

## ANÁLISIS DE LAS CONEXIONES ENTRE ESTACIONES DE TRABAJO CAJA / TÁCTIL

Se evidencia en los archivos logs de la aplicacion administrativa y POS que se presentan desconexiones en la base de datos

[illegible]

13:49:56.203 -> TFrDocumento\_Espacio.SERVIDORExecute, Connection Closed Gracefully.  
 13:49:56.203 -> TFrDocumento\_Espacio.SERVIDORExecute, Connection Closed Gracefully.  
 13:49:56.203 -> TFrDocumento\_Espacio.SERVIDORExecute, Connection Closed Gracefully.  
 13:49:56.203 -> TFrDocumento\_Espacio.SERVIDORExecute, Connection Closed Gracefully.  
 13:49:56.203 -> TFrDocumento\_Espacio.SERVIDORExecute, Connection Closed Gracefully.  
 13:49:56.203 -> TFrDocumento\_Espacio.SERVIDORExecute, Connection Closed Gracefully.  
 13:49:56.203 -> TFrDocumento\_Espacio.SERVIDORExecute, Connection Closed Gracefully.  
 13:49:56.203 -> TFrDocumento\_Espacio.SERVIDORExecute, Connection Closed Gracefully.  
 13:49:56.203 -> TFrDocumento\_Espacio.SERVIDORExecute, Connection Closed Gracefully.  
 13:49:56.203 -> TFrDocumento\_Espacio.SERVIDORExecute, Connection Closed Gracefully.  
 13:49:56.219 -> TFrDocumento\_Espacio.SERVIDORExecute, Connection Closed Gracefully.  
 13:49:56.219 -> TFrDocumento\_Espacio.SERVIDORExecute, Connection Closed Gracefully.  
 13:49:56.219 -> TFrDocumento\_Espacio.SERVIDORExecute, Connection Closed Gracefully.  
 13:49:56.219 -> TFrDocumento\_Espacio.SERVIDORExecute, Connection Closed Gracefully.  
 13:49:56.219 -> TFrDocumento\_Espacio.SERVIDORExecute, Connection Closed Gracefully.  
 13:49:56.219 -> TFrDocumento\_Espacio.SERVIDORExecute, Connection Closed Gracefully.  
 13:49:56.219 -> TFrDocumento\_Espacio.SERVIDORExecute, Connection Closed Gracefully.  
 13:49:56.219 -> TFrDocumento\_Espacio.SERVIDORExecute, Connection Closed Gracefully.  
 13:49:56.219 -> TFrDocumento\_Espacio.SERVIDORExecute, Connection Closed Gracefully.  
 13:49:56.219 -> TFrDocumento\_Espacio.SERVIDORExecute, Connection Closed Gracefully.  
 13:49:56.219 -> TFrDocumento\_Espacio.SERVIDORExecute, Connection Closed Gracefully.  
 13:49:56.219 -> TFrDocumento\_Espacio.SERVIDORExecute, Connection Closed Gracefully.

## **ESTACION CAJA**

Se evidenció a través de visor de eventos de Windows que tiene fallas el sistema operativo, como se muestra a continuación

### **Aplicaciones base del sistema operativo**

Nombre de la aplicación con errores: mmc.exe, versión: 10.0.10240.16384, marca de tiempo: 0x559f3976  
 Nombre del módulo con errores: KERNELBASE.dll, versión: 10.0.10240.16384, marca de tiempo: 0x559f38c3  
 Código de excepción: 0xe0434352  
 Desplazamiento de errores: 0x000000000002a1c8  
 Identificador del proceso con errores: 0x1020  
 Hora de inicio de la aplicación con errores: 0x01d64d8302e5f55b  
 Ruta de acceso de la aplicación con errores: C:\Windows\system32\mmc.exe  
 Ruta de acceso del módulo con errores: C:\Windows\system32\KERNELBASE.dll  
 Identificador del informe: 02a934e6-5460-48c5-88a9-f48980768180  
 Nombre completo del paquete con errores:  
 Identificador de aplicación relativa del paquete con errores:

### **Aplicaciones de seguridad de Windows**

El servicio de protección de software se programó correctamente para reiniciarse a las 2020-06-28T19:51:22Z. Motivo: RulesEngine.

### **Aplicaciones de autenticación y activación de Windows**

Error de la activación de licencia (slui.exe) con el siguiente código:  
 hr=0xC004F074  
 Argumentos de línea de comandos:  
 RuleId=502ff3ba-669a-4674-bbb1-601f34a3b968;Action=AutoActivateSilent;AppId=55c92734-d682-4d71-983e-d6ec3f16059f;SkuId=2de67392-b7a7-462a-b1ca-108dd189f588;NotificationInterval=1440;Trigger=UserLogon;SessionId=1

El motor de reglas informó de una activación de VL con errores.

Motivo:0xC004F074

Id. aplicación = 0ff1ce15-a989-479d-af46-f275c6370663, id. SKU = b13afb38-cd79-4ae5-9f7f-eed058d750ca

Desencadenador=UserLogon(1)

Error de la activación de licencia (slui.exe) con el siguiente código:

hr=0x8007139F

Argumentos de línea de comandos:

RuleId=502ff3ba-669a-4674-bbb1-601f34a3b968;Action=AutoActivateSilent;AppId=55c92734-d682-4d71-983e-d6ec3f16059f;SkuId=2de67392-b7a7-462a-b1ca-108dd189f588;NotificationInterval=1440;Trigger=NetworkAvailable

### **Aplicaciones de permisos y ejecución de Windows**

El motor de reglas informó de una activación de VL con errores.

Motivo:0xC004F074

Id. aplicación = 0ff1ce15-a989-479d-af46-f275c6370663, id. SKU = b13afb38-cd79-4ae5-9f7f-eed058d750ca

Desencadenador=NetworkAvailable

Performance counter shared memory setup failed with error -1. Reinstall sqlctr.ini for this instance, and ensure that the instance login account has correct registry permissions.

El motor de reglas informó de una activación de VL con errores.

Motivo:0xC004F074

Id. aplicación = 0ff1ce15-a989-479d-af46-f275c6370663, id. SKU = b13afb38-cd79-4ae5-9f7f-eed058d750ca

Desencadenador=TimerEvent

El sistema no puede encontrar el dispositivo especificado.

El servicio Programador de tareas encontró un error de configuración en la definición de NT TASK\OneDrive Standalone Update Task-S-1-5-21-779016508-2519227926-2058462369-1001. Datos adicionales: Valor del error: %localappdata%\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe.

El servicio Programador de tareas encontró un error de configuración en la definición de NT TASK\AutoKMS. Datos adicionales: Valor del error: C:\Windows\AutoKMS\AutoKMS.exe.

El servicio Sincronizar host\_Session2 terminó inesperadamente. Esto se ha repetido 1 veces. Se realizará la siguiente acción correctora en 10000 milisegundos: Reiniciar el servicio.

### **ESTACION TACTIL**

Ademas se evidencio apliaciones en la estacion tactil con aplicaciones y servicios desconocidos que el sistema pueda presentar anomalias

WebClient		Cliente web	Detenido	LocalService
Wecsvc		Recopilador de eventos de Windows	Detenido	NetworkService
WEHOSTSVC		Servicio host de proveedor de cifrado de Windows	Detenido	WepHostSvcGr...
wercplsupport		Ayuda del Panel de control de Informes de problemas y soluciones	Detenido	netsvcs
WerSvc		Servicio Informe de errores de Windows	Detenido	WerSvcGroup
WFDSConMgrSvc		Servicio de administrador de conexiones con servicios Wi-Fi Direct	Detenido	LocalServiceN...
WiaRpc		Eventos de adquisición de imágenes estáticas	Detenido	LocalSystemN...
WinDefend	4500	Servicio de Antivirus de Windows Defender	En ejecución	
WinHttpAutoProxySvc	2856	Servicio de detección automática de proxy web WinHTTP	En ejecución	LocalServiceN...
Winmgmt	2360	Instrumental de administración de Windows	En ejecución	netsvcs
WinRM		Administración remota de Windows (WS-Management)	Detenido	NetworkService
wisvc		Servicio de Windows Insider	Detenido	netsvcs
WlanSvc	3628	Configuración automática de WLAN	En ejecución	LocalSystemN...
wlidsvc	10776	Ayudante para el inicio de sesión de cuenta Microsoft	En ejecución	netsvcs
wlpassvc		Servicio de asistente para perfil local	Detenido	LocalServiceN...
WManSvc		Servicio de administración de Windows	Detenido	netsvcs
wmiApSrv		Adaptador de rendimiento de WMI	Detenido	
WMPNetworkSvc		Servicio de uso compartido de red del Reproductor de Windows Media	Detenido	
workfoldersvc		Carpetas de trabajo	Detenido	LocalService
WpcMonSvc		Control parental	Detenido	LocalService
WPDBusEnum		Servicio enumerador de dispositivos portátiles	Detenido	LocalSystemN...
WpnService	4560	Servicio del sistema de notificaciones de inserción de Windows	En ejecución	netsvcs
WpnUserService		Servicio de usuario de notificaciones de inserción de Windows	Detenido	UnistackSvcGr...
WpnUserService_1f9c4	2816	WpnUserService_1f9c4	En ejecución	UnistackSvcGr...
wscsvc	4424	Centro de seguridad	En ejecución	LocalServiceN...
WSearch	5608	Windows Search	En ejecución	
wuauerv		Windows Update	Detenido	netsvcs
WwanSvc		Configuración automática de WWAN	Detenido	LocalSystemN...
XblAuthManager		Administración de autenticación de Xbox Live	Detenido	netsvcs
XblGameSave		Partida guardada en Xbox Live	Detenido	netsvcs
XboxGipSvc		Xbox Accessory Management Service	Detenido	netsvcs
XboxNetApiSvc		Servicio de red de Xbox Live	Detenido	netsvcs

Nombre	PID	Descripción	Estado	Grupo
PimIndexMaintenanceSvc		Datos de contactos	Detenido	UnistackSvcGr...
PimIndexMaintenanceSvc_...	9892	PimIndexMaintenanceSvc_1f9c4	En ejecución	UnistackSvcGr...
plh		Registros y alertas de rendimiento	Detenido	LocalServiceN...
PlugPlay	960	Plug and Play	En ejecución	DcomLaunch
PNRPAutoReg		Servicio de publicación de nombres de equipo PNRP	Detenido	LocalServiceP...
PNRPsvc		Protocolo de resolución de nombres de mismo nivel	Detenido	LocalServiceP...
PolicyAgent	4008	Agente de directiva IPsec	En ejecución	NetworkServic...
Power	984	Energía	En ejecución	DcomLaunch
PrintNotify		Extensiones y notificaciones de impresora	Detenido	print
PrintWorkflowUserSvc		PrintWorkflow	Detenido	PrintWorkflow
PrintWorkflowUserSvc_1f9c4		PrintWorkflowUserSvc_1f9c4	Detenido	PrintWorkflow
ProfileSvc	1181	Servicio de perfil de usuario	En ejecución	netsvcs
PushToInstall		Servicio PushToInstall de Windows	Detenido	netsvcs
QWAVE		Experiencia de calidad de audio y vídeo de Windows (qWave)	Detenido	LocalServiceA...
RasAuto		Administrador de conexiones automáticas de acceso remoto	Detenido	netsvcs
RasMan	5004	Administrador de conexiones de acceso remoto	En ejecución	netsvcs
RemoteAccess		Enrutamiento y acceso remoto	Detenido	netsvcs
RemoteRegistry		Registro remoto	Detenido	LocalService
ReportServerSQLEXPRESS		SQL Server Reporting Services (SQLEXPRESS)	Detenido	
RetailDemo		Servicio de prueba comercial	Detenido	rdxgroup
RmSvc		Servicio de administración de radio	Detenido	LocalServiceN...
RpcEptMapper	672	Asignador de extremos de RPC	En ejecución	RPCSS
RpcLocator		Ubicador de llamada a procedimiento remoto (RPC)	Detenido	
RpcSs	672	Llamada a procedimiento remoto (RPC)	En ejecución	rpcss
SamSs	836	Administrador de cuentas de seguridad	En ejecución	
SCardSvc		Tarjeta inteligente	Detenido	LocalServiceA

## POSIBLES CAUSAS DE LA INESTABILIDAD DE LAS ESTACIONES

1. Actualizaciones de windows, que afectan la activacion de windows, detectando anomalias en el licenciamiento, limitando las funcionalidades del mismo como desconexiones de red, aplicaciones y servicios no ejecuten correctamente,

2. Posible spyware o aplicaciones piratas que se auto actualizan al descargar algun contenido de internet que pueden afectar el funcionamiento del sistema operativo

**Recomendaciones:**

1. Instalacion de antivirus en las estaciones
2. Formateo o reinstalacion de Window para corregir posibles archivo corruptos

**Acciones para mejorar la funcionalidad, pero no corrige las anomalias totalmente**

1. Desactivar el ahorro de energia e hibernacion de las 2 estaciones
2. Depurar aplicaciones innecesarias en la estacion tactil