

			
PROCESO GESTIÓN DE INCIDENTES EN EL SERVICIO		Página Nro. 1 de 49	
PROCEDIMIENTO MONITOREO SERVICIOS Y RECURSOS NOC		Código Nro. PRO-GIS-P02	
<div style="text-align: center; padding: 100px 0;"> <p> PROTOCOLO DE TRABAJO VIRTUAL MONITOREO REMOTO DEL AGENTE DE EQUIPO DE MONITOREO SERVICIOS Y RECURSOS NOC Y/O PASANTE </p> </div> <div style="text-align: right; margin-top: 100px;"> APROBADO </div> <div style="text-align: center; margin-top: 50px;"> <div style="border: 1px solid black; width: 500px; height: 100px; margin: 0 auto;"></div> <p>JEFE DIV. ASEGURAMIENTO SERVICIOS Y RECURSOS</p> </div>			
ELABORADO		VERSIÓN Nº 1	
POR: Monitoreo de Servicios y Recursos NOC Ing. Gonzalo Arévalo Alarcón Ing. Aldo Muñoz Oilos Nicole Castro Paez (Pasante) Andrés Espinoza Soria (Pasante) Melissa Gonzales Zubieta Pasante)		POR:	
FECHA: Enero 2021		FECHA:	

ÍNDICE

1.- ANTECEDENTES.....	3
2.- PROTOCOLO DE TRABAJO DEL PERSONAL DE MSR NOC.....	4
3.- MANUAL DE USO Y FUNCIONAMIENTO DE GESTORES.....	12
4.- RECOMENDACIONES PARA EL PERSONAL DEL MSR NOC.....	50

I. ANTECEDENTES

a) ALCANCE

El presente documento protocolar de actividades de trabajo remoto (virtual) , está enfocado a las instrucciones y responsabilidades que un agente o pasante de “Monitoreo de Servicios y Recursos NOC” debe llevar a cabo en su turno.

b) OBJETIVOS

- Definir protocolos de trabajo remoto (virtual) atribuibles a la secuencia de actividades y responsabilidades de los agentes de “Monitoreo de Servicios y Recursos NOC”, igualmente para los pasantes dentro de este departamento.
- Mejorar por medio de directrices las condiciones de actividades de trabajo remoto durante un turno respectivo.
- Proporcionar una guía de trabajo que ayude al desarrollo de los procedimientos pertinentes a las actividades de monitoreo remoto (virtual o también denominado teletrabajo).

c) GLOSARIO

MSR NOC.- Monitoreo Servicios y Recursos NOC.

VPN.- Red privada virtual (Virtual Private Network).

ID.- Número de Identificación.

NOC.- Centro de operaciones de redes (Networking Operation Center).

ITU.- Informe de turno.

DAC.- Difusión de Apertura y Cierre.

DIN.- Difusión de Información.

MRTG.- (Multi Router Traffic Grapher).

DWDM.- (Dense Wavelength Division Multiplexing).

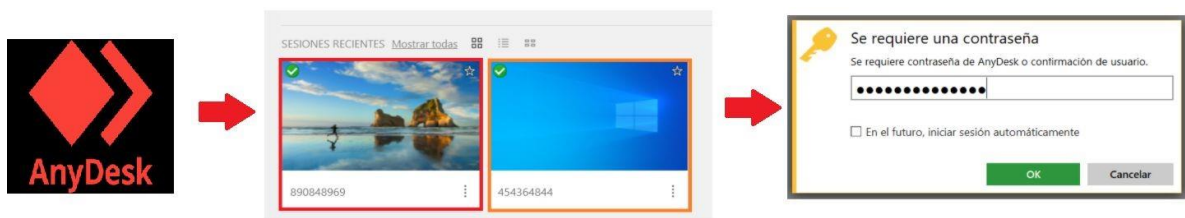
II. PROTOCOLO DE TRABAJO DEL PERSONAL MSR NOC

1. Inicio de trabajo virtual en turno

- a. Si se trata de un Agente de *“Monitoreo Servicios y Recursos NOC”* pasar al punto 1.0.
- b. Si se trata de un Pasante continúe con el paso 1.1.

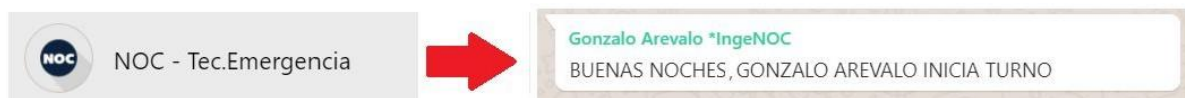
1.0. Proceda a conectarse con la VPN asignada como personal de Agente de *“Monitoreo Servicios y Recursos NOC”* de COMTECO, para conectarse remotamente a la máquina de trabajo. (pase al punto 1.2.)

1.1. Abrir y utilizar la plataforma AnyDesk, entrando con el número de computadora virtual y la contraseña proporcionada por el Jefe de Departamento, a cualquiera de las computadoras virtuales disponibles dentro el departamento de *“Monitoreo Servicios y Recursos NOC”* que representan las terminales de monitoreo para iniciar el trabajo remoto (virtual).



1.2. Indicar que se inicia el turno en el grupo de trabajo de WhatsApp *“NOC - Tec. Emergencia”*, utilizando la siguiente jerga ejemplo en los siguientes puntos.

- a. Si se trata de un Agente de *“Monitoreo Servicios y Recursos NOC”* colocar el inicio de la siguiente manera: “Saludo, (Nombre completo), inicia turno”.



- b. Si se trata de un pasante colocar de la siguiente manera: “Saludo, (Nombre completo) pasante, inicia turno”.






NOTA: este procedimiento es obligatorio, ya que, es controlado y registrado en Recursos Humanos.

1.3. Ingrese a su cuenta correspondiente en la aplicación “*Mantis*”, para proceder con la revisión del Informe de Turno (ITU) anterior.



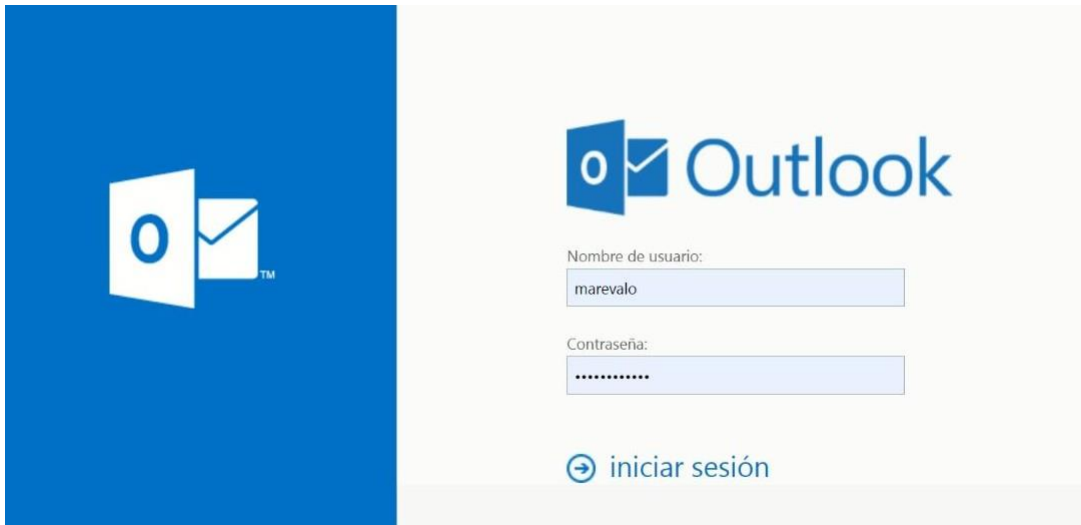
Inicio de sesión	
Usuario	<input type="text" value="marevalo"/>
Contraseña	<input type="password" value="....."/>
Recordar información de inicio de sesión	<input type="checkbox"/>
<input type="button" value="Iniciar sesión"/>	

1.4. Proceda al inicio de sesión en Outlook, de la cuenta de “*Monitoreo Servicios y Recursos NOC*” y verifique la recepción de correos que figuran desde el inicio de su turno.

	
	Nombre de usuario: <input type="text" value="noc"/>
	Contraseña: <input type="password" value="....."/>
	 iniciar sesión

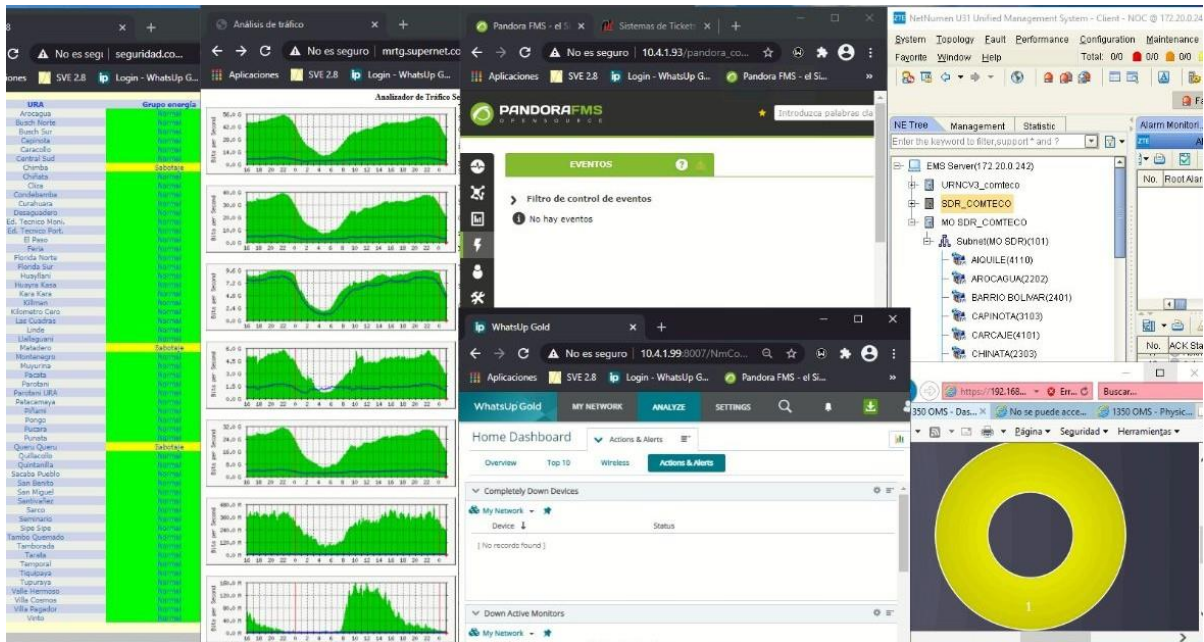
- a. En caso de no contar con correos correspondientes al turno, continúe con el paso 1.5.
- b. En caso de contar con correos correspondientes a trabajos pendientes, finalice el 1.5 y 1.6 para que posteriormente continúe con el paso 2.1

1.5. Proceda al inicio de sesión en Outlook:



- a. Si se trata de un Agente de “Monitoreo Servicios y Recursos NOC”, inicie sesión de *su cuenta personal de la empresa* en la plataforma de servicio de correo electrónico Outlook y verifique la recepción de correos.
- b. Si se trata de un pasante, inicie sesión de la cuenta para pasantes proporcionada por el Jefe de Departamento y verifique la recepción de correos.

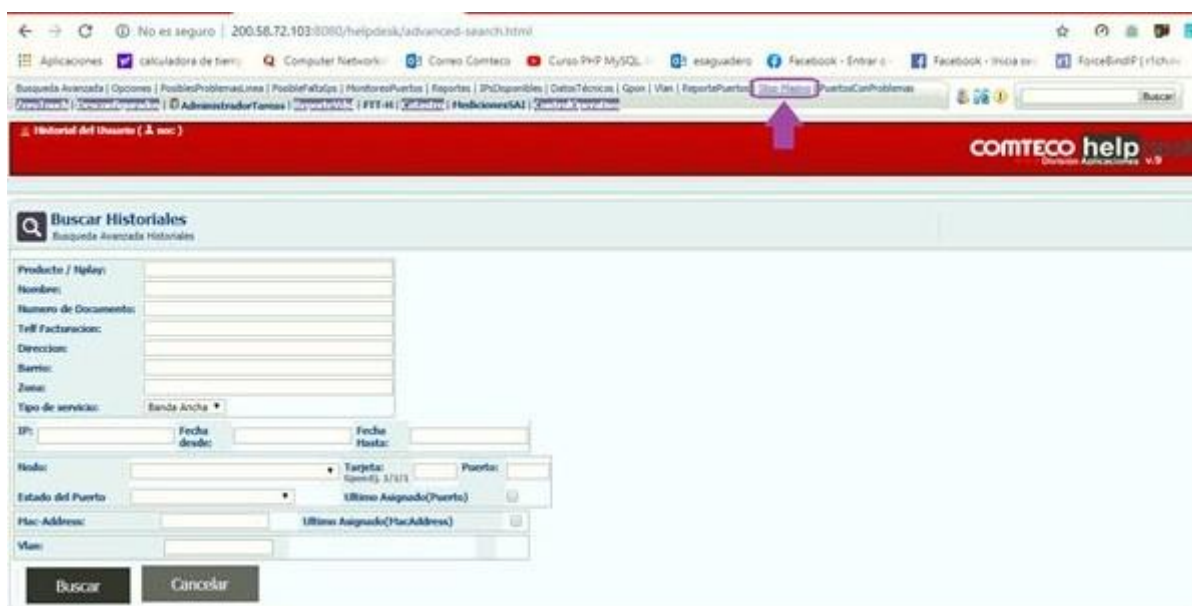
1.6. Proceda a ordenar la pantalla de monitoreo con los gestores de manera que sean visibles para la supervisión de alarmas. Por ejemplo:



NOTA: Mantenga abiertas las sesiones de Outlook, Mantis y Helpdesk durante su turno.

The screenshot displays a multi-monitor workstation with two applications open. The left monitor shows the Mantis Sistema de Tickets interface, which includes a list of incidents with columns for ID, Category, Severity, Status, Date, and Incident. The right monitor shows a webmail interface with an inbox and a list of emails.

ID	Categoría	Severidad	Estado	Fecha de Registro	Incidente
0015272	ITU	Calda Parcial	Enviada (Informe de Turno)	26-01-2021	Noche
0015271	ITU	Calda Parcial	Enviada (Informe de Turno)	26-01-2021	Tarde
0015270	ITU	Calda Parcial	Enviada (Informe de Turno)	26-01-2021	TURNOS MANANA
0015269	ITU	Calda Parcial	Enviada (Informe de Turno)	26-01-2021	Madrugada
0015268	ITU	Calda Parcial	Enviada (Informe de Turno)	25-01-2021	Noche
0015267	ITU	Calda Parcial	Enviada (Informe de Turno)	25-01-2021	Tarde
0015266	ITU	Calda Parcial	Enviada (Informe de Turno)	25-01-2021	TURNOS MAÑANA
0015265	ITU	Calda Parcial	Enviada (Informe de Turno)	25-01-2021	Madrugada



2. Monitoreo durante el turno

- a. En caso de no contar con trabajos pendientes en la previa revisión del Informe de Turno (ITU) anterior, continúe con el paso 2.4
- b. En caso de contar con trabajos pendientes en la previa revisión del Informe de Turno (ITU) anterior, continúe con el paso 2.1.

2.1. Realizar el seguimiento correspondiente a las indicaciones atribuibles a los trabajos (incidentes/alarmas de cualquier gestor, apertura o cierre de Tickets y recepción o envío de correos)

- a. En caso de tener pendiente el cierre de un DAC o DIN, continúe con el paso 2.2.
- b. En caso de no tener pendiente el cierre de ningún DAC o DIN, continúe con el paso 2.3

2.2. Ingresar a la aplicación “Mantis” al sector de DACs (Proyecto: 02 - Incidente DAC), ubicar el ID correspondiente al DAC abierto, en donde se encuentran todos los detalles e información respectiva al DAC, el cual estará escrita por el agente de un anterior turno previo al suyo.

NOTA: Del DAC, se abstrae información importante, detalles de: nombre del incidente, observaciones del agente o pasante (pequeño reporte de la notificación del incidente y con quienes se comunicó durante el mismo),

departamento responsable, que acciones tomo el agente de “*Monitoreo de Servicios y Recursos NOC*” en el turno en el que se presentó el incidente.

2.3. Con la información obtenida del DAC, se pide una actualización de la situación o problema al personal atribuible de la causa que pueden ser: Operadores, clientes, responsable perteneciente al departamento responsable de la alarma o problema por el que se generó el DAC. En caso esté pendiente de respuesta email del proveedor externo, se debe realizar el seguimiento hasta obtener la respuesta.

- a. Si es necesario, se debe hablar con el responsable que se encuentra pendiente de la situación y solicitar una actualización del estado del problema, con tal de complementar más información del problema/incidente con la opción de adjuntar notas al DAC (en estado: abierto) y así tener un informe con detalles y actualización constante.

NOTA: Como agente de turno, se debe preguntar al responsable del problema por parte de COMTECO, si hay necesidad de realizar un correo, proceder a contactar o realizar alguna acción que está dentro de las responsabilidades de un agente del departamento de “*Monitoreo Servicios y Recursos NOC*”. En caso del DAC, sea atribuible a Proveedores Externos, es importante complementar la información DAC, con respaldo de Fotografías (MRTG, incidentes externos en caso se tuviera.), correos, etc.

2.4. Verificar el estado de todos los gestores restantes: PANDORA, WhatsUP Gold!, MRTG, 4G, DWDM, HelpDesk, SVE (Seguridad Industrial). También, Correo electrónicos (ejm notifican ataques DDoS)

- a. Si se tiene alguna alarma en alguno de los gestores mencionados con anterioridad, debemos esperar un tiempo de 15 min. a excepción de las alarmas en los gestores de: DWDM, 4G y MRTG.

NOTA: Se esperan 15 min. como tiempo máximo para descartar y evitar la notificación de falsas alarmas, ya que, el tiempo de reinicio de la mayoría de los equipos es de 13 min. En caso la alarma sea menor del periodo mínimo para la notificación y este sea intermitente, debe también ser notificado. Siendo esto un aviso de una posible falla crítica.

- b. Por consiguiente, si se cumplió el tiempo de espera para descartar una falsa alarma, se procede a notificar dicha alarma o alarmas en el grupo de trabajo en Whatsapp “NOC - Tec.Emergencia”, mencionando al departamento

responsable a quien corresponde la alarma y al personal de turno de dicho departamento para que sea o sean atendidas a la brevedad posible.

NOTA: Para este paso es importante la recopilación de la información de la alarma como: la categorización, análisis, prueba de conectividad de la alarma, así como también verificar si se trata de un problema atribuible a un Cliente y/o Proveedor, esto con el fin de difundir efectivamente la notificación de la alarma al departamento o al proveedor de servicio correspondiente.

- c. Si no se tiene una respuesta pronta del departamento a quien compete la o las alarmas, se debe contactar al encargado de turno de forma personal e individual, para reafirmar la situación presentada y que se tomen las acciones competentes al caso.
- d. Si no se tiene una respuesta del encargado, ni de forma personal, contactarse con el Jefe del departamento responsable para que dicha persona tome cartas en el asunto.

NOTA: En el caso de no presentarse ningún incidente/alarma/problema, proceder a actualizar los gestores con regularidad y estar pendiente si se presentara algo (mensajes en el grupo de trabajo en Whatsapp: "NOC - Tec.Emergencia", correos en la cuenta específica de "*Monitoreo Servicios y Recursos NOC*" de Outlook, supervisión de estado activo de enlaces, incidencias/problemas/alarmas en los gestores).

3. Culminación de trabajo virtual en turno

3.1. Faltando 30 min. para finalizar el turno respectivo, se debe verificar el estado de cada uno de los gestores de: PANDORA, WhatsUP Gold!, MRTG, 4G, DWDM, HelpDesk, SVE (Seguridad Industrial), con la finalidad de prever posibles trabajos pendientes para el próximo turno de trabajo.

- a. Si no se presentan incidentes/alarmas/problemas, comenzar con la redacción del ITU correspondiente al turno actual. ver paso 3.2.
- b. Si se presenta incidentes/alarmas/problemas, ver el paso 2.4. a)

3.2. Ingresar a la aplicación "Mantis" al sector de ITU (Proyecto: 01 - Informe de Turno), seleccionando la opción de "Reportar Incidencia" para la apertura del nuevo ITU.

- a. Iniciando el ITU colocando el nombre del turno actual (Madrugada, Mañana, Tarde o Noche).
- b. Posteriormente se redactan todas las observaciones emitidas en el turno de trabajo respecto a los problemas, caídas y notificaciones importantes que se puede obtener en los grupos de apoyo existentes en WhatsApp, anotando la información oportuna de todos los eventos y problemas generados dentro del turno de trabajo.

3.3. Cualquier incidente/problema generado justo antes de finalizar el turno (5 min. a 1 min. antes), corresponde su notificación y observación respectiva añadida en el ITU y paralelamente corresponde a un accionar responsable del agente de turno, sin dejar dicha responsabilidad como un trabajo pendiente al siguiente turno.

3.4. Enviar este formulario al finalizar el turno, para que al inicio del siguiente turno el agente de "Monitoreo y Servicios NOC", proceda a leerlo e informarse de los precedentes del anterior turno.

3.5. Proceda a cerrar las sesiones de sus cuentas personales en Mantis y Outlook.

3.6. Indicar que se finaliza el turno en el grupo de trabajo de WhatsApp "NOC - Tec. Emergencia", utilizando la siguiente jerga ejemplo en los siguientes puntos.

- a. Si se trata de un Agente de "Monitoreo Servicios y Recursos NOC" colocar el inicio de la siguiente manera: "Despedida, (Nombre completo), finaliza turno".



- b. Si se trata de un pasante colocar de la siguiente manera: "Despedida, (Nombre completo) pasante, finaliza turno".



NOTA: este procedimiento es obligatorio, ya que, es controlado y registrado en Recursos Humanos.

III. MANUAL DE USO Y FUNCIONAMIENTO DE GESTORES

1. Inicialización de gestores y aplicaciones de monitoreo (Como ingresar o abrir los gestores)

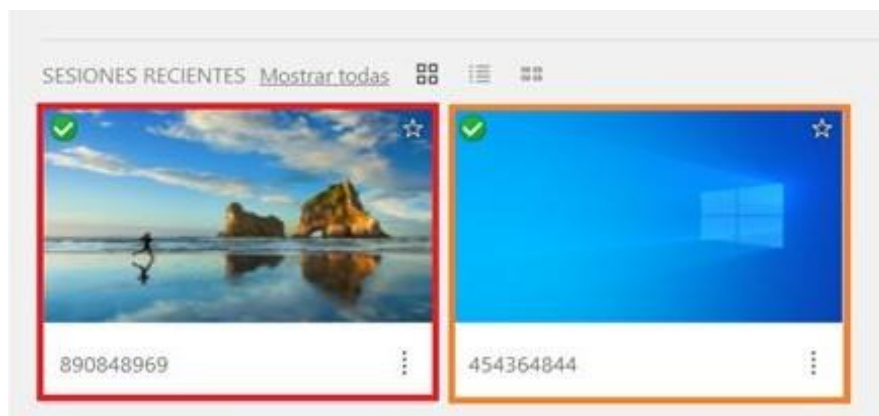
1.1. Anydesk

- a. Como primer paso, el agente debe tener descargado e instalado la aplicación oficial para trabajo remoto (virtual), la aplicación AnyDesk.



- b. El agente se debe proveer con el jefe del departamento, los números que representan las terminales virtuales asignadas, que permitirán ingresar remotamente a las computadoras físicas dentro del departamento de “Monitoreo Servicios y Recursos NOC”, en COMTECO.

Las computadoras virtuales disponibles con sus respectivos números son los que se muestran en la siguiente imagen:



El agente de turno debe ingresar a cualquiera de las dos terminales para poder acceder a la pantalla principal de monitoreo.

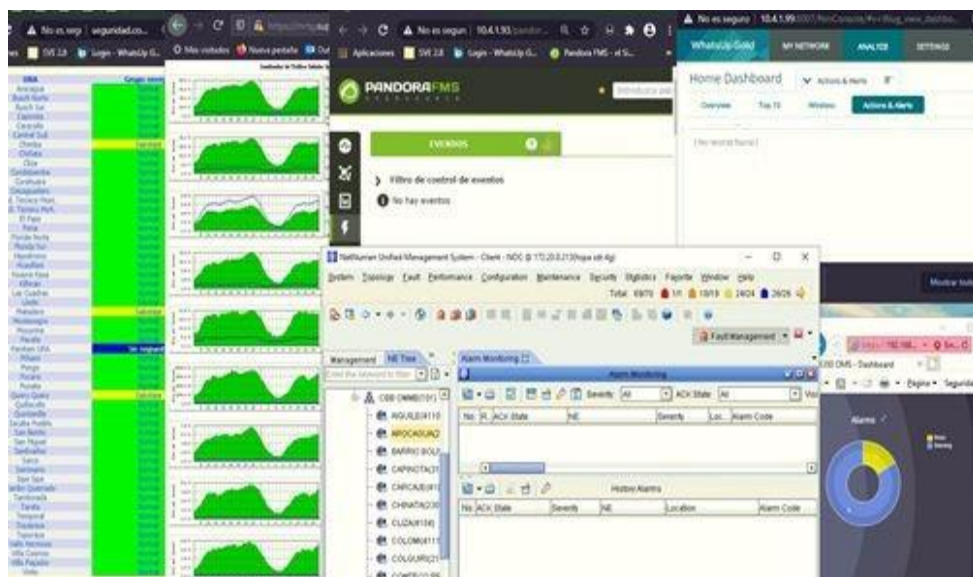
NOTA: El número asignado a la terminales pueden cambiar, en caso de un cambio, no dudar en solicitar información al jefe del departamento.

- c. Una vez ingresado a alguna de las computadoras virtuales, se le solicitará una contraseña que debe ser proporcionada por el jefe del departamento.



NOTA: La contraseña que brinde el jefe de departamento será la misma para ambas terminales virtuales.

- d. Cuando se logre cumplir con los anteriores pasos, el éxito del ingreso a una máquina terminal será la muestra de la pantalla principal de monitoreo general (si es que no se tienen los gestores cerrados).



1.2. Outlook

- Para poder utilizar la aplicación, dentro de un navegador se debe escribir **OUTLOOK** en el buscador o ingresar directamente a: <https://correo.comteco.com.bo/owa/#path=/mail>
- Con la ventana de la aplicación abierta, ingresar el usuario y contraseña correspondiente al "Monitoreo Servicios y Recursos NOC".

NOTA: El usuario y contraseña vigente debe ser proporcionado por el jefe del departamento.



1.3. Mantis

- a. Utilizando un navegador en la computadora se debe ingresar al siguiente link: <http://200.58.72.79/mantisnoc/view.php?id=14840>
- b. Dentro la interfaz de “Mantis” se debe ingresar el usuario y contraseña que cada agente del departamento posee, como cuenta propia.

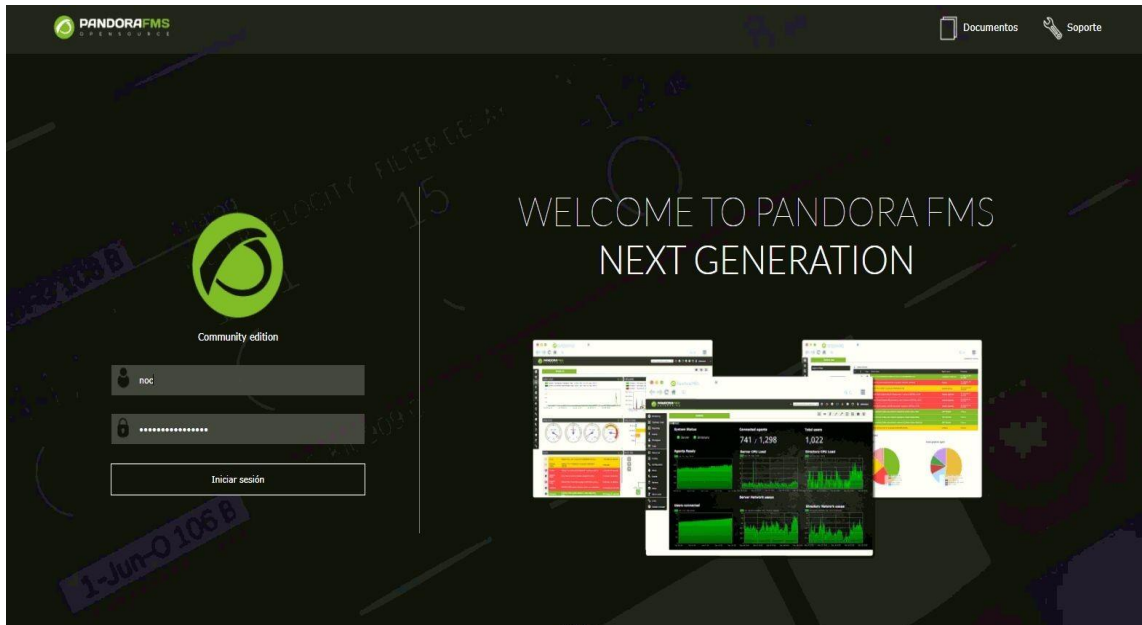


1.4. PANDORA

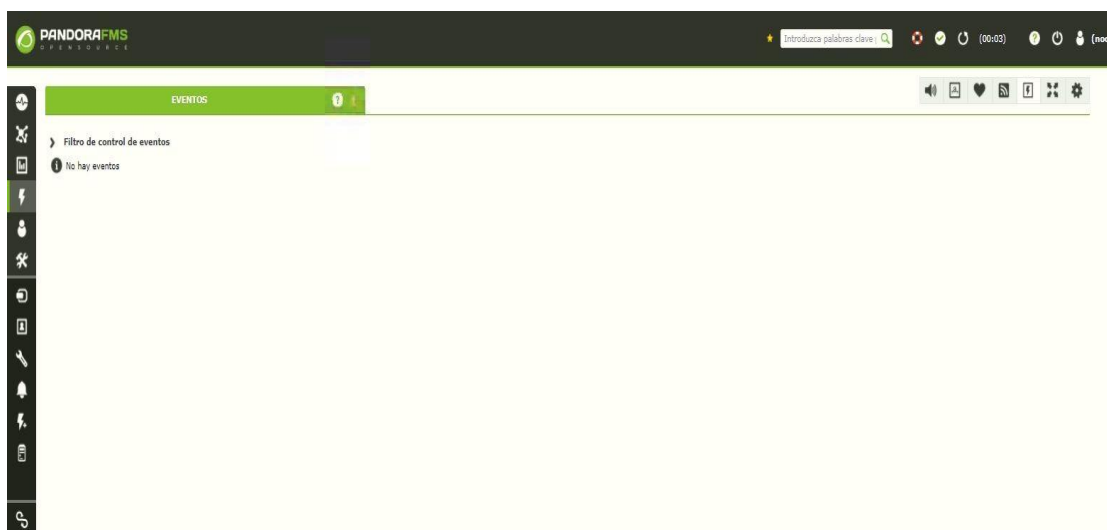
Para acceder a la aplicación del software de código abierto de monitorización de gestión de infraestructura TI, solo se requiere acceder a la página online de PANDORA.

a. El agente en turno debe ingresar al siguiente link:

→ http://10.4.1.93/pandora_console/index.php?login=1&login=1&sec=eventos&sec2=operation/events/events&refr=30v



b. Una vez seguido este paso solo se debe proceder a iniciar sesión en la plataforma haciendo uso del usuario y contraseña respectivo para el departamento de “Monitoreo de Recursos y Servicios NOC”, proporcionado por el jefe de departamento.



1.5. WhatsUp Gold

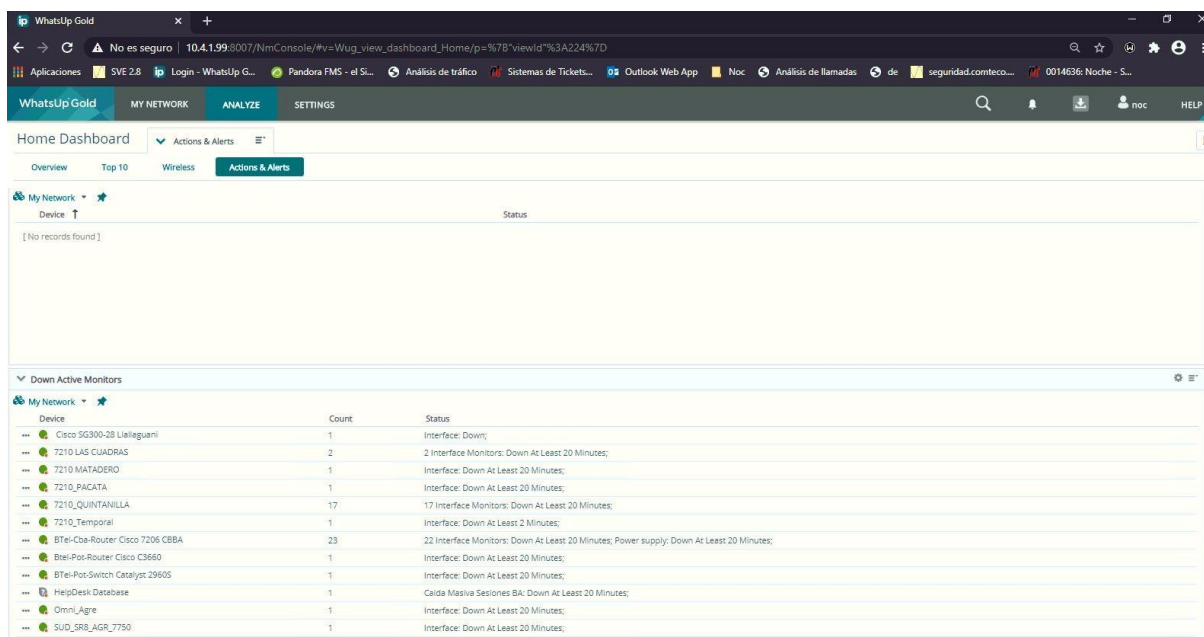
Para acceder a esta herramienta conformada por una interfaz de monitoreo de servicio solo se requiere acceder a la página online de WhatUp Gold.

- a. El agente en turno debe ingresar al siguiente link:

→ http://10.4.1.99:8007/NmConsole/#v=Wug_view_dashboard_Home/p=%7B%22viewId%22%3A224%7D



- b. Una vez seguido este paso solo se debe proceder a iniciar sesión en la plataforma haciendo uso del usuario y contraseña respectivo para el departamento de “Monitoreo de Recursos y Servicios NOC”, proporcionado por el jefe de departamento.



1.6. 4G

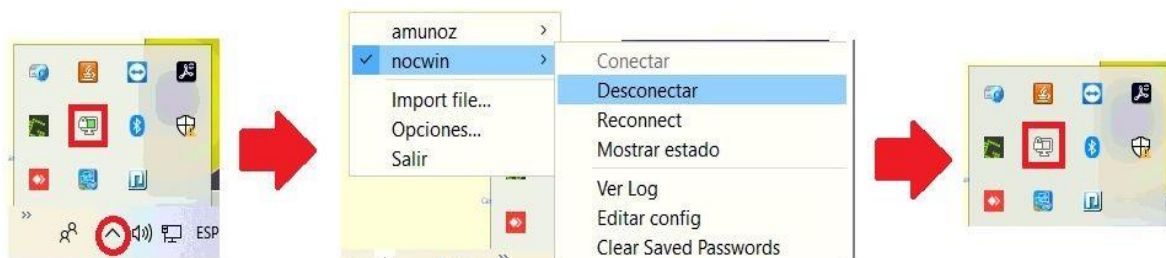
Para acceder a la aplicación de monitoreo de Radio bases 4G el agente en turno debe seguir una serie de pasos necesarios para iniciar correctamente la aplicación, ya que, si no es así no podrá ingresar a la aplicación.

Pasos para habilitar el sistema:

- a. Verificar la conexión a HSPA - 4G, ya que, si no estamos conectados no podremos ingresar al sistema.



- b. Desconectar la VPN del NOC denominado "OpenVPN GUI".

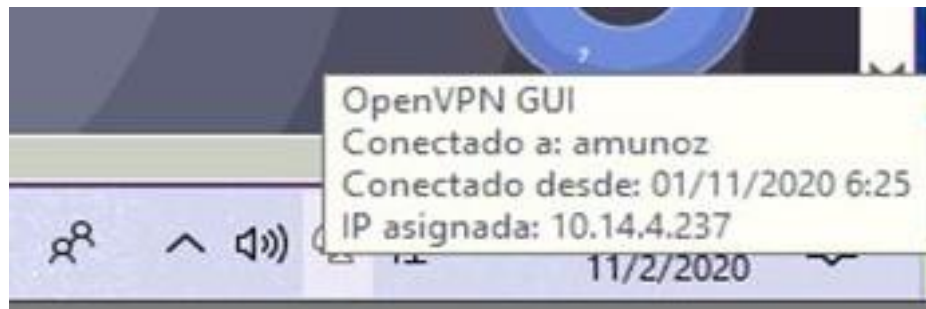


- c. Buscar en la computadora el acceso directo a NetNumen el cual está nombrado como HSPA SDR 4G y ejecutarla para desplegar una sub-ventana donde aparece “conectar” y hacer clic.
- d. Se desplegará el menú de inicio de la aplicación en el cual se debe iniciar sesión en la plataforma haciendo uso del usuario y contraseña respectivo para el departamento de “Monitoreo de Recursos y Servicios NOC”, proporcionado por el jefe de departamento.



- e. Una vez ingresada a la aplicación se debe proceder a conectar nuevamente la VPN del NOC denominado “OpenVPN GUI”.





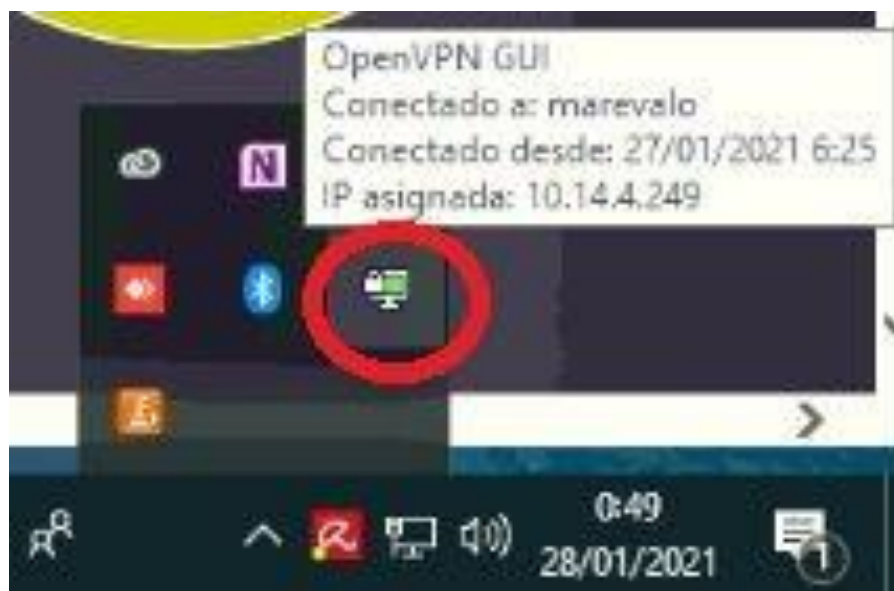
1.7. DWDM

El sistema funciona en base a una vpn individualizada que permite habilitar la interfaz en las máquinas de monitoreo.

Pasos para habilitar el sistema:

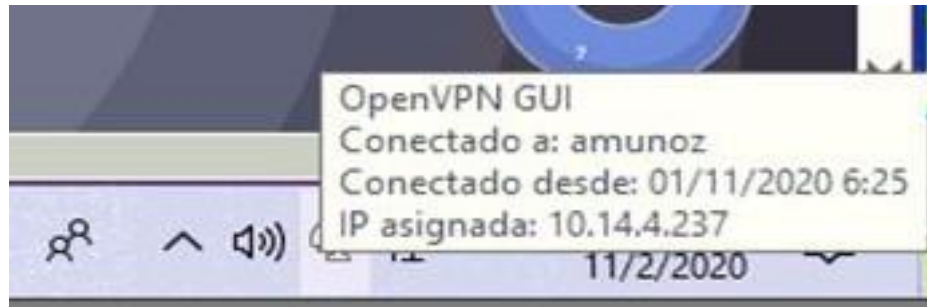
A. Activar la VPN denominada “*OpenVPN GUI*”.

a. Buscar el ícono de computadora con pantalla verde en miniatura en la barra de tareas (lado derecho inferior de la pantalla de escritorio), que tenga el nombre de “*OpenVPN GUI*”.



b. Clic derecho en el icono de la pantalla.

c. Desplazar el puntero a “Nocwin” y se desplegará una sub-ventana donde aparece “conectar” y hacer clic. Luego de haber realizado esta acción correctamente, se mostrará un mensaje de la siguiente manera:



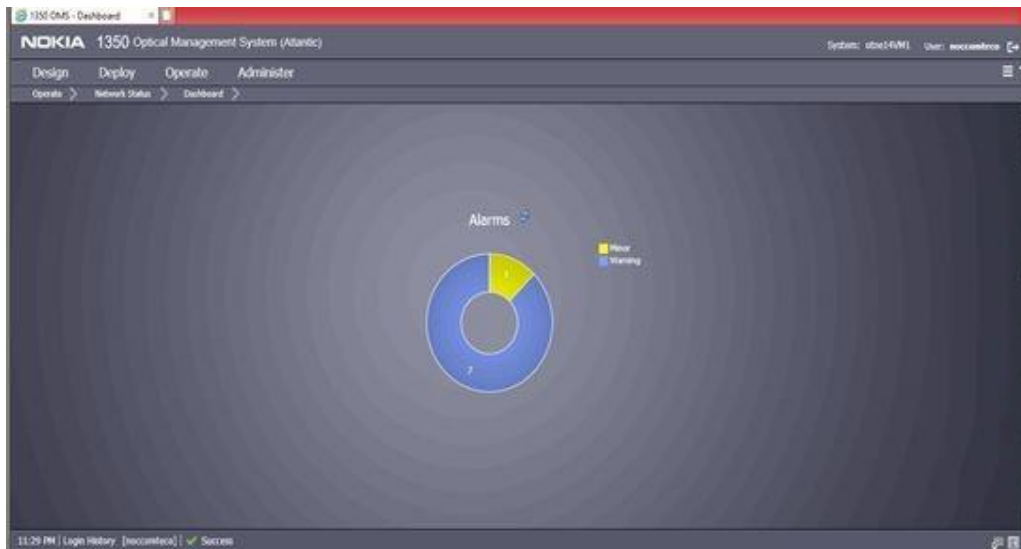
B. Abrir el explorador “Internet Explorer” e ingresar al siguiente link:

→ <https://192.168.104.3:8443/oms1350/pages/otn/mainOtn#/oms1350/pages/otn/D3dashboard?title=Operate%7CNetwork%20Status%7CDashboard%7C>

C. Ingresar el usuario y contraseña respectivo para el departamento de “Monitoreo de Recursos y Servicios NOC”, proporcionado por el jefe de departamento.



D. Una vez ingresados los datos correctamente, se mostrará el gestor de la siguiente manera:



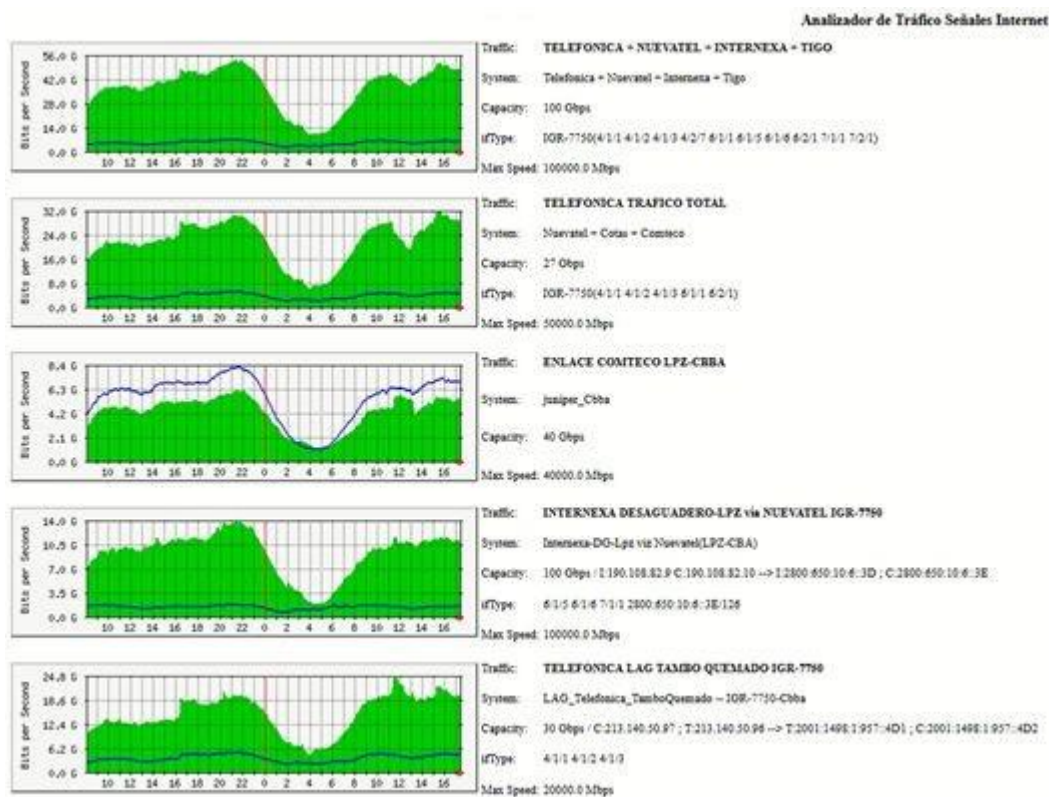
NOTA: El color de las alarmas dependen del estado actual de los enlaces a monitorear.

1.8. MRTG

A. Para acceder a la página desde un navegador se ingresa a este link:

→ <https://mrtg.supernet.com.bo/trafico/trafico/senales.html>

B. Una vez abierta la ventana, realizar un *refresh* a la misma. Luego de haber realizado correctamente este paso le saldrá el gestor de la siguiente manera:



1.9. SVE (Seguridad Industrial)

A. Para acceder a la página de inicio de sesión de SVE 2.8 se ingresa a este link:

→<http://seguridad.comteco.com.bo/Content/Main.php>

B. Ingresar el usuario y contraseña respectivo para el departamento de “Monitoreo de Recursos y Servicios NOC”, proporcionado por el jefe de departamento.

Usuario:

Contraseña:

Si tiene preguntas acerca de nuestros productos y servicios, [Contáctenos](#)

www.fase.bo

C. Una vez ingresados los datos correctamente, se mostrará el gestor de la siguiente manera:

URA	Grupo energía	Grupo puertos
Arochagua	Normal	Normal
Busch Norte	Normal	Normal
Busch Sur	Normal	Normal
Capacota	Normal	Normal
Caracollo	Normal	Normal
Central Sud	Normal	Normal
Chimba	Normal	Normal
Chifeta	Normal	Normal
Oliza	Normal	Normal
Condabamba	Normal	Normal
Curahuasi	Normal	Normal
Desaguadero	Normal	Normal
Ed. Técnico Mon.	Normal	Normal
Ed. Técnico Part.	Normal	Normal
El Paso	Normal	Normal
Feria	Normal	Normal
Florida Norte	Normal	Normal
Florida Sur	Normal	Normal
Higueras	Normal	Normal
Huacapisti	Normal	Normal
Huayra Falsa	Normal	Normal
Kilmes	Normal	Normal
Las Cañadas	Normal	Normal
Lande	Normal	Normal
Matadero	Normal	Normal
Montenegro	Normal	Normal
Mururina	Normal	Normal
Pacifica	Normal	Normal
Parutan URA	Normal	Normal
Pilluni	Normal	Normal
Pongo	Normal	Normal
Pozoca	Normal	Normal
Punata	Normal	Normal
Quinta Quera	Normal	Normal
Quillacollo	Normal	Normal
Quintanilla	Normal	Normal
Sacaba Pueblo	Normal	Normal
San Benito	Normal	Normal
San Miguel	Normal	Normal
Santa Cruz	Normal	Normal
Sarco	Normal	Normal
Seminario	Normal	Normal
Sipe Sipe	Normal	Normal
Tandil Quemado	Normal	Normal
Tenduerda	Normal	Normal
Tarija	Normal	Normal
Temperal	Normal	Normal
Tipapala	Normal	Normal
Tipopaya	Normal	Normal
Vale Hermoso	Normal	Normal
Villa Cosmos	Normal	Normal
Villa Pagador	Normal	Normal
Vinto	Normal	Normal

Normal Sin respuesta Sabotaje Alerta Alarma

Configurar usuarios

Reportes

NOTA: El color de las alarmas dependen del estado actual de los datos que brindan los sensores en las URAs a monitorear.

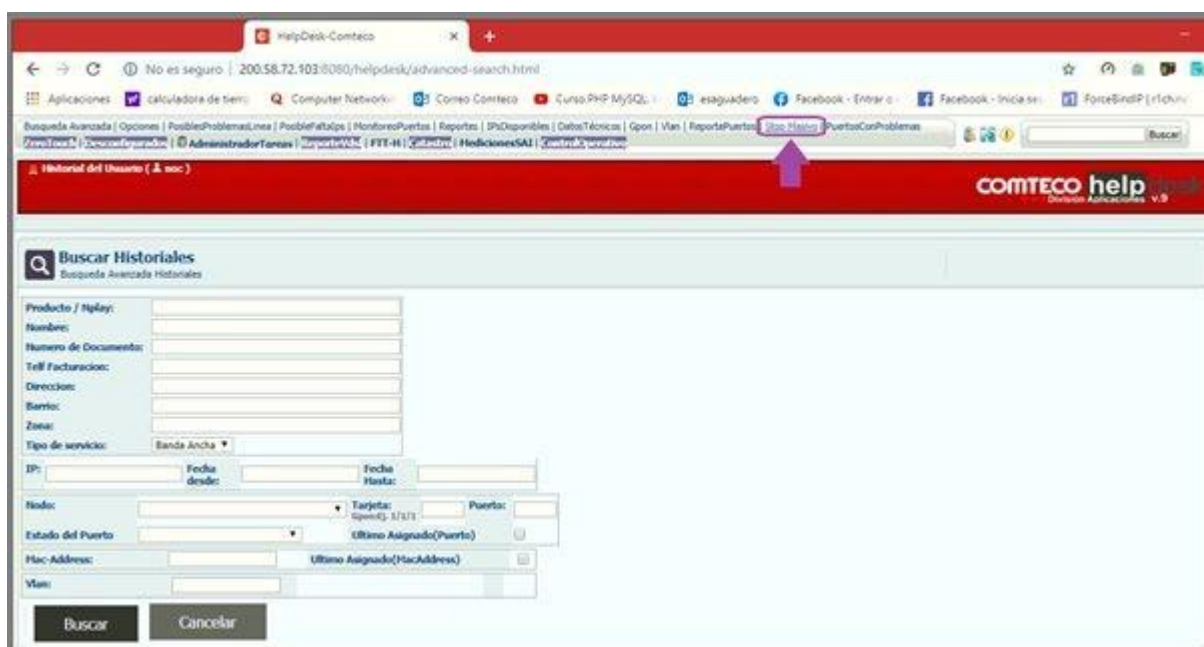
1.10. Help Desk

- A. Para ingresar a la aplicación debe abrir un navegador e ingresar al siguiente link: http://200.58.72.103:8080/helpdesk/login.jsp?login_error=1
- B. Ingresar el usuario y contraseña respectivo para el departamento de “Monitoreo de Recursos y Servicios NOC”, proporcionado por el jefe de



departamento.

- C. Una vez ingresados los datos correctamente, se mostrará el gestor de la siguiente manera:



2. Detalles y características de gestores y aplicaciones

2.1. Outlook

La aplicación “Outlook” es el medio de comunicación con los proveedores externos e internos a través de correos electrónicos.



NOTA: Siempre estar pendiente en la recepción de correo electrónicos, ya que la aplicación, no solo sirve para enviar mensajes de control y notificación, si no, recepción de información de trazados de posibles causas y control de status de problemas y situaciones alarmados por parte de proveedores (internos y externos) y clientes.

2.2. Mantis

Definición. - Es la Plataforma para la realización de reportes, tickets, incidencias e informes de turno.

Función. - Distribuidor de información y Base de datos de toda actividad dentro los turnos de monitoreo, clasificados de acuerdo a su severidad, daños, situaciones de causa “sin servicio” y todo el detalle generado para tener un respaldo de cualquier eventualidad.

The screenshot displays the Mantis Sistema de Tickets interface. At the top, there's a navigation bar with links like 'Principal', 'Mi Vista', 'Ver Incidencias', 'Reportar Incidencia', 'Administración', 'Editar Noticias', and 'Cerrar Sesión'. The main area is divided into several sections:

- Informes de Turno** (1 - 10 / 7738): A list of incident reports categorized by time of day (Tarde, Noche, Mañana) and date (12-02-2012).
- Difusión de Información** (1 - 10 / 399): A list of information dissemination incidents, including 'San Miguel' and 'LTA NB LaPaz'.
- Difusiones Abiertas** (1 - 10 / 182): A list of open dissemination incidents, such as 'Down at least 2 min SAT LP' and 'Up SAT LP'.
- Difusiones Cerradas** (1 - 10 / 3574): A list of closed dissemination incidents, including 'Corte de servicio internet' and 'Disminución de tráfico enlace'.

➤ Tipos de Tickets o Difusiones:

Dentro del sistema de tickets “Mantis” se manejan 3 tipos de reportes, clasificados según la situación o eventualidad (para más detalles, saltar al punto 3 del subtítulo III del informe), los cuales son:

- DAC (Difusión de Apertura y Cierre)
- DIN (Difusión de Información)
- ITU (Informe de Turno)

2.3. PANDORA

Definición: Software de código abierto de monitorización para gestión de infraestructura TI; puede monitorear el equipamiento de la red, servidores Windows y Unix, infraestructura virtualizada y otras aplicaciones, midiendo diferentes tipos de elementos de los mismos.

➤ En caso de presentar alarmas en el gestor:

The screenshot shows the PANDORA FMS interface. At the top, there's a search bar and a status bar. The main area displays a table of events (alarms) with the following columns: ID, Estado, Nombre del evento, Nombre del agente, Fecha/Hora, Tipo de evento, Alerta, and Acción.

ID	Estado	Nombre del evento	Nombre del agente	Fecha/Hora	Tipo de evento	Alerta	Acción
#478485	✓	Module 'Nort Alive' is going to NORMAL (1)	Tdala_ZHMO_8	2 horas	Subiendo a estado normal	🔍	🗑️
#478484	✓	Module 'Nort Alive' is going to CRITICAL (1)	Tdala_ZHMO_8	2 horas	Cayendo a estado crítico	🔍	🗑️

- a. Inicialmente se procede a analizar la alarma, observando las características técnicas de la alarma.
- b. Para obtener las características de dicha alarma, se hace clic en el nombre del agente (nombre de la alarma); para desplegar una ventana en la que se verifica la dirección IP, la cual ayudará a gestionar la alarma a la sección que corresponde atender la situación:



- c. Para saber obtener más información de dicha alarma como: la hora en la que cayó un equipo y también la hora en la que subió; la cual es importante para los reportes ITU, DAC o DIN. Se procede haciendo click izquierdo sobre el nombre del evento.

Total de elementos 4

ID	Estado	Nombre del evento	Nombre del agente	Fecha/Hora	Tipo de evento	Alerta
#478525	✓	Module 'Host Alive' is going to NORMAL (1)	IRPA_IRPA_ISAM VDGL	41 minutos 07 segundos	Subiendo a estado normal	
#478524	✓	Module 'Host Alive' is going to CRITICAL (0)	IRPA_IRPA_ISAM VDGL	46 minutos 13 segundos	Cayendo a estado crítico	
#478523	✓	Module 'Host Alive' is going to NORMAL (1)	Visrael_3	9 horas	Subiendo a estado normal	
#478522	✓	Module 'Host Alive' is going to CRITICAL (0)	Visrael_3	9 horas	Cayendo a estado crítico	

- d. Posteriormente se abrirá la siguiente ventana, donde podemos información específica: el grupo al que pertenece la alarma, el tipo de alarma, hora y fecha exacta en la que el equipo ha caído:

Module 'Host Alive' is going to CRITICAL (0) ✕

General Detalles Campos de agente Comentarios Respuestas

ID del evento	#478522
Nombre del evento	Module 'Host Alive' is going to CRITICAL (0)
Fecha/Hora	October 29, 2020, 1:58 pm
Propietario	N/A
Tipo	 Cayendo a estado crítico
Repetido	No
Gravedad	 Crítico
Estado	✓ Evento validado
Admitido por	(October 29, 2020, 2:03 pm)
Grupo	 Zhone
Etiquetas	N/A
ID extra	N/A

- e. De la misma manera se hace clic en la alarma verde con el mismo “nombre de agente” (su color indica que el equipo ha subido a un estado normal) para observar información específica de la alarma: el grupo al que pertenece la alarma, el tipo de alarma, hora y fecha exacta en la que el equipo ha subido:

Module 'Host Alive' is going to NORMAL (1) ✕

General Detalles Campos de agente Comentarios Respuestas

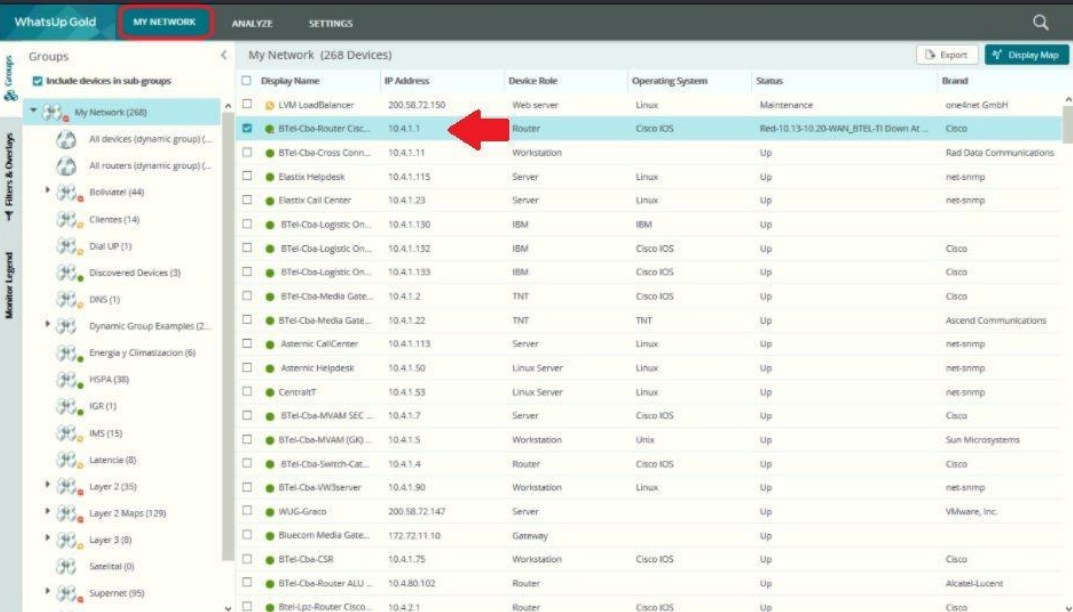
ID del evento	#478523
Nombre del evento	Module 'Host Alive' is going to NORMAL (1)
Fecha/Hora	October 29, 2020, 2:03 pm
Propietario	N/A
Tipo	 Subiendo a estado normal
Repetido	No
Gravedad	 Normal
Estado	✓ Evento validado
Admitido por	(October 29, 2020, 2:03 pm)
Grupo	 Zhone
Etiquetas	N/A
ID extra	N/A

2.4. WhatsUp Gold

Definición: Herramienta conformada por una interfaz de monitoreo de servicio y equipamiento; en el cual se puede obtener información del estado de los servidores

o actividades del host en la nube, recepción de alarmas de los diversos sistemas como son de las secciones de Broadband, MUX, Networking, MRTG, SDH, Radio y BoliviaTel dentro el departamento de “Monitoreo de Servicios y Recursos NOC”.

a. Si se requiere visualizar los dispositivos registrados en esta aplicación, el agente/pasante debe dirigirse a la la pestaña de “MY NETWORK”, dentro de esta sección se obtienen un listado de todos los equipos registrados y también las características generales de los equipos como IP, el rol del dispositivo, estado, sistema operativo y marca.



WhatsUp Gold MY NETWORK ANALYZE SETTINGS

Groups: My Network (268 Devices)

Include devices in sub-groups

Display Name	IP Address	Device Role	Operating System	Status	Brand
LVM LoadBalancer	200.58.72.150	Web server	Linux	Maintenance	one4net GmbH
BTel-Cba-Router Cisco...	10.4.1.1	Router	Cisco IOS	Red-10.13.10.20-WAN_BT...	Cisco
BTel-Cba-Cross Conn...	10.4.1.11	Workstation		Up	Rad Data Communications
Elastix Helpdesk	10.4.1.115	Server	Linux	Up	net-snmp
Elastix Call Center	10.4.1.23	Server	Linux	Up	net-snmp
BTel-Cba-Logistic On...	10.4.1.130	IBM	IBM	Up	
BTel-Cba-Logistic On...	10.4.1.132	IBM	Cisco IOS	Up	Cisco
BTel-Cba-Logistic On...	10.4.1.133	IBM	Cisco IOS	Up	Cisco
BTel-Cba-Media Gate...	10.4.1.2	TNT	Cisco IOS	Up	Cisco
BTel-Cba-Media Gate...	10.4.1.22	TNT	TNT	Up	Ascend Communications
Asterisk CallCenter	10.4.1.113	Server	Linux	Up	net-snmp
Asterisk Helpdesk	10.4.1.50	Linux Server	Linux	Up	net-snmp
CentralIT	10.4.1.53	Linux Server	Linux	Up	net-snmp
BTel-Cba-MVAM SEC ...	10.4.1.7	Server	Cisco IOS	Up	Cisco
BTel-Cba-MVAM (GR) ...	10.4.1.5	Workstation	Unix	Up	Sun Microsystems
BTel-Cba-Switch-Cat...	10.4.1.4	Router	Cisco IOS	Up	Cisco
BTel-Cba-VW3server	10.4.1.90	Workstation	Linux	Up	net-snmp
WUG-Graco	200.58.72.147	Server		Up	VMware, Inc.
Bluecom Media Gate...	172.72.11.10	Gateway		Up	
BTel-Cba-CSR	10.4.1.75	Workstation	Cisco IOS	Up	Cisco
BTel-Cba-Router ALU ...	10.4.80.102	Router		Up	Alcatel-Lucent
BTel-Lpo-Router Cisco...	10.4.2.1	Router	Cisco IOS	Up	Cisco

b. Si el agente/pasante requiere información de un equipo en cuestión dentro de la lista mostrada anteriormente, se procede a hacer clic derecho sobre el nombre del equipo, aparecerá un menú en el cual se pueden ver: las propiedades del equipo, el estado del equipo y el stage change timeline del dispositivo:



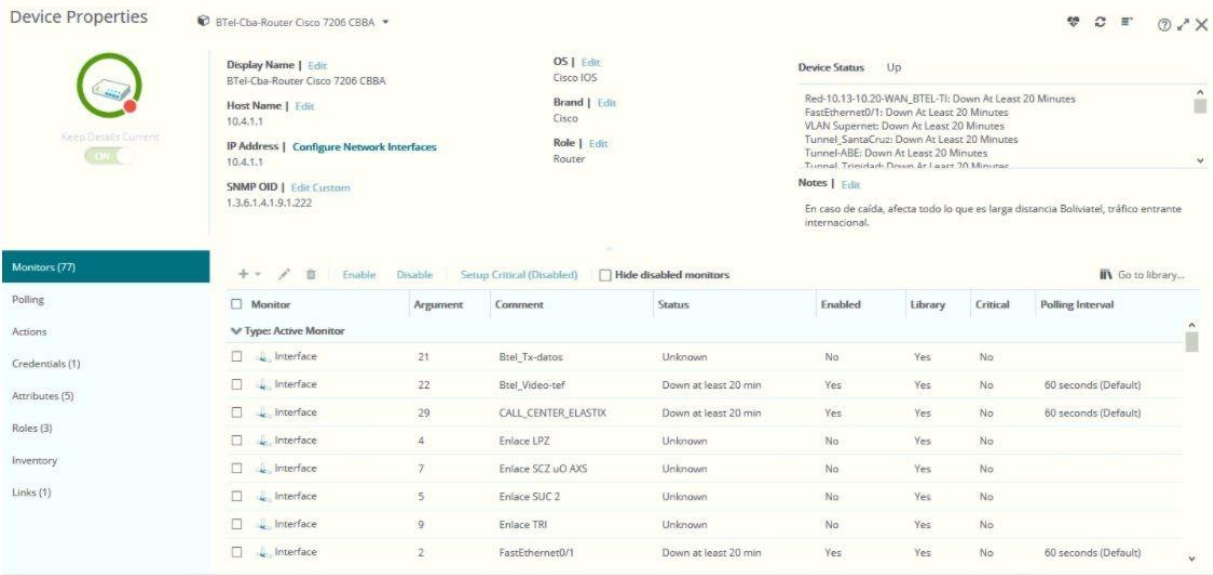
My Network (268 Devices)

Display Name	IP Address	Device Role	Operating System	Status	Brand
LVM LoadBalancer	200.58.72.150	Web server	Linux	Maintenance	one4net GmbH
BTel-Cba-Router Cisco...	10.4.1.1	Router	Cisco IOS	Red-10.13.10.20-WAN_BT...	Cisco
BTel-Cba-Cross Conn...	10.4.1.11	Workstation		Up	Rad Data Communications
Elastix Helpdesk	10.4.1.115	Server	Linux	Up	net-snmp
Elastix Call Center	10.4.1.23	Server	Linux	Up	net-snmp
BTel-Cba-Logistic On...	10.4.1.130	IBM	IBM	Up	
BTel-Cba-Logistic On...	10.4.1.132	IBM	Cisco IOS	Up	Cisco
BTel-Cba-Logistic On...	10.4.1.133	IBM	Cisco IOS	Up	Cisco
BTel-Cba-Media Gate...	10.4.1.2	TNT	Cisco IOS	Up	Cisco

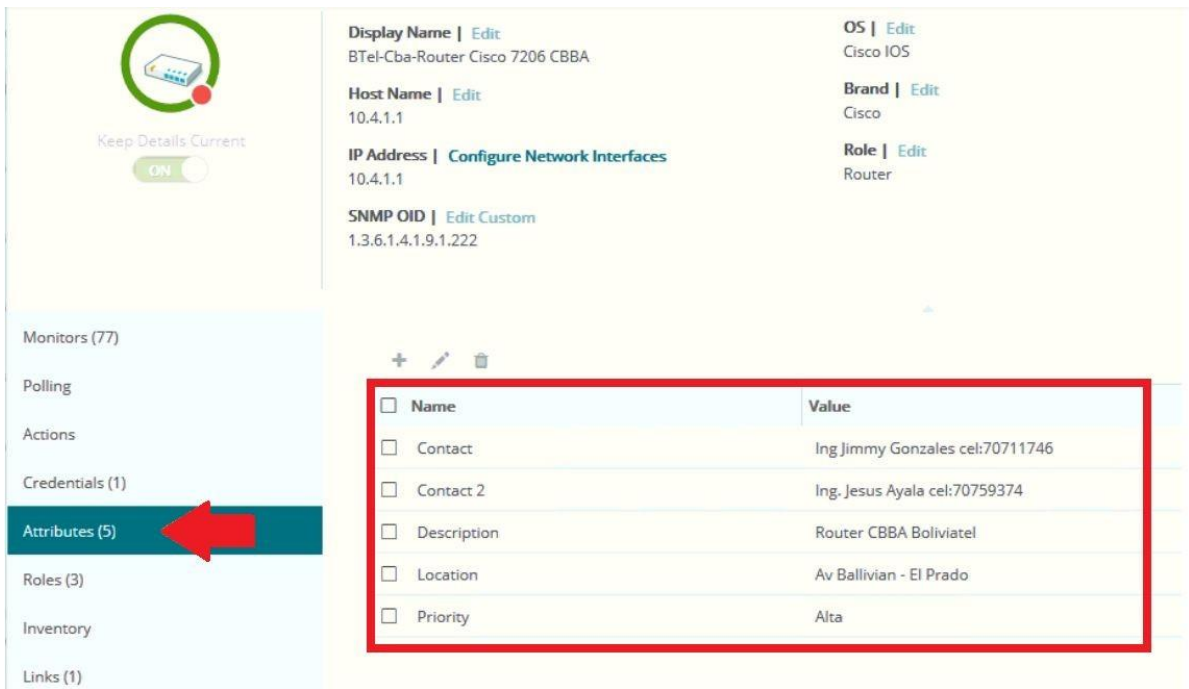
Context Menu for BTel-Cba-Router Cisco...:

- Device Properties
- Device Status
- State Change Timeline

Seleccionando la primera opción (las propiedades del equipo) dentro del menú anteriormente desplegado, se abrirá la siguiente ventana, en la que se muestra todas las propiedades específicas del equipo:



Dentro de la ventana se puede ingresar a una opción denominada atributos del equipo, en el cual, se obtiene el nombre y número de los responsables del equipo (a los cuales se precisa contactar si se tuviera alguna alarma con dicho equipo), así como la ubicación del equipo:



2.5. 4G

Definición: El servicio de telefonía e Internet con acceso inalámbrico fijo denominada “Hogar 4G” de Comteco, permite el acceso a usuarios y zonas de la ciudad que hasta ahora no cuentan con estos servicios y les brinda conectividad.

La aplicación SDR_COMTECO sirve para visualizar todas las radio bases que COMTECO posee (sección verde) y monitorear las mismas verificando si se presentan incidentes/ alarmas (sección lila):

The screenshot displays the NetNumen US1 Unified Management System interface. On the left, the 'NE Tree' shows a hierarchy of network elements, with 'SDR_COMTECO' highlighted in green. The main window is divided into two sections: 'Alarm Monitoring' and 'History Alarms'. The 'Alarm Monitoring' section shows a table of active alarms for 'Subnet(MO SDR)(101)'. The 'History Alarms' section shows a list of past alarms with columns for No., ACK State, Severity, NE, Location, System Type, Alarm Code, Raised Time, NE Type, and Alarm Type.

No.	ACK State	Severity	NE	Location	System Type	Alarm Code	Raised Time	NE Type	Alarm Type
146	Acknowledged	Minor	TOTORA(4108)	Equipment Resource(M)	Platform Alarm	The RRU link is broken(19809...	2020-10-23 00:59:17	ME(MO SDR)	Processi
147	Acknowledged	Minor	HOTEL CANADA(2300)	Equipment Resource(M)	Platform Alarm	External extended device fault...	2020-10-23 00:57:15	ME(MO SDR)	Equipme
148	Acknowledged	Minor	HOTEL CANADA(2300)	Equipment Resource(M)	Platform Alarm	External extended device fault...	2020-10-23 00:57:15	ME(MO SDR)	Equipme
149	Unacknowledged	Major	ME(UMTS)(101)	EQRNCID=101_RACKNO...	Controller Publ...	Association link broken(19806...	2020-11-01 10:17:42	ME(UMTS)	Commur
150	Unacknowledged	Major	ME(UMTS)(101)	EQRNCID=101_RACKNO...	Controller Publ...	Association link broken(19806...	2020-11-01 10:17:42	ME(UMTS)	Commur
151	Unacknowledged	Major	VIRGARZAMA(4113)	Equipment Resource(M)	Platform Alarm	The SCTP association is brok...	2020-11-01 10:18:03	ME(MO SDR)	Commur
152	Unacknowledged	Major	ENTRE RIOS(4112)	Equipment Resource(M)	Platform Alarm	The SCTP association is brok...	2020-11-01 10:18:04	ME(MO SDR)	Commur
153	Acknowledged	Minor	HOTEL CANADA(2300)	Equipment Resource(M)	Platform Alarm	External extended device fault...	2020-10-23 00:57:15	ME(MO SDR)	Equipme
154	Acknowledged	Minor	HOTEL CANADA(2300)	Equipment Resource(M)	Platform Alarm	FCE fan failure(198092069)	2020-11-01 11:27:37	ME(MO SDR)	Equipme
155	Acknowledged	Minor	HOTEL CANADA(2300)	Equipment Resource(M)	Platform Alarm	External extended device fault...	2020-10-23 00:57:15	ME(MO SDR)	Equipme
156	Acknowledged	Minor	TOTORA(4108)	Equipment Resource(M)	Platform Alarm	The RRU link is broken(19809...	2020-10-23 00:59:17	ME(MO SDR)	Processi
157	Acknowledged	Minor	HOTEL CANADA(2300)	Equipment Resource(M)	Platform Alarm	FCE fan failure(198092069)	2020-11-01 11:27:37	ME(MO SDR)	Equipme
158	Acknowledged	Minor	HOTEL CANADA(2300)	Equipment Resource(M)	Platform Alarm	External extended device fault...	2020-10-23 00:57:15	ME(MO SDR)	Equipme
159	Acknowledged	Minor	HOTEL CANADA(2300)	Equipment Resource(M)	Platform Alarm	FCE fan failure(198092069)	2020-11-01 11:27:37	ME(MO SDR)	Equipme
160	Acknowledged	Minor	HOTEL CANADA(2300)	Equipment Resource(M)	Platform Alarm	External extended device fault...	2020-10-23 00:57:15	ME(MO SDR)	Equipme
161	Acknowledged	Minor	HOTEL CANADA(2300)	Equipment Resource(M)	Platform Alarm	External extended device fault...	2020-10-23 00:57:15	ME(MO SDR)	Equipme

➤ En caso de presentar alarmas en el gestor:

a. Inicialmente el icono de la estación base se pintara de un color segun la severidad de la alarma en cuestion: rojo (severidad Crítica), naranja (severidad Mayor), amarillo (severidad Menor).

En el caso de este ejemplo se tiene la alarma menor en la estación base de “Santivañes”, cuya información se ve en la pestaña de monitoreo de alarma.

NE Tree Management

Alarm Monitoring 33 Active Alarms: Subnet(MO SDR)(101)

Alarm Monitoring

Visibility Visible SANTIVANEZ(3104) Alarm Data Total: 1 Critical 0 Major 0 Minor 1 Warning 0

Keyword to filter, support * and ?

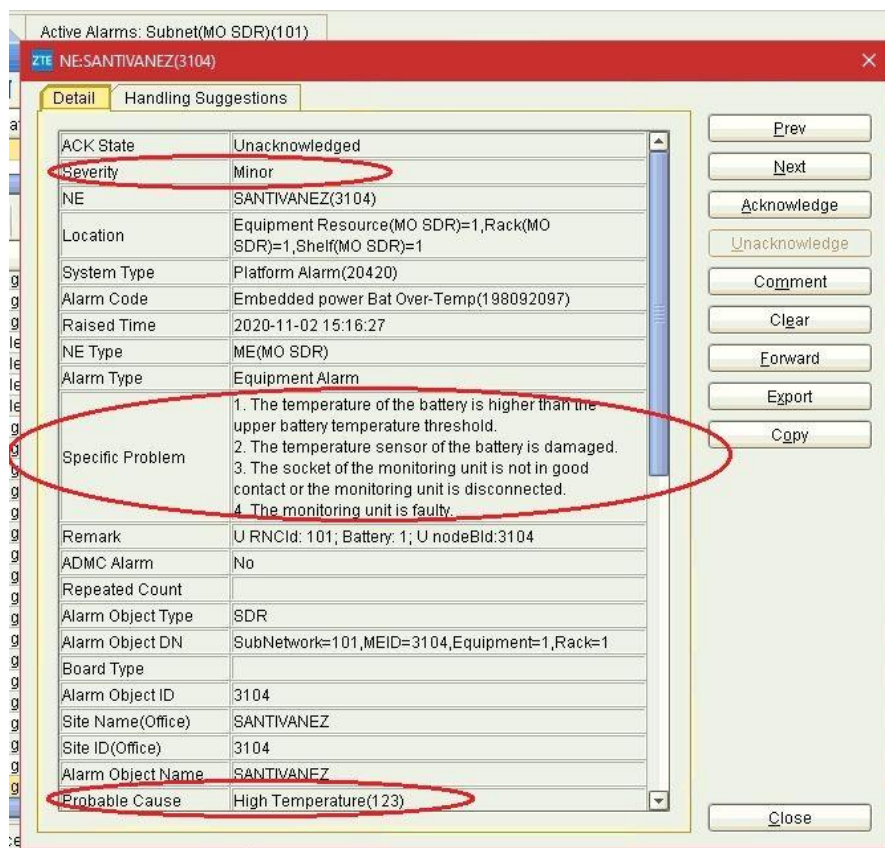
No.	Root Alarm Indicator	ACK State	Severity	NE	Location	System Ty	Alarm Code	Raised Time	NE
146	Unacknowledged	Minor	SANTIVANEZ(3104)	Equipment Resour...	Platform A...	Embedded power Bat Over-Temp(198092097)	2020-11-02 15:16:27	ME	

History Alarms

No.	ACK State	Severity	NE	Location	System Type	Alarm Code	Raised Time	NE Type	Alarm Ty
146	Acknowledged	Major	TOTORA(4108)	Equipment Resource(M...	Platform Alarm...	The RRU link is broken(19809...	2020-10-23 00:59:17	ME(MO SDR)	Processi...
147	Acknowledged	Minor	HOTEL CANADA(2300)	Equipment Resource(M...	Platform Alarm...	External extended device fault...	2020-10-23 00:57:15	ME(MO SDR)	Equipme...
148	Acknowledged	Minor	HOTEL CANADA(2300)	Equipment Resource(M...	Platform Alarm...	External extended device fault...	2020-10-23 00:57:15	ME(MO SDR)	Equipme...
149	Unacknowledged	Major	ME(UMTS)(101)	Equipment Resource(M...	Platform Alarm...	Association link broken(19806...	2020-11-01 10:17:42	ME(UMTS)	Commur...
150	Unacknowledged	Major	ME(UMTS)(101)	Equipment Resource(M...	Platform Alarm...	Association link broken(19806...	2020-11-01 10:17:42	ME(UMTS)	Commur...
151	Unacknowledged	Major	MIRGARZAMA(4113)	Equipment Resource(M...	Platform Alarm...	The SCTP association is brok...	2020-11-01 10:18:03	ME(MO SDR)	Commur...
152	Unacknowledged	Major	ENTRE RIOS(4112)	Equipment Resource(M...	Platform Alarm...	The SCTP association is brok...	2020-11-01 10:18:04	ME(MO SDR)	Commur...
153	Acknowledged	Minor	HOTEL CANADA(2300)	Equipment Resource(M...	Platform Alarm...	External extended device fault...	2020-10-23 00:57:15	ME(MO SDR)	Equipme...
154	Acknowledged	Minor	HOTEL CANADA(2300)	Equipment Resource(M...	Platform Alarm...	FCE fan failure(198092069)	2020-11-01 11:27:37	ME(MO SDR)	Equipme...
155	Acknowledged	Minor	HOTEL CANADA(2300)	Equipment Resource(M...	Platform Alarm...	External extended device fault...	2020-10-23 00:57:15	ME(MO SDR)	Equipme...
156	Acknowledged	Major	TOTORA(4108)	Equipment Resource(M...	Platform Alarm...	The RRU link is broken(19809...	2020-10-23 00:59:17	ME(MO SDR)	Processi...
157	Acknowledged	Minor	HOTEL CANADA(2300)	Equipment Resource(M...	Platform Alarm...	FCE fan failure(198092069)	2020-11-01 11:27:37	ME(MO SDR)	Equipme...

OJO.- Para agilizar la solución de la posible alarma se notifica el contenido de la pestaña “Alarm Code” conjuntamente con el “NE” que están dentro de la pestaña de “Alarm Monitoring” , al personal de turno de área de 4G .

b. Si se hace click en la alarma se abrirá la siguiente ventana, en la que se obtiene información específica de dicha alarma como: la posible causa:



Active Alarms: Subnet(MO SDR)(101)	
ZTE NE:SANTIVANEZ(3104)	
Detail Handling Suggestions	
ACK State	Unacknowledged
Severity	Minor
NE	SANTIVANEZ(3104)
Location	Equipment Resource(MO SDR)=1,Rack(MO SDR)=1,Shelf(MO SDR)=1
System Type	Platform Alarm(20420)
Alarm Code	Embedded power Bat Over-Temp(198092097)
Raised Time	2020-11-02 15:16:27
NE Type	ME(MO SDR)
Alarm Type	Equipment Alarm
Specific Problem	1. The temperature of the battery is higher than the upper battery temperature threshold. 2. The temperature sensor of the battery is damaged. 3. The socket of the monitoring unit is not in good contact or the monitoring unit is disconnected. 4. The monitoring unit is faulty.
Remark	U RNCId: 101; Battery: 1; U nodeBId:3104
ADMC Alarm	No
Repeated Count	
Alarm Object Type	SDR
Alarm Object DN	SubNetwork=101,MEID=3104,Equipment=1,Rack=1
Board Type	
Alarm Object ID	3104
Site Name(Office)	SANTIVANEZ
Site ID(Office)	3104
Alarm Object Name	SANTIVANEZ
Probable Cause	High Temperature(123)

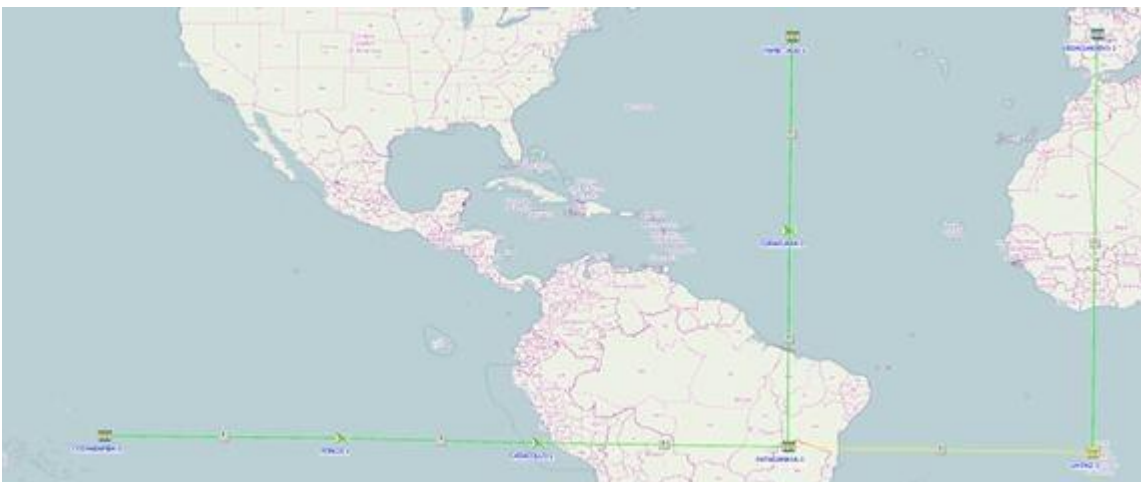
2.6. DWDM

Definición: El departamento de Multiplexación por división en longitud de onda (*"Dense Wavelength Division Multiplexing"*) se encarga de la gestión de todas las redes de fibra óptica desplegadas a nivel nacional pertenecientes a COMTECO R.L.

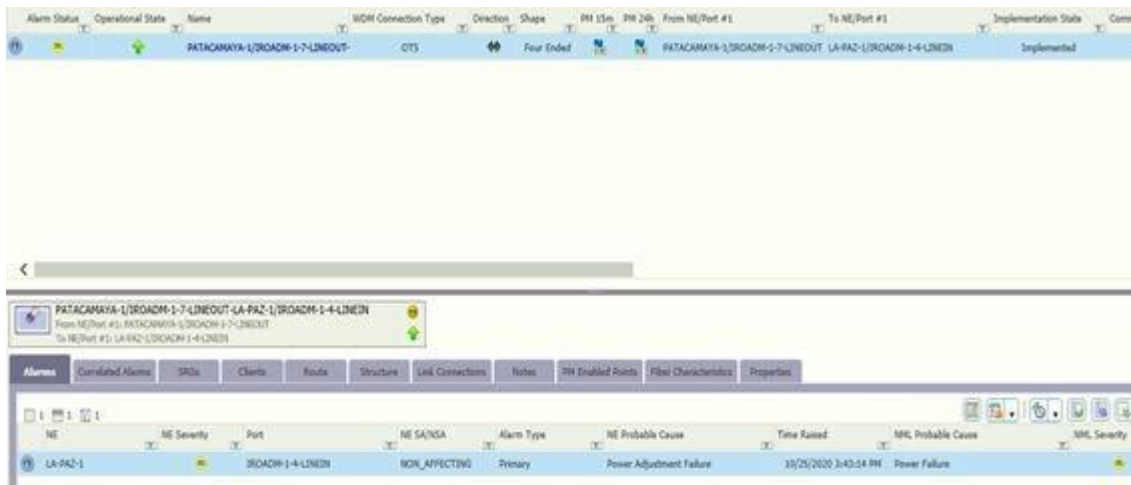
Para el monitoreo de los enlaces se trabaja con una interfaz de la marca NOKIA presentada en la pantalla de monitoreo; en esta, se debe monitorear una "rosca" o "dona" que representa las alarmas tanto críticas, mayores, menores y advertencias (cada una representada con un color característico), que son indicadores directos del estado actual de los equipos, centrales, nodos y arquitectura de red de fibra óptica desplegada en sí.

➤ En caso de presentar alarmas en el gestor:

- A. Luego de haber cumplido con los pasos a partir del punto 2.4. de la sección 2 "Monitoreo durante el turno". Se puede buscar mayor información de la alarma de la siguiente manera:
 - a. Realizar clic en la opción de la ventana *"Operate"* y luego clic en *"Network Map"*. Esta opción abrirá la pantalla de un mapa que refleja de forma superficial la arquitectura de la red de fibra óptica desplegada, en la cual, el tramo o el equipo afectado se torna del color de la alarma. En ese sentido, se abrirá una nueva pestaña y se mostrará de la siguiente manera:



- b. Luego, se hace clic derecho en el equipo que se encuentra afectado, para poder notar en la pantalla que emerge la causa posible de la alarma. En ese sentido, se abrirá una ventana dentro de la pestaña actual y se mostrará de la siguiente manera:



OJO. El realizar estos pasos es sólo con el fin de adquirir información y no así para generar una respuesta a la alarma, esto lo debe respaldar el responsable del área DWDM.

2.7. MRTG

Definición: Es una herramienta para supervisar la carga de tráfico de interfaces de red. MRTG genera páginas HTML con gráficos que proveen una representación visual de este tráfico.

En las gráficas se pueden observar los datos tomados a partir de los routers de borde de dos colores:

- De color verde: representa el tráfico que ingresa por la interfaz al router de borde.
- De color azul: representa el tráfico de salida del router de frontera hacia esa interfaz.

En todas las gráficas se puede ver lo siguiente:

- Ancho de banda máximo de cada enlace.
- En algunos enlaces, la velocidad de transmisión medidos en Gbps o Mbps.
- Las gráficas están tasadas en ancho de banda por horas (consumo variable dependiendo del horario).
- En la mayoría de las gráficas se describen las características técnicas del enlace como el sistema perteneciente.

En los enlaces que representan las salidas internacionales como todas las gráficas de Telefónica, INTERNEXA y NUEVATEL el tráfico que desde el internet entra hacia COMTECO para llegar a los abonados es mucho mayor.

Entre otras gráficas del MRTG, están:

- La gráfica de enlace de TIGO, representa una pequeña sección de ancho de banda máxima de 6 Gbps, se la considera como proveedor.
- PIT (Punto de Interconexión de Tráfico) → donde la línea azul es el tráfico de va de COMTECO a los otros operadores nacionales (ENTEL, TIGO, VIVA, AXS, etc), y el área verde el tráfico de los Operadores hacia COMTECO. La gráfica del PIT, muestra el tráfico de intercambio con los operadores nacionales, lo que viene a ser tráfico nacional que ya no sale al internet, por ejemplo el acceso a portales de las Universidades. Este Nodo físicamente está en La Paz en la Autoridad de Transporte y Telecomunicaciones ATT
- HSPA+ → muestra el tráfico de la red inalámbrica celular de COMTECO, ya que se tienen SIM cards con números locales que los usuarios pueden tenerlos en un celular; en esta gráfica la línea azul es tráfico que baja del internet con contenido hasta los dispositivos móviles de usuarios, y el área verde es tráfico que sube de los abonados al Internet con las peticiones de contenido.
- La gráfica de tráfico interno como operador COMTECO, muestra un comportamiento diferente al resto, ya que son 4 canales locales (ATB, UNITEL, BOLIVISIÓN y BOLIVIA TV), los cuales están digitalizados y se envían al Terrapuerto que tiene TELEFÓNICA en Lurín Perú, para que puedan subirlos al Satélite (Amazonas II si mal no recuerdo), para que los Abonados que tienen TvSatelital DTH, en zonas donde no tenemos cobertura de red cableada, puedan sintonizar estas señales nacionales en su receptor satelital.

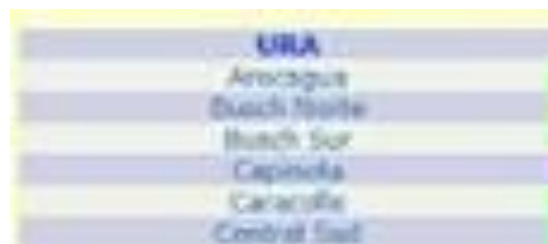
Las últimas gráficas expuestas en la aplicación MRTG son de los clientes que la empresa COMTECO, tiene como usuarios en las cuales se identifica en las gráficas:

- En los enlaces que representan las gráficas para clientes, como las gráficas de COTES, COTEOR, COTAP y COTEL. La salida de tráfico hacia el cliente es mayor, porque es la descarga del internet, que lo que ingresa del cliente a la empresa, notoria en la gráfica de área verde (gráfica de subida) y la línea azul demuestra el tráfico de descarga.

2.8. SVE

Definición: SVE (seguridad industrial) es una aplicación en entorno WEB creada para la configuración y supervisión de estados de los diferentes detectores, sensores, actuadores, puntos de acceso, etc., para proporcionar información de componentes básicos del sistema de seguridad como ser: detectores de humo, sensores de temperatura, detectores de movimiento, botones de pánicos, detectores de puerta abierta, etc

La lista de las unidades de control que forman parte del sistema de seguridad/control de acceso se muestra a la izquierda (bajo el nombre de URA).



Al hacer clic en cualquiera de las URAs se desplegará una ventana que mostrará el estado de cada uno de elementos conectados a esa unidad de control, como en el siguiente ejemplo en el que se accedió a la URA Hipódromo, donde se visualiza el estado de los sensores de temperatura, voltaje AC, voltaje DC y el boton de panico, que en este caso se encuentran en estado normal.

Unidad de Control 36 Hipódromo (Último sondeo 2020-10-29 18:05:45).

Botones de pánico				Sensores temperatura				
ID	Descripción	Activado	Estado	ID	Descripción	Nivel	Estado	Graficar
892	Pánico	Armado	Normal	701	Temp. Torre C&C	24.3	Normal	Ver
899	Pánico Remoto	Armado	Normal	Sensores humedad				
				ID	Descripción	Nivel	Estado	Graficar
				801	Humed. Torre C&C	27.2	Normal	Ver
				Sensores voltaje AC				
				ID	Descripción	Nivel	Estado	Graficar
				701	Volt. E	225.5	Normal	Ver
				702	Volt. S	225.0	Normal	Ver
				703	Volt. T	226.0	Normal	Ver
				Sensores voltaje DC				
				ID	Descripción	Nivel	Estado	Graficar
				701	Volt. Control	32.7	Normal	Ver

Reportes	
Normal	Sin respuesta
Sabotaje	Disparado
Alerta	Alarma

➤ Ejemplo de análisis de reporte “Sin Respuesta”:

Unidad de Control 41 Capinota (Ultimo sondeo 2020-10-27 18:45:05).

Detectores voltaje				Sensores temperatura				
ID	Descripción	Activado	Estado	ID	Descripción	Nivel	Estado	Graficar
51	Det.Vol: 1	Armado	Sin respuesta	601	Temp. MDF	25.7	Sin respuesta	Hoy
52	Det.Vol: 2	Armado	Sin respuesta	602	Temp. Conmut.	23.5	Sin respuesta	Hoy
53	Det.Vol: 3	Armado	Sin respuesta					
				Sensores humedad				
ID	Descripción	Activado	Estado	ID	Descripción	Nivel	Estado	Graficar
801	Pánico	Armado	Sin respuesta	651	Hume. MDF	44.2	Sin respuesta	Hoy
899	Pánico Remoto	Armado	Sin respuesta	652	Hume. Conmut.	32.0	Sin respuesta	Hoy
				Sensores voltaje AC				
ID	Descripción	Activado	Estado	ID	Descripción	Nivel	Estado	Graficar
				701	Vac. R	225.7	Sin respuesta	Hoy
				702	Vac. S	223.6	Sin respuesta	Hoy
				703	Vac. T	224.8	Sin respuesta	Hoy
				Sensores voltaje DC				
ID	Descripción	Activado	Estado	ID	Descripción	Nivel	Estado	Graficar
				721	Vdc Bat. 1	54.5	Sin respuesta	Hoy
				722	Vdc Bat. 2	53.4	Sin respuesta	Hoy
				723	Vdc Carga	53.5	Sin respuesta	Hoy
				Sensores corriente DC				
ID	Descripción	Activado	Estado	ID	Descripción	Nivel	Estado	Graficar
				761	Idc Bat. 1	2.9	Sin respuesta	Hoy
				762	Idc Bat. 2	17.8	Sin respuesta	Hoy
				763	Idc Carga	1.2	Sin respuesta	Hoy

Normal Sin respuesta SabotajeDisparado Alerta Alarma

Reportes

El el caso de presentarse este tipo de reporte se cuenta 30 minutos para la reposición, ya que puede tratarse de un corte en cualquier enlace y eso tarda entre 30 min a 45 min en reponerse en algunos lugares; pero no afectan al sistema ya que pasados los 30 min se reconecta automáticamente y si esto no fuera así el encargado de Seguridad Industrial al cual ya se notificó, lo conecta manualmente.

➤ Ejemplo de análisis de reporte “Alarma”:

Unidad de Control 41 Capinota (Ultimo sondeo 2020-10-27 18:45:05).

Detectores voltaje				Sensores temperatura				
ID	Descripción	Activado	Estado	ID	Descripción	Nivel	Estado	Graficar
51	Det.Vol: 1	Armado	Normal	601	Temp. MDF	23.8	Nivel normal	Hoy
52	Det.Vol: 2	Armado	Normal	602	Temp. MDF	25.5	Nivel normal	Hoy
53	Det.Vol: 3	Armado	Normal	603	Temp. Conmut.	25.0	Nivel normal	Hoy
54	Det.Vol: 4	Armado	Normal					
				Sensores humedad				
ID	Descripción	Activado	Estado	ID	Descripción	Nivel	Estado	Graficar
801	Pánico	Armado	Normal	651	Hume. Conmut.	32.8	Nivel normal	Hoy
899	Pánico Remoto	Armado	Normal					
				Sensores voltaje AC				
ID	Descripción	Activado	Estado	ID	Descripción	Nivel	Estado	Graficar
				701	Vac. R	225.7	Nivel normal	Hoy
				702	Vac. S	223.6	Nivel normal	Hoy
				703	Vac. T	224.8	Nivel normal	Hoy
				Sensores voltaje DC				
ID	Descripción	Activado	Estado	ID	Descripción	Nivel	Estado	Graficar
				721	Vdc Bat. 1	54.5	Nivel normal	Hoy
				722	Vdc Bat. 2	54.3	Nivel normal	Hoy
				723	Vdc Carga	54.3	Nivel normal	Hoy
				Sensores corriente DC				
ID	Descripción	Activado	Estado	ID	Descripción	Nivel	Estado	Graficar
				761	Idc Bat. 1	0.5	Nivel normal	Hoy
				762	Idc Bat. 2	1.6	Nivel normal	Hoy
				763	Idc Carga	81.5	Nivel normal	Hoy

Normal Sin respuesta SabotajeDisparado Alerta Alarma

Reportes

➤ Ejemplo de análisis de reporte “Sabotaje”:

Unidad de Control 10 Chimba (Ultimo sondeo 2020-10-27 19:17:15).

Detectores voltaje			
ID	Descripción	Activado	Estado
51	Det.Vdc-1	Armado	Normal
52	Det.Vdc-2	Armado	Normal
53	Det.Vdc-3	Armado	Normal
54	Det.Vdc-4	Armado	Normal
55	Det.Vdc-5	Armado	Normal
56	Det.Vdc-6	Armado	Normal
57	Det.Vdc-7	Armado	Normal
58	Det.Vdc-8	Armado	Normal

Botones de pánico			
ID	Descripción	Activado	Estado
899	Pánico	Armado	Normal
899	Pánico Remoto	Armado	Normal

Sensores temperatura				
ID	Descripción	Nivel	Estado	Graficar
601	Temp. Baterías	0.0	Sabotaje	Hoy
602	Temp. Control-1	28.5	Nivel normal	Hoy
603	Temp. Reservorio	33.0	Nivel normal	Hoy
604	Temp. Control-2	24.0	Nivel normal	Hoy

Sensores humedad			
ID	Descripción	Nivel	Estado
654	Humedad Control	32.2	Nivel normal

Sensores voltaje AC			
ID	Descripción	Nivel	Estado
701	Vdc-B	228.7	Nivel normal
702	Vdc-C	222.1	Nivel normal
703	Vdc-T	222.0	Nivel normal

Sensores voltaje DC			
ID	Descripción	Nivel	Estado
721	Vdc Bat-1	56.5	Nivel normal
722	Vdc Bat-2	56.4	Nivel normal
723	Vdc Carga	56.8	Nivel normal

Sensores corriente DC			
ID	Descripción	Nivel	Estado
761	Icc Bat-1	16.5	Nivel normal
762	Icc Bat-2	1.4	Nivel normal
763	Icc Carga	49.2	Nivel normal

Normal Sin respuesta SabotajeDisparado Alerta Alarma

Reportes

Si se quiere obtener más información acerca de los sensores o de un sensor en específico se debe ingresar a “Reportes”; este botón se encuentra en la parte inferior de la gráfica de descripción de los tipos de alarmas.



- Luego, se abrirá una nueva pestaña donde se podrá obtener el Histórico y Gráficas de los sensores de la siguiente manera:

Reportes

Histórico sensores	Todas	UC CA10	Fecha inicio(aaaa-mm-dd)	2020-10-27	Fecha final(aaaa-mm-dd)	2020-10-27	Hora in.(HH:mm)	19	23	Hora fin.(HH:mm)	19	23	Generar reporte
Graficar sensores	Todas	Ninguno	Fecha inicio(aaaa-mm-dd)	2020-10-27	Fecha final(aaaa-mm-dd)	2020-10-27	Hora in.(HH:mm)	19	23	Hora fin.(HH:mm)	19	23	Graficar
Reporte apertura de puertas	URA	Todas	Fecha inicio(aaaa-mm-dd)	2020-10-27	Fecha final(aaaa-mm-dd)	2020-10-27	Hora in.(HH:mm)	19	23	Hora fin.(HH:mm)	19	23	Generar reporte

Para obtener información de los Históricos de los sensores se deberá seleccionar:

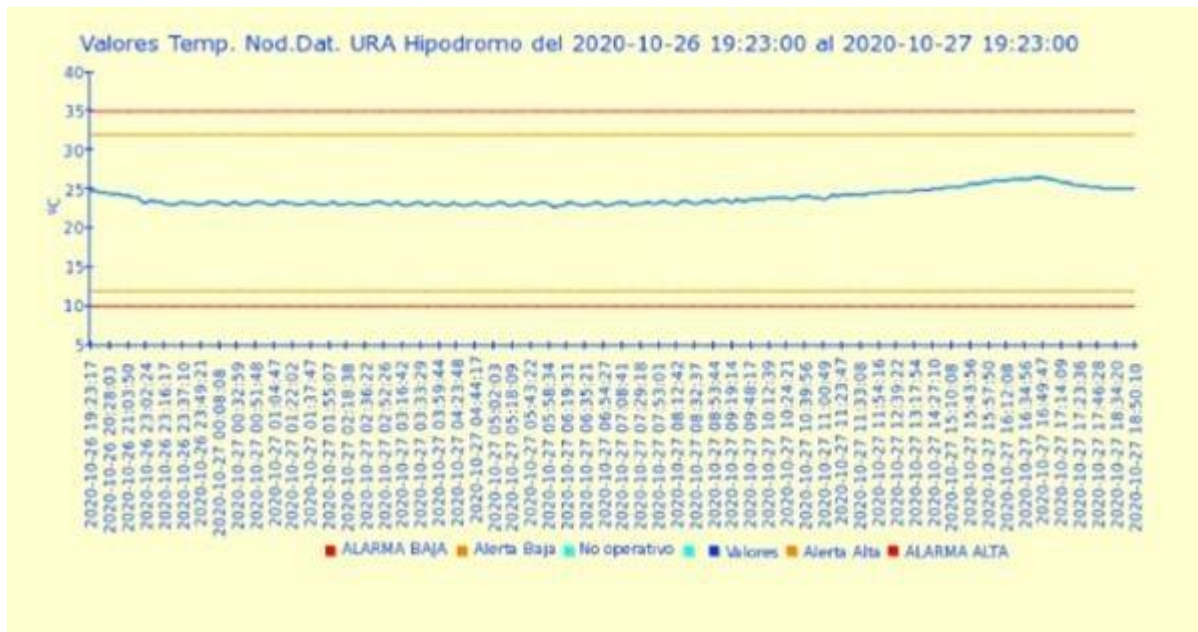
- Una unidad en específico o la opción Todas, si se quiere reporte de todas las unidades.
- Seleccionar un sensor en específico en caso de tener una unidad seleccionada. En caso de tener seleccionada la opción Todas en el paso 3.1. aparecerá por defecto una sola opción en esta casilla.

- Seleccionar fecha y hora de inicio donde se quiere el reporte.
- Seleccionar fecha y hora final para el reporte.
- Finalmente, seleccionar el botón Generar Reporte para obtener el mismo.
- Luego, se abrirá una nueva pestaña donde aparecerá el reporte generado con atributos el IDI, Descripción, Nivel de seguridad, Activo, Estado, Zona, Fecha y hora de cada momento de actualización. En la parte superior se tiene el botón para Guardar como hoja Excel. En caso de ser demasiados datos no se podrá guardar, ya que la aplicación actualiza los datos cada 10 segundos aproximadamente.

Guardar como hoja Excel							
Usuario		Fecha inicio			Fecha fin		
noc		2020-10-26			2020-10-27		
UC-CA10	IDI	Descripción	Nivel de seguridad	Activo	Estado	Zona	Fecha y hora
36	10	Puerta Nod.Dat.			Sin respuesta	0	2020-10-26 21:22:01
36	10	Puerta Nod.Dat.			Presente	0	2020-10-26 22:01:02
36	10	Puerta Nod.Dat.			Sin respuesta	0	2020-10-26 22:16:28
36	10	Puerta Nod.Dat.			Presente	0	2020-10-26 23:00:49
36	201	Puerta Nod.Dat.	NC(Sire.OFF)Mail.ON(Sonde.ON	Armado	Sin respuesta	10	2020-10-26 21:22:01
36	201	Puerta Nod.Dat.	NC(Sire.OFF)Mail.ON(Sonde.ON	Armado	Normal	10	2020-10-26 22:01:02
36	201	Puerta Nod.Dat.	NC(Sire.OFF)Mail.ON(Sonde.ON	Armado	Sin respuesta	10	2020-10-26 22:16:28
36	201	Puerta Nod.Dat.	NC(Sire.OFF)Mail.ON(Sonde.ON	Armado	Normal	10	2020-10-26 23:00:49
36	601	Temp. Nod.Dat.	Sire.OFF)Mail.ON(Sonde.ON	24.8	Nivel normal	0	2020-10-26 19:23:17
36	601	Temp. Nod.Dat.	Sire.OFF)Mail.ON(Sonde.ON	24.7	Nivel normal	0	2020-10-26 19:23:30
36	601	Temp. Nod.Dat.	Sire.OFF)Mail.ON(Sonde.ON	24.8	Nivel normal	0	2020-10-26 19:23:43
36	601	Temp. Nod.Dat.	Sire.OFF)Mail.ON(Sonde.ON	24.7	Nivel normal	0	2020-10-26 19:24:23
36	601	Temp. Nod.Dat.	Sire.OFF)Mail.ON(Sonde.ON	24.8	Nivel normal	0	2020-10-26 19:24:37
36	601	Temp. Nod.Dat.	Sire.OFF)Mail.ON(Sonde.ON	24.7	Nivel normal	0	2020-10-26 19:25:32
36	601	Temp. Nod.Dat.	Sire.OFF)Mail.ON(Sonde.ON	24.8	Nivel normal	0	2020-10-26 19:25:45
36	601	Temp. Nod.Dat.	Sire.OFF)Mail.ON(Sonde.ON	24.7	Nivel normal	0	2020-10-26 19:26:26

En caso de requerir las gráficas se deberá:

- Seleccionar una unidad en específico dentro las opciones de la lista, o si se requiere, seleccionar Todas las unidades.
- Seleccionar el sensor del cual se quiere obtener la gráfica.
- Seleccionar fecha y hora de inicio.
- Seleccionar fecha y hora final.
- Presionar el botón Graficar para obtener la gráfica.
- Se abrirá una nueva pestaña donde se mostrará la gráfica requerida



En el eje horizontal de la gráfica se tiene el tiempo medido por fecha y hora. En el eje vertical se tiene el parámetro seleccionado en este caso Temperatura. Las líneas color naranja y rojo delimitan la alerta baja y alarma baja respectivamente, es decir, si el nivel de temperatura sobrepasa la línea naranja, se activará la Alerta Baja. Y la línea azul es el comportamiento del sensor con los datos de temperatura tomados en el rango de tiempo.

2.9. Help Desk

Definición: Es la plataforma de servicio de atención al cliente, sirve para recepcionar todos los reclamos existentes del o de los usuarios.

Dentro de la página de *Help Desk* se ingresa a la etiqueta que dice “*Stop Masivo*”, para redireccionarlos a otra pantalla, en la cual se visualizan las caídas masivas, donde se nos presenta una lista de productos que no pueden ingresar a sus sesiones conjuntamente con la zona afectada, esto se verifica cuando se tienen alarmas críticas(rojas) en Pandora o WhatsUp Gold, en este ejemplo no se presentan alarmas y la lista está en blanco:



También está la pestaña de “MedicionesSAI”, donde se ve detalladamente el listado de mediciones SAI:

LISTADO MEDICIONES SAI

TECNOLOGIA	MODULO	LATENCIA	JITTER	% DOWN ALCANZADO	% UP ALCANZADO	ULTIMA LECTURA
VDGL	CENTRO_I_SAI	13.54	86.22	95	95	2020/11/02 20:31:49
VDGL	CORDEZ_I_SAI	13.43	86.45	95	95	2020/11/02 20:31:50
VDGL	SACHE_I_SAI	13.39	86.21	92	94	2020/11/02 20:31:50
VDGL	SAGBA_PUEBLO_I_SAI	15.21	86.25	90	97	2020/11/02 20:31:50
VDGL	NORTE_I_SAI	13.57	86.25	95	94	2020/11/02 20:32:00
VDGL	HPO_I_SAI	13.37	86.22	95	95	2020/11/02 20:31:51
VDGL	MANA_I_SAI	18.09	86.35	95	99	2020/11/02 20:31:49
VDGL	Danipco	12.33	86.29	92	97	2020/11/02 20:31:49
GPON	GPON_LIN_SAI	82.38	86.23	90	94	2020/11/02 20:31:52
GPON	GPON_LIN_QueraQuera	82.31	86.11	90	90	2020/11/02 20:31:50
GPON	GPON_LIN_NORTE	82.29	86.25	92	92	2020/11/02 20:31:49
GPON	GPON_LIN_HOPOGONGO	82.94	86.87	90	90	2020/11/02 20:31:48
ADSL	ISAPL_SAI	15.31	86.31	90	95	2020/11/02 20:31:52
ADSL	ISAPL_PAGOTA	18.31	87.34	90	90	2020/11/02 20:31:48
ADSL	ISAPL_BESUD	46.98	81.55	87	94	2020/11/02 20:31:53

actualiza cada 10 minutos

Ejemplo de detección de falla:

- Para detectar falla en un equipo en la herramienta Help Desk, una vez ingresado se debe ir a la opción de Datos Técnicos.



- Luego se mostrará en la ventana la LISTA DETALLADA DE DATOS TÉCNICOS, y en ésta se debe seleccionar el equipo del cual se requieren ver los datos técnicos.
- Se puede seleccionar un número de bloque en específico o la opción Todos. Estos bloques son las tarjetas de abonados del equipo seleccionado.
- También, se puede seleccionar el estado del equipo o la opción Todos por defecto.



- Al seleccionar los datos anteriores se abrirá en la ventana la lista detallada de datos técnicos del equipo que se muestra como en la siguiente imagen y se debe seleccionar un Producto. Este atributo significa el número de orden del abonado o ID.
- Posteriormente se abrirá una nueva ventana donde se podrá ver el Detalle Actual de Navegación; en ese sentido, si se tiene una falla en el último atributo Tipo se encontrará en Stop.
- Caso contrario al anterior o cuando el equipo ya se encuentre levantado, se encontrará en Start.

3. Desarrollo de tickets o difusiones

Se desarrolló un punto específico para el conocimiento de la realización de todos los informes/tickets/difusiones que se manejan dentro del trabajo.

En este apartado del documento se hablará de de los 3 tipos de informes dentro el programa “Mantis”, a lujo de detalle y de fácil comprensión.

3.1 DAC (Difusión de Apertura y Cierre)

Estas difusiones o tickets, se caracterizan por la causa del incidente, la cual siempre es “Desconocida” y tener una duración de 1 hora, o ser indeterminado o inclusive más de un turno (6 horas).

Estos incidentes generalmente pueden tratarse de caídas de equipos o caídas de enlaces los cuales tienen afección a algún servicio.

- Desarrollo:

- 1.- Para proceder a abrir un DAC se selecciona 02 - Incidente DAC en opciones de Proyecto.
- 2.- Se selecciona la opción Reportar Incidencia, la cual abrirá la ventana en la que se llenará toda la información pertinente del DAC.
- 3.- Se verifica que la categoría esté en DAC y el tipo de Severidad del DAC coincida con el incidente.
- 4.- Se especifica el nombre del Incidente, el cual involucra el nombre del enlace o equipos afectados, y también la causa del incidente la cual inicialmente es "Desconocida".

- 5.- Se redacta todo el procedimiento que el personal del "Monitoreo Servicios y Recursos NOC" en turno ha realizado para la notificación del incidente al área correspondiente y también a su personal de turno, redactando las indicaciones que se dieron.

Incidente	0014834: En estado Down BSP TELEFONICA 2 DESAGUADERO-LPZ vía NUEVATEL - TELEFONICA 1 DESAGUADERO vía COMTECO IGR-7750 TELEFONICA 2 DES
Causa del Incidente	Desconocido
Acción tomada (por agente NOC)	se informo a DWDM Ing R. Martinez y por Whats up se publico en el Noc Emergencia, Pamela indica que lo esta revisando

6.- Se coloca la hora y fecha pertinente al incidente el cual se lo saca de WhatsUP Gold o Pandora, o también lo puede indicar el responsable de área con el que se comunicó para dar solución al incidente, y también la hora de notificación del incidente el cual debe ser en el transcurso de 10 minutos y no más.

7.- Se seleccionan las áreas a las cuales se haya notificado el incidente, luego se coloca el nombre del o los encargados en turno con el que se comunicó.

8.- Se finaliza enviando el reporte; ya en el transcurso del turno se complementarán los detalles faltantes del DAC o incluso si el DAC se cierra en el mismo turno, se complementa toda la información y se cierra el mismo DAC.

NOTA: La obtención de más información por parte de los responsables, debe ser acotado al DAC abierto, rellenando información en los apartados de acuerdo a la información. De igual forma cualquier detalle nuevo de status del problema referido por medio del responsable u correos electrónicos, deben ser añadidos como NOTAS dentro del ticket DAC abierto.

3.2 DIN (Difusión de Información)

Este tipo de difusión se caracteriza por llenarse generalmente cuando el evento/incidente es atribuible a un equipo de la empresa o proveedor interno, se caracteriza por tener la información completa del evento/incidente (nombre de incidente, causa, hora inicio, hora final y acción tomada por el agente de "Monitoreo de Servicios y Recursos NOC"), que se llena cuando la duración del problema transcurre dentro del turno .

➤ Desarrollo:

MANTIS Sistema de Tickets

Proyecto: [03 - Incidente DIN] [Cambiar] **1**

Principal | Mi Vista | Ver Incidencias | **Reportar Incidencia** **2** | Mi Cuenta | Cerrar Sesión

Buscar: [] Filtrar [] [Filtros avanzados] [Crear Enlace Permanente]

Mostrando Incidencias (1 - 50 / 120) [Imprimir Informes] [Gráfico] [Exportar a CSV]

ID	Categoría	Severidad	Estado	Fecha de Registro	Descripción
0014725	DIN	Caída Parcial	Informada (usuario29)	13-10-2020	CAIDA DE ENLACE CAPINOTA - IRPA IRPA - TRANSPORTE
0013633	DIN	Caída Parcial	Informada (usuario29)	29-02-2020	Down enlaces: TELEFONICA 1 DESAGUADERO vía CC
0014617	DIN	Caída Parcial	Informada (usuario29)	23-09-2020	MADRUGADA
0014293	DIN	Caída Parcial	Informada (usuario29)	15-07-2020	Reclamos por acceso a Herramienta HelpDesk
0014128	DIN	Caída Parcial	Informada (usuario29)	15-07-2020	Reclamos por acceso a Herramienta HelpDesk

1. Al ingresar a la aplicación Mantis se debe seleccionar la opción 03 - Incidente DIN.
2. Posteriormente, se selecciona la opción Reportar Incidencia para crear una nueva.
3. Al ingresar a la nueva incidencia (DIN) se debe confirmar la categoría.
4. Luego, se debe seleccionar la seguridad.

5. Se debe dar una breve descripción del incidente indicando la causa, lugar y afección en el apartado Incidente.

6. En el apartado Causa del Incidente se debe dar una descripción del mismo según los datos brindados del o los encargados de las áreas donde se presenta el incidente.
7. En el apartado Acción tomada (por agente Monitoreo de Servicios y Recursos NOC) se debe describir los pasos y acciones que se siguieron desde que se reconoce la alarma, hasta

que se comunica al o los encargados de las áreas y se obtiene información acerca de la causa de las alarmas.

8. Se debe llenar el inicio del incidente que se obtiene de Pandora o WhatsUp Gold; luego, la hora de notificación del incidente que es la hora en la que se notifica al área correspondiente y al grupo de Emergencia en WhatsApp que no debe pasar los 10 minutos de diferencia con la hora de inicio y luego, la hora de solución del incidente cuando se obtiene este dato del encargado del área a la que se notifica.

9. En el apartado Duración de la Incidencia se debe colocar la resta en minutos desde que se inicia hasta que se termina el incidente.

10. También, se deben seleccionar los servicios afectados según la información obtenida.

11. Del mismo modo, seleccionar los servicios afectados de manera específica.

12. Se deben describir los servicios afectados.

13. También, se deben seleccionar los enlaces afectados.

14. Se debe especificar el tramo afectado.

15. También, si el incidente es atribuible a equipos, y especificar los mismos.

16. En caso de ser atribuible a equipos, colocar su descripción.

17. Seleccionar el área o las áreas a las que se notificó el incidente.

18. De la misma manera, describir a los responsables con los que se comunicó para la notificación del incidente.

19. En el apartado Observaciones se debe describir con más detalle la causa del incidente según la información obtenida.

20. Se tiene la opción de subir archivos y notas para tener más información y respaldo del incidente.

21. Finalmente, se debe seleccionar Enviar Reporte.

The image shows a web form for incident reporting. The form is divided into several sections with a blue sidebar on the left. The sidebar contains the following labels: « Tramo Afectado, Atribuible a Equipos, Descripción Equipos, Áreas Notificadas, Se informó al responsable(s), and Observaciones de cierre (por agente NOC). The main form area contains several input fields and checkboxes. Red circles with numbers 14 through 21 are placed over specific parts of the form to indicate where information should be entered or selected. The form includes a 'Subir Archivo' section at the bottom left, a 'Seleccionar archivo' dropdown, and an 'Enviar Reporte' button at the bottom right.

14. Tramo Afectado

15. Atribuible a Equipos

16. Descripción Equipos

17. Áreas Notificadas

18. Se informó al responsable(s)

19. Observaciones de cierre (por agente NOC)

20. Subir Archivo (Tamaño Máximo: 5,000K)

21. Enviar Reporte

3.3 ITU (Informe de Turno)

Este es un tipo de reporte, generado para justificar, anotar y guardar todos los eventos y problemas generados dentro un turno de trabajo específico; también, todas las observaciones emitidas en el turno de trabajo respecto a problemas, caídas y notificaciones importantes que se puede obtener en los grupos de apoyo existentes como el de WhatsApp.

➤ Desarrollo:

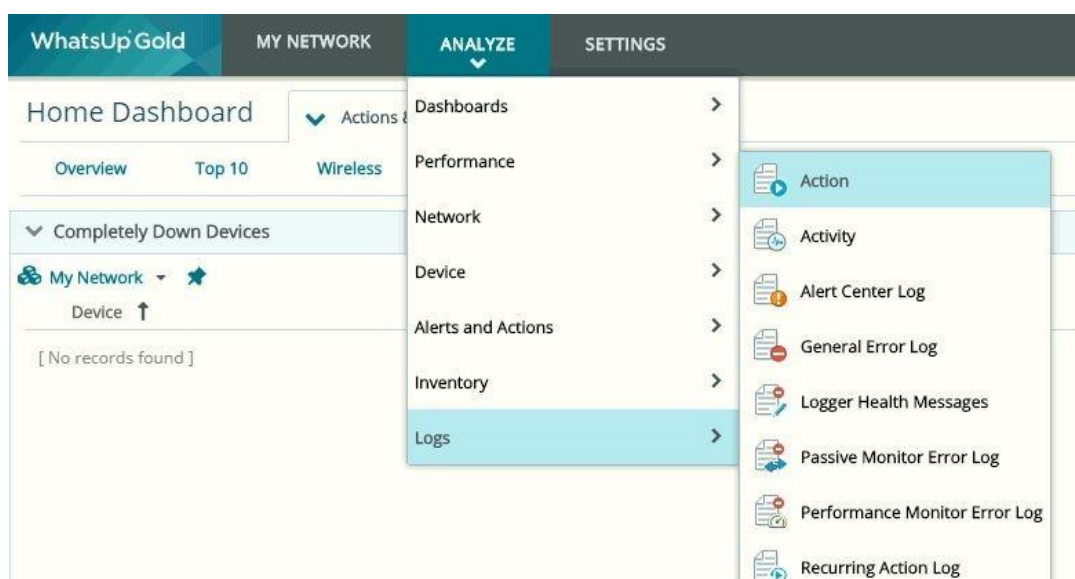
1. Una vez ingresado a la aplicación Mantis, se busca en la interfaz, la parte superior izquierda, y se realiza clic derecho en “Proyecto” para que se despliegue el menú y luego seleccionar “01 - Informe de Turno”, como se muestra en la siguiente imagen.
2. Una vez abierta la ventana para realizar el ITU, se debe seleccionar el turno en el que se tuvo la actividad laboral, que puede ser (madrugada, mañana, tarde o noche).

3. En la sección de “Observaciones” se debe ingresar todas las incidencias que se tuvieron durante el turno de trabajo, con el mayor detalle posible, especificando horarios, nombre del personal que atendió alguna anomalía o problema, situaciones de DAC cerrados en el turno, incidencias menores o mayores de cualquier índole.
4. En la sección de Trabajos Pendientes, se debe escribir todas las alarmas pendientes a realizar seguimiento; de la misma forma con algún DAC abierto,

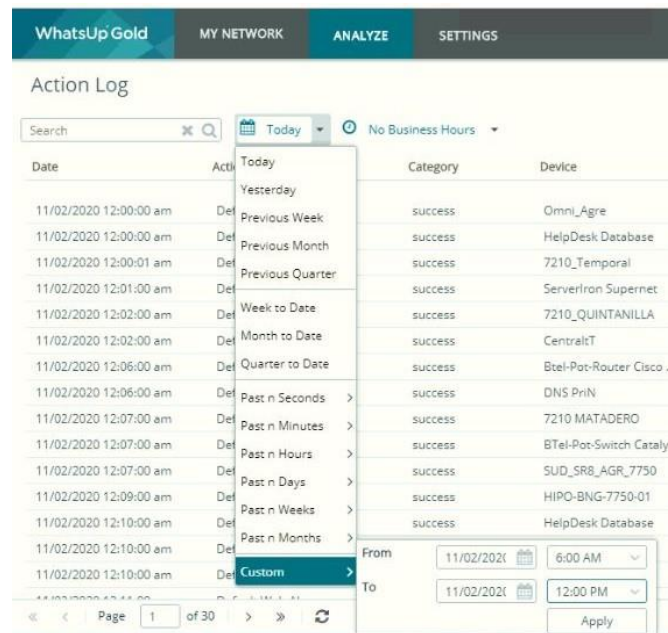
esperando ser cerrado en el próximo turno. Este apartado del formulario se lo utiliza cuando lo que se queda en stand by sale del horario de trabajo y le corresponde al siguiente personal de turno estar pendiente de la o las situaciones.

5. En el apartado de “Servicios Afectados” solo marcar el ícono de NINGUNO si no se presentaron eventos con afección de servicio; caso contrario, marcar los servicios afectados correspondientes a la afección de servicio.
6. En el apartado de “Actividades del Turno (Monitoreo)” realizar clic derecho a todos los íconos, excepto al de BACK UP DIARIO.
7. En este apartado se debe extraer la información de todas las alertas de SUPERNET y Boliviatel de WhatsUp Gold

7.1 En la interfaz de WhatsUp Gold, ingresar a ANALYZE, luego a Logs y por último a Action.



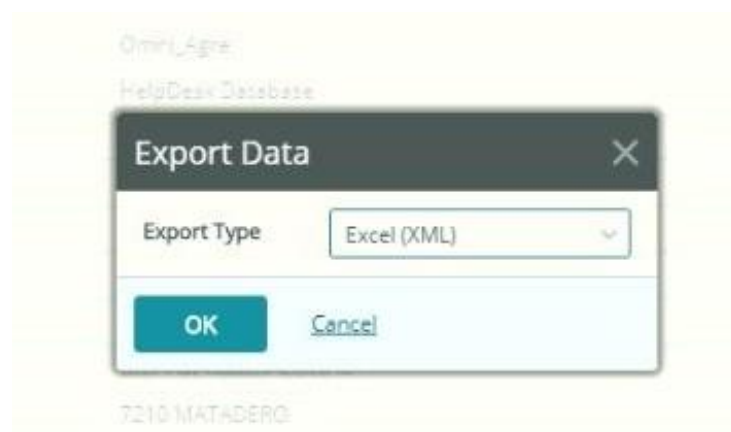
7.2. Luego seleccionar la fecha y horas correspondientes al turno.



7.3. En la parte superior derecha se selecciona la opción Data.



7.4. Posteriormente aparecerá el cuadro para seleccionar el formato del documento a guardar y se deberá seleccionar formato .xml; de esta manera se podrá abrir el documento en excel.



7.5. Se guarda como extensión excel, lo que se exporta desde el WhatsUp Gold, se abre en un Excel y se extrae una tabla dinámica con los datos específicos de

Supernet y Boliviatel. Los datos que corresponden a Boliviatel se deben colocar en el apartado de Alertas Boliviatel y las demás en Alertas Supernet.

	A	B	C	D	E	F	G	H	I
1	Action Log								
2	Date Range: 11/02/2020 12:00 PM - 11/02/2020 6:00 PM, Business Hours: No Business Hours								
3									
4	Date	Action	Category	Device	Active Monitors	Active Monitors	Active Monitors	Active Monitors	Details
5	44137.5	Default W success		7210 Tem					Down at 11 Action was successful.
6	44137.5	Default W success		HelpDesk					Down at 11 Action was successful.
7	44137.5	Default W success		Omni Ag					Down at 11 Action was successful.
8	44137.5	Default W success		ServerIron					Down at 11 Action was successful.
9	44137.5	Default W success		7210 QUI					Down at 11 Action was successful.
10	44137.5	Default W success		CentralT					Down at 11 Action was successful.
11	44137.5	Default W success		Btel-Pot					Down at 11 Action was successful.
12	44137.5	Default W success		DNS Prin					Down at 11 Action was successful.
13	44137.5	Default W success		Btel-Pot					Down at 11 Action was successful.
14	44137.5	Default W success		SUD SR8					Down at 11 Action was successful.
15	44137.5	Default W success		7210 MAT					Down at 11 Action was successful.
16	44137.51	Default W success		HIPO-BNC					Down at 11 Action was successful.
17	44137.51	Default W success		Cisco SG3					Down at 11 Action was successful.
18	44137.51	Default W success		7210 HUA					Down at 11 Action was successful.
19	44137.51	Default W success		CENTRO-B					Down at 11 Action was successful.
20	44137.51	Default W success							Down at 11 Action was successful.
21	44137.51	Default W success							Down at 11 Action was successful.
22	44137.51	Default W success							Down at 11 Action was successful.
23	44137.51	Default W success							Down at 11 Action was successful.
24	44137.51	Default W success							Down at 11 Action was successful.
25	44137.51	Default W success							Down at 11 Action was successful.

Alertas Supernet
7.5

Alertas Boliviatel
7.5

Subir Archivo (Tamaño Máximo: 5,000K)
Seleccionar archivo
Ningún archivo seleccionado

* Requerido

Enviar Reporte
7.6

7.6. Finalmente se selecciona Enviar Reporte a la hora “en punto” al finalizar el turno.

IV. RECOMENDACIONES PARA EL PERSONAL DEL MSR NOC

1. Siempre respetar horarios de trabajo, tanto de entrada y salida.
2. Como departamento de Monitoreo de Servicios y Recursos NOC en la empresa, el personal de turno debe estar pendiente de los responsables que estén de turno de igual forma en los otros departamentos para un ámbito de trabajo más eficiente y óptimo.
3. Al inicio del trabajo en turno es obligatorio revisar el ITU o informe de turno anterior para revisar las observaciones que se han dado conjuntamente con las tareas pendientes que se pudieran dejar para el turno vigente.
4. El trabajo y monitoreo debe darse hasta el último minuto del turno ya que cualquier eventualidad o alarmas masivas pueden ocurrir en ese corto lapso.
5. Una difusión DAC, solo debe ser creada ante cualquier situación generada en los gestores como alarmas críticas y mayores que generen una afectación de servicios.
6. Las alarmas para cada gestor o ventana de monitoreo deben ser notificadas en los grupos correspondientes pasado los 15 min y se tiene un máximo de 10 min. para generar un reporte o difusión que respaldada por la respuesta del personal responsable a la que le compete dicha alarma, si es que se mantienen en los gestores en esos lapsos.
7. Si los responsables de turno en otras áreas no llegan a contestar las llamadas o mensajes, se procede a llamar al jefe de área para obtener más información sobre las alarmas que se presentan correspondientes a dicha área, con el fin de no dejar pasar el tiempo.
8. El personal de turno del departamento de Monitoreo de Servicios y Recursos NOC, debe estar continuamente pendiente de los emails, recepcionados en Outlook, por la importancia que dichos emails pueden generar, no se debe olvidar que esta aplicación es el medio de comunicación con proveedores internos y externos.
9. Siempre ser claro y minucioso al realizar las distintas difusiones o reportes, ya que, la veracidad de lo que se escribe, la calidad de escritura para ser coherente y entendible (horas de caída, notificaciones, personal responsable, etc.) ayudará a gestionar los problemas que puedan ocurrir con mayor eficiencia.
10. Ser proactivo y práctico para realizar el monitoreo en el departamento de Monitoreo de Servicios y Recursos NOC; el tiempo es importante y no se debe subestimar alarmas que puedan ser menores, mayores o críticas, ya que pueden desencadenar en "AUSENCIA DE SERVICIO" que va en contra de la regla principal de la empresa.
11. Como personal del departamento de Monitoreo de Servicios y Recursos NOC, siempre estar regularmente al tanto de posibles cambios de contraseñas o actualizaciones y notificarlas al grupo en común.