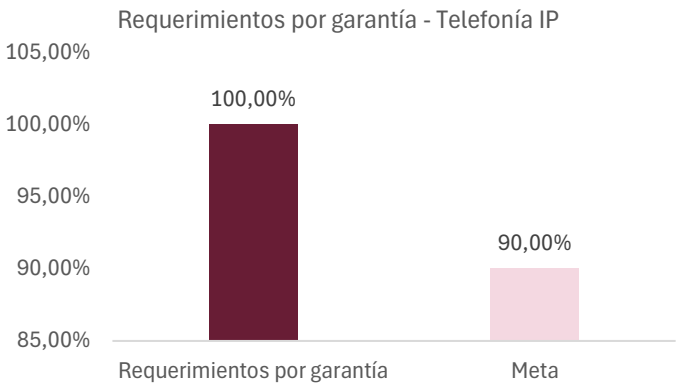


Ilustración *202 Requerimientos por garantía*

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

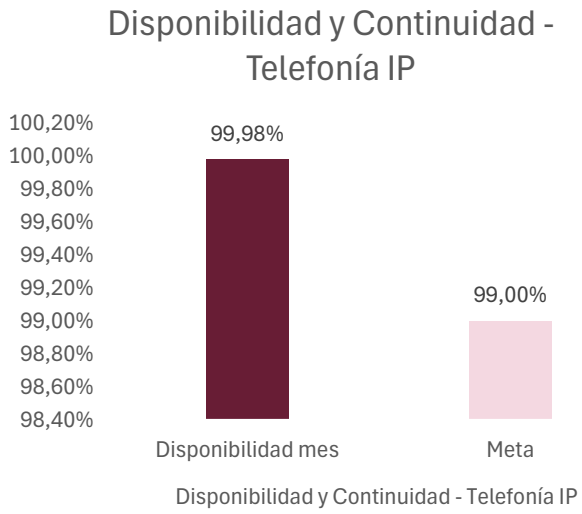


Ilustración 203 *Disponibilidad y Continuidad TOIP*

En el periodo correspondiente al mes de marzo, 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	99,98%	99,00%
TIP-3	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 101 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 102 Inventario de UPS – 10kVA

Las novedades presentadas son:

- **Territorial Tolima:** La acometida está en cable rígido y es de una dimensión más grande para las borneras de la UPS, se recomienda el cambio.
- **OE Barrancabermeja:** El 07 de octubre 2024 se realiza instalación de la UPS en la nueva oficina de Barrancabermeja; se debe tener en cuenta que aún está pendiente la subsanación de las recomendaciones que el especialista solicita que se adelanten por parte del Ministerio para una óptima operación del equipo y que fueron informadas en el mes de septiembre 2024:
    - Breaker totalizador de UPS: Se solicita reemplazar por un totalizador de 3x60 amperios.
    - Llave de Bypass: Se solicita reemplazar por una llave de 60 amperios.
    - Tomas para conexión de nueva UPS: Se solicita la instalación de clavija de 50 amperios en cada toma y a esta clavija la instalación de cola de cable encauchetado

3x8 de 2 metros, con esto se realizara la conexión de la nueva UPS.
- Instalación de Aire Acondicionado.



RE_ Disposición de
UPS en la sede del mi

- **Territorial Caldas:** Se remitió informe técnico a la entidad donde se recomienda:
  - Realizar la correcta instalación en los puestos de trabajo afectados de las tomas normales, con su debida independización de acometidas, utilizando los colores según reglamento de instalaciones eléctricas RETIE.
  - Realizar una validación del estado actual de todas las conexiones eléctricas y acometidas de distribución tanto normales como reguladas de la oficina MINITRABAJO MANIZALES, con el fin de identificar o descartar otros casos similares donde la red regulada y normal estén interconectadas.
  - Es recomendable una reestructuración urgente de cableado eléctrico de las acometidas de distribución en la oficina, debido a las condiciones no adecuadas de instalación en sus acometidas eléctricas, las cuales cuentan con muchas conexiones y derivaciones hechizas o caseras, sin el debido reglamento de instalaciones eléctricas RETIE siendo esto posibles causas del bloqueo del equipo UPS



informe UPS
Manizales.pdf

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 supervisión del contrato en el INFORME UT GESTION TIC 2023 - ENTREGA LINEA DE SERVICIO EER UPS

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

4.4.3. UPS 20 kVA

SEDE	POBLACIÓN Y/O CIUDAD	UBICACIÓN EN LA SEDE	MARCA	REFERENCIA UPS	NUMERO DE SERIE UPS
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 23	ABLEREX	KRONOS UL20D	TD8004CC80020
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 22	ABLEREX	KRONOS UL20D	TD2110B2M0006
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 21	ABLEREX	KRONOS UL20D	TD8004CC80001
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 20	ABLEREX	KRONOS UL20D	TD8004CC80025
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 19	ABLEREX	KRONOS UL20D	TD8004CC80023
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 18	ABLEREX	KRONOS UL20D	TD8004CC80012
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 17	ABLEREX	KRONOS UL20D	TD2110B2M0004
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 10	ABLEREX	KRONOS UL20D	TD9121BAS0008
SEDE NIVEL CENTRAL	BOGOTÁ	Centro de cableado piso 9	ABLEREX	KRONOS UL20D	TD8004CC80015

SEDE	POBLACIÓN Y/O CIUDAD	UBICACIÓN EN LA SEDE	MARCA	REFERENCIA UPS	NUMERO DE SERIE UPS
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 103 Inventario de UPS – 20Kva

- **Gestión del servicio**

Las UPS se encuentran operativas en cada sede de tal manera que actúen en caso de presentarse falla en el fluido eléctrico, no se presentan fallas en el servicio que requieran cambios de equipos en ninguna sede ni gestión de garantías.

Se escala al ministerio en febrero 2025, novedad con la UPS en la territorial de Santander (Bucaramanga) propiedad de la entidad, ya que se encontró que hay picos de voltaje de entrada con valores de 135V, se requiere hacer validación con la empresa proveedora de energía ya que de lo contrario sería necesario adquirir un regulador de voltaje para corregir las alertas que está presentando la UPS. Al cierre de este período no se tiene ningún avance por parte de la entidad.

Durante el período del informe se presentan los siguientes casos de soporte para los equipos de Energía Regulada UPS:

- IM-92452, IM-92455, IM-92463, IM-92466, IM-92489, IM-92497, IM-92500, IM-92502, IM-92503, IM-92505, IM-92509, IM-92510 y IM-92511, asociados al Mantenimiento Eléctrico en Nivel Central a cargo del edificio WTC.
- IM-95587 de la UPS de la DT Antioquia / Medellín asociada a pruebas de la sede, se realiza encendido de los equipos sin novedad después de las pruebas realizadas.

- **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 104 Medición ANS Energía Eléctrica UPS

4.5. No aplica

4.6. Outsourcing de Impresión

A continuación, se relacionan las actividades relevantes para este servicio:

Para el mes de marzo, el responsable del servicio gestionó un total de 891 solicitudes escaladas a través de Aranda. Al corte del mes, 878 casos quedaron en estado *Cerrado/Solucionado, 13 en estado Suspendido* (los casos suspendidos se deben a cambio de toners a espera que se agoten),

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

Nombre de Usuario	Nombre Completo	Ubicación	Blanco y Negro
lforrero	Lizeth Dahiana Forero Peralta	Nivel Central - Subdirección De Gestion Del Talento Humano	3981
pnustes	Patricia Celestial Nustes Barrera	Nivel Central - Grupo Interno De Trabajo De Relaciones Laborales	3966
bhernandez	Bibiana Hernandez Hernandez	DT Magdalena	2916
xbetancourth	Xiomara Hasleidy Betancourth Olaya	DT Florencia	2781
vfierro	Viviana Fierro Herrera	DT Valle del Cauca	2599
mnavarrog	Maria Alejandra Navarro Garcia	DT Tolima	2567
llondono	Leydy Johanna Londono Ramos	DT Valle del Cauca	2387
gcontractual	Gestion Contractual	Nivel Central – Grupo Gestión Contractual	2364
amateus	Andrea Johana Mateus Parra	DT Santander	2269
amestre	Andrea Marcela Mestre Rozo	Nivel Central - Subdirección De Gestion Del Talento Humano	2257

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

Clics Marzo.xlsx

El alcance del Outsourcing de Impresión comprende los siguientes equipos con el objetivo de proveer los servicios de impresión requeridos por la entidad:

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

Nombre de la impresora	Blanco y negro	Total Páginas
ricoh-cali-piso4	14810	14810
ricoh-bmanga-ofc305	14655	14655
ricoh-bmanga-ofc205	13936	13936
Sede central ricohpiso5a	13405	13405
Sede central ricohpiso19a	13246	13246
Sede central ricohpiso12a	12803	12803
ricoh-cali-piso3	12738	12738
ricoh-cali-piso2-atc	12700	12700
Sede central ricohpiso5b	12103	12103
Bogotá calle 32 ricohcl32-rcc	10602	10602

Tabla 106 Top 10 de impresoras con mayor uso

impresoras mas usadas Marzo.xlsx

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

Nombre de Usuario	Nombre Completo	Color
mserrano	Maguiber Serrano Nieto	2890
ymedinag	Yeisson Medina Gonzalez	1393
bhernandez	Bibiana Hernandez Hernandez	162
jrojas	Juanita Rojas Rodriguez	41

- En la siguiente tabla se muestra el Top de oficinas con mayor volumen de impresión a blanco y negro

Oficina	Blanco y negro
Centrales Dt	142116
D. T. Valle Del Cauca	57209
D. T. Bogota	48163
D. T. Santander	41433
D. T. Antioquia	35792
D. T. Norte De Santander	19400
D. T. Risaralda	16041
D. T. Quindio	13650
D. T. Tolima	13275
D. T. Huila	11214

Tabla 107 Top oficinas



Informe por oficinas marzo.xlsx

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 108 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 109 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 marzo de 2025:

MES	DETALLE	CANTIDAD
marzo	Multifuncional blanco y negro rango medio - Clic de impresión tóner y papel carta	615.807
	TOTAL	615.807

Tabla 110 Clics de Impresión de marzo 2025 – Multifuncional B/N

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

Mes 2025	Enero	Febrero	Marzo
Cantidad de clics consumidos	532.919	599.860	615.807

*Tabla 111 T*endencia 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 543.174 clics de impresión y 72.633 de fotocopias para un total de 615.807 para este servicio, superando el estimado del mes por 165.807

El administrador del servicio de outsourcing de impresión remitió semanalmente vía correo electrónico a la supervisión del contrato 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.

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

Nombre	Copias
ricoh-medellin-piso1	38395
Bogotá calle 32 ricohcl32-gau-b	33516
Bogotá calle 32 ricohcl32-rcc	31259
ricoh-bmanga-ofc205	22452
Sede central ricohpiso5b	18852
ricoh-cali-piso4	16782
ricoh-caqueta-piso1-ppal	15572
Sede central ricohpiso9a	13454
RICOH-BMANGA-OFC305	12397
Bogotá calle 32 ricohcl32-gau-a	12363

Tabla 112 Top 10 impresoras más usadas del servicio de fotocopiado

Reporte de
Fotocopias marzo.xl

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 marzo de 2025:

MES	DETALLE	CANTIDAD
marzo	Impresora color rango medio - Cargo fijo mensual - Clic de impresión tóner y papel carta	**4.078**
	TOTAL	**4.078**

Tabla 113 Clics de Impresión de marzo 2025 – Impresora Color

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

Mes 2025	Enero	Febrero	Marzo
Cantidad de clics consumidos	3.760	7.200	4.078

Tabla 114 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 4.078 clics para este servicio, superando el estimado del mes por 2.578 clics.

Asimismo, el administrador del servicio de outsourcing de impresión remitió semanalmente vía correo electrónico a la supervisión del contrato 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.



Asignacion cuotas Marzo.xlsx

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

Nombre de Usuario	Nombre Completo	Tipo de transacción	Cuota asignada en el mes	número de veces que se aumento
sleonm	Sandrith Mariana Leon Martinez	ADJUST	2027	7
xbetancourth	Xiomara Hasleidy Betancourth Olaya	ADJUST	2828	6
sdiazr	Susana Milena Diaz Reyes	ADJUST	2108	6
dmontenegro	Diana Maria Montenegro Baltazar	ADJUST	1942	6
mlopez	Maria Elda Lopez Osorio	ADJUST	1764	6
njimenez	Nidia Xiomara Jimenez Caicedo	ADJUST	1566	6
lkpena	Luz Karime Peña Garcia	ADJUST	1397	6
pgarcia	Piedad Garcia Guerrero	ADJUST	1386	6
pnustes	Patricia Celestial Nustes Barrera	ADJUST	4460	5
lforrero	Lizeth Dahiana Forero Peralta	ADJUST	3866	5

Tabla 115 Ampliación de cuota de impresión

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

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

	ene-25		feb-25		mar-25	
	Resmas Carta	Resmas Oficio	Resmas Carta	Resmas Oficio	Resmas Carta	Resmas Oficio
Total Resmas	132	153	535	455	309	182
Total Cajas por Tamaño	13,2	15,3	53,5	45,5	30,9	18,2
Total Cajas Enviadas	**28,5**		**99**		**49,1**	

Tabla 116 Despacho de papel a sedes del Ministerio del Trabajo

Durante el período, se despacharon a sedes del Ministerio un total de 54 tóners para impresora B/N, 1 unidad fusora y 2 unidades de imagen.

- **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 117 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 marzo 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.

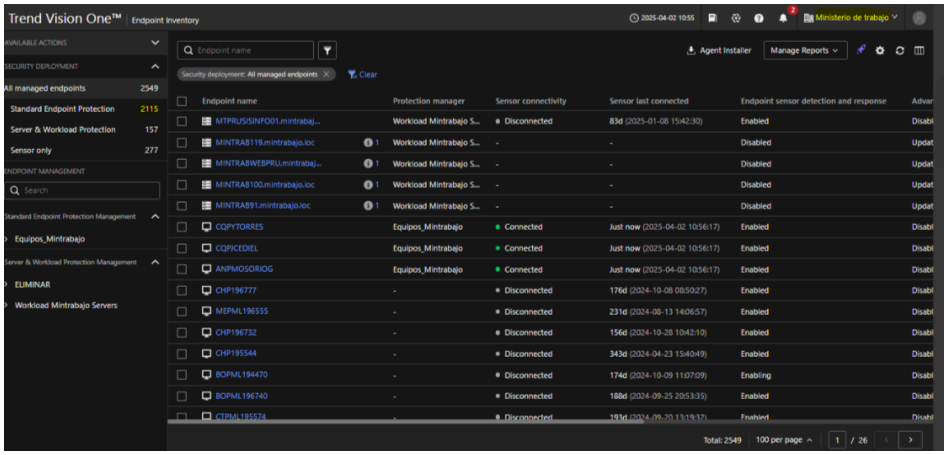


Ilustración 204 Equipos consola antivirus

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 (2115) de Mintrabajo

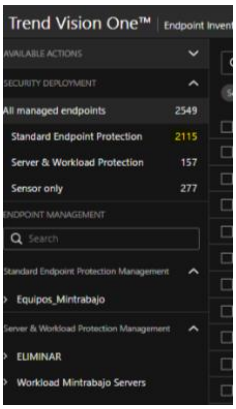


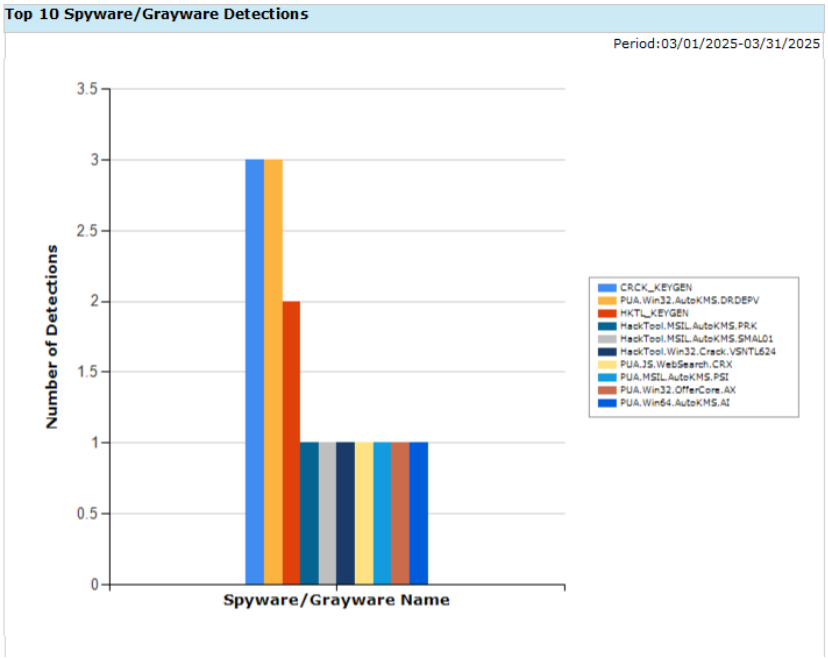
Ilustración 205 Gestión consola antivirus – equipos usuario final

4.7.3. Top 10 spyware

- Los datos reflejan la detección de herramientas potencialmente peligrosas (HackTools y PUA) en varios dispositivos tipo "Desktop".
- **HackTools (HKTL / HackTool)**:
  - **KEYGEN y AutoKMS**: Herramientas comúnmente utilizadas para la activación ilícita de software, lo que representa un riesgo de seguridad y cumplimiento normativo.
  - **RemoteAdmin y PassView**: Herramientas que pueden ser utilizadas para administración remota y recuperación de contraseñas, lo que puede indicar intentos de acceso no autorizado.
- **PUA (Potentially Unwanted Applications)**:
  - **Babylon, KeyGen, OfferCore**: Aplicaciones potencialmente no deseadas que pueden incluir adware o comportamientos que comprometen la seguridad del sistema.

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

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



Top 10 Spyware/Grayware Detections

Spyware/Grayware Name	# of Detections	Detected By
CRCK_KEYGEN	3	Desktop (3)
PUA.Win32.AutoKMS.DRDEPV	3	Desktop (3)
HKTL_KEYGEN	2	Desktop (2)
HackTool.MSIL.AutoKMS.PRK	1	Desktop (1)
HackTool.MSIL.AutoKMS.SMAL01	1	Desktop (1)
HackTool.Win32.Crack.VSNTL624	1	Desktop (1)
PUA.JS.WebSearch.CRX	1	Desktop (1)
PUA.MSIL.AutoKMS.PSI	1	Desktop (1)
PUA.Win32.OfferCore.AX	1	Desktop (1)
PUA.Win64.AutoKMS.AI	1	Desktop (1)

Tabla 118 Top spayware

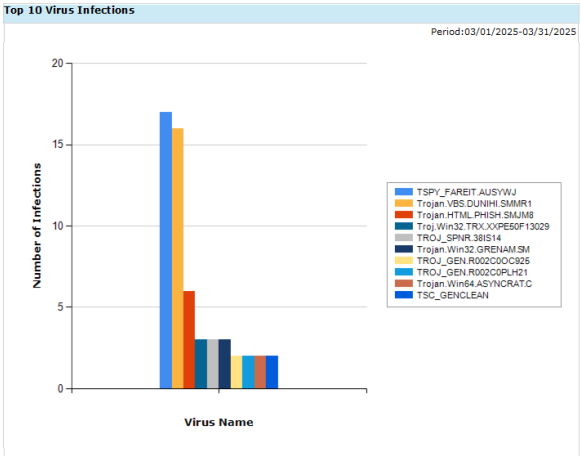
4.7.4. Top 10 Virus Detectados

Los datos reflejan la detección de múltiples amenazas de malware en equipos de escritorio, lo que sugiere una posible infección activa y un riesgo significativo para la seguridad del entorno.

Nombre del Virus	Número de Infecciones	Dispositivos Afectados	Descripción General (si aplica)
TSPY_FAREIT.AUSYWJ	17	Desktop (17)	Troyano espía que roba credenciales y datos.
Trojan.VBS.DUNIHI.SMMR1	16	Desktop (16)	Troyano basado en VBS, utilizado para descargas maliciosas.
Trojan.HTML.PHISH.SMJM8	6	Desktop (6)	Código HTML malicioso usado en ataques de phishing.

Troj.Win32.TRX.XXPE50F13029	3	Desktop (3)	Variante de troyano que afecta sistemas Windows de 32 bits.
TROJ_SPNR.38IS14	3	Desktop (3)	Troyano genérico detectado por heurística.
Trojan.Win32.GRENAM.SM	3	Desktop (3)	Troyano que puede modificar archivos del sistema.
TROJ_GEN.R002C0OC925	2	Desktop (2)	Detección genérica de un troyano en Windows.
TROJ_GEN.R002C0PLH21	2	Desktop (2)	Detección genérica de un troyano en Windows.
Trojan.Win64.ASYNCRAT.C	2	Desktop (2)	RAT (Remote Access Trojan) que permite control remoto del sistema.
TSC_GENCLEAN	2	No especificado	Posible detección genérica de un archivo sospechoso.

Tabla 119 Top 10 virus detectados



Top 10 Virus Infections

Virus Name	# of Infections	Detected By
TSPY_FAREIT.AUSYWJ	17	Desktop (17)
Trojan.VBS.DUNIHI.SMMR1	16	Desktop (16)
Trojan.HTML.PHISH.SMJM8	6	Desktop (6)
Troj.Win32.TRX.XXPE50F13029	3	Desktop (3)
TROJ_SPNR.38IS14	3	Desktop (3)
Trojan.Win32.GRENAM.SM	3	Desktop (3)
TROJ_GEN.R002C0OC925	2	Desktop (2)
TROJ_GEN.R002C0PLH21	2	Desktop (2)
Trojan.Win64.ASYNCRAT.C	2	Desktop (2)
TSC_GENCLEAN	2	Desktop (2)

Ilustración 206 Top *infección virus*

4.7.5. Servicio de Vulnerabilidades

A continuación, se muestra un resumen de los resultados, actividades y procesos relacionados al servicio de gestión de vulnerabilidades, que han sido llevadas a cabo durante el mes de marzo 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 Mauricio Fernández, Caterin Lozano.

Se informó al Ministerio de trabajo y equipo infraestructura que comenzará a ejecutar el plan de trabajo para el ethical hacking correspondiente al primer semestre 2025.

Plan de acción y remediación de vulnerabilidades

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

4.7.5.1. Inventario y licenciamiento

El inventario de activos registrado en la herramienta Tenable Nessus Professional se basa en la línea base de activos del segundo semestre proporcionada por el cliente, así como en los resultados del escaneo inicial de Discovery. En total, se han registrado 292 activos de TI.

En marzo, se alcanzó un registro de 292 activos de TI (99 %) de la línea base documentada en la herramienta.

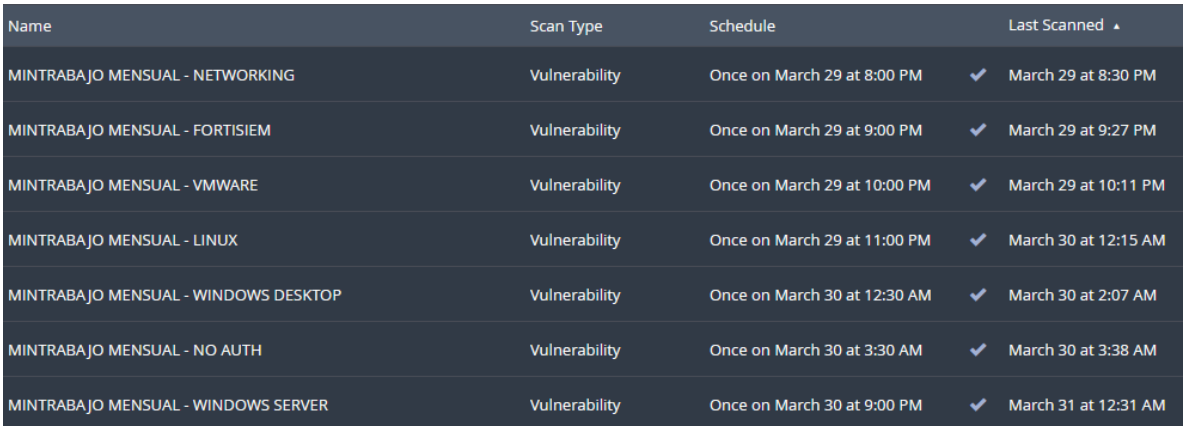


Ilustración 207 Gestión consola Nessus

4.7.5.2. Escaneos programados

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

- MINTRABAJO MENSUAL – VMWARE.
- MINTRABAJO MENSUAL – NETWORKING.
- MINTRABAJO MENSUAL – FORTISIEM.
- MINTRABAJO MENSUAL – LINUX. Rtinet.



Name	Scan Type	Schedule	Last Scanned
MINTRABAJO MENSUAL - NETWORKING	Vulnerability	Once on March 29 at 8:00 PM	March 29 at 8:30 PM
MINTRABAJO MENSUAL - FORTISIEM	Vulnerability	Once on March 29 at 9:00 PM	March 29 at 9:27 PM
MINTRABAJO MENSUAL - VMWARE	Vulnerability	Once on March 29 at 10:00 PM	March 29 at 10:11 PM
MINTRABAJO MENSUAL - LINUX	Vulnerability	Once on March 29 at 11:00 PM	March 30 at 12:15 AM
MINTRABAJO MENSUAL - WINDOWS DESKTOP	Vulnerability	Once on March 30 at 12:30 AM	March 30 at 2:07 AM
MINTRABAJO MENSUAL - NO AUTH	Vulnerability	Once on March 30 at 3:30 AM	March 30 at 3:38 AM
MINTRABAJO MENSUAL - WINDOWS SERVER	Vulnerability	Once on March 30 at 9:00 PM	March 31 at 12:31 AM

	Críticas	Altas	Medias	Bajas
MES				
Noviembre 2024	30.823	16.460	19.526	3.179
Diciembre 2024	28.604	28.530	5.316	1.836
Enero 2025	255	258	1.310	436
Febrero 2025	133	323	1.073	411
Marzo 2025	1.352	5.487	439	74

Tabla 120 Total de vulnerabilidades

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

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

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

4.7.5.3. TOP 10 – Vulnerabilidades más explotables

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

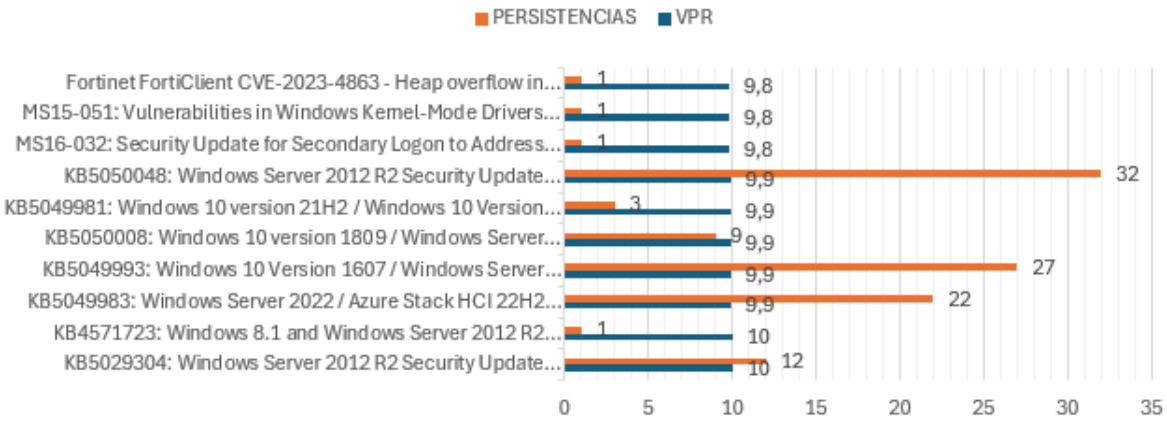


Tabla 121 TOP 10 - Activos más explotables

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

4.7.5.4. Estrategia de remediación y/o mitigación

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

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

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

4.7.5.5. Resumen de mitigación efectuada

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

- 695 vulnerabilidades críticas.
- 798 vulnerabilidades altas.
- 1.848 vulnerabilidades medias.
- 441 vulnerabilidades bajas.

Durante el periodo de marzo 2025, no se remediaron vulnerabilidades semestrales debido a varias actividades prioritarias que tenían que gestionar el área de infraestructura. Por otro lado, con relación a indicadores semestrales, se han gestionado un total de 858 vulnerabilidades TI, de las cuales, 155

fueron en la severidad crítica, 150 en la severidad alta, 488 en la severidad media y 65 en la severidad baja.

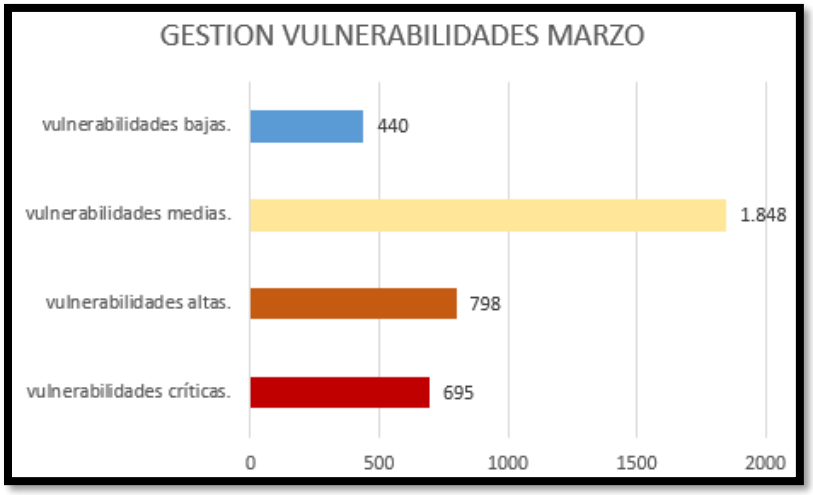


Ilustración 208 Vulnerabilidades gestionadas vs en remediación

Dando cumplimiento al reporte semestral de vulnerabilidades, se realiza envió a la supervisión del contrato, el informe de vulnerabilidades correspondiente al primer semestre del 2025, se adjunta informe socializado.

Reporte
Vulnerabilidades Mi

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

MINTRABAJO -
VULNERABILIADES C

4.7.5.6. Ethical Hacking Primer semestre 2025

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

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

- **Medición de ANS Antivirus**

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

ID	Indicadores	Resultado	Meta
AV-1	Cobertura de antivirus	97,70%	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 122 Medición de ANS Antivirus

5. GESTIÓN DE CALIDAD DE INFORMACIÓN

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

- **Calidad documental de Casos:** Realizando la revisión y cumplimiento de los criterios definidos en la calidad documental de los casos registrados en la herramienta de gestión.

- **Calidad de Llamadas:** Realizando la revisión y cumplimiento de los criterios definidos en los casos atendidos por el centro de servicio por medio de llamadas telefónicas.

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

5.1 Metodología calidad documental de casos

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



Ilustración 209 Criterios calidad documental casos

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

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

Criterios	Parámetros
Redacción y Ortografía	Se evalúa la ortografía y redacción de la documentación, además que se encuentre de acuerdo con los criterios establecidos y en coherencia con la solución.

Tabla 123 Criterios y parámetros calidad documental casos

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

5.2 Evaluación calidad documental de casos

En marzo, se realizó la evaluación cuantitativa de la muestra de 267 casos documentados en la Herramienta de Gestión.

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

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

Tabla 124 Errores cometidos

Se identificaron 17 errores con un porcentaje de cumplimiento consolidado de 99,51%.

De la muestra evaluada, se tiene el siguiente el top 3 de los ítems con más errores identificados:

En la evaluación del periodo, se presentaron 6 errores en solución, 4 novedades en ortografía y redacción y 4 en cumplimiento de ANS

Las retroalimentaciones a los especialistas/responsables, se realizará en el mes de abril a través de sesiones para las mejoras correspondientes

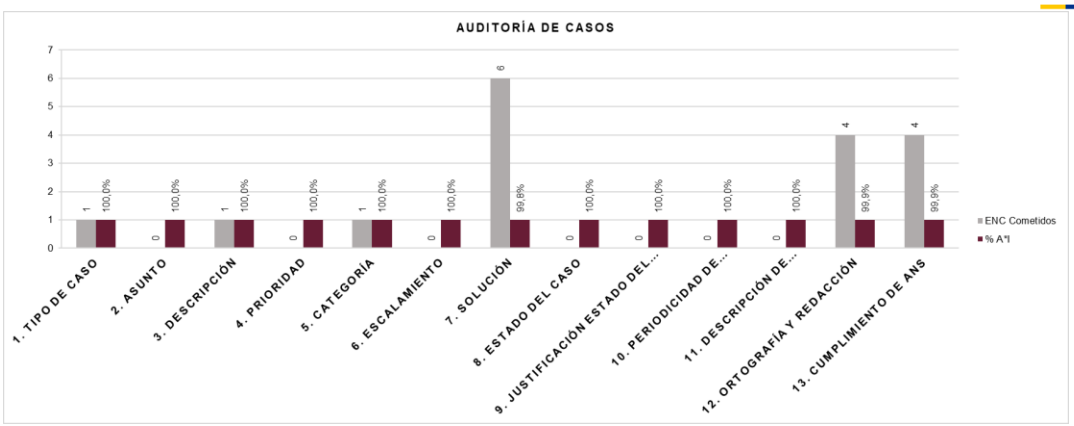


Ilustración 210 Resultados auditoria de casos

5.3 Metodología de calidad de llamadas

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

PRECISIÓN ERROR NO CRÍTICO – PENC



Ilustración 211 Precisión error no Critico de llamadas

PRECISIÓN ERROR CRÍTICO – PEC

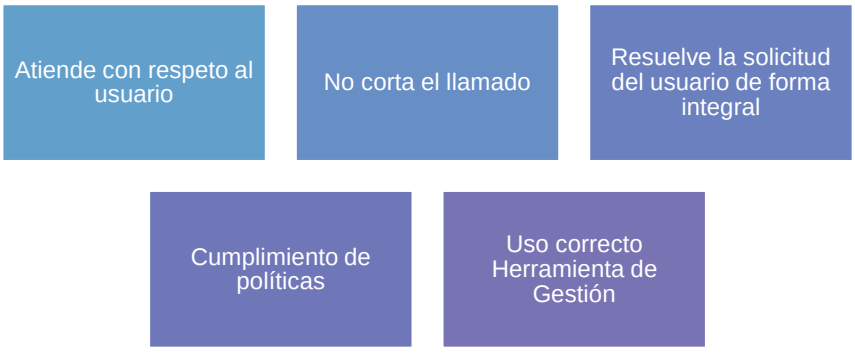


Ilustración 212 Precisión error Critico de llamadas

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

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

PRECISIÓN ERROR NO CRÍTICO – PENC

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

Tabla 125 PRECISIÓN ERROR NO CRÍTICO – PENC

PRECISIÓN ERROR CRÍTICO – PEC

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

Tabla 126 Criterios y parámetros calidad de llamadas

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

PRECISIÓN ERROR NO CRÍTICO - PENC
1. Bienvenida y Personalización (10%)
2. Escucha Activa (10%)

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

Tabla 127 Calificación Calidad llamadas

5.4 Evaluación de calidad de llamadas

En el mes de marzo de 2025, se realizó la evaluación cuantitativa de la muestra de las llamadas presentadas con una duración mayor a 1:30 minutos

Para el cálculo de llamadas, se evalúan por cada caso, los criterios definidos, obteniendo el siguiente resultado:

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

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

Tabla 128 Resultado de criterios y parámetros - Calidad de llamadas

Una vez realizada la revisión individual de las llamadas, se realiza el siguiente análisis frente a los resultados de las 17 llamadas evaluadas:

Se presentaron con la categoría de errores no críticos por los siguientes criterios:

- Escucha Activa, Empatía y adaptabilidad al usuario y Bienvenida y Personalización:

Del análisis realizado, se presenta el siguiente resultado global por categoría:

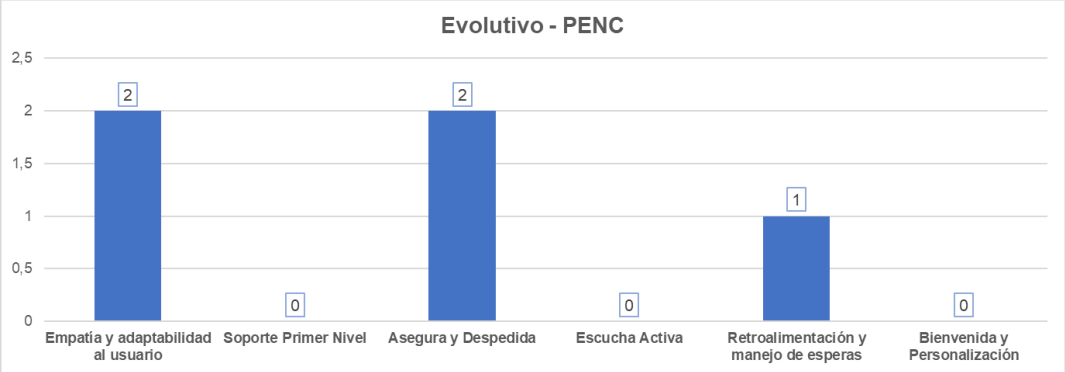


Ilustración 213 Resultados llamadas PENC

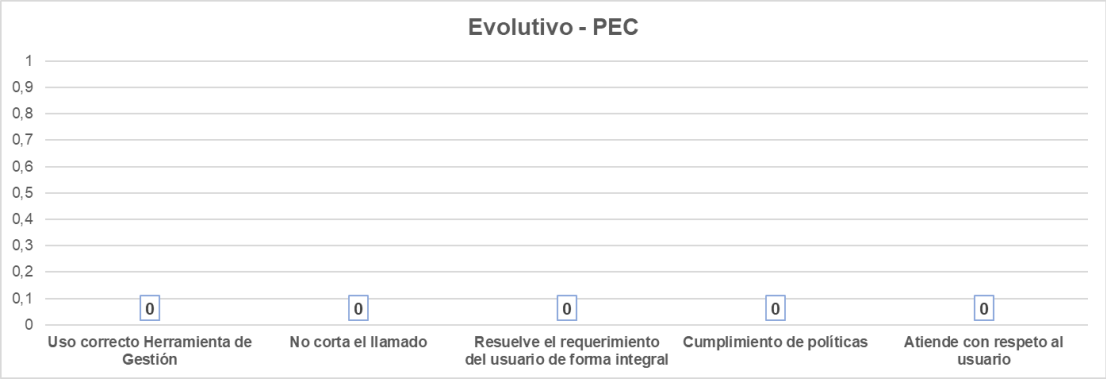


Ilustración 214 Resultados llamadas PEC

6. GESTION DE RIESGOS

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

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

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

SERVICIO/ PRÁCTICA	NOMBRE	DESCRIPCIÓN	¿MATERIALIZADO?	ACCIONES PARA REALIZAR
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 129 Seguimiento a riesgos

7. BOLSA DE RECURSOS

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

Descripción	Cantidad	Precio total antes de IVA
Switch de acceso 48 puertos	8	$3.949.912
Clics adicionales blanco y negro	145878	$ 20.422.920
Clics adicionales color	2578	$ 1.482.350
	Subtotal	$ 25.855.182

Tabla 130 Bolsa de Recursos

8. MEDICIÓN DE ACUERDOS DE NIVEL DE SERVICIO

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

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

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

Se incluye información actualizada del reporte de ANS

Área	Nombre Indicador	Resultado	Meta
Mesa de Servicio	Tiempo de atención de solicitudes por soporte en sitio	99,09%	95,00%
	Tiempo de solución de incidentes por soporte en sitio	100,00%	90,00%
	Tiempo de solución de requerimientos por soporte en sitio	100,00%	90,00%
	Tiempo de respuesta de la mesa de servicio	100,00%	85,00%
	Abandono de llamadas	0%	Máximo 8,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Equipos de usuario final	Tiempo de solución de requerimientos de garantía	93,75%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
ANTIVIRUS	Cobertura de antivirus	97,70%	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%

Área	Nombre Indicador	Resultado	Meta
	Continuidad y disponibilidad del datacenter alterno	100,00%	99,60%
	Continuidad y disponibilidad de la plataforma de procesamiento, almacenamiento y respaldo	100,00%	99,70%
	Tiempo de solución de incidentes asociado a los servicios de aplicaciones especializadas	100,00%	90,00%
	Tiempo de solución de requerimientos asociado a los servicios de aplicaciones especializadas	100,00%	90,00%
	Continuidad y disponibilidad de los servicios de directorio activo	100,00%	99,60%
	Continuidad y disponibilidad de los servicios de seguridad informática	100,00%	99,90%
	Tiempo de solución de incidentes asociado a los servicios de administración, soporte y monitoreo	100,00%	90,00%
	Tiempo de solución de requerimientos asociado a los servicios de administración, soporte y monitoreo	100,00%	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	99,98%	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 131 Medición de Acuerdos de Niveles de Servicio marzo 2025

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

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

Cumplimiento en la entrega del informe de gestión mensual para todos los servicios

Meta de cumplimiento del indicador del **100%**, se entrega el informe a la Supervisión del Contrato dentro del tiempo comprometido.

9. ANEXOS

- Certificación_backup_servidores
- Asignacion cuotas Marzo
- detalle_llamadas_recibidas_(01.03.2025-31.03.2025)
- Datos_Mintrabajo_marzo

FIN DEL DOCUMENTO