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

Enero de 2025

DOCUMENTO/ ARCHIVO	
Código:	**Informe Gestión - Unión Temporal Gestión TIC 2023**
Nombre Archivo:	**Informe Gestión - Unión Temporal Gestión TIC 2023 – Enero 2025**
Fecha:	10/02/2025
Versión:	1

REGISTRO DE CAMBIOS			
Versión	**Páginas**	**Fecha Modificación**	**Motivo del cambio**
1	205	10/02/2025	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 15
Objetivo 15
Alcance 15
Definición de Siglas y Expresiones Técnicas 15
1 GERENCIA Y/O ADMINISTRACIÓN 17
2 LÍNEA DE GESTIÓN DE SERVICIOS 17
2.1. Gestión del Servicio 17
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 22
2.1.2.3. Práctica Activos 22
2.1.2.4. Práctica Catálogo de servicios 23
2.1.2.5. Práctica de Problemas 24
2.1.2.6. Práctica de Incidentes 27
2.1.2.7. Práctica de Requerimientos 31
2.1.2.8. Práctica de Eventos 33
2.1.2.9. Práctica de Disponibilidad 42
2.1.2.10. Práctica de Implementación 44
2.2. Mesa de Servicios y Soporte en Sitio 45
3. LINEA DE SERVICIOS CENTRALES 64
3.1. Datacenter 64
3.1.1. Datacenter Principal 64
3.1.2. Datacenter Alterno y DRP 71
3.1.3. Procesamiento, Almacenamiento y Respaldo 74
3.1.4. Aplicaciones Especializadas 79
3.1.5. **No aplica** 141
3.1.6. Seguridad Informática 141
3.1.6.1. Firewalls de nueva generación 141
3.1.6.2. Sandbox – Amenazas día 0 145
3.1.6.3. SIEM - Solución de correlación de eventos de seguridad, disponibilidad y recursos 147
3.1.6.4. WAF - Servicio de tipo "Firewall de Aplicaciones Web" 153
3.1.6.5. Solución de Anti-DDoS 154
3.1.7. Licenciamiento 158
3.1.8. Administración, soporte y monitoreo 158
3.2. No aplica 159
3.3. Conectividad WAN, SDWAN e Internet 159
3.3.1. Canales WAN 159
3.3.1.1. Incidentes de Conectividad 160
3.3.1.2. Topología Actual 161
3.3.2. Canales SDWAN e Internet Dedicado 161
4. LINEA DE SERVICIOS EN SEDE 167
4.1. Equipos de Cómputo de usuario final 167
4.1.1. Equipos de Escritorio 169
4.1.2. Equipos Portátiles 169
4.2. Conectividad LAN y WLAN 170
4.2.1. Switch CORE Sede Principal 171
4.2.2. Switch para conexiones perimetrales (EDGE) en sede principal 171
4.2.3. Switch de acceso 24 puertos 171
4.2.4. Switch de acceso 48 puertos 172
4.2.5. Puntos de Acceso 173
4.3. Telefonía IP 174
4.3.1. Teléfono Gama Media 174
4.3.2. Teléfono Gama Baja 174

4.3.3. Troncales SIP 175
4.3.4. No Aplica 175
4.3.5. No Aplica 175
4.3.6. Módems 4G – Con plan de 50 Gbps 175
4.4. Energía Regulada UPS 180
4.4.1. UPS 10 kVA 181
4.4.2. UPS 15 kVA 182
4.4.3. UPS 20 kVA 182
4.5. No aplica 183
4.6. Outsourcing de Impresión 183
4.6.1. No aplica 185
4.6.2. Multifuncional B/N rango medio – Cargo fijo mensual 185
4.6.3. Impresora Color rango medio – Cargo fijo mensual 185
4.6.4. No aplica 185
4.6.5. Multifuncional B/N rango medio – Clic de impresión 185
4.6.6. Impresora Color rango medio – Clic de impresión 186
4.7. Antivirus 188
4.7.1. Instalaciones de antivirus en servidores 188
4.7.2. Instalación de antivirus PCs usuarios final 188
4.7.3. Top 10 spyware 189
4.7.4. Top 10 Virus Detectados 190
4.7.5. Servicio de Vulnerabilidades 191
4.7.5.1. Inventario y licenciamiento 192
4.7.5.2. Escaneos programados 192
4.7.5.3. TOP 10 – Vulnerabilidades más explotables 194
4.7.5.4. Estrategia de remediación y/o mitigación 195
4.7.5.5. Resumen de mitigación efectuada 195
4.7.5.6. Ethical Hacking Primer sementre 2025 196
5. GESTIÓN DE CALIDAD DE INFORMACIÓN 196
5.1 Metodología calidad documental de casos 197
5.2 Evaluación calidad documental de casos 197
5.3 Metodología de calidad de llamadas 198
5.4 Evaluación de calidad de llamadas 201
5.5 Mejora Encuesta de Satisfacción de Aranda 202
6. GESTION DE RIESGOS 203
7. BOLSA DE RECURSOS 206
8. MEDICIÓN DE ACUERDOS DE NIVEL DE SERVICIO 206
9. ANEXOS 208

Índice de Tablas

Tabla 1 Atención de solicitudes por grupo de especialistas 20
Tabla 2 Tipificación de cambios 22
Tabla 3 Categorías Inactivas 24
Tabla 4 Novedad Matriz de Escalamiento 24
Tabla 5 Detalle problema 47834 25
Tabla 6 Detalle problema 58357 26
Tabla 7 Listados Incidentes 27
Tabla 8 Top 10 Categorías Incidentes 27
Tabla 9 Incidentes Mayores Registrados 29
Tabla 10 KPI Práctica de Incidentes 29
Tabla 11 Causas Reaperturas 31
Tabla 12 Estados Requerimientos 32
Tabla 13 Top 10 Categorías Requerimientos 32
Tabla 14 Detalle de KIP Practica de Requerimientos 32
Tabla 15 Consolidado disponibilidad de servidores 42
Tabla 16 alarmas presentadas en el mes de enero 42
Tabla 17 Consolidada disponibilidad de Directorio Activo 42
Tabla 18 Desagregado de Disponibilidad Directorio Activo 43
Tabla 19 Consolidado disponibilidad de equipos Datacenter principal 43
Tabla 20 Desagregado de Disponibilidad Datacenter Principal 43
Tabla 21 Consolidado disponibilidad de equipos Datacenter alterno 43
Tabla 22 Desagregado Disponibilidad de equipos Datacenter alterno 43
Tabla 23 Consolidado disponibilidad de equipos redes y conectividad 43
Tabla 24 Consolidado disponibilidad de equipos de seguridad 44
Tabla 25 Disponibilidad de equipos Seguridad de la Información 44
Tabla 26 Consolidado disponibilidad de equipos de telefonía 44
Tabla 27 Consolidado disponibilidad de plataforma antivirus 44
Tabla 28 Atención de Llamadas 45
Tabla 29 Top 10 administración de servidores 46
Tabla 30 Top 10 redes y conectividad 46
Tabla 31 Top 10 seguridad informática 47
Tabla 32 Top Telefonía IP 47
Tabla 33 Top 10 soporte aplicaciones 47
Tabla 34 Top 10 soporte microinformática 48
Tabla 35 Casos Anulados por Servicio 48
Tabla 36 Casos Suspendidos por Servicio 48
Tabla 37 Incidentes solucionados por Soporte Territoriales 49
Tabla 38 Requerimientos solucionados por Mesa de Servicios 50
Tabla 39 Requerimientos solucionados por Soporte en sitio 50
Tabla 40 Requerimientos solucionados por Soportes Territoriales 51
Tabla 41 Casos cerrados por la mesa de servicios 52
Tabla 42Casos cerrados por soporte en sitio 54
Tabla 43 Casos cerrados por Territoriales 56
Tabla 44 Medio de ingreso de casos 57
Tabla 45 Visitas en sedes sin Soporte en Sitio 63
Tabla 46 Consolidado de Visitas en sedes sin Soporte en Sitio 63
Tabla 47 Medición ANS Mesa de Servicios 64
Tabla 48 capacidades de acuerdo con las fichas técnicas 67
Tabla 49 Capacidades consumidas (Sin servidores de backup) 68
Tabla 50 Capacidades SI – IVC 77
Tabla 51 Almacenamiento asignado - SI – IVC 78
Tabla 52 Instancias, documentos & radicados 104
Tabla 53 Dimensionamiento Servers IBM - Virtualización Optima 105

Tabla 54 Apps & DDBB Oracle 109
Tabla 55 Escenario de Capacidades Oracle - Estado de consumo Actual 110
Tabla 56 *Top tráfico de aplicaciones* 143
Tabla.57 Listado de requerimientos atendidos 156
Tabla 58 Licenciamiento 158
Tabla 59 Medición ANS Datacenter 159
Tabla 60 Medición ANS Nube Pública 159
Tabla 61 Novedades servicio de internet 161
Tabla 62 Sedes configuradas en enero 2025 165
Tabla 63 Medición de ANS Conectividad WAN e Internet 165
Tabla 64 Desagregado sedes con novedad un solo enlace 166
Tabla 65 Desagregado sedes con novedad doble enlace 166
Tabla 66 Cantidades de equipos a distribuir a nivel nacional 167
Tabla 67 Solicitudes de Equipos Usuario Final – Según Grupo Responsable 169
Tabla 68 Solicitudes de Equipos Usuario Final – Según Tipificación y Categoría 170
Tabla 69 Medición ANS Equipos de Usuario Final 170
Tabla 70 Top 5 de categorías en el Servicio de conectividad LAN-WLAN 171
Tabla 71 Distribución y Cantidades de switch 24 puertos 172
Tabla 72 Distribución y Cantidades de Switch 48 puertos 173
Tabla 73 Distribución de puntos de acceso 173
Tabla 74 Medición ANS LAN y WLAN 174
Tabla 75 Equipos gama media 174
Tabla 76 Sedes cerradas 175
Tabla 77 Consolidado de teléfonos gama baja 175
Tabla 78 Consolidado equipos MIFI 175
Tabla 79 Minutos, consumos 177
Tabla 80 Top 5 llamadas LDN 177
Tabla 81 Top 5 llamadas LDI 178
Tabla 82 Top 5 llamadas Celular 178
Tabla 83 Top 5 llamadas locales 179
Tabla 84 Medición ANS Telefonía IP 180
Tabla 85 Inventario de UPS – 10kVA 181
Tabla 86 Inventario de UPS – 20Kva 182
Tabla 87 Medición ANS Energía Eléctrica UPS 183
Tabla 88 Consumo de impresiones por usuario - Impresoras B/N 183
Tabla 89 Top 10 de impresoras con mayor uso 184
Tabla 90 Top de usuarios que más generaron impresiones a color 184
Tabla 91 Top oficinas 185
Tabla 92 Cargo mensual multifuncional rango medio 185
Tabla 93 Cargo mensual impresora color 185
Tabla 94 Clics de Impresión de enero 2025 – Multifuncional B/N 185
Tabla 95 tendencia de consumo de clics B/N 185
Tabla 96 Top 10 impresoras mas usadas del servicio de fotocopiado 186
Tabla 97 Clics de Impresión de enero 2025 – Impresora Color 186
Tabla 98 tendencia de consumo de clics color 186
Tabla 99 Ampliación de cuota de impresión 187
Tabla 100 Despacho de papel a sedes del Ministerio del Trabajo 187
Tabla 101 Medición ANS Outsourcing de Impresión 187
Tabla 102 Top spayware 190
Tabla 103 Total de vulnerabilidades 193
Tabla 104 TOP 10 - Activos más explotables 194
Tabla 105 Medición de ANS Antivirus 196
Tabla 106 Criterios y parámetros calidad documental casos 197
Tabla 107 Errores cometidos 198
Tabla 108 Criterios y parámetros calidad de llamadas 200
Tabla 109 Calificación Calidad llamadas 200

Tabla 110 Seguimiento a riesgos 206
Tabla 111 Medición de Acuerdos de Niveles de Servicio enero 2025 208

Tabla 1 Atención de solicitudes por grupo de especialistas 20
Tabla 2 Tipificación de cambios 22
Tabla 3 Categorías Inactivas 24
Tabla 4 Novedad Matriz de Escalamiento 24
Tabla 5 Detalle problema 47834 25
Tabla 6 Detalle problema 58357 26
Tabla 7 Listados Incidentes 27
Tabla 8 Top 10 Categorías Incidentes 27
Tabla 9 Incidentes Mayores Registrados 29
Tabla 10 KPI Práctica de Incidentes 29
Tabla 11 Causas Reaperturas 31
Tabla 12 Estados Requerimientos 32
Tabla 13 Top 10 Categorías Requerimientos 32
Tabla 14 Detalle de KIP Practica de Requerimientos 32
Tabla 15 Consolidado disponibilidad de servidores 42
Tabla 16 alarmas presentadas en el mes de enero 42
Tabla 17 Consolidada disponibilidad de Directorio Activo 42
Tabla 18 Desagregado de Disponibilidad Directorio Activo 43
Tabla 19 Consolidado disponibilidad de equipos Datacenter principal 43
Tabla 20 Desagregado de Disponibilidad Datacenter Principal 43
Tabla 21 Consolidado disponibilidad de equipos Datacenter alterno 43
Tabla 22 Desagregado Disponibilidad de equipos Datacenter alterno 43
Tabla 23 Consolidado disponibilidad de equipos redes y conectividad 43
Tabla 24 Consolidado disponibilidad de equipos de seguridad 44
Tabla 25 Disponibilidad de equipos Seguridad de la Información 44
Tabla 26 Consolidado disponibilidad de equipos de telefonía 44
Tabla 27 Consolidado disponibilidad de plataforma antivirus 44
Tabla 28 Atención de Llamadas 45
Tabla 29 Top 10 administración de servidores 46
Tabla 30 Top 10 redes y conectividad 46
Tabla 31 Top 10 seguridad informática 47
Tabla 32 Top Telefonía IP 47
Tabla 33 Top 10 soporte aplicaciones 47
Tabla 34 Top 10 soporte microinformática 48
Tabla 35 Casos Anulados por Servicio 48

Tabla 36 Casos Suspendidos por Servicio 48
Tabla 37 Incidentes solucionados por Soporte Territoriales 49
Tabla 38 Requerimientos solucionados por Mesa de Servicios 50
Tabla 39 Requerimientos solucionados por Soporte en sitio 50
Tabla 40 Requerimientos solucionados por Soportes Territoriales 51
Tabla 41 Casos cerrados por la mesa de servicios 52
Tabla 42Casos cerrados por soporte en sitio 54
Tabla 43 Casos cerrados por Territoriales 56
Tabla 44 Medio de ingreso de casos 57
Tabla 45 Visitas en sedes sin Soporte en Sitio 63
Tabla 46 Consolidado de Visitas en sedes sin Soporte en Sitio 63
Tabla 47 Medición ANS Mesa de Servicios 64
Tabla 48 capacidades de acuerdo con las fichas técnicas 67
Tabla 49 Capacidades consumidas (Sin servidores de backup) 68
Tabla 50 Capacidades SI – IVC 77
Tabla 51 Almacenamiento asignado - SI – IVC 78
Tabla 52 Instancias, documentos & radicados 104
Tabla 53 Dimensionamiento Servers IBM - Virtualización Optima 105
Tabla 54 Apps & DDBB Oracle 109
Tabla 55 Escenario de Capacidades Oracle - Estado de consumo Actual 110
Tabla 56 *Top tráfico de aplicaciones* 143
Tabla.57 Listado de requerimientos atendidos 156
Tabla 58 Licenciamiento 158
Tabla 59 Medición ANS Datacenter 159
Tabla 60 Medición ANS Nube Pública 159
Tabla 61 Novedades servicio de internet 161
Tabla 62 Sedes configuradas en enero 2025 165
Tabla 63 Medición de ANS Conectividad WAN e Internet 165
Tabla 64 Desagregado sedes con novedad un solo enlace 166
Tabla 65 Desagregado sedes con novedad doble enlace 166
Tabla 66 Cantidades de equipos a distribuir a nivel nacional 167
Tabla 67 Solicitudes de Equipos Usuario Final – Según Grupo Responsable 169
Tabla 68 Solicitudes de Equipos Usuario Final – Según Tipificación y Categoría 170
Tabla 69 Medición ANS Equipos de Usuario Final 170
Tabla 70 Top 5 de categorías en el Servicio de conectividad LAN-WLAN 171
Tabla 71 Distribución y Cantidades de switch 24 puertos 172
Tabla 72 Distribución y Cantidades de Switch 48 puertos 173

Tabla 73 Distribución de puntos de acceso 173
Tabla 74 Medición ANS LAN y WLAN 174
Tabla 75 Equipos gama media 174
Tabla 76 Sedes cerradas 175
Tabla 77 Consolidado de teléfonos gama baja 175
Tabla 78 Consolidado equipos MIFI 175
Tabla 79 Minutos, consumos 177
Tabla 80 Top 5 llamadas LDN 177
Tabla 81 Top 5 llamadas LDI 178
Tabla 82 Top 5 llamadas Celular 178
Tabla 83 Top 5 llamadas locales 179
Tabla 84 Medición ANS Telefonía IP 180
Tabla 85 Inventario de UPS – 10kVA 181
Tabla 86 Inventario de UPS – 20Kva 182
Tabla 87 Medición ANS Energía Eléctrica UPS 183
Tabla 88 Consumo de impresiones por usuario - Impresoras B/N 183
Tabla 89 Top 10 de impresoras con mayor uso 184
Tabla 90 Top de usuarios que más generaron impresiones a color 184
Tabla 91 Top oficinas 185
Tabla 92 Cargo mensual multifuncional rango medio 185
Tabla 93 Cargo mensual impresora color 185
Tabla 94 Clics de Impresión de enero 2025 – Multifuncional B/N 185
Tabla 95 tendencia de consumo de clics B/N 185
Tabla 96 Top 10 impresoras mas usadas del servicio de fotocopiado 186
Tabla 97 Clics de Impresión de enero 2025 – Impresora Color 186
Tabla 98 tendencia de consumo de clics color 186
Tabla 99 Ampliación de cuota de impresión 187
Tabla 100 Despacho de papel a sedes del Ministerio del Trabajo 187
Tabla 101 Medición ANS Outsourcing de Impresión 187
Tabla 102 Top spayware 190
Tabla 103 Total de vulnerabilidades 193
Tabla 104 TOP 10 - Activos más explotables 194
Tabla 105 Medición de ANS Antivirus 196
Tabla 106 Criterios y parámetros calidad documental casos 197
Tabla 107 Errores cometidos 198
Tabla 108 Criterios y parámetros calidad de llamadas 200
Tabla 109 Calificación Calidad llamadas 200

Tabla 110 Seguimiento a riesgos 206
Tabla 111 Medición de Acuerdos de Niveles de Servicio enero 2025 208

Ilustración 1 Volumetría de casos en el períodoio 20
Ilustración 2 KPI Efectividad de Resolución de Incidentes de Servicio 30
Ilustración 3 KPI Incidentes de Reabiertos en el periodo 30
Ilustración 4 KPI Efectividad de Resolución de Requerimientos de Servicio 33
Ilustración 5 KPI Requerimientos de Reabiertos en el periodo 33
Ilustración 6 Access Point alarmados por sede 35
Ilustración 7 Causas de alertamiento AP 35
Ilustración 8 Servidores alertados por plataforma 36
Ilustración 9 Distribución de servidores alertados 36
Ilustración 10 Causas de alertamientos (Servidores) 37
Ilustración 11 Casos solucionados vs casos suspendidos (servidores) 37
Ilustración 12 Switches alarmados por sede 38
Ilustración 13 Casos solucionados vs casos suspendidos 38
Ilustración 14 Causas de incidentes (Switches) 39
Ilustración 15 Routers alarmados por sede 39
Ilustración 16 Causas de alertamiento (Routers) 40
Ilustración 17 Grafica de CPU 41
Ilustración 18 Grafica de memoria Zabbix 41
Ilustración 19 Atención de Llamadas 45
Ilustración 20 Incidentes Solucionados por Soportes Territoriales 49
Ilustración 21 Requerimientos Solucionados por la Mesa de Servicios 50
Ilustración 22 Requerimientos Solucionados por Soporte en sitio 50
Ilustración 23 Requerimientos solucionados por Soportes Territoriales 51
Ilustración 24 Casos cerrados por la mesa de servicios 52
Ilustración 25 Casos cerrados por Soporte en Sitio 54
Ilustración 26 Casos cerrados por Territoriales 56
Ilustración 27 Modo de Ingreso de Solicitudes 57
Ilustración 28 Guion inicial para el modelo de machine learning 58
Ilustración *29* Cumplimiento WSUS 65
Ilustración 30 Estado final de los casos Windows 66
Ilustración 31 Casos por categorías Windows 66
Ilustración 32 *Estado final de los casos Nube privada* 67
Ilustración 33 Casos por categoría Nube privada y pública 67
Ilustración 34 Proyección de Modelo de Suscripción 69
Ilustración 35 Modelo de Tenant bajo arquitectura 69
Ilustración 36 Comportamiento SWCORE Datacenter Colombia XV 70
Ilustración 37. Grafica de consumo canal Internet Datacenter 70
Ilustración 38 Diagrama Interoperabilidad Bogotá CXV 71
Ilustración 39 VM Replicadas a través de site recovery 72
Ilustración 40 Diagrama de Replicación CXV - Santa Mónica 72
Ilustración 41 Grafica de consumo LanToLan extremo Cali 73
Ilustración 42 Estado SWCORE Datacenter alterno 73
Ilustración 43 Detalle servidor 78
Ilustración 44 consumo de almacenamiento 79
Ilustración *45* Estado final de casos – Aplicaciones Especializadas 85
Ilustración 46 categorías Apps 86
Ilustración 47 Grafica de indisponibilidad del servicio 86
Ilustración 48 Acceso FILCO tras la indisponibilidad 87
Ilustración 49 Evento Alto - Trend Vision One 87
Ilustración 50 Historial de Eventos Anti-Malware 88
Ilustración 51 Estad Anti-Malware Servidores reportados 88
Ilustración 52 Eventos Noviembre FILCO 88
Ilustración 53 Evento Ejecución línea de comando 89

Ilustración 54 Evento terminado - Ejecución Línea de comando 89
Ilustración 55 Evento terminado - Ejecución línea de comando 90
Ilustración 56 Archivos modificados durante el evento 90
Ilustración 57 Estado pre-ventana 94
Ilustración 58 Generación de Backups DDBB 94
Ilustración 59 Validación Tablas DDBB 95
Ilustración 60 Validación Tablas DDBB 95
Ilustración 61 Validación Tablas DDBB 95
Ilustración 62 Validación Tablas DDBB 96
Ilustración 63 Validación Tablas DDBB 96
Ilustración 64 Validación Tablas DDBB 96
Ilustración 65 validación Tablas DDBB 97
Ilustración 66 Verificación Registros 97
Ilustración 67 Verificación Registros 97
Ilustración 68 Verificación Registros tras ejecución de procesos 98
Ilustración 69 Validación de estado de tablas tras ejecución de procesos 98
Ilustración 70 Estado de instancias DDDB 98
Ilustración 71 Eliminación de instancias 99
Ilustración 72 Disminución de instancias tras ejecución de proceso 99
Ilustración 73 Estado del servidor - pre-desfragmentación 99
Ilustración 74 Ejecución desfragmentación 100
Ilustración 75 Ejecución desfragmentación 100
Ilustración 76 Ejecución desfragmentación 100
Ilustración 77 Reconstrucción de Índices 101
Ilustración 78 Validación de tamaños de tablas 101
Ilustración 79 Validación de tamaños de tablas 101
Ilustración 80 Validación de tamaños de tablas 102
Ilustración 81 Validación de tamaños de tablas 102
Ilustración 82 Validación de tamaños de tablas 102
Ilustración 83 Validación de tamaños de tablas 103
Ilustración 84 Validación de tamaños de tablas 103
Ilustración 85 Ejecución de estadísticas de validación 103
Ilustración 86 Antes del Mantenimiento. 105
Ilustración 87 Después del Mantenimiento. 105
Ilustración 88 Distribución de licencias Oracle 106
Ilustración 89 Licencias ambientes 106
Ilustración 90 Estado final casos GD 106
Ilustración 91 casos DDBB 108
Ilustración *92* Estado Bases de Datos 108
Ilustración 93 Información base de datos – Servidor 110
Ilustración 94 Estadísticas CPU 110
Ilustración 95 Estadísticas Memoria 111
Ilustración 96 Estadísticas Pool compartido 111
Ilustración 97 Tamaño DDBB 111
Ilustración 98 Tamaño Esquema DDBB 111
Ilustración 99 Rendimiento DDBB 112
Ilustración 100 DDBB por Server 112
Ilustración 101 Host e Instancia CPU 112
Ilustración 102 Estadísticas Memoria 112
Ilustración 103 Estadística Shared Pool 113
Ilustración 104 Tamaño DDBB DBMINTRA 113
Ilustración 105 Tamaño Esquema DDBB 113
Ilustración 106 Rendimiento DDBB MINTRASG 113
Ilustración 107 Información DDBB PLIFERAY 114
Ilustración 108 Host e Instancia CPU 114
Ilustración 109 Estadísticas Memoria 114

Ilustración 110 Estadísticas Shared Pool 114
Ilustración 111 Tamaño DDBB PLifeRay 115
Ilustración 112 Tamaño Esquemas DDBB 115
Ilustración 113 Rendimiento DDBB PlifeRay 115
Ilustración 114 Información DDBB SIGEP 116
Ilustración 115 Estadística Host e Instancia 116
Ilustración 116 Estadística Memoria 116
Ilustración 117 Estadística Shared Pool 116
Ilustración 118 Tamaño DDBB SIGEP 117
Ilustración 119 Tamaño Esquema DDBB 117
Ilustración 120 Rendimiento DDBB SIGEP 117
Ilustración 121 Información DDBB DBSIMPC 118
Ilustración 122 Estadística CPU 118
Ilustración 123 Estadística Memoria 118
Ilustración 124Estadística Shared Pool 118
Ilustración 125 Tamaño DDBB SIMPC 119
Ilustración 126 Tamaño Esquema DDBB 119
Ilustración 127 Rendimiento DDBB 119
Ilustración 128 Información servidor DBBB 120
Ilustración 129 Host e Instancia CPU 120
Ilustración 130 Estadística memoria 120
Ilustración 131 Estadística Shared Pool 120
Ilustración 132 Tamaño DDBB MINTRASD 121
Ilustración 133 Tamaño Esquemas 121
Ilustración 134 Rendimiento MINTRASD 121
Ilustración 135 Información Server DDBB 122
Ilustración 136 Host e Instancia CPU 122
Ilustración 137 Estadística Memoria 122
Ilustración 138 Estadística Shared Pool 123
Ilustración 139 Tamaño DDBB 123
Ilustración 140 Tamaño DDBB 123
Ilustración 141 Rendimiento DDBB 123
Ilustración 142 Información Server DDBB 124
Ilustración 143 Host e Instancia CPU 124
Ilustración 144 Estadística Memoria 124
Ilustración 145 Estadística Shared Pool 125
Ilustración 146 Tamaño DDBB 125
Ilustración 147 Tamaño Esquemas DDBB 125
Ilustración 148 Rendimiento DDBB 126
Ilustración 149 Información Server DDBB 126
Ilustración 150 Estadística CPU 126
Ilustración 151 Estadística Memoria 127
Ilustración 152Estadística Shared Pool 127
Ilustración 153 Tamaño Esquemas DDBB 127
Ilustración 154 Comportamiento DDBB 128
Ilustración 155 Almacenamiento ASM 128
Ilustración 156 DiskGroup Data 128
Ilustración 157 DiskGroup Flash 129
Ilustración 158 DiskGroup Reco 129
Ilustración 159 DiskGroup Redo 129
Ilustración 160 Licenciamiento adicional componente IBM 129
Ilustración 161 Capacidades MINTRABGD08A 130
Ilustración 162 Capacidades MINTRABGD07A 130
Ilustración 163 Capacidades MINTRABGD03A 131
Ilustración 164 Capa de DDBB previo al cambio 131
Ilustración 165 Consumos capa de aplicación previo al cambio 132

Ilustración 166 Consumos capa de aplicación tras aumento de capacidades 132
Ilustración 167 Consumos capa de aplicación tras aumento de capacidades 133
Ilustración 168 Consumos capa de aplicación tras aumento de capacidades 133
Ilustración 169 Consumos capa de DDBB tras aumento de capacidades en capa de aplicación . 134
Ilustración 170 Consumos capa de DDBB tras aumento de capacidades en capa de aplicación . 134
Ilustración 171 Cantidad de instancias Antes de la Migración vs después de la Migración..... 136
Ilustración 172 Funcionalidad imprimir etiqueta..... 137
Ilustración 173 Funcionalidad imprimir etiqueta 1..... 137
Ilustración 174 Pruebas Radicación..... 137
Ilustración 175 Pruebas Radicación 1..... 138
Ilustración 176 Pruebas Radicación 2..... 138
Ilustración 177 Radicación de PQRSD 138
Ilustración 178 Comportamiento MinstrasG Cluster 140
Ilustración 179 Concurrencia de sesiones 140
Ilustración 180 Escritura sobre instancias..... 141
Ilustración181 Disponibilidad firewall 141
Ilustración182 Comportamiento ancho de banda 142
Ilustración 183 Reporte consumo ancho de banda..... 142
Ilustración Top184 tráfico de aplicaciones 143
Ilustración 185 Top 15 Authenticated Logins by VPN Connections..... 144
Ilustración 186 Failed Login Attempts by User..... 145
Ilustración 187 estadísticas de escaneo 145
Ilustración 188 performance..... 146
Ilustración 189 Licenciamiento 147
Ilustración 190 Casos de uso 148
Ilustración 191 Disponibilidad..... 149
Ilustración 192 Autenticación de seguridad 151
Ilustración 193 Violación de políticas 151
Ilustración194 Incidentes..... 151
Ilustración Disponibilidad195 de servidores- Seguridad 152
Ilustración Desempeño196 CPU 153
Ilustración 197 Top attack types..... 153
Ilustración 198 Top de ataques 154
Ilustración 199 Login fallidos 155
Ilustración *200*. Grafica de consumo canal MPLS Datacenter 159
Ilustración 201. Grafica estado del equipo MPLS Datacenter 160
Ilustración 202. Topología actualizada..... 161
Ilustración 203. Interface Fortimanager 162
Ilustración 204. Interface MPLS HUB SDWAN 162
Ilustración 205. Interface Internet HUB SDWAN..... 163
Ilustración 206. VPN SDWAN establecidas 163
Ilustración 207. Estado HUB SDWAN Datacenter 164
Ilustración 208. Recursos Fortimanager 164
Ilustración 209 Estado de casos Redes y Conectividad 171
Ilustración 210. Licencias y extensiones 176
Ilustración 211 Estadística de tráfico 176
Ilustración 212 Top LDN..... 177
Ilustración 213 *Top LDI* 178
Ilustración 214 Top Celular 178
Ilustración 215 Top Local 179
Ilustración *216 Requerimientos por garantía* 180
Ilustración 217 *Disponibilidad y Continuidad TOIP* 180
Ilustración 218 Equipos consola antivirus 188
Ilustración 219 Gestión consola antivirus – equipos usuario final 189
Ilustración 220 Top *infección virus* 191
Ilustración 221 Gestión consola Nessus 192

Ilustración 222 Puntuación VPR 193
Ilustración 223 Vulnerabilidades gestionadas vs en remediación 195
Ilustración 224 Criterios calidad documental casos 197
Ilustración 225 Resultados auditoria de casos 198
Ilustración 226 Precisión error no Critico de llamadas 199
Ilustración 227 Precisión error Critico de llamadas 199
Ilustración 228 Resultados llamadas PENC 202
Ilustración 229 Resultados llamadas PEC 202
Ilustración 230 Nueva Encuesta de Satisfacción Aranda 203

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 enero 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:

- **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.
  - Comunicado de manejo de garantías de diademas.

    20241018 garantiaDiadema.pptx
  - Actualización del fondo de pantalla para promover el diligenciamiento de la Encuesta de Satisfacción de Aranda para evaluar los servicios de TI prestados. Esto se realizó por dos semanas a partir del 9 de enero 2025.

    Publicación fondo de pantalla.msg

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

  - Apoyo para la publicación de la pieza relacionada con los Canales de Atención de la MDS para publicación en la Intranet y Guía Rápida de uso del Portal de Autogestión de Usuarios. A la fecha de corte nos indicaron que se encuentra pendiente de atención por parte del Grupo de Comunicaciones ya que actualmente no cuentan con contratista.

    20241112 Autogestión Aranda.p
  - 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.
  - Generación de comunicado para informar a funcionarios y contratistas como realizar el proceso de firmas del formato de entrega de bienes por parte del Grupo de Soporte Informático para el VoBo.

    Publicación mensaje entrega de bienes .ms
  - Generación de comunicado para recordar que la solicitud de creación de usuarios de contratistas se debe tramitar a través de la Mesa de Servicios.

RE_ Publicación
mensaje creación de u

- **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 enero 2025 no se tuvo respuesta ni novedades al respecto.

  - **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 enero 2025 no se tuvo respuesta ni novedades al respecto.

  - **Apertura Inspección de trabajo Segovia:** La sede entraba en operación en diciembre 2024 según lo informado a la UT, durante el período la inspectora asignada estuvo ausente por capacitación, sin embargo se concertó el despacho de los equipos de la sede (equipo de cómputo de escritorio con diadema, impresora con bandeja adicional, teléfono IP con su respectivo adaptador, equipo de seguridad Fortinet). También se realiza visita a la sede para conexión de equipos y verificación de equipos de conectividad WAN, los cuales no fueron encontrados, por lo anterior se está gestionando con el proveedor de servicios de conectividad la habilitación del servicio incluyendo equipos nuevos. La usuaria entro en período de vacaciones en el mes de enero 2025, el proveedor de conectividad realizó aprovisionamiento del servicio y la UT realiza visita para afinación final de servicios.

- **Gestión de cuentas de contratistas que finalizan contrato el 31/12/2024:** Se han venido reportando por demanda las novedades de contratistas desde las áreas a la MDS, pero debido a que no se cuenta con una información precisa por parte del Grupo de Gestión Contractual ya que aún se encuentran en esta gestión, el 27/01/2025 el Ing. Elkin Morales realiza la modificación a las 439 cuentas habilitadas y que tenían Account expires 31 de enero 2025 y se dejan a 15 de febrero de 2025, se relaciona el listado de cuentas modificadas.

Modificacion Account
expire a 15_feb_2025.

- 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.

- 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 12 sedes del ministerio y ETB en 37 sedes del ministerio. Esta actividad continuará para el siguiente período.

- Debido a las vulnerabilidades del Aplicativo RUI a nivel de seguridad que generó que el mismo fuera retirado de internet y dejado para uso interno, fue necesario concertar con el área funcional la gestión de los usuarios externos que normalmente generan transacciones en el aplicativo. Para esto, se entrega a la MDS un procedimiento para la creación de usuarios VPN de RUI y entrega de la contraseña de acceso cifrada al funcionario designado como enlace con los terceros.

  Se asigna personal dedicado de MDS para priorizar la creación de las cuentas, se generaron mesas de trabajo con el área funcional para afinamiento del procedimiento y apoyo al funcionario. Estas cuentas se crean en el AD con una caducidad de 15 días calendario.

- El 21 de enero 2025 se remite actualización de la Matriz de Escalamiento de la MDS con las siguientes novedades:
  - Se revisa y actualiza la distribución de Dependencias a Nivel Central.
  - Se realiza actualización de analistas de mesa de servicios en el que se incluye a Juan Camilo Padua Mayordomo y se actualiza al soporte de la territorial Casanare incluyendo a Angel David Bohorquez Morales

- Se gestionaron 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.
  - Divulgación por correo electrónico el 7/01/2025 para el personal del NOC relacionado con las cuentas de correo electrónico a las que deben copiar en el envío de evidencias por fallas en los enlaces del proveedor de conectividad.
  - El 16 de enero 2025 se realizó Socialización del Modelo Machine Learning implementado por Indra a todas las operaciones con el propósito de automatizar la auditoria de llamadas telefónicas de la MDS, se impartió a todo el personal de la Mesa de Servicios por Microsoft Teams y se divulgo el guion avalado por la Coordinadora de MDS para el protocolo de llamadas a evaluar.
  - Divulgación por correo electrónico el 21/01/2025 para el personal de Soporte en Sitio relacionado con el escalamiento para temas de garantías en Aranda y los responsables de su gestión. Enfocado a garantías de equipos de cómputo, antenas de contingencia Starlink y UPS.
  - Refuerzo del Flujo de Atención de Incidentes Mayores el 31 de enero 2025, impartida a los especialistas de la Línea de Servicios Centrales y Línea de Servicios en Sede.

- **Volumetría de Solicitudes Gestionadas:** En el mes de enero 2025 se registraron en la herramienta ITSM 8502 casos, 6444 requerimientos de servicio, 2047 incidentes y 11 cambios, no se registraron problemas. 4 casos fueron anulados por la MDS.

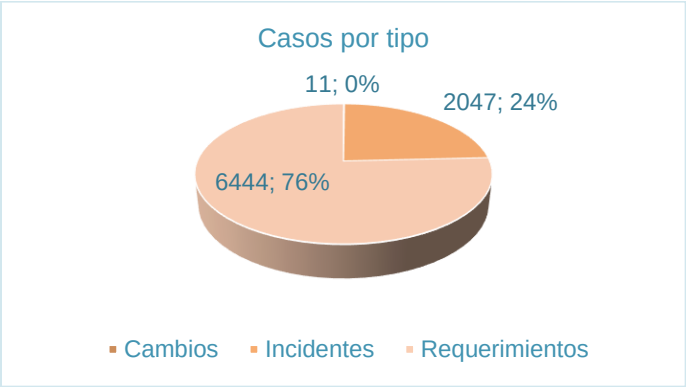


Ilustración 1 Volumetría de casos en el períodoio

- 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_Impresoras	2872	33,78
Responsable_Soporte_Territoriales	1805	21,23
NOC	1159	13,63
Responsable_Soporte_Bogota	1096	12,89
Responsable_Mesa_De_Servicio	802	9,43
Especialistas_IBM	345	4,06
Responsable_De_Servidores_Windows	111	1,31
Especialista Nube Publica	89	1,05
SOC	46	0,54
Especialista Redes	30	0,35
Especialista Base de datos	24	0,28
Especialista Herramientas de Gestion	21	0,25
Responsable Antena Starlink	17	0,20
Especialista Aplicaciones JAVA	16	0,19
Científico de Datos	16	0,19
Responsable Garantías Equipos	14	0,16
Especialista_Telefonía_IP	12	0,14
Especialista Aplicaciones .Net	9	0,11
CAB Servicios en Sede	4	0,05
Almacenamiento y Backups	4	0,05
Liferay	4	0,05
CAB Servicios Centrales	2	0,02
Gestor de Inventarios	2	0,02
Responsable_de_Energia Electrica Regulada - UPS	1	0,01
Apicom	1	0,01
TOTAL	**8502**	**100**

Tabla 1 Atención de solicitudes por grupo de especialistas

2.1.1. Herramienta de Gestión ITSM

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

- Modificación del árbol de categorías del servicio de aplicaciones especializadas y telefonía.
- Cargue masivo de casos para aumento de cuotas de impresión.

- Implementación de case creator integrado con zabbix para la creación de casos por alarmas relacionadas a CI´s TIGO.
- Se optimizó la integración entre zabbix y Aranda permitiendo que la clasificación de los casos sea más rápida y sin dependencias.
- Se creó un árbol de categorías en cada servicio basado en los CI´s clasificados en zabbix.
- Se realizó capacitación en cargue masivo y actualización de CI´s a los miembros de gestión de activos.
- Se realizó cargue masivo de CI´s al monitoreo de impresoras actualizando cada una de las novedades.
- Se realizó la creación del reporte de cambios el cual permite listas todos los cambios junto a sus campos adicionales.
- Configuración preliminar en Aranda para automatización de bitácora de NOC desde la configuración de campos adicionales.

2.1.2. Prácticas ITIL 4

En el marco de la adopción de las prácticas ITIL, durante el mes de enero 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 enero 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

• Actualización Ficha Técnica hoja de vida ANS

Para este período se empezó con la revisión y actualización de las fichas técnicas de la hoja de vida de los ANS. Con el propósito de medir la efectividad y cumplimiento de los estándares tecnológicos y operativos, así como la correcta integración de los sistemas de información.

Se ha completado los siguientes servicios:

1. Mesa de servicio
2. Soporte en Sitio
3. Equipo de Usuario Final
4. Datacenter
5. Nube Privada
6. Antivirus
7. Outsourcing de Impresión
8. Telefonía

Se está trabajando en los siguientes servicios:

1. LAN – WLAN
2. Conectividad WAN e Internet
3. KPI Prácticas ITIL

• **Actualización Guía Práctica ANS**

De acuerdo con el punto anterior, se revisó punto a punto la Guía práctica de ANS, con el fin de asegurar que los procedimientos y directrices estén alineados con los cambios tecnológicos y operativos recientes, optimizando así la implementación y ejecución de los 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 enero 2025. Este apartado contiene información relevante sobre actividades realizadas y novedades presentadas.

- **Tipificación de los cambios:** Durante el mes de enero de 2025 se gestionaron 11 tickets tipificados como Cambios, clasificados en las siguientes categorías:

CATEGORÍAS	NÚMERO DE CASOS	PORCENTAJE (%)
Administración de Bases de Datos. Servidor de base de datos	1	9,09
Aplicaciones Especializadas.Portal Web	1	9,09
Aplicaciones Especializadas.Servidor de base de datos	1	9,09
Telefonía IP.Infraestructura de telefonía	1	9,09
Aplicaciones Especializadas.Cobro Coactivo	2	18,18
Aplicaciones Especializadas.Servidor de aplicaciones	2	18,18
Aplicaciones Especializadas.SIRITI	3	27,27
Total general	**11**	**100%**

Tabla 2 Tipificación de cambios

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

- **Relación casos registrados**

  A continuación, se presenta la relación de casos registrados del 1 al 31 de enero de 2025, en total se crearon 11 tickets de los cuales se gestionaron 9 como cambios de normales y 2 cambios de emergencia los cuales se describen a continuación:



Sesion_HC_Enero.xlsx

- **Cambios por estado:** Al corte del 31 de enero, 31 casos quedaron 9 en *estado Cerrado, 1 en estado implementar cambio y 1 en estado comité de implementación.*

2.1.2.3. Práctica Activos

Durante el mes de enero de 2025, la Práctica de Activos ha implementado una serie de acciones estratégicas, cuyo principal objetivo ha sido garantizar el óptimo funcionamiento y la disponibilidad de los servicios dentro de la entidad. A continuación, se detallan las principales acciones ejecutadas:
Actualización del Agente Aranda: En el marco de las iniciativas para mejorar la gestión y control de los equipos de la organización, se ha llevado a cabo la actualización del agente Aranda. Este proceso, que se encuentra en desarrollo, traerá consigo una serie de beneficios clave que optimizarán el rendimiento y la eficiencia operativa:

- **Actualización de la versión del agente Aranda:** Se realizó la actualización de la versión 9.20 a la versión 9.21 del agente Aranda. Este proceso se ejecuta de manera remota a través del directorio activo, lo que permite actualizar todos los equipos de forma centralizada y eficiente, sin necesidad de intervención manual en cada uno de ellos.

- **Integración de Aranda Device Management y Aranda CMDB:** Además, se avanzó en la integración de las aplicaciones Aranda Device Management y Aranda CMDB (Configuration Management Database). Esta integración tiene como objetivo mejorar la visibilidad de los equipos, proporcionando información en tiempo real sobre su estado, ubicación y persona responsable, todo ello vinculado directamente al directorio activo. Esta medida facilita la gestión proactiva de los activos, contribuyendo a una mejor planificación y seguimiento de los recursos tecnológicos.

Estas acciones forman parte de un plan integral para mejorar el monitoreo, control y gestión de los equipos dentro de la entidad. La actualización y la integración de las herramientas Aranda permitirán una gestión más eficiente y una respuesta más ágil ante posibles incidencias, lo que impactará positivamente en la operatividad de los servicios. Además, estas acciones garantizan una actualización constante y una integración de datos en tiempo real, lo que mejora la trazabilidad y el control de los activos tecnológicos, contribuyendo al cumplimiento de los estándares de calidad y eficiencia establecidos por la entidad.

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:

- **Modificación de Categorías de los siguientes servicios:**
  - Administración Base de Datos
  - Administración de Servidores
  - Aplicaciones Especializadas
  - Seguridad Informática

  De la actualización realizada, se inactivaron las siguientes categorías dado a que estas no se utilizan o algunas estaban en los servicios no correspondientes

Aplicaciones Especializadas	Daño Fisico	Reportar una falla.Monitor Pc.Daño Fisico
Aplicaciones Especializadas	Falla- Error	Reportar una falla.Monitor Pc.Falla- Error
Aplicaciones Especializadas	No enciende	Reportar una falla.Monitor Pc.No enciende
Aplicaciones Especializadas	Bloqueo malware (spam, spoofing, gusano, troyano)	Reportar una falla.Seguridad de la Información.Bloqueo malware (spam, spoofing, gusano, troyano)
Aplicaciones Especializadas	Almacenamiento de contraseñas en texto claro	Reportar una falla.Uso inadecuado de credenciales.Almacenamiento de contraseñas en texto claro
Aplicaciones Especializadas	Fuga de credenciales	Reportar una falla.Uso inadecuado de credenciales.Fuga de credenciales
Aplicaciones Especializadas	Transmicion insegura de contraseñas	Reportar una falla.Uso inadecuado de credenciales.Transmicion insegura de contraseñas
Aplicaciones Especializadas	No conecta	Reportar una falla.VPN Cliente.No conecta
Aplicaciones Especializadas	Falla conexión VPN	Reportar una falla.VPN site to site.Falla conexión VPN

Aplicaciones Especializadas	Falla aplicación	Reportar una falla.VPN.Falla aplicación
Aplicaciones Especializadas	Falla conexión	Reportar una falla.VPN.Falla conexión
Aplicaciones Especializadas	Falla instalacion	Reportar una falla.VPN.Falla instalacion

Tabla 3 Categorías Inactivas

- **Creación Árbol de Categorías Alarmas Zabbix**

Con el fin de identificar las alarmas generadas en Zabbix y los CI afectados, se ajustó el árbol de categorías creando

Servicio/Categoría
Reportar una falla.Alarma Zabbix.Router
Reportar una falla.Alarma Zabbix.Impresora
Reportar una falla.Alarma Zabbix.Switch
Reportar una falla.Alarma Zabbix.AP
Reportar una falla.Alarma Zabbix.Servidor Linux
Reportar una falla.Alarma Zabbix.Servidor Windows
Reportar una falla.Alarma Zabbix.FortiGate

- **Actualización Matriz de Escalamiento**

  En enero 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
20/01/2025	Se revisa y actualiza la distribución de Dependencias a Nivel Central
21/01/2025	Se realiza actualización de Analistas de mesa de servicios en el que se incluye a Juan Camilo Padua Mayordomo y se actualiza al soporte de la territorial Casanare incluyendo a Angel David Bohorquez Morales

Tabla 4 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 enero 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 problemas relacionados con el gestor documental.

ID Problema	Servicio TI/ Gestion ITIL Afectado	CI	Prioridad	Problema identificado	Causa Raiz	Solución	# Casos Relacionados	Estado Aranda

47834	Gestor documental	Modulos de radicación	ALTO	Teniendo en cuenta que las incidencias del gestor documental se siguen presentando de manera recurrente y que a través de la práctica de problemas se creó el PM31928, donde se identificó como causa raíz que "Los componentes que conforman la plataforma transaccional pueden procesar una cantidad limitada de solicitudes y al superar dicha capacidad de transacción presenta incidencias." y que para dar solución a dicha causa raíz se requiere un proceso de adquisición de infraestructura que está a cargo de la entidad y no se encuentra dentro del alcance de la Unión Temporal se requiere crear un caso tipo problema adicional que permita relacionar los nuevos incidentes reportados por los usuarios a través de la Mesa de Servicios. La identificación de la causa raíz del nuevo problema es la misma del caso PM31928 en tal sentido, este caso queda en el estado "error conocido" por tiempo indefinido hasta tanto el proceso de adquisición de infraestructura sea finalizado por la entidad.	Los componentes que conforman la plataforma transacciona una cantidad limitada de solicitudes y al superar dicha capaicidad de transacción presenta incidencias.	Mantenimiento de la plataforma del Gestor Documental y 2 ventanas de mantenimiento al mes Mantenimiento sobre la capa de presentación del gestor para bajar los consumos de procesamiento actuales,	PM 31928	Error conocido

Tabla 5 Detalle problema 47834

Se realizó mesa de trabajo para la revisión del PM- 47834 el cual fue abierto en el mes de octubre cuya causa raíz es: Los componentes que conforman la plataforma transacciona una cantidad limitada de solicitudes y al superar dicha capacidad de transacción presenta incidencias. Dicho caso relacionaba los diferentes incidentes que se presentaron en la operación por errores en las transacciones.

Se concluyó dar cierre al caso con la siguiente solución: Se da cierre al problema en estado error conocido teniendo en cuenta los resultados y el análisis de la ejecución de las ventanas de mantenimiento realizadas entre los meses de noviembre y diciembre de 2024. se elaboró un informe sobre el estado actual del servicio de Gestor Documental de la entidad, los hallazgos, actividades, reportes y mitigaciones que se han realizado a nivel de maniobras técnicas el equipo de Especialistas de Servicios Central, así como componentes de TI que soportan la infraestructura tecnológica en el Ministerio del Trabajo. Se relaciona al problema los controles de cambio RFC-53177 y RFC-63200
Se adjuntó informe de Ampliación y Mejoramiento de la infraestructura del Gestor Documental del Ministerio del Trabajo

Se informó a la Mesa de servicio que el problema se cerró y no se realizará relaciones con dicho caso. En tal sentido todas las incidencias que se presenten se deben escalar al grupo de especialistas de IBM siguiendo las indicaciones de la matriz de escalamiento,
Adicionalmente, en el marco de la práctica de incidentes se validará la recurrencia de reportes y se realizará mesa de trabajo para identificar la creación de un caso tipo problema.

ID Problema	Servicio TI/ Gestion ITIL Afectado	CI	Prioridad	Problema identificado	Causa Raiz	Solución	# Casos Relacionados	Estado Aranda

58357	Gestor documental	Modulos de radicación	ALTO	A traves de la mesa de servicio se han recibido solicitudes de los usuarios como: 1) Al ingresar al radicado, no encuentra información del trámite ni los documentos del mismo dentro del flujo de trámites y servicios. No es válido de que la solución que den sea que debe consultar la documentación en el modulo de "Consultar Documentos". 2) el aplicativo no permite el diligenciamiento de los campos: la entidad tiene pactos o convenciones colectivas? y su empresa esta obligada a tener reglamento? adjuntaron captura de pantalla.3) Desde el grupo de atención al ciudadano adjunto imagen de los “ESTADOS PQRSD” y “SUBESTADOS” que actualmente se evidencian en el reporte adjunto y algunos casos puntuales para que sean de su análisis y adjunto archivo word con ejemplos de ESTADOS y SUBESTADO del informe que se adjunta.4) SOLICITUD ELIMINACION RADICADOS - PERSISTE ERROR RADICADOS TRAMITE NO PERMITE CONTINUAR - ERROR DE SELECCION DTMETA-PUERTO GAITAN	La entidad realizó las verificaciones internas y confirmó que no tiene disponible el código fuente de la aplicación	El especialista de la UT realizará una verificación detallada sobre la aplicación para identificar si es posible proveer alguna solución alternativa a los casos reportados	38447 38482 38511 38513 38522 40509 40564 40910 45714 46793 47357 51908 52173	Error conocido

Tabla 6 Detalle problema 58357

Se realizó mesa de trabajo para la revisión del PM 58357 el cual fue abierto en el mes de noviembre cuya causa raíz es: La entidad realizó las verificaciones internas y confirmó que no tiene disponible el código fuente de la aplicación.

Se concluyó dar cierre al caso con la siguiente solución: Se cierra el caso en estado "error conocido" se realizó la verificación de los casos registrados y se determinó que la UT validará si se cuenta con los insumos necesarios para brindar solución a los casos futuros que se reporten a la Mesa de Servicios, en caso contrario se indicará al usuario como respuesta, Teniendo en cuenta que dentro de la información (técnico funcional) del Gestor documental no se cuenta con el insumo necesario para dar atención a la solicitud se informa al usuario que no es posible dar atención a su requerimiento.

Se informó a la Mesa de servicio que el problema se cerró y no se realizará relaciones con dicho caso. En tal sentido todas las incidencias que se presenten se deben escalar al grupo de especialistas de IBM siguiendo las indicaciones de la matriz de escalamiento.
En el marco de la práctica de incidentes se validará la recurrencia de reportes y se realizará mesa de trabajo para identificar la creación de un caso tipo problema.

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 enero 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 2048 casos tipo incidente quedando en los siguientes estados:

Estado	Cantidad
Cerrado	2008
Solucionado	20
Suspendido	13
En proceso	5
Registrar	1
Anulado	1
Total	2048

Tabla 7 Listados Incidentes

- Los casos anulados corresponden a los siguientes tickets:

  IM-71759: El caso fue anulado debido a un mal escalamiento generado por la herramienta automatizada "Case Creator" en el proceso de creación de casos.

- A cierre del mes de enero, quedaron 13 casos en estado suspendido de los cuales 3 tickets quedaron asignados al equipo NOC por escalamientos realizados al proveedor de telecomunicaciones, 1 caso asignado al equipo Especialista Herramientas de Gestión, este corresponde a un caso de pruebas de algunos ajustes en la herramienta de gestión Aranda, 2 casos asignados al equipo de redes de los cuales 1 fue atendido y se dará cierre en febrero y el otro está en gestión para revisión del cableado del rack en la sede de puerto Inírida.

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	689
Reportar una falla.Alarma Zabbix.Impresora	390
Reportar una falla.Alarma Zabbix.Switch	130
Reportar una falla.Alarma Zabbix.AP	128
Reportar una falla.Alarma Zabbix.Servidor Linux	98
Reportar una falla.Alarma Zabbix.Servidor Windows	68
Reportar una falla.Alarma Zabbix.FortiGate	57
Reportar una falla.Falla impresora.No imprime	56
Reportar una falla.Falla impresora.Atasco	40
Reportar una falla.Monitoreo Zabbix.Alarma desde Zabbix	40

Tabla 8 Top 10 Categorías Incidentes

- La categoría “Reportar una falla.Monitoreo Zabbix.Alarma desde Zabbix” corresponde a los casos generados mediante la función Case Creator, para esto, en enero se terminó de realizar el ajuste de los servicios y categorías con el fin de que cada caso creado por alarmas, se categorice automáticamente según CI afectado.
- 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, esto ya

fue escaldo a la supervisión dado a que se está viendo afectada la disponibilidad. 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 o fallas del fluido eléctrico los cuales son gestionados en el momento en el que se presenta la novedad.

De los incidentes generados, se registraron 5 incidentes mayores los cuales se muestran a continuación:

Ticket Arada	SERVICIO AFECTADO	NOVEDAD	CAUSA RAÍZ	AFECTACIÓN DE USUARIOS	ESTADO ARANDA	FECHA INICIO	FECHA FIN	HORA FIN
IM-67262	**Gestor Documental**	Error radicación de salida. no aparece el destinatario en la etiqueta	El error identificado se debió a un problema en el envío de la información desde las variables de entorno hacia los contenedores nuevos de la Base de Datos en el entorno RAC de Oracle. Este inconveniente se originó durante los procesos de BPM, lo que provocó que la información no fuera correctamente direccionada y procesada por los contenedores correspondientes.	General	Cerrado	3/01/2025	3/01/2025	6:03 p. m.
IM-67787	**Internet**	Falla Masiva Servicio Internet	Afectación por una falla de alto impacto debido a una atenuación en el enlace YUMBO – SANTA MÓNICA por una doble apertura	• Sincelejo • Santa Marta • Cali • Pereira • Medellín • Facatativá • Monteria • Puerto Boyacá • Apartadó • Santa Fe de Antioquia	Cerrado	7/01/2025	7/01/2025	4:26 p. m.

				• Yarumal • Sonsón				
IM-74607	**Internet**	Falla servicio Internet Call 32	Corte de Fibra	Call 32	Cerrado	29/01/2025	29/01/2025	12:39 p. m.
IM-75113	**Internet**	Falla Internet Zona Norte	Corte de Fibra	Patia, Puerto Wilches, Barbosa, Cartagena, Los Patios	Cerrado	30/01/2025	30/01/2025	3:06 p. m.

Tabla 9 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 Enero
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=2031**/2048*100 **EF= 99,17%**
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= 10**/2048*100 **RRP= 0,48%**

Tabla 10 KPI Práctica de Incidentes

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

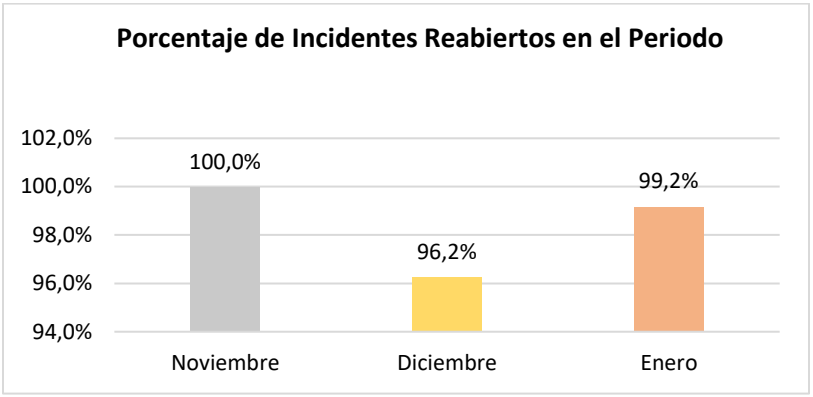


Ilustración 2 KPI Efectividad de Resolución de Incidentes de Servicio

En enero se evidenciaron 17 casos que no cumplieron el ANS, aun así, se evidencia mejora en cuanto al cumpliendo de los casos asignados a los especialistas, de estos casos que presentan incumplimiento, se validaron con cada responsable y se realizó el feedback correspondiente.

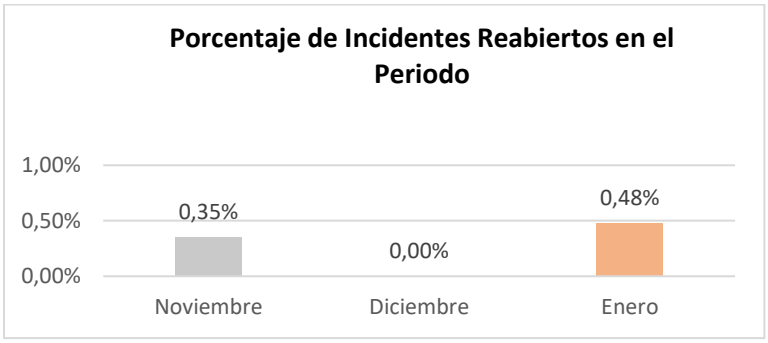


Ilustración 3 KPI Incidentes de Reabiertos en el periodo

En cuanto a los incidentes reabiertos, en enero se presentaron 10 reaperturas de los cuales 8 hacen parte del NOC, al validar, estos corresponden a alarmas que aun aparecían en Zabbix pero al validar en sede, el servicio estaba operativo, también a casos que fueron solucionados por error. A continuación, se relaciona mayor detalle:

Caso	Descripción de la solicitud	Grupo responsable	Causa	Atención al caso
IM-70020	Reportar una falla.Monitoreo Zabbix.Alarma desde Zabbix	NOC	Caso reabierto dado a alarma generada por apagado de equipos en sede y en horario no hábil. El ticket se cerró mientras la sede estaba con mantenimiento	Se procede a cerrar el caso ya que el alertamiento presente en la herramienta de zabbix se encuentra en estado solventado, adicional a ello en horas de la noche no se cuenta con personal en sitio para realizar las respectivas validaciones
IM-70081	Reportar una falla.Monitoreo Zabbix.Alarma desde Zabbix	NOC	Se procede a re-abrir el caso ya se evidencio intermitencia, sin embargo, la funcionaria se encontraba en semana de receso por lo que no era posible validar la falla exactamente.	La novedad fue solventada luego de validar que los equipos estaban apagados por corte de energía debido al no pago de la factura.
IM-70692	Reportar una falla.Gestor Documental.Falla error - Producir documento	Especialistas_IBM	la funcionaria realiza el proceso nuevamente pero no pasa del documento producido. se adjuntan fotos y video del proceso.	Se realiza la validación técnica de la aplicación y se encuentra funcional, por favor verificar nuevamente la conexión a internet, ventanas emergentes o bloqueos en el

				navegador o intentar desde otro computador para descartar inconvenientes.
IM-72118	Reportar una falla.Mouse - Teclado - Base - Diadema.Falla General	Responsable Soporte Bogota	El caso fue relacionado a un incidente mayor por equivocación lo cual provoco su cierre	Se realiza cancelación del caso, ya que está siendo verificado con el numero RF-72128, el cual está siendo tramitado por garantía con el proveedor.
IM-72255	Reportar una falla.Alarma Zabbix.Router	NOC	El caso se solucionó por error, se reabrió y se dio continuidad a la gestión	se habilitó el canal MPLS y el Firewall quedo funcional. Se realiza ping y se encuentra funcional la sede.
IM-73008	Reportar una falla.Alarma Zabbix.Router	NOC	Caso reabierto dado a alarma generada por apagado de equipos en sede y en horario no hábil. El ticket se cerró mientras la sede estaba con mantenimiento	Se procede a cerrar el caso ya que el alertamiento se solvento después de que proveedor eléctrico termino su mantenimiento programado el día de ayer 22/01/2025 se adjunta evidencia de la programación:
IM-73509	Reportar una falla.Alarma Zabbix.Router	NOC	Caso reabierto dado a alarma generada por apagado de equipos en sede y en horario no hábil. El ticket se cerró mientras la sede estaba con mantenimiento	Se procede a cerrar el caso ya que el alertamiento presente en la herramienta de Zabbix está en estado solventado, adicional a ello no se cuenta con personal en sitio para realizar las correspondientes validaciones de primer nivel
IM-73677	Reportar una falla.Alarma Zabbix.Router	NOC	Caso reabierto dado a alarma generada por apagado de equipos en sede y en horario no hábil. El ticket se cerró mientras la sede estaba con mantenimiento	27/01/2025 en validación por parte del ingeniero Jesus Gonzalez notifica que realmente la falla fue porque el funcionario desconecto el cable del Fortinet sin intención y por eso fue el motivo de la falla, ya se observa operativo
IM-73685	Reportar una falla.Alarma Zabbix.Router	NOC	Caso reabierto dado a alarma generada por apagado de equipos en sede y en horario no hábil. El ticket se cerró mientras la sede estaba con mantenimiento	Se procede a cerrar el caso ya que el alertamiento presente en la herramienta de Zabbix está en estado solventado, ya que se indican que apagaron los equipos en sede ya se encuentran en gestión
IM-73832	Reportar una falla.Alarma Zabbix.Router	NOC	Caso reabierto dado a alarma generada por apagado de equipos en sede y en horario no hábil. El ticket se cerró mientras la sede estaba con mantenimiento	Se procede a cerrar el caso ya que el alertamiento presente en la herramienta Zabbix está en estado solventado, adicional a ello se procede a realizar pruebas de Ping de manera exitosa ya que los fines de semana no se cuenta con personal en sitio para realizar las validaciones de primer nivel como de las evidencias por parte de Proveedor ETB.

Tabla 11 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 enero 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 6447 casos tipo requerimiento quedando en los siguientes estados:

Tabla 12 Estados Requerimientos

Estado	Cantidad
Cerrado	6306
Solucionado	33
Suspendido	67
En proceso	36
Registrado	2
Anulado	3
Total General	**6447**

- Los casos en estado anulado corresponden a tickets duplicados.

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

Categoría	Cantidad
Aumento de cuota	2390
Asesoría - Consulta	1029
Configuración	515
Solicitud Papel	319
Instalación - Configuración	279
Cambiar contraseña	184
Reportar Solicitud/Falla	151
Asesoría Excel	108
Creación de usuario	87
Conectar a red Mintrabajo	75

Tabla 13 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 el seguimiento de los requerimientos reabiertos por los usuarios, por lo tanto, para el periodo no se reportó solicitudes de reapertura.

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=** 6330/6447*100 **EF= 99,16%**
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=** 0/6339*100 **RRP= 0,022%**

Tabla 14 Detalle de KIP Practica de Requerimientos

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

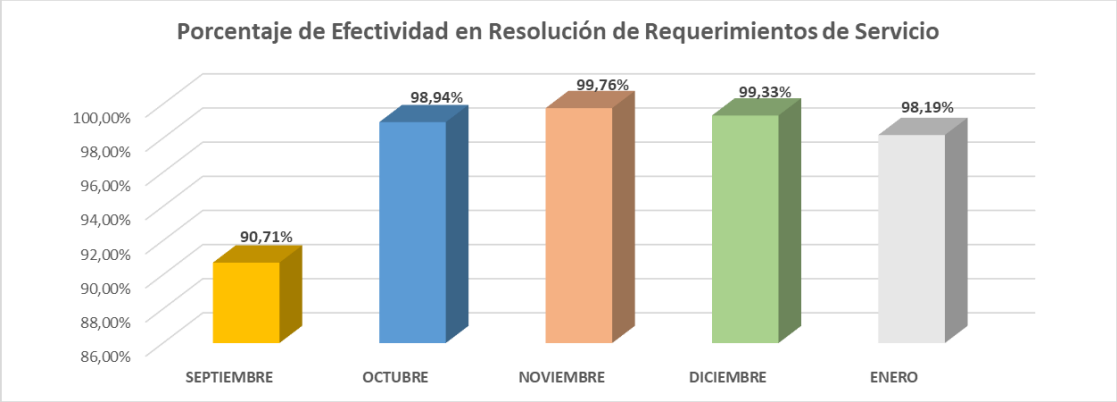


Ilustración 4 KPI Efectividad de Resolución de Requerimientos de Servicio

Durante el periodo, se evidencia el cumplimiento del 98,19% en efectividad de la solución de los requerimientos, los cuales se verifica de 6447 casos registrados en los diferentes canales oficinales de la Mesa de Servicio fueron solucionados 6339 casos, los cuales 66330 tickets cumplieron con los tiempos de solución del ANS.

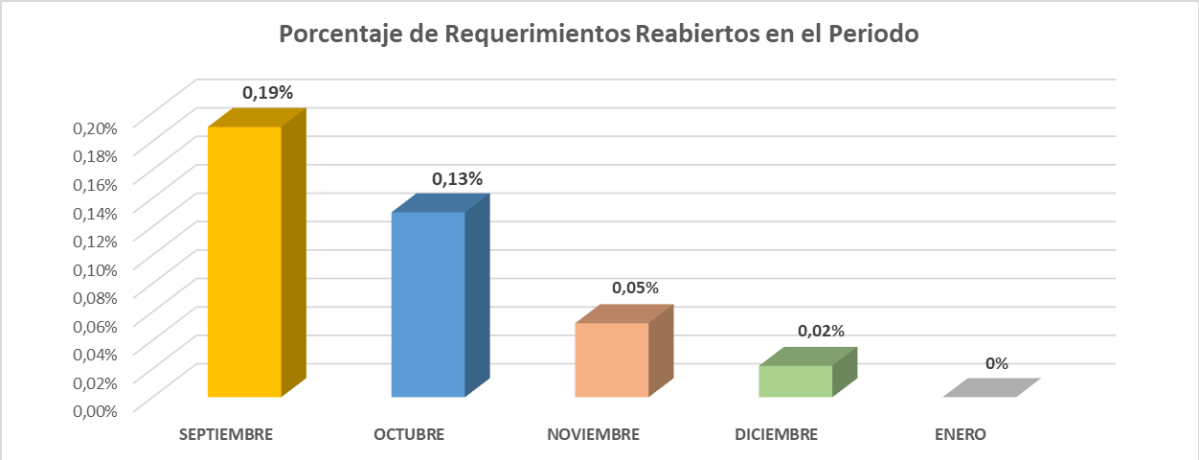


Ilustración 5 KPI Requerimientos de Reabiertos en el periodo

Durante el periodo, se realizó el seguimiento de los requerimientos reabiertos por los usuarios, se ha evidenciado durante los últimos meses una disminución de reaperturas, lo cual para este mes no presento ningún caso reabierto, por lo tanto, se puede concluir que los usuarios se encontraron satisfechos con las soluciones brindadas por la Mes de Servicios y sus especialistas.

2.1.2.8. Práctica de Eventos

Para el mes de enero, 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 1054 tickets escalados mediante la herramienta de gestión de los cuales 918 alarmas fueron gestionadas por el NOC, los casos restantes corresponden a tickets generados por incidentes masivos que se relacionaron a los mismos.

- **Actividades Ejecutadas por el Líder de herramientas con Apoyo de Gestor de Eventos**

  - ✓ Creación de host tipo Starlink
  - ✓ Creación de host tipo SDWAM
  - ✓ Creación de categorías para asignación de casos automáticos según CI Afectado
  - ✓ Ajuste de Categorización automática en los casos generados mediante Case Creator

- ✓ Creación de mantenimientos programados a sedes
- ✓ Creación de campos adicionales en herramienta ITSM para automatización de bitácora NOC

Novedades identificadas – Gestión de Eventos
Como medida preventiva frente a las altas cargas eléctricas y los frecuentes cortes de energía en las regiones, se ha programado un mantenimiento para los equipos de cómputo y comunicaciones. Los equipos se apagarán de acuerdo con el siguiente horario para evitar posibles daños:

Horarios de Mantenimiento Programado:
- **Lunes a viernes**: 04:30 pm a 07:30 am
- **Sábados y festivos**: 24 horas

Equipos en Mantenimiento:
- Router_Bosconia
- Router_Orito
- Router_Chiriguana
- Router_Granada
- Router_Ubate
- Router_San_Marcos
- Router_Puerto_Asis
- Router_Mariquita
- Router_Fundacion
- Router_Campo_de_la_Cruz
- Router_Socorro
- Router_Puerto_Gaitan
- Router_Tocancipa
- Router_Plato
- Router_Tulua
- Router_Manzanares
- Router_El_Doncello
- Router_Lorica
- Router_Acacias
- Router_Zipaquira
- Router_Concordia
- Router_Cisneros
- Router_Turbo

Acción Requerida: Tener en cuenta los horarios de mantenimiento para evitar la afectación de la disponibilidad de los servicios.
Retroalimentación y Ajustes: En caso de que se reciba retroalimentación respecto a los ajustes realizados, se podrá cambiar el estado según los lineamientos previamente informados, con el fin de asegurar que la configuración se ajuste a las necesidades operativas y de disponibilidad.

- **Informe Operación NOC**

Access Point
Desde el centro de operaciones NOC durante el mes de enero se escalaron 72 incidentes relacionados con equipos de red Access Point en diferentes sedes a nivel nacional.
- Se evidencia que en la sede Bolívar se presenta mayor recurrencia de incidentes con los dispositivos Wifi; correspondiente al 25% de los eventos de esta categoría generando 18 casos de los 72 manejados por parte del NOC en cuanto a dispositivos AP refiere.

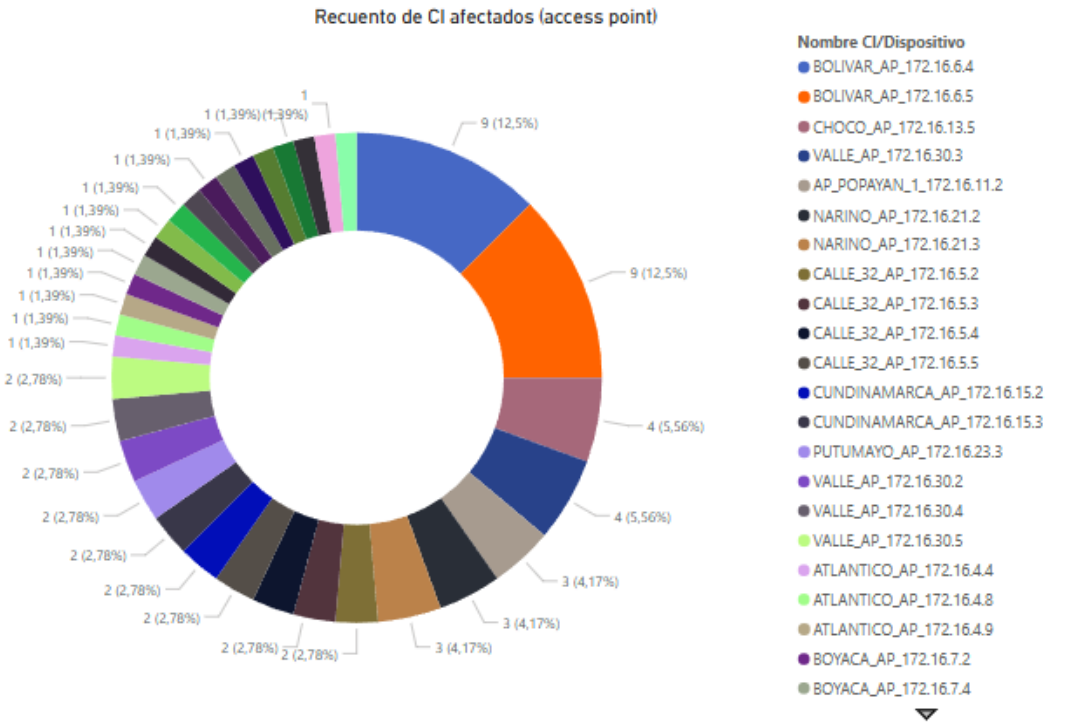


Ilustración 6 Access Point alarmados por sede

- Para el mes de enero se solucionaron con éxito la totalidad de los 72 casos generados en Aranda para gestión de alarmas proactivas por Access Point, es decir el 100% de los casos fueron resueltos.

- De los 72 alertamientos por Access Point 38 fueron por causa de intermitencia de red, 17 sin energía eléctrica, 12 por falla en red de proveedor, 4 por no responde ping y 1 por actividad programada.

- Se evidencia que el 53% de las alertas registradas por AP´s fueron por causa de intermitencia de red, siendo esta la mayor causa de indisponibilidad para la categoría.

- Se evidencia que se presenta mayor número de incidencias en cuanto a dispositivos de red inalámbrica en la sede Bolívar; esto debido a que en enero presento mayor cantidad de alarmas para Access Point.

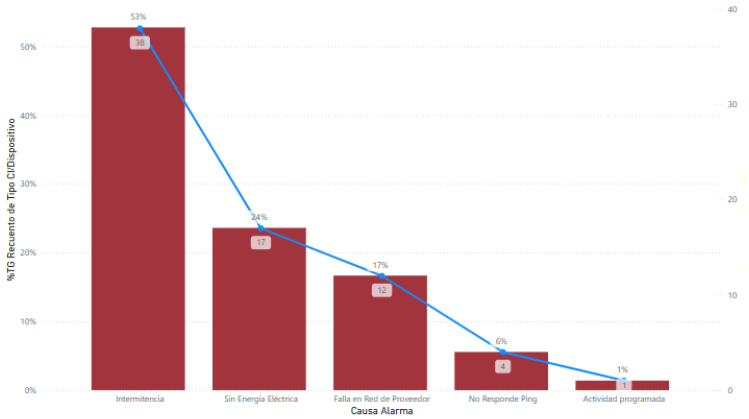


Ilustración 7 Causas de alertamiento AP

Servidores

Por parte del grupo NOC en el mes de enero, se evidenciaron un total de 86 alarmas presentadas sobre servidores mostradas a continuación:

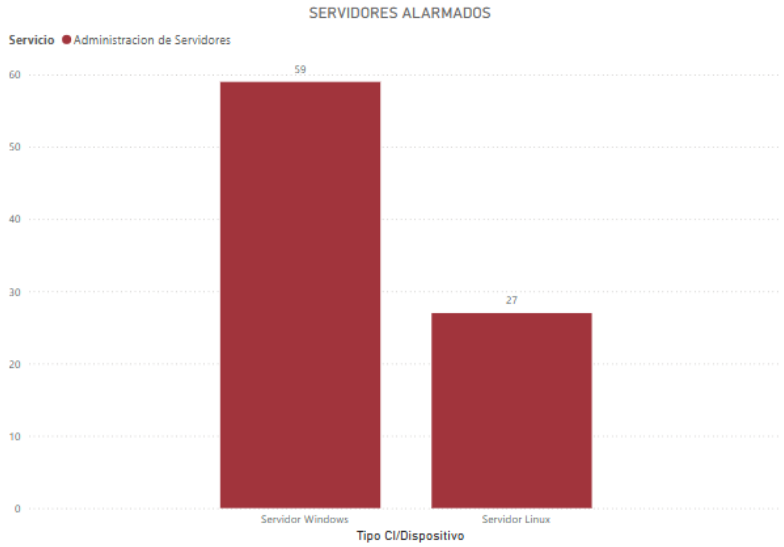


Ilustración 8 Servidores alertados por plataforma

- De acuerdo con las validaciones realizadas por parte del NOC, de las 86 alarmas que se presentaron durante el mes de enero en lo relacionado con los servidores, 59 pertenecen a plataformas Windows y 27 a plataforma Linux.

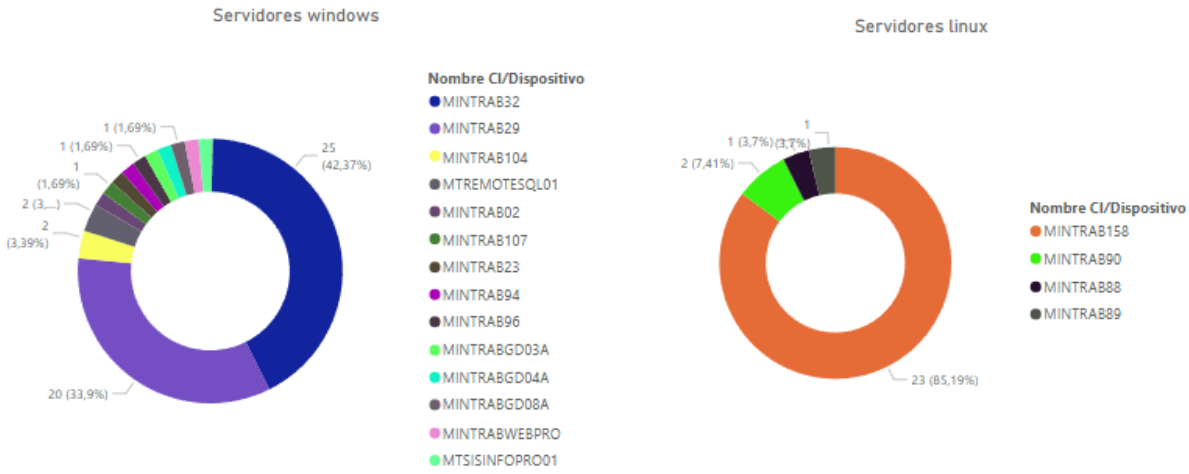


Ilustración 9 Distribución de servidores alertados

- De acuerdo con las validaciones realizadas por parte del NOC, de las alertas generadas para plataforma Windows se evidencia el servidor con mayor cantidad de alarmas recurrentes o masivas fue el servidor MINTRAB32, siendo este el que mayor cantidad de alarmas genero (25).
- En plataformas Linux el servidor con mayor porcentaje de alertamientos es MINTRAB158 con el 85.19% del total de alarmas generadas para servidores (23 alarmas de las cuales

todas son recurrentes debido a un proceso de backup que se realiza entre las 5am y 6 am) (las alarmas sobre este servidor son recurrentes en informes pasados).

Para las 86 alertas presentadas en el mes de enero el equipo NOC realizó gestión de cada una junto a los especialistas a cargo.

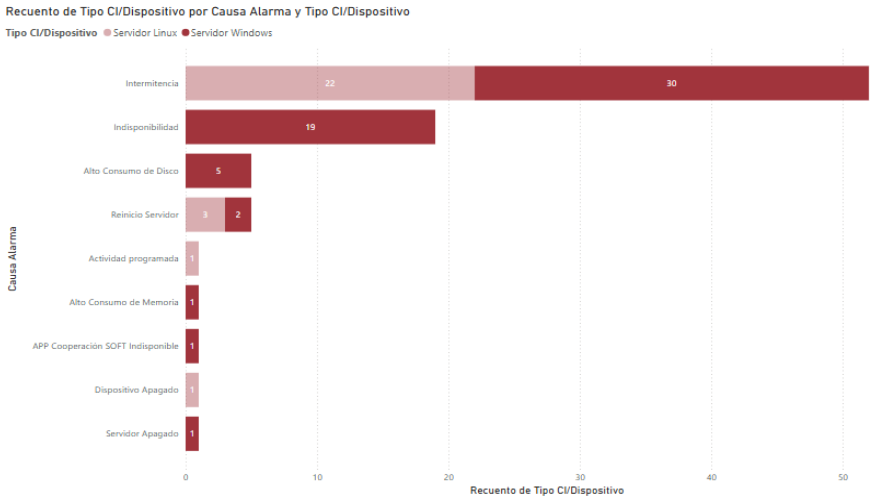


Ilustración 10 Causas de alertamientos (Servidores)

- Entre el TOP4 de los servidores con más alarmas presentadas durante el mes de enero se destaca el MINTRAB32 y el MINTRAB29 relacionados a Windows y relacionados a Linux el MINTRAB158 y MINTRAB90.

- Para el mes de enero el NOC gestionó en conjunto con los especialistas un total de 86 casos referentes a servidores tanto Windows como Linux y virtual, se cumplió a cabalidad con el escalamiento de los 86 casos generados en Aranda y todos listan como solucionados.

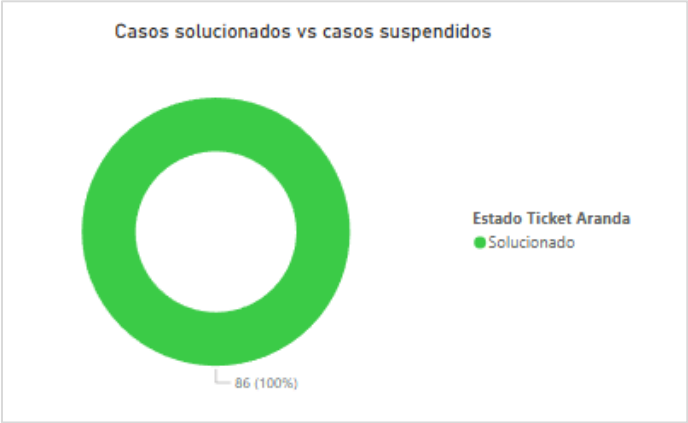


Ilustración 11 Casos solucionados vs casos suspendidos (servidores)

Switches

- Por parte del grupo NOC en el mes de enero, se evidenciaron un total de 67 alarmas presentadas sobre Switches de las distintas sedes mostradas a continuación:

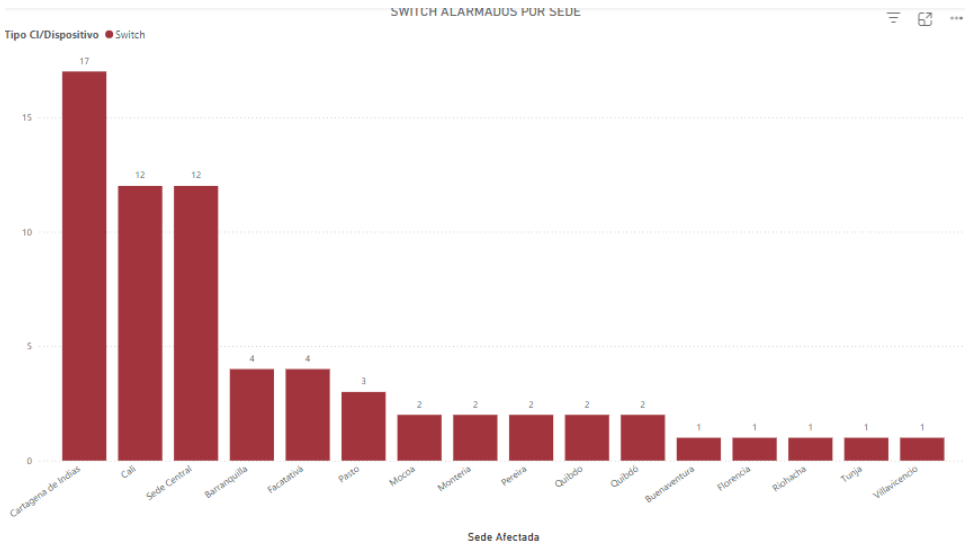


Ilustración 12 Switches alarmados por sede

- Durante el mes de enero se generaron 67 casos referentes a Switches en la herramienta de monitoreo Zabbix, las alarmas están distribuidas por diferentes sedes a nivel nacional.
- La sede Cartagena de Indias tiene la mayor cantidad de casos, especialmente relacionados con intermitencias en la red.
- 37 de los casos para el mes de enero referidos a Switch son relacionados con temas de intermitencia, mientras que los demás se debieron a fallas en red de proveedor y fallas de energía.
- Con base a la información registrada, se dio solución a la totalidad los casos generados por incidentes con dispositivos de red Switch.

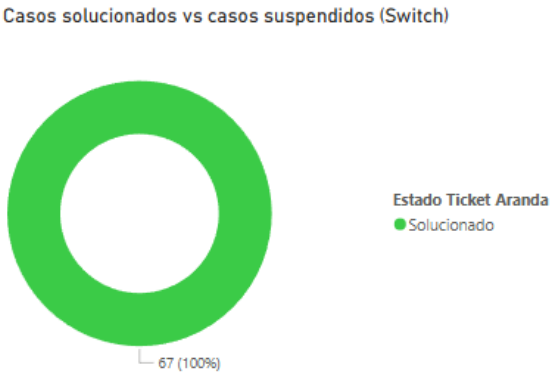


Ilustración 13 Casos solucionados vs casos suspendidos

- Se evidencia que la mayor recurrencia de alertamiento es debido a intermitencia de red (37) con el 55,22% de los incidentes generados a lo largo del mes de enero.

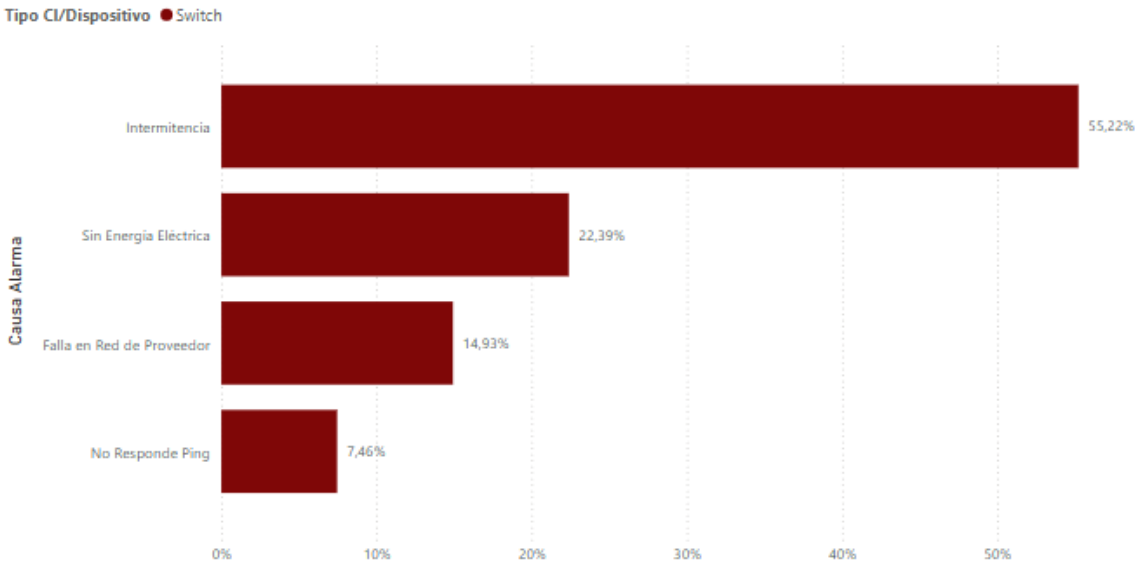


Ilustración 14 Causas de incidentes (Switches)

Routers

- Por parte del grupo NOC en el mes de enero, se evidenciaron un total de 573 alarmas presentadas sobre Routers de las distintas sedes, se muestran a continuación el top 8 de eventos. Donde se observa que las sedes que mayor cantidad de eventos generaron fueron Salazar de las Palmas y Guapi.

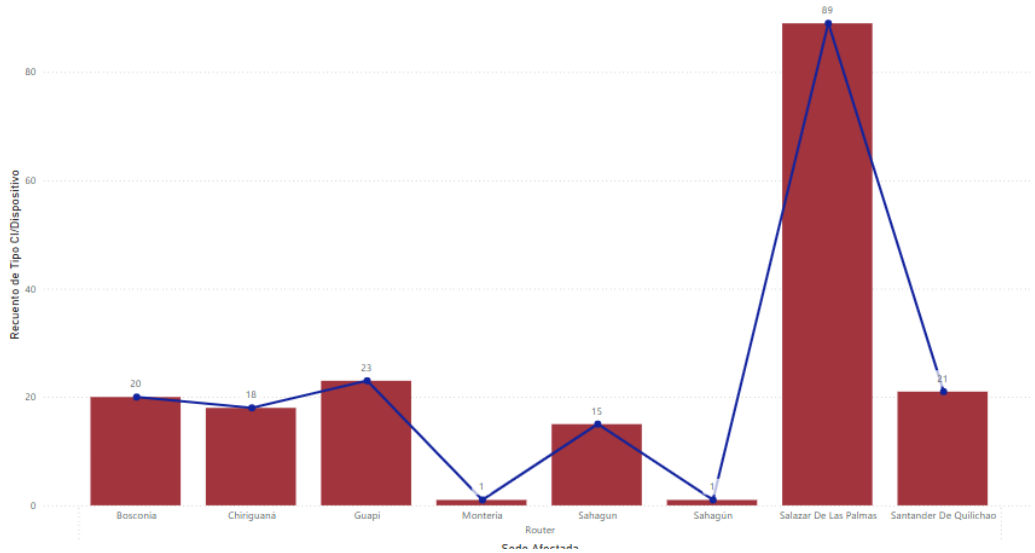


Ilustración 15 Routers alarmados por sede

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

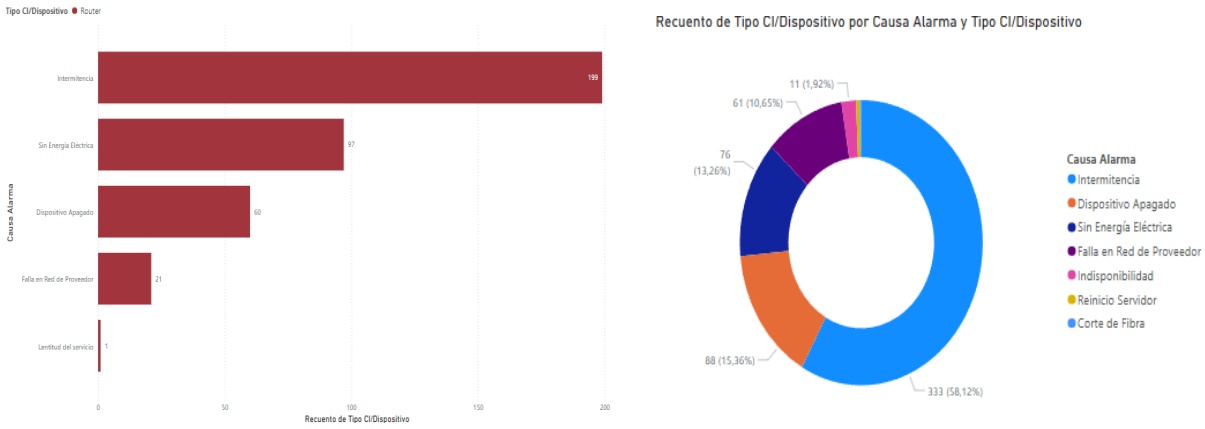


Ilustración 16 Causas de alertamiento (Routers)

- Se evidencia que la mayor causa por la que se evidencian alarmas es por intermitencia en la red que corresponde al 58.12% del total de los caos.

Alarmas Escaladas con el Proveedor de Telecomunicaciones

- Se generaron para el mes de enero 69 tickets con proveedor, de los cuales 68 fueron solucionados, quedando el 99% de los casos gestionados y en estado solucionado.
- Durante el mes de enero se presentaron 3 incidentes masivos debido a fallas de red y escaladas con proveedor los cuales fueron gestionados con los casos IM-67787**,** IM-74041 y IM-75113

Causas de Fallas Escaladas a Proveedor

- Se evidenciaron las causas que falla de red con proveedor, dentro de las cuales predomina falla de red debido a infraestructura de este como cortes de fibra óptica.
- Durante el mes de enero se reportaron con proveedor 69 incidentes referentes a fallas en red de proveedor que denotan afectación en diferentes sedes a nivel nacional.
- Se evidenciaron 21 incidentes provocados por intermitencias prolongadas de red, dichos incidentes generan indisponibilidades de manera masiva al servicio en mayor o menor impacto.

Relación 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 y se realiza seguimiento.

Falla Masiva zona Norte - IM-67787 (07/01/2025 13:33): Realizando seguimiento a la novedad presentada, Sobre las 09:02 am se confirma operatividad del servicio: Causa Raíz: Afectación por una falla de alto impacto debido a una atenuación en el enlace YUMBO – SANTA MÓNICA por una doble apertura, Acciones Realizadas: el área correspondiente realiza una compensación sobre el enlace. Tiempo de Indisponibilidad: 2 horas y 52 minutos.

Falla Masiva zona Puerto Wilches- IM-75113 (30/01/2025 12:00): Se presenta afectación masiva que genera indisponibilidad en sedes de la zona norte del país, Se evidencia restablecimiento de las sedes afectadas por falla en red del proveedor la cual afectó sedes en la zona norte del país.

Falla Masiva zona Cartagena de Indias- IM-74041 (27/01/2025 09:13am): "De manera atenta quiero informarles que la afectación en el servicio CAV3000077666 que se está gestionando bajo el caso 21456754. Se encuentra operativo, luego de que nuestro equipo de especialistas solventase y solucionaran una falla de alto impacto sucedida en la zona, esta se ocasiono por corte en el medio de transmisión (Fibra Óptica)."

Grafica de CPU Zabbix de Todo El Mes Sobre Servidores.

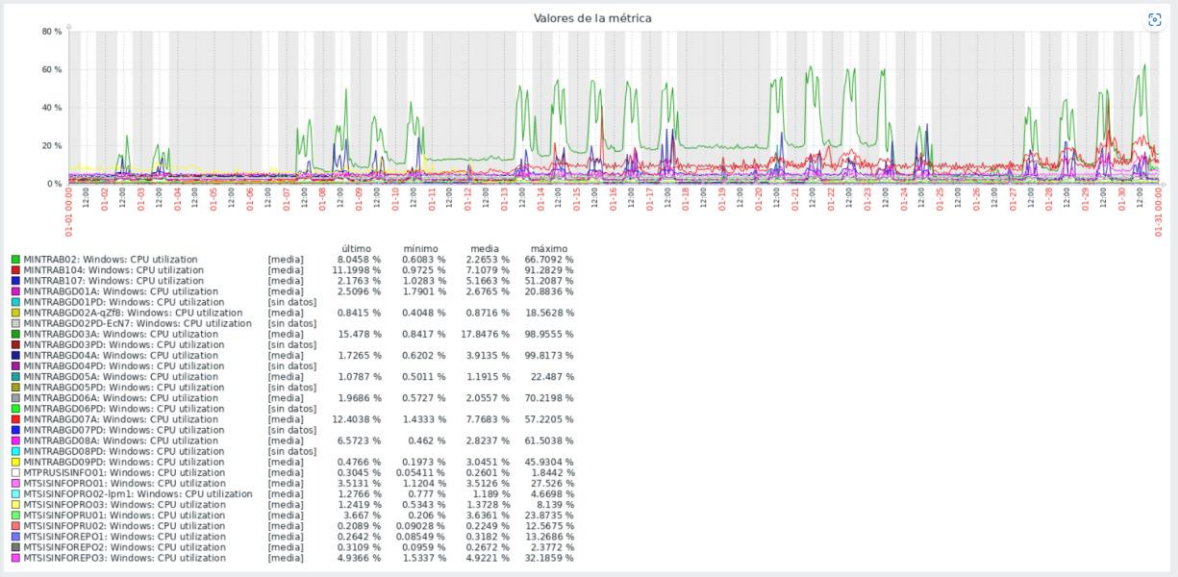


Ilustración 17 Grafica de CPU

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 17.8476%
2. MINTRABGD07A 7.7683%
3. MINTRAB104 7.1079%
4. MINTRAB107 5.1663%
5. MTSISINFOREPO3 4.9221%

Grafica De Memoria Zabbix De Todo El Mes Sobre Servidores

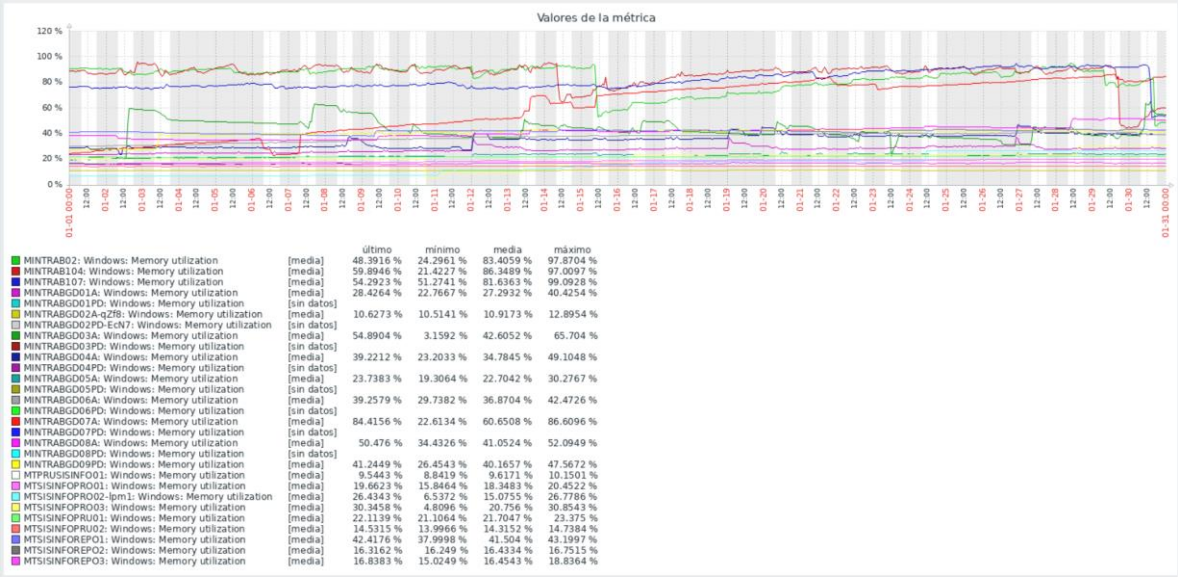


Ilustración 18 Grafica de memoria Zabbix

- 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 86.3489%
2. MINTRAB02 83.4059%
3. MINTRAB107 81.6363%
4. MINTRABGD07A 60.6508%
5. MINTRABGD03A 42.6052%

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 enero de 2025. Las novedades de dichos dispositivos se gestionan a través del monitoreo del NOC.

Servidores

Cantidad de dispositivos	Disponibilidad consolidada
106	99,99%

Tabla 15 Consolidado disponibilidad de servidores

El siguiente equipo presentó mayor alarma en el umbral de monitoreo durante el periodo:

Servidor	Disponibilidad	Servicio alojado
MINTRAB32	99,98%	BD Oracle

Tabla 16 alarmas presentadas en el mes de enero

Directorio Activo

Cantidad de dispositivos	Disponibilidad consolidada
3	100%

Tabla 17 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 18 Desagregado de Disponibilidad Directorio Activo

Datacenter Principal

Cantidad de dispositivos	Disponibilidad consolidada
8	100%

Tabla 19 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 20 Desagregado de Disponibilidad Datacenter Principal

Datacenter Alterno

Cantidad de dispositivos	Disponibilidad consolidada
5	*100%*

Tabla 21 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 22 Desagregado Disponibilidad de equipos Datacenter alterno

Redes y conectividad

Cantidad de dispositivos	Disponibilidad consolidada
339	*99,20%*

Tabla 23 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
7	100%

Tabla 24 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_FW_Sede_Central	99,99%
SOC_SandBox	100,00%
SOC_WAF	100,00%

Tabla 25 Disponibilidad de equipos Seguridad de la Información

Telefonía

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

Tabla 26 Consolidado disponibilidad de equipos de telefonía

Antivirus

Cantidad de dispositivos	Disponibilidad consolidada
1	100%

Tabla 27 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 socializó el formato de Plan de Disponibilidad a los Servicios de la operación para documentar el plan de trabajo de las pruebas de Alta Disponibilidad.
- Se realizó sesiones para la programación de las pruebas de alta disponibilidad con los servicios de Seguridad Información, Conectividad LAN, WLAN, SD-WAN y Telefonía IP.

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 enero de 2025.

Actividades en curso:

- Seguimiento a los resultados de los cambios presentados en el CAB por partes de especialistas durante el periodo.
- Revisión y seguimiento a los 11 cambios ejecutados durante el periodo con el fin de verificarla correcta documentación de las evidencias de los planes de Pruebas Previas y Posteriores de cada RFC, se relaciona el cuadro de seguimiento de cambios Implementados del periodo.

Seguimiento de cambios Implementac

- Se encuentra en proceso de modificación la Guía Operacional de la Práctica a las actividades y flujograma del proceso para la para la implementación de nuevos o modificaciones de productos según los lineamientos de la oficina TIC de la entidad.

2.2. Mesa de Servicios y Soporte en Sitio

A continuación, se relaciona la gestión desarrollada en el transcurso del mes de enero 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 enero, en el Ministerio del trabajo a la MDS ingresaron 418 llamadas de usuarios finales para solicitar servicios de Soporte Tecnológico, a continuación, se discrimina donde se clasificaron según el servicio solicitado:

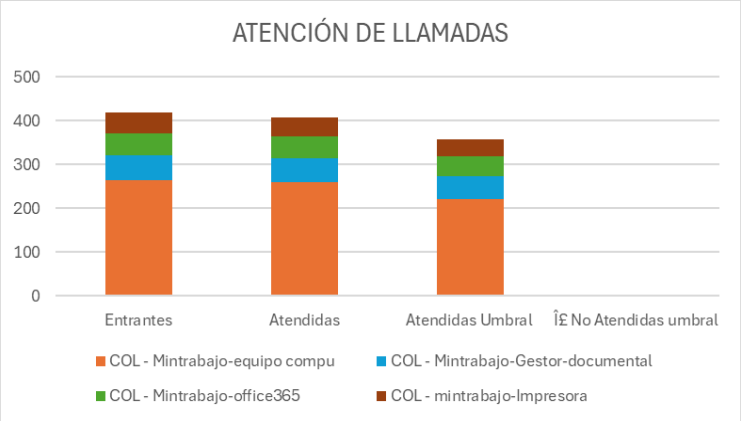


Ilustración 19 Atención de Llamadas

Servicio	Entrantes	Atendidas	Atendidas Umbral	No Atendidas umbral
COL - Mintrabajo-equipo compu	264	260	221	1
COL - Mintrabajo-Gestor-documental	57	54	51	1
COL - Mintrabajo-office365	49	49	46	0
COL - mintrabajo-Impresora	48	45	40	0
TOTAL	418	408	358	2

Tabla 28 Atención de Llamadas

El servicio más solicitado a través de la atención de llamadas es: *Equipo de cómputo* con 264 llamadas entrantes, se atendieron 260 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 enero solo se tiene 6 categorías: Directorio Activo con 402 casos corresponde al 59,12%, Alarma Zabbix *con* 165 casos, corresponde al 24,26%, Correo Electrónico con 57 casos que corresponden al 8,38%, Servidores 39 casos que corresponden al 5,74%, File Server 17 casos, que corresponden al 2,50% para un total de 680 casos.

ADMINSTRACION DE SERVIDORES	TOTAL
Directorio Activo	402
Alarma Zabbix	165
Correo Electronico	57
Servidores	39
File Server	17

Tabla 29 Top 10 administración de servidores

Top 10 de Redes y Conectividad: para el mes de enero se tiene 5 categorías más representativos de redes y conectividad que corresponden a las siguientes categorías: Alarmas Zabbix 1033 que corresponden al 96,00%, Internet con 28 casos que corresponden al 2,60%, LAN con 12 casos, corresponde al 1,12%, WLAN con 2 casos, corresponde al 0,19% y Enlace sedes (Mpls) con 1 caso, corresponde al 0,09%, para un total de 1076 casos.

REDES Y CONECTIVIDAD	TOTAL
Alarma Zabbix	1033
Internet	28
LAN	12
WLAN	2
Enlace sedes (Mpls)	1

Tabla 30 Top 10 redes y conectividad

Top 10 de Seguridad Informática: para este top solo se generan 5 categorías durante el mes de enero Los más representativos de seguridad informática que corresponden a las siguientes categorías: Firewall con 22 casos que corresponde al 37,29%, Servicios SOC con 14 caso que corresponde al 23,73%, Seguridad de la Información con 10 casos que corresponde al 16,95%, Ingeniería Social con 4 casos que corresponde cada uno al 6,78%, Reportes con 3 casos que corresponde al 5,08%, VPN cliente con 2 casos que corresponde al 3,39%, VPN Site to Site con 2 casos que corresponde al 3,39%, Soporte Antivirus con 2 casos que corresponde al 3,39%, para un total de 59 casos de Seguridad Informática.

SEGURIDAD INFORMATICA	TOTAL
Firewall	22
Servicios SOC	14
Seguridad de la Información	10
Ingeniería Social	4
Reportes	3

VPN cliente	2
VPN Site to Site	2
Soporte Antivirus	2

Tabla 31 Top 10 seguridad informática

Top 10 de Telefonía IP: Durante este periodo se gestionaron 11 casos de Telefonía IP que corresponden a: Softphone con 6 casos corresponde al 54,55%, Servicios con 2 casos corresponde al 18,18%, Hardphone con 2 casos corresponde al 18,18%, Garantía con 1 caso que corresponden al 9,09%.

TELEFONIA IP	TOTAL
Softphone	6
Servicios	2
Hardphone	2
Garantía	1

Tabla 32 Top Telefonía IP

Top 10 de Aplicaciones Especializadas: Para el mes de enero se tienen los casos más representativos de la gestión de soportes de aplicaciones que corresponden a las siguientes categorías: Gestor Documental con 309 casos que corresponde al 92.24%, Servidor de aplicaciones con 11 casos que corresponden al 3,28%, SICIP con 8 casos que corresponde al 2,39%, Datacap con 4 casos que corresponden al 1,19%, Sisinfo con 3 casos, que corresponde al 0,90%, para un total de 335 casos.

APLICACIONES ESPECIALIZADAS	TOTAL
Gestor Documental	309
Servidor de aplicaciones	11
SICIP	8
Datacap	4
Sisinfo	3

Tabla 33 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 3076 casos corresponde al 51,06%, Equipo de cómputo con 786 casos, corresponden al 13,05%, Ofimática con 419 casos que representa el 6,96%, Alarma Zabbix con 390 casos que representan el 6,47%, Correo Electrónico con 216 casos que representan el 3,59%, Solicitud información con 196 casos que representan el 3,25%, Navegadores con 155 casos que representan el 2,57%, Software Adicional con 152 casos que representan el 2,52%, Falla impresora con 118 casos que representan el 1,96%, One Drive con 117 casos que representan el 1,94$ y Microsoft Teams con 72 casos correspondientes al 1,20%con un total de casos 6024.

SOPORTE MICROINFROMATICA	TOTAL
Impresora	3076
Equipo de computo	786
Ofimática	419
Alarma Zabbix	390
Correo Electrónico	216
Solicitud información	196

Navegadores	155
Software Adicional	152
Falla impresora	118
One Drive	117
Microsoft Teams	72

Tabla 34 Top 10 soporte microinformática

- **Análisis de Casos Anulados por Servicio**

Para este periodo se tiene 4 casos anulados de los siguientes servicios:

CASOS ANULADOS	TOTAL
Administración de servidores	2
Soporte Microinformática	1
Herramientas de Gestión	1
Total general	**4**

Tabla 35 Casos Anulados por Servicio

Administración de servidores: se tiene 2 casos creados, 1 de solicitud de cambio de contraseña y 1 de solicitud de cambio de contraseña, por duplicidad.

Soporte Microinformática: se tiene 1 caso, anulados por duplicidad.

Herramientas de Gestión: se tiene 1 caso, anulados por duplicidad Monitoreo desde zabbix.

- **Análisis de Casos Suspendidos por Servicio**

Para el periodo del mes de enero, quedaron en estado suspendidos 79 casos de los siguientes servicios:

CASOS SUSPENDIDOS	TOTAL
Soporte Microinformática	42
Administración de servidores	13
Aplicaciones Especializadas	9
Redes y Conectividad	8
Telefonía IP	4
Administración de Bases de Datos	1
Seguridad informática	1
Herramientas de Gestión	1
Total general	**79**

Tabla 36 Casos Suspendidos por Servicio

Soporte Microinformática: 42 casos suspendidos debido a que se ha solicitado información complementaria a los usuarios por: Cambio Tóner con 13 casos; Cambio de periférico 8; Solicitud Backup 3 casos; Asesoría - Consulta, Instalación- Configuración, con 2 casos; Backup, Mantenimiento preventivo, Instalación - Configuración, Instalación y configuración VPN, Daño físico, Préstamo, Devolución de equipo (portátil o PC), Soporte Aplicaciones Office 365, Falla - Error conexión a red, Impresora con 1 caso cada uno.

Administración de servidores: 13 casos suspendidos por: Asignación de licencia con 4 casos, Inactivar usuario con 3 casos, Creacion de usuario, Habilitar usuario, Cambio de grupo, Cambiar contraseña, Modificar usuarios, Configuración con 1 aso cada categoría.

Aplicaciones Especializadas: 9 casos suspendidos debido a que se ha solicitado información complementaria a los usuarios: Gestor Documental con 8 casos y Servidor de aplicaciones con 1 caso.

Redes y Conectividad: 8 casos suspendidos debido a: Alarma de Zabbix en router 4 casos, Internet sin servicio con 3 casos, revisión de canal con 1 caso.

Telefonía IP: 4 casos suspendidos por: Softphone con 2 casos por configuración de extensión, 1 caso por daño físico, 1 caso por cambio de teléfono.

Administración de Bases de Datos: 1 caso suspendidos debido a que se ha solicitado información complementaria al usuario: por backup.

Seguridad Informática: **1** casos suspendidos debido a: permisos de acceso Firewall.

Herramienta de Gestion: 1 casos suspendidos debido a: alarma Zabbix.

Análisis General de Casos Solucionados - Incidentes y Requerimientos

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

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

Incidentes solucionados por Soporte Territoriales: para el mes de enero quedaron estado solucionado 3 casos, discriminados de la siguiente manera.

INCIDENTES SOLUCIONADOS TERRITORIALES	TOTAL
Envió y recepción de correos	2
Impresora	1
Total general	**2**

Tabla 37 Incidentes solucionados por Soporte Territoriales

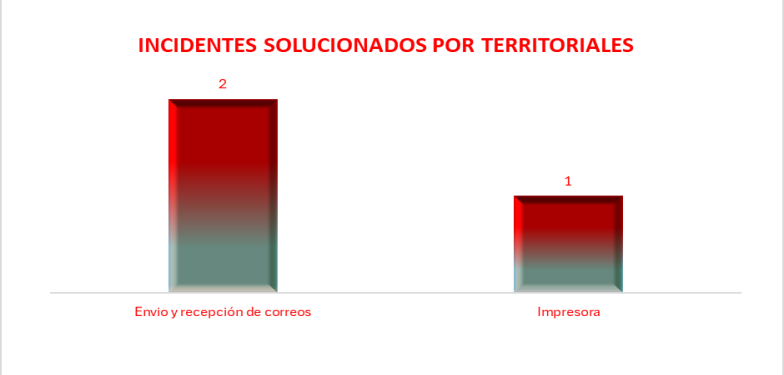


Ilustración 20 Incidentes Solucionados por Soportes Territoriales

Requerimientos solucionados por la Mesa de Servicios: Para el mes de enero quedaron 5 requerimientos discriminados de la siguiente manera:

GRUPO ASIGNADO	TOTAL
Creacion de usuario	4
Instalación - Configuración	1
Total general	**5**

Tabla 38 Requerimientos solucionados por Mesa de Servicios

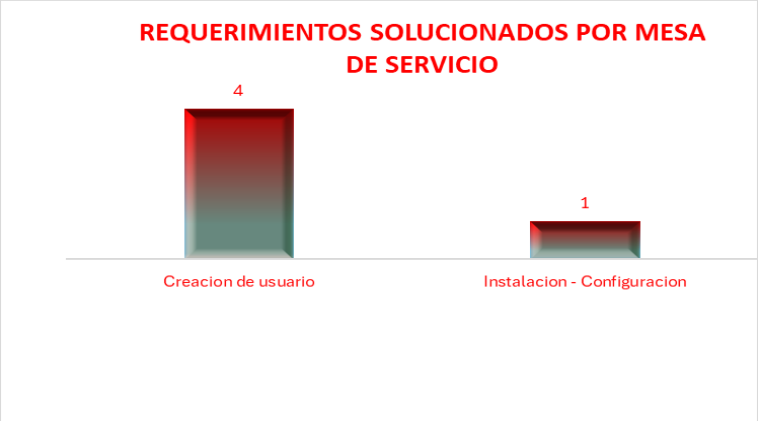


Ilustración 21 Requerimientos Solucionados por la Mesa de Servicios

Requerimientos solucionados por Soporte en sitio Bogotá: Para el mes de enero quedaron 2 requerimientos discriminados de la siguiente manera:

REQUERIMIENTOS SOLUCIONADOS POR SOPORTE EN SITIO	TOTAL
Backup	1
Asignación de equipo (portátil o PC)	1
Total general	**2**

Tabla 39 Requerimientos solucionados por Soporte en sitio

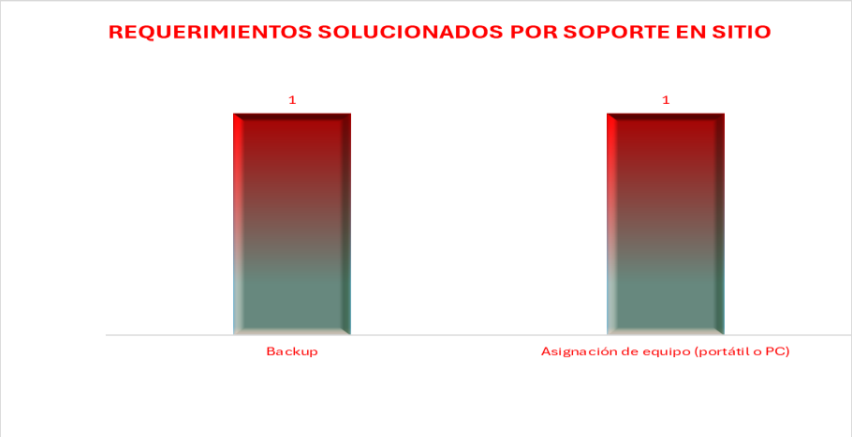


Ilustración 22 Requerimientos Solucionados por Soporte en sitio

Requerimientos solucionados por Soportes Territoriales: Para el mes de enero se solucionaron 6 requerimientos discriminados de la siguiente manera:

REQUERIMIENTOS SOLUCIONADOS POR TERRITORIALES	TOTAL
Asesoría Word	1
Traslado - Movimiento	1
Configuración	1
Asesoría Excel	1
Asesoría - Consulta	1
Asesoría PDF	1
Total general	**6**

Tabla 40 Requerimientos solucionados por Soportes Territoriales



Ilustración 23 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 enero se cerraron 633 casos, discriminados así: Asesoría – Consulta con 218 casos, Cambiar contraseña 178, Creacion de usuario con 110 casos, Cambio de grupo con 28 casos, Habilitar usuario con 21 casos, Inactivar usuario 20 casos, Accesos por fuerza bruta con 9 casos, Modificar usuarios e Instalación y configuración VPN con 8 casos, cada categoría, Configuración con 5 casos.

CERRADOS POR LA MESA DE SERVICIOS	TOTAL
Asesoría - Consulta	218
Cambiar contraseña	178
Creacion de usuario	110
Cambio de grupo	28
Habilitar usuario	21
Inactivar usuario	20
Accesos por fuerza bruta	9
Modificar usuarios	8
Instalación y configuración VPN	8

CERRADOS POR LA MESA DE SERVICIOS	TOTAL
Configuración	5
Asignación - Modificación Roles	3
Reporte conexión de usuario	3
Informes de usuarios	2
Falla - Error	2
Backup	2
Asignar Radicado TYS	2
Aumento de cuota	2
Permisos	2
Informes y Reportes	1
Impresión deficiente	1
Envió y recepción de correos	1
Solicitud depuración carpeta	1
Asignación de licencia	1
Copia de información	1
Asignación	1
Permitir acceso	1
Falla Funcional	1
Falla instalación	1
Total general	**633**

Tabla 41 Casos cerrados por la mesa de servicios

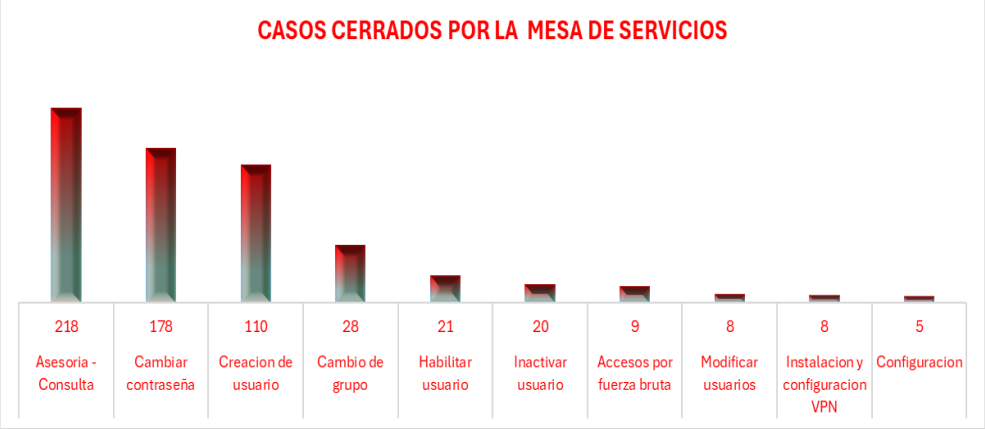


Ilustración 24 Casos cerrados por la mesa de servicios

Casos Cerrados por Soporte en Sitio: Se indica el top 10 de Requerimientos cerrados por soporte en sitio, para el mes de enero se cerraron 1081 casos discriminados así: Configuración con 254 casos, Asesoría – Consulta con 204 casos, Solicitud Papel con 118 casos, Instalación - Configuración con 104 casos, Asesoría Excel con 32 casos, No imprime con 29 casos, Préstamo con 25 casos, Conectar a red Mintrabajo con 24 casos, Envió y recepción de correos, y Asesoría Word con 20 cada categoría,

CERRADOS POR SOPORTE EN SITIO	TOTAL
Configuración	254
Asesoría - Consulta	204

CERRADOS POR SOPORTE EN SITIO	TOTAL
Solicitud Papel	118
Instalación - Configuración	104
Asesoría Excel	32
No imprime	29
Préstamo	25
Conectar a red Mintrabajo	24
Envió y recepción de correos	20
Asesoría Word	20
Asignación de equipo (portátil o PC)	17
Falla - Error	16
Soporte Aplicaciones Office 365	14
Asesoría PDF	14
Instalación y configuración VPN	13
Solicitud instalación	13
Asesoría Consulta	13
Solicitud Backup	12
Traslado - Movimiento	12
Aumento de cuota	9
Lentitud - Bloqueo	9
Falla - Error conexión a red	9
Cambio Toner	8
Mantenimiento preventivo	7
Error sincronización	7
Backup	5
Atasco	5
Falla aplicación	4
No Escanea	4
Falla Aplicaciones Office 365	4
Falla Excel	4
Falla Cargue página web	4
No enciende	3
Borrado seguro PC	3
Asesoría en ZIP	3
Borrado seguro Portátil	3
No conecta	3
Falla General	3
Instalación	3
Falla de sistema operativo	2
Asignar Pin	2
Conectar a red Invitados	2
Devolución de equipo (portátil o PC)	2
Falla ZIP	1

CERRADOS POR SOPORTE EN SITIO	TOTAL
Falla	1
Asesoría Power Point	1
Bloqueo Navegador	1
Cambio de unidad de imagen	1
Préstamo Equipo (portátil o PC)	1
Cambio Equipo Periférico	1
Solicitud depuración carpeta	1
Intermitencia - Lentitud	1
Instalación - Configuración	1
Configuración de PST	1
Instalar - Configurar	1
Lentitud	1
Copia de información	1
Falla Aplicativo	1
Error de aplicación	1
Asignación de recursos	1
Falla radicación	1
Falla PDF	1
Total general	**1081**

Tabla 42Casos cerrados por soporte en sitio



Ilustración 25 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 1779 casos, los requerimientos discriminados a continuación: Asesoría - Consulta 505 casos, Configuración con 221 casos, Instalación - Configuración con 162 casos, Solicitud de papel con 127, Asesoría Excel con 74 casos, Asesoría PDF 54 casos, Asesoria Word con 52 casos, Soporte Aplicaciones Office 365 con 51 casos, Conectar a red Mintrabajo con 50 casos y Traslado – Movimiento con 47 casos.

CASOS CERRADOS POR SOPORTE TERRITORIAL	TOTAL
Asesoría - Consulta	505

CASOS CERRADOS POR SOPORTE TERRITORIAL	TOTAL
Configuración	221
Instalación - Configuración	162
Solicitud Papel	127
Asesoría Excel	74
Asesoría PDF	54
Asesoría Word	52
Soporte Aplicaciones Office 365	51
Conectar a red Mintrabajo	50
Traslado - Movimiento	47
Asesoría Consulta	38
Atasco	35
No imprime	27
Solicitud instalación	26
Instalación y configuración VPN	23
Impresora	22
Falla - Error conexión a red	20
Copia de información	17
Solicitud Backup	16
Instalación - Configuración	15
Cambio Toner	14
No Escanea	14
Aumento de cuota	13
No enciende	12
Asignación de equipo (portátil o PC)	12
Mantenimiento preventivo	11
Borrado seguro PC	10
Instalacion	10
Devolución de equipo (portátil o PC)	8
Falla - Error	8
Cambio Equipo Periférico	7
Envió y recepción de correos	6
Falla aplicación	6
Préstamo	5
Asignar Pin	5
Falla Cargue página web	5
Error sincronización	5
Falla Aplicaciones Office 365	4
Cambio de unidad de imagen	3
Falla de sistema operativo	3
Falla General	3
Instalar - Configurar	3
Borrado seguro Portátil	3

CASOS CERRADOS POR SOPORTE TERRITORIAL	TOTAL
No conecta	2
Préstamo Equipo (portátil o PC)	2
Falla de instalación	2
Asesoría Power Point	2
Conectar a red Invitados	2
Falla radicación	2
Lentitud - Bloqueo	2
Caída - Degradación	1
Falla Word	1
Lentitud	1
Bloqueo Navegador	1
Backup	1
Falla error - Producir documento	1
Falla- Error	1
Falla del lector	1
Borrado seguro (Portátil o PC)	1
Falla	1
Falla Aplicativo	1
Falla Funcional	1
Configuración de PST	1
Total general	**1779**

Tabla 43 Casos cerrados por Territoriales



Ilustración 26 Casos cerrados por Territoriales

- **Casos Atendidos a Usuarios VIP**

Duran este periodo se crearon 1096 solicitudes para ser atendidas por soporte en sitio, de estas solicitudes se evidencio 119 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	13	13
Requerimientos	106	106
Total general	**119**	**119**

Se atendieron 977 solicitudes para el resto de los usuarios discriminados así;

TIPO DE CASO-NO-VIPS	CUMPLIMIENTO	TOTAL
Incidentes	124	124
Requerimientos	853	853
Total general	**977**	**977**

- **Medio de Ingreso de Casos**

Durante el mes de enero ingresaron a la mesa de servicio 8506 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
Web	2116
Load Massive	1879
Correo	1722
Alarma Zabbix	1663
Gestión	679
Telefónico	348
Case Creator	99
Total general	**8506**

Tabla 44 Medio de ingreso de casos



Ilustración 27 Modo de Ingreso de Solicitudes

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

Durante el mes de enero de 2025, se trabajó en el desarrollo y ajuste del guion inicial para el modelo de **machine learning** utilizado en la auditoría de llamadas. Este guion fue diseñado de manera

colaborativa entre algunos integrantes de la Mesa de Servicios y las Prácticas ITIL, con el objetivo de optimizar el proceso de auditoría y medición de la calidad en las interacciones de servicio.

Además de la construcción del guion, se ha llevado a cabo un proceso de socialización con el resto del equipo. El propósito es asegurar que todos los miembros comprendan de manera clara y detallada cómo se llevará a cabo la medición de las llamadas y qué aspectos serán susceptibles de auditoría. La socialización ha permitido garantizar que el equipo esté alineado con los objetivos del proyecto, así como con las metodologías y herramientas que se emplearán durante el proceso de auditoría.

Así mismo, se verificará si es necesario realizar ajustes adicionales en el modelo de machine learning o en el guion, en función de los resultados obtenidos durante la implementación inicial y de los comentarios recogidos del equipo. Esta revisión permitirá realizar las mejoras necesarias para optimizar la precisión y la efectividad del proceso de auditoría, garantizando así que se cumplan los estándares de calidad y eficiencia establecidos.

Fase	Criterio	Tipo de Error	Guion empleado
Bienvenida	Protocolo de bienvenida y presentacion	Crítico	Buen (día, tarde o noche) bienvenido a la mesa de servicios del ministerio de trabajo, mi nombre es (Nombre y Apellido del analista) ¿con quién tengo el gusto de hablar?
Identificacion	Identificación/captura de datos del usuario.	Crítico	Señor(a) (nombre del usuario) con el fin de registrar la llamada/crear la solicitud, ¿Me podría confirmar:
			Nombre completo
			Nombre de usuario/ Usuario de red
			Territorial o sede / área
			¿Se encuentra en casa o en sede/oficina?
			Señor(a) [Nombre del Usuario] ¿en qué le puedo ayudar?
Solucion	Realización de Pre-diagnóstico o lista de chequeo correspondiente al reporte.	No crítico	"Señor(a) (nombre del usuario) * ¿Me confirma por favor si su equipo es personal o asignado por el ministerio?
			¿Por favor me puede confirmar: -el error que esta apareciendo/presentando? -el mensaje de error que está apareciendo/presentando?
	Comunicación del mensaje de espera.	Crítico	Señor (a) [Nombre del Usuario] Agradezco me permita en línea un momento, mientras realizo/valido xxxxx.
	Agradecimiento del tiempo en línea.	No crítico	Señor(a) [Nombre del Usuario] Gracias por su espera en línea
	Personalización de la llamada.	No crítico	Señor (a) [Nombre del Usuario]
Despedida	Entrega de la información necesaria y completa al usuario.	Crítico	Señor (a) [Nombre del Usuario], ¿usted me autoriza darle solucion al caso/ solicitud?
			Señor (a) [Nombre del Usuario]), le informamos que su solicitud sera escalada al siguiente nivel para su gestion.
	Comunicación ID solicitud.	Crítico	Señor(A) (Nombre del funcionario), su solicitud ha sido registrada con numero de caso N° RF/IM XXXX
	Protocolo de despedida.	No crítico	¿Hay algo más en lo que le puedo colaborar?, Gracias por comunicarse, recuerde que hablo con (Nombre del Analista).
	Confirmacion de satisfaccion/encuesta.	Crítico	No olvide diligenciar la encuesta de satisfacción que le llegara a su correo electrónico, que tenga un buen (día, tarde, noche)

Ilustración 28 Guion inicial para el modelo de machine learning

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

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

- Se continúa gestionando el retiro de equipos por parte del anterior operador de servicios tecnológicos.
- Se realiza él envió de insumos para las impresoras a nivel nacional como Toners y papel.
- Se construyó el cronograma para los mantenimientos preventivos de las impresoras.
- Se realiza organización de cableado en las inspecciones: de los Patios, Salazar de las Palmas, Santa Barbara, Turbo, Sevilla, Tuquerres y Roldanillo.
- En la territorial de Caldas se adaptó un Hub para el trasladó de una AP.

- **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	Direccion Territorial	Sede	Descripción de la Solicitud	Actividad ejecutada para dar solución	Caso Aranda / Proveedor
7/01/2025	Caqueta	Doncello	Se desplaza personal de Soporte en Sitio para hacer revisión en la sede de temas de canal, conectividad de internet y demás servicios. Lo anterior con el apoyo y la gestión de Sergio Villareal desde Nivel Central.	- Se realiza instalación de cable ethernet del teléfono Audio códec serial SC13910418 y se realiza configuración colocando el código para validar el perfil del inspector al teléfono con éxito, se adjunta registro fotográfico. - Soporte llega al sitio, la inspección el Doncello y encuentra los equipos encendidos pero sigue con la alerta, se comienza hacer pruebas de primer nivel y se envía registro fotográfico al Ing. Sergio Villareal. Se hacen pruebas desconectando el cable de internet starlink que va a la WAN 2 del dispositivo de seguridad Fortinet y hay navegación. El ing. realiza ajustes en el fortines y se hacen pruebas desconectado la WAN 1 simulando caídas del servicio y siguen con internet el equipo. El soporte en sitió queda hasta la hora de la tarde para ver si vuele a generar la falla. Hasta el momento sin novedades. se adjuntan evidencia fotográficas. - Se recomienda Regulador de voltaje o Ups para los equipos de comunicaciones y de computo. en la inspeccion el Doncello se presenta muchas falla del fluido electrico.	RF-67570 IM-67614 RF-69713 RF-68622
10/01/2025	Vichada	Puerto Carreño	Se requiere apoyo para desplazar personal a la sede y suministrar cable UTP de 8mts requerido para asegurar conexión a red cableada de la usuaria con equipo SN MJQLS5O2.	Se realiza desplazamiento a la sede, se asiste con el cable requerido para hacer la conexión y dar solución a la conectividad LAN. Se ajusta el cable por la pared con apoyo de grapas plasticas, se deja operativo el servicio de internet en el equipo de la usuaria.	No aplica
15/01/2025	Guajira	Maicao	Reorganizción de equipos en sede por cambios al interior de la sede. Revisión apuntamiento de	- Enrique Jesus Barrios: Se realiza verificación y se ajustan los puertos de salida que envía datos al equipo, obteniendo así una mejor eficiencia	RF-70397 RF-71722 RF-71743 RF-

Fecha de visita	Direccion Territorial	Sede	Descripción de la Solicitud	Actividad ejecutada para dar solución	Caso Aranda / Proveedor
			la antena Starlink, verificación de configuración de impresora en equipos	en el servicio de internet, se realiza pruebas obteniendo acceso a los aplicativos del ministerio y servicios de internet. - Traslado equipos en la misma oficina: Se realiza la atención a la funcionaria se realiza movimientos de equipos en la misma oficina, se desinstala todo el equipo y nuevamente se instala en otro punto, se verifica que el equipo este tomando internet, que pueda imprimir, y que pueda entrar a los aplicativos, una vez realizada las pruebas se entrega el equipo al funcionario con todo en orden. - Configuración de impresora en los equipos en Maicao.	71746 RF-71715
15/01/2025	Risaralda	Dos Quebradas	Cable de red de equipo de usuario con problemas, se desplaza personal de soporte para verificar la situación y dar solución.	Se realizan las siguientes acciones en la sede para atender las necesidades de ajustes de servicios, con relación de usuarios: RF71726 - Lgalviso - Revisión Teléfono RF71720 - Dgiraldo - Impresora RF71716 - Dgiraldo - Conexión a internet	RF-71726 RF-71720 RF-71716
16/01/2025	Cesar	Cienaga	Se desplaza personal de soporte a la inspección para verificar ponchado de equipo en la sede y verificación de un usuario que reporta tener problemas con la impresora se desconecta repetidamente	Se realiza visita a la inspección y se verifica el problema de conectividad reportado por el funcionario Fernando Candanoza. Se procede a cambiar los terminales del cable RJ-45, dando así solución al inconveniente. Para el usuario Alfredo Ulloa, se realiza verificación de la falla reportada y se evidencia que la impresora se encontraba en impresión normal. se procede a realizar la configuración según esta establecido y se da solución a la falla	IM-72400 IM-72845
15/01/2025	Vaupes	Mitu	Reportan en la sede que la antena Starlink esta encendida, WiFi les funciona pero no tienen conectividad LAN. Se agenda visita de técnico para verificación del servicio.	Técnico asiste a sitio, se verifica el cable de red que lleva el internet a la red LAN pasando por el Fireall, se encuentra que todo esta bien ajustado y conectado. Se lleva a cabo revisión del Switch Starlink, se apaga y se sueltan los cables, se retira el adaptador ethernet y se limpian contactos; se enciende nuevamente la antena Starlink la cual inicia sin problemas y se restaura el servicio de internet.	No aplica
16/01/2025	Valle del Cauca	Palmira	Se agenda visita a la Inspección de Trabajo con el propósito de atender solicitudes varias de usuarios finales para prestación correcta de los servicios de TI.	A continuación, se realiza el informe del servicio realizado dicho día a los funcionarios de la sede: • Debido a la baja velocidad de internet en el computador del funcionario Gerson Jair Cifuentes, se procede a: - Se realiza borrado de cache en buscador Google Chrome. - Se realiza cambio de cable de red (Se instala cable nuevo de 15 m). - Se realiza cambio de Switch por uno ubicado en la sede de Cali. - Se observa cableado en pésimas condiciones, estoy super atento y disponible para realizar organización de el cableado del segundo piso, es un cableado muy sencillo, con unas buenas canaletas y un ponchado de algunos cables se puede obtener un cableado más organizado. Dependiendo de lo que se acuerde	A continuación, se relacionan los casos: - Validación de Hosts de equipos: RF-73667, RF-73669, RF-73670, RF-73671, RF-73674 - Revisión de antivirus: RF-73717, RF-73725, RF-73746, RF-73751, RF-73753 - Mantenimiento de equipo

Fecha de visita	Direccion Territorial	Sede	Descripción de la Solicitud	Actividad ejecutada para dar solución	Caso Aranda / Proveedor
				con el área de redes, quedo atento a la orden del ingeniero Manuel para proceder con el servicio. - Se realizan pruebas y se observa un cambio notorio en la velocidad de conexión. • Se solucionaron inconvenientes al equipo del señor Carlos Mejía: - Se realiza mantenimiento preventivo. - Se le da un asesoramiento de un archivo PDF el cual se le dificultaba editar y abrir. - Se valida la velocidad de internet del equipo (Optima). • Se realiza revisión de host de equipos de la sede: - Diana Montenegro (Revisado). - Hernán Vásquez (Revisado). - Carlos Alberto Mejía (Revisado). - Gerson Jair (Revisado). - Beder Alonso Mondragón (Revisado). • Se revisa que todos los equipos en sede tengan instalado el antivirus corporativo del Ministerio.	software: RF-73660, RF-73663 - Motor de Búsqueda: RF-73585 - Borrado de cache: RF-73589 - Cambio de cableado: RF-73618 - Asesoría de PDF: RF-73644
20/01/2025	OE Buenaventura	OE Buenaventura	Se agenda visita a la Oficina Especial con el propósito de atender solicitudes varias de usuarios finales para prestación correcta de los servicios de TI.	A continuación se realiza un compendio de las actividades realizadas en la oficina. - Revisión de cableado de puntos de red: RF-73424, RF-73428, RF-73434, RF-73435, RF-73437, RF-73438, RF-73442, RF-73444, RF-73452 - Revisión de nombramiento de equipos: RF-73595, RF-73653, RF-73655, RF-73656, RF-73658, RF-73661, RF-73662, RF-73664, RF-73665, RF-73666, RF-73668 - Revisión de antivirus: RF-73672, RF-73703, RF-73705, RF-73706, RF-73708, RF-73713, RF-73714, RF-73716, RF-73734, RF-73735, RF-73737 - Ajustes de puntos: RF-73743 y RF-73744 - Traslados de puestos de trabajo: RF-73747 y RF-73748 - Reubicación de AP: RF-73756 - Revisión de teléfonos: RF-73760, RF-73761, RF-73764 - Ponchado de cables: RF-73767 - Asignación de equipo de comúnto Helmer Antonio Atehortúa: RF-73782, RF-73783, RF-73786, RF-73790, RF-73798	Ya se relacionan
22/01/2025	Antioquia	Turbo	Se desplaza personal de soporte para hacer pruebas de conectividad y recopilar evidencias fotográficas sobre el estado del servicio de internet que se enviaron al especialista de redes para el escalamiento con el proveedor correspondiente.	Se realiza el ajuste en conexiones y configuración del Fortinet con ayuda de soporte Jesus Gonzalez, se deja sede operativa. Se da cierre al caso.	RF-72967
23/01/2025	Guainia	Inirida	Asignación de equipo a usuaria SANDRA MILENA ALVARADO CORRALES cuya posesión se dio en el mes de enero 2025.	Se realiza desplazamiento a la sede y se realiza la configuración del equipo para entrega al usuario final, se genra el acta de asignación correspondiente.	No aplica

Fecha de visita	Direccion Territorial	Sede	Descripción de la Solicitud	Actividad ejecutada para dar solución	Caso Aranda / Proveedor
23/01/2025	Vichada	Puerto Carreño	Asignación de equipo a usuaria LAURA MARIA RUIZ QUINTERO cuya posesión se dio en el mes de enero 2025.	Se realiza desplazamiento a la sede y se realiza la configuración del equipo para entrega al usuario final, se genra el acta de asignación correspondiente.	No aplica
24/01/2025	Cesar	El Copey	Edward Torres solicita desplzamiento de soporte para la inspección de Copey, se requiere revisar el firewall ya que los equipos no están tomando dirección IP, la VPN a través de la Starlink se observa caída y se debe habilitar el canal MPLS instalado con ETB. En validación con el usuario solo alude tener problemas con la impresora.	Se realiza cambio de equipo en la configuración del servicio de internet, donde todos los equipos e impresora quedan trabajando	No aplica
30/01/2025	Valle del Cauca	Roldanillo	Se programa visita en sede ya que no se tiene servicio de conectividad LAN pero se descartan fallas del enlace del proveedor.	A continuación se relaciona detalle de la visita en sitio de Roldanillo el día 30 de enero • En la presente visita se valida de que la falla principal de la sede es la conectividad de internet ya que el toma de energía se encontraba haciendo corto en uno de sus entradas, adicional que este había dañado el Multitomas donde estaba conectado los elementos como: Impresora (Un puerto), Equipo de computo (Dos puertos) Risecom (1 puerto) BDcom (1 puerto) Se comprueba que esta sobrecarga de todos estos elementos conectados a ese punto produjo el fallo de energía resultando en la desconexión del servicio reportado por el NOC • Se procede a comprar otro multitomas y conexión distribuidas para que no ocurra esta gestion, Además que ya se le notifico a la usuaria solicitar el cambio del Toma ya que este esta presentando fallas Debido a esto también se realiza organización de estos tres elementos (BDcom, Risecom y Fortinet) esto para que no esté a la vista de cualquier usuario porque este elemento se encontraba en la sala de atención al ciudadano • También con esto, se realiza el cambio de cables de Cat 5e a Cat 7(Azules), estos cables proceden de la territorial del valle en donde se encontraban en una caja. • Se realiza soporte con Edward Reyes para el proceso de reconfiguración del Fortinet luego de las actividades previas. • Por último, se le indica a la única funcionaria de la sede sobre la recolección de dos escritorios de los cuales uno esta empacado y el otro está instalado en otro escritorio. Me menciona de que solo pueden llevarse uno ya que dice que necesita	No aplica

Fecha de visita	Direccion Territorial	Sede	Descripción de la Solicitud	Actividad ejecutada para dar solución	Caso Aranda / Proveedor
				dos para la labor que ella realiza, una de atención al ciudadano y la otra para realizar tramites de el puesto de trabajo de la funcionaria Se revisa de que el otro equipo cuenta con los audífonos y demás elementos para su entrega.	
29/01/2025	Valle del Cauca	Sevilla	Se programa visita en sitio para atención de varias solicitudes de soporte que requieren los usuarios y verificación de la conexión a internet del usuario Gustavo Mafla.	A continuación se relaciona detalle de la visita en sitio de Roldanillo el día 29 de enero: • Se realiza atención y soporte en sitio para el inconveniente de conectividad a internet del funcionario Gustavo Mafla (Se reparo y reconfiguro ciertos parámetros del router de internet junto con acompañamiento del área de redes). • Se le asesora al funcionario con la edición de documentos PDF, explicándole como puede manipularlo de acuerdo a su necesidad. • Se le asesora al funcionario con la manipulación de la impresora RICOH ubicada en sitio (Se le explica como imprimir en ambas caras, que hacer si no le sale la impresión, entre otras cosas). • Se hace acompañamiento al funcionario para la creación de su firma digital. • Se le realiza mantenimiento lógico al equipo de cómputo.	Problemas de conectividad internet: RF-75047 Revision de antivirus: RF-75139 Asesoria de Impresora: RF-75459 Host del equipo: RF-75373 Mantenimiento de equipo: RF-75056 Asesoria de PDF: RF-75457
31/01/2024	Riohacha	Fonseca	Jose Alberto Solano solicita el acompañamiento de soporte en sitio, para reubicar los equipos de computo dentro de la Inspección.	Se realiza atencion al usuario, se procede a trasladar el equipo en la misma oficina, se organiza el punto de red para su conexion a internet y se prueba que todo este funcionando correctamente, una vez realizado el traslado se entrega al funcionario el equipo en funcionamiento.	RF-74400

Tabla 45 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 2024 y enero de 2025 en lo corrido de la fase de operación del servicio de soporte:

Mes/Año	Cantidad visitas Ejecutadas Mes	Total Visitas Contractuales
Octubre 2024	12	8
Noviembre 2024	7	8
Diciembre2024	13	8
Enero 2025	15	8
Total general	**47**	**32**

Tabla 46 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	99,28%	95,00%

ID	Indicadores	Resultado	Meta
MDS 2	Tiempo de solución de incidentes por soporte en sitio	96,02%	90,00%
MDS 3	Tiempo de solución de requerimientos por soporte en sitio	99,83%	90,00%
MDS 4	Tiempo de respuesta de la mesa de servicio	87,99%	85,00%
MDS 5	Abandono de llamadas	0,72%	Máximo el 8%
MDS 6	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 47 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.

Asociada a esta depuración identifican requerimientos en donde se solicita reactivación de la cuenta por pérdida de acceso a un formulario de forms asociada a dicha cuenta, este escenario se ha presentado con formularios expuestos a la ciudadanía para registro o consolidación de información, pero la entidad a nivel técnico-funcional, no tiene identificado el propietario o cuenta con un inventario que les permita validar a que cuenta de Office está asociado el formulario esto en el marco de los formularios expuestos en la página web o que se usen para recolectar información.

Se recomienda centralizar estos formularios en cuentas de servicio que posean un propietario funcional que tenga acceso a dicha cuenta y que puedan administrar los accesos y/o modificaciones asociadas a cada formulario y evitar incidencias en donde el formulario este asociado a una cuenta de usuario que se desvincula de la entidad por ende su cuenta es inactivado. Es importante mencionar, que las políticas por defecto de Microsoft indica que tras inactivada una cuenta del tenant de Office, pasados 30 días todos los forms dejarán de estar disponibles, tanto la información recolectada como el propio formulario, así este se encuentre publicado en algún recurso público de la entidad. 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.

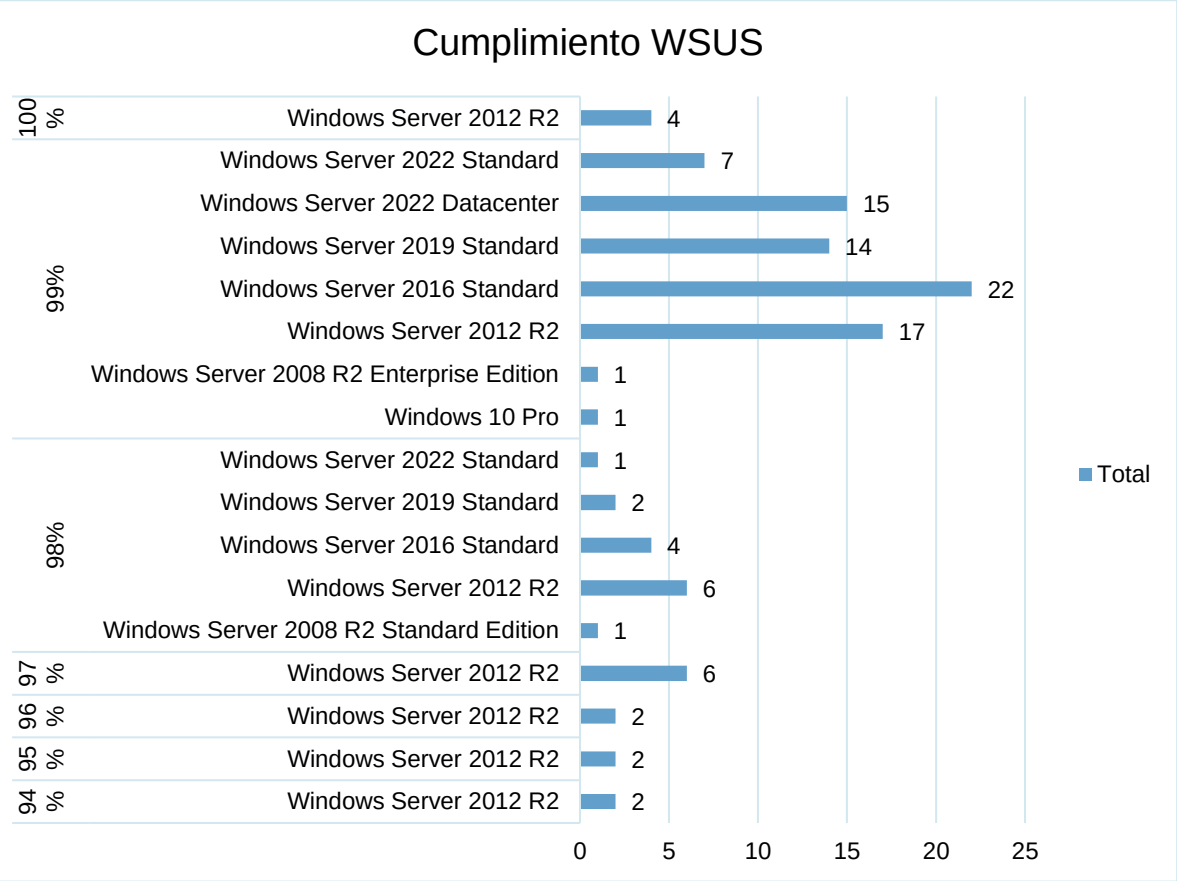


Ilustración *29* Cumplimiento WSUS

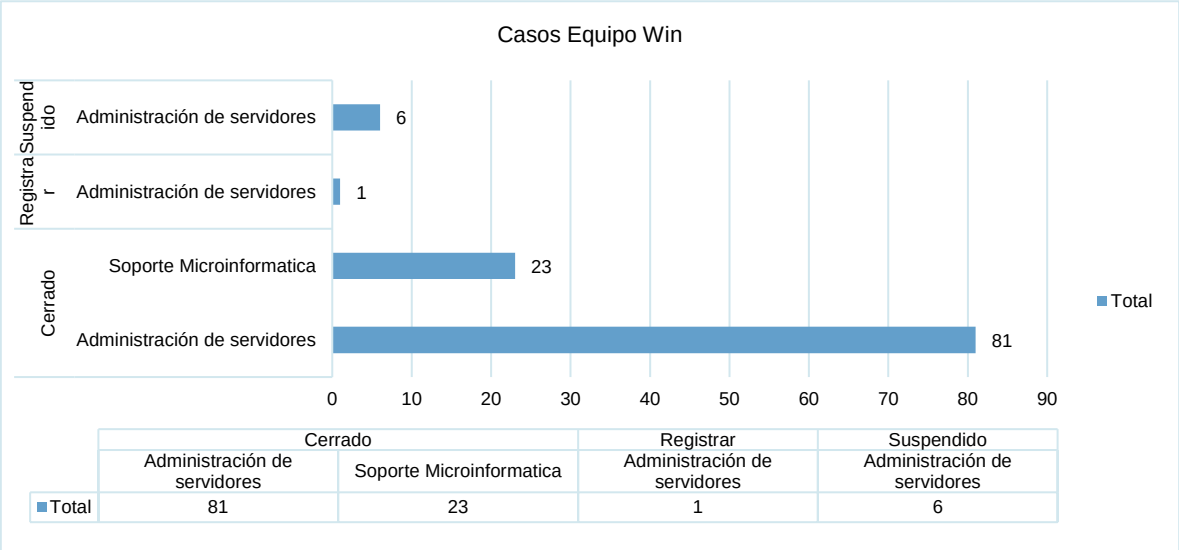


Ilustración 30 Estado final de los casos Windows

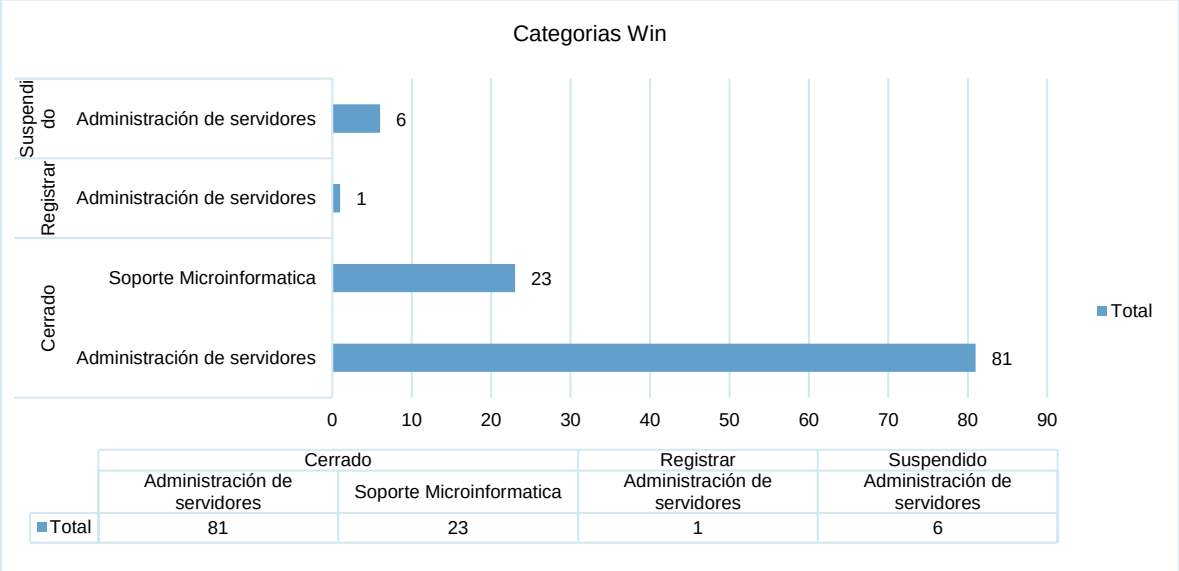


Ilustración 31 Casos por categorías Windows

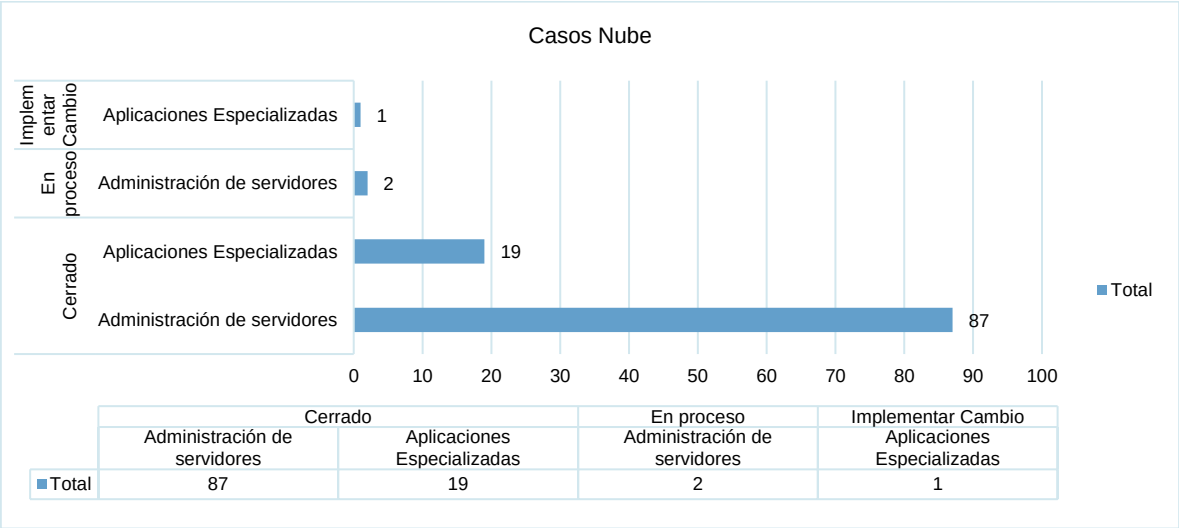


Ilustración 32 Estado final de los casos Nube privada

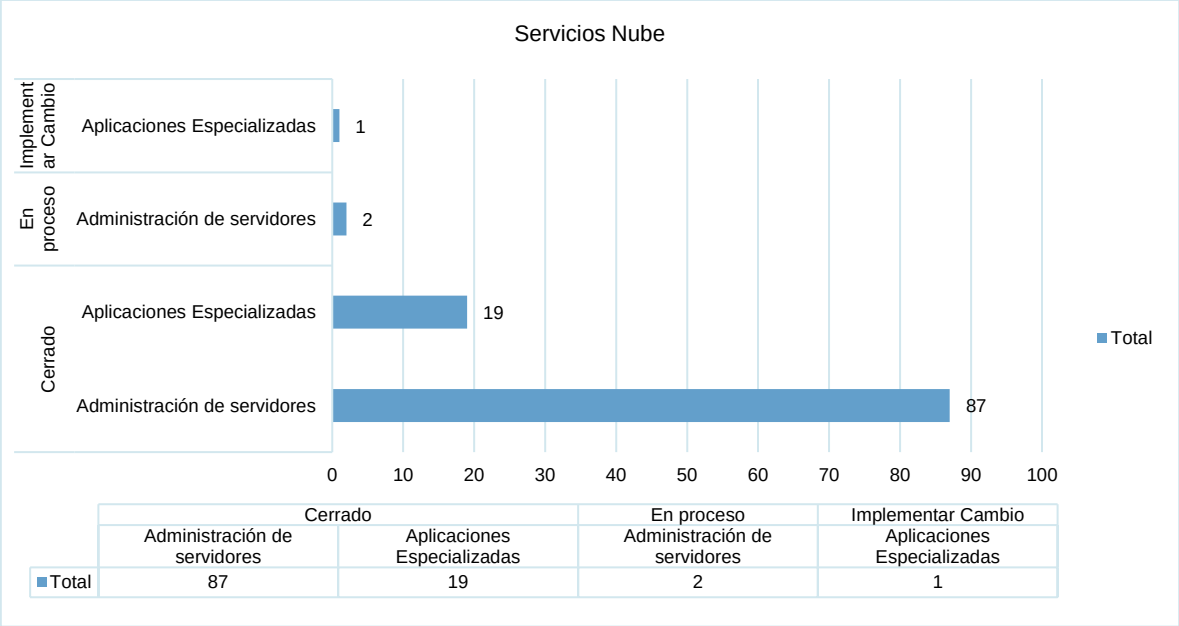


Ilustración 33 Casos por categoría Nube privada y pública

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 48 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

vCPU Ficha: **657** a vCPU consumida: 604
Memoria Ficha: **2.6 TB** a Memoria consumida: **2.3 TB**
Almacenamiento Ficha: **120 TB** a Almacenamiento consumido: **95.5 TB**
Número de Servidores Ficha: **106** a Numero de Servidores disponibles: **87**

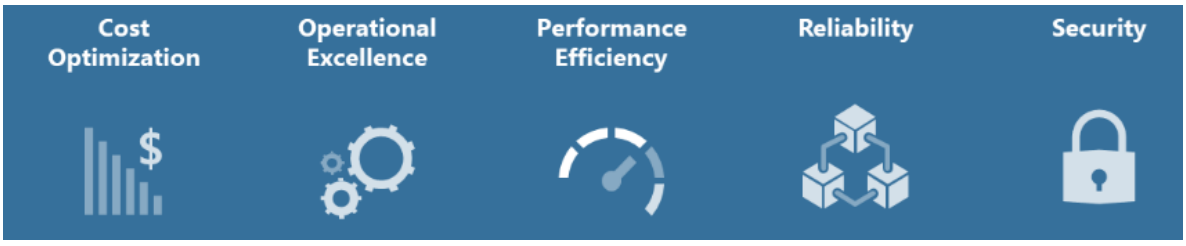
Se realizó validación de los datos, realizando exclusión de la información asociada a las capacidades consumidas por parte de los servidores de servicios de la operación, es decir máquinas aprovisionadas para operar un servicio y que no hicieron parte de la virtualización de la nube privada de la entidad, 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	**604**	**2,3 TB**	**95.5 TB**

Tabla 49 Capacidades consumidas (Sin servidores de backup)

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:

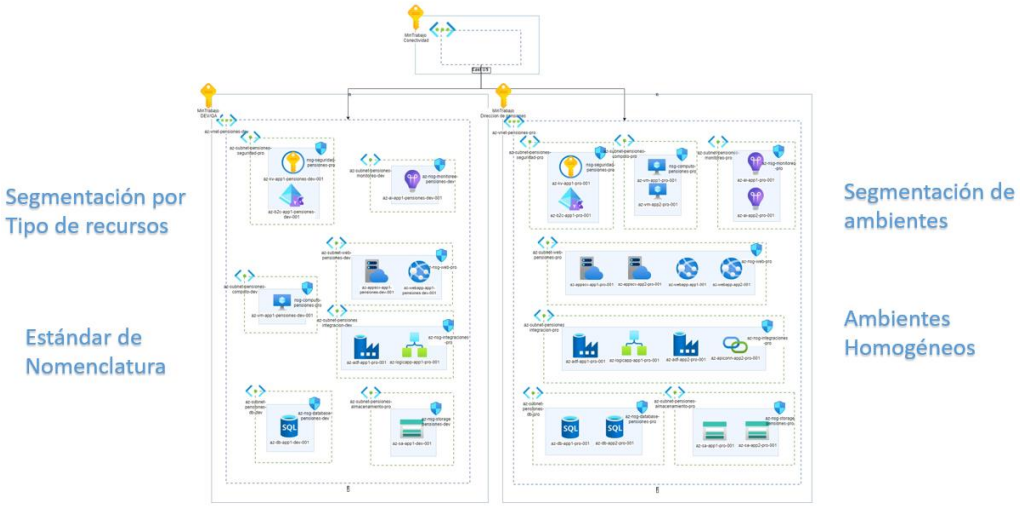


Ilustración 34 Proyección de Modelo de Suscripción

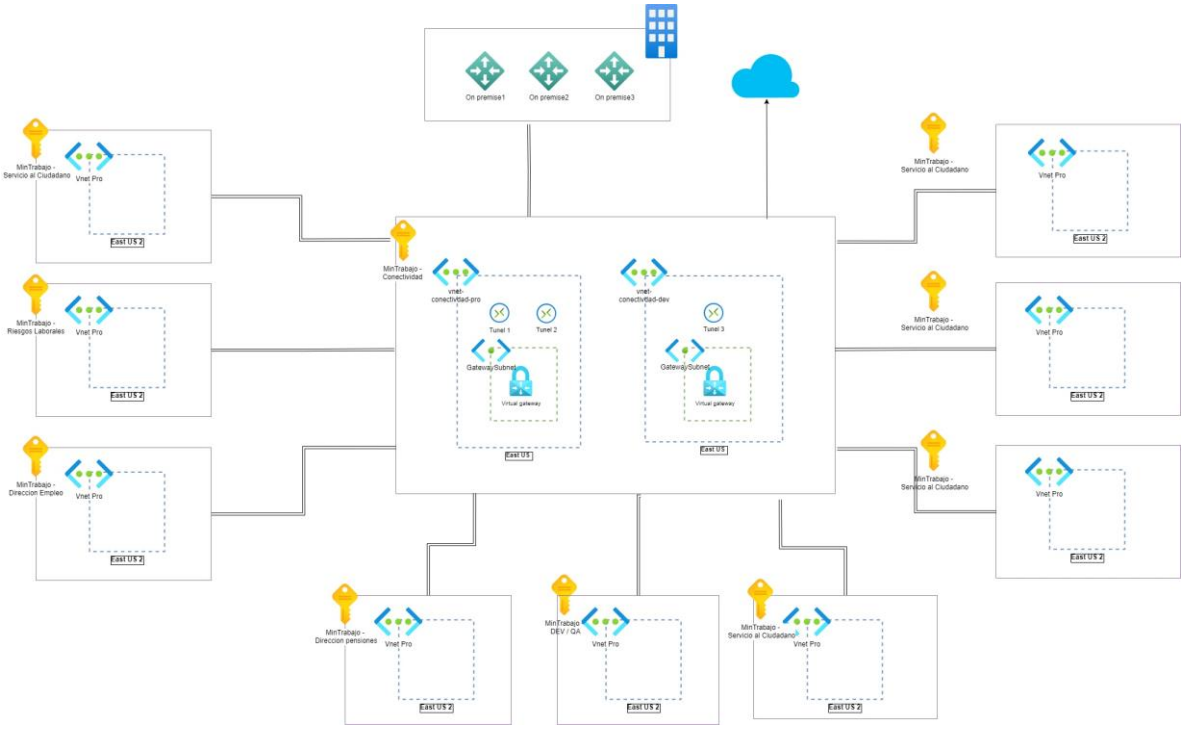


Ilustración 35 Modelo de Tenant bajo arquitectura

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 36 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 321.71 Mbps de recepción y 350.56 Mbps de transmisión.

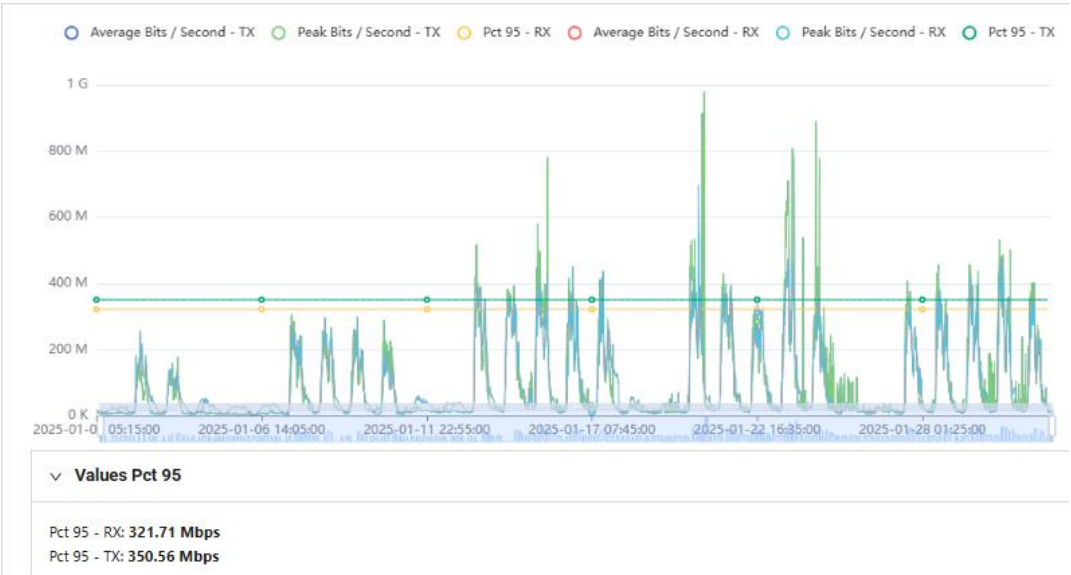


Ilustración 37. Grafica de consumo canal Internet Datacenter

Durante el mes de enero 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.

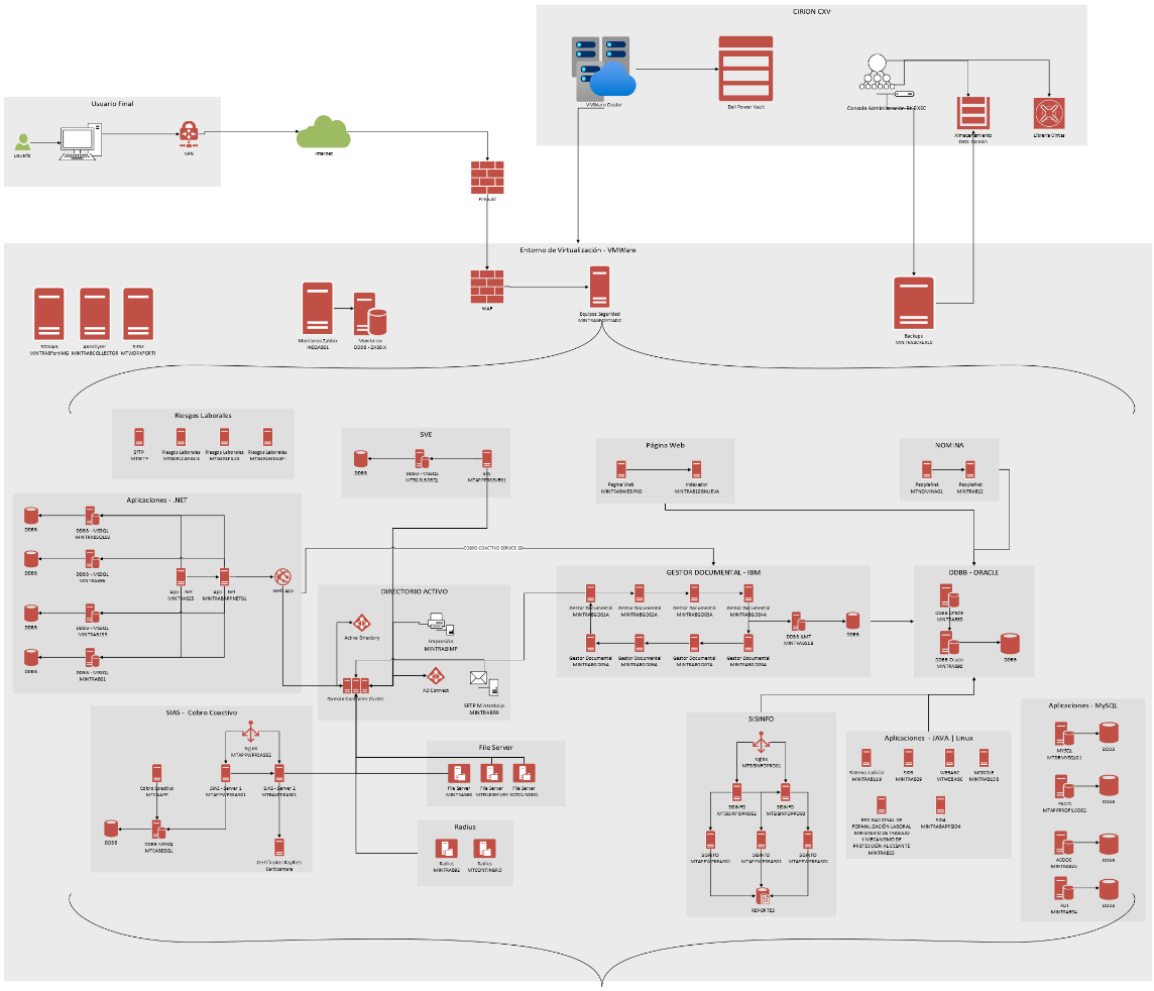


Ilustración 38 Diagrama Interoperabilidad Bogotá CXV

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 39 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.

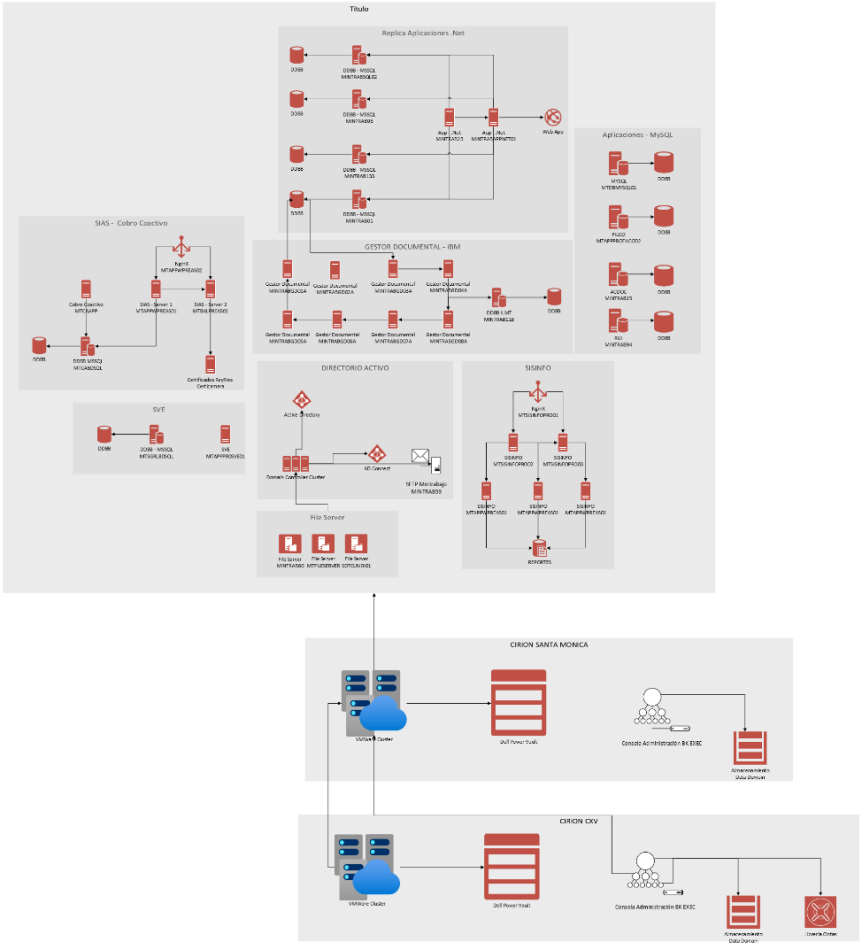


Ilustración 40 Diagrama de Replicación CXV - Santa Mónica

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 470.53Mbps de transmisión y 18.8 Mbps de recepción.

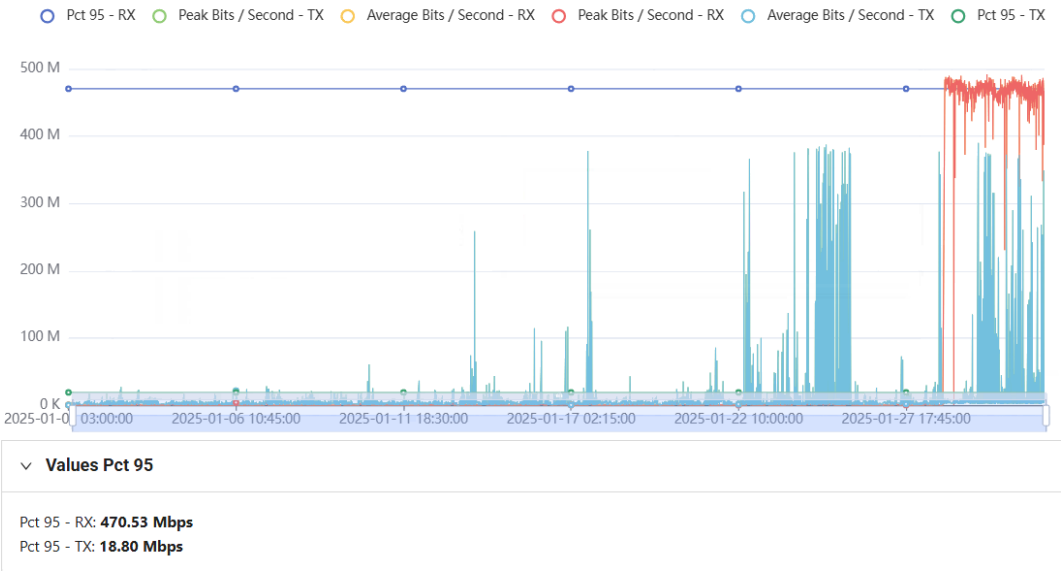


Ilustración 41 Grafica de consumo LanToLan extremo Cali

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



Ilustración 42 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 50 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

VM	NOMBRE DISCO	CAPACIDAD MB	CAPACIDAD 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 51 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:

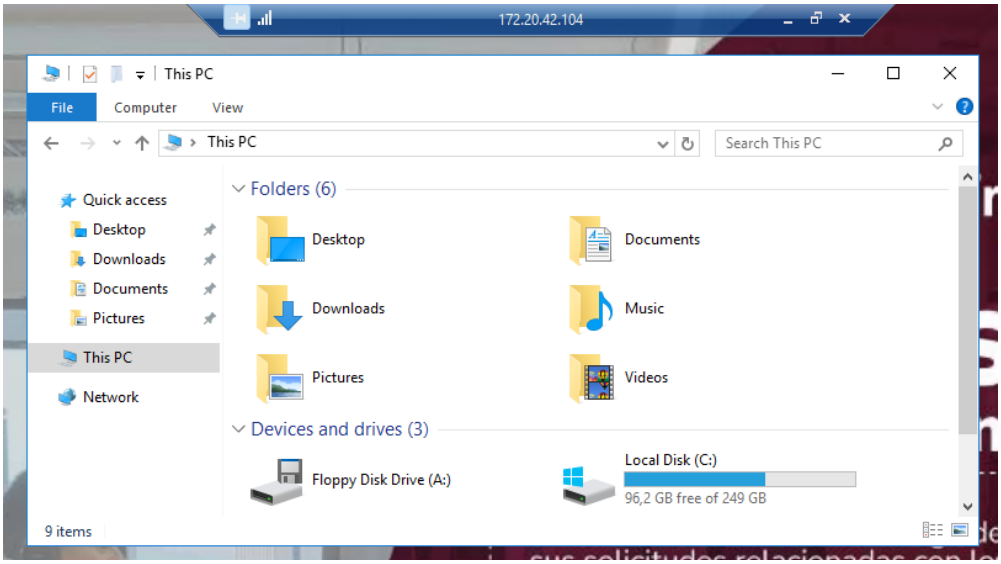


Ilustración 43 Detalle servidor

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)

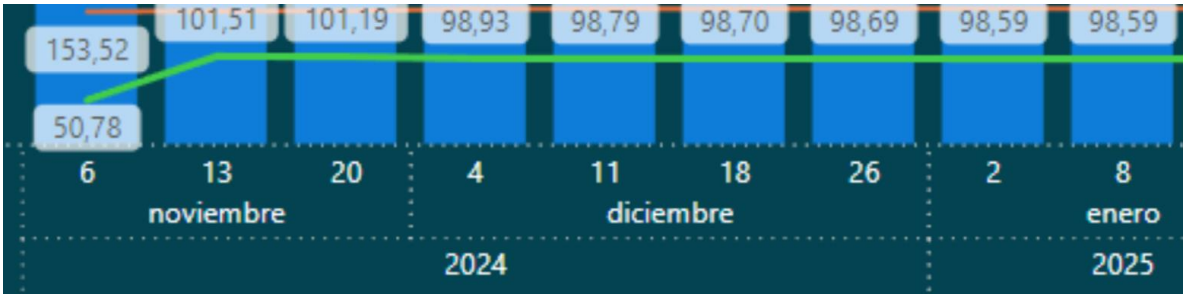


Ilustración 44 consumo de almacenamiento

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.

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.

Las vulnerabilidades encontradas asociadas a Office:

- Security Updates for Microsoft Office Products (February 2024)
- Security Updates for Microsoft Office Products (February 2024)
- Security Updates for Microsoft Office Products (August 2022)
- Security Updates for Microsoft Office Products (November 2019)
- Security Update for Microsoft Office Products (April 2017) (Petya)
- Security Updates for Microsoft Office Products (November 2017)
- MS15-099: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3089664)
- MS16-133: Security Update for Microsoft Office (3199168)
- MS16-148: Security Update for Microsoft Office (3204068)
- Security Update for Microsoft Office Products (July 2017)
- Security Updates for Microsoft Office Products (January 2018)
- Security Updates for Microsoft Office Products (October 2017)
- MS16-029: Security Update for Microsoft Office to Address Remote Code Execution (3141806)
- Security Updates for Microsoft Office Products (January 2019)
- MS15-131: Security Update for Microsoft Office to Address Remote Code Execution (3116111)
- MS16-042: Security Update for Microsoft Office (3148775)
- MS15-081: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3080790)
- MS15-116: Security Update for Microsoft Office to Address Remote Code Execution (3104540)
- MS16-015: Security Update for Microsoft Office to Address Remote Code Execution (3134226)
- MS16-054: Security Update for Microsoft Office (3155544)
- MS16-070: Security Update for Microsoft Office (3163610)
- MS16-099: Security Update for Microsoft Office (3177451)
- MS16-121: Security Update for Microsoft Office (3194063)
- Security Update for Microsoft Office Products (June 2017)
- Security Update for Microsoft Office Products (May 2017)
- Security Updates for Microsoft Office Products (May 2018)

- Security Updates for Microsoft Office Products (September 2017)
- Security Updates for Microsoft Office Products (March 2021)
- Security Updates for Microsoft Office Products (June 2024)
- Security Updates for Microsoft Office Products (March 2023)
- Security Updates for Microsoft Office Products (September 2019)
- MS15-110: Security Updates for Microsoft Office to Address Remote Code Execution (3089440)
- MS16-004: Security Update for Microsoft Office to Address Remote Code Execution (3124585)
- MS16-088: Security Update for Microsoft Office (3170008)
- MS16-107: Security Update for Microsoft Office (3185852)
- MS17-002: Security Update for Microsoft Office (3214291)
- MS17-014: Security Update for Microsoft Office (4013241)
- Security Update for Microsoft Office Excel Products (September 2017)
- Security Updates for Microsoft Office Products (April 2018)
- Security Updates for Microsoft Office Products (April 2019)
- Security Updates for Microsoft Office Products (April 2020)
- Security Updates for Microsoft Office Products (August 2019)
- Security Updates for Microsoft Office Products (August 2020)
- Security Updates for Microsoft Office Products (December 2020)
- Security Updates for Microsoft Office Products (February 2018)
- Security Updates for Microsoft Office Products (February 2019)
- Security Updates for Microsoft Office Products (January 2021)
- Security Updates for Microsoft Office Products (January 2022)
- Security Updates for Microsoft Office Products (July 2019)
- Security Updates for Microsoft Office Products (July 2023)
- Security Updates for Microsoft Office Products (November 2018)
- Security Updates for Microsoft Office Products (November 2020)
- Security Updates for Microsoft Office Products (October 2018)
- Security Updates for Microsoft Office Products (October 2020)
- Security Updates for Microsoft Office Products (October 2022)
- Security Updates for Microsoft Office Products (September 2022)
- Security Updates for Microsoft Office Products (December 2019)
- Security Updates for Microsoft Office Products (June 2018)
- Security Updates for Microsoft Office Products (May 2019)
- Security Updates for Microsoft Office Products (November 2023)
- Security Updates for Microsoft Office Products (November 2021)
- Security Updates for Microsoft Office Products (December 2021)
- Security Updates for Microsoft Office Products (October 2021)
- Security Updates for Microsoft Office Products (September 2021)
- Security Updates for Microsoft Office Products (April 2021)
- Security Updates for Microsoft Office Products (April 2022)
- Security Updates for Microsoft Office Products (June 2021)
- Security Updates for Microsoft Office Products (May 2021)
- Security Updates for Microsoft Office Products (February 2022)
- Security Updates for Microsoft Office Products (January 2020)
- Security Updates for Microsoft Office Products (September 2020)

- Security Updates for Microsoft Office Products (July 2021)
- Security Updates for Microsoft Office Products (July 2022)
- Security Updates for Microsoft Office Products (September 2023)
- Security Updates for Microsoft Office Products (August 2018)
- Security Updates for Microsoft Office Products (June 2020)

Vulnerabilidades asociadas a Capa Media:

- Apache Log4j SEoL (<= 1.x)
- Apache Log4j 1.x Multiple Vulnerabilities
- Apache Tomcat 9.0.0.M1 < 9.0.83
- Apache Tomcat 9.0.0.M1 < 9.0.86 multiple vulnerabilities
- Apache Tomcat 9.0.0.M1 < 9.0.68
- Apache Tomcat 9.0.0.M1 < 9.0.71
- Apache Tomcat 9.0.0 < 9.0.35
- Apache Tomcat 9.0.0.M1 < 9.0.43 multiple vulnerabilities
- Apache Log4j 1.2 JMSAppender Remote Code Execution (CVE-2021-4104)
- Apache Tomcat 9.0.0.M1 < 9.0.81 multiple vulnerabilities
- Apache Tomcat 9.0.0.M1 < 9.0.36
- Apache Tomcat 9.0.0.M1 < 9.0.40 multiple vulnerabilities
- Apache Tomcat 9.0.13 < 9.0.63
- Apache Tomcat 9.0.0.M1 < 9.0.46
- Apache Tomcat 9.0.0.M1 < 9.0.37 multiple vulnerabilities
- Apache Tomcat 9.0.0.M1 < 9.0.44 multiple vulnerabilities
- Apache Tomcat 9.0.0.M1 < 9.0.80
- Apache Tomcat 9.0.30 < 9.0.65
- Apache Tomcat 9.0.0.M1 < 9.0.38
- Apache Tomcat 9.0.0.M1 < 9.0.48
- Apache Tomcat 9.0.0.M1 < 9.0.72
- Apache Tomcat 9.0.0.M1 < 9.0.90
- Apache Tomcat Default Files
- Apache Tomcat 9.0.0.M1 < 9.0.62 Spring4Shell CVE-2021-43980

Vulnerabilidades asociadas a otros componentes:

- 7-Zip < 23.00 Multiple Vulnerabilities
- Notepad++ < 8.5.7 Multiple Buffer Overflow Vulnerabilities
- Mozilla irefox < 126.0
- Mozilla Firefox < 24.0.1
- Mozilla Firefox < 127.0
- Mozilla Firefox < 125.0
- Mozilla Firefox < 123.0
- Mozilla Firefox < 124.0

Vulnerabilidades asociadas a Oracle JAVA:

- Oracle Java SE 1.7.0_321 / 1.8.0_311 / 1.11.0_13 / 1.17.0_1 Multiple Vulnerabilities (October 2021 CPU)
- Oracle Java SE Multiple Vulnerabilities (April 2023 CPU)

- Oracle Java SE Multiple Vulnerabilities (January 2024 CPU)
- Oracle Java SE Multiple Vulnerabilities (July 2023 CPU)
- Oracle Java SE 1.7.0_271 / 1.8.0_261 / 1.11.0_8 / 1.14.0_2 Multiple Vulnerabilities (Jul 2020 CPU)
- Oracle Java SE 1.7.0_311 / 1.8.0_301 / 1.11.0_12 / 1.16.0_2 Multiple Vulnerabilities (July 2021 CPU)
- Oracle Java SE Multiple Vulnerabilities (April 2022 CPU)
- Oracle Java SE Multiple Vulnerabilities (July 2022 CPU)
- Oracle Java SE 1.7.0_301 / 1.8.0_291 / 1.11.0_11 / 1.16.0_1 Multiple Vulnerabilities (Apr 2021 CPU)
- Oracle Java SE 1.7.0_281 / 1.8.0_271 / 1.11.0_9 / 1.15.0_1 Multiple Vulnerabilities (Oct 2020 CPU)
- Oracle Java SE 1.7.0_291 / 1.8.0_281 / 1.11.0_10 / 1.15.0_2 Information Disclosure (Windows Jan 2021 CPU)
- Oracle Java SE 1.7.0_331 / 1.8.0_321 / 1.11.0_14 / 1.17.0_2 Multiple Vulnerabilities (January 2022 CPU)
- Oracle Java SE Multiple Vulnerabilities (October 2022 CPU)
- Oracle Java SE Multiple Vulnerabilities (October 2023 CPU)
- Oracle Java SE Multiple Vulnerabilities (January 2023 CPU)

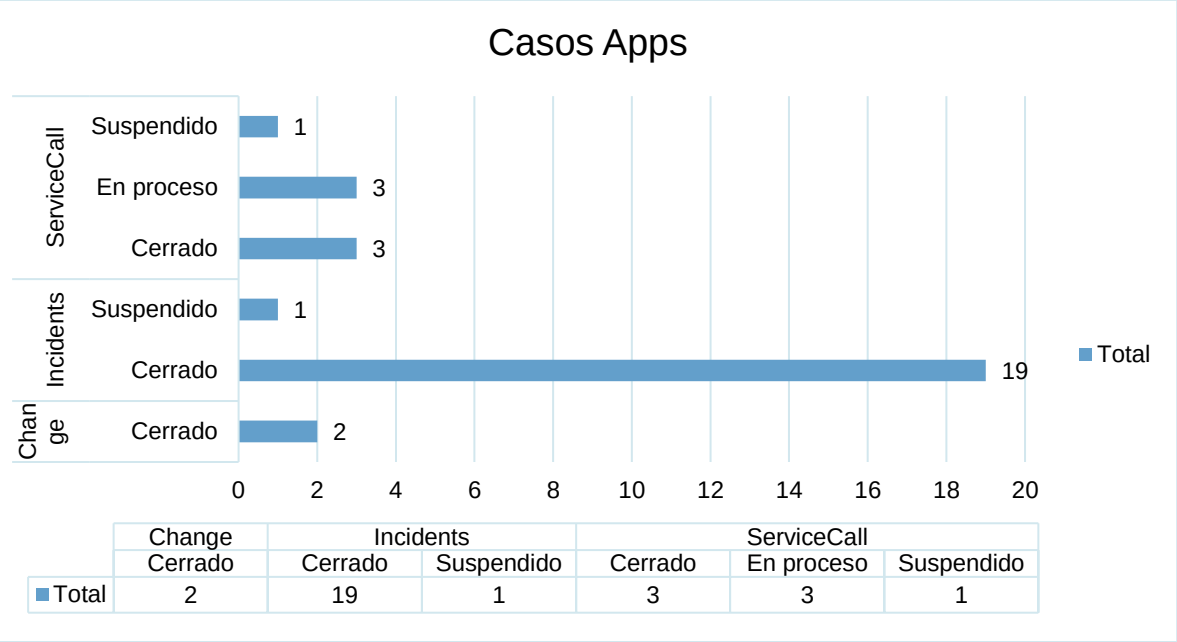
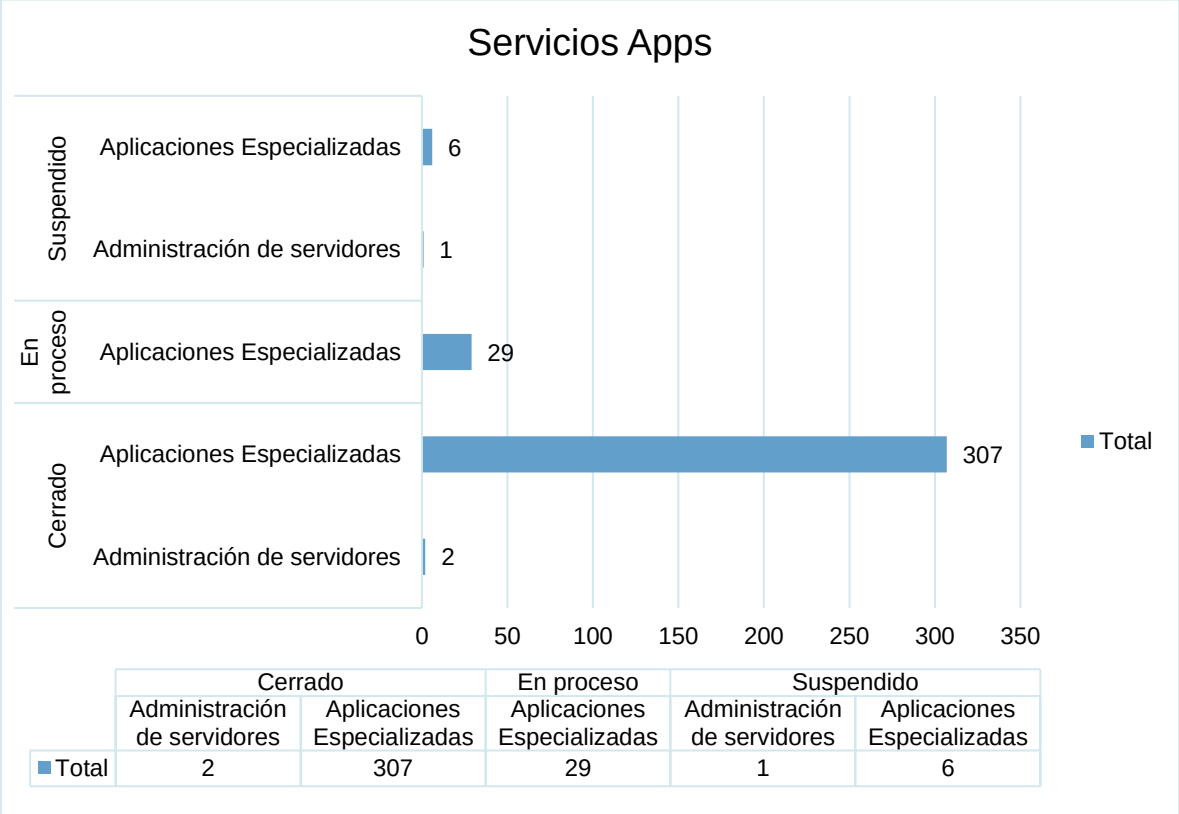


Ilustración *45* Estado final de casos – Aplicaciones Especializadas



	Cerrado		En proceso	Suspendido	
	Administración de servidores	Aplicaciones Especializadas	Aplicaciones Especializadas	Administración de servidores	Aplicaciones Especializadas
Total	2	307	29	1	6

Ilustración 46 categorías Apps

Retomando el evento presentado durante noviembre donde se materializó un evento de seguridad asociado a esta aplicación (SIAS) en donde se presentó una posible vulneración sobre el servidor que aloja los servicios de balanceo de esta aplicación, provocando publicación de micrositios no asociados a la funcionalidad del sistema de información. Dentro del análisis realizado y para evitar una posible propagación de esta incidencia, se toma la decisión de apagar los servicios de balanceo y remover temporalmente la publicación de esta aplicación hasta validación con áreas funcionales pasos a seguir, mitigación de vulnerabilidades asociadas a desarrollo dentro del código de la aplicación, acciones a tomar a corto, mediano y largo plazo y por último aceptación del riesgo y definición de compromisos con las áreas responsables.

Durante la madrugada del día 18 de noviembre de 2024 se detectó a través de la herramienta de monitoreo Zabbix, la indisponibilidad de la página del sistema FILCO el cual se encuentra alojado en el servidor virtual 172.20.44.51 con nombre MTAPPPROFILCO02.

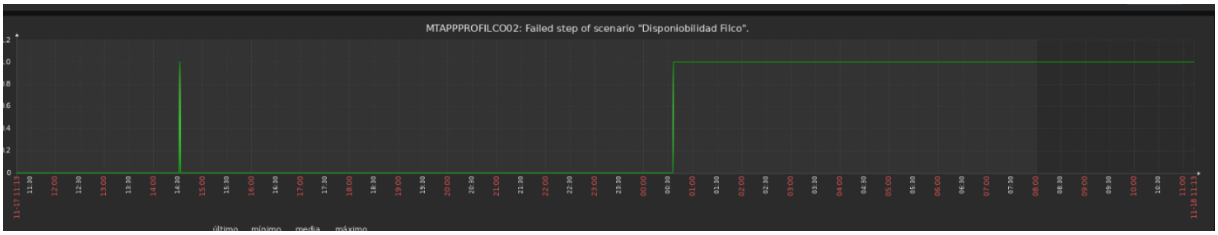


Ilustración 47 Grafica de indisponibilidad del servicio.

Al realizar la validación del servicio, dentro del servidor de aplicación por parte del especialista de aplicaciones, se observa una indisponibilidad sobre la página web de acceso al sistema de información FILCO, mostrando la siguiente información:

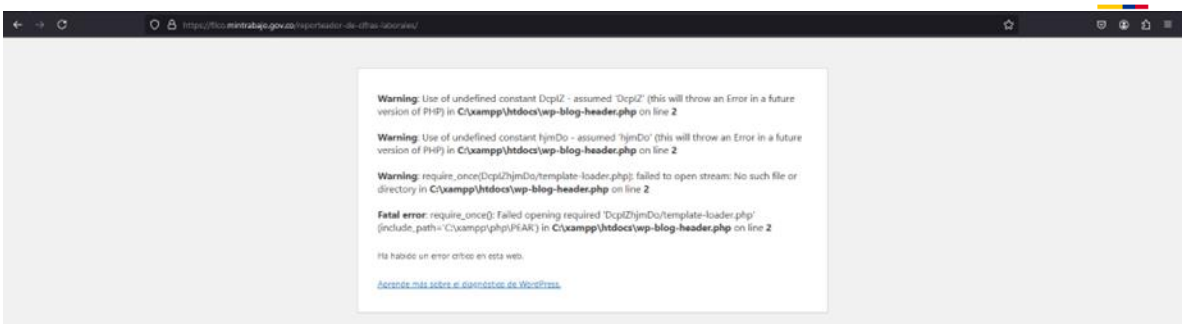


Ilustración 48 Acceso FILCO tras la indisponibilidad

Se realiza un análisis del evento presentado, en donde se observa que la aplicación está intentando realizar el llamado de algunos archivos que no está encontrando dentro de sus rutas de configuración habitual. Se observa que FILCO está intentado cargar archivos de configuración de WordPress que es el medio el cual está precargando archivos no configurados por defecto en la aplicación. Por lo cual se entra a validar las rutas especificadas en la anterior captura. Se observa que algunos archivos tipo encabezado fueron modificados durante la madrugada del día 18 de noviembre, esto se observa en los logs del servidor que aloja la aplicación.
Tras análisis del antivirus sobre la máquina afectada se observan eventos categoría alta relacionados con URL maliciosas durante el rango de horas que ocurrió la afectación del servicio:

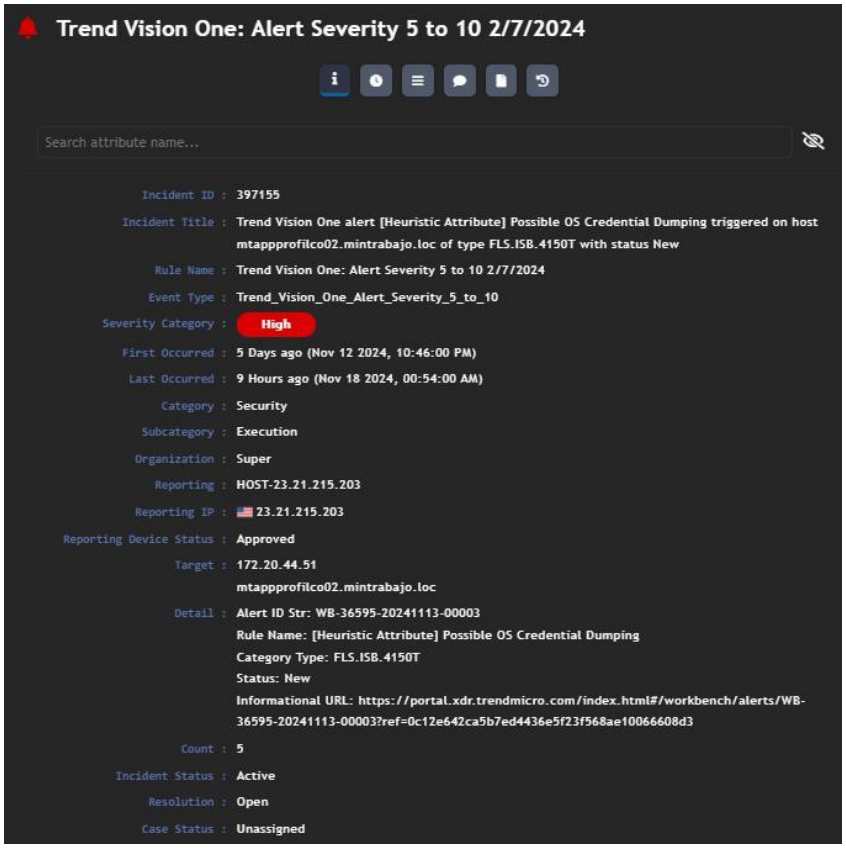


Ilustración 49 Evento Alto - Trend Vision One

Al realizar análisis de este comportamiento con las herramientas especializadas del equipo de seguridad informática del proyecto, se observa el siguiente comportamiento:
Historial de eventos Anti-Malware para el servidor:

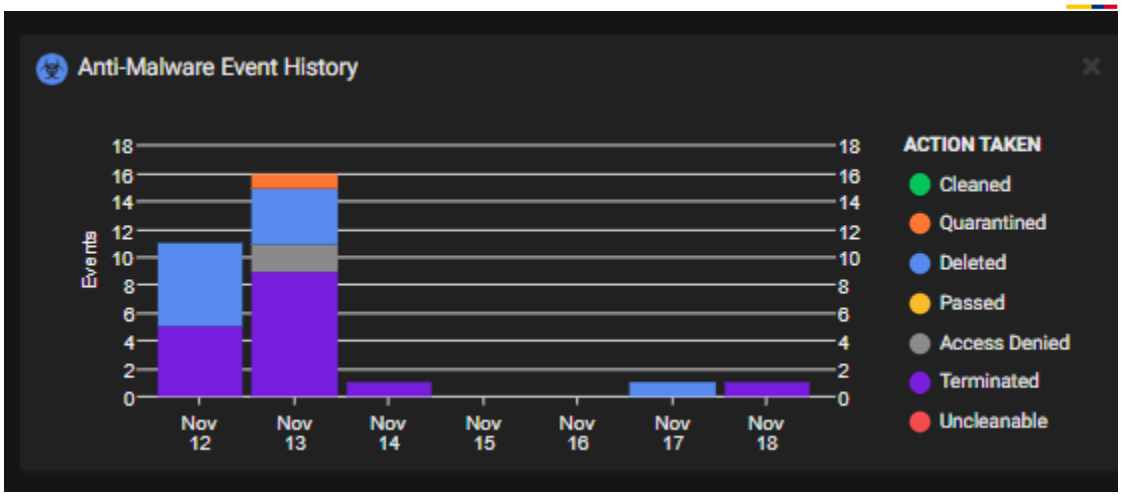


Ilustración 50 Historial de Eventos Anti-Malware

Estado Anti-Malware – Eventos limpiados sobre el servidor afectado 5

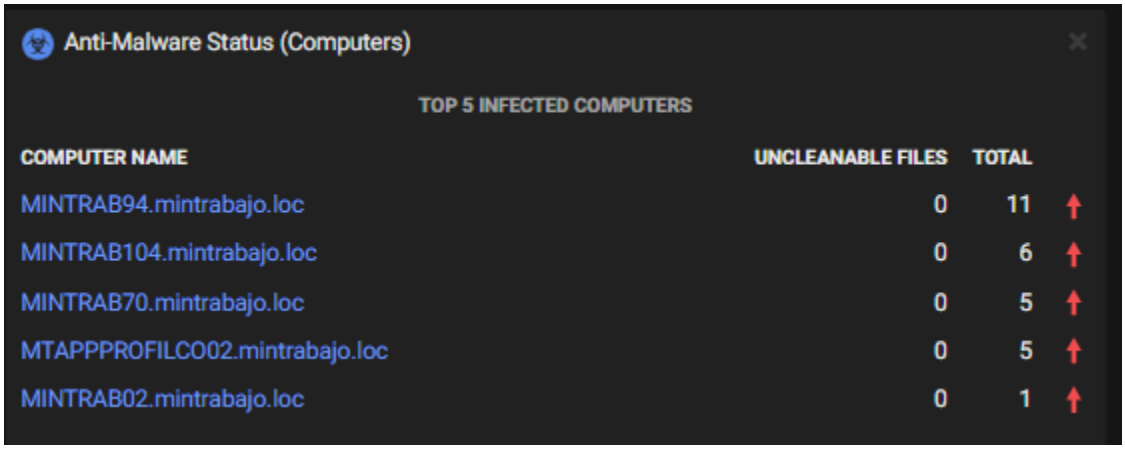


Ilustración 51 Estad Anti-Malware Servidores reportados

Eventos noviembre para el servidor de aplicación de FILCO:

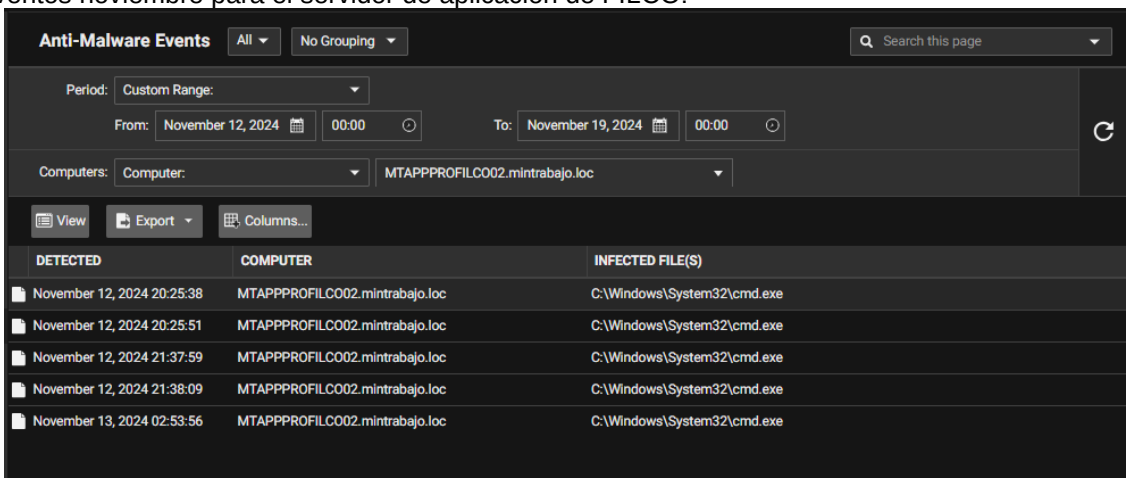


Ilustración 52 Eventos Noviembre FILCO

Línea de comando hilo detectado desde herramienta de monitoreo y análisis del equipo de seguridad, encontrando intentos de ejecución de líneas de comando desde el servidor de aplicación.

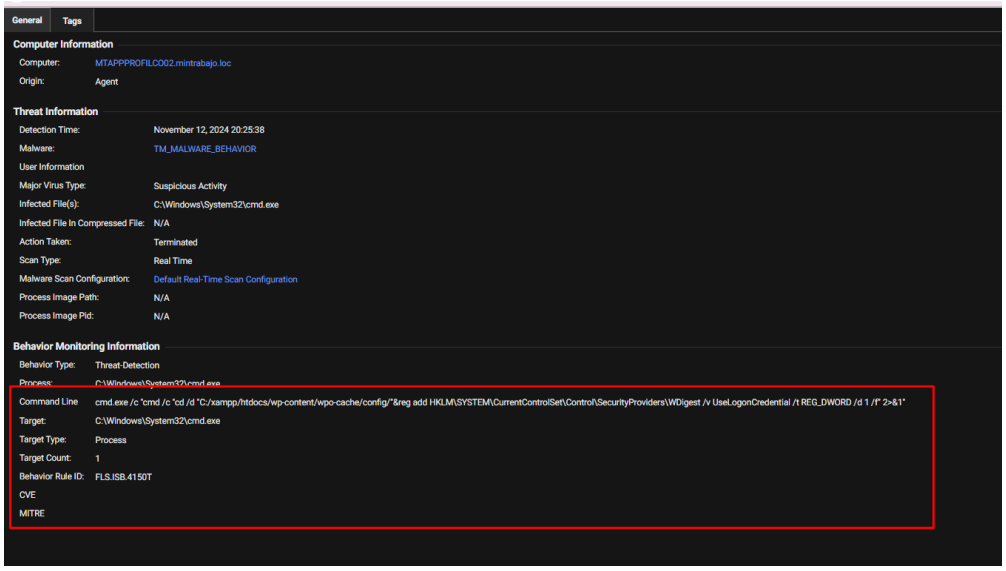


Ilustración 53 Evento Ejecución línea de comando

Se observa que, a través de la propia aplicación de seguridad, la actividad fue terminada y no permitió su ejecución:

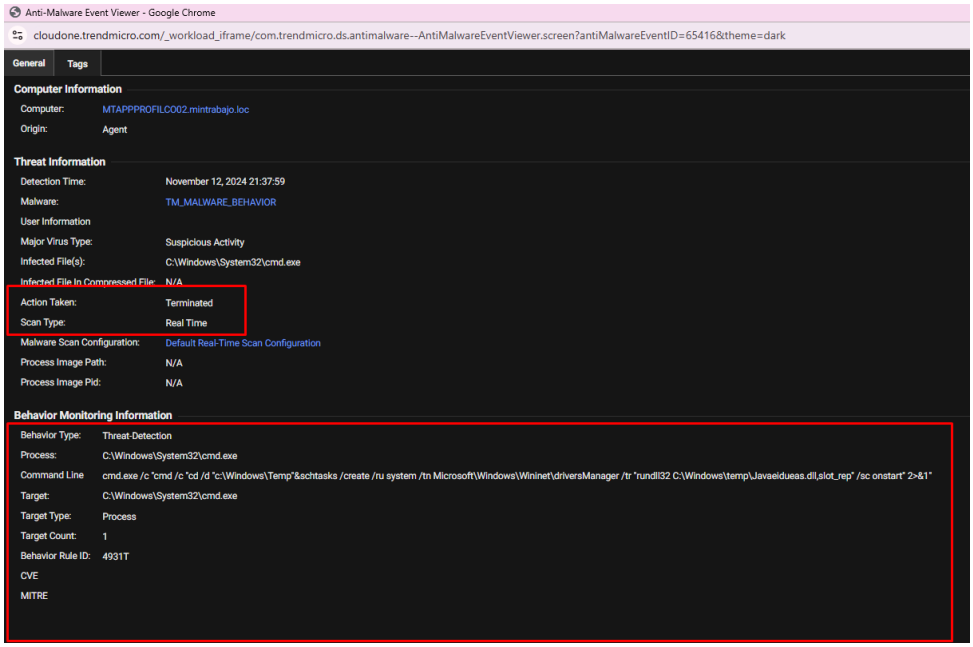


Ilustración 54 Evento terminado - Ejecución Línea de comando

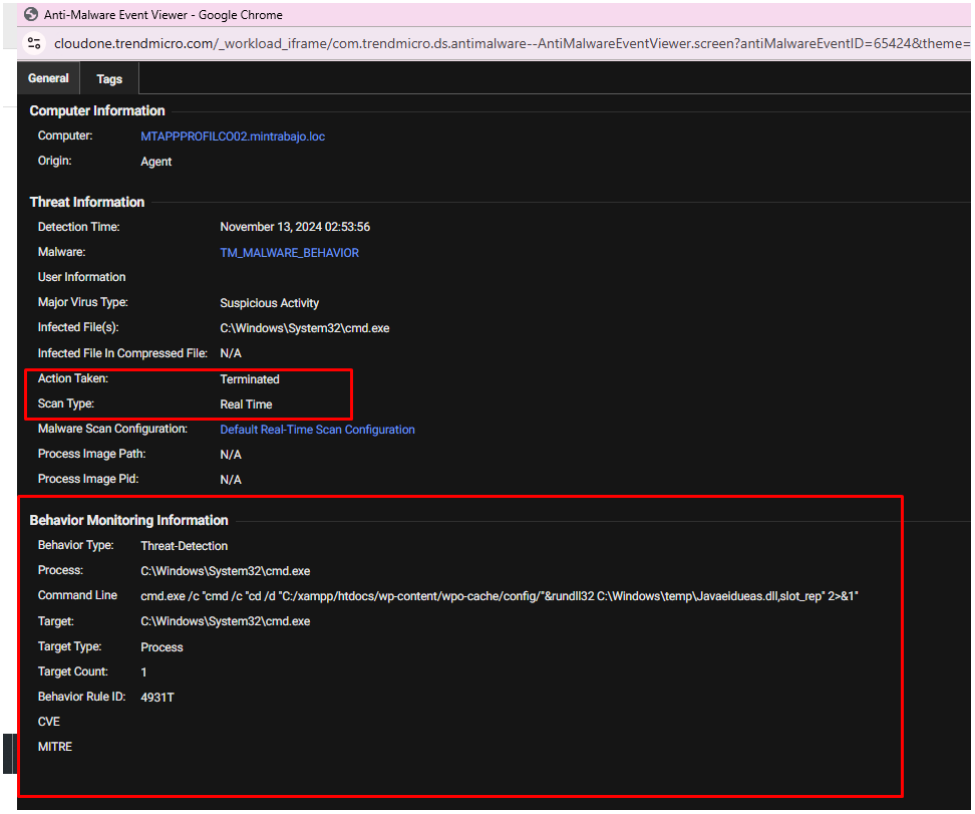


Ilustración 55 Evento terminado - Ejecución línea de comando

De igual forma se da visibilidad de los archivos modificados durante la madrugada del lunes 18 de noviembre de 2024, archivos PHP wp-blog-header.php.

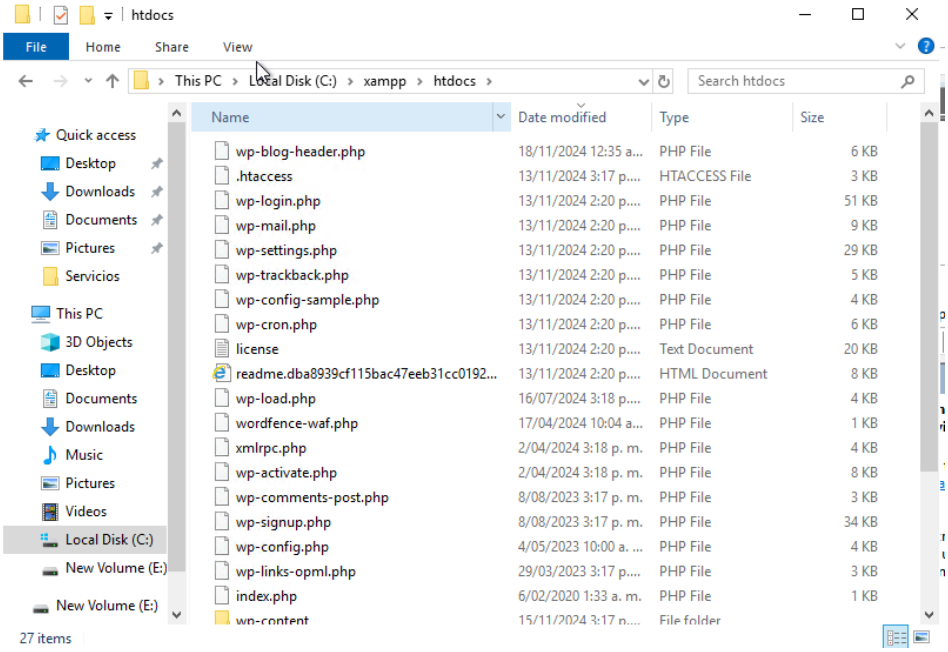


Ilustración 56 Archivos modificados durante el evento

Tras esta interacción sospechosa sobre el servidor, con fines de salvaguardar la información y la seguridad de los activos tecnológicos y la nube privada de la entidad, la cual aloja servicios e

información crítica, se tomó la decisión de apagar la máquina virtual que aloja el sistema de información FILCO de manera indefinida, ya que aunque se realizaron análisis y el caso aún continua en estudio, como medida preventiva se realizó el apagado de esta máquina hasta no tener certeza de que este evento de seguridad, no representa un incidente de seguridad informática para la entidad y un riesgo de pérdida de información o evento malintencionado que comprometa la información o seguridad de la entidad.

Es importante mencionar que WordPress es una herramienta de uso libre la cual se ha reportado como una herramienta con múltiples vulnerabilidades que permiten a entidades externas y/o malintencionadas la ejecución de código remota o realizar este tipo de actividades sospechosas, por lo cual no se recomienda su uso para alojar aplicaciones misionales o transversales de la entidad. De igual forma esto se ha comunicado a la entidad a través del informe xss FILCO remitido por el área de ciberseguridad del proyecto a la entidad.

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.*

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.

- ## 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 a 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 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:

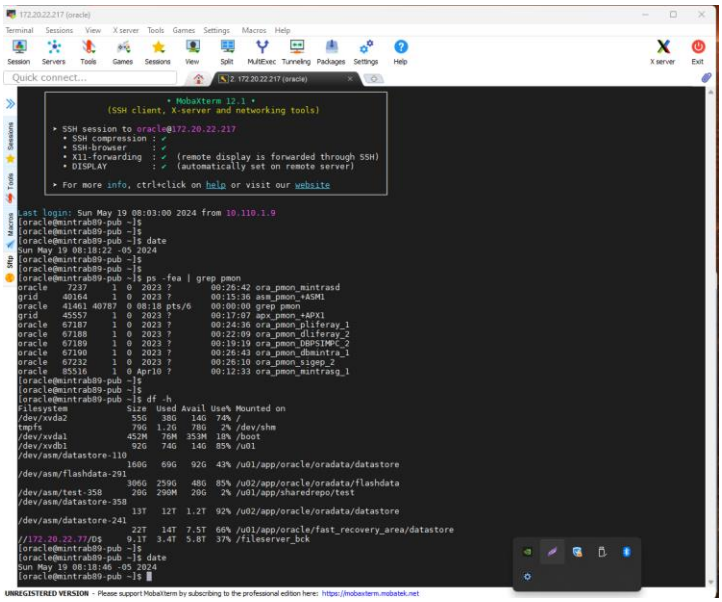


Ilustración 57 Estado pre-ventana

- **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

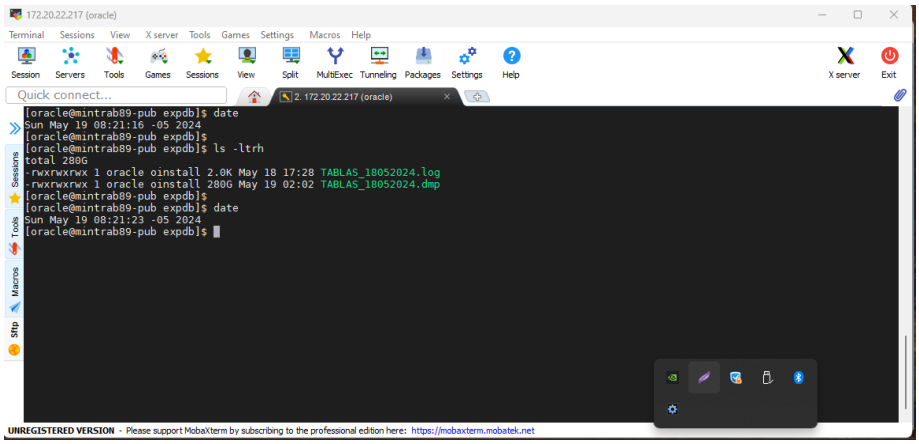


Ilustración 58 Generación de Backups DDBB

Validación tablas:

- **Tabla STORED_SYMBOL_TABLE:**

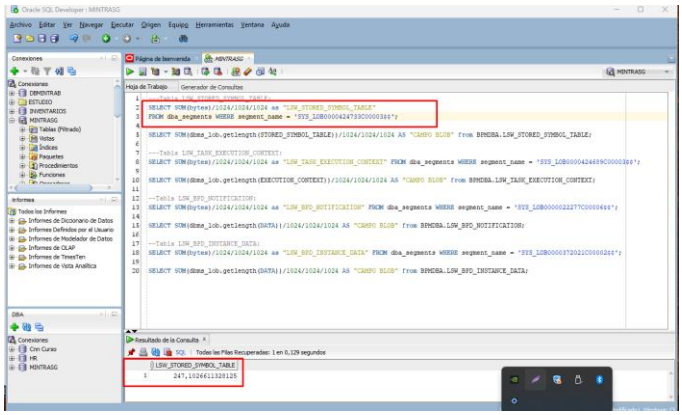


Ilustración 59 Validación Tablas DDBB

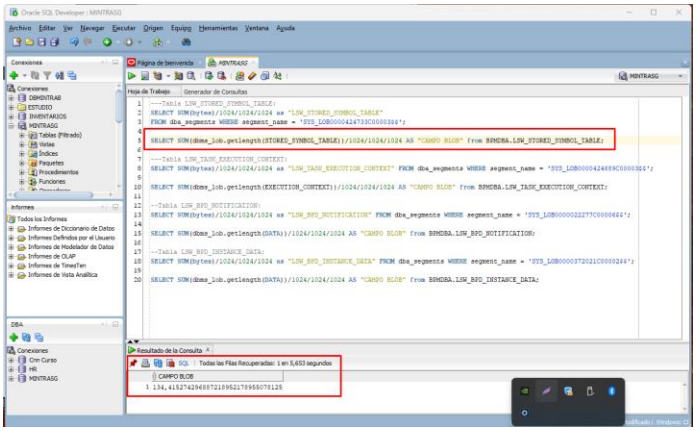


Ilustración 60 Validación Tablas DDBB

- **Tabla LSW_TASK_EXECUTION_CONTEXT:**

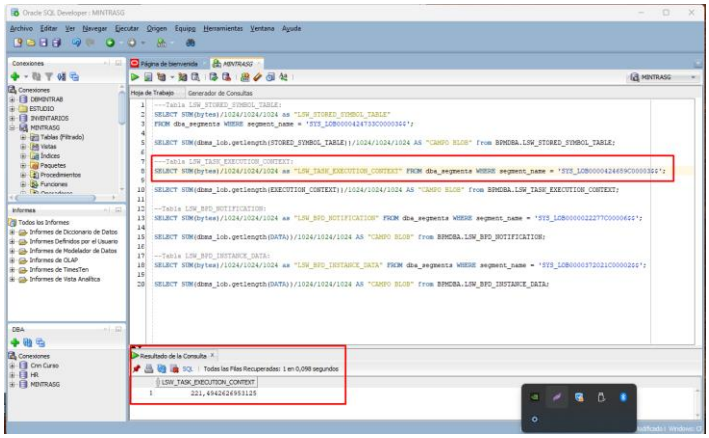


Ilustración 61 Validación Tablas DDBB

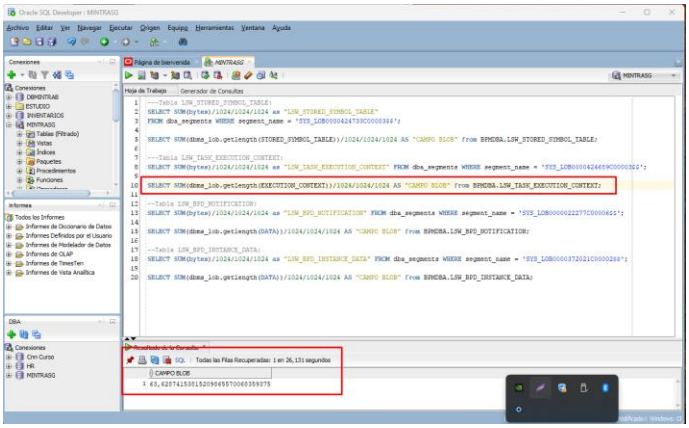


Ilustración 62 Validación Tablas DDBB

- **Tabla LSW_BPD_NOTIFICATION:**

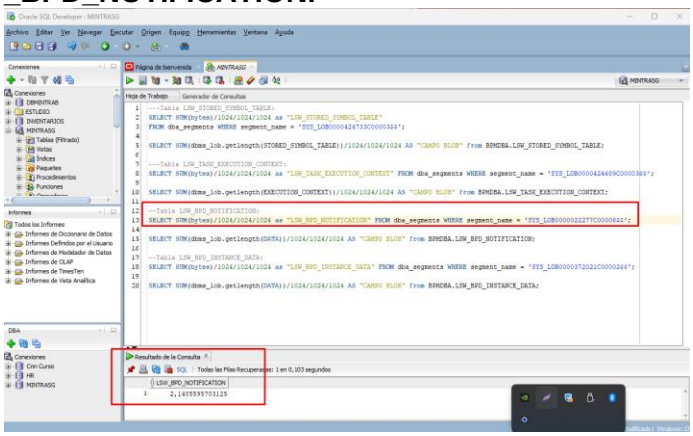


Ilustración 63 Validación Tablas DDBB

- **Tabla LSW_BPD_INSTANCE_DATA:**

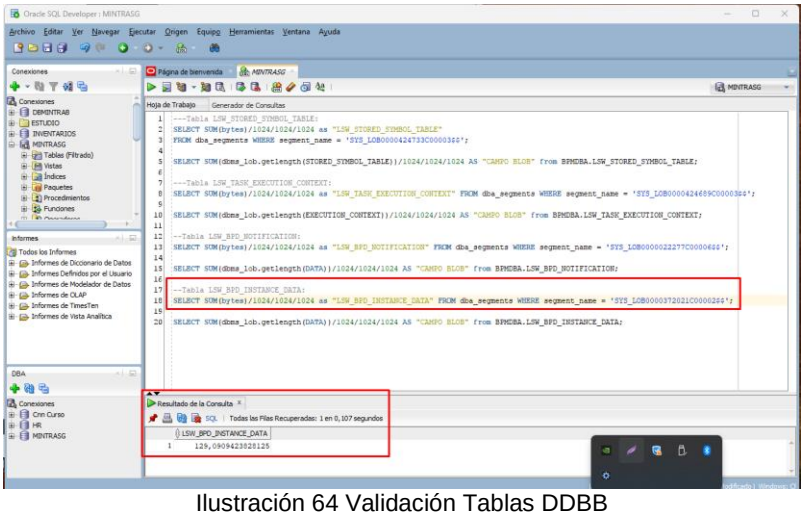


Ilustración 64 Validación Tablas DDBB

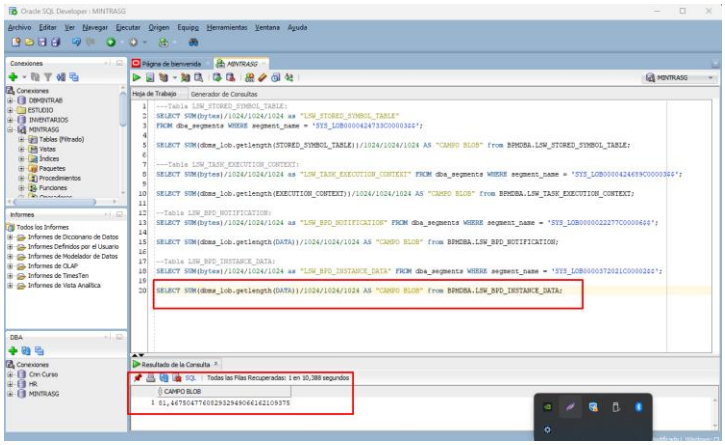


Ilustración 65 validación Tablas DDBB

- **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.

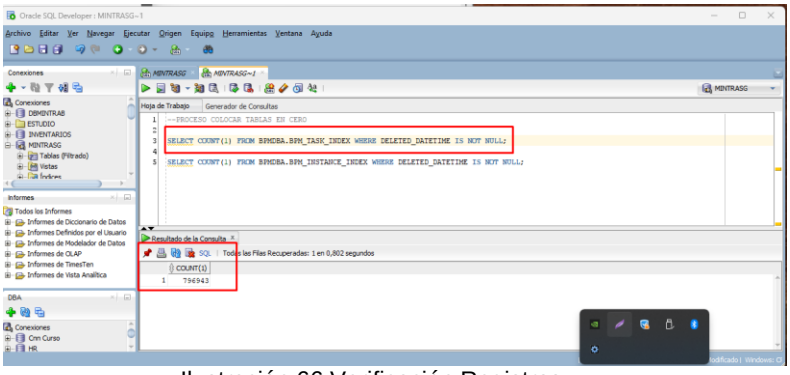


Ilustración 66 Verificación Registros

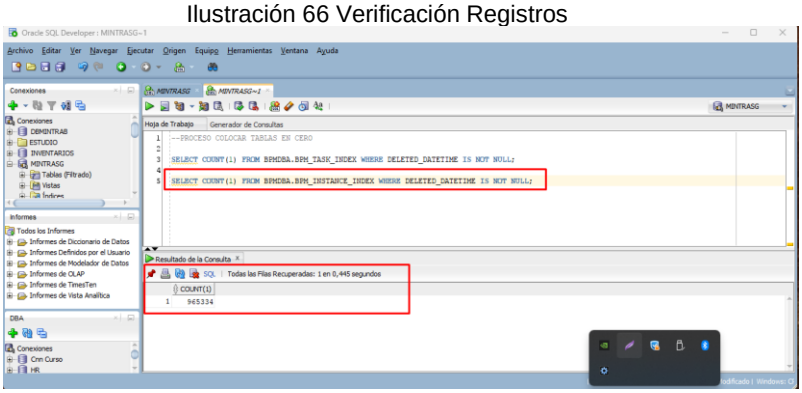


Ilustración 67 Verificación Registros

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

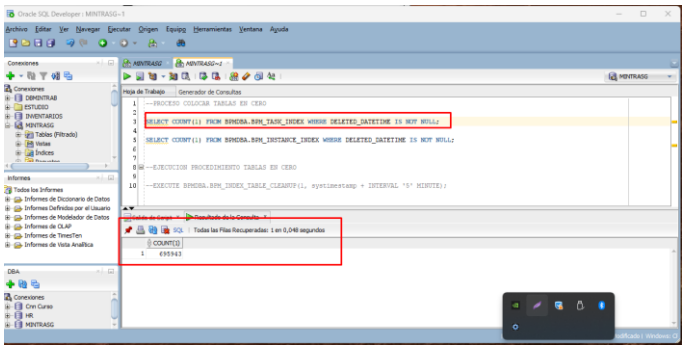


Ilustración 68 Verificación Registros tras ejecución de procesos

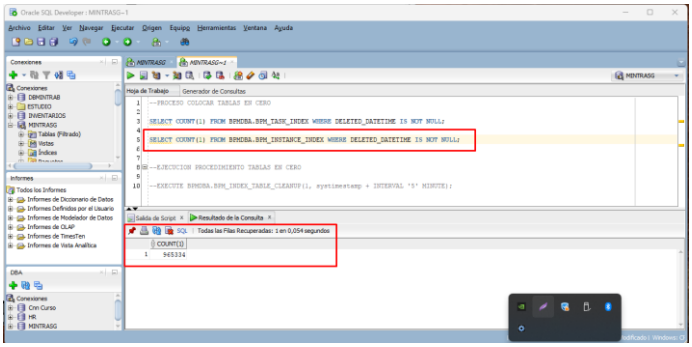


Ilustración 69 Validación de estado de tablas tras ejecución de procesos

- **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.

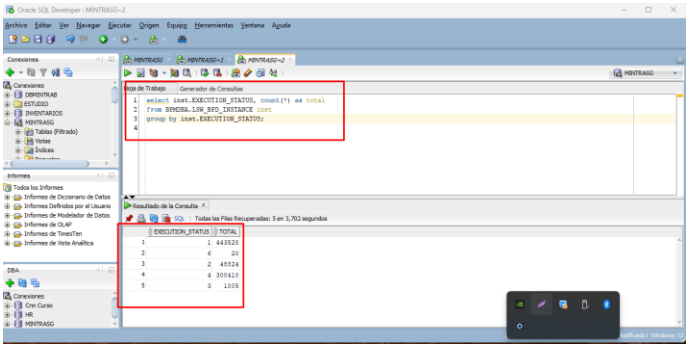


Ilustración 70 Estado de instancias DDDB

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

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

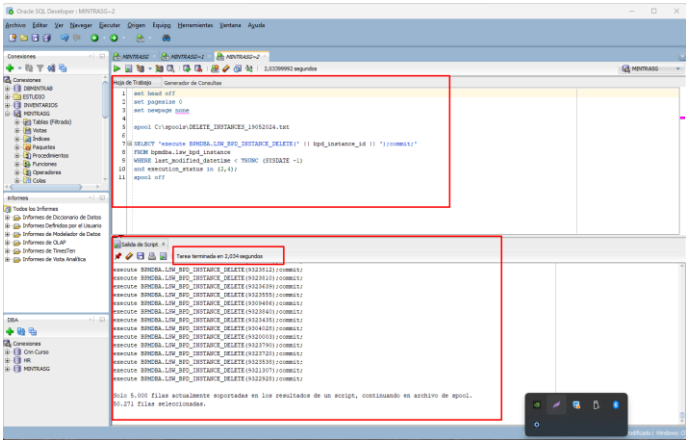


Ilustración 71 Eliminación de instancias

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

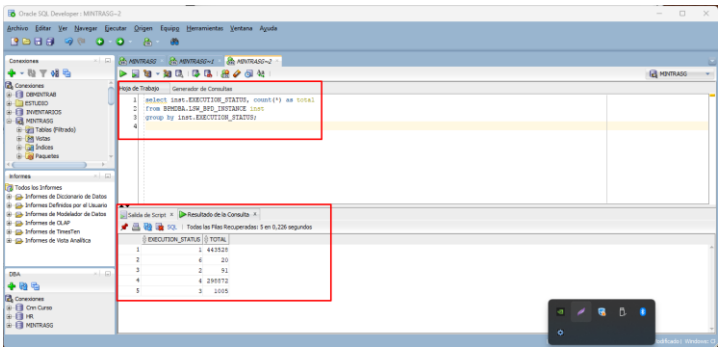


Ilustración 72 Disminución de instancias tras ejecución de proceso

- Estado del servidor antes de la desfragmentación de tablas:

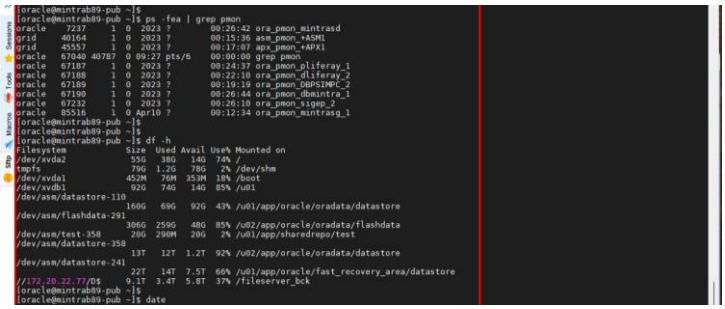


Ilustración 73 Estado del servidor - pre-desfragmentación

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:

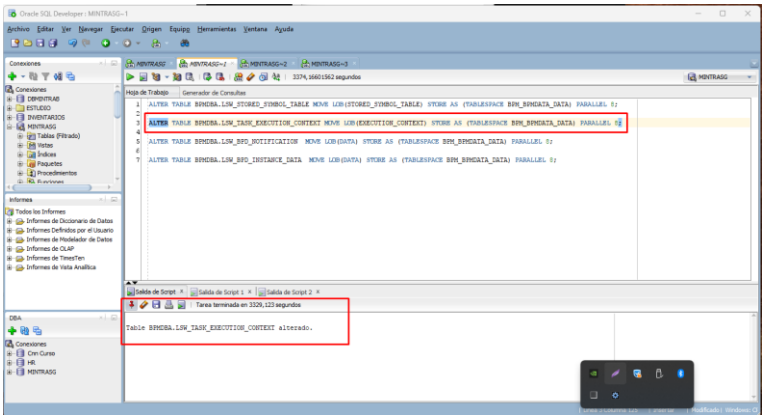


Ilustración 74 Ejecución desfragmentación

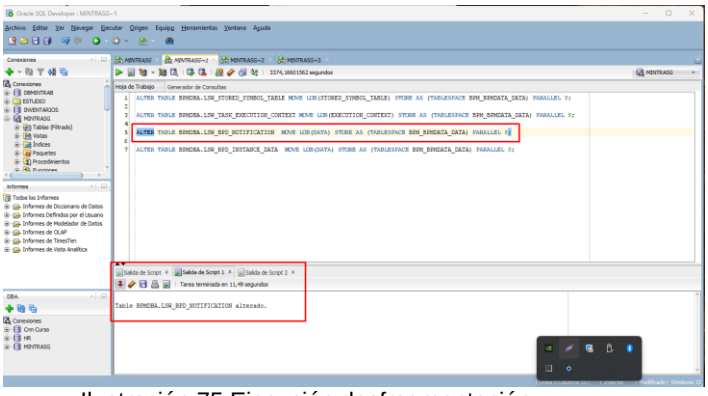


Ilustración 75 Ejecución desfragmentación

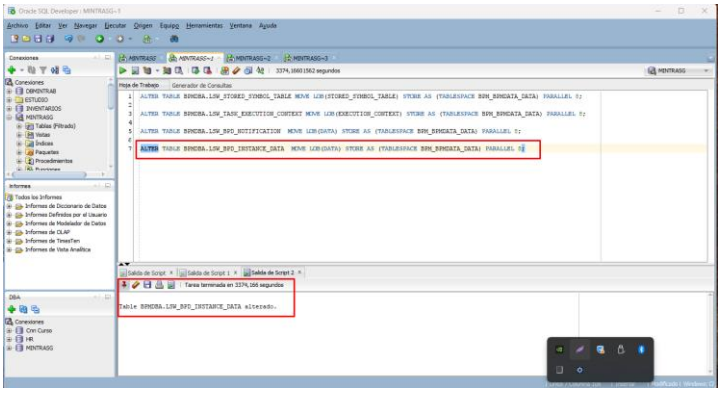


Ilustración 76 Ejecución desfragmentación

- **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.

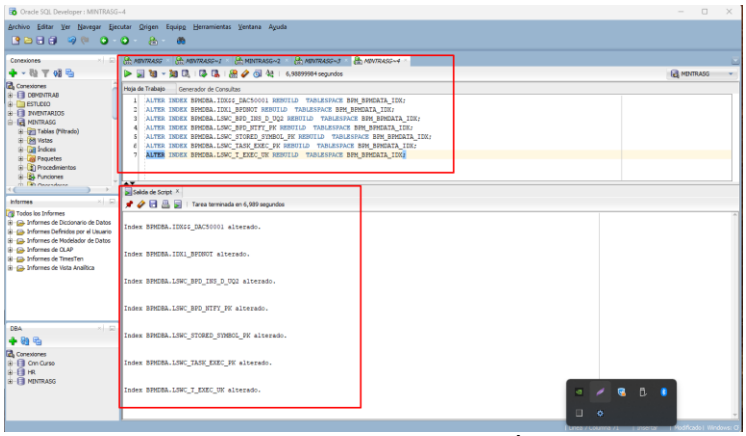


Ilustración 77 Reconstrucción de Índices

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

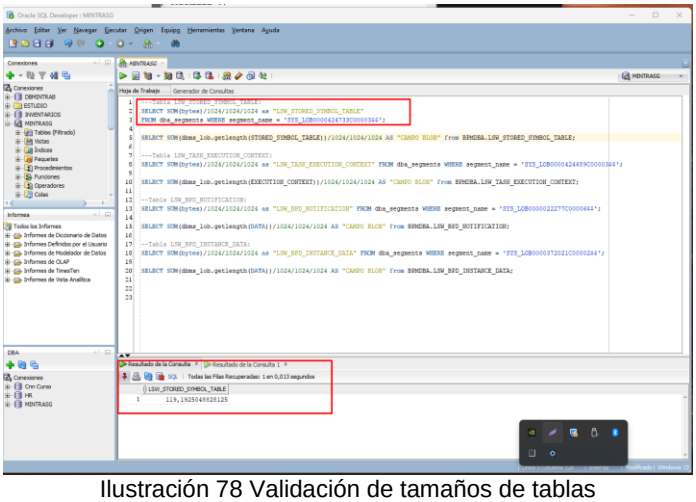


Ilustración 78 Validación de tamaños de tablas

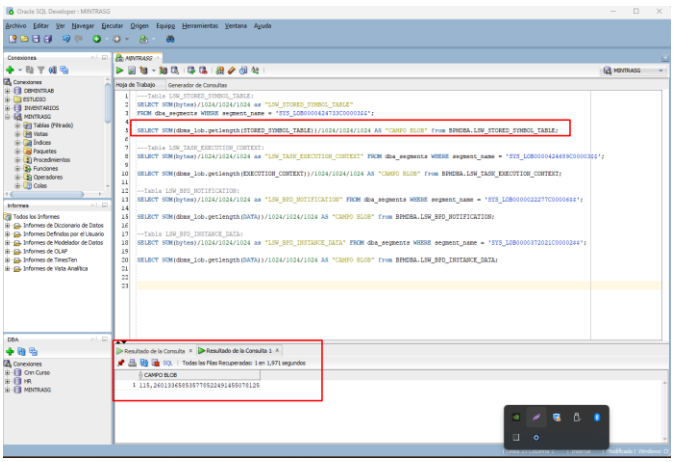


Ilustración 79 Validación de tamaños de tablas

- **Tabla LSW_TASK_EXECUTION_CONTEXT:**

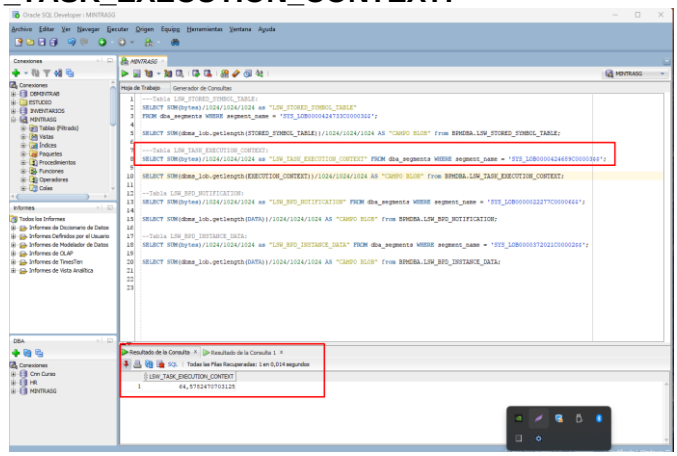


Ilustración 80 Validación de tamaños de tablas

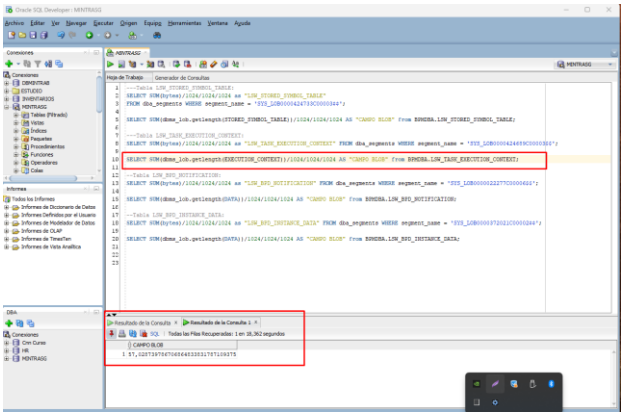


Ilustración 81 Validación de tamaños de tablas

- **Tabla LSW_BPD_NOTIFICATION:**

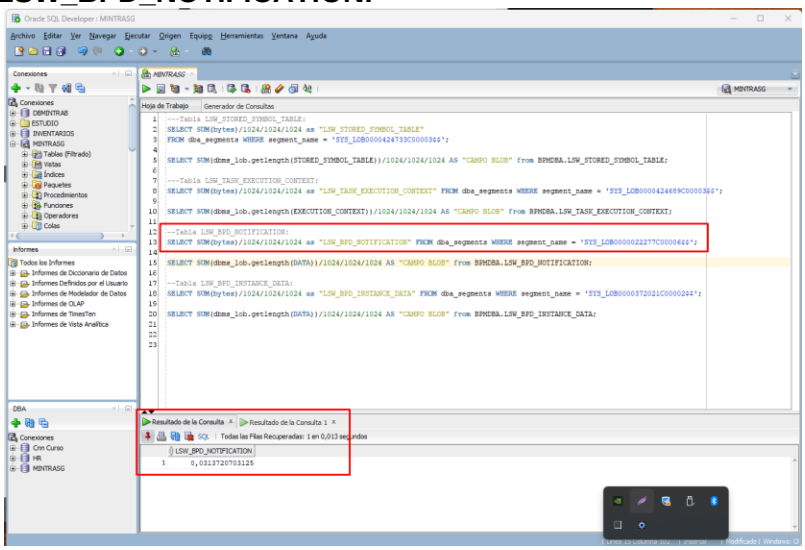


Ilustración 82 Validación de tamaños de tablas

- **Tabla LSW_BPD_INSTANCE_DATA:**

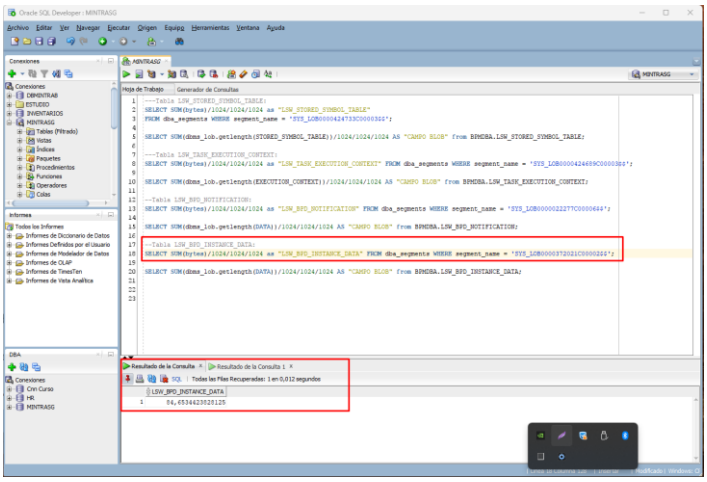


Ilustración 83 Validación de tamaños de tablas

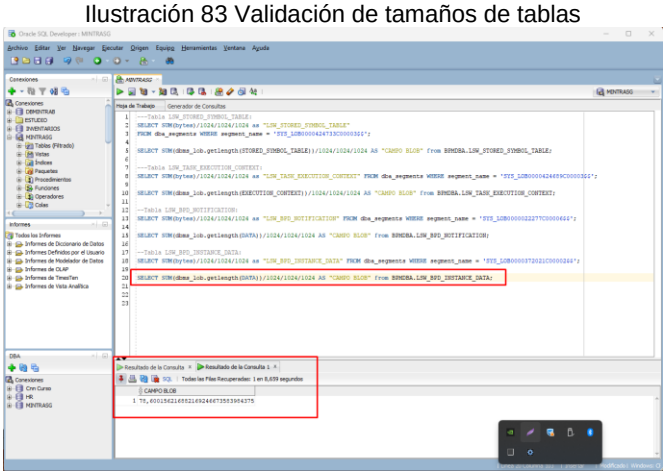


Ilustración 84 Validación de tamaños de tablas

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.

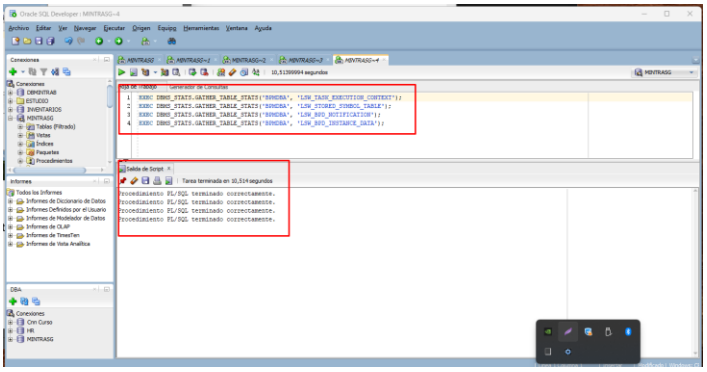


Ilustración 85 Ejecución de estadísticas de validación

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 del último trimestre de 2024 y enero de 2025:

Mes	Suma de Total Instancias
Octubre 2024	128286
Noviembre 2024	116327
Diciembre 2024	93157
Enero 2025	111854
Total acumulado T4 2024 + Ene	**449.624**

Mes	Suma de Total Documentos
Octubre 2024	207050
Noviembre 2024	188193
Diciembre 2024	142068
Enero 2025	149454
Total acumulado T4 2024 + Ene	686765

Mes	Suma de Total radicados
Octubre 2024	70895
Noviembre 2024	63756
Diciembre 2024	50836
Enero 2025	59197
Total acumulado T4 2024 + Ene	244684

Tabla 52 Instancias, documentos & radicados

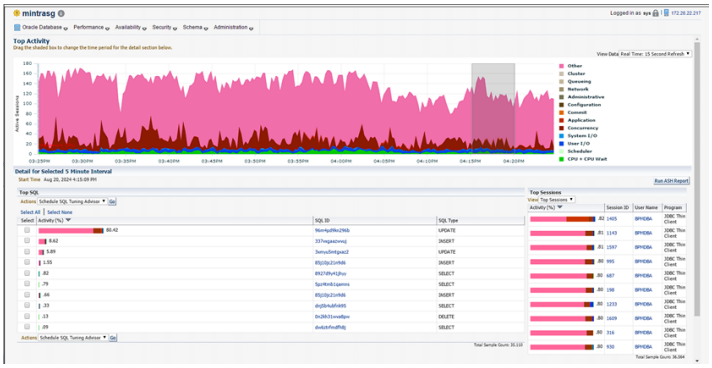


Ilustración 86 Antes del Mantenimiento.

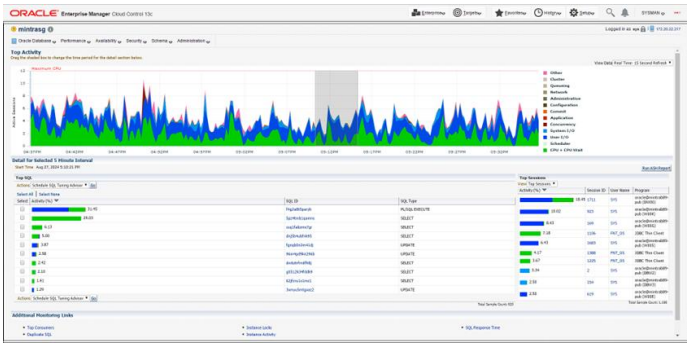


Ilustración 87 Después del Mantenimiento.

Acciones adicionales sobre el Gestor

- A nivel de la plataforma de IBM BPM se eliminaron 350.000 Instancias de proceso que no se había terminado.
- se limpiaron 120.000 documentos temporales sobre el servidor de Integraciones.
- Se limpiaron cache de los servidores que componen la plataforma Gestor Documental
- Se realiza la configuración de los DataSource, configurando tiempos de espera y número de conexiones hacia la Base de Datos.
- Se terminaron los Batch de Datacap con estado HOLD.

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 53 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

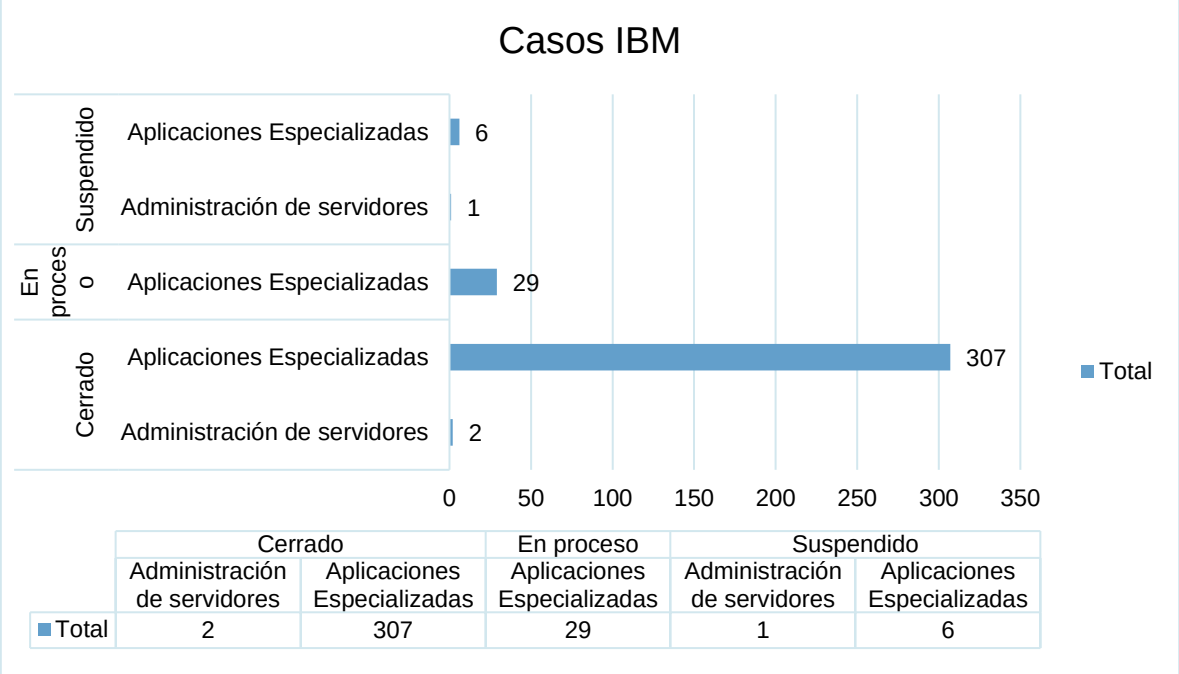
Ilustración 88 Distribución de licencias Oracle

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

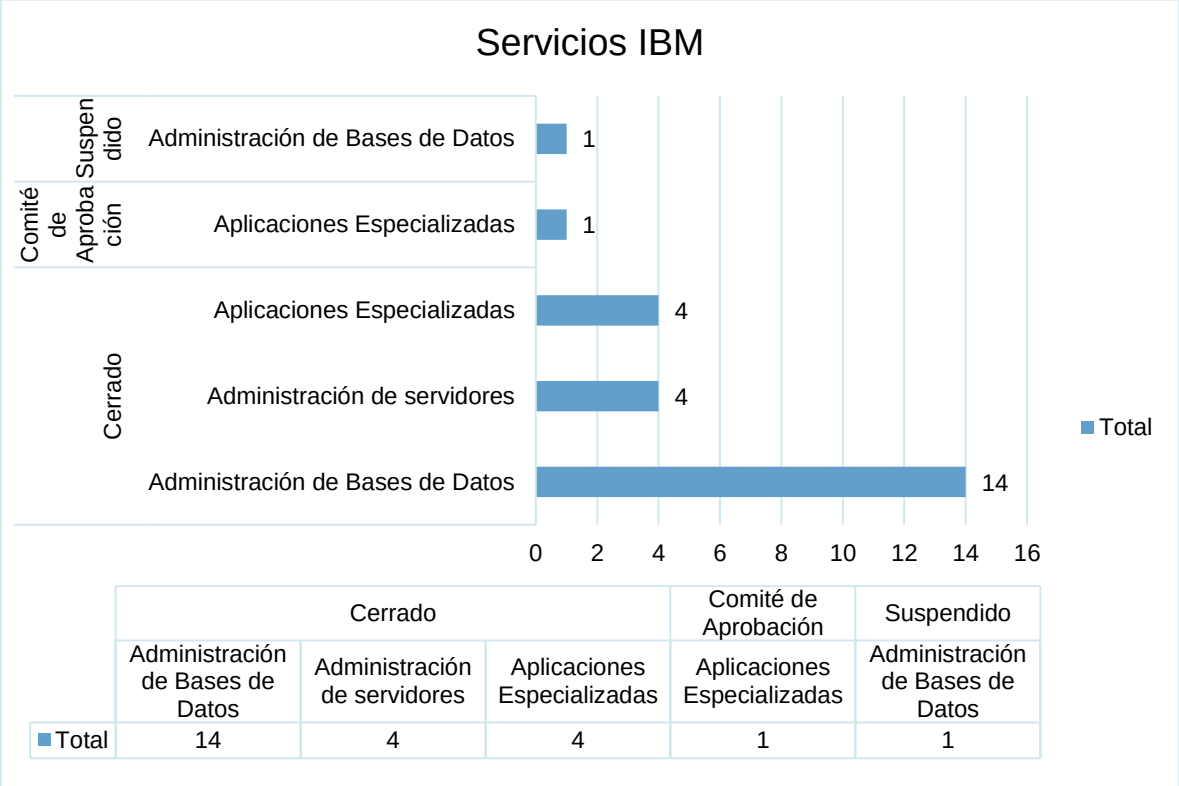
Ilustración 89 Licencias ambientes

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.



	Cerrado		En proceso	Suspendido	
	Administración de servidores	Aplicaciones Especializadas	Aplicaciones Especializadas	Administración de servidores	Aplicaciones Especializadas
Total	2	307	29	1	6

Ilustración 90 Estado final casos GD



	Cerrado			Comité de Aprobación	Suspendido
	Administración de Bases de Datos	Administración de servidores	Aplicaciones Especializadas	Aplicaciones Especializadas	Administración de Bases de Datos
Total	14	4	4	1	1

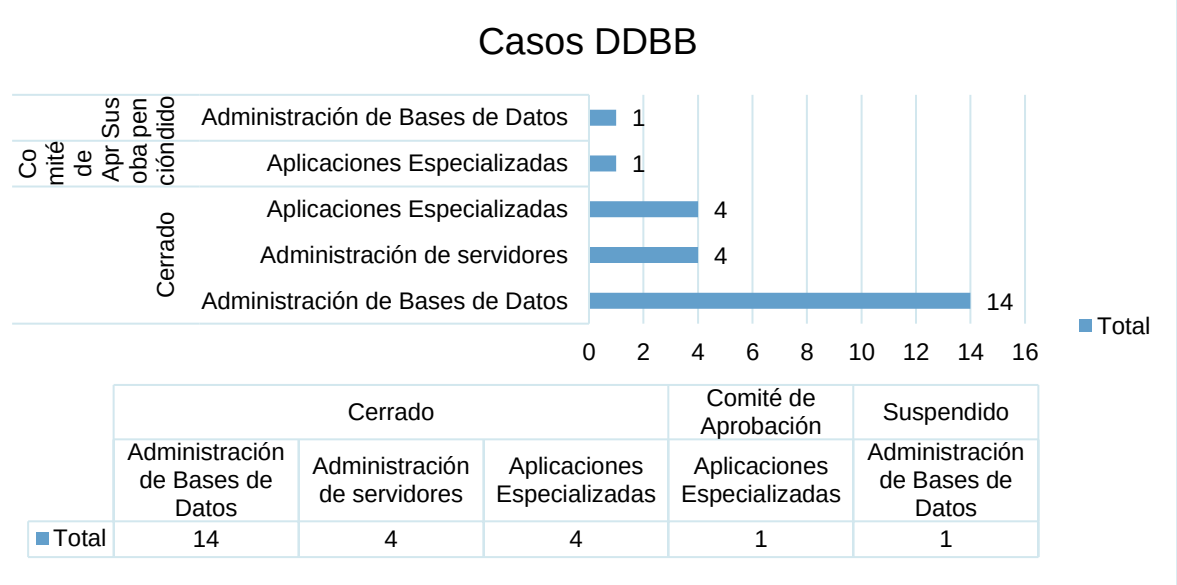
- **Estado de las Bases de Datos**

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.



	Cerrado			Comité de Aprobación	Suspendido
	Administración de Bases de Datos	Administración de servidores	Aplicaciones Especializadas	Aplicaciones Especializadas	Administración de Bases de Datos
Total	14	4	4	1	1

Ilustración 91 casos DDBB

A continuación, se relacionan los casos gestionados y los cambios realizados durante enero de 2025:

- **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 los mismos:

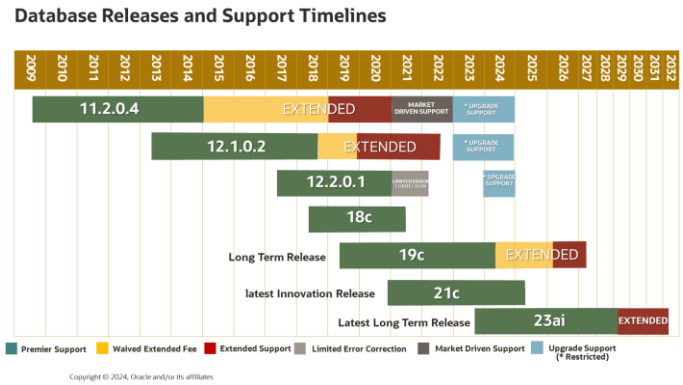


Ilustración *92* Estado Bases de Datos

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 54 Apps & DDBB Oracle

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

Es importante mencionar que, ante un escenario de virtualización, las recomendaciones de fabrica a nivel de asignación de recursos/capacidades están asociadas a las capacidades de la infraestructura que ofrece como fabricante, es decir, las capacidades de un ODA X-10 HA suelen ser las recomendadas para cubrir un escenario de alta disponibilidad y de crecimiento de servicios. El crecimiento de las capacidades está directamente relacionado con el crecimiento de los componentes Oracle/DDBB de la propia entidad.

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

INST_NAME	IP	SERVER_NAME	AMBIENTE	Version_Motor	S.O	MEMORIA GB	CPU	STORAGE ASIG GB	STORAGE USED GB	STORAGE FREE GB
mintrasg_1	172.20.22.217	mintrab89-pub	PRODUCCION	Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	Oracle Linux 4.9.2-6.2.0.3	40	12	5677	1713	3964
pliferay_1	172.20.22.217	mintrab89-pub	PRODUCCION	Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	Oracle Linux 4.9.2-6.2.0.3	4	2	235	139	95
dbmintra_1	172.20.22.217	mintrab89-pub	PRODUCCION	Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	Oracle Linux 4.9.2-6.2.0.3	8	4	2225	1967	257
DBPSIMPC_2	172.20.22.217	mintrab89-pub	PRODUCCION	Oracle Database 12c Enterprise Edition Release 12.1.0.2.0	Oracle Linux 4.9.2-6.2.0.3	2	2	47	5	42

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

Tabla 55 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**

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 93 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 94 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 95 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 96 Estadísticas Pool compartido

Tamaño base de datos MINSTRASG:

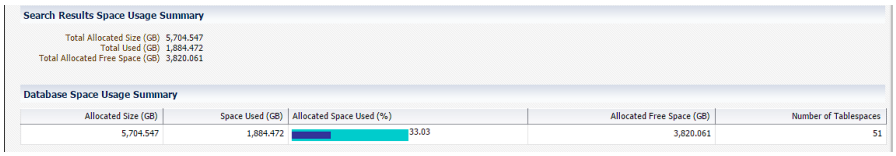


Ilustración 97 Tamaño DDBB

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 98 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

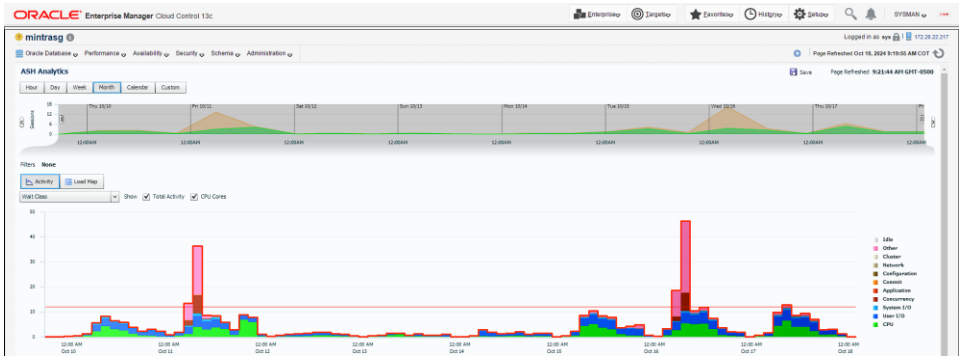


Ilustración 99 Rendimiento DDBB

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 100 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 101 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 102 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 103 Estadística Shared Pool

Tamaño base de datos DBMINTRA:

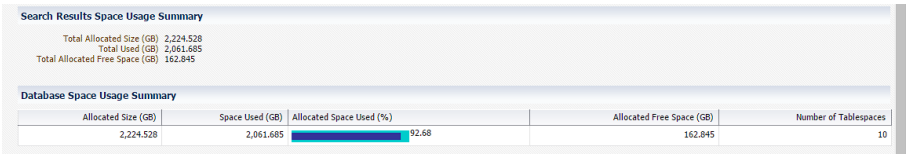


Ilustración 104 Tamaño DDBB DBMINTRA

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 105 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

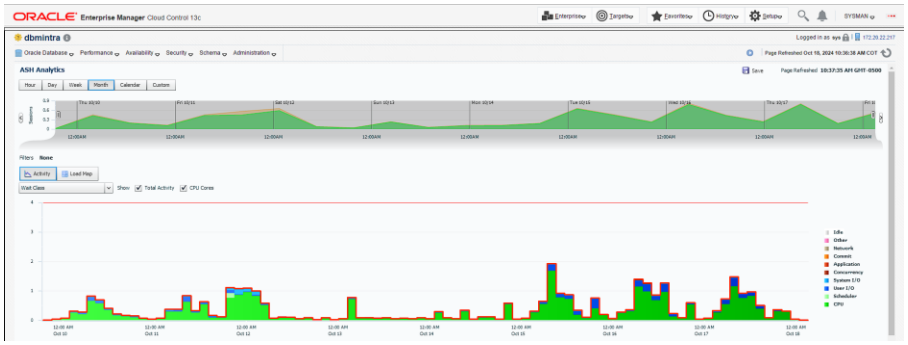


Ilustración 106 Rendimiento DDBB MINTRASG

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 107 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 108 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 109 Estadísticas Memoria

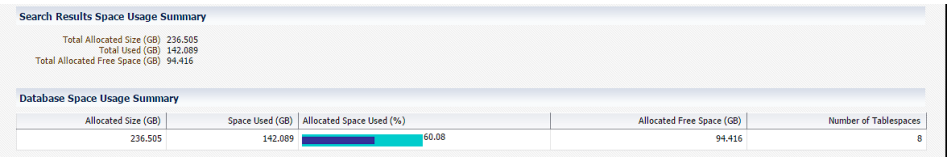
Shared pool, para el caso de la BD PLIFERAY (Portal Web) se observa que los usos de la SGA son idénticos entre los snapshots del reporte.

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 110 Estadísticas Shared Pool

Tamaño base de datos PLIFERAY:



Search Results Space Usage Summary

Total Allocated Size (GB) 236.505
Total Used (GB) 142.089
Total Allocated Free Space (GB) 94.416

Database Space Usage Summary

Allocated Size (GB)	Space Used (GB)	Allocated Space Used (%)	Allocated Free Space (GB)	Number of Tablespaces
236.505	142.089	60.08	94.416	8

Ilustración 111 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 112 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

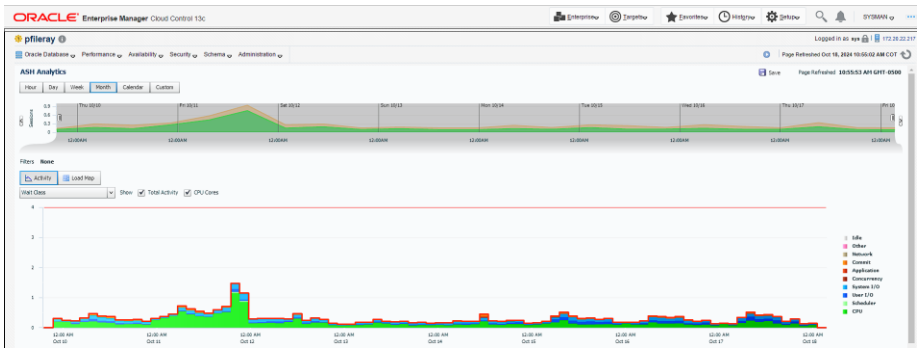


Ilustración 113 Rendimiento DDBB PlifeRay

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 114 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 115 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 116 Estadística Memoria

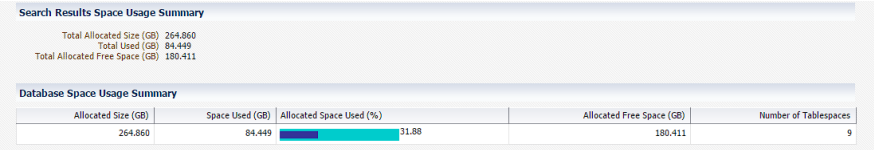
Shared pool, para el caso de la BD SIGEP (Nomina) se observa que los usos de la SGA son idénticos entre los snapshots del reporte.

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 117 Estadística Shared Pool

Tamaño base de datos SIGEP:



Search Results Space Usage Summary

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

Database Space Usage Summary

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

Ilustración 118 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 119 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

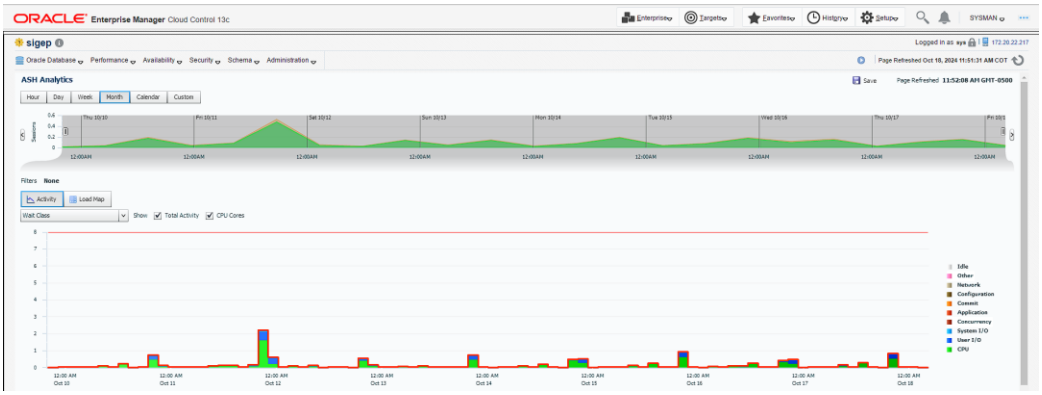


Ilustración 120 Rendimiento DDBB SIGEP

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 121 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 122 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 123 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 124Estadística Shared Pool

Tamaño base de datos DBSIMPC:

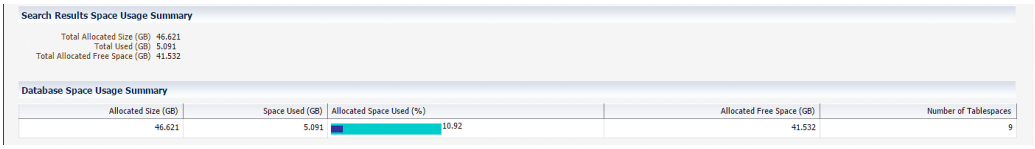


Ilustración 125 Tamaño DDBB SIMPC

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 126 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

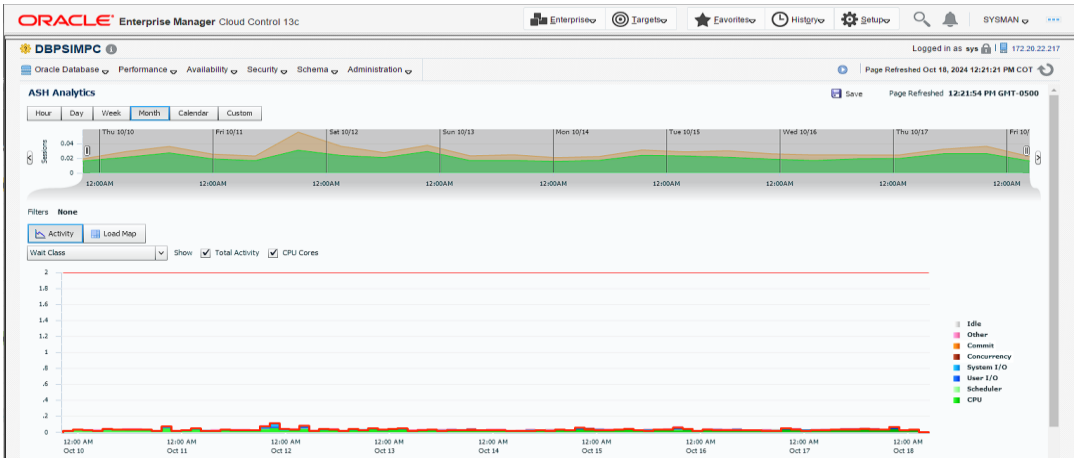


Ilustración 127 Rendimiento DDBB

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 128 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 129 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 130 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 131 Estadística Shared Pool

Tamaño base de datos MINTRASD:

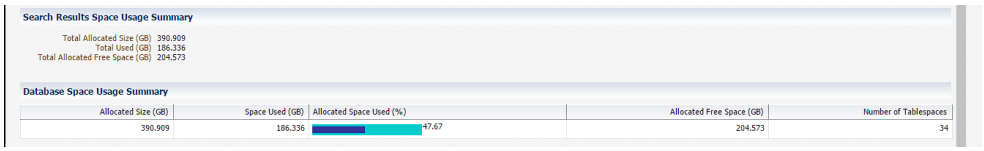


Ilustración 132 Tamaño DDBB MINTRASD

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 133 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

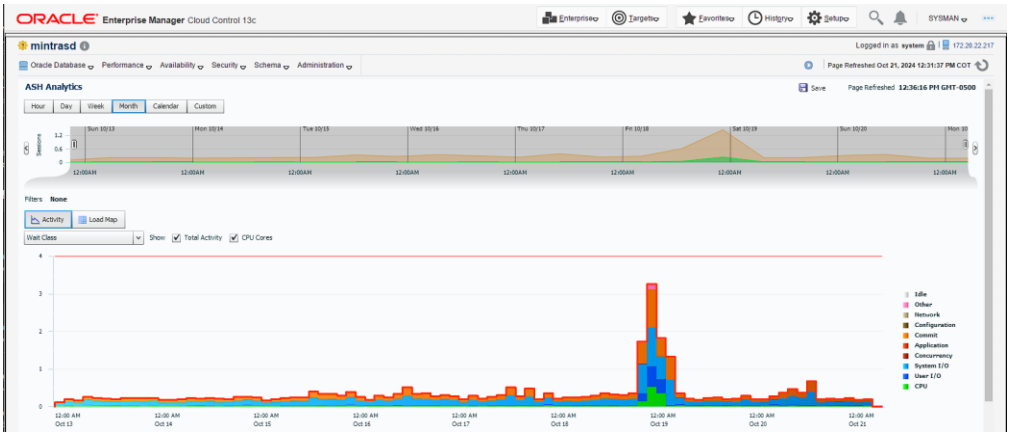


Ilustración 134 Rendimiento MINTRASD

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 135 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 136 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 137 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 138 Estadística Shared Pool

Tamaño base de datos MINTRASD:

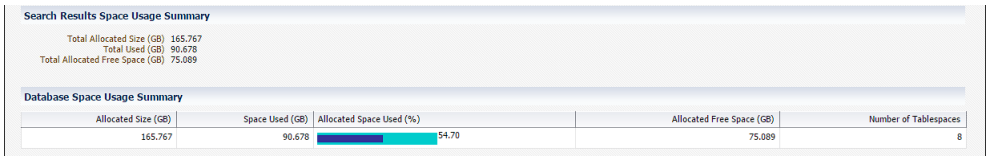


Ilustración 139 Tamaño DDBB

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

Tamaño de esquemas de base de datos:

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

Ilustración 140 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

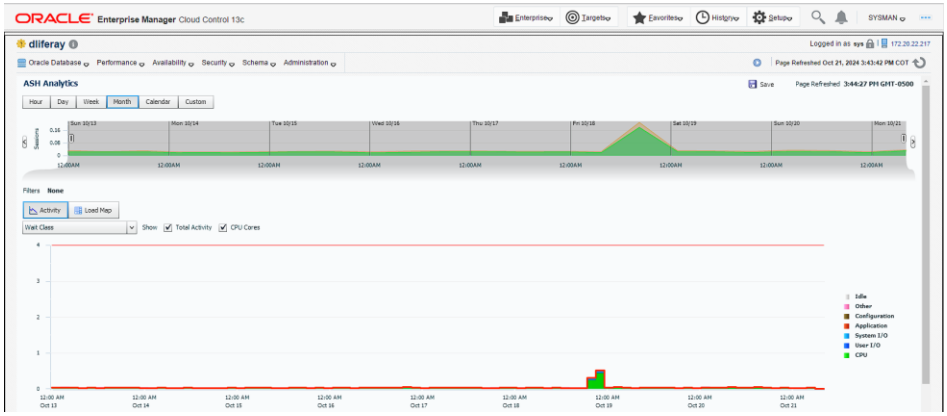


Ilustración 141 Rendimiento DDBB

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 Lucumy, 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 142 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 143 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 144 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 145 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 146 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 147 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

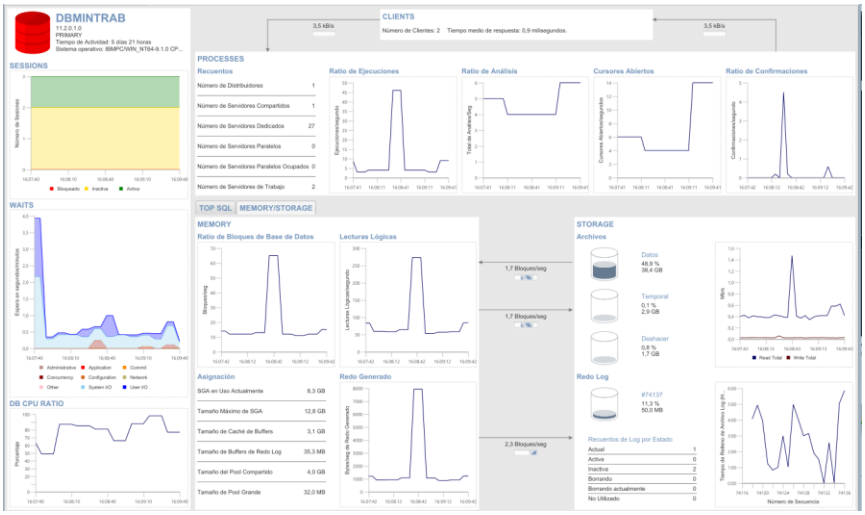


Ilustración 148 Rendimiento DDBB

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 149 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 150 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 151 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 152Estadística 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 153 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

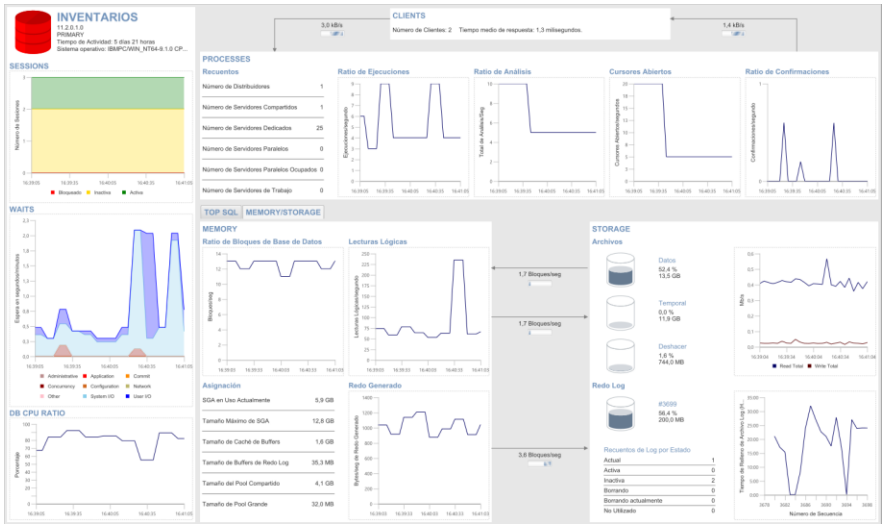


Ilustración 154 Comportamiento DDBB

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 155 Almacenamiento ASM

DISKGROUP DATA:

Disk Groups | Clients | Space History | IO History

Lower Pane: Show Related Items

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

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

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

Ilustración 156 DiskGroup Data

DISKGROUP FLASH:

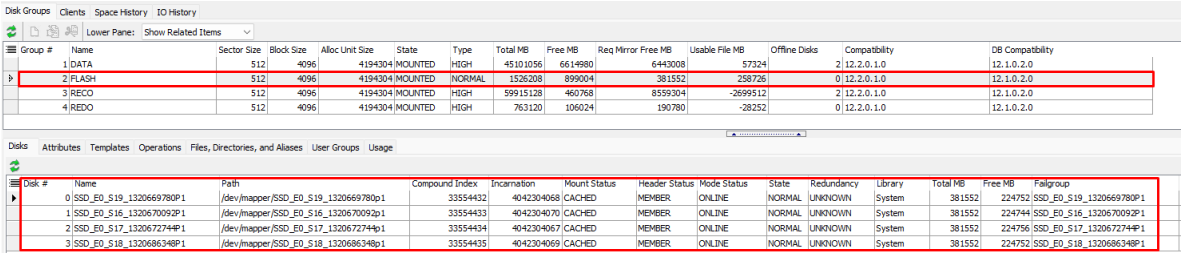


Ilustración 157 DiskGroup Flash

DISKGROUP RECO:

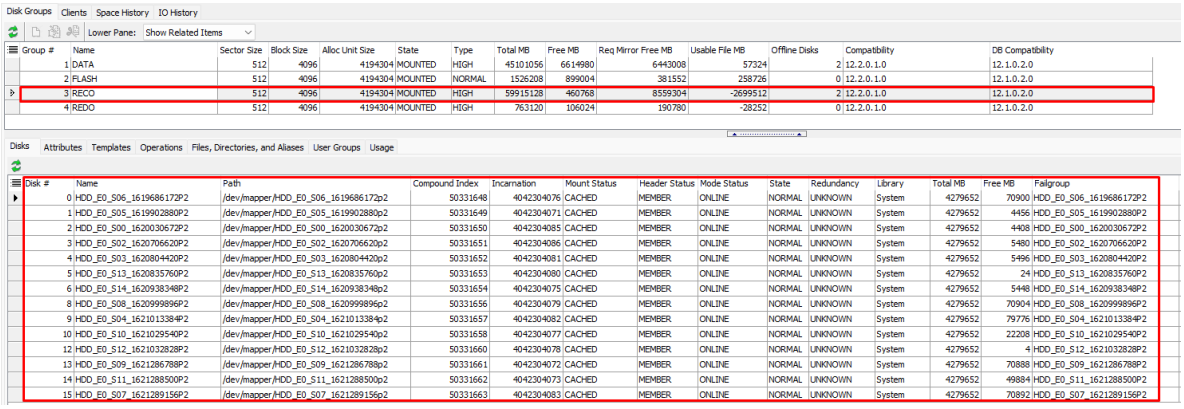


Ilustración 158 DiskGroup Reco

DISKGROUP REDO:

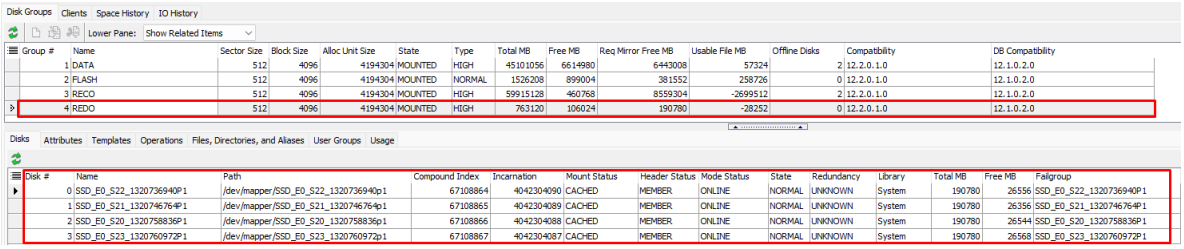


Ilustración 159 DiskGroup Redo

Durante la ventana de mantenimiento realizada los días 16 y 17 de noviembre de 2024, se realizó ampliación de capacidades de los siguientes servidores de gestor documental, que operan con licenciamiento IBM, de acuerdo con lo definido contractualmente la distribución de licenciamiento sobre la capa de aplicación es la siguiente:

- Servidor WANSD: 7 cores asignados actualmente à transición a 8 cores.
- Servidor BAW: 5 Cores asignados actualmente à 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 160 Licenciamiento adicional componente IBM

La adición de estas capacidades se puede observar en la evidencia tomada el sábado 16 de noviembre de 2024:

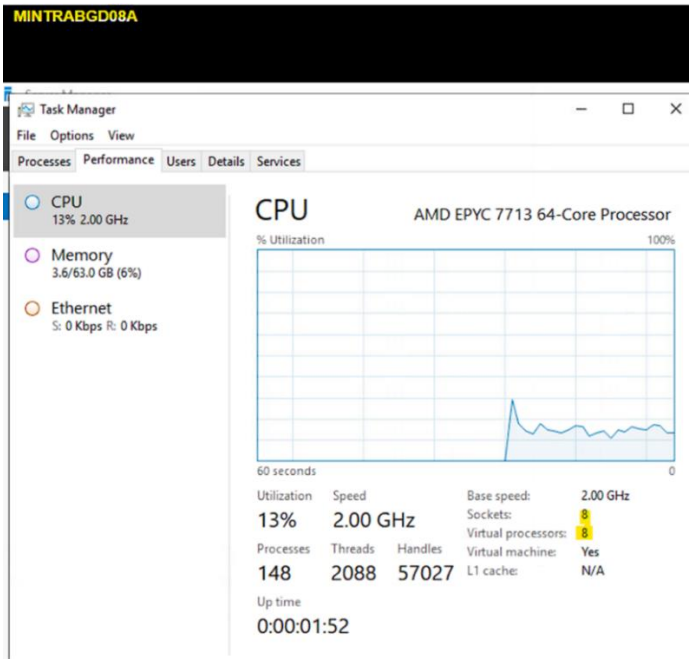


Ilustración 161 Capacidades MINTRABGD08A

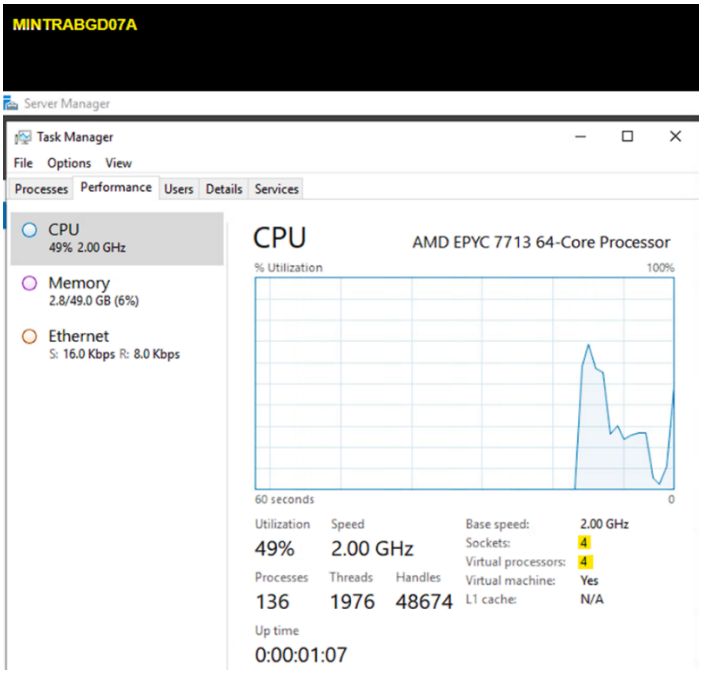


Ilustración 162 Capacidades MINTRABGD07A

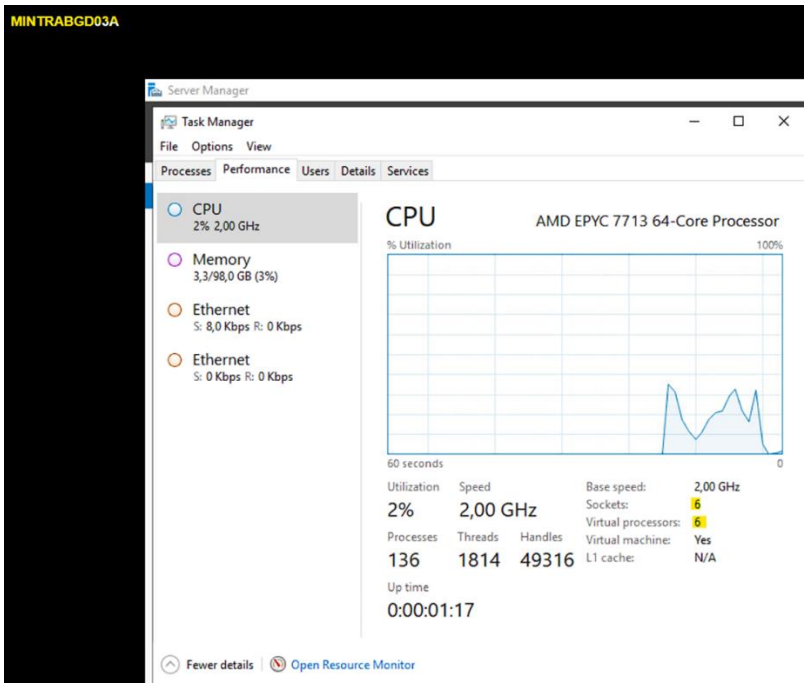


Ilustración 163 Capacidades MINTRABGD03A

A continuación, se muestra el comportamiento de la aplicación la semana previa al cambio, en donde los picos de color rojo hacen referencia a concurrencia de usuario y transaccionalidad:

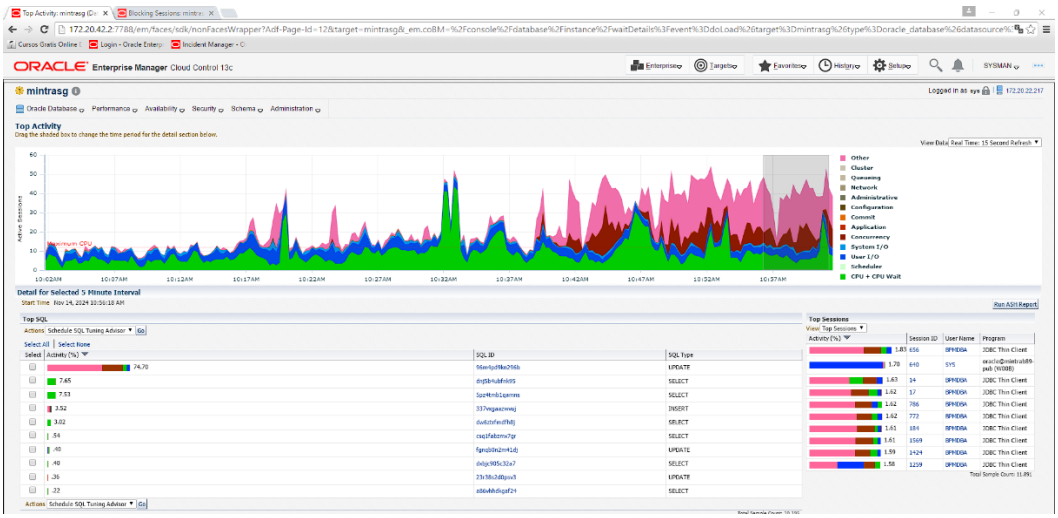


Ilustración 164 Capa de DDBB previo al cambio

Y capa de aplicación con el consumo del 100%

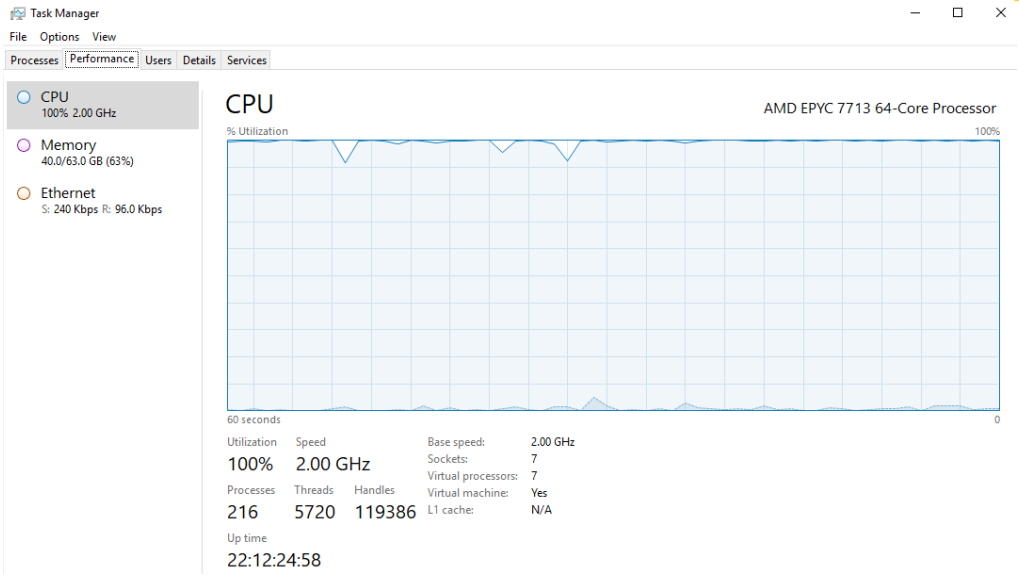


Ilustración 165 Consumos capa de aplicación previo al cambio

Una vez realizado el aumento de estas capacidades, se observa el siguiente comportamiento sobre la capa de base de datos y aplicación de la siguiente forma.
Altos consumos a nivel de servidores de aplicación intervenidos, de la siguiente forma:

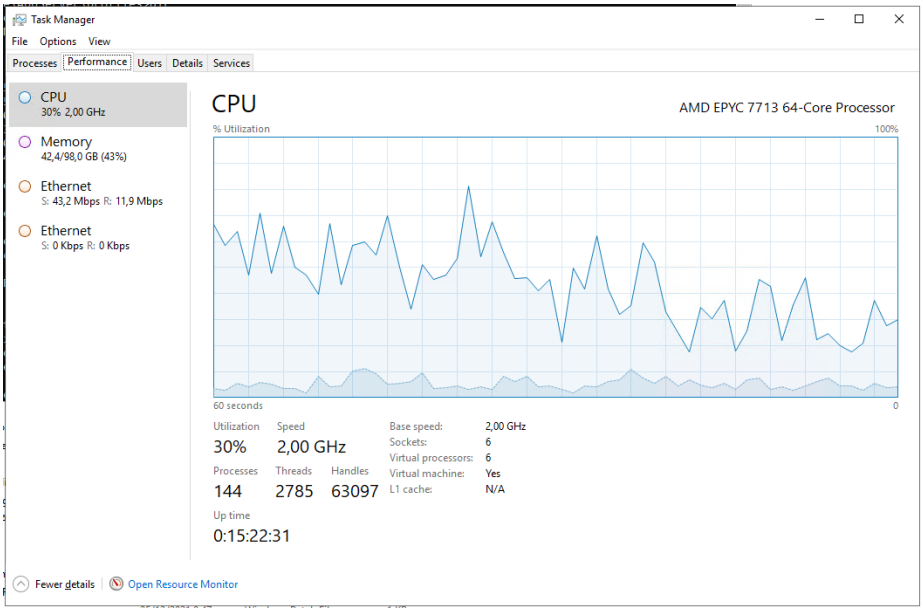


Ilustración 166 Consumos capa de aplicación tras aumento de capacidades

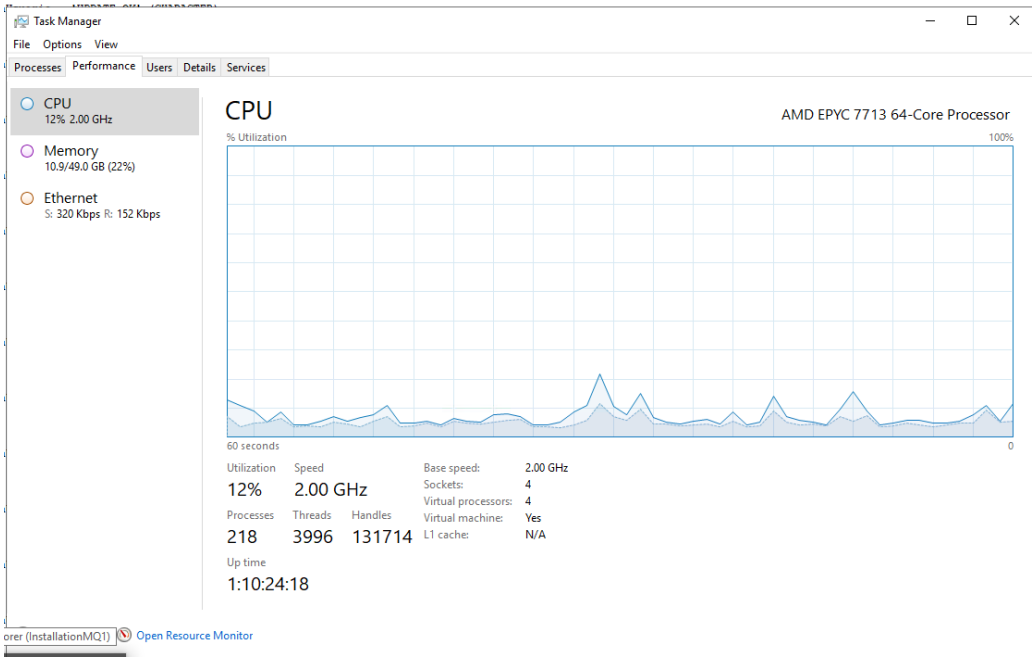


Ilustración 167 Consumos capa de aplicación tras aumento de capacidades

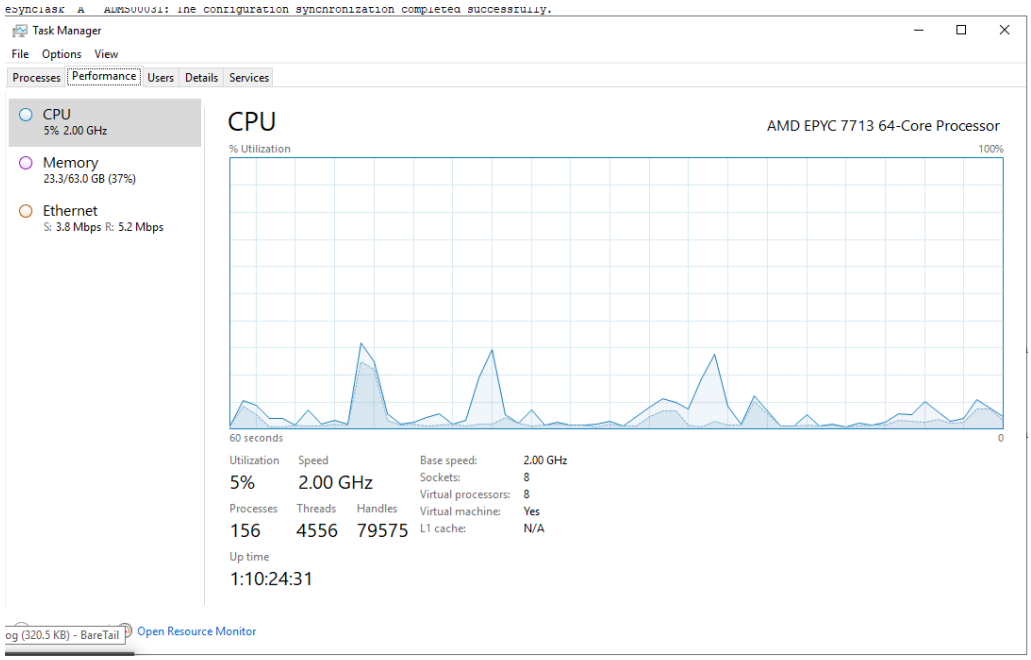


Ilustración 168 Consumos capa de aplicación tras aumento de capacidades

A nivel de base de datos se observa una reducción de la concurrencia y una estabilización de la transaccionalidad recepcionada por la capa de aplicación.

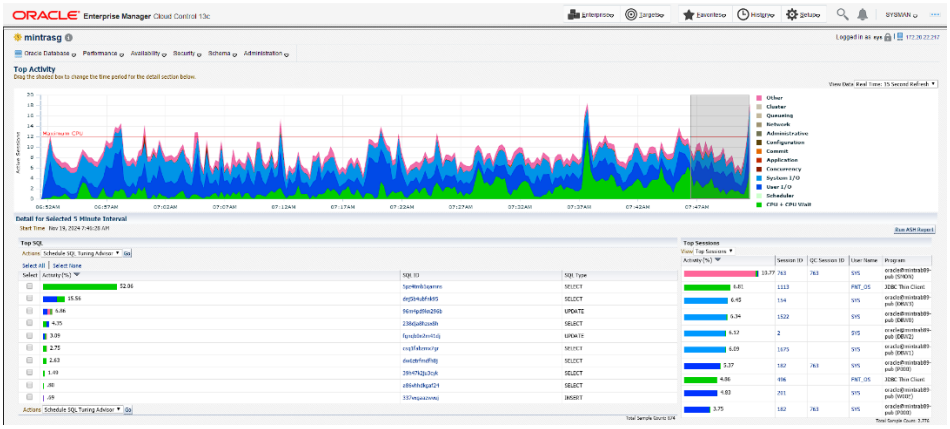


Ilustración 169 Consumos capa de DDBB tras aumento de capacidades en capa de aplicación

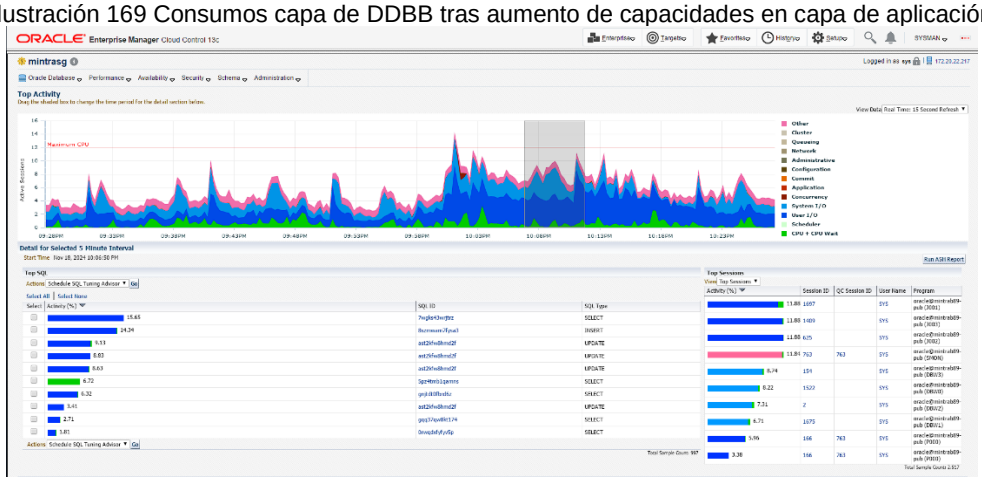


Ilustración 170 Consumos capa de DDBB tras aumento de capacidades en capa de aplicación

Una vez realizado el cambio, se observa una reducción del consumo de capacidades sobre la capa de aplicación y una reducción del tráfico y transaccionalidad hacia la capa de bases de datos Oracle, optimizando los tiempos de respuesta de los servidores y brindando un mejor rendimiento de la aplicación de cara a los usuarios.

Es importante mencionar que este aumento, aunque mejora las capacidades, tiempos de respuesta y rendimiento de la aplicación y capa de base de datos, se requiere realizar los mantenimientos periódicos al sistema de información, ya que esta actividad permite optimizar a nivel de transaccionalidad y liberación de capacidades consumidas y mantener un rendimiento óptimo de la misma, esto debido a la arquitectura con la cual se diseñó, estructuró y entró en producción el sistema de información.

Para estas actividades de migración de DDBB se requirieron de diferentes escenarios y laboratorios realizados por el equipo de trabajo de Servicios Centrales del proyecto, con el fin de determinar un correcto proceder en la definición de prerrequisitos, aprovisionamiento, configuración, pruebas de conectividad, revisión de errores y corrección de estos, así como los ajustes del despliegue y la salida a producción de todo el modelo de clúster en nube privada para el componente de Base de Datos Oracle. Se definieron actividades globales mencionadas con anterioridad en este documento:

- Aprovisionamiento de Contenedores Infraestructura Nube Privada Oracle
- Ajuste de prerrequisitos técnicos Contenedores Infraestructura Nube Privada Oracle
- Instalación Software Oracle & Asignación de almacenamientos Infraestructura Nube Privada Oracle
- Indisponibilidad controlada de capa de aplicación
- Generación Backup completo base de datos Oracle

- Restauración de Base de datos en Infraestructura Nube Privada Oracle
- Pruebas de conectividad capa de aplicación hacía base de datos en Infraestructura Nube Privada Oracle
- Pruebas del servicio Gestor Documental en Infraestructura Nube Privada Oracle
- Configuración, despliegue y salida a producción
-

Las cuales se desglosan en el siguiente detalle técnico:

- Creación servidores virtuales
  - Asignación infraestructura
  - Asignación CPU
  - Asignación memoria
  - Asignación almacenamiento
  - Asignación red
- Ajustar prerrequisitos de servidor virtual DDBB
  - Creación de directorios para instalación
  - Creación de rutas /u01/app para bd
  - Creación de rutas /u02/app para grid
  - Creación de grupos de usuarios
  - Creación de grupos oinstall, dba, oper, backupdba, dgdba, kmdba, asmdba, asmoper,asmadmin
  - Creación de usuarios oracle, grid
  - Instalación de paquetes
  - Instalación de paquetes requeridos por medio de yum install
  - Ajuste de parámetros KERNEL servidor
  - Ajuste de valores optimos para funcionamiento de grid infraestructure, motos de bd 12c r1
  - Configuración de variables de entorno
  - Ajuste bash profile bd oracle
  - Ajuste bash profile bd grid
  - Creación arhivo db_env bd
  - Creación arhivo db_env grid
  - Asignación de direccionamiento ip
  - Asignación direccionamiento ip para 4 interfaces de red (red privada, red pública, red vip, scan)
  - Configuración archivo resolv.conf
  - Configurar servidor DNS para la resolución de nombres.
- Validación de interconectividad servers
  - Pruebas de conexión entre servidores
  - Validación conectividad CSP
- Instalación de software ORACLE
  - Copiado de binarios GRID Infraestructure
  - Proceso de desempaquetado de binarios GRID y alojarlos en /u02/app/grid
  - Instalación de binarios GRID
  - Copiado de binarios Oracle
  - Proceso de desempaquetado de binarios DDBB y alojarlos en /u01/app/oracle
  - Instalación de binarios Oracle
  - Aplicar parche para release 1 Oracle 12c home DDBB
- Asignación de almacenamiento a ASM
  - Solicitar luns a sistemas operativos

- Crear luns con sus respectivas etiquetas de Sistema operativo y particiones.
- Creación de discos ASM a partir de particiones
- Creación de discos ASM para dejarlos en estado candidatos.
- Creación de diskgroups ASM
- Se crean los diskgroups y se asignan los discos candidatos ASM

- Restauración DDBB mintrasg
  - Llevar full backup a servidor virtual vmw
  - Catalogar fullbackup en rman
  - Iniciar restauración de DDBB
  - Restaurar archives logs
  - Abrir base de datos
  - Validación de errores
- Pruebas de conectividad a la DDBB
  - Pruebas de conectividad por clientes
  - Pruebas de conectividad por aplicación
  - Validación de errores
  - Ajustar parámetros
- Pruebas de servicio con aplicación
  - Validar componentes de aplicación a la DDBB
  - Revisar transaccionalidad de servidores de aplicación a la DDBB
  - Validar métricas de procesamiento a la DDBB
  - Validar tiempos de respuesta.
  - Ajuste de parámetros de DDBB y aplicación
- Aprobación de cambio
  - Validación por parte de equipo IBM para poner en producción

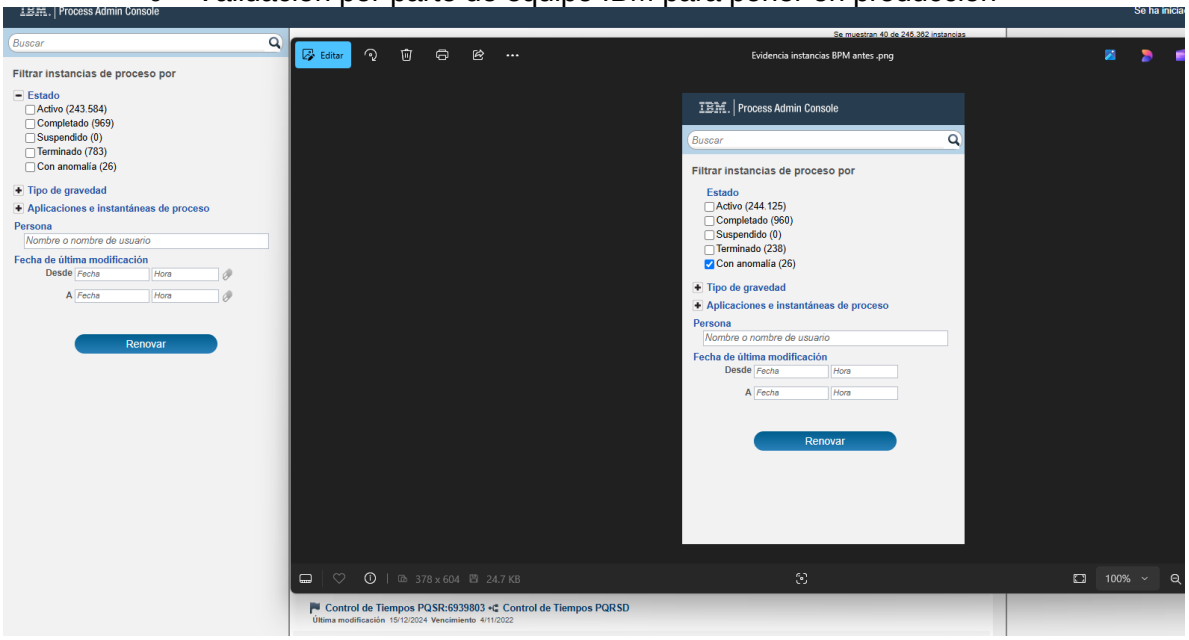


Ilustración 171 Cantidad de instancias Antes de la Migración vs después de la Migración

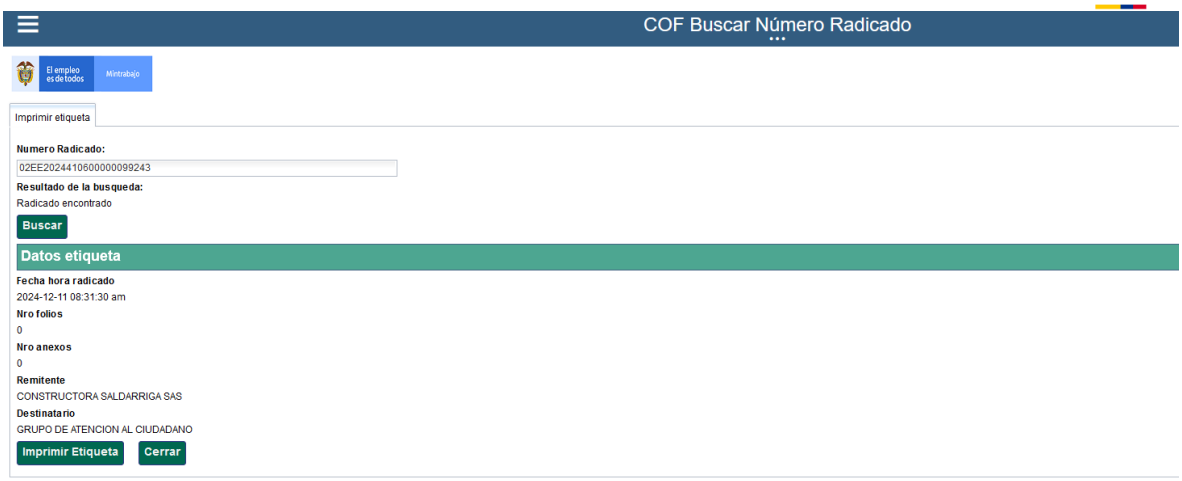


Ilustración 172 Funcionalidad imprimir etiqueta

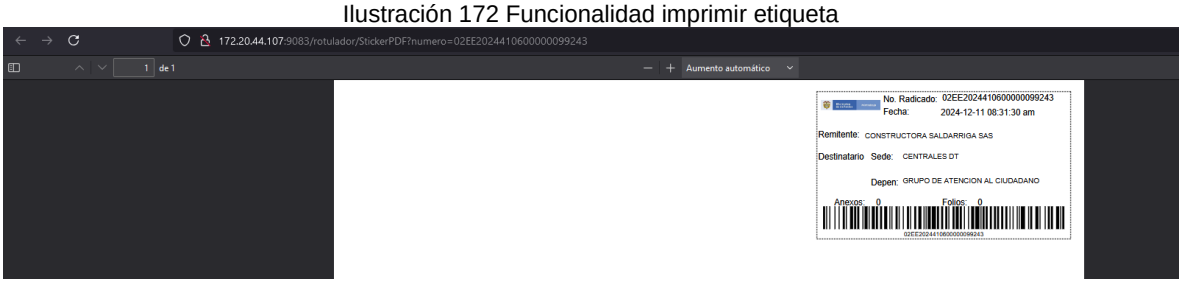


Ilustración 173 Funcionalidad imprimir etiqueta 1

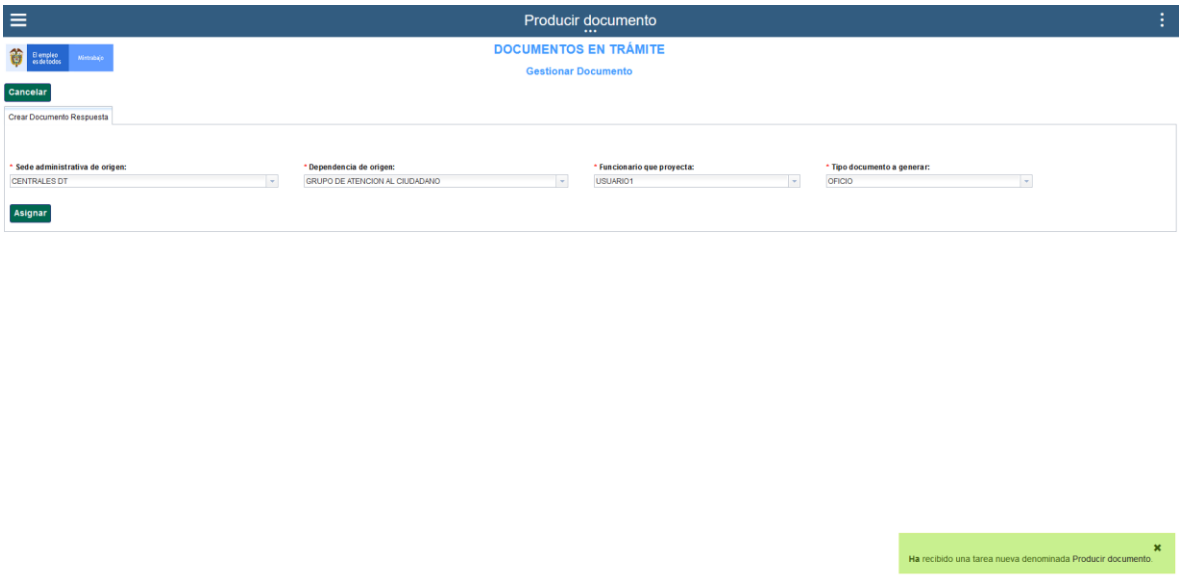


Ilustración 174 Pruebas Radicación



Ilustración 175 Pruebas Radicación 1

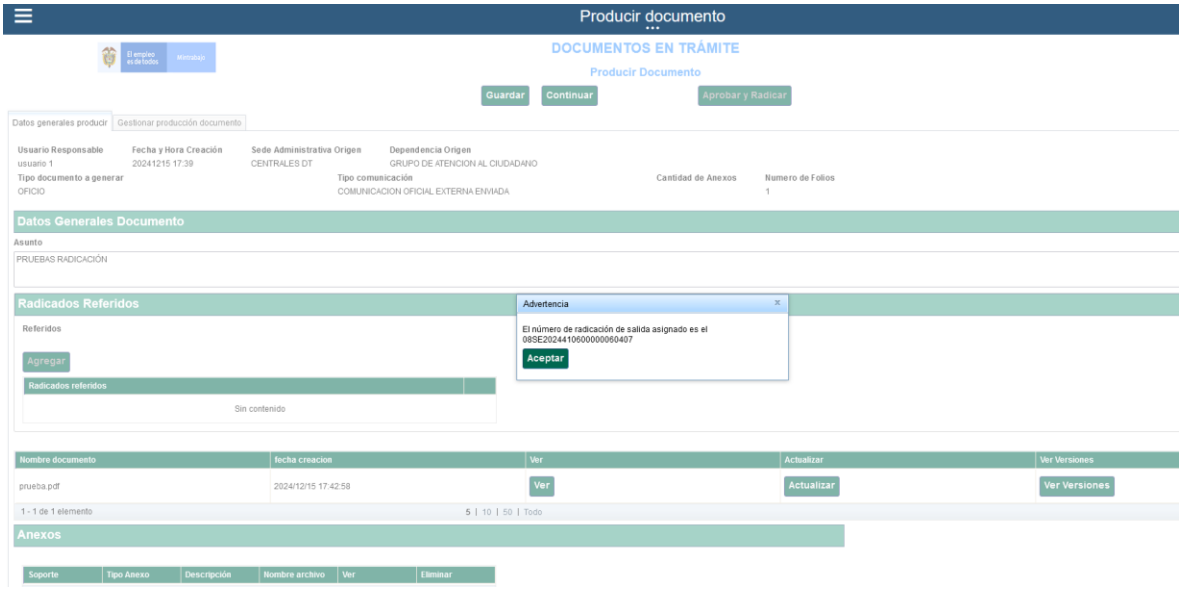


Ilustración 176 Pruebas Radicación 2

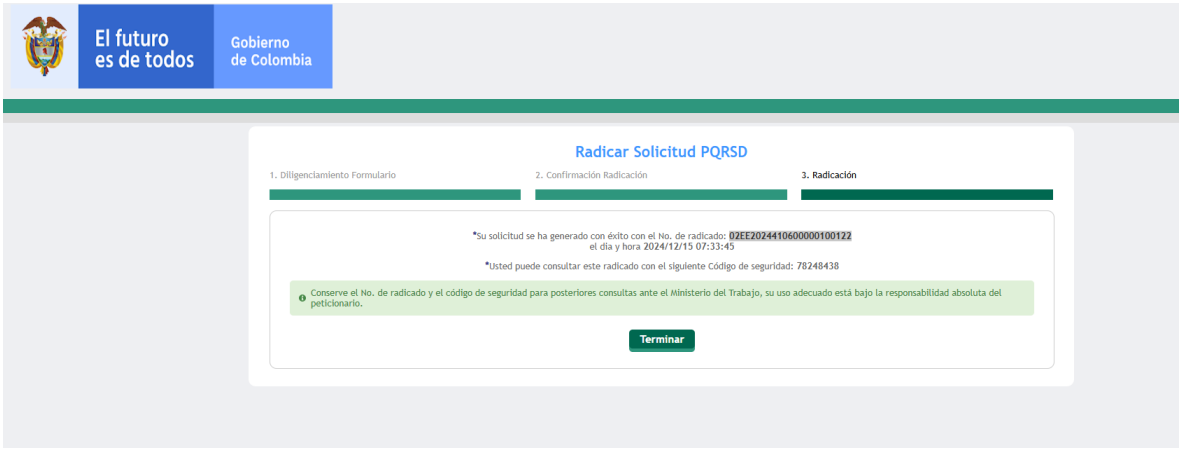


Ilustración 177 Radicación de PQRSD

- **Mejoras en Disponibilidad y Resiliencia**
  - La infraestructura virtualizada con clústeres de alta disponibilidad garantiza un tiempo de actividad cercano al 100%, ya que los nodos del clúster pueden asumir el trabajo en caso de fallo de un nodo.
  - Este enfoque minimiza las interrupciones y asegura la continuidad del negocio, lo que es crucial para sistemas de bases de datos críticas.
- **Optimización del Uso de Recursos**
  - La virtualización permite aprovechar mejor los recursos de hardware, reduciendo la sobreutilización o el desperdicio en la infraestructura.
  - Los recursos pueden asignarse dinámicamente entre máquinas virtuales según las necesidades de carga, lo que mejora el rendimiento general.
- **Escalabilidad**
  - Las soluciones virtualizadas y en clúster facilitan el escalado horizontal (añadiendo más nodos al clúster) y vertical (asignando más recursos a las máquinas virtuales).
  - Esto hace que la infraestructura sea más flexible y adaptable a futuros crecimientos en la demanda.
- **Reducción de Costos Operativos**
  - Aunque la inversión inicial puede ser alta, el modelo virtualizado reduce los costos a largo plazo al disminuir la necesidad de mantenimiento físico y mejorar la eficiencia energética.
  - La automatización y las herramientas de gestión en entornos virtualizados reducen la carga administrativa
- **Modernización y Compatibilidad**
  - La migración a una infraestructura moderna asegura que las bases de datos estén en un entorno compatible con las últimas tecnologías y actualizaciones.
  - También permite integrar fácilmente servicios de nube híbrida o pública, extendiendo la flexibilidad operativa.
- **Complejidad en la Migración**
  - La migración de datos desde infraestructura obsoleta a una nueva requiere planificación cuidadosa para evitar pérdida de datos o tiempos de inactividad prolongados.
  - La configuración del clúster de alta disponibilidad y la virtualización requieren conocimientos especializados para garantizar un diseño óptimo.
- **Mayor Seguridad**
  - La virtualización y la alta disponibilidad incluyen características como replicación de datos, snapshots y tolerancia a fallos que incrementan la protección contra desastres o ciberataques.
  - Se pueden implementar herramientas de respaldo automatizado y recuperación ante desastres (DR).

Tras la migración y ejecución de actividades técnicas se observa un comportamiento balanceado durante el mes de enero de 2025, en donde los procesos y sesiones activas a nivel del performance de las bases de datos. En el siguiente grafico podemos observar cómo oscilan los procesos durante horas pico en los dos nodos de DDBB para la base de datos MINTRASG:

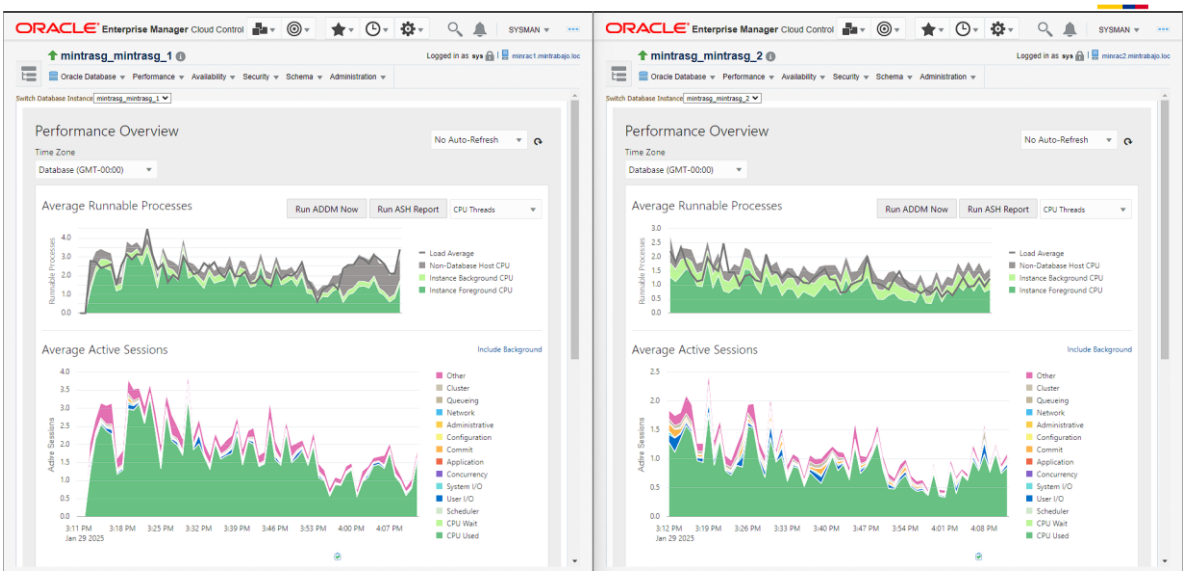


Ilustración 178 Comportamiento MinstrasG Cluster

Observamos una alta concurrencia de sesiones activas y un crecimiento en horas pico en donde la entidad hace uso de la plataforma a sus máximas capacidades sin afectar rendimiento de la misma:

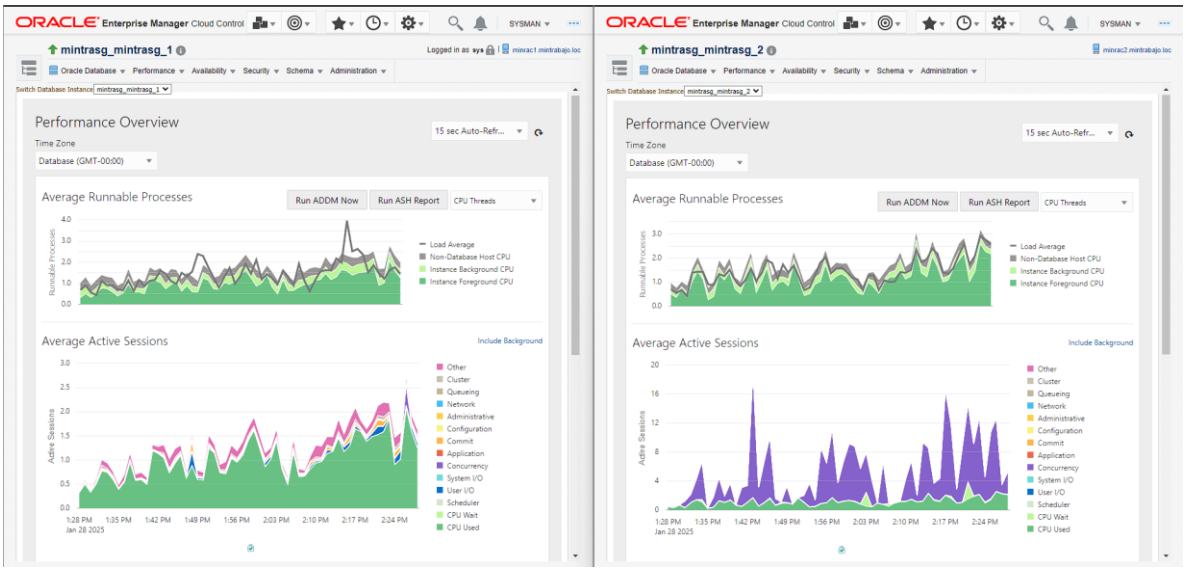
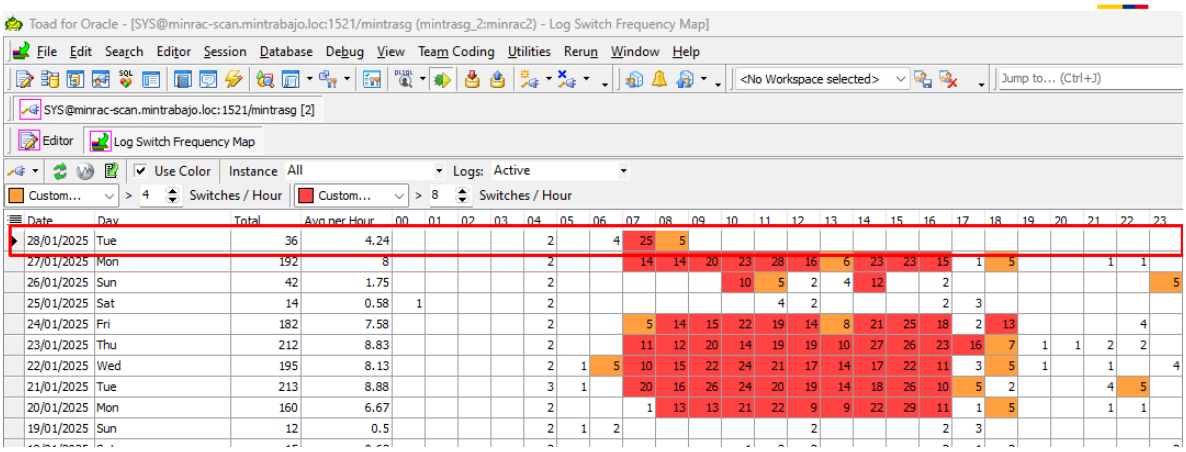


Ilustración 179 Concurrencia de sesiones

Se observa que en algunos casos en específico se presentan alto cambio en los redologos (switcheo) esto es tradujo en altos procesos de escritura en los datafiles de las instancias.



Date	Day	Total	Avg per Hour	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
28/01/2025	Tue	36	4.24					2		4	25	5															
27/01/2025	Mon	192	8					2			14	14	20	23	28	16	6	23	23	15	1	5			1	1	
26/01/2025	Sun	42	1.75					2						10	5	2	4	12		2							5
25/01/2025	Sat	14	0.58	1				2							4	2				2	3						
24/01/2025	Fri	182	7.58					2			5	14	15	22	19	14	8	21	25	18	2	13				4	
23/01/2025	Thu	212	8.83					2			11	12	20	14	19	19	10	27	26	23	16	7	1	1	2	2	
22/01/2025	Wed	195	8.13					2	1	5	10	15	22	24	21	17	14	17	22	11	3	5	1		1		4
21/01/2025	Tue	213	8.88					3	1		20	16	26	24	20	19	14	18	26	10	5	2			4	5	
20/01/2025	Mon	160	6.67					2			1	13	13	21	22	9	9	22	29	11	1	5			1	1	
19/01/2025	Sun	12	0.5					2	1	2						2				2	3						

Ilustración 180 Escritura sobre instancias

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 enero 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

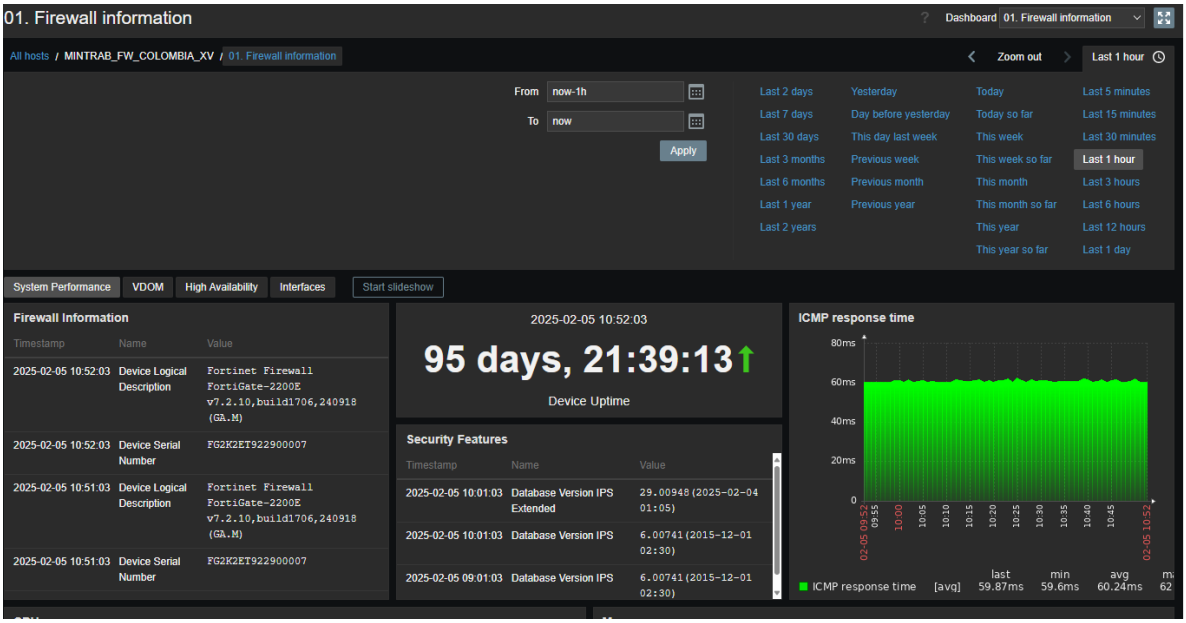


Ilustración181 Disponibilidad firewall

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 enero. 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 9 TB.

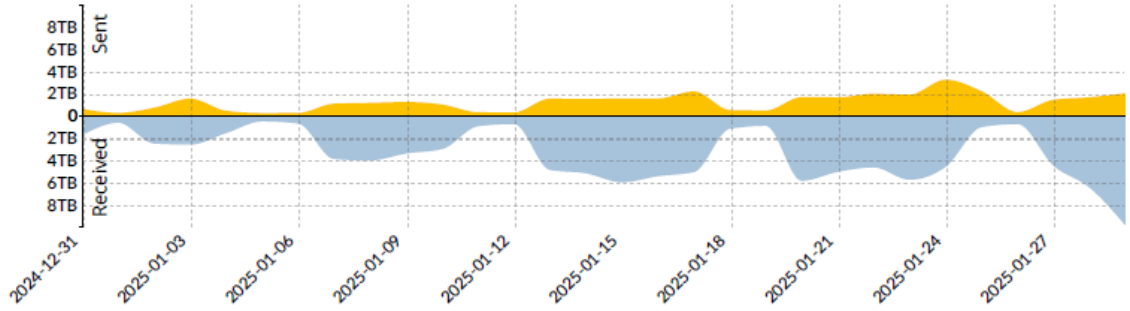


Ilustración182 Comportamiento ancho de banda

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 enero. 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	Adminbck			6.49 TB
2	172.28.28.38			4.95 TB
3	172.20.22.194			3.61 TB
4	172.16.52.43			2.97 TB
5	serviciosgestor			2.70 TB
6	172.20.22.32			2.07 TB
7	172.20.22.251			2.03 TB
8	172.16.60.23			1.65 TB
9	172.25.0.132			1.58 TB
10	172.20.22.179			1.40 TB

Ilustración 183 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 enero. A continuación, se detallan los hallazgos más relevantes:

Top Users by Sessions

#	User (or IP)	Sessions
1	172.25.0.5	258,498,444
2	172.20.22.234	32,890,447
3	FORTINET	24,514,916
4	172.20.22.3	18,173,096
5	172.20.22.32	17,689,939
6	172.20.22.40	15,935,270
7	vulnerabilidadindra	10,789,309
8	172.20.22.228	10,068,078
9	172.50.0.2	6,692,638
10	172.50.0.1	6,692,308

- Durante enero 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 en la nube, como Azure, 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	SMB			37.64 TB
2	HTTPS			37.57 TB
3	SYSLOG			7.01 TB
4	tcp/16713			5.64 TB
5	TCP/1521			4.62 TB
6	Microsoft.Portal			4.60 TB
7	TCP/9200			3.59 TB
8	Microsoft.SharePoint			3.47 TB
9	HTTP			3.03 TB
10	HTTPS.BROWSER			2.65 TB

Ilustración Top184 tráfico de aplicaciones

Observación	Descripción
Mayor Uso de Ancho de Banda	- Microsoft Portal 4.60GB, indicando alta actividad colaborativa.
	- **Microsoft** SharePoint 3.47 TB, reflejando la importancia de servicios de red seguros y transferencia de archivos seguros y transferencia de archivos.

Tabla 56 *Top tráfico de aplicaciones*

Categoría de Aplicaciones por Ancho de banda

En enero, 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**: 4.60 TB
  - **Microsoft SharePoint**: 3.47TB

- **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): 37.64TB 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 enero

Authenticated Logins

#	User	Type	First Used	Total Number of Connections	Total Duration Connected(HH:MM:SS)
1	ygalindo	ssl-tunnel	2025-01-02 09:13:37	103	170:30:02
2	dfdiazd@noc_indra	ssl-tunnel	2024-12-31 00:07:56	96	662:50:55
3	cjimenez	ssl-tunnel	2024-12-31 11:51:06	88	75:37:34
4	jdduque	ssl-tunnel	2024-12-31 14:05:55	78	114:58:39
5	fgomezr	ssl-tunnel	2024-12-31 15:06:48	61	119:24:29
6	ablanco	ssl-tunnel	2024-12-31 07:28:47	61	86:41:06
7	melucumi	ssl-tunnel	2024-12-31 08:32:33	56	59:39:56
8	atobar	ssl-tunnel	2024-12-31 09:48:07	54	41:39:50
9	jcalderonf	ssl-tunnel	2025-01-02 09:31:13	54	31:35:20
10	yguataquira	ssl-tunnel	2025-01-02 12:40:24	52	84:49:26
11	lbricenos	ssl-tunnel	2024-12-31 10:14:37	52	152:47:56
12	lanzola	ssl-tunnel	2024-12-31 13:11:55	50	60:05:57
13	cabuitragoo	ssl-tunnel	2024-12-31 06:51:23	50	238:26:51
14	eserrano	ssl-tunnel	2025-01-07 09:09:26	47	36:35:14
15	yrcifuentes	ssl-tunnel	2024-12-31 09:26:55	47	254:44:52

Ilustración 185 Top 15 Authenticated Logins by VPN Connections

Usuarios con Uso Frecuente:

Usuarios como ygalindo, 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	administrator	ssl-web	1,170
2	admin	ssl-web	455
3	Administrator	ssl-web	401
4	Doctor	ssl-web	292
5	guest	ssl-web	75
6	test	ssl-web	61
7	Admin	ssl-web	58
8	support	ssl-web	57
9	meperez	ssl-web	49
10	it	ssl-web	46

Ilustración 186 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 enero de 2025, se generaron 60 eventos analizados, los cuales fueron limpiados de algún tipo de amenazas

Scan Statistics - Last 4 Weeks

Inputs	*Pending*	*Processing*	Malicious	High Risk	Medium Risk	Low Risk	Clean	Other	Total
Device	*0*	*0*	0	0	0	0	*60*	0	*60*
Adapter	*0*	*0*	0	0	0	0	0	0	*0*
On Demand	*0*	*0*	0	0	0	0	0	0	*0*
Network Share	*0*	*0*	0	0	0	0	0	0	*0*
Sniffer	*0*	*0*	0	0	0	0	0	0	*0*
URL	*0*	*0*	0	0	0	0	0	0	*0*
All Sources	*0*	*0*	0	0	0	0	60	0	*60*

Realtime jobs as of Feb-06 15:35

File Scan - Last 4 Weeks

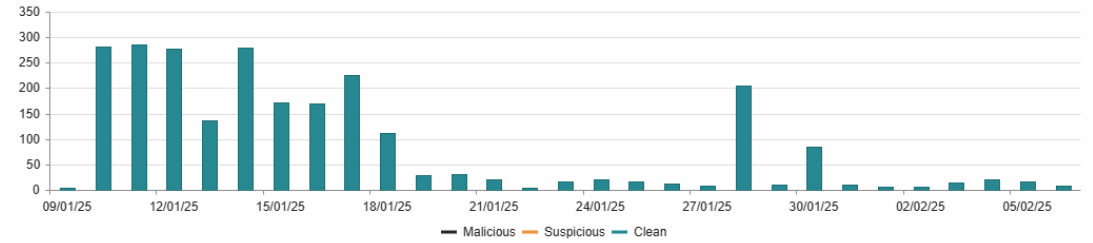


Ilustración 187 estadísticas de escaneo

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

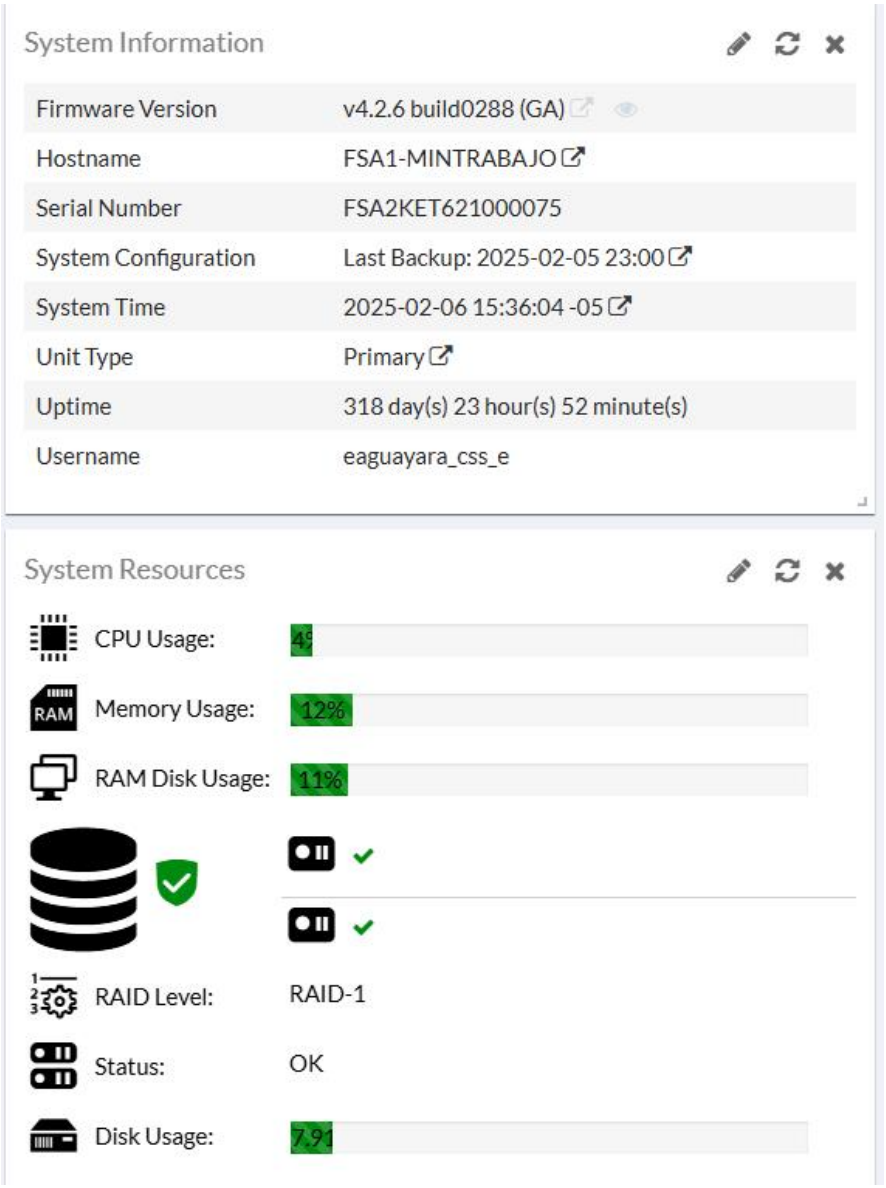


Ilustración 188 performance

Licencia Sandbox

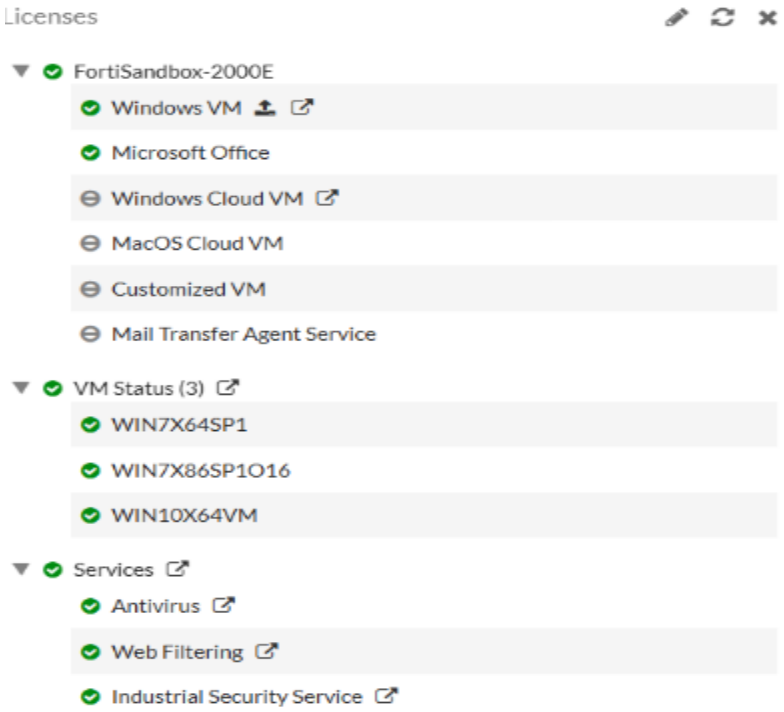


Ilustración 189 Licenciamiento

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

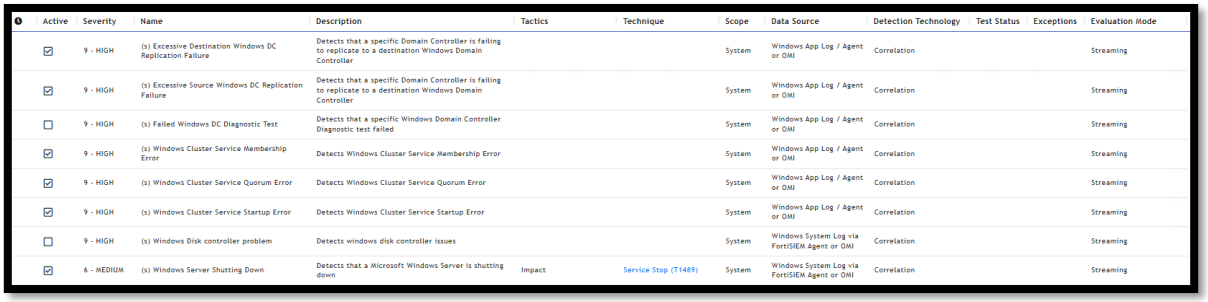
Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☑	9 - HIGH	(s) Server Intf Util Critical	Detects that interface utilization of a network device has reached a critical level (utilization greater than 50% based on 2 successive 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 190 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/OMI	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 191 Disponibilidad

3.1.6.3.3. Seguridad (Security) Autenticación:

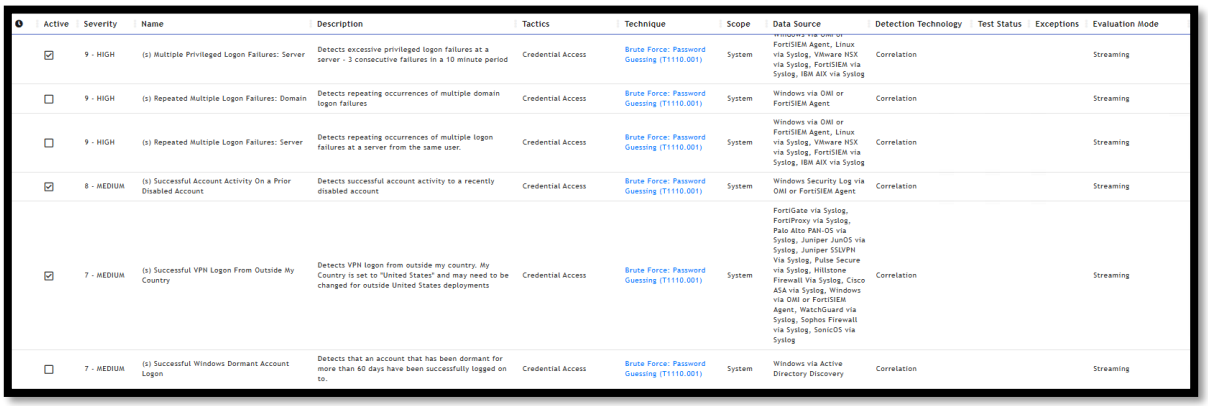
Los casos de uso de seguridad de autenticación en el FortiSIEM se centran en garantizar la integridad y la autenticidad de las credenciales de usuario en todos los dispositivos que tienen instalado el agente. Se muestran los casos Autenticación configurados para el ministerio de trabajo:

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

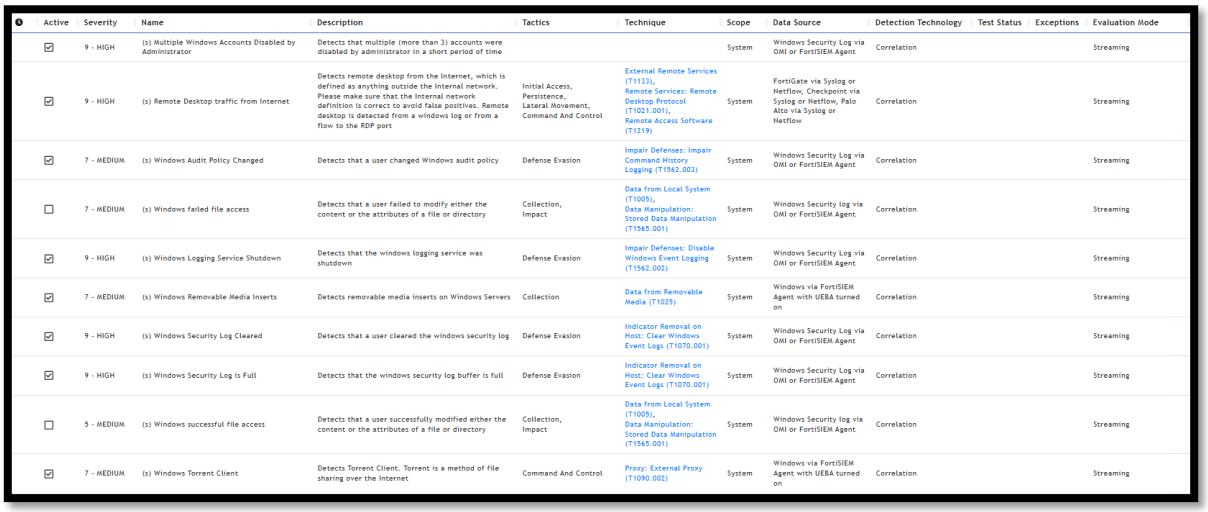


Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Technology	Test Status	Exceptions	Evaluation Mode
☑	9 - HIGH	(s) Multiple Privileged Logon Failures: Server	Detects excessive privileged logon failures at a server - 3 consecutive failures in a 10 minute period	Credential 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 192 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 193 Violación de políticas

3.1.6.3.5. Overview incidentes

Durante el mes de enero, 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:



Ilustración194 Incidentes

La imagen muestra un panel con los principales incidentes de seguridad detectados en el entorno monitoreado. A continuación, un análisis resumido de los eventos críticos identificados:

Violación de política de acceso web (5 incidentes).

Se han detectado accesos de alto volumen a sitios web desde cinco direcciones IP internas.
Esto podría indicar uso indebido de recursos, actividades no autorizadas o incluso tráfico malicioso.

Problemas de monitoreo en FortiSIEM (5 incidentes)

Varias instancias del sistema FortiSIEM están experimentando fallas en la monitorización de relés.
Esto puede impactar la capacidad de detección de amenazas y eventos de seguridad.

Latencia crítica en discos de servidores (2 incidentes)

Dos servidores presentan problemas de latencia en los discos, lo que puede afectar el rendimiento y disponibilidad de servicios críticos.
Es necesario evaluar si hay problemas de sobrecarga o fallos en el hardware de almacenamiento.

Falta de registros desde dispositivos (1 incidente)

Un colector/supervisor no está recibiendo logs de ningún dispositivo.
Esto representa un riesgo ya que podría ocultar actividades maliciosas o anomalías en la red.

Memoria crítica en servidor (1 incidente)

Un servidor muestra un uso crítico de memoria, lo que puede generar interrupciones o fallos en los servicios hospedados.
Se recomienda revisar los procesos en ejecución y la posibilidad de aumentar la capacidad de memoria.

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 enero. Ofrece información valiosa sobre los patrones de disponibilidad de servidores. A continuación, se presentan los hallazgos más relevantes:

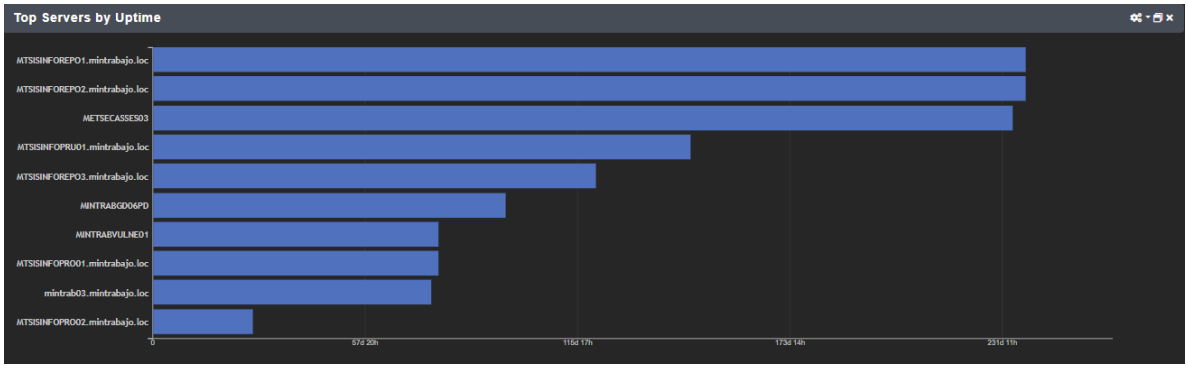


Ilustración Disponibilidad195 de servidores- Seguridad

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 enero, 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 Desempeño196 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 enero 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.

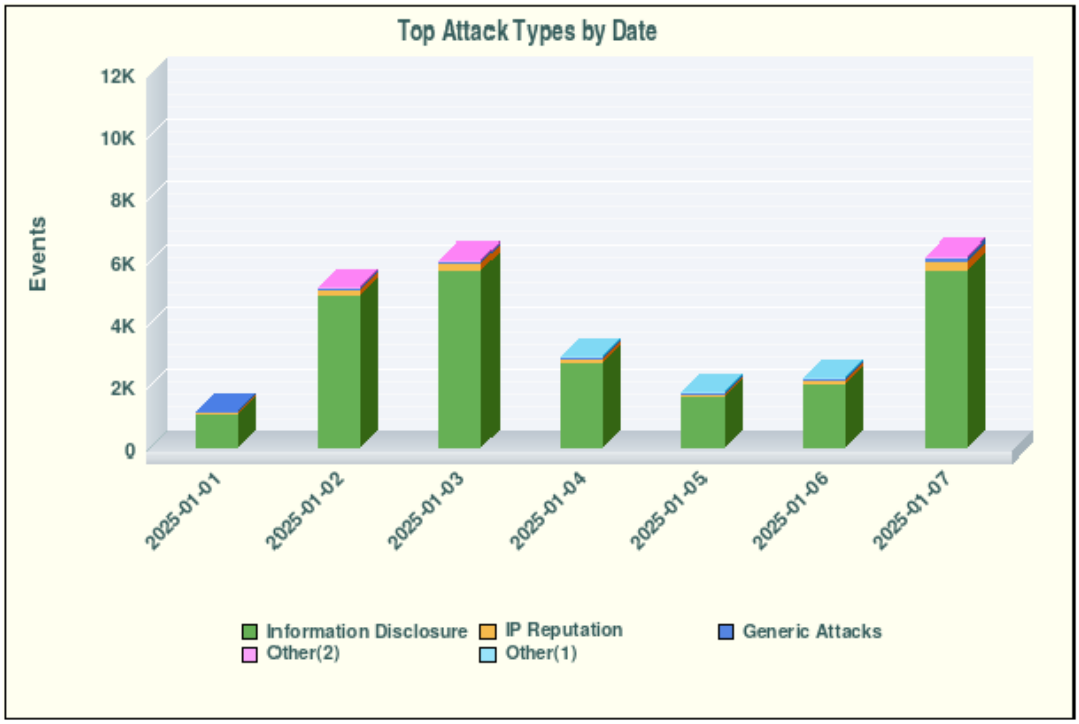


Ilustración 197 Top attack types

3.1.6.5. Solución de Anti-DDoS

Durante el período del mes de enero, se registraron eventos de ataques de denegación de servicio distribuido (DDoS) a las aplicaciones publicadas en internet por el Ministerio de Trabajo.
Una vez detectado los ataques DDoS, el FortiDDoS tomo medidas automáticas para bloquear y filtrar el tráfico malicioso, evitando así que se afecte los servicios protegidos.

A continuación, se detallan los hallazgos más relevantes que nos permite ver la plataforma.

Top Attacks

Attack	SPP	Direction	Drops	Events
Protocol flood	default	Inbound	71,489,589	5
State Anomalies: Outside window	APP_MINT	Inbound	14,674,435	29
State Anomalies: Outside window	PAGINA_MINTRABAJO	Inbound	13,861,739	36
State Anomalies: State transition error	PAGINA_MINTRABAJO	Inbound	3,818,454	4
State Anomalies: Outside window	Acceso_Web	Inbound	126,109	27
State Anomalies: Foreign packet (Out of State)	Acceso_Web	Inbound	16,927	2
State Anomalies: Foreign packet (Out of State)	PAGINA_MINTRABAJO	Inbound	1,820	2
State Anomalies: Foreign packet (Out of State)	APP_MINT	Inbound	650	3
State Anomalies: Outside window	SVE	Inbound	343	4
SSL/TLS Version Anomaly	Acceso_Web	Inbound	230	6

Ilustración 198 Top de ataques

Análisis Detallado:

State Anomalies: Outside Window

Descripción: Estas anomalías ocurren cuando los paquetes recibidos están fuera de la ventana de tiempo esperada, indicando posible manipulación de paquetes o intentos de evadir detección.
Principales Afectados:
APP_MINT: 824.453 drops (34 eventos)
PAGINA_MINTRABAJO: 2.314.046 drops (37 eventos)
Acceso_Web: 126,109 drops (37 eventos)

3.1.6.6.2 Login Fallidos

Durante el mes de enero, 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(172.30.31.7)	2025-02-06	08:50:39
dfcavanzo@css_e	GUI(172.30.31.11)	2024-10-08	10:47:22
admin	GUI(172.30.31.3)	2024-09-20	20:33:57
admin	GUI(172.30.31.3)	2024-09-20	20:33:47
admin	GUI(172.30.31.3)	2024-09-20	20:33:35
admin	GUI(172.30.31.3)	2024-09-20	20:33:34
admin	GUI(172.30.31.3)	2024-09-20	20:32:34
dfcavanzo@css_e	GUI(172.30.31.17)	2024-08-14	12:09:28
cmgarciac@css_e	GUI(172.30.31.7)	2024-07-19	11:16:20
admin	GUI(172.30.31.7)	2024-07-19	11:16:12

Ilustración 199 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

Para el mes de enero no se registraron incidentes en la herramienta de gestión.

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-75543	31/01/2025 16:35	RV: CV	SOC	Análisis de evento
RF-75458	31/01/2025 13:43	[Fortisiem] -- Mintrabajo // [Brute Force]	SOC	Reportes Seguridad Informática
RF-75168	30/01/2025 15:20	Creación Caso SOC - Solicitud enrutamiento	SOC	Correo Malicioso (Phishing, Smishing, whaling, otros)
RF-74761	29/01/2025 11:35	RE: Solicitud enrutamiento sedes Remostas SDWAN	SOC	Análisis de Correos
RF-74507	28/01/2025 15:05	Implementación de regla en Firewall.	SOC	Ajuste de configuraciones (Crear - Eliminar)
RF-74503	28/01/2025 15:00	RV: Parasitic greece Revealed.3	SOC	Revisar correo malicioso
RF-74191	27/01/2025 14:55	RE: Derecho de petición	SOC	Accesos por fuerza bruta
RF-73519	24/01/2025 8:07	Correo sospechoso	SOC	Permitir acceso
RF-73392	23/01/2025 14:45	RE: CORREO MALISIOSO	SOC	Ajustar política
RF-73370	23/01/2025 14:05	RE: CENDO RAMA JUDICIAL - Oficio 392 - OFICIO Y DETALLE DE ACTUACIÓN JUDICIAL	SOC	Permitir acceso
RF-73341	23/01/2025 11:30	habilitar acceso a full internet a la ip 172.16.60.20	SOC	Revisar correo malicioso

RF-73247	23/01/2025 8:40	Solocitd activación rutas SDWAN	SOC	Revisar correo malicioso
RF-73002	22/01/2025 9:21	Validación trafico política id 7	SOC	Revisar correo malicioso
RF-72995	22/01/2025 9:05	RE: Parasitic greece Revealed.3	SOC	Revisar correo malicioso
RF-72436	20/01/2025 11:01	MINTRABAJO // Habilitar ruta de sede San Gil	SOC	Revisar correo malicioso
RF-71926	16/01/2025 15:10	Solicitud Habilitar trafico VPN	SOC	Permitir acceso
RF-71841	16/01/2025 11:40	Solicitud Habilitar trafico VPN	SOC	Análisis - Concepto técnico Software
RF-71828	16/01/2025 11:20	Solicitud de habilitación de trafico	SOC	Ajustar política
RF-71804	16/01/2025 10:45	Correo sospechoso	SOC	Revisar correo malicioso
RF-71525	15/01/2025 12:21	RE: Solicitud enrutamiento sedes Remostas SDWAN	SOC	Modificacion VPN
RF-71440	15/01/2025 10:05	RV: Equipo de sistema	SOC	Agregar puerto
RF-71339	15/01/2025 7:28	Correo sospechoso	SOC	Agregar puerto
RF-71285	14/01/2025 16:35	MINTRABAJO // Habilitar rutas de sedes	SOC	Permitir acceso
RF-71200	14/01/2025 14:00	RV: Solicitud de creación de caso para servidores Zabbix	SOC	Revisar correo malicioso
RF-71152	14/01/2025 11:30	Habilitar rutas de sedes	SOC	Análisis de Herramienta
RF-70531	10/01/2025 21:00	RE: Solicitud enrutamiento sedes Remostas SDWAN	SOC	Revisar correo malicioso
RF-70523	10/01/2025 18:00	RE: Solicitud enrutamiento sedes Remostas SDWAN	SOC	Correo Malicioso (Phishing, Smishing, whaling, otros)
RF-70470	10/01/2025 15:15	RE: Habilitar rutas de sedes	SOC	Permitir acceso
RF-70394	10/01/2025 12:10	Correo sospechoso	SOC	Permitir acceso
RF-70253	9/01/2025 20:45	RE: Solicitud enrutamiento sedes Remostas SDWAN	SOC	Permitir acceso
RF-70209	9/01/2025 15:55	Solicitud de creación de caso para servidores Zabbix	SOC	Análisis de Malware
RF-70206	9/01/2025 15:45	RE: MINT // RF-70111 // Crear politica Datapump	SOC	Ajustar política
RF-70185	9/01/2025 14:45	RV: Permisos ILMT	SOC	Ajustar política
RF-70179	9/01/2025 13:55	RV: Solicitud enrutamiento sedes Remostas SDWAN	SOC	Correo Malicioso (Phishing, Smishing, whaling, otros)
RF-70111	9/01/2025 10:05	Crear politica Datapump	SOC	Análisis de Herramienta

Tabla.57 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 enero:

- **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.

- **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.

- **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.

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

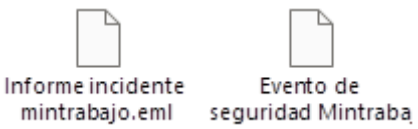
Dentro las activades realizadas en el mes de enero, se realizó la revisión, ajuste, observaciones de algunos procedimientos y políticas que describimos a continuación;

- Se envió correo al Ministerio de Trabajo (28/01/2025) en el cual se informa la identificación de extensiones de archivos ejecutables comunes que representan un riesgo significativo para la seguridad informática, explica los peligros asociados con cada tipo de archivo y detalla las medidas de mitigación recomendadas. Este análisis aplica a todos los sistemas y redes del ministerio, incluyendo equipos de escritorio, servidores y dispositivos conectados a la infraestructura corporativa.

- Se realizó reunión técnica del 23/01/2025, en la que se presentaron las vulnerabilidades de la relacionada a Informe a la infraestructura de mintrabajo, se envia correo a la ingeniera Caterrin Lozano con la matriz actulizada de las vulnerabilidades presentes

- Se envió análisis de correo (23/01/2025) phishing de la ministra de Trabajo donde se realizó análisis de este correo presenta múltiples señales claras de ser un intento de phishing.

- Se adjunta correos enviados al cliente como evidencia de las acciones realizada



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 58 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.
- 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.
- 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 enero 2025.
- Se ajustaron nuevos umbrales para diferentes aplicaciones y servicios a nivel de bases de datos MSSQL Server.
- 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.

• 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%	90,00%
DC-2	Continuidad y disponibilidad del datacenter principal	100%	99.95%
DC-3	Continuidad y disponibilidad del datacenter alterno	100%	99,60%
DC-4	Continuidad y disponibilidad de la plataforma de procesamiento, almacenamiento y respaldo	100%	99,70%
DC-5	Tiempo de solución de incidentes asociado a los servicios de aplicaciones especializadas	100%	90,00%
DC-6	Tiempo de solución de requerimientos asociado a los servicios de aplicaciones especializadas	100%	90,00%

ID	Indicadores	Resultado	Meta
DC-7	Continuidad y disponibilidad de los servicios de directorio activo	100%	99,60%
DC-8	Continuidad y disponibilidad de los servicios de seguridad informática	100%	99,90%
DC-9	Tiempo de solución de incidentes asociado a los servicios de administración, soporte y monitoreo	95,29%	90,00%
DC-10	Tiempo de solución de requerimientos asociado a los servicios de administración, soporte y monitoreo	99,84%	90,00%
DC-11	Cumplimiento en la entrega del informe de gestión mensual	100%	100,00%

Tabla 59 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 60 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, donde se observó el tráfico generado por las sedes, el canal ha trabajado de forma estable, no presentaron caídas ni saturación, se relaciona gráfica de consumo en la cual se puede observar que no se presenta caídas de tráfico, los días que se observa disminución de tráfico, corresponde a periodos de fin de semana.

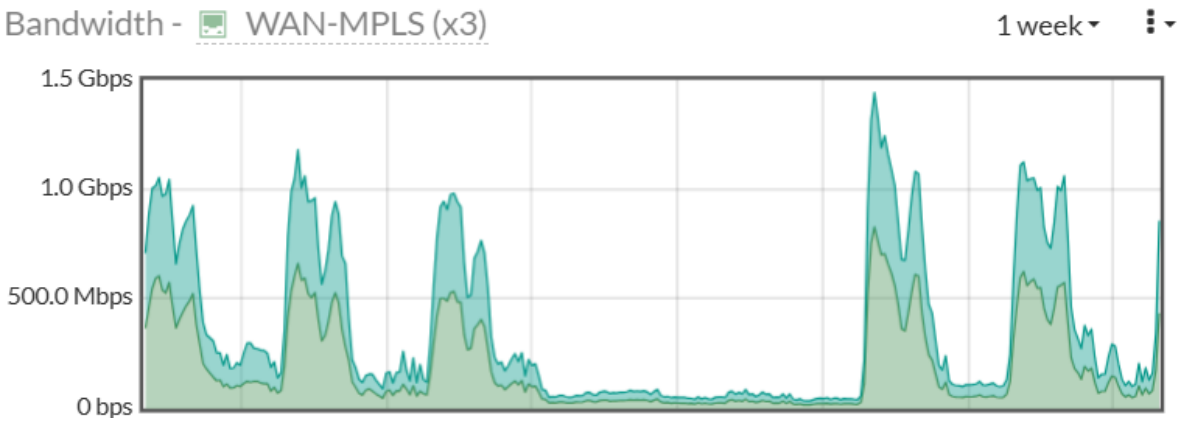


Ilustración *200*. Grafica de consumo canal MPLS Datacenter

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.

```
etb@INDRA_BOG_K68C169A_D# run show system uptime
Current time: 2025-02-05 07:54:51 COT
Time Source:  LOCAL CLOCK
System booted: 2024-07-25 11:12:28 COT (27w5d 20:42 ago)
Protocols started: 2024-07-25 11:13:28 COT (27w5d 20:41 ago)
Last configured: 2025-01-10 21:30:29 COT (3w4d 10:24 ago) by etb
 7:54AM  up 194 days, 20:42, 2 users, load averages: 0.20, 0.32, 0.32

[edit]
etb@INDRA_BOG_K68C169A_D#
```

```
etb@INDRA_BOG_K68C169A_D# run show system memory
System memory usage distribution:
       Total memory: 1950508 Kbytes (100%)
    Reserved memory:   50132 Kbytes (  2%)
       Wired memory:  252524 Kbytes ( 12%)
      Active memory:   66916 Kbytes (  3%)
    Inactive memory: 1350876 Kbytes ( 69%)
       Cache memory:       0 Kbytes (  0%)
        Free memory:  230060 Kbytes ( 11%)
```

Ilustración 201. Grafica estado del equipo MPLS Datacenter

3.3.1.1. Incidentes de Conectividad

Durante el mes de enero, 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
Sede Territorial Bogotá WTC	IM-70534	92,44
Sede Territorial Florencia	IM-74592	98,39
Sede Territorial Pasto	IM-67227	92,18
Cisneros	IM-75185	97,71
Concordia	IM-67488	99,53
Sonsón	IM-71624	94,29
Campo De La Cruz	IM-70168	99,59
Calle 32	IM-67099	78,86
Sede Territorial Cartagena	IM-74991	99,22
Sede Territorial Tunja	IM-67472	98,97
Anserma	IM-71429	81,00
Paz De Ariporo	IM-70395	96,96
El Bordo Patía	IM-67580	99,52
Agustín Codazzi	IM-73357	97,00
Chía	IM-73202	97,63
Girardot	IM-75438	98,17
Tocancipá	IM-70075	71,57
Ubaté	IM-71505	97,12
Zipaquirá	IM-73222	84,77
Garzón	IM-73183	96,26
Granada	IM-67506	98,62
Puerto Gaitán	IM-75006	99,33

Dirección Territorial	Caso Asociado	Disponibilidad
Los Patios	IM-74987	98,64
Puerto Wilches	IM-74992	99,12
Sabana De Torres	IM-74930	98,61
San Gil	IM-74931	98,61
Socorro	IM-74956	98,61
Vélez	IM-71323	83,12
Mariquita	IM-73509	82,56
Mosquera	IM-73142	51,61
Turbo	IM-71613	84,66

Tabla 61 Novedades servicio de internet

3.3.1.2. Topología Actual

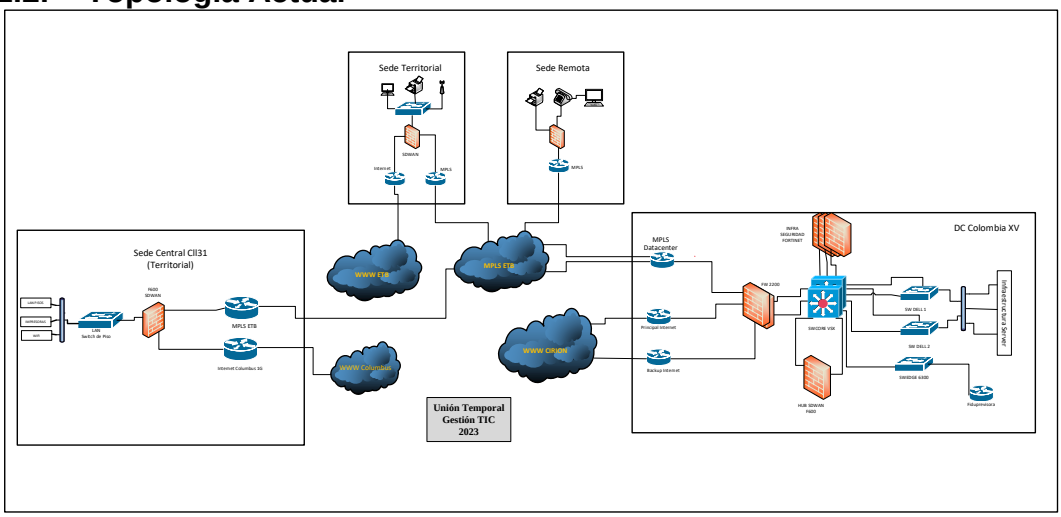


Ilustración 202. Topología actualizada

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.

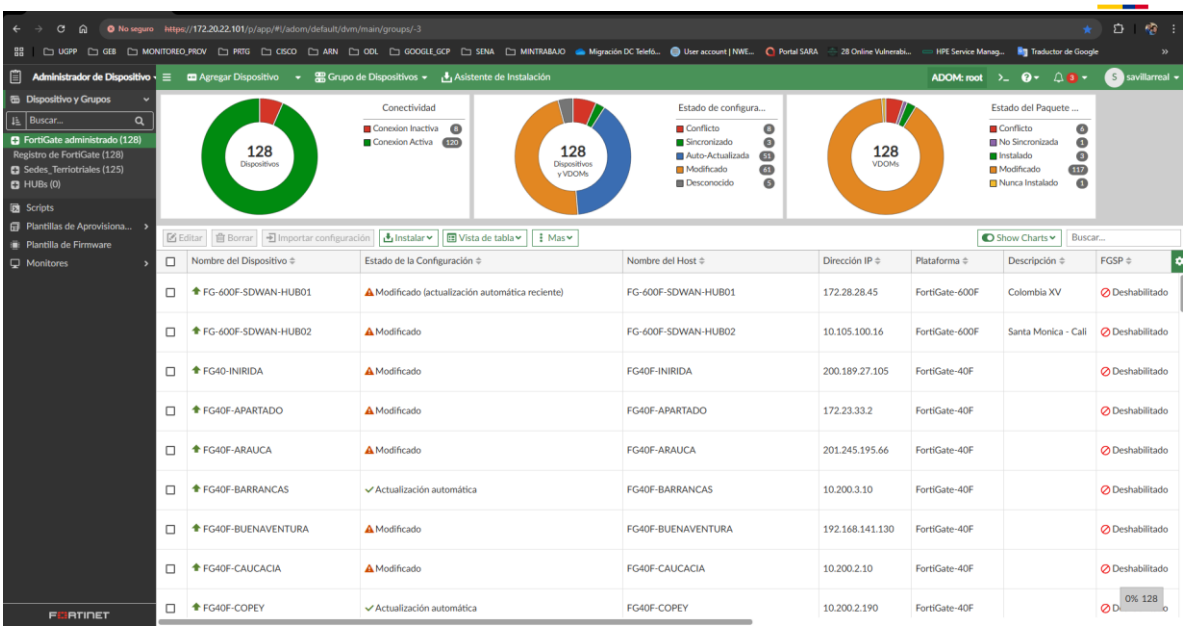


Ilustración 203. Interface Fortimanager

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

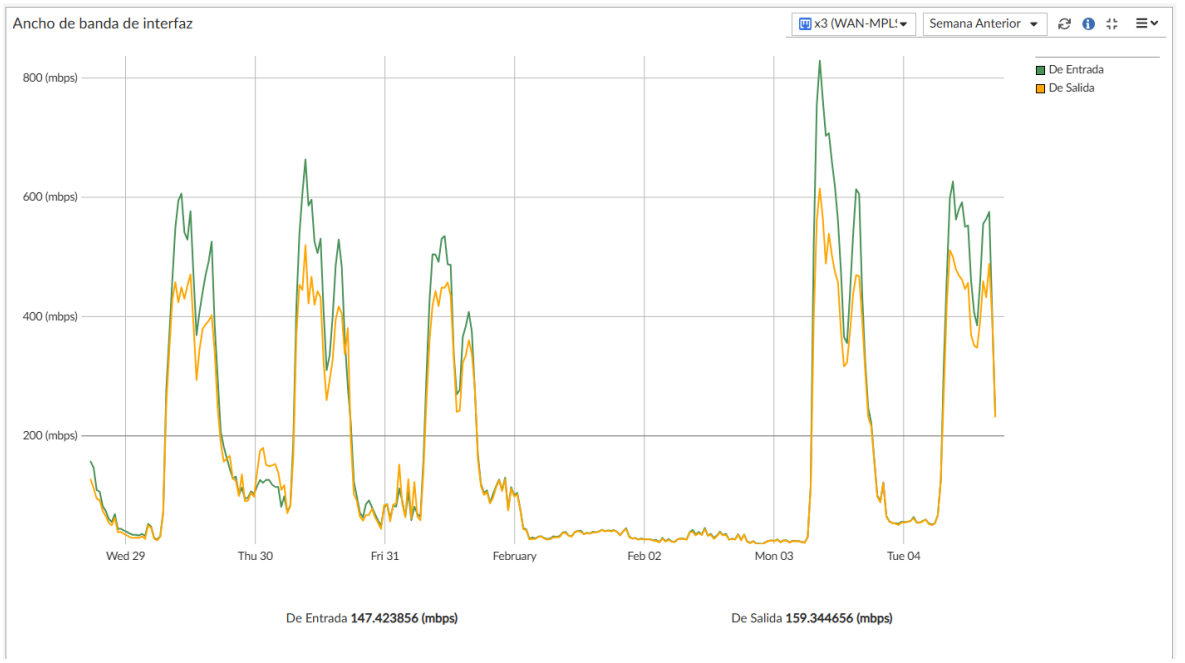


Ilustración 204. Interface MPLS HUB SDWAN

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

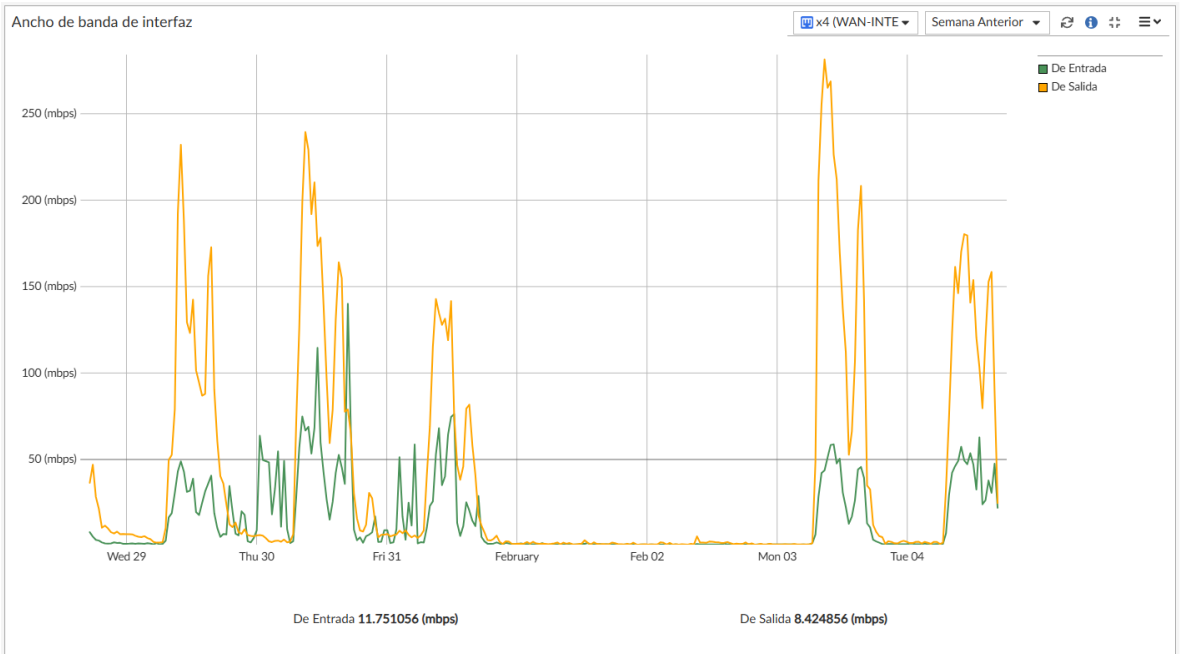


Ilustración 205. Interface Internet HUB SDWAN

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.

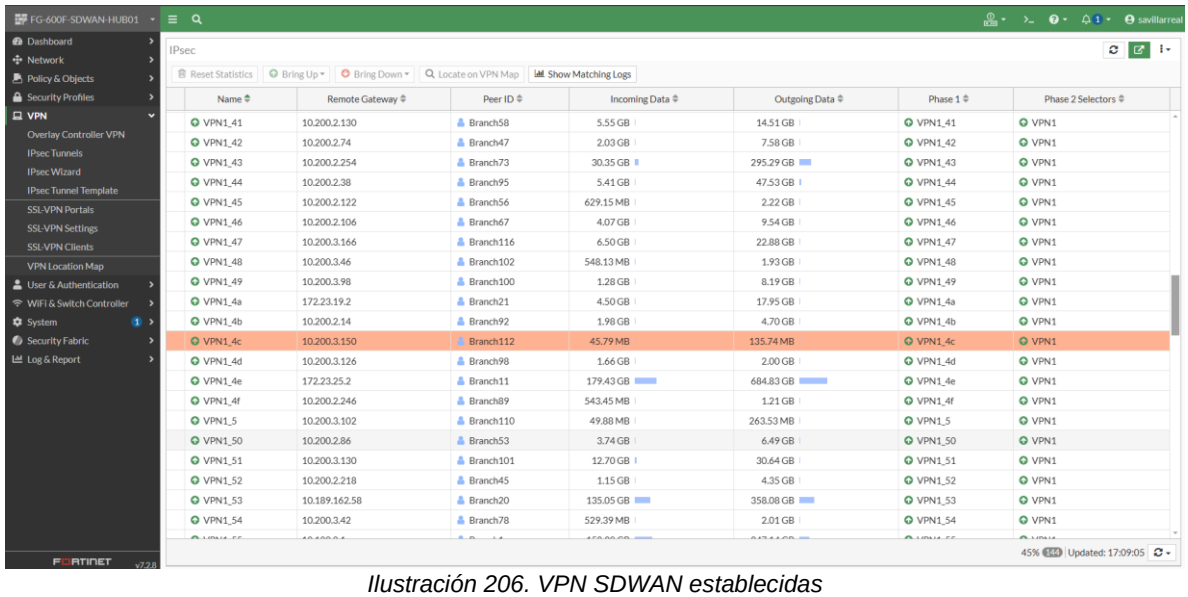


Ilustración 206. VPN SDWAN establecidas

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

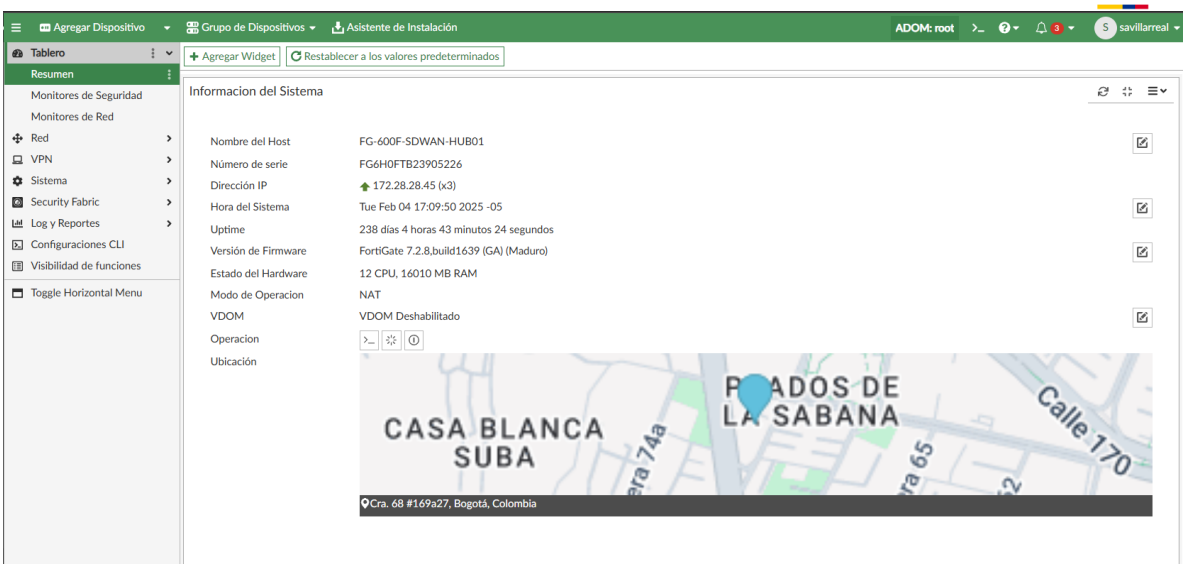


Ilustración 207. Estado HUB SDWAN Datacenter

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

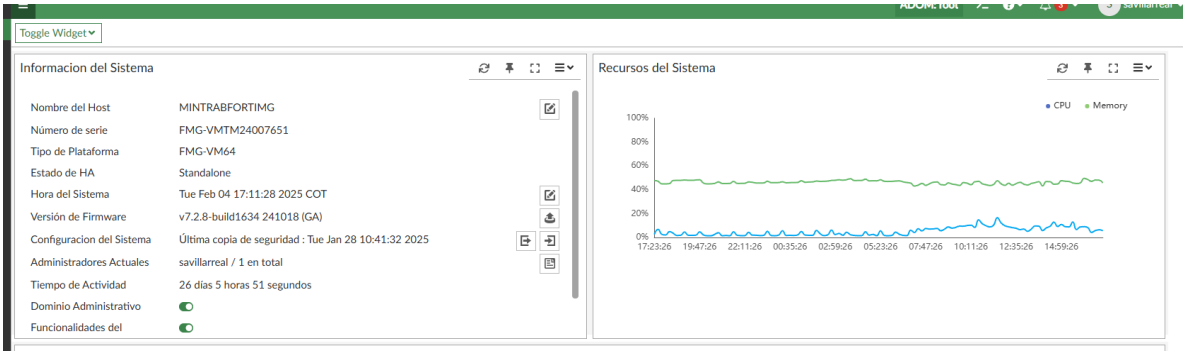


Ilustración 208. Recursos Fortimanager

Actualmente, se está trabajando en 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 enero se realizó la configuración del equipo Fortinet en 18 sedes, relacionadas en la siguiente tabla.

Sede	Operativo
Bugalagrande	1
Cartago	1
Chaparral	1
Dosquebradas	1
Fundación	1
Girardot	1
La Virginia	1
Málaga	1
Orito	1
Pamplona	1

Pitalito	1
Roldanillo	1
Salazar	1
San Vicente de Chucurí	1
Santa Rosa de Cabal	1
Sevilla	1
Tolu Viejo	1
Tuquerres	1
Total general	**18**

Tabla 62 Sedes configuradas en enero 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 63 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 diciembre:

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

Dirección Territorial	Disponibilidad	% Penalidad	Valor Penalidad un enlace
Cisneros	97,71	3%	$ 8.742
Concordia	99,53	3%	$ 8.742
Sonsón	94,29	10%	$ 29.140
Campo De La Cruz	99,59	3%	$ 8.742
Calle 32	78,86	20%	$ 582.809
Anserma	81,00	10%	$ 29.140
Paz De Ariporo	96,96	3%	$ 8.742
El Bordo Patía	99,52	3%	$ 8.742
Agustín Codazzi	97,00	3%	$ 8.742
Chía	97,63	3%	$ 8.742
Girardot	98,17	3%	$ 8.742
Tocancipá	71,57	50%	$ 145.702
Ubaté	97,12	3%	$ 8.742
Zipaquirá	84,77	20%	$ 58.281
Garzón	96,26	3%	$ 8.742
Granada	98,62	3%	$ 8.742

Dirección Territorial	Disponibilidad	% Penalidad	Valor Penalidad un enlace
Puerto Gaitán	99,33	3%	$ 8.742
Los Patios	98,64	3%	$ 8.742
Puerto Wilches	99,12	3%	$ 8.742
Sabana De Torres	98,61	3%	$ 8.742
San Gil	98,61	3%	$ 8.742
Socorro	98,61	3%	$ 8.742
Vélez	83,12	20%	$ 58.281
Mariquita	82,56	20%	$ 58.281
Mosquera	51,61	100%	$291.404
Turbo	84,66	20%	$ 58.281
TOTAL			**$ 1.459.936**

Tabla 64 Desagregado sedes con novedad un solo enlace

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

Dirección Territorial	Disponibilidad	% Penalidad	Valor Penalidad doble enlace
Sede Territorial Bogotá WTC	92,44	10%	$ 384.394
Sede Territorial Florencia	98,39	3%	$ 23.064
Sede Territorial Pasto	92,18	10%	$ 115.318
Sede Territorial Cartagena	99,22	3%	$ 34.595
Sede Territorial Tunja	98,97	3%	$ 34.595
Total			**$ 591.966,00**

Tabla 65 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	**2292**

Tabla 66 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.
- **Asignación y entrega de kits periféricos USB**: Se realizó la entrega de kits periféricos USB en territorio para usuarios con equipos de cómputo portátil. Estos kits fueron adquiridos por la entidad en el Nivel Central, DT Bogotá y Sedes Territoriales. La entrega fue ejecutada por el personal de soporte en sitio, junto con la generación del acta de asignación correspondiente. Esta actividad continuará en el siguiente período.
- **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 15 casos de garantía a corte del periodo. A continuación, se detallan los estados asociados a estos casos:

Estado de caso	Cantidad
Cerrado	**4**
En proceso	**1**
Suspendido	**10**
Total	**15**

Tabla 66 Estado de casos de garantía.

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

ANS	Cerrado	En proceso	Suspendido	Total
CUMPLE	4	1	9	14
NO CUMPLE			1	1
Total	4	1	10	15

Tabla 67 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	Diadema	Teléfono	DT	Parte afectada	ESTADO
VELANDIA ARENALES GILMER ADEMIR	PW09ZT5D	No aplica	No aplica	CUCUTA	Equipo con gel o bolas de plastico en la parte del plug de audio	Reportado a la supervisión, a la espera de cotización
LLANES IBARGUEN TATIANA	MJ0LS5SH	HC3BBTK3	No aplica	ANTIOQUIA	Diadema sin etiqueta, fallo en auricular	Reportado a la supervisión, a la espera de cotización
PARADA MIEL KELLY JOHANA	MJ0LS47P	HC3BBLTW	No aplica	ARAUCA	Diadema sin etiqueta	Reportado a la supervisión, a la espera de cotización
ORTIZ RODRIGUEZ IVAN ALFREDO	No aplica	HC3BBL04	No aplica	NIVEL CENTRAL	Diadema sin etiqueta	Reportado a la supervisión, a la espera de cotización
MUÑOZ SUESCUN YISETH ANDREA	PWA3BE0	No aplica	No aplica	CAUCA	Equipo mojado, componentes internos sulfatados	Reportado a la supervisión, a la espera de cotización
SALAZAR GARCIA MONICA MARIA	No aplica	No aplica	SC13912179	NIVEL CENTRAL	Bocina del teléfono pegada a la carcasa	Reportado a la supervisión, a la espera de cotización
GOMEZ ORTIZ HENRY SAMIR	PW0A36X6	No aplica	No aplica	NIVEL CENTRAL	Hurto de equipo	Reportado a la supervisión, a la espera de cotización

Tabla 68 ANS Equipos en siniestro

Avance en Instalaciones de Equipos y Entrega a Usuarios Finales:

A continuación, se presenta el avance alcanzado durante el periodo del informe en relación con las instalaciones de equipos y su entrega a los usuarios finales:

Tipo de equipo	Instalados	Almacenados	Garantias	Siniestros
Portátil	898	322		3
Escritorio	1082	110		
Teléfono	231	184		1
Diademas	2384	28	9	3

Tabla 69 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.

- **Asignación de equipos portátiles adicionales: ** Durante el mes, no se recibieron solicitudes de asignación de equipos de cómputo portátiles adicionales ni requerimientos de activos en las sedes.

- **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 enero, desde la gestión de equipos de cómputo se relacionan las solicitudes de soporte atendidas para este servicio:

- Se registraron en Aranda un total de 787 solicitudes tipificadas así:
  - Incidentes – 77 casos
  - Requerimientos de Servicio – 710 casos.
- Al corte de mes quedaron en estado:
  - Cerrado – 773 casos.
  - Solucionado – 10 casos
  - Suspendido – 2 casos.
  - En Proceso – 2 casos.
- 68 casos corresponden a solicitudes de usuarios VIP y 719 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_Soporte_Territoriales	372
Responsable_Soporte_Bogota	324
Responsable_Mesa_De_Servicio	80
NOC	2
Responsable_Soporte_Impresoras	2
Responsable Garantías Equipos	2
Responsable_De_Servidores_Windows	2
Gestor de inventarios	1
SOC	1
Especialistas de redes	1
Total general	**787**

Tabla 67 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	**77**
Falla - Error conexión a red	33

Tipificación / Categoría	Cantidad de solicitudes
Falla - error	15
No enciende	12
Lentitud - Bloqueo	11
Falla de sistema operativo	5
Daño Fisico	1
Requerimiento de servicio	**710**
Configuracion	268
Asesoria - Consulta	199
Conectar a red Mintrabajo	75
Traslado - Movimiento	55
Asignación de equipo (portátil o PC)	32
Solicitud Backup	31
Borrado seguro PC	13
Mantenimiento preventivo	11
Devolución de equipo (portátil o PC)	11
Borrado seguro Portátil	6
Conectar a red Invitados	4
Préstamo Equipo (portátil o PC)	3
Análisis Equipo de Computo	1
Borrado seguro (Portátil o PC)	1
TOTAL	**787**

Tabla 68 Solicitudes de Equipos Usuario Final – Según Tipificación y Categoría

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

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

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

Tabla 69 Medición ANS Equipos de Usuario Final

4.2. Conectividad LAN y WLAN

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

- Se realizó seguimiento a la falla del canal MPLS en sede central bajo el ticket 20965385, no se tuvo afectación de servicio debido a que se operó por el canal alterno.
- Se gestionó la instalación e implementación de antena Starlink y firewall en la inspección de Mosquera debido a la falla del canal MPLS por parte de ETB.
- Se realizó gestión y seguimiento a las constantes caídas de servicio MPLS en la territorial de Cartagena bajo el ticket 21456754.
- Se realizó gestión y seguimiento a la intermitencia en el servicio de la antena Starlink en la Inspección de Sabanalarga.

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

- Para el mes de enero, los especialistas responsables del servicio gestionaron un total de 44 solicitudes escaladas a través de la herramienta Aranda. Al corte del mes, 40 casos quedaron en estado *Cerrado, 3 casos en estado suspendido y 1 caso en proceso.*

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

Categoría	Cantidad de solicitudes
Starlink	17
Sin servicio	14
Degradación	3
Revisión estado del canal	3
Caída	2

Tabla 70 Top 5 de categorías en el Servicio de conectividad LAN-WLAN



Ilustración 209 Estado de casos Redes y Conectividad

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

4.2.1. Switch CORE Sede Principal

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

4.2.2. Switch para conexiones perimetrales (EDGE) en sede principal

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

4.2.3. Switch de acceso 24 puertos

Se encuentran operativos y en monitoreo los siguientes equipos:

Dirección Territorial	Población y/o ciudad de ubicación	Cantidad switches 24 puertos
Territorial Atlántico	BARRANQUILLA	1
Territorial Bolívar	Cartagena	1
Territorial Boyacá	TUNJA	1
Territorial Caldas	MANIZALEZ	1
Territorial Caquetá	FLORENCIA	1

Dirección Territorial	Población y/o ciudad de ubicación	Cantidad switches 24 puertos
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 71 Distribución y Cantidades de switch 24 puertos

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

4.2.4. Switch de acceso 48 puertos

Se encuentran operativos y en monitoreo los siguientes equipos:

Dirección Territorial	Población y/o ciudad de ubicación	Cantidad switches 48 puertos
Territorial Antioquia	MEDELLIN	4*
Territorial Arauca	ARAUCA	1
Territorial Atlántico	BARRANQUILLA	2
OE Barrancabermeja	BARRANCABERMEJA	1
Calle 32	BOGOTA	5
Territorial Bolívar	Cartagena	1
Territorial Boyacá	TUNJA	1
Territorial Caldas	MANIZALEZ	1
Territorial Cauca	POPAYAN	1
Territorial Cesar	VALLEDUPAR	1
Territorial Chocó	QUIBDÓ	1
Territorial Córdoba	MONTERIA	1
Territorial Cundinamarca	FACATATIVÁ	1
Territorial Guajira	RIOHACHA	1
Territorial Huila	NEIVA	1
Territorial Magdalena	SANTA MARTA	1
Territorial Meta	VILLAVICENCIO	1
Territorial Nariño	PASTO	1
Territorial Norte de Santander	CÚCUTA	1
Territorial Quindío	ARMENIA	1
Territorial Risaralda	PEREIRA	1
Territorial Santander	BUCARAMANGA	2
Territorial Sucre	SINCELEJO	1
Territorial Tolima	IBAGUÉ	1
OE Urabá Apartadó	APARTADÓ, ANTIOQUIA	1
Territorial Valle	CALI	2
OE Buenaventura	BUENAVENTURA	1
Sede Nivel Central	BOGOTA	34*

Dirección Territorial	Población y/o ciudad de ubicación	Cantidad switches 48 puertos
	Total	**71**

Tabla 72 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	5*
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	2*
Territorial Putumayo	MOCOA	1
Territorial Quindío	ARMENIA	3
Territorial Risaralda	PEREIRA	2
Territorial Santander	BUCARAMANGA	0
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	45
	Total	**108**

Tabla 73 Distribución de puntos de acceso

(*) Novedades en la instalación de puntos de acceso

No instalados: 4
Territorial Bogotá: 2 AP fueron retirados debido a que el área donde iban ubicados ya no pertenece al Ministerio del Trabajo.
Territorial Norte de Santander - Cúcuta: El director territorial permitió la instalación de 3 AP y 1 equipo restante se encuentra en Stock.
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 74 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 75 Equipos gama media

(*) Novedades en la instalación de teléfonos
Nivel Central pendientes 4, 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
SEGOVIA	SEGOVIA	1	Sede reabierta (Diciembre-Enero)
AMAGA	AMAGA	1	Cerrada se envió teléfono a Medellín
MONTERREY	MONTERREY	1	Cerrada
BOLIVAR	BOLIVAR	1	Cerrada
TIERRA ALTA	TIERRA ALTA	1	Cerrada

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

Tabla 76 Sedes cerradas

Estado	Cantidad
Operativos	326
Inspecciones cerradas	9(*)
Pendiente por MinTrabajo (usuario no disponible, usuario en licencia, usuarios no recibieron equipo, adecuaciones de cableado o físicas, asignación usuarios)	15
Total	**350**

Tabla 77 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	26
Proceso de reposición	1
Pendientes definición de usuario por parte de la supervisión para asignación	3
Total	30

Tabla 78 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 enero de 2024, 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.
- En el presente mes se gestionaron 6 casos correspondientes a activación, aprovisionamiento de licencias de telefonía Phone System las cuales se gestionaron de manera oportuna.
- Se realizó la recolección de 1 Mifi el cual estaba asignado de manera temporal, solicitado directamente por el Ing. Mauricio Fernandez, asignado temporalmente para el funcionario Carlos Umaña.
- Se llevo a cabo proceso de actualización sobre la infraestructura de telefonía la cual se realizó de manera satisfactoria. La misma se ejecutó bajo el cambio RFC-71079.

- **Asignación de Licencias - Extensiones**

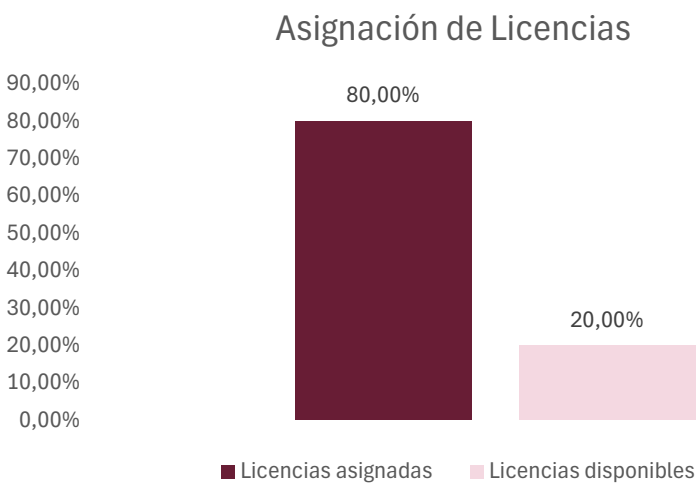


Ilustración 210. Licencias y extensiones

Durante el mes en gestión, se han asignado un total de 1.420 extensiones a nivel nacional. Actualmente, permanecen disponibles 280 extensiones.

- **Estadísticas de Tráfico**

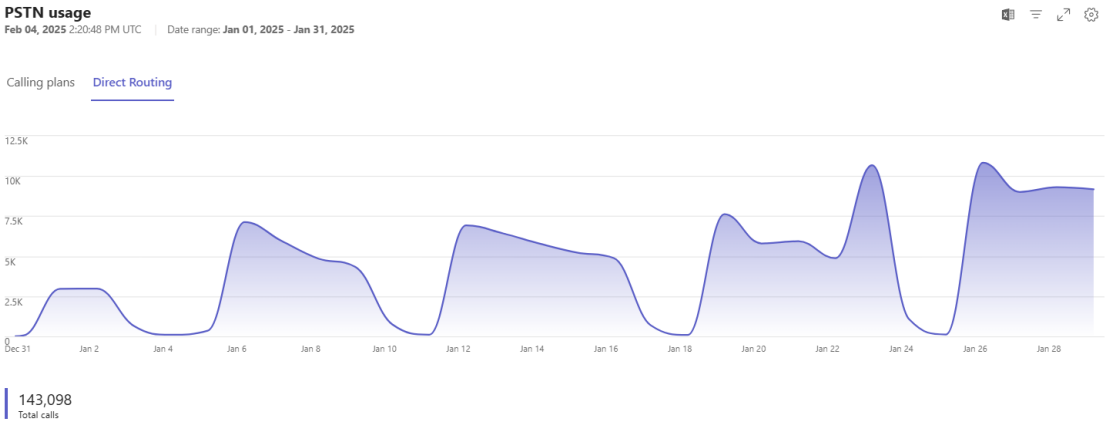


Ilustración 211 Estadística de tráfico

En la gráfica anterior se visualizan las tendencias de uso del servicio, en el periodo correspondiente al mes de enero de 2025, donde se atendieron un total de 143,098 llamadas.

Servicio	Minutos Disponibles	Minutos Utilizados
Locales	Ilimitados	828.38
Celular	1000	666.63
Nacional	Ilimitados	137.8
Internacional	700	5.03
Total		1637.84

Tabla 79 Minutos, consumos

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

Con respecto a las llamadas realizadas a destinos larga distancia nacional en el mes de enero de 2025, se identifica que se realizaron llamadas con una duración total de 137.8 minutos.

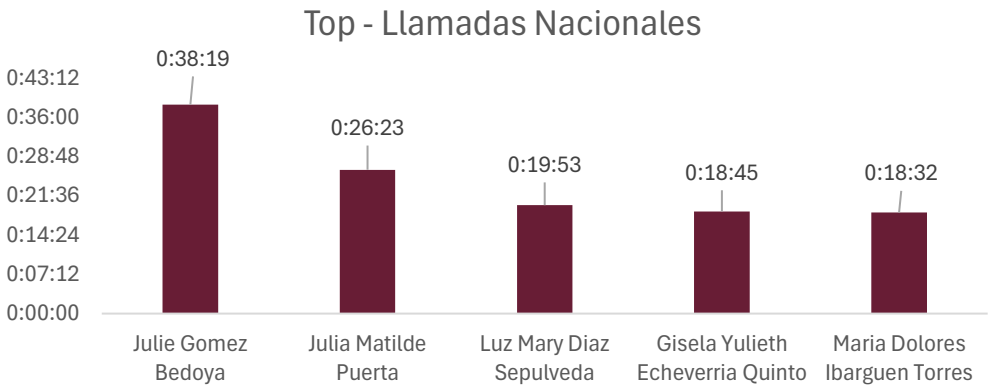


Ilustración 212 Top LDN

N°	Usuario	Área	Tiempo llamadas
1	Julie Gomez Bedoya	Grupo De Atencion Al Ciudadano Y Tramites-Valle del Cauca	0:38:19
2	Julia Matilde Puerta	Grupo comisiones 1 - Medellín	0:26:23
3	Luz Mary Diaz Sepulveda	Grupo comisiones 1 - Medellín	0:19:53
4	Gisela Yulieth Echeverria Quinto	Grupo comisiones 2 - Uraba	0:18:45
5	Maria Dolores Ibarguen Torres	Grupo De Resolucion De Conflictos – Conciliacion - Apartado	0:18:32

Tabla 80 Top 5 llamadas LDN

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

Con respecto a las llamadas internacionales en el mes de enero 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 213 *Top LDI*

Como se puede observar en el grafico anterior, se evidencia que, en el mes de enero 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	0:05:03

Tabla 81 Top 5 llamadas LDI

- **Consumo de llamadas destinos celulares**

Con respecto a las llamadas realizadas a celular en el mes de enero de 2025, se identifica que se realizaron llamadas con una duración total de 666.63 minutos.

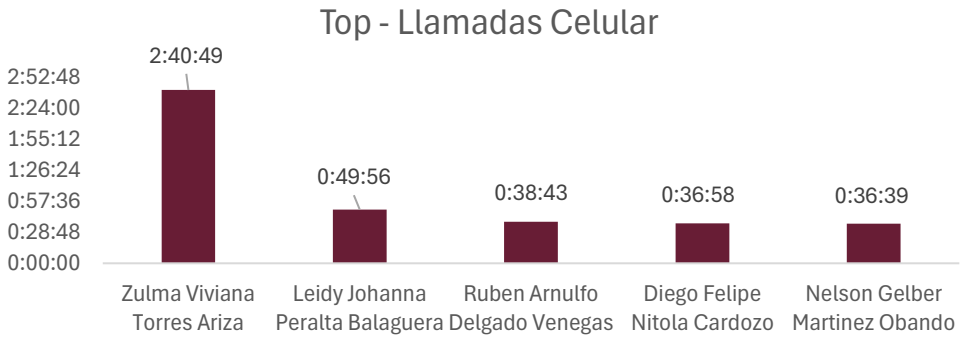


Ilustración 214 Top Celular

N°	Usuario	Área	Tiempo llamadas
1	Zulma Viviana Torres Ariza	Oficina Asesora Jurídica – DT Bogotá	02:40:49
2	Leidy Johanna Peralta Balaguera	Grupo piv-rcc Boyacá	00:49:56
3	Ruben Arnulfo Delgado Venegas	Atención ciudadana – DT Cundinamarca	00:38:43
4	Diego Felipe Nitola Cardozo	Grupo piv-rcc Boyacá	00:36:58
5	Nelson Gelber Martinez Obando	Grupo de Gestión Administrativa DRL	00:36:39

Tabla 82 Top 5 llamadas Celular

- **Consumo de llamadas locales**

Con respecto a las llamadas realizadas a destinos locales en el mes de enero de 2025, se identifica que se realizaron llamadas con una duración total de 828.38 minutos.

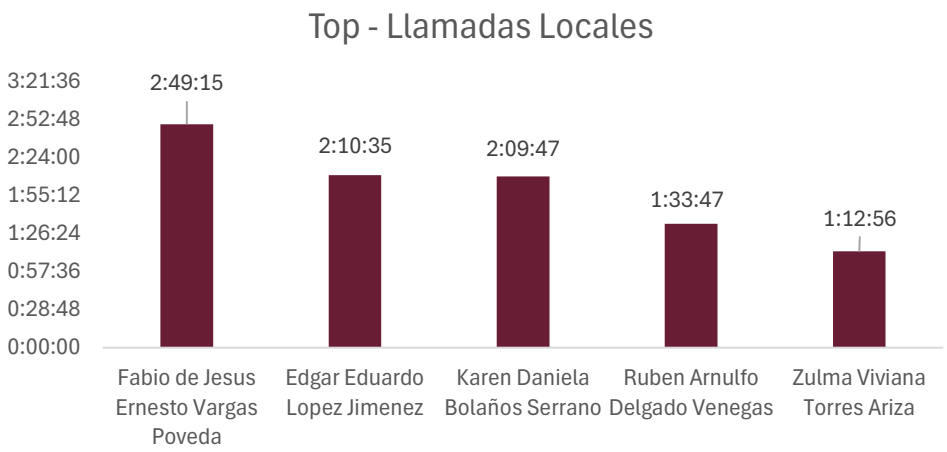


Ilustración 215 Top Local

N°	Usuario	Área	Tiempo llamadas
1	Fabio de Jesus Ernesto Vargas Poveda	Grupo Interno De Trabajo De Inspeccion, Vigilancia Y Control De Bogotá	02:49:15
2	Edgar Eduardo Lopez Jimenez	Grupo rcc Bogotá	02:10:35
3	Karen Daniela Bolaños Serrano	Despacho del viceministro de relaciones laborales	02:09:47
4	Ruben Arnulfo Delgado Venegas	Atención ciudadana – DT Cundinamarca	01:33:47
5	Zulma Viviana Torres Ariza	Oficina Asesora Jurídica – DT Bogotá	01:12:56

Tabla 83 Top 5 llamadas locales

- **Capacitaciones y divulgaciones**

En el mes de enero no se realizó proceso de capacitación y/o 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

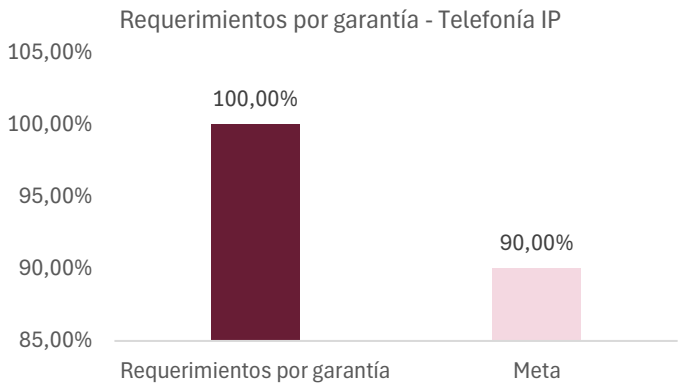


Ilustración *216 Requerimientos por garantía*

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

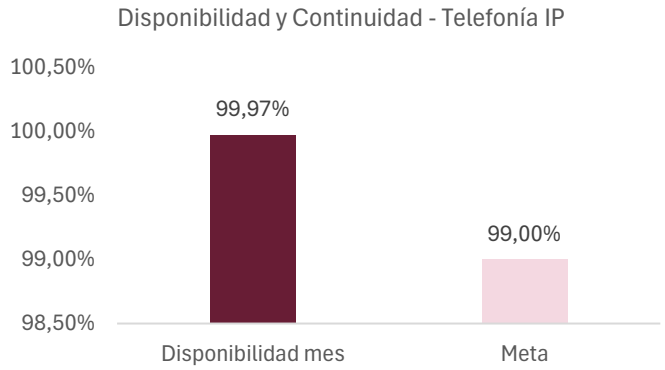


Ilustración 217 *Disponibilidad y Continuidad TOIP*

En el periodo correspondiente al mes de enero, 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	99,97%	99,00%
TIP-3	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%

Tabla 84 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 85 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 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 86 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, novedad con la UPS en la territorial de Santander (Bucaramanga) propiedad de la entidad, ya que se encuentró 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.

Durante el período del informe no se presentan casos de soporte para los equipos de Energía Regulada UPS.

- **Medición de ANS Energía regulada**

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

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

Tabla 87 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 Enero, el responsable del servicio gestionó un total de 2.872 solicitudes escaladas a través de Aranda. Al corte del mes, 2.858 casos quedaron en estado *Cerrado/Solucionado, 14 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	blanco y negro
cjunco	Carlos Julio Junco Arenas	6359
gcontractual	Gestion Contractual	5240
pnustes	Patricia Celestial Nustes Barrera	4856
cbecerra	Catherin Adriana Becerra Becerra	3884
lforrero	Lizeth Dahiana Forero Peralta	3236
jgutierrezb	Jarvi Giovanni Gutierrez Beltran	2954
jboyaca	Jenny Samantha Boyaca Carreño	2792
oyate	Oscar Javier Yate Gaviria	2745
jrodriguezar	Jeffer Karlyu Rodriguez Arevalo	2581
vfierro	Viviana Fierro Herrera	2492

Tabla 88 Consumo de impresiones por usuario - Impresoras B/N

Clics enero.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
Ricoh-cali-piso4	16318
Sede central ricohpiso5a	14681
Sede central ricohpiso8b	14211
ricoh-bmanga-ofc205	13264
Sede central ricohpiso21a	11424
Sede central ricohpiso19a	10566
ricoh-cali-piso3	9953
Sede central ricohpiso9a	9769
Sede central ricohpiso5b	9030
ricoh-medellin-piso1	8940

Tabla 89 Top 10 de impresoras con mayor uso

impresoras mas usadas enero.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	2099
ymedinag	Yeisson Medina Gonzalez	700
wguavita	Wendy Lorena Guavita Trujillo	558
bhernandez	Bibiana Hernandez Hernandez	221
jrojas	Juanita Rojas Rodriguez	164
escoltas2	Escoltas2	17
cniampira	Cristian Jesus Niampira Ramirez	9

Tabla 90 Top de usuarios que más generaron impresiones a color

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	141550
D. T. Valle Del Cauca	48979
D. T. Bogota	31279
D. T. Antioquia	30264

D. T. Santander	29142
D. T. Norte De Santander	13671
D. T. Risaralda	13308
D. T. Cundinamarca	12680
D. T. Tolima	12549
D. T. Quindio	9724

Tabla 91 Top oficinas



Informe por oficinas enero.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 92 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 93 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 enero de 2024:

MES	DETALLE	CANTIDAD
Enero	Multifuncional blanco y negro rango medio - Clic de impresión tóner y papel carta	532.919
	TOTAL	532.919

Tabla 94 Clics de Impresión de enero 2025 – Multifuncional B/N

A continuación, se indica la tendencia de consumo para el primer trimestre de 2025

Mes	Enero
Cantidad de clics consumidos	532.919

Tabla 95 tendencia de consumo de clics B/N

El consumo mensual establecido para el servicio es de 450.000 clics de impresión en B/N a nivel nacional, para el período del informe se presentó un consumo de 450.676 clics de impresión y 82.243 de fotocopias para un total de 532.919 para este servicio, superando el estimado del mes por 82.919

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)

Impresora	Fotocopias
ricoh-medellin-piso1	32050
Calle 32 ricoh-rcc	26943
Calle 32 ricoh-gau-b	26425
ricoh-bmanga-ofc205	16530
Sede central ricohpiso5b	16022
ricoh-cali-piso4	12948
ricoh-caqueta-piso1-ppal	12072
ricoh-baq-dir	10126
Ricoh-bmanga-ofc305	10066
ricoh-monteria-piso2	10027

Tabla 96 Top 10 impresoras mas usadas del servicio de fotocopiado

Reporte Copias Enero.xlsx

4.6.6. Impresora Color rango medio – Clic de impresión

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

MES	DETALLE	CANTIDAD
Enero	Impresora color rango medio - Cargo fijo mensual - Clic de impresión tóner y papel carta	3.760
	TOTAL	3.760

Tabla 97 Clics de Impresión de enero 2025 – Impresora Color

A continuación, se indica la tendencia de consumo para el primer trimestre de 2025

Mes	Enero
Cantidad de clics consumidos	3.760

Tabla 98 tendencia de consumo de clics color

El consumo mensual establecido para el servicio por la entidad es de 1500 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 3.760 clics para este servicio, superando el estimado del mes por 2.260 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.

Asignaciones cuota enero.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.

Usuario	Nombre Completo	Tipo de transacción	Cuota asignada en el mes	Cantidad de veces que se aumentó el saldo
cbecerra	Catherin Adriana Becerra Becerra	ADJUST	3948	13
jboyaca	Jenny Samantha Boyaca Carreño	ADJUST	2780	9
cjunco	Carlos Julio Junco Arenas	ADJUST	6512	8
gcolonia	Gustavo Adolfo Colonia Trochez	ADJUST	1598	7
hpena	Helena Peña Urrego	ADJUST	1509	7
jmendezm	Jaime Alberto Mendez Millan	ADJUST	1467	7
jrodriguezar	Jeffer Karlyu Rodriguez Arevalo	ADJUST	3097	7
lforrero	Lizeth Dahiana Forero Peralta	ADJUST	4839	7
pnustes	Patricia Celestial Nustes Barrera	ADJUST	4876	7
rmicolta	Ruby Aracely Micolta Banguera	ADJUST	1628	7

Tabla 99 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 de 2024 la etapa de operación del servicio:

	oct-24		nov-24		dic-24	
	Resmas Carta	Resmas Oficio	Resmas Carta	Resmas Oficio	Resmas Carta	Resmas Oficio
Total Resmas	993	950	319	235	537	345
Total Cajas por Tamaño	99,3	95	31,9	23,5	53,7	34,5
Total Cajas Enviadas	**194,3**		**55,4**		**88,2**	

Tabla 100 Despacho de papel a sedes del Ministerio del Trabajo

Durante el período, se despacharon a sedes del Ministerio un total de 45 tóners para impresora B/N y se realiza cambio de 2 unidades de tambor.

- **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 101 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 enero 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.

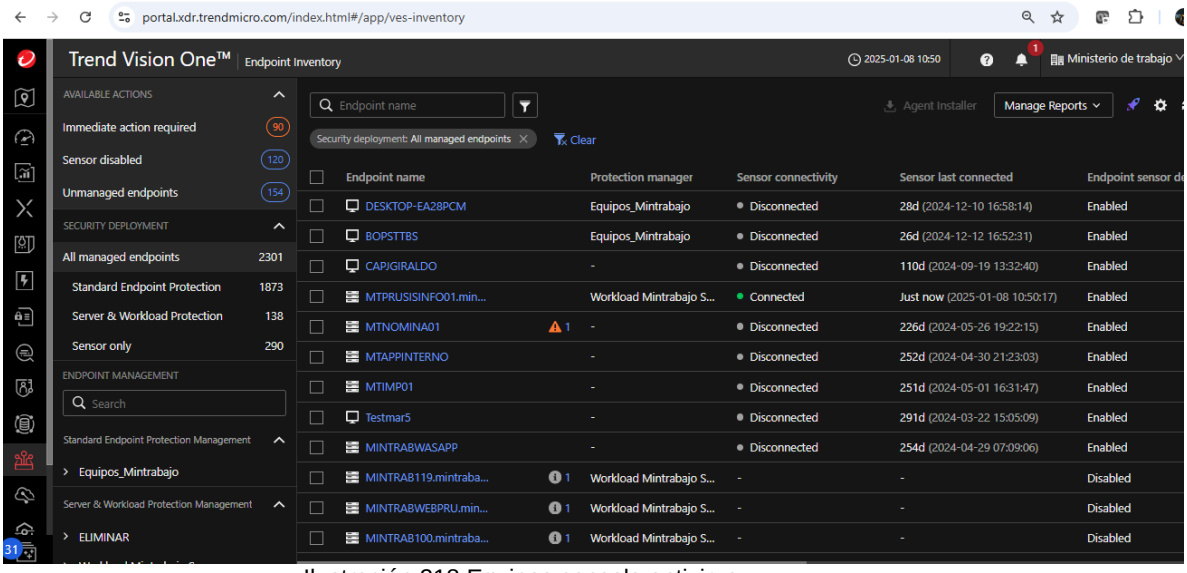


Ilustración 218 Equipos consola antivirus

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 de Mintrabajo

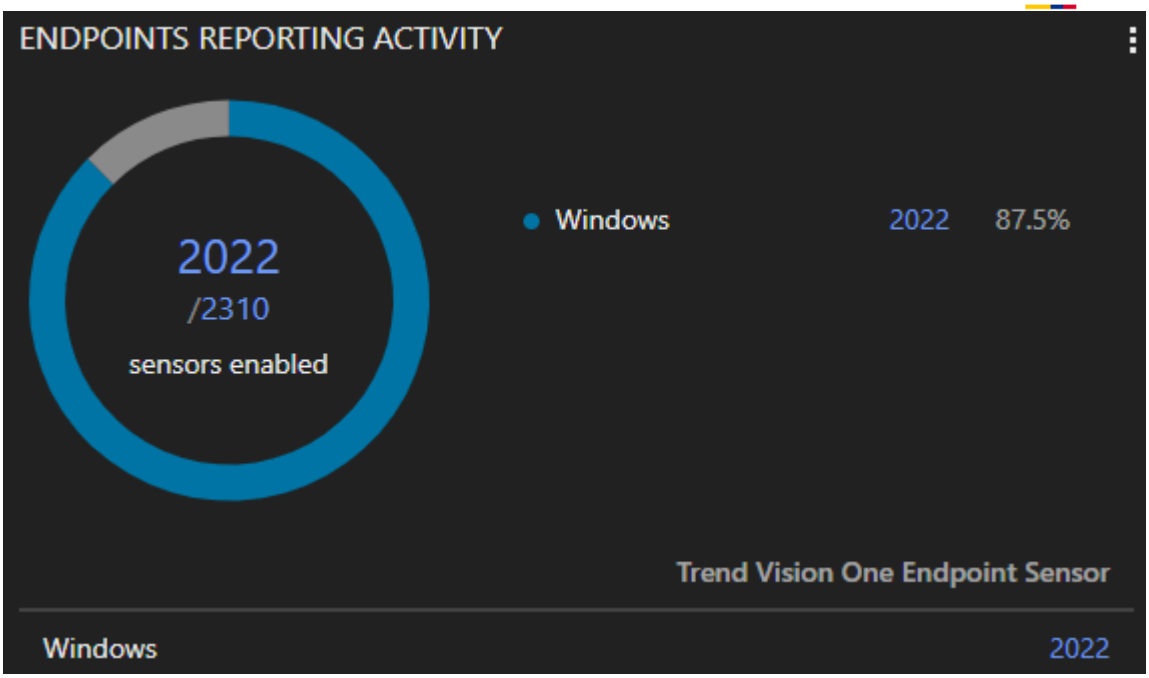


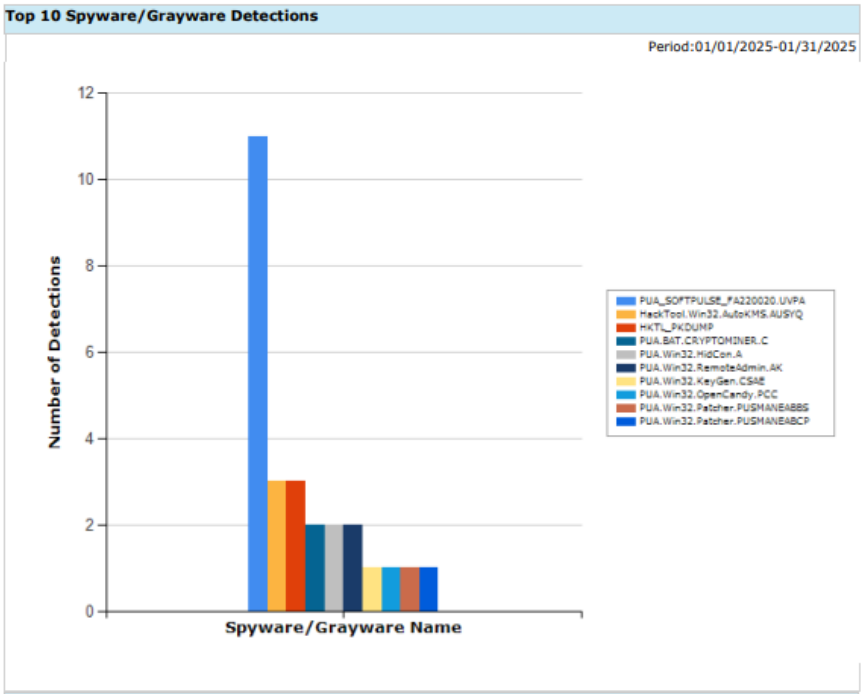
Ilustración 219 Gestión consola antivirus – equipos usuario final

4.7.3. Top 10 spyware

Las detenciones relacionadas con herramientas clasificadas como **HackTool** y **PUA** (Potentially Unwanted Applications), asociadas específicamente con variantes de **AutoKMS** y **CRCK_REMWAT**. Estas herramientas son utilizadas principalmente para realizar activaciones no autorizadas de software, lo cual representa no solo un incumplimiento legal, sino también un riesgo significativo para la seguridad del entorno.

Variantes Detectadas:

- Se detectaron **11 casos** de **PUA_SOFTPULSE_FA220020.UVPA**, lo que indica una presencia significativa de software potencialmente no deseado (PUA).
- Se identificaron **herramientas de activación ilegal y keygens** como **HackTool.Win32.AutoKMS** y **PUA.Win32.KeyGen.CSAE**, que pueden representar un riesgo de malware oculto.
- **Presencia de criptomineros** (**PUA.BAT.CRYPTOMINER.C**) que pueden afectar el rendimiento y comprometer la seguridad de los equipos.
- **Software de administración remota no autorizado** (**PUA.Win32.RemoteAdmin.AK**) que podría facilitar accesos no controlados.



Top 10 Spyware/Grayware Detections

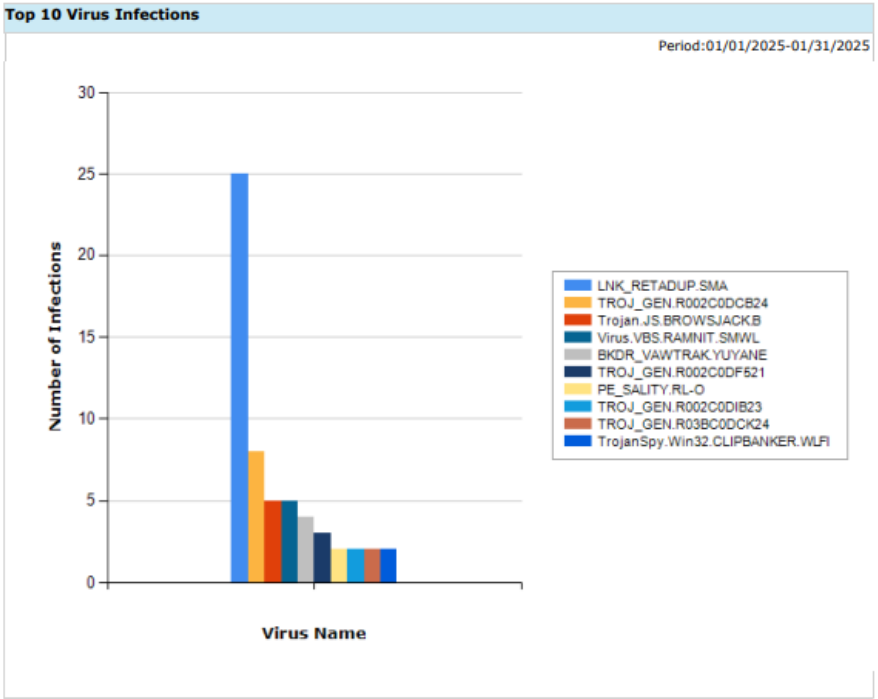
Spyware/Grayware Name	# of Detections	Detected By
PUA_SOFTPULSE_FA220020.UVPA	11	Desktop (11)
HackTool.Win32.AutoKMS.AUSYQ	3	Desktop (3)
HKTL_PKDUMP	3	Desktop (3)
PUA.BAT.CRYPTOMINER.C	2	Desktop (2)
PUA.Win32.HidCon.A	2	Desktop (2)
PUA.Win32.RemoteAdmin.AK	2	Desktop (2)
PUA.Win32.KeyGen.CSAE	1	Desktop (1)
PUA.Win32.OpenCandy.PCC	1	Desktop (1)
PUA.Win32.Patcher.PUSMANEABBS	1	Desktop (1)
PUA.Win32.Patcher.PUSMANEABCP	1	Desktop (1)

Tabla 102 Top spayware

4.7.4. Top 10 Virus Detectados

La información presentada detalla múltiples infecciones detectadas en equipos de escritorio (Desktop), relacionadas con diferentes tipos de malware. A continuación, se realiza un análisis de cada amenaza y los riesgos asociados:

- **LNK_RETADUP.SMA** con **25 detecciones**, un malware asociado a la propagación de troyanos a través de accesos directos.
- **Presencia de troyanos y backdoors:** Varias detecciones de **troyanos genéricos (TROJ_GEN)** y **BKDR_VAWTRAK.YUYANE**, que pueden comprometer credenciales y permitir accesos no autorizados.
- **Infección por virus polimórficos: PE_SALITY.RL-O** y **Virus.VBS.RAMNIT.SMWL**, conocidos por propagarse agresivamente y desactivar medidas de seguridad.
- **Amenazas de robo de información: TrojanSpy.Win32.CLIPBANKER.WLFI**, diseñado para interceptar datos sensibles, como credenciales bancarias.



Top 10 Virus Infections

Virus Name	# of Infections	Detected By
LNK_RETADUP.SMA	25	Desktop (25)
TROJ_GEN.R002C0DCB24	8	Desktop (8)
Trojan.JS.BROWSJACK.B	5	Desktop (5)
Virus.VBS.RAMNIT.SMWL	5	Desktop (5)
BKDR_VAWTRAK.YUYANE	4	Desktop (4)
TROJ_GEN.R002C0DF521	3	Desktop (3)
PE_SALITY.RL-O	2	Desktop (2)
TROJ_GEN.R002C0DIB23	2	Desktop (2)
TROJ_GEN.R03BC0DCK24	2	Desktop (2)
TrojanSpy.Win32.CLIPBANKER.WLFI	2	Desktop (2)

Ilustración 220 Top *infección virus*

4.7.5. Servicio de Vulnerabilidades

Se muestra un resumen de las actividades y procesos relacionados con la Gestión de Vulnerabilidades del segundo semestre realizadas en enero de 2025, sobre activos propios de la infraestructura tecnológica de MINTRABAJO.

Se llevó a cabo una socialización con los Ingenieros Mauricio Fernández y Caterin Lozano sobre las 98,030 vulnerabilidades detectadas en el escaneo de vulnerabilidades del presente año 2025. Durante la reunión, se discutieron los riesgos asociados con estas vulnerabilidades y se destacó que el parque tecnológico actual presenta cierto grado de obsolescencia.

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 Fernández, Caterinb 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 294 activos de TI.

En enero, se alcanzó un registro de 293 activos de TI (99 %) de la línea base documentada en la herramienta.

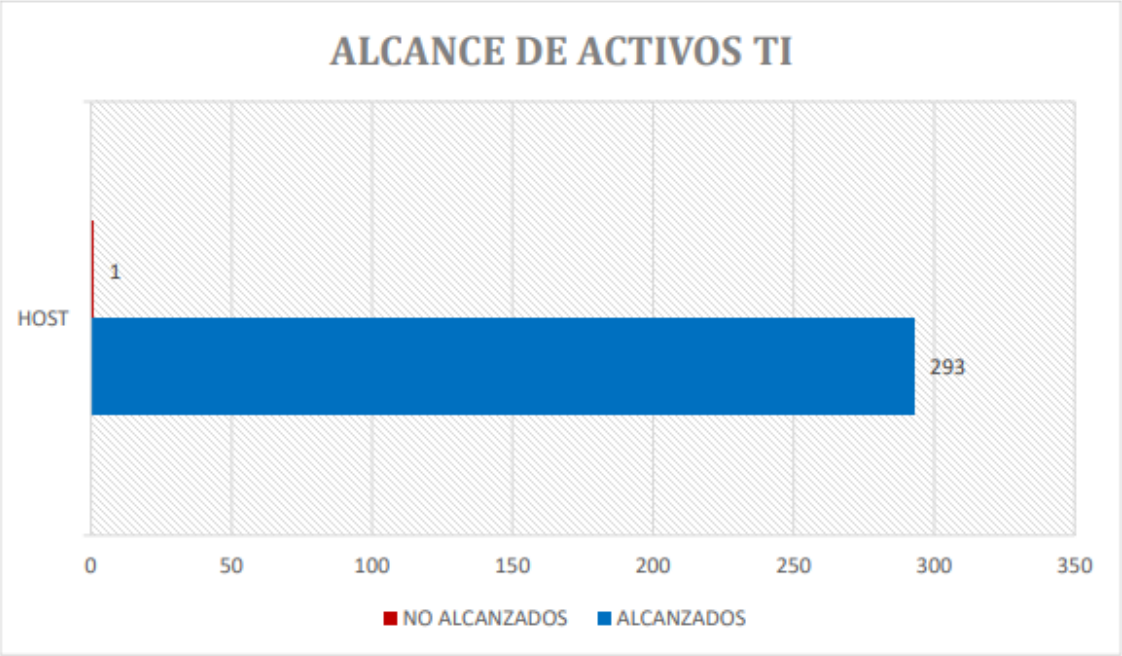
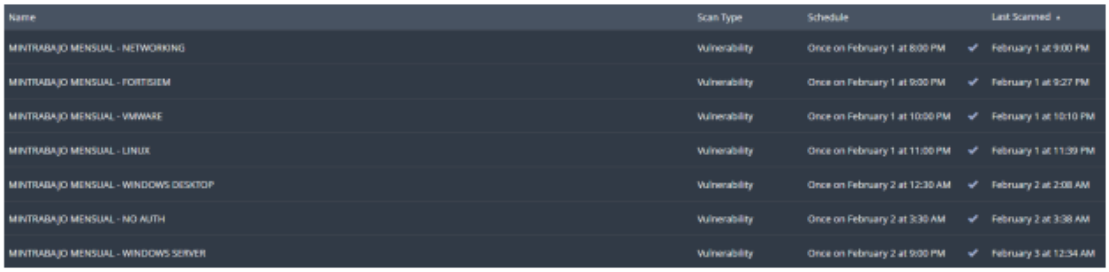


Ilustración 221 Gestión consola Nessus

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.
-



	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	1310	436

Tabla 103 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).

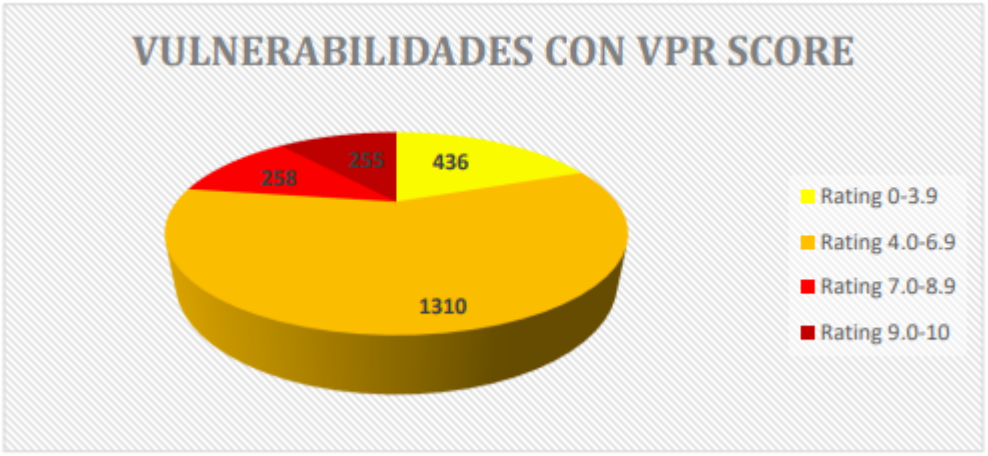


Ilustración 222 Puntuación VPR

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:

VULNERABILIDAD	PUNTUACIÓN VPR	CANTIDAD
KB5005573: Windows 10 Version 1607 and Windows Server 2016 September 2021 Security Update	10	60
KB5000853: Windows 8.1 and Windows Server 2012 R2 March 2021 Security Update	10	54
KB5005627: Windows 8.1 and Windows Server 2012 R2 September 2021 Security Update	10	52
KB5000851: Windows 7 and Windows Server 2008 R2 March 2021 Security Update	10	46
Rocky Linux 8 : git (RLSA-2024:4084)	9.9	15
Security Updates for Internet Explorer (March 2021)	10	4
Security Updates for Internet Explorer (September 2021)	10	4
Apache Log4j < 2.15.0 Remote Code Execution (Windows)	10	4
Amazon Linux AMI : java-1.8.0-openjdk, java-1.7.0-openjdk, java-1.6.0-openjdk (ALAS-2021-1553)	10	2
Apache Log4Shell RCE detection via Raw Socket Logging (Direct Check)	10	1

Tabla 104 TOP 10 - Activos más explotables

Durante el mes de enero el top 10 de vulnerabilidades explotables tienen las puntuaciones VPR más altas (10 y 9.9), sin embargo, la que más tiene presencia en la infraestructura corresponde a “KB5005573: Windows 10 Version 1607 and Windows Server 2016 September 2021 Security Update”, la cual hace alusión a que hay activos TI con sistema operativo Windows Server 2016 pendientes por la actualización de seguridad de septiembre 2021, por lo que es bastante antigua la vulnerabilidad, lo que justifica la puntuación VPR tan alta. Sin embargo, actualmente el entorno Windows Server 2016 se encuentra en proceso de migración a 2022, de tal forma que se remediarían 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

Durante el mes de enero, se gestionaron un total de 399 vulnerabilidades TI, en las severidades:

63 vulnerabilidades críticas.
73 vulnerabilidades altas.

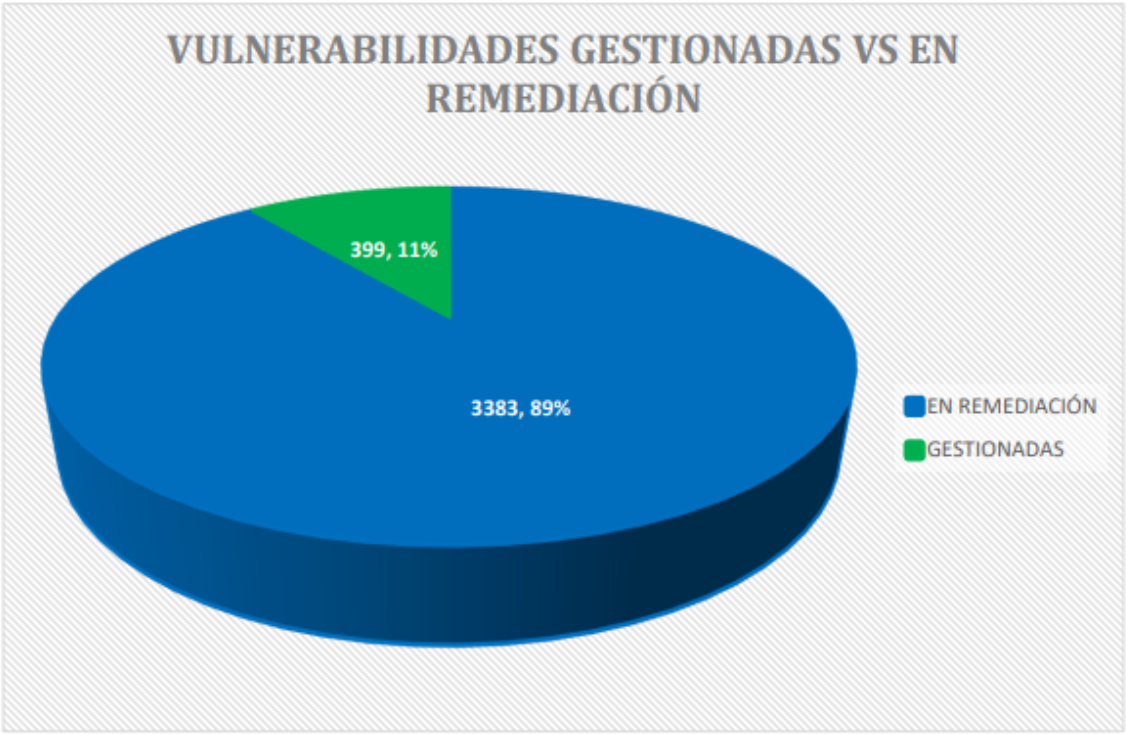


Ilustración 223 Vulnerabilidades gestionadas vs en remediación

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 enero, se llevó a cabo la socialización de la actividad de **Ethical Hacking** primer semestre 2025 que se ejecutara durante los próximos meses, liderada por el equipo de especialistas del **SOC (Centro de Operaciones de Ciberseguridad)**.

Se socializó el plan de pruebas a realizar con la herramienta BloodHound, cuyo objetivo es identificar vulnerabilidades en los controladores de Active Directory. Durante la sesión, se explicó la metodología a emplear y se destacó la importancia de este análisis para fortalecer la seguridad del directorio. Asimismo, se informó que se proporcionarán actualizaciones sobre el progreso y los resultados en las próximas reuniones.

- **Medición de ANS Antivirus**

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

ID	Indicadores	Resultado	Meta
AV-1	Cobertura de antivirus	97,49%	95,00%
AV-2	Continuidad y disponibilidad de la plataforma	100%	98,00%
AV-3	Cumplimiento en la entrega del informe de gestión mensual	100%	100,00%

Tabla 105 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 224 Criterios calidad documental casos

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

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

Tabla 106 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 enero, se realizó la evaluación cuantitativa de la muestra de 331 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:

Ítems Evaluados	Error No Critico Cometidos	% de Cumplimiento
1. Tipo de caso	6	99,9%
2. Asunto	0	100,0%
3. Descripción	6	99,9%
4. Prioridad	0	100,0%
5. Categoría	8	99,8%
6. Escalamiento	1	100,0%
7. Solución	14	99,7%
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	10	99,8%
13. Cumplimiento de ANS	1	100,0%

Tabla 107 Errores cometidos

Se identificaron 46 errores con un porcentaje de cumplimiento consolidado de 98,93%.

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 14 errores en el ítem “Solución” lo que corresponde a 99.70% de cumplimiento; 10 errores en el ítem “Ortografía y redacción” que corresponde al 99.80% de cumplimiento y 8 errores en el ítem “categoría” que corresponde al 99.80% de cumplimiento.

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

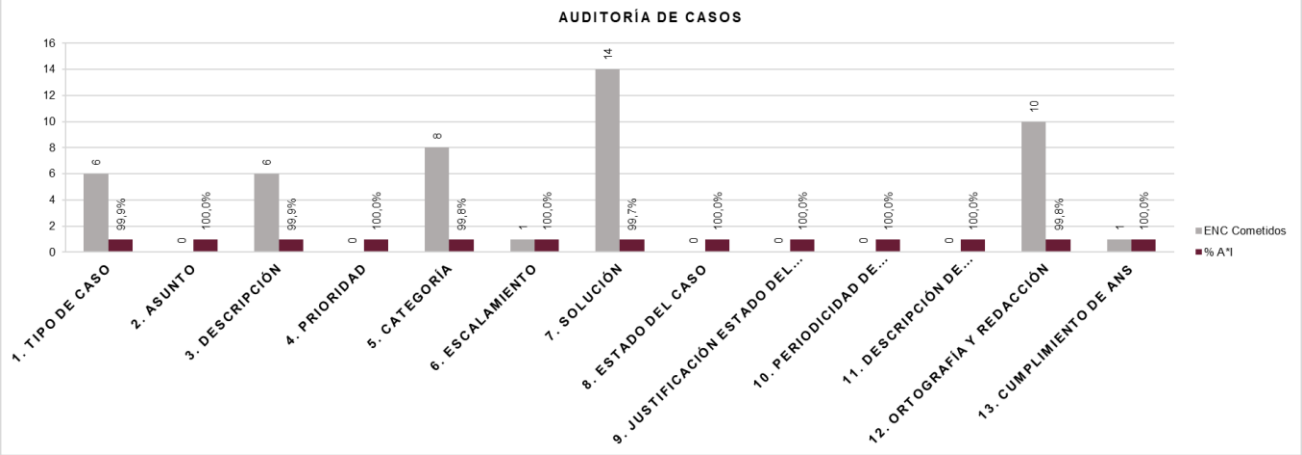


Ilustración 225 Resultados auditoria de casos

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 226 Precisión error no Critico de llamadas

PRECISIÓN ERROR CRÍTICO – PEC

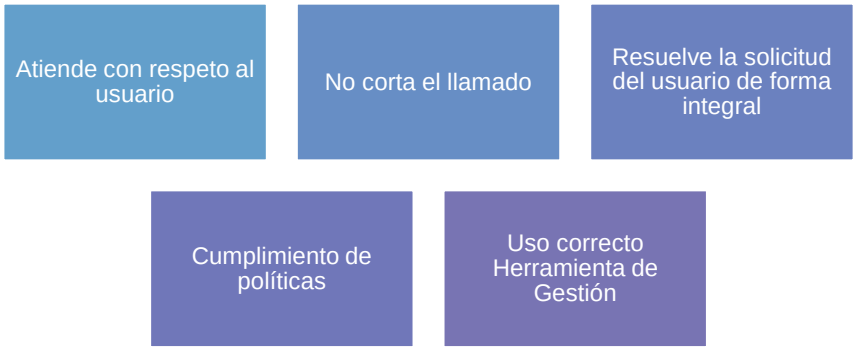


Ilustración 227 Precisión error Critico de llamadas

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

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

PRECISIÓN ERROR NO CRÍTICO – PENC

Criterios	Parámetros
Bienvenida y Personalización	- Se evalúa que el agente cumpla con los protocolos de llamada al inicio da la bienvenida al usuario a la línea telefónica y se presenta correctamente. - Se evalúa si el agente está tomando los datos asignados del usuario de forma eficiente, es decir, que el usuario no tenga que repetir varias veces la misma información. - Se evalúa que el agente verifique la identidad del usuario antes de realizar cualquier procedimiento
Escucha Activa	- Se evalúa que el agente esté atento en la llamada, atendiendo y preguntando los datos necesarios, de tal forma que el usuario no tenga que repetir información antes dada.
Retroalimentación y manejo de espera	- Se evalúa que el agente comunique al usuario que lo dejará un momento en línea. - Se evalúa que el agente no deje al usuario esperando en línea por más de dos minutos. Si las actividades que debe realizar duran mayor tiempo el agente debe retomar e informar al usuario los procedimientos que está realizando. - Se evalúa que el agente comunique al usuario su agradecimiento por su espera en línea. - Se evalúa que el agente aplique el mute en la llamada cuando requiera que el usuario espere un momento.

Criterios	Parámetros
Empatía y adaptabilidad al usuario	- Se evalúa que el agente en la llamada mantenga respeto, amabilidad y empatía con el usuario al momento de atender la solicitud. - Se evalúa si el agente mantiene un tono de voz adecuado, además si la información que suministra al usuario es clara y entendible utilizando un vocabulario adecuado.
Proceso técnico y/o lineamientos	- Se evalúa que el agente comunique eficazmente la información al usuario, para que conozca las actividades realizadas y el estado de su solicitud. - Se evalúa si se evidencia que el asesor posee agilidad en la consulta y en el manejo de los aplicativos y procedimientos
Asegura y Despedida	- Se evalúa si el agente informa al usuario el número de ticket generado. - Se evalúa que el agente cumpla con el protocolo de despedida

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 108 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 109 Calificación Calidad llamadas

5.4 Evaluación de calidad de llamadas

En el mes de enero 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	ENERO 2025	%
Escucha Activa	0	100%
Retroalimentación y manejo de esperas	2	100%
Empatía y adaptabilidad al usuario	1	100%
Asegura y Despedida	0	100%
Bienvenida y Personalización	1	100%
Soporte Primer Nivel	0	100%

PRECISIÓN ERROR CRÍTICO - PEC	ENERO 2025	%
Uso correcto Herramienta de Gestión	8	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%

Una vez realizada la revisión individual de las llamadas, se realiza el siguiente análisis frente a los resultados de las 26 llamadas evaluadas:

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

- Retroalimentación y manejo de espera: Mantiene al usuario informado sobre las gestiones que está realizando
- Empatía y adaptabilidad al usuario: Se adapta al usuario y a la situación presentada.
- Bienvenida y Personalización: Utilizar el saludo de acuerdo con el script de atención de la mesa de forma completa y correcta, conociendo el nombre del usuario y lo utiliza por lo menos al comienzo y al final de la conversación. No deben pasar más de 5 segundos sin realizar la bienvenida

Se presentaron en la categoría de errores críticos por los siguientes criterios:

- Uso correcto Herramienta de Gestión: Ingreso del ticket en la herramienta de registros Ingreso correcto y completo en la herramienta de registros.

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

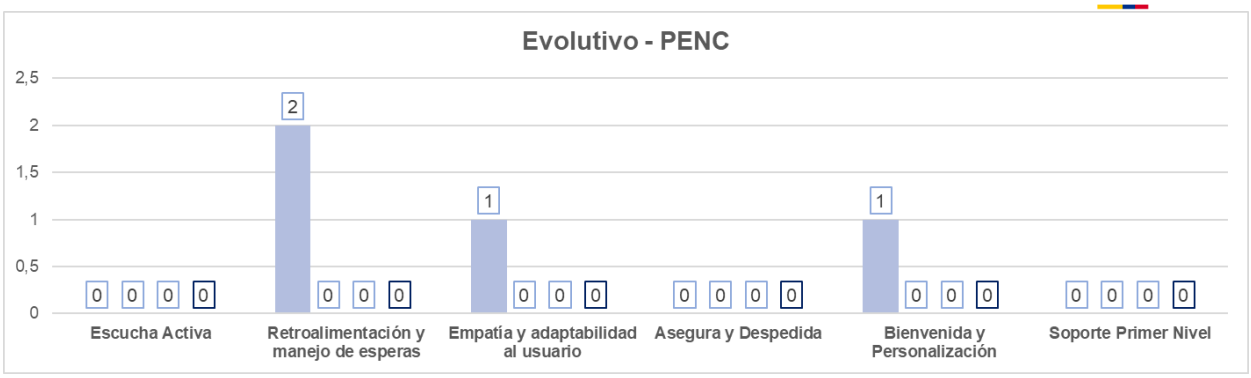


Ilustración 228 Resultados llamadas PENC

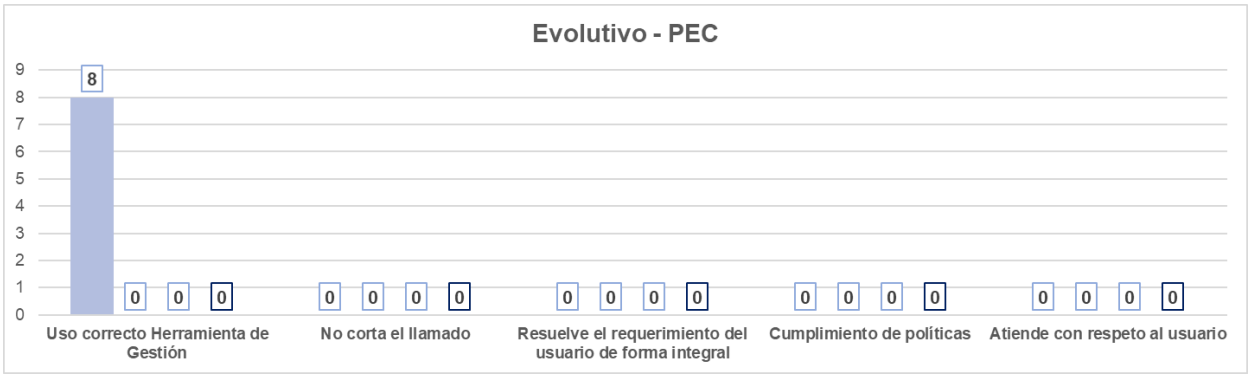


Ilustración 229 Resultados llamadas PEC

5.5 Mejora Encuesta de Satisfacción de Aranda

El equipo de procesos trabajo en una iniciativa de mejora de las preguntas de la encuesta de satisfacción de Aranda, con el propósito de ser más claros frente a las respuestas y obtener mayor información de la percepción del usuario final. Se hizo revisión conjunta de la propuesta y finalmente fue aprobada a nivel interno por la líder de línea y gerente del proyecto para ser aplicada a partir del 02/01/2025.

A continuación, se presenta la lista de preguntas definidas con sus opciones de respuesta:

1. ¿Qué tan fácil fue utilizar los canales de contacto de la Mesa de Servicios?
Responda la pregunta en una escala de 1 a 5, donde 1 significa muy difícil y 5 muy fácil.

2. ¿Cuál es el grado de satisfacción con el servicio brindado por los agentes de la Mesa de Servicios?
Responda la pregunta en una escala de 1 a 5, donde 1 significa nada satisfecho y 5 totalmente satisfecho

3. ¿Las personas que atendieron su solicitud demostraron el conocimiento y experiencia necesarios para resolverla?
Responda la pregunta en una escala de 1 a 5, donde 1 significa que la atención fue mala y 5 que la atención fue excelente.

4. ¿La atención recibida en la solicitud fue amable y cortes?
Respuesta SI y NO

5. ¿Se logró resolver de manera oportuna su solicitud? (Se habilita con el campo de Justificación)
Respuesta SI y NO

En caso de que su respuesta es NO, por favor indíquenos ¿por qué?

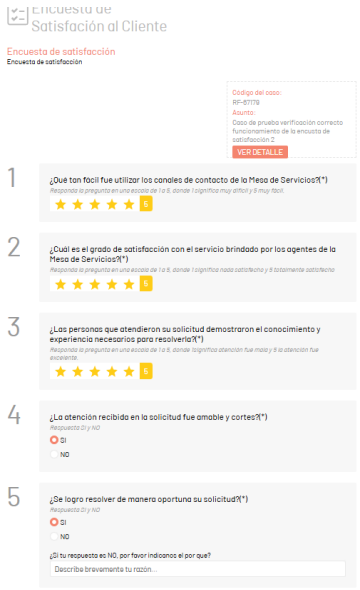


Ilustración 230 Nueva Encuesta de Satisfacción Aranda

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 polizas 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 correspondiente
Todos	Ausencia del personal asignado	Ausencia del personal, encargado de gestionar, administrar y operar los servicios.	NO	El personal asignado estuvo disponible durante el periodo.

Todos	Imposibilidad de acceso a la Herramienta de Gestión Aranda	Falla de acceso a la herramienta de gestión.	NO	La herramienta de gestión ha estado disponible
Eventos/ servicio de monitoreo	Imposibilidad de acceso a la Herramienta de monitoreo (Zabbix)	Falla de acceso a la herramienta de monitoreo	NO	La herramienta de gestión ha estado disponible
Mesa de servicios	Problemas de funcionalidad en la cuenta de soportemt@mintrabajo.gov.co.	Falla en el acceso y/o sincronización del correo soportemt@mintrabajo.gov.co	NO	El correo electrónico institucional ha estado disponible
Mesa de servicios	Imposibilidad de contacto por la línea telefónica de la mesa de servicios	Falla en el ingreso de las llamadas a la mesa de servicios	NO	La línea telefónica ha estado disponible
Mesa de servicios	Desborde de solicitudes (vía correo electrónico y/o llamadas) en la Mesa de Servicios	Aumento eventual de la cantidad de solicitudes que supera la capacidad de atención de los Agentes de la Mesa de servicios	NO	No se ha presentado desborde de solicitudes
Mesa de servicios	Riesgo de seguridad de la información que comprometan la confidencialidad, integridad o disponibilidad de la información.	Posibilidad de uso indebido de la cuenta genérica del cliente asignada para la Mesa de servicios	NO	No se ha presentado dicha situación.
Soporte en sitio	Incumplimiento de los compromisos pactados por atención de actividades urgentes - no planeadas	Solicitud de realización de actividades urgentes no planeadas que afectan la prestación del servicio de acuerdo con lo planeado	NO	No se ha presentado dicha situación.
Todas las prácticas	Deficiencias en la adopción de las prácticas de ITIL	Resistencia a la adopción de las prácticas de ITIL por las partes interesadas	NO	Se proporcionó capacitación a los involucrados
Práctica de Activos	Posibilidad de pérdida de inventario	La pérdida de inventario se produce cuando las cantidades reales del inventario son inferiores a las registradas en el módulo de gestión	NO	Se realizó seguimiento con el equipo de trabajo para revisar el inventario en la herramienta de gestión
Todos	Ausencia del personal asignado	Ausencia del personal, encargado de gestionar, administrar y operar los servicios.	NO	El personal asignado estuvo disponible durante el periodo.
Todos	Indisponibilidad de la nube privada que afecte la prestación de servicios de TI	Falla en la prestación de los servicios de TI por falla en la infraestructura de TI provista por la UT	NO	Se dispuso de la infraestructura y recursos que soportan las estrategias de contingencia y recuperación. El suministro del servicio de energía eléctrica fue normal en los sitios alternos. Se realización copias de respaldo de las bases de datos, información y

				sistemas de información se realiza de acuerdo con la política institucional de copias de respaldo.
Todos	Pérdida de información	Falla en la generación de las copias de respaldo de la información centralizada	NO	Se realizan pruebas de restauración de backups generados por la herramienta definida para el proyecto
Todos	Pérdida de disponibilidad	Perdida de disponibilidad de la infraestructura que soporta los servicios y activos de información de TI	NO	No se ha presentado dicha situación.
Todos	Pérdida de integridad	La ausencia de actualizaciones de seguridad en las aplicaciones podría poner en riesgo la integridad y disponibilidad de los sistemas, permitiendo la ejecución de código malicioso.	NO	Se realizó la planeación del primer ejercicio de Ethical Hacking. Se ejecutaron de manera oportuna y permanente las actualizaciones y controles necesarios para remediar las vulnerabilidades detectadas durante las pruebas de seguridad.
DRP	Indisponibilidad de servicios de TI	Indisponibilidad de la Infraestructura principal alojada en Datacenter Cirion Colombia XV	NO	Se dispuso de la infraestructura y recursos que soportan las estrategias de contingencia y recuperación. El suministro del servicio de energía eléctrica fue normal en los sitios alternos. Se realización de copias de respaldo de las bases de datos, información y sistemas de información se realiza de acuerdo con la política institucional de copias de respaldo.

Servicios centrales Servicios en sede	Fallas en los servicios de TI que afecten las actividades de la entidad producto realizar cambios no programados	Presentación de incidentes en la infraestructura tecnologica	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 110 Seguimiento a riesgos

7. BOLSA DE RECURSOS

Para el período del informe no se presentaron valores asociados a la 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	99,28%	95,00%
	Tiempo de solución de incidentes por soporte en sitio	96,02%	90,00%
	Tiempo de solución de requerimientos por soporte en sitio	99,83%	90,00%
	Tiempo de respuesta de la mesa de servicio	87,99%	85,00%
	Abandono de llamadas	0,72%	Máximo 8,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Equipos de usuario final	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
ANTIVIRUS	Cobertura de antivirus	97,49%	95,00%
	Continuidad y disponibilidad de la plataforma	100,00%	98,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
LAN y WLAN	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Energía Regulada	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Cumplimiento en la entrega del informe de gestión mensual	100,00%	100,00%
Datacenter	Tiempo de solución de requerimientos de garantía	100,00%	90,00%
	Continuidad y disponibilidad del datacenter principal	100,00%	99.95%
	Continuidad y disponibilidad del datacenter alterno	100,00%	99,60%
	Continuidad y disponibilidad de la plataforma de procesamiento, almacenamiento y respaldo	100,00%	99,70%
	Tiempo de solución de incidentes asociado a los servicios de aplicaciones especializadas	100,00%	90,00%
	Tiempo de solución de requerimientos asociado a los servicios de aplicaciones especializadas	100,00%	90,00%
	Continuidad y disponibilidad de los servicios de directorio activo	100,00%	99,60%
	Continuidad y disponibilidad de los servicios de seguridad informática	100,00%	99,90%
	Tiempo de solución de incidentes asociado a los servicios de administración, soporte y monitoreo	95,29%	90,00%
	Tiempo de solución de requerimientos asociado a los servicios de administración, soporte y monitoreo	99,84%	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	99,97%	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%

Área	Nombre Indicador	Resultado	Meta
	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 111 Medición de Acuerdos de Niveles de Servicio enero 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
- Cuotas enero
- detalle_llamadas_recibidas_(01.01.2025-30.01.2025)

FIN DEL DOCUMENTO