



AGENCIA PARA LA REINCORPORACIÓN Y NORMALIZACIÓN (ARN)

GUÍA SERVICIO CENTRO DE GESTIÓN Y OPERACIONES DE RED - NOC

	GUÍA SERVICIO CENTRO DE GESTIÓN Y OPERACIONES DE RED - NOC	CÓDIGO: TI-G-13	
		FECHA 2021-06-10	VERSIÓN V- 1

BOGOTÁ D.C. JUNIO DE 2021

Tabla de contenido

1. OBJETIVO.....	3
2. ALCANCE.....	3
3. DEFINICIONES	3
4. CONTENIDO Y DESARROLLO.....	3
5. MODELO OPERATIVO	5
5.1. HERRAMIENTAS TECNOLÓGICAS	5
5.2. GRUPO DE MONITOREO.....	5
5.3. GRUPO DE OPERACIÓN	6
5.4. RECURSOS	6
5.5. OPERACIÓN DEL NOC.....	8
5.1. Descripción de Actividades.....	8
5.6. ENTRADAS	10
5.7. SALIDAS	10
5.8. INDICADORES DE GESTIÓN (ANS).....	10
5.9. INFORMES PERIÓDICOS.....	10
5.10. FORMATOS	10

	GUÍA SERVICIO CENTRO DE GESTIÓN Y OPERACIONES DE RED - NOC	CÓDIGO: TI-G-13	
		FECHA 2021-06-10	VERSIÓN V- 1

1. OBJETIVO

Monitorear la infraestructura de red y conectividad de la ARN a nivel de Data Center, Enlaces WAN, Equipos LAN/WLAN, Telefonía IP, Storage, Servidores, servicios web, monitoreo de cumplimiento de ANS de terceros (canales de datos, servicio de centro de datos), Aplicaciones y Transacciones, mediante la herramienta de monitoreo SolarWinds, para anticipar eventos y prevención de problemas.

2. ALCANCE

Aplica para todos los servicios TI que están relacionados en el catálogo de servicios y que pueden implementarse en la herramienta de SolarWinds.

3. DEFINICIONES

ANS: Acuerdos de Niveles de Servicio.

ARN: Agencia para la Reincorporación y la Normalización.

ARANDA: Herramienta de Gestión.

BW (Bandwidth): Ancho de Banda de un canal de comunicaciones.

CAB (Change Advisory Board): Comité de Cambios

CI: Cualquier componente u otro activo del servicio que necesite ser gestionado con el objeto de proveer un servicio de TI. Elemento de configuración.

CMDB (Configuration Management Data Base): Base de Datos de la gestión de Configuración.

ECAB (Emergency Change Advisory Board): Comité de Cambios de Emergencia.

GT: Grupos Territoriales.

LAN (Local Area Network): Red de área local.

KDB (Knowledge data base): Base de Datos de Conocimiento.

NOC (Network Operation Center): Centro de Gestión y Operaciones de Red.

SOLARWINDS: Herramienta utilizada para monitorear el desempeño de la Infraestructura TI y los servidores enfocados a Datacenter.

PM (PROBLEMA): Incidentes repetitivos o de gran impacto, de los cuales se desconocen las causas que los originan.

RFC (REQUEST FOR CHANGE): Es una solicitud formal para la implementación de un Cambio.

4. CONTENIDO Y DESARROLLO

- La atención del servicio NOC tiene una disponibilidad de 7x24

	GUÍA SERVICIO CENTRO DE GESTIÓN Y OPERACIONES DE RED - NOC	CÓDIGO: TI-G-13	
		FECHA 2021-06-10	VERSIÓN V- 1

- Para gestionar los incidentes una vez presentado el evento o alerta en la herramienta de monitoreo SolarWinds se debe verificar si la causa se atribuye a un evento masivo, el cual afecta la operación y disponibilidad de algún servicio TI.
- Si el incidente se presenta en horario hábil, se registra en la herramienta Aranda, se contacta al Soporte Nivel 2 o Asistentes de Información cuando sea una alerta en GT; pero si se trata de un servidor, servicio y/o aplicación, contacta al especialista responsable según matriz de escalamiento.
- Se revisa la gráfica de consumo de BW de la sede o las sedes que apliquen. Para ello se utiliza la herramienta de monitoreo SolarWinds.
- Se analiza la gráfica de monitoreo de SolarWinds y si se evidencia una caída significativa en el tráfico, debe informarse de inmediato al responsable según matriz de escalamiento, esto teniendo en cuenta el horario de disponibilidad del personal y la criticidad.
- Se realizan pruebas de conectividad desde el NOC hacia la(s) sede(s), verificando en la herramienta de SolarWinds y corroborando la información a través de cisco Meraki.
- Si se presenta una falla eléctrica en la(s) sede(s), el NOC revisa la matriz de contactos, donde realiza los siguientes niveles de consulta:
 - Nivel de consulta 1: Guarda de Seguridad la(s) sede(s),
 - Nivel de consulta 2: Asistente de Información de la(s) sede(s),
 - Nivel de consulta 3: Asistente Administrativo de la(s) sede(s),
 - Nivel de consulta 4: Profesional Especializado 21C de la OTI sede Central
 - Nivel de consulta 5: Profesional Especializado 19G de la OTI sede Central
 - Nivel de consulta 6: Jefe de Oficina 20 de la OTI sede Central
 - Los horarios de consulta se relacionan en la matriz de contactos ARN.
- Si las pruebas realizadas son exitosas, el NOC realiza el escalamiento al líder de conectividad para descartar alguna falla a nivel de gestión desde el Datacenter (donde se encuentran alojados los servidores de las herramientas de gestión y monitoreo).
- Se realiza la apertura de un caso para seguimiento con los proveedores involucrados. Esto dependiendo del resultado del diagnóstico realizado anteriormente.

 <p>Agencia para la Reincorporación y la Normalización - ARN</p>	GUÍA SERVICIO CENTRO DE GESTIÓN Y OPERACIONES DE RED - NOC	CÓDIGO: TI-G-13	
		FECHA 2021-06-10	VERSIÓN V- 1

Está dentro alcance NOC: reportar latencias, fallas en enlaces WAN, novedades a nivel LAN, WLAN, Telefonía IP, aplicaciones y servidores físicos y virtuales. No está dentro del alcance del NOC: configurar tarjeta de UPS, sin embargo, se debe incluir en la bitácora.

5. MODELO OPERATIVO

El NOC está conformado por las herramientas y recursos que constituyen:

5.1. HERRAMIENTAS TECNOLÓGICAS

Su implementación está orientada a la detección de eventos relevantes y seguimiento de las acciones de respuesta e incluye:

- **Herramientas de Monitoreo:** Detecta y recolecta eventos e incidentes sobre la infraestructura de servicio a través del monitoreo continuo y automatizado, facilitando la gestión operativa y acciones de respuesta por parte del personal encargado.
- **Herramienta de Gestión:** permite realizar el registro y seguimiento de los Incidentes, Requerimientos, Problemas y Cambios a través de todo su ciclo de vida.

5.2. GRUPO DE MONITOREO

Organizado por los ingenieros a cargo de la gestión a través de las Herramientas de Monitoreo en primera línea, su función está enfocada a la gestión de alarmas, que incluye la verificación, categorización, priorización, diagnóstico básico y verificación de las condiciones del entorno en que se presentan las alarmas, para generar el escalamiento correspondiente.

En comunicación con los asistentes de información de la ARN, pueden solicitar desplazamiento para verificación de condiciones físicas y eléctricas. Cuentan con acceso para ejecución de listas de chequeo sobre componentes de la plataforma y en caso de ser requerido, realizan escalamiento a personal más especializado.

En las actividades programadas por parte del cliente para renovación o mantenimiento del servicio, se informa al NOC por parte de los administradores y se recolectan pruebas iniciales antes de la ventana de mantenimiento y pruebas finales después de la actividad.

 <p>Agencia para la Reincorporación y la Normalización - ARN</p>	GUÍA SERVICIO CENTRO DE GESTIÓN Y OPERACIONES DE RED - NOC	CÓDIGO: TI-G-13	
		FECHA 2021-06-10	VERSIÓN V- 1

5.2.1. Objetivo del Grupo de Monitoreo

- Identificar alarmas para detectar incidentes, ejecutar procedimientos operativos básicos y realizar escalamientos para reestablecer el servicio en el menor tiempo posible.
- Coordinar actividades con los grupos de Mesa de Servicio, Soporte en Sitio, Red LAN / WLAN, Telefonía IP, Gestión de Eventos, Gestión de Incidentes y Gestión de Proveedores.
- Este equipo está enfocado a la gestión de eventos detectados en las Herramientas de Monitoreo, por lo que no atiende solicitudes de servicio y no hace parte del esquema de comunicación y reportes hacia el usuario final.

5.3. GRUPO DE OPERACIÓN

5.3.1. Objetivo del Grupo de Operación

Este grupo está orientado a la ejecución de procedimientos de verificación de las plataformas, para monitorear de manera proactiva y sistemática los diferentes componentes. Su objetivo es identificar riesgos potenciales, para que se generen acciones preventivas y correctivas por parte del líder de cada servicio.

5.4. RECURSOS

5.4.1. Recursos de Personal

- Analista NOC
- Coordinador NOC
- Líder NOC

5.4.2. Roles y Responsabilidades

Rol	Responsabilidades
Analista NOC	<ul style="list-style-type: none"> - Monitorear, realizar pruebas de primer nivel, reportar, documentar los eventos que se observen en las herramientas definidas para el servicio. - Informar y / o notificar a líderes de servicios o a proveedores de acuerdo con la matriz de escalamiento.

	GUÍA SERVICIO CENTRO DE GESTIÓN Y OPERACIONES DE RED - NOC	CÓDIGO: TI-G-13	
		FECHA 2021-06-10	VERSIÓN V- 1

Rol	Responsabilidades
	<ul style="list-style-type: none"> - Realizar seguimiento a tickets y notificar al líder NOC la falta de avances.
Coordinador NOC	<ul style="list-style-type: none"> - Garantizar el seguimiento a los eventos generados de forma proactiva desde el NOC. - Garantizar la calidad de la información entregada en la bitácora, "BitacoraMMAAAAMTBF.xlsx" - Realizar escalamientos internos a proveedores en los casos donde no se tenga avances. - Garantizar el cubrimiento del servicio 7 x 24 con la asignación de turnos.
Líder NOC	<ul style="list-style-type: none"> - Realizar gestión al seguimiento de los casos donde no se tenga avances. - Buscar planes de mejora donde se identifiquen fallas o deficiencias en la prestación del servicio que pongan en riesgo el cumplimiento de los ANS.
Líder de Servicio	<ul style="list-style-type: none"> - Reportar cualquier evento relacionado con los servicios que se monitorean para que sean verificados en las herramientas y así se tomen las acciones que correspondan para prevenir eventos que afecten los servicios - Informar ventanas de mantenimiento y cambios relacionados con infraestructura y elementos de configuración monitoreados, actualizaciones, fallas masivas que puedan generar alarmas en la herramienta, con el objetivo de evitar el reporte de incidencias relacionadas con el mantenimiento o ventanas programadas, sino que se haga seguimiento a la actividad reportada.
Dueño Servicio NOC	<ul style="list-style-type: none"> - Velar por el buen funcionamiento del servicio y tomar las decisiones pertinentes. - Revisar que se está dando cumplimiento a los ANS - Revisar y dar el visto bueno a los informes mensuales

5.4.3. Recursos técnicos

Herramienta	Nombre	Alcance
Software	Aranda	Gestión de incidentes y requerimientos

	GUÍA SERVICIO CENTRO DE GESTIÓN Y OPERACIONES DE RED - NOC	CÓDIGO: TI-G-13	
		FECHA 2021-06-10	VERSIÓN V- 1

Herramienta	Nombre	Alcance
Software	SolarWinds	Visualizaciones de eventos e incidentes
Portal web	Cisco Meraki	Visualizaciones de alamas y gestión de equipos activos
Hardware	Pc estándar	Herramienta de cómputo para uso operativo
Hardware	Teléfono móvil	Matriz de contactos de ARN / Matriz de escalamiento
Telecomunicaciones	Canal dedicado / internet / VPN	Tener acceso a la infraestructura de la ARN para brindar soporte

5.5. OPERACIÓN DEL NOC

5.1. Descripción de Actividades

No.	Actividad	Descripción
1	Realizar el Monitoreo de las herramientas	El Proceso se realiza 7 x 24 gestionando los eventos y/o incidentes una vez se visualicen en las herramientas asignadas para tal fin.
2	Generar caso en la herramienta de gestión	<p>Registrar en la herramienta de gestión la falla presentada, adjuntando todas las pruebas y las validaciones realizadas. Posteriormente se envía correo al dueño del servicio indicando la falla y se asigna de acuerdo con la matriz de escalamiento.</p> <p>En caso de falla en la herramienta de gestión, se debe documentar de forma manual y posteriormente se registrará en la herramienta de gestión cuando esté disponible.</p>
3	¿Es un incidente masivo?	Si es un incidente masivo pasar a la actividad No.14 Si no es un incidente masivo pasar a la actividad No. 4
4	Diligenciar CheckList NOC	Realizar el diligenciamiento del CheckList NOC. del servicio que corresponda y hacer validaciones con el personal encargado según la matriz de escalamiento.

	GUÍA SERVICIO CENTRO DE GESTIÓN Y OPERACIONES DE RED - NOC	CÓDIGO: TI-G-13	
		FECHA 2021-06-10	VERSIÓN V- 1

No.	Actividad	Descripción
5	Documentar en la herramienta de gestión	Documentar adecuadamente en la herramienta de gestión adjuntando los soportes correspondientes identificados en el CheckList.
6	¿Está dentro del Alcance del NOC?	Si está dentro del alcance del NOC, pasar a la actividad 7 Si no está dentro del alcance del NOC, pasar a la actividad 14 (Ver las Consideraciones Generales)
7	Realizar seguimiento y actividades	Realizar seguimiento y actividades necesarios para reestablecer el servicio, si está dentro del alcance del NOC
8	Entregar turno	El analista del NOC una vez finaliza su turno debe entregar el estado del monitoreo y la gestión de los casos, así como el seguimiento relacionado. Pasa a la actividad No. 1
9	¿Se solucionó la alarma?	Si se solucionó la alarma pasar a la actividad 10 Si no se solucionó la alarma regresa a la actividad 9
10	Documentar Bitácora	Registrar la misma documentación que se tiene en Aranda indicando el estado final para que en la entrega de turno estén los pendientes.
11	Enviar el reporte informando	Una vez se detecta la alarma se debe enviar el reporte informando a los interesados
12	Documentar el cierre	Documentar el cierre indicando su causa, la solución, y a quien es atribuible.
13	Comunicar al líder del servicio y el líder NOC	Una vez se detecta que es un incidente masivo, es decir afectación de más de 2 sedes, un servicio completo, una aplicación centralizada, o cualquier falla fuera de lo común que afecta el servicio, se debe comunicar por vía telefónica y por correo al líder del servicio afectado que se encuentra en la Matriz de escalamiento, al líder del NOC y registrar el incidente en la herramienta de gestión. Si es una falla eléctrica en alguna de las sedes, se debe remitir a la Matriz de escalamiento en el apartado NOC
14	Analizar la falla reportada	El líder del servicio analiza la falla y determina la solución a aplicar.
15	¿Se requiere RFC?	Si se requiere RFC, pasa a la actividad No. 16 Si no se requiere RFC, pasa a la actividad No. 17

	GUÍA SERVICIO CENTRO DE GESTIÓN Y OPERACIONES DE RED - NOC	CÓDIGO: TI-G-13	
		FECHA 2021-06-10	VERSIÓN V- 1

No.	Actividad	Descripción
16	Generar RFC	El líder del servicio genera el RFC y lo pasa a la gestión de Cambios.
17	Gestionar y Solucionar	El Líder del servicio se encargará con sus guías o escalando a proveedor la solución del ticket. (si ha sido escalado)

5.6. ENTRADAS

Entradas	Procedencia
Información de CI	Gestión de Activos y configuración

5.7. SALIDAS

Salidas	Procedencia
Asignación de Tickets	Herramienta de gestión
Informe de Gestión	Informe

5.8. INDICADORES DE GESTIÓN (ANS)

Según los ANS presentes en la gestión de ANS y su respectiva ficha técnica.

5.9. INFORMES PERIÓDICOS

Nombre	Objetivo	Frecuencia	Dirigido a
Informe de Gestión Mensual	Validar el cumplimiento de la prestación del servicio	Mensual	Jefatura OTI

5.10. FORMATOS

Matriz de Escalamiento
Check List NOC