

ESTRUCTURACIÓN DE UN CENTRO DE OPERACIÓN DE REDES (NOC)

Autores

Antonio García-Zaballos
Maribel Dalio
Jesús Garran
Enrique Iglesias
Pau Puig
Ricardo Martínez Garza

ESTRUCTURACIÓN DE UN CENTRO DE OPERACIÓN DE REDES (NOC)

Este documento se construyó con un esfuerzo multidisciplinario coordinado por la División de Conectividad, Mercados y Finanzas del Sector de Instituciones para el Desarrollo del Banco Interamericano de Desarrollo. Los autores agradecen las revisiones editoriales de Philip Keefer, Sarah Schineller y Julia Gomila; el apoyo logístico de Claudia Márquez, Silvana Cardozo y Shoany Flores, y el trabajo de diseño realizado por Word Express. Se agradece especialmente al Fondo General de España por el apoyo en la realización de la publicación y por el compromiso con el despliegue de infraestructura de conectividad digital en la región.

Código JEL: L52, L86, L88, O33, Q55

Palabras clave: infraestructura digital, centro de datos, regulación de telecomunicaciones, tecnologías de la información y la comunicación

Copyright © 2022 Banco Interamericano de Desarrollo. Esta obra se encuentra sujeta a una licencia Creative Commons IGO 3.0 Reconocimiento-NoComercial-SinObrasDerivadas (CC-IGO 3.0 BY-NC-ND) (<http://creativecommons.org/licenses/by-nc-nd/3.0/igo/legalcode>) y puede ser reproducida para cualquier uso no-comercial otorgando el reconocimiento respectivo al BID. No se permiten obras derivadas.

Cualquier disputa relacionada con el uso de las obras del BID que no pueda resolverse amistosamente se someterá a arbitraje de conformidad con las reglas de la CNUDMI (UNCITRAL). El uso del nombre del BID para cualquier fin distinto al reconocimiento respectivo y el uso del logotipo del BID no están autorizados por esta licencia CC-IGO y requieren de un acuerdo de licencia adicional.

Nótese que el enlace URL incluye términos y condiciones adicionales de esta licencia.

Las opiniones expresadas en esta publicación son de los autores y no necesariamente reflejan el punto de vista del Banco Interamericano de Desarrollo, de su Directorio Ejecutivo ni de los países que representa.



Banco Interamericano de Desarrollo
1300 New York Avenue, N.W.
Washington, D.C. 20577
www.iadb.org

Índice

Introducción	v
1 Centro de procesos de datos, centro de operaciones de seguridad y centro de operaciones de red	1
1.1 ¿Qué es un CPD?	1
1.2 ¿Qué es un SOC?	2
1.3 ¿Qué es un NOC?	3
<i>Gestión de red.</i>	5
Monitorización del tiempo de actividad	5
Gestión del rendimiento	6
Monitorización de la disponibilidad	6
Monitorización de los paquetes	6
<i>Conectividad.</i>	7
Monitorización de las URL	7
Gestión y monitorización de la LAN	7
Monitorización de ethernet	7
Monitorización de redes inalámbricas	8
<i>Gestión de los dispositivos de red</i>	8
Monitorización de routers	8
Monitorización de switches	8
Prevención del intrusismo en la red	8
2 ¿Cuál es la clave para que un NOC sea eficiente?	11
2.1 Organización y personas	14
2.2 Información y tecnología	17
2.3 Socios y proveedores	18
2.4 Flujos de valor y procesos	19

3	NOC: Punto clave en la digitalización	21
3.1	Cuestiones clave en la infraestructura de un país	25
3.2	Cuestiones clave en la infraestructura de las empresas	28
4	Estructura de un NOC	29
4.1	Modelo de servicio	29
4.2	Canales de atención	33
4.3	Niveles de soporte (TIERS)	34
	<i>Nivel 1 (Tier 1): Supervisar y responder</i>	35
	<i>Nivel 2 (Tier 2): Analizar, reparar e informar</i>	36
	<i>Nivel 3 (Tier 3): Administrar y mantener</i>	36
	<i>Nivel 4 (Tier 4): Proveedores (Nivel experto)</i>	37
4.4	Diferentes niveles de servicios	38
	<i>¿Qué debe incluir un ANS?</i>	38
	<i>Creación y mantenimiento del ANS</i>	39
	<i>ANS que debería implementar un NOC</i>	40
	<i>Prioridad del servicio</i>	41
	<i>Cuantificación de los ANS</i>	43
4.5	Servicio gestionado	43
	<i>Plan de calidad del servicio</i>	46
	<i>Informes de nivel de servicio</i>	46
	<i>Modelo de gobierno</i>	49
4.6	Herramientas del servicio	52
	<i>Herramienta de monitorización de la infraestructura de red</i>	53
	<i>Herramienta de ticketing</i>	54
	<i>Repositorio de documentación</i>	56
	<i>Herramienta de business intelligence</i>	57
	<i>Base de datos con los recursos y su conocimiento</i>	59
5	Beneficios de la implementación de un NOC eficiente	61

Introducción

La revolución digital está transformando todas nuestras prácticas socioeconómicas a nivel individual y colectivo, ya sea como ciudadanos, consumidores, empresas o sociedad.

Por su parte, las comunicaciones son un factor estratégico en el desarrollo de los países, y en concreto en América Latina, donde la brecha digital es más pronunciada que por ejemplo en Estados Unidos o Europa. Esta brecha digital es mayor si se tiene en cuenta la ubicación geográfica (ciudad o entorno rural).

La digitalización en la que se encuentra inmerso el mundo requiere de una infraestructura de comunicaciones potente, que va ligada a una velocidad mayor que la actual y a un menor tiempo de latencia. Esto se conseguirá con la tecnología 5G. El despliegue de esta nueva generación de tecnología habilitará la fusión del mundo físico (*Operational Technology, OT*) con el mundo digital (*Information Technology, IT*), a través del dato (conjuntamente con todo lo que conlleva: internet de las cosas, aprendizaje automatizado, prototipado, digital twin, etc.).

Para ello, es clave tener en funcionamiento centros de operaciones de red (*Network Operations Center, NOC*). Las empresas y las administraciones públicas necesitan organizar su infraestructura de red, sobre todo cuando deben traspasar grandes cantidades de datos, algo que es muy común en la actualidad. Como con todo sistema, es necesario contar con un grupo de control que se ocupe de mantener todo en orden, y aquí es donde entra la figura del NOC. Todas las empresas medianamente grandes tienen un NOC, ya sea propio o subcontratado. Son una pieza clave, ya que a través de sus redes mueven una cantidad ingente de información (muy sensible), la cual puede ser susceptible de ser monetizada.

El NOC¹ es un área especializada para el seguimiento y el control de las redes de comunicación, ya sean de internet, satélite o televisión. Podrá ser local o nacional, privado o público. Incluso en algunos casos podría llegar a ser híbrido, con servicios de

¹ En algunos países, al NOC se lo conoce como centro de control de red (CCR).

redes públicos (a ministerios, organizaciones públicas, empresas públicas) que escalan a ciudadanos o empresas. Su función principal es la de monitorizar las redes, atender los incidentes de red y, en casos de averías, desviar el tráfico a conveniencia, hasta que se resuelva el incidente. En pleno siglo XXI resulta impensable que se caigan las comunicaciones de un país o de una empresa, ya que el impacto económico y reputacional sería enorme.

Por otra parte, un NOC tiene que contar con un sistema de gestión de servicios con procesos, tecnología y un equipo profesional correctamente organizado. Si el NOC no está estructurado y sus procesos estandarizados —cómo se gestionan los incidentes de red y quién los atiende en cada caso— se incurrirá en demoras, quejas y reclamos en cuanto a la atención de requerimientos e incidentes, con lo que puede verse afectada la experiencia del cliente o ciudadano.

El objetivo principal de un NOC es que la infraestructura de red esté operativa. Para ello tendrá que cumplir dos objetivos secundarios: mejorar la disponibilidad y el rendimiento e incrementar la efectividad.

Centro de procesos de datos, centro de operaciones de seguridad y centro de operaciones de red

Hoy en día se confunden diferentes conceptos de gestión de infraestructura, como son el centro de procesos de datos (CPD), el centro de operaciones de seguridad (*Security Operation Center*, SOC) y el centro de operaciones de red (*Network Operations Center*, NOC). Normalmente, un CPD es más amplio y, en algunos casos, el proveedor de servicios puede estar suministrando los tres servicios desde allí.

En líneas generales, todas las empresas medianas y grandes así como las Administraciones de los países necesitan de los tres servicios.

1.1 ¿Qué es un CPD?

El CPD es un espacio físico con los siguientes componentes: hardware informático; equipos de red (routers, switches, etc.); sistema de seguridad física y perimetral (*firewalls*), y sistemas de almacenamiento. Los servicios que desarrollan dependerán de lo que haya contratado el cliente, llegando a una disponibilidad de 24 horas al día, 7 días de la semana, 365 días al año (24x7x365), con los acuerdos de nivel de servicio (ANS) (*Service Level Agreement*) contratados.

El CPD debe disponer de una infraestructura para poder realizar su actividad, la cual se compone básicamente de:

- Suministro de energía ininterrumpida (*Uninterruptible Power Supply*, UPS) en redundancia, con conexiones eléctricas y circuitos separados de la red normal y computacional.
- Sistemas de cableado estructurado con alta velocidad.
- Sistemas de aire acondicionado de precisión, así como controles automáticos de humedad y temperatura.
- Sistema de generador de energía, que brinde una función de misión crítica.
- Seguridad física y videovigilancia.

Además, tendrá una infraestructura de servidores con los que se brinde servicio de alojamiento a los clientes. Los servicios que puede brindar un CPD son los siguientes:

- *Housing*: servicio donde básicamente se alquila el espacio físico para que el cliente aloje sus servidores. Suministra la energía, la refrigeración, el acceso a internet y la protección física del servidor. Normalmente no les gusta a los gestores de infraestructura, ya que no aporta ningún valor.
- *Hosting*: conjunto de servicios donde se alquilan los servidores dedicados, se administran las aplicaciones (normalmente sistema operativo, bases de datos, servidor web y servidor de correo), se hacen las copias de seguridad y se monitoriza el sistema.
- *Cloud*: el uso de servidores remotos es la gran diferencia; están conectados a internet para almacenar, administrar y procesar datos. En lugar de depender de un servicio físico instalado, se tiene acceso a una estructura donde el hardware y el software están en formato virtual. Los gestores de infraestructura *Cloud*, tienen tres modalidades:
 1. *Cloud* pública: se utilizan y comparten servidores y servicios con otros usuarios.
 2. *Cloud* privada: la infraestructura es de un solo cliente. La gran diferencia con el *hosting* es la forma de pago (que es por uso) y la escalabilidad.
 3. *Cloud* híbrida: se tiene infraestructura en un entorno público (aquellas aplicaciones o servicios web que no son *core business*) y otra en un entorno privado (normalmente aquellas que son *core business*).

Por otro lado, el CPD tendrá una infraestructura para monitorizar el correcto funcionamiento de dichos aplicativos (propios o de cliente), así como las integraciones con otros sistemas (internos o externos a la compañía). A su vez, puede alojar al SOC y al NOC dentro de la misma ubicación, pero normalmente son áreas de trabajo separadas por seguridad física (por ejemplo, tarjeta de acceso a un área reservada). Se trata de grupos de trabajo diferentes, con diferentes conocimientos, pero que sí tienen que colaborar de forma conjunta.

1.2 ¿Qué es un SOC?

El SOC puede estar dentro de las instalaciones del CPD, pero es un servicio autónomo y con medidas de seguridad independientes. Se responsabiliza de monitorizar, identi-

ficar, investigar, priorizar, resolver o escalar los incidentes que tendrán un efecto sobre la seguridad de la información de la organización pública o privada.

El análisis debe realizarse en tiempo real; es decir, cualquier incidente de seguridad a nivel informático debe ser detectado instantáneamente (lo cual no siempre es posible) y gestionado a través de la plataforma y las herramientas del SOC.

Su función más importante es garantizar la continuidad del negocio de la empresa o Administración pública. En algunos casos, cuando se da una falla de seguridad, le corresponde resolver el problema en el menor tiempo posible para que la empresa o Administración pública pueda seguir con su actividad, o incluso aislar el perímetro de la empresa hasta que se resuelva el problema.

El SOC también se encarga de distribuir soluciones de seguridad: instalación y actualización de los antivirus, antimalware, antiransomware y cifrados para garantizar la seguridad de las comunicaciones.

1.3 ¿Qué es un NOC?

El NOC es responsable de monitorizar, identificar, investigar, priorizar, resolver o escalar incidentes en la red que pueden afectar o que estén afectando su disponibilidad o rendimiento.

El NOC tiene que ser capaz de desviar el tráfico cuando surge un problema en un componente de red. Hoy en día, las comunicaciones de las organizaciones —telefonía, satélite, LAN, WAN, etc.— son imprescindibles para el funcionamiento de los negocios. Esto se debe a: i) la extensión y el asentamiento del teletrabajo como consecuencia de la pandemia de COVID-19; ii) el aumento exponencial del comercio electrónico en los últimos tiempos, y iii) la digitalización de las empresas y su integración con la economía conectada.

Por lo tanto, los ANS de un NOC tienen que ser muy altos, ya que las empresas no pueden permitirse interrumpir sus operaciones. En la actualidad, es absolutamente necesario garantizar el desempeño de la red, con una disponibilidad de 24 horas al día, los 7 días de la semana y los 365 días del año (24x7x365).

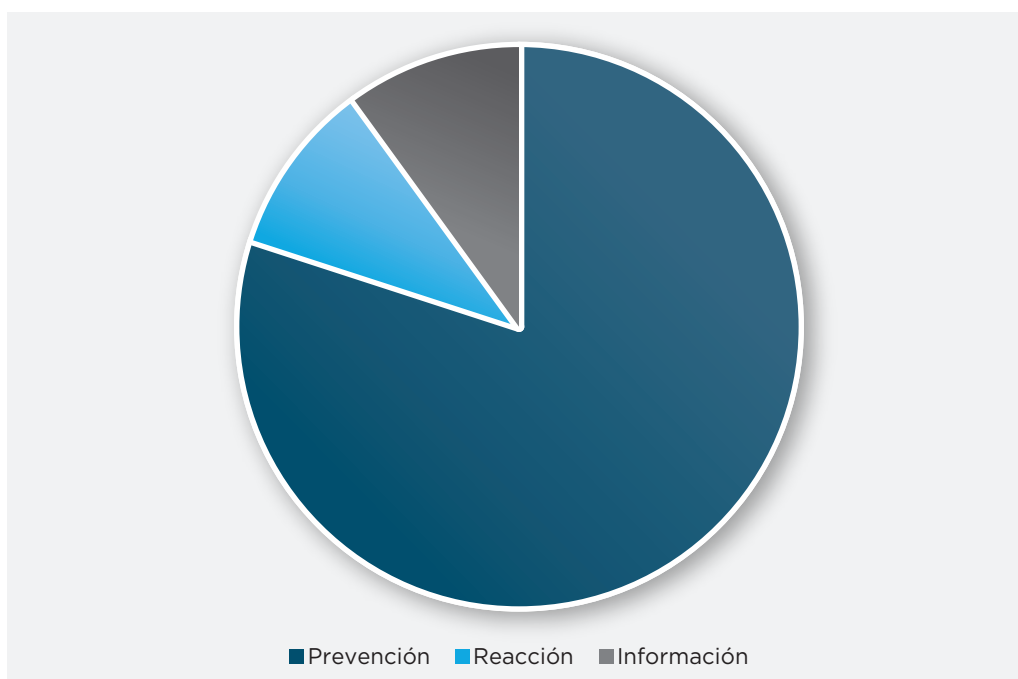
Un NOC cuenta con notificación instantánea de fallas: trabajará continuamente en las fallas detectados por las distintas soluciones de monitorización de la red implementadas. Por otra parte, debe tener disponibilidad de datos de salud y rendimiento en vivo, utilizando mapas en tiempo real y consolas completas (*dashboards*), con el fin de recopilar y supervisar el rendimiento de los dispositivos de la red.

Los nutridos conjuntos de *dashboards* tienen códigos de colores presentados en grandes pantallas que muestran las variaciones de color para diferenciar las métricas clave y los datos críticos.

El ciclo de trabajo de un NOC estaría basado en seis líneas:

1. Monitorización continua: a todos los elementos de la red (servicios de red, conectividad, dispositivos, etc.).
2. Detección de fallas: trabajo proactivo para evitar las paradas de la red.
3. Respuesta a incidentes: celeridad necesaria para resolver un problema.
4. Análisis: trazabilidad de incidentes determinando causa/raíz.
5. Informes: para ver el cumplimiento de los ANS y de los informes de gestión.
6. Mantenimiento: del software y del hardware desplegados en la red, incluidas actualizaciones de versión o instalación de parches, para que todo siga funcionando correctamente.

GRÁFICO 1 Distribución del tiempo en un NOC



Fuente: elaboración propia.

Nota: se refiere a los estándares de mercado.

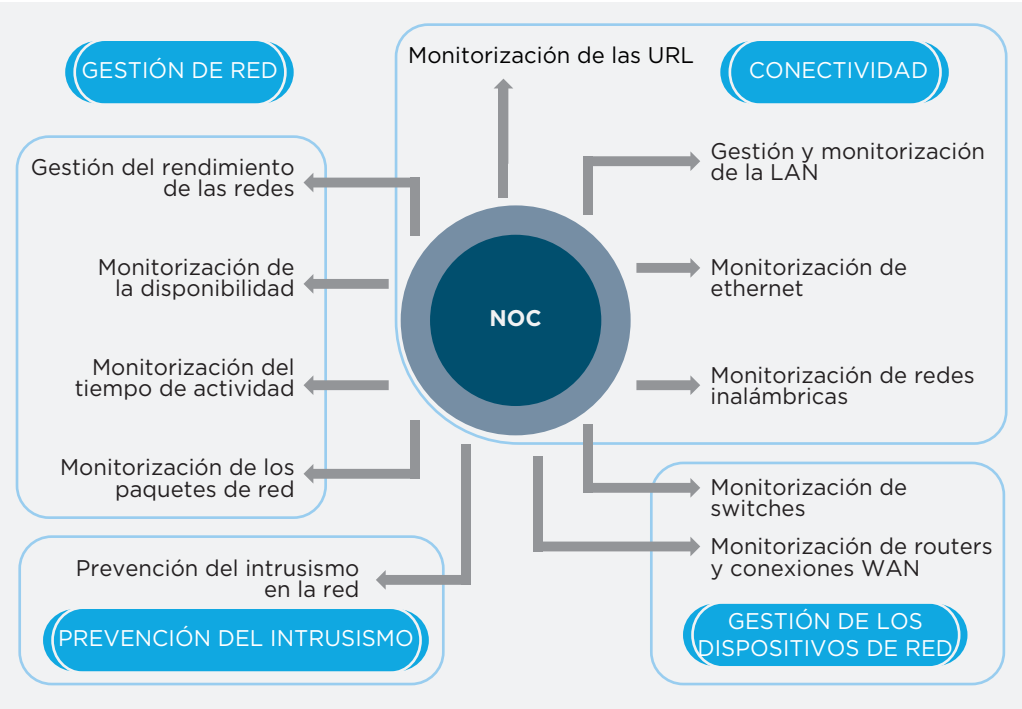
La distribución del tiempo en un NOC es la siguiente (gráfico 1):

- 80% o más se destina a la prevención; es decir, a la gestión proactiva de la infraestructura de red (puntos 1, 2, 4 y 6).
- 10% o menos se destina a la reacción; es decir, la intervención cuando ha surgido un problema no esperado (punto 3).

- 10% o menos se destina a la información; es decir, la generación de información de la gestión del NOC para la aplicación de planes de mejora (punto 5).

En este caso, se hará especial hincapié en los servicios que tienen que ver con la prevención (gráfico 2).

GRÁFICO 2 Prevención en un NOC



Fuente: elaboración propia.

Gestión de red

Monitorización del tiempo de actividad

El tiempo de actividad es la medida de disponibilidad de los dispositivos de red, de los sitios web y de otros servicios.

El tiempo de actividad de la red, en la mayoría de los casos, se mide en percentiles como “cinco nueves”: es decir, que el sistema está operativo el 99,999% del tiempo. El objetivo de un NOC es no superar los cinco minutos de indisponibilidad al año. Esto obliga a que la actividad de monitorización de la red sea un servicio 24x7x365.

El tiempo de actividad de la red se traduce en eficiencia en la utilización de los recursos de red. Si la red tiene una actividad muy alta, habrá que analizar si se está

utilizando de manera correcta (y no para usos particulares en el entorno empresarial) o si se necesita más ancho de banda.

Gestión del rendimiento

Un mundo conectado y globalizado como el de hoy en día, e incluso las empresas pequeñas, no pueden permitirse el lujo de una interrupción de red. La gestión del rendimiento de la red ayuda a prever posibles interrupciones y a solucionar los problemas de red de manera proactiva.

Esta actividad evitará la congestión de la red para el óptimo funcionamiento de las empresas, la Administración e incluso los ciudadanos. El software de gestión de rendimiento de redes permite monitorizar el rendimiento de cualquier dispositivo basado en el protocolo de internet (*Internet Protocol*, IP).

Monitorización de la disponibilidad

Como ya se señaló, las razones por las que es necesario monitorizar la disponibilidad de red son básicamente: i) un mundo globalizado; ii) el teletrabajo como práctica cada vez más frecuente; iii) el dinero que pierden las empresas cuando la red no está disponible, y iv) el malestar del ciudadano cuando no puede interactuar con la Administración debido a que la red no está disponible.

A su vez, se monitoriza porque los NOC no pueden superar los cinco minutos de indisponibilidad al año.

Monitorización de los paquetes

Los paquetes, o paquetes de red, son pequeñas unidades de datos transportados a través de una red. Estas unidades de datos son pequeñas y discretas, que por sí solas no tienen mucho sentido. Son solo partes del mensaje general que se está transmitiendo, reunidas en varias capas. Cuando se combinan, dichos paquetes tienen un significado.

Un usuario puede experimentar la pérdida de paquetes en forma de interrupción de la red (microcortes o cortes de más tiempo), un servicio lento o incluso la pérdida total de conectividad de la red. La pérdida de los paquetes puede darse por varias razones:

- Congestión de la red: cuando el tráfico de la red alcanza la capacidad máxima y los paquetes tienen que esperar para ser entregados.
- Problemas con el hardware de la red: firewalls, routers y conmutadores de red están viejos o desactualizados, lo que puede generar la pérdida de paquetes.
- Errores de software: los errores de software no verificados en los dispositivos de red pueden influir en la pérdida de paquetes.
- Dispositivos sobrecargados: dispositivos que se ejecutan a una capacidad mayor que para la que fueron diseñados.

- Amenazas de seguridad: si una amenaza entra en los routers de red, esto puede provocar la pérdida de paquetes.
- Cambios de configuración defectuosos: este tipo de cambio provocará la pérdida de paquetes.

Conectividad

Monitorización de las URL

En la economía actual, las empresas y las Administraciones públicas no pueden dejar la disponibilidad de sus sitios web libradas al azar. Las empresas gastan muchísimo dinero en marketing para atraer nuevos clientes, y las Administraciones, en brindar información y servicios al ciudadano. Por lo tanto, no es aceptable que los clientes/ciudadanos no puedan interactuar con el sitio web o el sitio de comercio electrónico por motivos de indisponibilidad.

Las actividades típicas de monitorización de la URL son:

- Monitorización de las aplicaciones externas y de intranet.
- Recepción de notificaciones cuando un hacker pone en peligro nuestra red.
- Monitorización de las páginas web que requieren autenticarse.

Gestión y monitorización de la LAN

La gestión de la red de área local (*Local Area Network*, LAN) es el proceso de monitorización, configuración y gestión de infraestructura de la LAN para garantizar una comunicación interna sólida y la prestación satisfactoria de los servicios empresariales. La gestión de la LAN es crucial para cualquier empresa u organismo, sin importar su tamaño.

La gestión de la LAN ayuda a:

- Entender su salud y rendimiento.
- Identificar vulnerabilidades de seguridad.
- Supervisar, monitorizar y gestionar la utilización de sus recursos.
- Garantizar una recuperación más rápida de los desastres.

Monitorización de ethernet

Ethernet es una tecnología de red de área local, con redes que tradicionalmente operan dentro de un solo edificio, conectando dispositivos cercanos. Todos los routers de banda ancha cuentan con puertos ethernet. Gracias a esta configuración, varios ordenadores conectados a una red pueden llegar a internet y a los otros dispositivos y switches conectados en la red.

Es probable que la monitorización de ethernet no le lleve mucho a un técnico de redes, pero desde luego sería lo primero que habría que mirar cuando se produce una falla en la red.

Monitorización de redes inalámbricas

Hoy en día, gracias a la tecnología existente, la mayoría de los ordenadores y dispositivos se conectan a la red por medio de una conexión inalámbrica (wifi). Es por eso que la monitorización ha ganado mucha importancia en los últimos tiempos, desfavoreciendo la monitorización por ethernet.

Gestión de los dispositivos de red

Monitorización de routers

Los routers o enrutadores de red son dispositivos hardware que se encargan de dirigir las comunicaciones entrantes y salientes de un equipo a través de una red.

Las conexiones WAN y los routers asociados suelen ser la parte más costosa de la red; por otra parte, gestionar la asignación de ancho de banda puede ser una tarea compleja.

Este tipo de monitorización es básica por algunas razones:

- Financieras: no pagar más ancho de banda del que realmente se necesita.
- Productividad diaria: esto permite que la organización pueda trabajar y los administradores puedan entregar la información requerida. En definitiva, se trata de encontrar el equilibrio adecuado entre rendimiento, tasa de información comprometida (CIR), tasa de ráfaga y congestión, tiempo de respuesta y descartes.

Monitorización de switches

Los switches son el activo más importante de la LAN. Cualquier problema en los switches afecta a una gran parte de los usuarios de la LAN. La implantación de un sistema de monitorización de los switches ayudará a detectar los problemas con antelación y evitar problemas futuros.

Prevención del intrusismo en la red

El análisis proactivo y la monitorización de la red permiten identificar amenazas o posibles amenazas que allí se producen y, en colaboración con los expertos en seguridad, impedirán que se produzca un problema de intrusismo en la red.

Básicamente, este servicio se encarga de la configuración de los firewalls y de la red privada virtual (*Virtual Private Network*, VPN) de la organización, con el objetivo de evitar el intrusismo. Ante un caso de intrusismo, se trabaja conjuntamente con el SOC.

El NOC también llevará a cabo actividades de análisis y monitorización de voz por protocolo de internet (*Voice over Internet Protocol*, VoIP), lo que permite supervisar el uso de las llamadas y analizar su rendimiento. A su vez, permite visualizar y detectar problemas relacionados con las llamadas en toda la red y acota el consumo de tráfico en función de las necesidades. También realizará tareas de operación, como las copias de seguridad de los dispositivos de red.

¿Cuál es la clave para que un NOC sea eficiente?

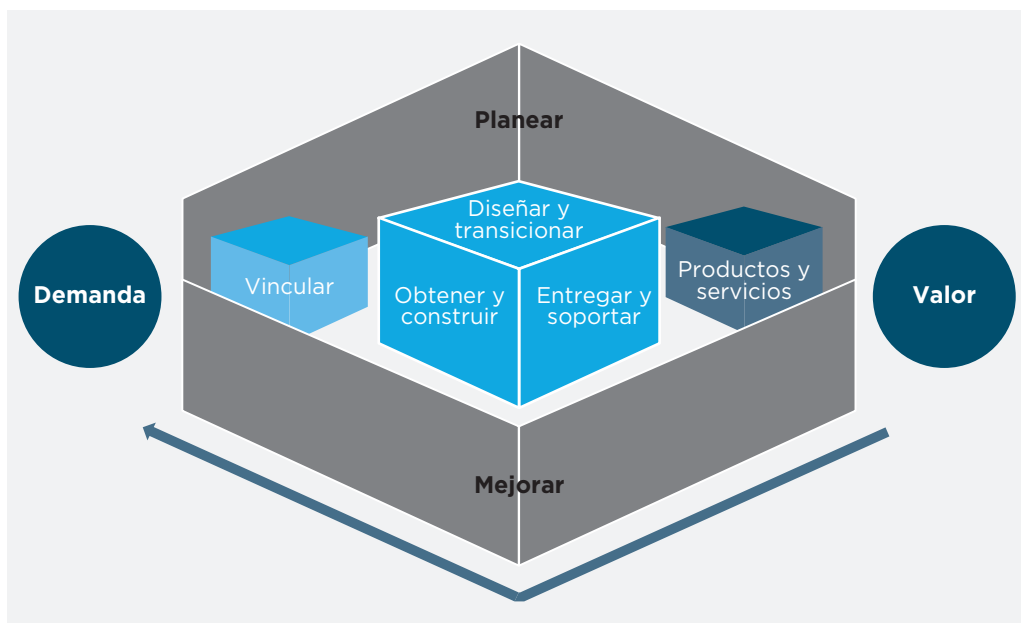
El centro de operaciones de red (*Network Operations Center*, NOC) es un servicio, entendiéndose por servicio un conjunto de recursos (humanos, herramientas, etc.) que trabaja con una metodología.

Cuando se construye una infraestructura tecnológica (ya sea un centro de procesos de datos, un NOC o un centro de operaciones de seguridad [*Security Operation Center*, SOC]), se está llevando a cabo una inversión importante, que incluye inversión en: i) bienes de capital (adquisición del hardware necesario para la realización del trabajo, terreno para edificar, etc.); ii) contratación de mano de obra (con diferentes niveles de cualificación, pero en definitiva cualificada y competente, lo cual conlleva recursos caros al compararlos con el resto de la población laboral de un país), y iii) sub-contrataciones (la obra civil conexas, expertos de los fabricantes de software, etc.).

En vista de lo anterior, e independientemente de que se trate de un organismo público o de una empresa privada, el NOC debe ser eficiente; es decir, debe trabajar de acuerdo a los estándares de mercado, brindando un servicio de calidad a los clientes.

La metodología que tendríamos que implementar en un NOC es un estándar de mercado: ITIL (gráfico 3). Se trata de una metodología orientada a la gestión de servicios mediante incidentes. Según ITIL Foundations (2019), el valor es el beneficio percibido, la utilidad y la importancia de algo. Esto quiere decir que, a través de la gestión de servicios, se logra mejorar la experiencia del usuario, realizar las actividades operativas de manera correcta y mantener un alineamiento de la gestión.

GRÁFICO 3 Descripción de la metodología ITIL



Fuente: ITIL Foundation (edición ITIL v4, 2019).

La metodología ITIL se estructura alrededor de cinco fases del ciclo de vida de un servicio, a saber:

1. Estrategia: propone tratar la gestión de servicios no solo como una capacidad sino como un activo estratégico.
2. Diseño: cubre los principios y métodos necesarios para transformar los objetivos estratégicos en portafolios de servicios y activos.
3. Transición: cubre el proceso de transición para la implementación de nuevos servicios o su mejora.
4. Operación: cubre las mejores prácticas para la gestión del día a día en la operación del servicio.
5. Mejora continua: proporciona una guía para la creación y el mantenimiento del valor ofrecido a los clientes a través del diseño, transición y operación del servicio optimizado.

La metodología ITIL diferencia entre funciones y procesos:

- Una **función** es una unidad especializada en llevar a cabo una actividad determinada y responsabilizarse de su resultado. Las funciones incorporan todos los recursos y capacidades necesarias para el correcto desarrollo de la actividad y tienen como prin-

cipal objetivo dotar a las organizaciones de una estructura acorde con el principio de especialización. Sin embargo, la falta de coordinación entre funciones puede tener como resultado la creación de nichos contraproducentes para el rendimiento de la organización a nivel global. En este último caso, un modelo organizativo basado en procesos puede ayudar a mejorar la productividad de la organización en su conjunto.

- Un **proceso** es un conjunto de actividades interrelacionadas orientadas a cumplir un objetivo específico. Los procesos comparten las siguientes características:
 - Son cuantificables y se basan en el rendimiento.
 - Dan resultados específicos.
 - Tienen un cliente final que es el receptor del resultado.
 - Se inician como respuesta a un incidente.

El último concepto importante dentro de la metodología ITIL es el rol. Un rol es un conjunto de actividades y responsabilidades asignado a una persona o grupo. Una persona o grupo puede desempeñar simultáneamente más de un rol. Los roles principales dentro de ITIL son:

- Propietario del proceso: asegura que todo funcione de acuerdo con lo definido en las especificaciones; se ocupa del diseño y patrocinio de la gestión del cambio (por ejemplo, define el proceso de gestión de incidentes).
- Gestor del proceso: investiga cómo ponerlo en práctica; busca los recursos necesarios, informa sobre el rendimiento y propone mejoras (por ejemplo, ejecuta la gestión de incidentes).
- Practicante del proceso: ejecuta las acciones del proceso y las documenta para informar de su progreso.
- Propietario del servicio: en su calidad de responsable del servicio, supervisa la implementación, el mantenimiento y la mejora continua del servicio.

Para que un NOC sea eficiente nos basaremos en el modelo de cuatro dimensiones de ITIL v4, a saber:

1. Organización y personas: orientada a la gestión organizativa y de recursos, y centrada en los roles y funciones que desempeñan, la integración entre áreas y la cultura corporativa.
2. Información y tecnología: herramientas tecnológicas orientadas a optimizar los procesos mediante la implementación y/o el desarrollo de tecnología.
3. Socios y proveedores: gestión de los aliados estratégicos, tanto proveedores como clientes, con miras a que también sean considerados como una variable clave en el desarrollo de procesos.

4. Flujos de valor y procesos: como centro de las operaciones, establecen cómo, cuándo, dónde y quién va a realizar determinada tarea/actividad; por su parte, las actividades son parte de los planes de acción, que están orientados a los flujos de valor en el servicio.

Estos cuatro componentes y su adecuada implementación permitirán poder contar con un NOC eficiente. En las subsecciones siguientes se describen en mayor detalle.

2.1 Organización y personas

La complejidad de las organizaciones es cada vez mayor, por lo que resulta importante asegurarse de que la forma en que una organización está estructurada y administrada, así como sus roles, responsabilidades y sistemas de autoridad y comunicación, estén bien definidos y respalden su estrategia general y operativa.

Por ejemplo, es útil promover una cultura de confianza y transparencia en una organización que alienta a sus miembros a plantear y escalar problemas y que facilita las acciones correctivas antes de que un problema afecte a los clientes.

Las personas —ya sean clientes, empleados de proveedores, empleados del proveedor de servicios o cualquier otro interesado en la relación de servicio— son un elemento clave en esta dimensión. Se debe prestar atención no solo a las habilidades y competencias de los equipos o miembros individuales, sino también a los estilos de gestión y liderazgo, y a las habilidades de comunicación y colaboración. A medida que evolucionan las prácticas, las personas también necesitan actualizar sus habilidades y competencias. Resulta cada vez más importante que las personas comprendan las interfaces entre sus especializaciones y roles, así como las de otros en la organización, a fin de garantizar niveles adecuados de colaboración y coordinación.

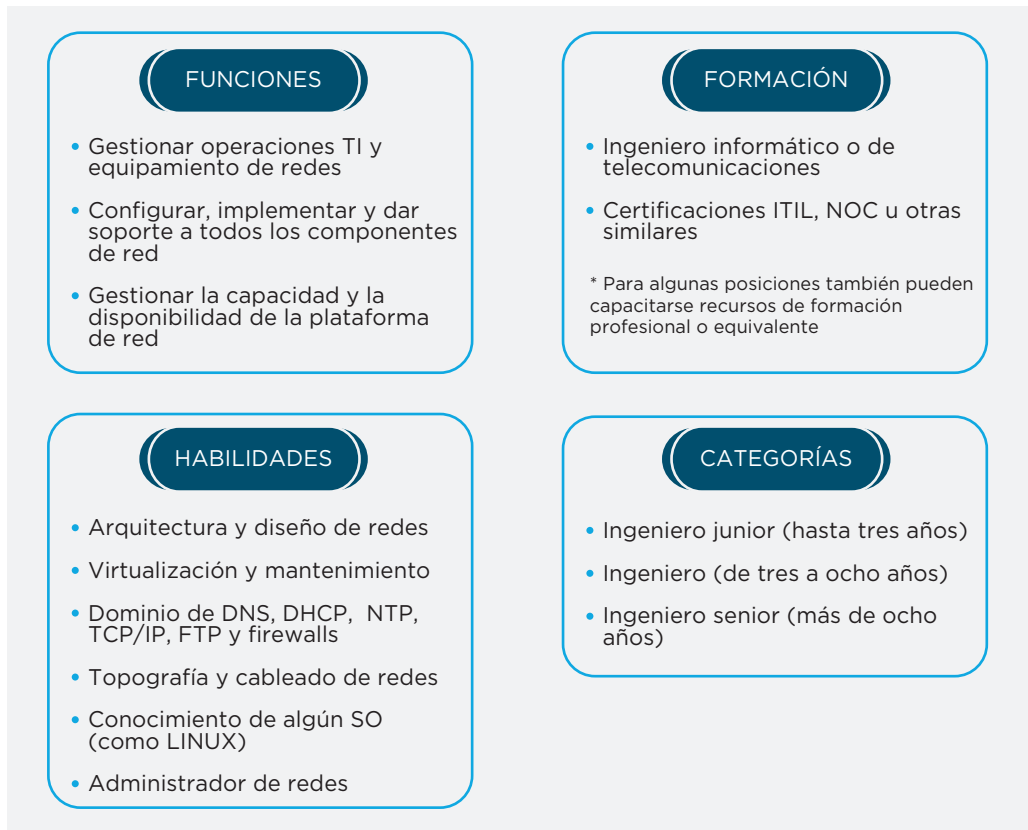
En esta dimensión deben cubrirse roles y responsabilidades, estructuras organizativas y competencias requeridas, lo cual está enteramente relacionado con la creación, entrega y mejora de un servicio.

A continuación, se abordará con mayor detalle el apartado personas y el perfil de un ingeniero NOC: funciones, formación, habilidades y carrera profesional (gráfico 4).

Sus responsabilidades incluyen:

- Gestionar las operaciones de TI y el equipamiento de redes como routers, switches, firewalls y puntos de acceso.
- Operar, monitorizar y garantizar la estabilidad de los sistemas de redes.
- Solucionar incidentes de los sistemas de redes.
- Configurar, implementar y brindar soporte a todos los componentes de red.
- Gestionar proveedores de tecnología que implementan soluciones de red (tanto operadores de telecomunicaciones como fabricantes de HW y SW).

GRÁFICO 4 Perfil del ingeniero NOC



Fuente: elaboración propia.

- Gestionar, completar, verificar y restaurar respaldos (siempre tiene que existir una alternativa de servicio).
- Garantizar el completo funcionamiento y disponibilidad de la plataforma.
- Gestionar requerimientos, problemas, incidentes y entornos de datos.
- Brindar soporte para resolver problemas relacionados con la infraestructura de red, documentando todos los cambios realizados y gestionando accesos a la red.
- Redactar y mantener actualizada la documentación técnica del entorno de redes.

Las habilidades que debería poseer un ingeniero NOC son las siguientes:

- Experiencia en gestión y monitorización de redes, así como conocimiento experto en resolución de problemas técnicos y en modelos de incidentes y herramientas de diagnóstico.

- Manejo de herramientas comunes como productos Microsoft y servicios de internet.
- Buena comunicación tanto oral como escrita.
- Pensamiento analítico para la automatización de procesos y flujos de trabajo.
- Conocimiento en virtualización y mantenimiento (herramientas como por ejemplo VMWare).
- Comprensión sólida de conceptos de redes como DNS, DHCP, NTP, TCP/IP, FTP y firewall, entre otras.
- Conocimiento de topología, cableado y clasificación de redes.
- Nociones básicas de seguridad de la información.
- Capacidad para trabajar bajo presión.

La formación que se requiere para ser un ingeniero NOC es habitualmente la de ingenieros informáticos o de telecomunicaciones. Sin embargo, personas con otros estudios pueden ser formados en esta materia, dependiendo del rol que desempeñen y del momento en que comienzan su formación. Cabe señalar que ingenieros en otras ramas o profesionales de distinta formación pueden ser capacitados en esta materia nada más acabar sus estudios.

El profesional NOC —dependiendo de su rol— debería contar con una certificación NOC (certificaciones estándar de mercado; por ejemplo, las de CISCO) o ITIL. Por otra parte, los cursos cortos en este campo son una excelente opción para mejorar el perfil profesional.

Las categorías permiten asignar las tareas del día a día, así como el escalado de los incidentes que surjan, a saber:

- Ingeniero junior: estará aprendiendo durante los primeros años de su carrera profesional, trabajando muy de la mano del ingeniero. Se le asignarán los incidentes más sencillos o más habituales junto con documentación de resolución.
- Ingeniero: es el que trabajará más en el día a día de la monitorización de las redes, su virtualización, etc. Tiene un conocimiento más amplio que el ingeniero junior, pero menos experiencia que el ingeniero senior.
- Ingeniero senior: profesional con sólidos conocimientos y experiencia, por lo que se dedicará más a la definición de la arquitectura y el diseño de las redes. También participará en aquellos incidentes de red que se le escalen o se le asignen por su complejidad.

Es fundamental que los profesionales estén formados en los procesos y la metodología del NOC, o al menos que tengan documentados los procesos de trabajo para saber cómo desenvolverse en cada caso.

Estamos ante un entorno donde el talento digital escasea a nivel mundial, y faltan recursos en el mundo entero. Si el recurso no se encuentra cómodo o no se siente

respaldado, y si no se le asignan las actividades correctamente, lo más probable es que abandone la organización y busque un entorno donde pueda evolucionar profesionalmente.

Los equipos tienen que estar inmersos en una formación continua. El sector tecnológico avanza muy rápido, y debe tenerse en cuenta que por lo menos 5% de las horas de trabajo anuales tienen que estar dedicadas a la formación. En este sentido, también resulta clave que el recurso realice actividades acordes con su nivel de formación.

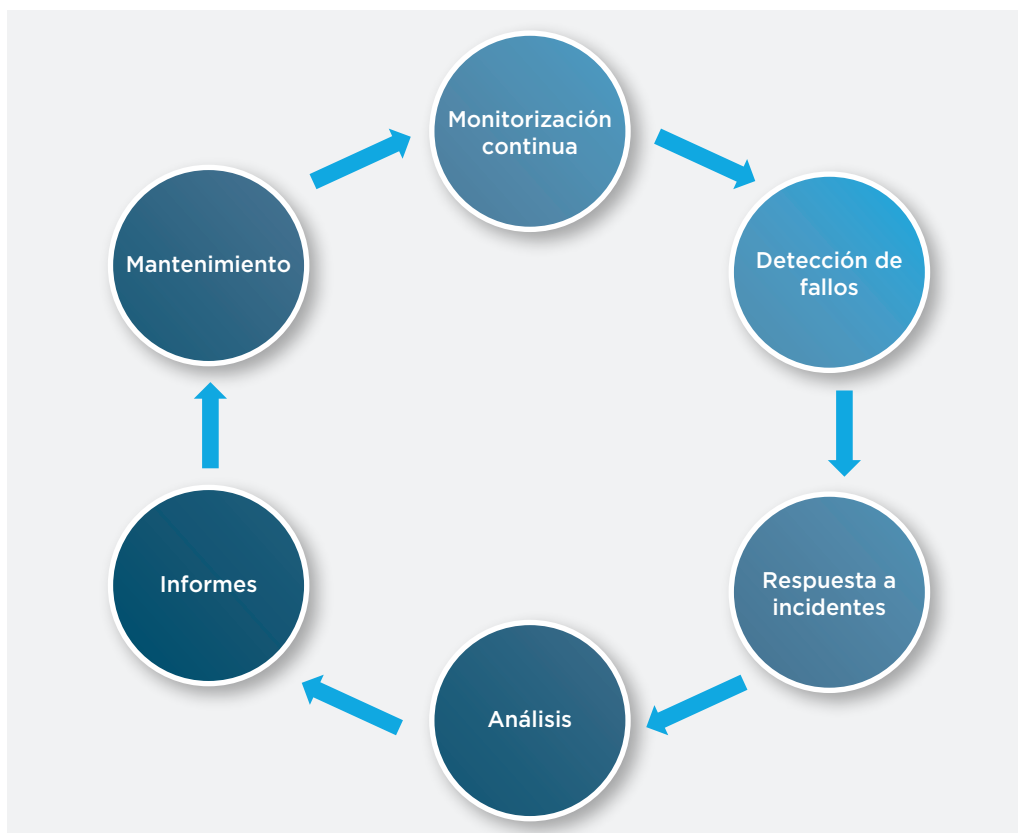
2.2 Información y tecnología

Las tecnologías que respaldan la administración de servicios incluyen, entre otras, sistemas de administración de flujo de trabajo, bases de conocimiento, sistemas de inventario, sistemas de comunicación y herramientas analíticas. La gestión de servicios se beneficia cada vez más de los avances tecnológicos. La inteligencia artificial (IA), el aprendizaje automático (*Machine Learning*) y otras soluciones de computación cognitiva se utilizan en todos los niveles, desde la planificación estratégica y la optimización de la cartera hasta la supervisión del sistema y la asistencia al usuario.

Dentro de este apartado es muy importante la información creada, administrada y utilizada en el curso de la prestación del NOC, así como las tecnologías que respaldan y habilitan el servicio.

La tecnología es necesaria en toda la cadena de valor de un NOC (gráfico 5). A continuación, se enumeran algunas de las herramientas que consideramos indispensables:

- Software de monitorización de los servicios de red, de los elementos de hardware y de lo que hemos llamado “conectividad”: permite anticipar problemas y, en caso de encontrarlos, actuar más rápidamente, lo que redundará en la reducción de costos.
- Herramienta de ticketing: con ella se implementa toda la lógica de negocio del NOC: i) tipología del ticket (incidente, mantenimiento, etc.); ii) prioridades (alta, media, baja); iii) categorización del ticket (breve descripción para su identificación y posterior catalogación); iv) niveles de tolerancia (lo que nos permitirá configurar alarmas para los diferentes gestores); v) recursos (categoría de acuerdo con la complejidad del incidente), y vi) informes (para clientes o de gestión).
- Repositorio de documentación: aquí acuden los técnicos en busca de una solución documentada cuando les asignen una actividad. Esto ayuda a que puedan cerrar cuanto antes el incidente, o permite mayor productividad de los técnicos y cerrar un mayor número de incidentes al mismo tiempo.
- Herramienta de *Business Intelligence*: permite medir los procesos y el desempeño de los técnicos, para luego lanzar planes de mejora continua y poder contar con un servicio de mayor calidad.

GRÁFICO 5 Actividades que realiza un NOC

Fuente: elaboración propia.

- Base de datos con sus recursos y conocimiento: permite asignar los recursos a los incidentes de manera más eficiente. Se irá alimentando con los cursos y la formación que fueran recibiendo.

2.3 Socios y proveedores

Esta tercera dimensión va ligada a la gestión del servicio y la relación con terceros. En este caso, se trata de la relación y el contrato que tengamos firmado con los operadores de telecomunicaciones, con los fabricantes de algunos de los componentes de hardware de la infraestructura de red, y por supuesto con los fabricantes de software de dicha infraestructura.

Este apartado es relevante en lo que respecta al NOC, en términos de si se implementa dentro de la organización o se subcontrata. Por otro lado, en el caso de crear un

NOC a nivel país para la Administración pública, contempla los acuerdos para brindar el servicio a cada uno de los organismos públicos. Las relaciones entre organizaciones pueden implicar varios niveles de integridad y formalidad. En el caso de los proveedores, esto incluye contratos formales con una separación clara de responsabilidades.

Los factores que pueden influir en la estrategia de una organización o Administración al utilizar proveedores incluyen:

- **Enfoque estratégico:** en el caso de Administraciones públicas, se suelen decantar por permanecer lo más autosuficientes posible, manteniendo el control total o parcial de la infraestructura de redes. Esto normalmente surge de la necesidad de contar con redes muy seguras (caso de Defensa, Seguridad Ciudadana, Justicia, etc.) y de proteger la información que fluye por la infraestructura de red (Hacienda y Agencia Tributaria, Salud, etc.).
- **Cultura de externalización:** no todos los países, ni las Administraciones públicas dentro de un país, tienen la misma madurez para trabajar con servicios gestionados (y concretamente con un NOC).
- **Escasez de recursos:** si un recurso o un conjunto de habilidades requeridos son escasos, puede ser difícil para la Administración adquirir —por motivos de mayor salario en el sector privado que en el público— lo que necesita sin contratar a un proveedor.
- **Presupuesto:** la Administración licitará el NOC con el presupuesto que tenga asignado en la partida presupuestaria. Teniendo en cuenta que sería concurso público, la competencia está asegurada. La parte económica dentro de los pliegos públicos es un apartado muy importante y cuantitativo a la hora de asignar el servicio.
- **Experiencia en el tema:** si hay proveedores implantados en el país (locales o globales) que aporten experiencia y referencias en la gestión e implantación de un NOC, el proceso siempre será más rápido que si la Administración pública comienza de cero.

2.4 Flujos de valor y procesos

Esta cuarta dimensión define actividades, flujos de trabajo, controles y procedimientos necesarios para cubrir la gestión de infraestructuras y su disponibilidad.

Se entiende por “flujo de valor” una serie de pasos que emprende una organización para crear y entregar productos y servicios a los consumidores. En el caso que nos ocupa, serían los pasos que la Administración pública de un país emprende para poder ofrecer servicios a los diferentes organismos públicos que la comprenden, y con ello brindar el servicio esperado a sus ciudadanos. Por lo tanto, estructurar las actividades del organismo público en forma de flujos de valor permitirá tener una idea clara de cómo ofrecer y mejorar los servicios de infraestructuras de red.

El trabajo del día a día tiene que estar procedimentado. Para que el NOC sea eficiente, el proceso debe tener bien definidas las entradas (*inputs*) y las salidas (*outputs*). En el mismo sentido, es fundamental que cada recurso sepa qué tareas debe desarrollar y de qué forma.

Los procesos que implementemos nos permitirán definir la forma en que se generan los incidentes y cómo se escalan, así como los protocolos en caso de fallas en el sistema de red y los protocolos de actuación ante intrusismo en la red. Esto, a su vez, permitirá definir los flujos de escalado, los niveles de tolerancia, etc. Asimismo, generará información para conocer la actividad y a quién corresponde preguntar (algo que resulta obvio pero no siempre fácil). Gracias al proceso se podrán medir tiempos de actuación que servirán para: i) preparar la incorporación de nuevos organismos al NOC, conociendo con mayor precisión los costos del servicio, el número de recursos que deben incorporarse para cubrir los nuevos servicios, etc., y ii) realizar las asignaciones de forma más certera; por ejemplo, no asignar a una persona temas complejos y demorar mucho la resolución ni tampoco poner un recurso caro a resolver incidentes de bajo nivel.

Si la decisión pasa por externalizar el NOC, se tendrá que exigir al tercero que tenga los procesos bien definidos, que utilice una metodología estándar de gestión de incidentes (por ejemplo, ITIL), que cuente con las herramientas para brindar un servicio adecuado y que además incorpore dentro del servicio todo el modelo de entrega de informes que necesite la Administración.

En el mercado, existen ejemplos de operadores de infraestructuras tecnológicas que tienen unos costos muy elevados en la operación y que no son competitivos, lo que lleva a que los servicios se vayan degradando.

Las cuestiones analizadas anteriormente deben tenerse en cuenta para que las actividades se lleven a cabo como si se tratara de una fábrica (lo que en el argot del sector se denomina “servicios industrializados”).

NOC: Punto clave en la digitalización

Con la expansión del mundo conectado, la digitalización, las redes sociales y el mundo globalizado, las comunicaciones son cruciales para que el mundo funcione y la sociedad avance.

Veinticinco años atrás, las empresas conectaban sus organizaciones con líneas punto a punto, que permitían a las empresas/organismos públicos conectar sus diferentes ubicaciones. Dentro de las oficinas existía un cableado para conectar los servicios a los diferentes usuarios. Además, se gastaba mucho dinero en desplazamientos a reuniones en diferentes ubicaciones. No había mucha actividad en internet, y las páginas web de las compañías no eran transaccionales y además no se les daba mucha importancia.

En los últimos años, el entorno ha cambiado radicalmente y las conexiones punto a punto no son tan frecuentes, solo para entornos de mucha seguridad. Las empresas y los organismos públicos interactúan entre sí, con los consumidores y los ciudadanos. Además, el uso del wifi se ha disparado entre la población, permitiendo el acceso a diferentes servicios desde ordenadores, tablets, dispositivos móviles o smart TV.

Hoy en día, estamos ante otra revolución digital, que vendrá acompañada de tecnología 5G, internet de las cosas, aprendizaje automático, big data, data analytics y metaverso, entre otras.

Estudios de la Universidad de Columbia indican que un aumento del 1% del índice de digitalización genera un incremento de 0,32% en el producto interno bruto (PIB);

0,26% en la productividad laboral; 0,23% en la productividad multifactorial, y 0,09% en la contribución de las TIC a la productividad laboral.

Industrias como telecomunicaciones, proveedores de servicios de internet, energía y servicios públicos, así como las Administraciones públicas, proveen servicios fundamentales a usuarios o ciudadanos. Por ello, necesitan proteger sus redes y asegurar que la comunicación fluya perfectamente, entregando el servicio esperado a los usuarios.

Este mundo que se describe sería imposible de imaginar sin las comunicaciones, y el centro de mando para que todo funcione reside en el NOC. No se pueden concebir las inversiones digitales sin tener bien implementado el tema de las comunicaciones. Tampoco podemos, en la actualidad, pensar en la economía conectada y la digitalización de empresas y Administraciones públicas sin un funcionamiento óptimo de la red. Y para que la red funcione de manera óptima se necesita un NOC.

¿Cuál es el impacto de una falla de red o de una interrupción?

- Pérdidas de ingresos significativas.
- Altos costos de reparación.
- Menor productividad de los empleados.
- Pérdida o fuga de datos.
- Efectos en la imagen reputacional.

La red puede verse afectada, básicamente por cinco factores:

1. Errores humanos:
 - A medida que la red de la organización (empresa o Administración) se vuelve más compleja, también aumenta la probabilidad de errores humanos, sobre todo cuando se gestionan redes críticas y/o privadas.
 - Las razones principales del error humano en la gestión de redes radican en los procesos manuales, como ajustes o configuración, distracciones o estrés.
 - Es importante resaltar que los ciberdelincuentes utilizan técnicas avanzadas de ingeniería social para introducir malware mediante ataques de phishing.
 - Para minimizar los errores humanos es esencial automatizar las tareas complejas, monitorizar las actividades, establecer procedimientos, realizar formaciones periódicas y tener definido un buen plan.
2. Cambios en la configuración:
 - Los cambios de configuración incorrectos y la configuración manual pueden provocar largos tiempos de inactividad.
 - En los entornos de red multifabricante es normal que haya muchos elementos de proveedores y tecnologías diferentes. Es sumamente importante que estén

conectados, y que se los haga funcionar entre ellos. Por lo tanto, deben crearse circuitos de manera rápida, segura y controlada.

- En redes IP, los problemas de enrutamiento son los más comunes. Cuando hablamos de redes IP no existen circuitos, sino tablas de ruta que dependen del destino de los datos. Las tablas de ruta son dinámicas, y si falla la red, pueden ser reconfiguradas para poder enviar la información por una ruta alternativa. Sin embargo, si la configuración no está bien ejecutada, la información podría ser enviada a un área no deseada e incluso pueden perderse sus datos.
3. Equipos obsoletos:
- Es muy complicado mantener los sistemas antiguos y los nuevos con actualizaciones de algunos softwares. Un equipo anticuado que por lo general está desactualizado puede afectar directamente el rendimiento de la red y su normal funcionamiento. Ello ocurre porque los sistemas antiguos y desactualizados ya no respaldan las últimas actualizaciones de los sistemas operativos (SO) recientes.
 - A medida que el tiempo pasa, la red evoluciona e incorpora nuevos equipamientos y nuevos sistemas. Hoy día, es frecuente encontrar empresas que todavía gestionan equipamiento “*legacy*” (que puede tener más de 20 años), con sistemas y dispositivos nuevos. Es por eso que la gestión puede volverse compleja.
 - La compatibilidad de los equipos es un problema engorroso. Para solucionarlo, habrá que implementar una buena herramienta de gestión y monitorización de redes para llevar a cabo el inventario y programar las actualizaciones pertinentes de forma periódica.
4. Amenazas de ciberseguridad y ataques:
- Existen muchas amenazas de seguridad en la actualidad. Por ello, se deberían poder detectar anomalías en el tráfico de datos, determinar consumos disparatados de recursos y evitar los accesos no autorizados.
 - Los ataques de denegación de servicios (DDoS, por sus siglas en inglés) son los más empleados por los ciberdelincuentes, y generan la pérdida de control de la red. Herramientas como los sistemas de detección de intrusos (*Intrusion Detection System*, IDS), firewalls y VPN, entre otras, ayudan a prevenir los ataques de denegación de servicios.
 - Otro aspecto que debe tenerse muy en cuenta es que los hackers también aprovechan para atacar a través de los sistemas obsoletos. Por ello, resulta fundamental que todos los dispositivos estén actualizados.
5. Cortes de energía:
- La teleprotección es el sistema clave para los servicios públicos, ya que protege las redes de las fallas de energía y la propagación de la falla por la red.
 - Además, en caso de falla de energía hay que asegurar que los sistemas de respaldo suministren suficiente energía para que la infraestructura siga

funcionando, de modo que se puedan resolver los problemas en el menor tiempo posible.

- Las fallas de red no tienen preaviso.

A continuación figuran algunos ejemplos de empresas que tuvieron problemas de falla de red y del impacto que eso tuvo en sus negocios:

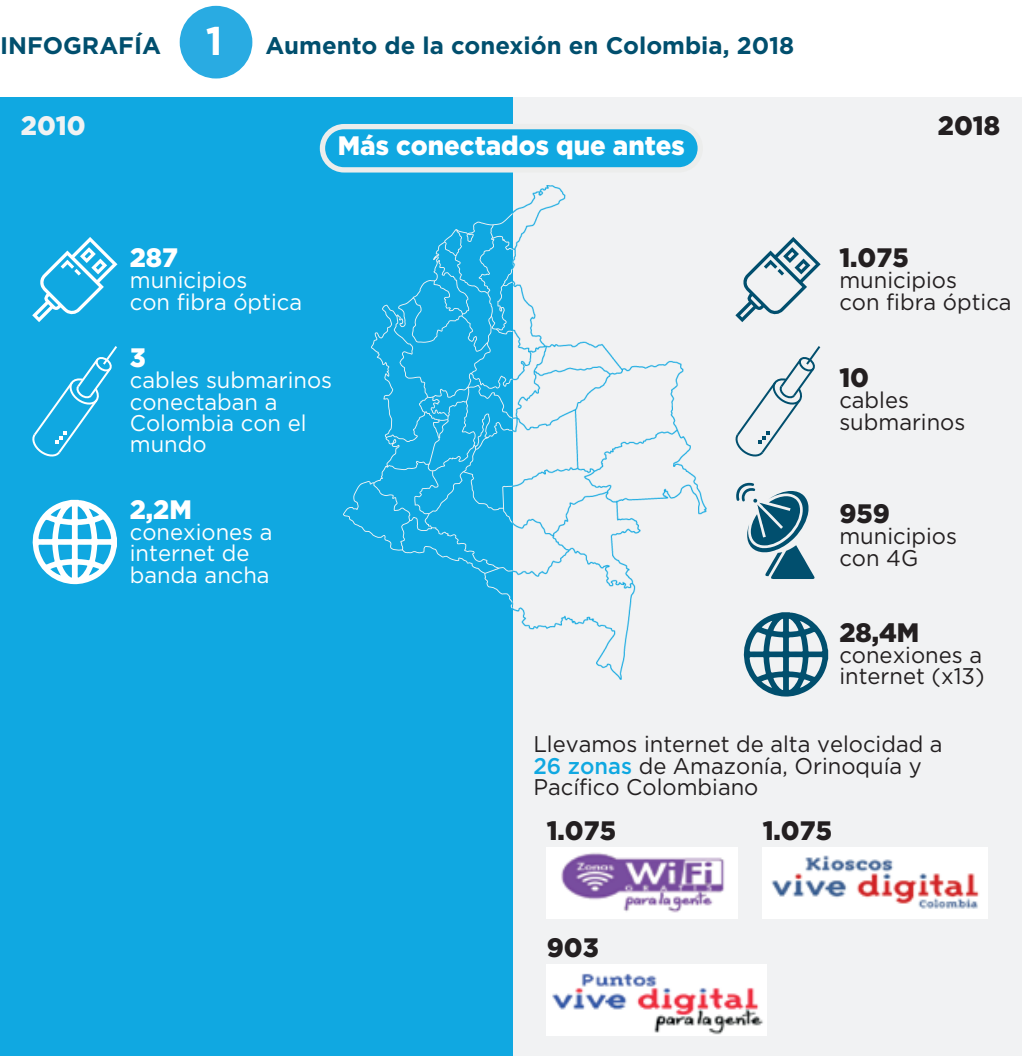
- En 2018, Delta Air Lines tuvo un considerable tiempo de inactividad en su red. La causa de la interrupción fue la falla de un equipo que estaba afectando al centro de procesos de datos (CPD). Como resultado, se cancelaron miles de vuelos y la compañía enfrentó un impacto económico de USD 150 millones.
- En 2018, O₂ sufrió una caída del servicio, debido a un certificado caducado. El servicio de internet se interrumpió y la compañía tardó casi un día en resolver el problema y restaurar el servicio. Tuvo que compensar a los usuarios por el tiempo sin servicio.
- En 2018, Century Link sufrió una inactividad de casi dos días. La causa de la falla fue la incorrecta configuración de red que estaba impactando directamente en el CPD. La tarjeta de gestión de red estaba transmitiendo paquetes de datos inválidos a través de la infraestructura. La interrupción eliminó las llamadas de voz al 911 en algunos estados de Estados Unidos, y afectó a los datos móviles de Verizon, la entrega de efectivo de cajeros automáticos, sorteos de lotería y el registro de pacientes en hospitales. El problema incluso se agravó, ya que durante la crisis se perdió la visibilidad de la red mientras se intentaba resolver el problema.
- Caída de redes sociales (Facebook, Instagram y WhatsApp) del 4 de octubre de 2021. El problema no fue de redes, pero acabó afectándolas. Los trabajadores de Facebook no pudieron acceder a sus instalaciones porque las tarjetas de identificación no funcionaban. Como no podían acceder a las instalaciones, ni a los ordenadores o a la red interna, tardaron más tiempo en reconfigurar los routers.

El último caso cobró mucha relevancia en América Latina, ya que había pequeñas empresas y profesionales independientes que ofrecían sus servicios o recibían los pedidos a través de WhatsApp. Algunas fuentes indican que, por ejemplo, 21% de peruanos lanzan sus emprendimientos a través de redes sociales como Facebook, WhatsApp o páginas web.

Debido a que estamos atravesando una nueva revolución digital y al volumen de impacto en los negocios, resulta absolutamente necesario que las empresas y la Administración cuenten con NOC profesionalizados, competentes y dispuestos a resolver los problemas que surjan en el menor tiempo posible. Lo más importante, sin embargo, es tomar medidas de prevención para que no se produzcan interrupciones.

3.1 Cuestiones clave en la infraestructura de un país

Veamos, a través del ejemplo de Colombia, cómo se dispararon las necesidades de conexión en el transcurso de ocho años, y la forma en que se llevaron muchas más conexiones a los municipios (algunos con 4G) y crecieron exponencialmente las conexiones a internet (infografía 1).



Los gobiernos deben centrar sus esfuerzos principalmente en dos frentes: i) contar con infraestructura y conectividad sólidas a fin de reducir la brecha digital respecto de los países de la Organización para la Cooperación y el Desarrollo Económicos (OCDE); ii) complementar lo anterior con una política pública que incorpore la capacitación de las personas en el uso de dispositivos e internet.

Además, la disponibilidad de infraestructura de redes habilitará la digitalización en tres líneas diferentes:

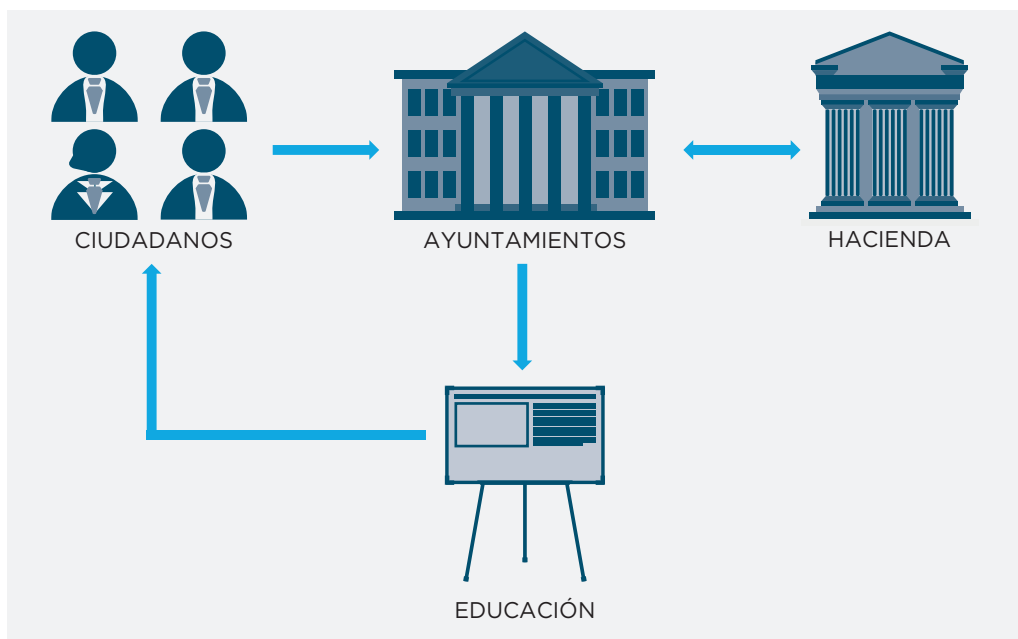
1. Interconexión entre diferentes organismos/agentes públicos:

Los gobiernos de los países tienen que esforzarse en ofrecer a todos sus organismos dependientes una red única, lo cual evitará los silos de información y los protocolos de comunicación más complejos. La interconexión o interoperabilidad entre los diferentes organismos públicos permitirá que puedan compartir información de manera ágil y fiable. Por ejemplo, un funcionario público entra en la red de la Administración pública del país y desde allí podrá acceder a los servicios informáticos en los que esté habilitado como usuario (es decir, tendrá a su disposición la información en función de su categoría y los permisos asignados). La interoperabilidad permite actuar con un único interlocutor de la Administración, que a su vez se relaciona con el resto para brindar el servicio al ciudadano (infografía 2).

INFOGRAFÍA

2

Ejemplo de interoperabilidad: inscribir a un niño en un colegio

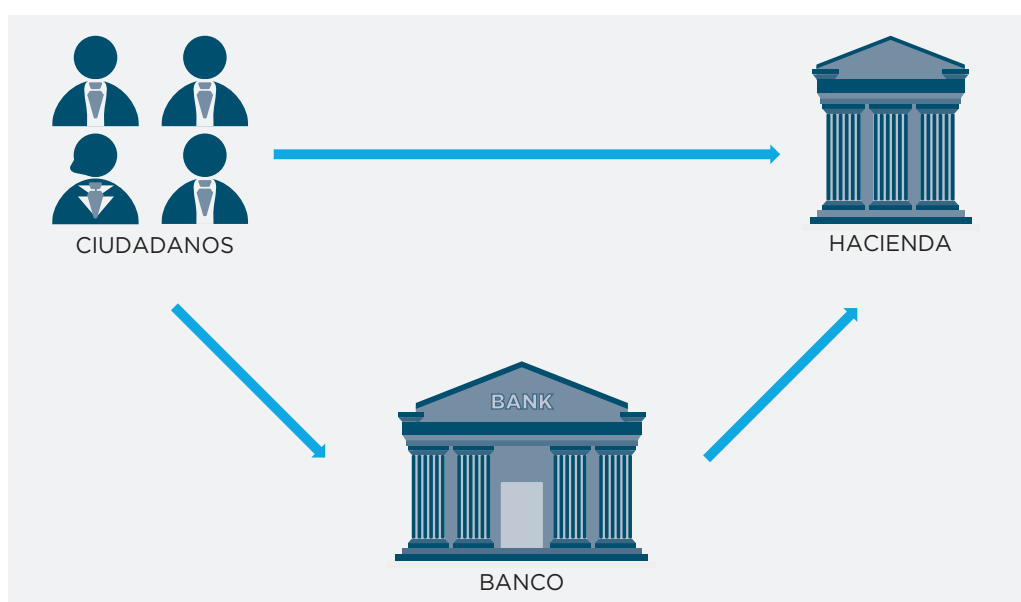


Fuente: elaboración propia.

2. Acceso a los servicios públicos por parte del ciudadano (infografía 3). Esto significa que las herramientas que habilitan los servicios básicos como salud, educación y urgencias, entre otros, tienen que estar funcionando. Sin acceso a los servicios públicos y a la interconexión, no podrán brindarse los servicios que hoy en día demandan los ciudadanos. El acceso a los servicios públicos tendrá que ser más transaccional que informacional; es decir, permitir realizar trámites a través del portal público antes que brindar una gran cantidad de información.

Las comunicaciones habilitan, en cualquier procedimiento, la interacción física o digital del ciudadano con la Administración, siendo decisión de cada ciudadano la elección de un canal u otro. Dicho esto, no quedan dudas de que el NOC permitirá que la interacción con la Administración se realice de manera segura.

INFOGRAFÍA 3 Ejemplo de acceso a los servicios públicos: pago de impuestos



Fuente: elaboración propia.

3. Lo anterior tiene que ser una palanca de desarrollo del país en dos frentes: i) pequeñas empresas y trabajadores cuentapropistas, para que puedan desarrollar su actividad de una manera más segura que a través de WhatsApp, y además operar en una economía global sin moverse de su domicilio, y ii) capacitación en habilidades tecnológicas de la población, lo que le permitirá trabajar desde su escritorio para cualquier lugar del mundo, conformando una competencia respecto de otros países, como India o China.

En concreto, diferentes análisis coinciden en que en América Latina se requiere entre tres y cuatro veces más infraestructura que la que existe actualmente para satisfacer la demanda de conectividad. Este dato tiene que orientarse hacia una política pública digital integral, porque también existe una brecha de uso: la población que vive en determinados lugares sin cobertura no utiliza la conectividad y tampoco sabe cómo usarla.

3.2 Cuestiones clave en la infraestructura de las empresas

Normalmente, las empresas (grandes y medianas) tienen un servicio de gestión de redes interno o subcontratado. De acuerdo con un estudio de Gartner (2014), un minuto de inactividad le cuesta a una empresa USD 5.600 en promedio. Es por ello que las empresas consideran estratégico que sus comunicaciones no se caigan.

Dicho esto, resulta importante que se logre incorporar este tipo de servicio a las pequeñas empresas, que en ocasiones lo pueden tener subcontratado con la operadora. No obstante, existen otros casos en los que no se contará con dicho servicio. Así, un apagón de redes sociales como el que se produjo a fines de 2021 tiene repercusiones económicas y sociales muy graves, algo que debe tenerse muy en cuenta sobre todo en América Latina, donde —como ya se señaló— el servicio de WhatsApp es una herramienta de negocio muy extendida.

Según investigaciones de Activa Perú, alrededor de 21% de peruanos puso en marcha su emprendimiento a través de redes sociales como Facebook, WhatsApp o Web. Por otra parte, durante la pandemia, un 31% de peruanos realizó compras por internet. No cabe duda, entonces, que una caída de las comunicaciones tendrá un impacto fuerte y directo en los negocios.

Estructura de un NOC

4.1 Modelo de servicio

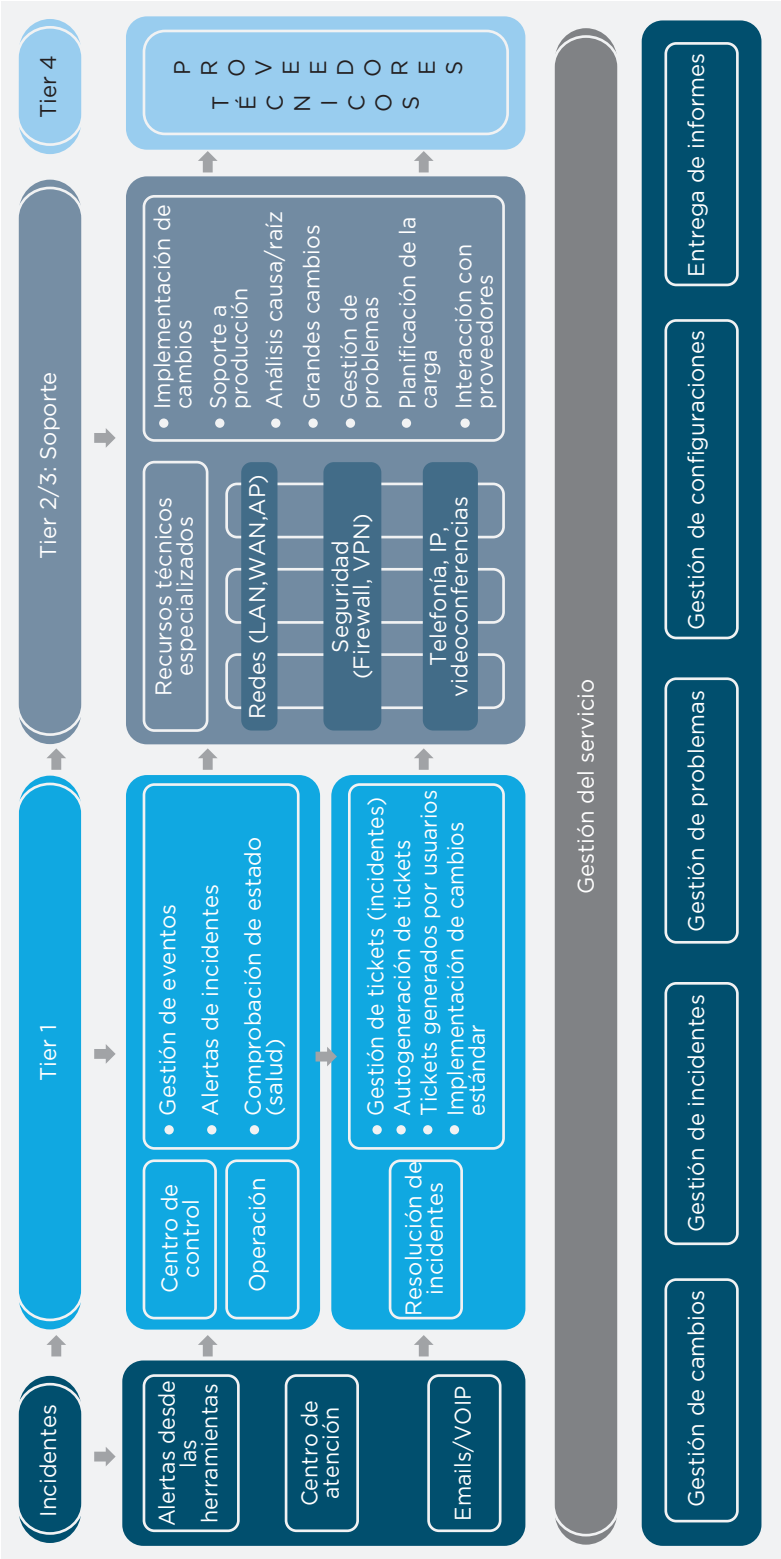
Desde un punto de vista conceptual, el modelo de servicio de un NOC estará estructurado por los incidentes que se generen desde cualquier punto de la arquitectura de red. Estos incidentes podrán ser reportados por algún usuario o podrán haber sido detectados por las herramientas de monitorización que se hayan implementado (gráfico 6).

El servicio será gestionado por incidentes, que tienen que ser incorporados en la herramienta de ticketing para su seguimiento y asignación, así como el paso a otros niveles de apoyo. Los incidentes pueden ser:

- Cambios: cuando se tenga que actualizar algún componente de la arquitectura de las comunicaciones. Se seguirá el mismo formato, se registra en la herramienta de ticketing y, según la complejidad, se asigna a un perfil específico.
- Incidentes: cuando la red ha sido afectada por algún tipo de incidente, que podrá derivar en un problema o que se cerrará, pero seguirá el mismo procedimiento, es decir, registro en la herramienta y asignación a un técnico.
- Problema: cuando el incidente se ha convertido en problema (mayor gravedad) o directamente se ha generado un problema en la red. El procedimiento es el descrito anteriormente.

El incidente podrá surgir en cualquier punto de la infraestructura montada. Puede ser reportado por el ciudadano o las empresas luego de haber intentado ingresar a un

GRÁFICO 6 Diseño de la herramienta de identificación y gestión de incidentes



Fuente: elaboración propia.

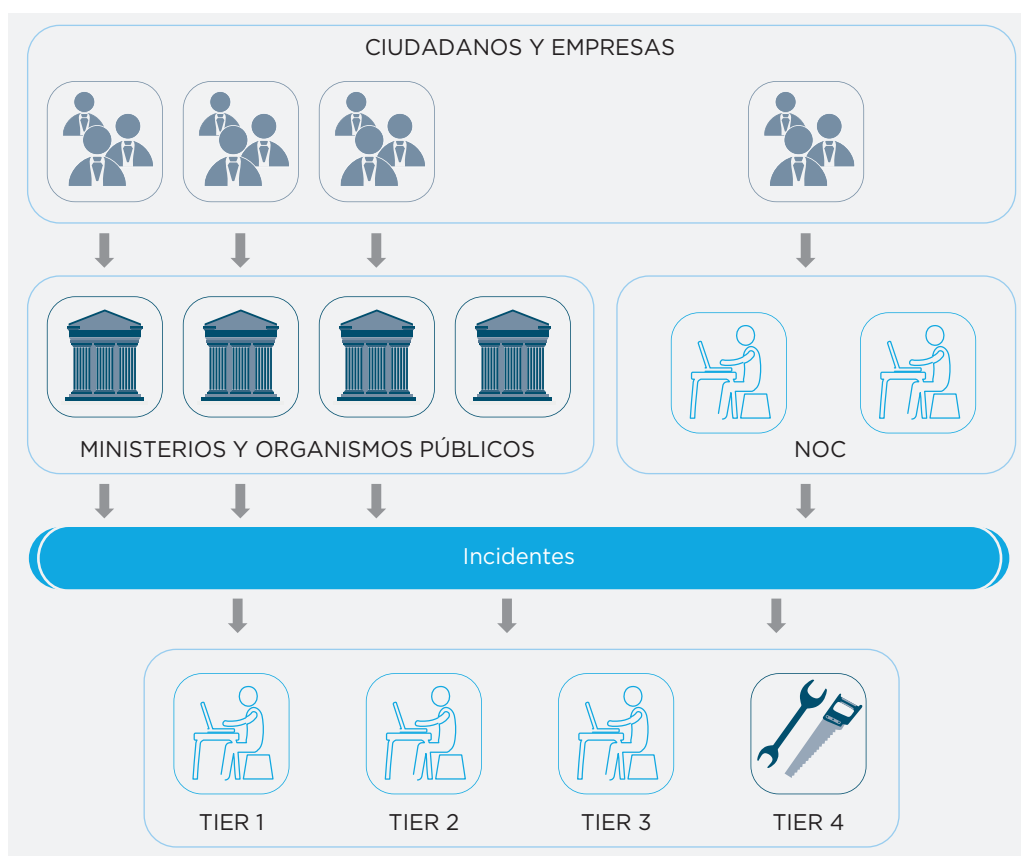
servicio público y haber encontrado un error de conexión. Además, puede ser reportado por un ministerio/organismo público cuando está fallando algún componente de red. Incluso puede ser reportado por el propio NOC, al detectarse anomalías de funcionamiento en la red.

En algunos casos, el error puede venir reportado desde el soporte de alguna aplicación. Por ejemplo, que falle el envío de un correo electrónico como finalización de un proceso en determinada aplicación; entonces, el proceso no se da por finalizado. Puede que el origen del problema sea renovar un certificado. También es posible que un funcionario reciba una notificación de error en un proceso que suele demorar, pero que finalmente es un error. O puede tratarse de un problema del wifi del organismo público. En estos casos, el error habrá sido abierto por el equipo de soporte de la aplicación y, una vez detectado el problema y el origen, tendrán que comunicarse con el NOC para que abran el incidente.

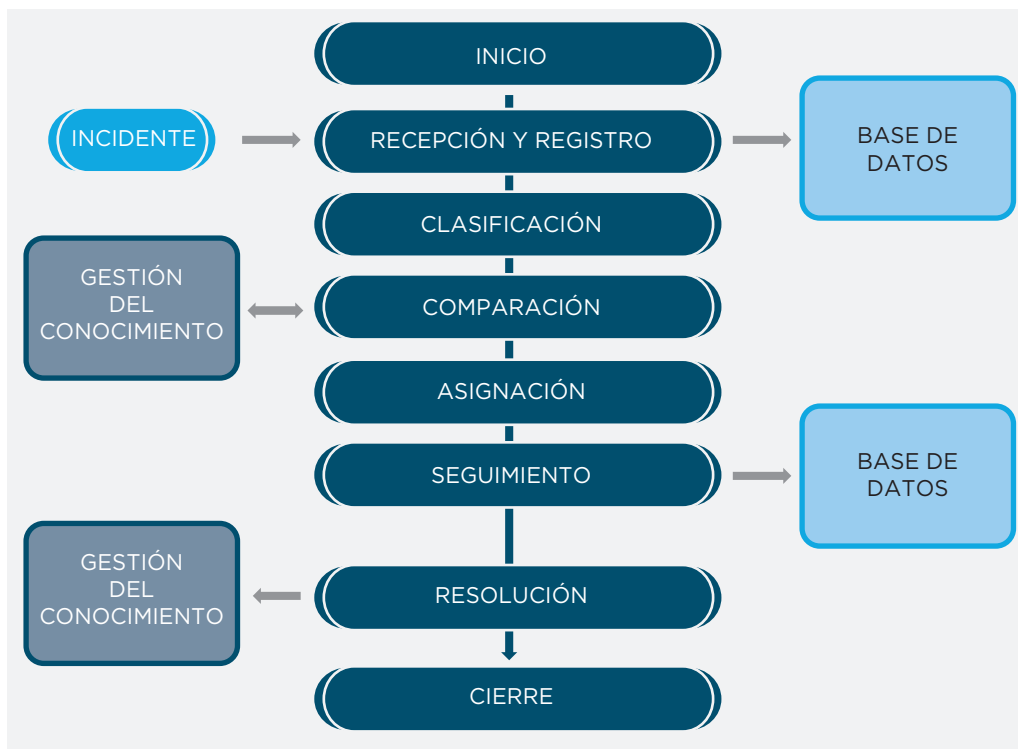
INFOGRAFÍA

4

Cadena de valor de un NOC



Fuente: elaboración propia.

GRÁFICO 7 Proceso que se implementaría para solucionar un incidente

Fuente: elaboración propia.

Cualquier incidente siempre debe ser registrado dentro de la herramienta de ticketing (gráfico 7), donde el registro de un incidente debería llevar la siguiente información:

- Número de incidente (#ID): numeración única del incidente que permite hacer su seguimiento.
- Descripción del incidente: en este campo debe consignarse toda la información posible para poder identificar y entender cuál es el problema.
- Usuario: persona que reporta el incidente, con quien se hace el seguimiento y se le da un cierre.

Cuando el incidente está registrado, se debería clasificar. Este proceso es importante ya que de ello dependerá la asignación del incidente al equipo correspondiente (por ejemplo, el equipo de telefonía), y a un nivel de prioridad (urgente, media o baja).

El siguiente paso será identificar en la base de conocimiento que se haya creado si el incidente se repite; en caso de que ese incidente haya sido identificado y resuelto en el pasado, se implementará la misma solución, se probará y se cerrará el incidente.

Si no se encuentra ningún incidente similar en la base del conocimiento, el equipo gestor asignará el incidente al equipo de resolución. Dependiendo de la complejidad del incidente, se asignará a los diferentes niveles.

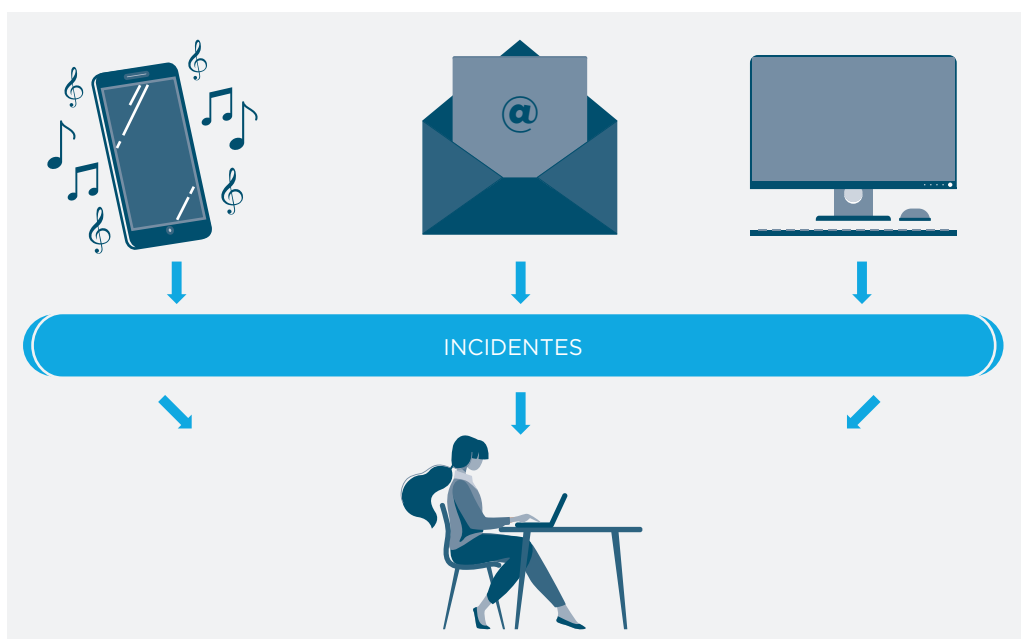
Cuando el equipo técnico resuelve el incidente, debe documentar la solución y actualizar la base de conocimiento, a fin de tenerlo a disposición en caso de que en el futuro surja un incidente similar.

Con la solución implementada y la documentación generada, se cierra el incidente. Llega el momento entonces de medir los tiempos de respuesta del equipo del NOC, y dicha información (estadísticas) es lo que indicará si se están cumpliendo los acuerdos de nivel de servicio (ANS).

4.2 Canales de atención

Un NOC deberá disponer, al menos, de tres canales de atención, siendo los más comunes el teléfono, el correo electrónico y una página web que incluya un formulario para informar el incidente (infografía 5).

INFOGRAFÍA 5 Tres canales para informar un incidente



Fuente: elaboración propia.

Los tres canales llegarán al centro de atención, que será el responsable de atender el incidente en un primer nivel, resolviéndolo o escalándolo al equipo adecuado según corresponda.

El centro de atención es muy importante, ya que de allí se llevará la primera impresión el usuario que esté reportando el incidente (ya sea un ciudadano, una empresa o un organismo público). Además, porque el perfil de quien atiende un centro de atención tiene una cualificación inferior a la de los técnicos de redes del NOC. Esto permite que se organice el trabajo sin colapsar a los técnicos, siendo el gestor del servicio el que asignará los incidentes en función de la criticidad y los ANS que se hayan firmado. Si el NOC no contara con este filtro intermedio, podrían llegar a colapsar los recursos de cualificación alta.

En el caso de que el incidente llegue por teléfono, el agente del centro de atención tendrá que realizar el registro en la herramienta de ticketing, recabando del usuario toda la información necesaria para poder dar de alta el incidente, y definiendo muy en claro sus características para su posterior asignación y seguimiento.

Cuando el canal seleccionado por el usuario sea el correo electrónico, el centro de atención transcribirá la información desde el correo electrónico al registro estándar de la herramienta. Si llegara a faltar información, será el centro de atención el que se pondrá en contacto con el usuario para completarla según sea necesario (este canal puede ser automatizado y se registraría directamente en la herramienta de ticketing).

Si el canal de comunicación escogido es la página web, el formulario preparado para registrar la información permitirá solicitar toda aquella información relevante y necesaria para dar ingreso al incidente en la herramienta de ticketing. Las ventajas de que la mayoría de los incidentes los reciba el centro de atención a través de este canal son las siguientes:

- Mientras el usuario registra el incidente, se le pueden dar opciones de hablar con alguien para completar lo necesario o incluso para resolver el incidente en línea (siempre y cuando la base de datos de conocimiento identifique un incidente parecido que pueda ser aplicado por el usuario).
- La posibilidad de migrar todos estos incidentes que residen en la base de datos de la página web a la base de datos de la herramienta de ticketing, creando el incidente de manera automática.

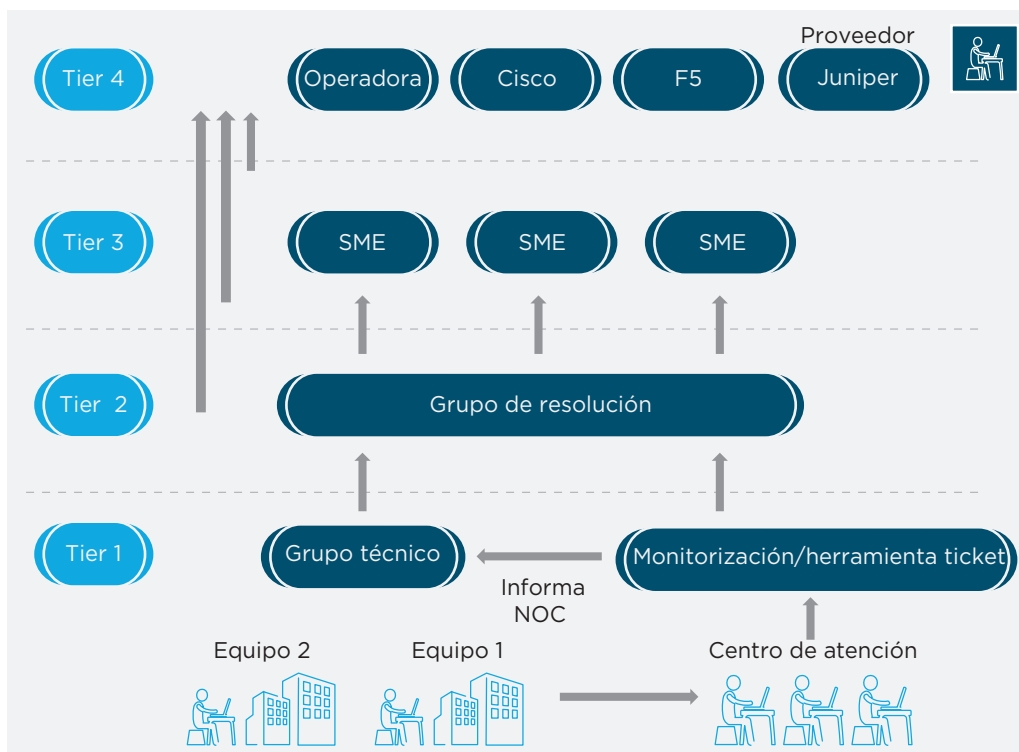
4.3 Niveles de soporte (TIERS)

Los niveles de soporte conforman otro de los puntales necesarios cuando se estructura un NOC. En nuestro caso, irán del nivel 1 al nivel 4 (sin tener en cuenta el centro de atención, que básicamente registra los incidentes) (infografía 6).

INFOGRAFÍA

6

Proceso de escalado dentro del NOC



Nivel 1 (Tier 1): Supervisar y responder

Dentro de los perfiles de técnicos de redes, el grupo del Nivel 1 serán los recursos con menos experiencia, y dentro de sus responsabilidades figuran:

- Acceder a la herramienta de ticketing para verificar si hay una solución identificada. En caso de tratarse de un problema repetitivo cuya solución está identificada, tendrá que implementar la solución.
- Monitorizar la conectividad y el tiempo de actividad de la red.
- Monitorizar el rendimiento de la red.
- Escalar el problema crítico al siguiente nivel (normalmente en los 15 minutos subsiguientes a que se le haya asignado el incidente).
- Escalar los problemas importantes de rendimiento al siguiente nivel (normalmente en los 30 minutos subsiguientes a que haya sido detectado el problema de rendimiento).

Nivel 2 (Tier 2): Analizar, reparar e informar

El Nivel 2 monitoriza al Nivel 1, para que no se atasque ningún incidente. Pero además tiene a cargo las siguientes tareas:

- Supervisar el hardware, la VPN, el protocolo de enrutamiento y el estado de la interfaz.
- Implementar parches y actualizaciones.
- Automatizar aquellas actividades de red repetitivas (por ejemplo, la gestión de accesos).
- Ofrecer servicios adicionales de optimización de red.
- Realizar copias de seguridad de los elementos de la red.
- Escalar el incidente/problema al siguiente nivel en caso de no poder resolverlo, siempre con la antelación necesaria para no incumplir los ANS del contrato.
- Documentar la resolución del incidente, clasificarla y cargarla en la base de conocimiento.

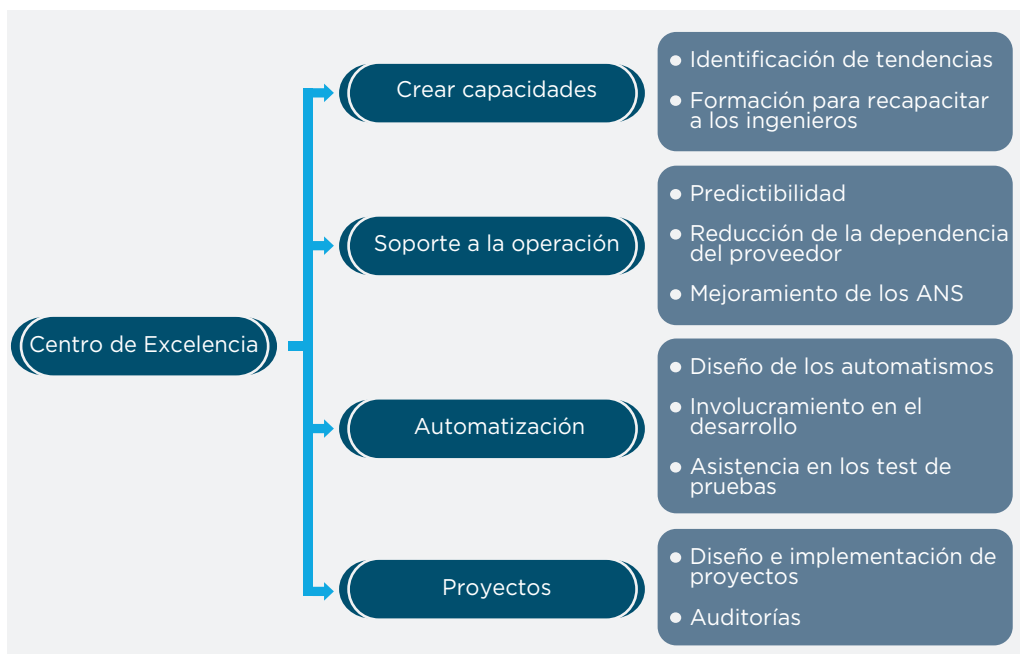
Nivel 3 (Tier 3): Administrar y mantener

El Nivel 3 comprende los técnicos de redes con más experiencia, quienes estarán monitorizando al Nivel 2 para que no se atasque ningún incidente y eso impacte en los niveles de servicio. Este grupo tiene encomendadas las siguientes tareas:

- Gestionar proveedores, incluida la reparación y/o reemplazo de dispositivos que no funcionen.
- Gestionar las redes y/o dispositivos en su totalidad.
- Crear y mantener túneles VPN en los dispositivos adecuados.
- Gestionar la configuración de todos los dispositivos.
- Resolver incidentes escalados desde el Nivel 2.
- Realizar el seguimiento y apoyo de los incidentes que escalan al Nivel 4 (Proveedores).
- Generar documentación sobre configuraciones y resolución de incidentes críticas.
- Gestionar políticas de grupo y cuentas de Active Directory.

Hay una tendencia en el mercado que pretende que los diferentes proveedores tengan una mayor independencia. A tal fin, se ha comenzado a manejar el concepto de Centro de Excelencia (*Center of Excellence*) (gráfico 8). En algunos casos, se podrá prescindir del Nivel 4, ya que estaría provisto por los recursos del NOC, mientras que, en otros, se contactará con ellos en contadas ocasiones.

GRÁFICO 8 Centro de Excelencia



Fuente: elaboración propia.

El Centro de Excelencia tendrá perfiles “Top”, que utilizaría en cuatro líneas de acción:

1. **Creación de capacidades:** en esta instancia será necesario adelantarse al mercado. El equipo del NOC tiene que estar a la vanguardia, siguiendo las tendencias del mercado en cuanto a qué perfiles deben formarse y de qué forma (lo ideal sería que la formación se imparta antes de que los conocimientos estén obsoletos).
2. **Soporte a la operación:** se trata básicamente de lograr que la operación del NOC sea fiable y predecible, con un objetivo doble: reducir su dependencia de terceros y mejorar los ANS.
3. **Automatización del servicio:** se trata de una parte muy importante para garantizar los tiempos de respuesta y de disponibilidad de la infraestructura.
4. **Participación en proyectos:** ya sean complejos o estratégicos, y ciertamente auditando aquellos que hayan llevado a cabo otros antes de que sean transferidos a producción.

Nivel 4 (Tier 4): Proveedores (Nivel experto)

El escalado viene del Nivel 3 y es el nivel de resolución experto que brinda el proveedor del dispositivo de hardware de comunicaciones, del software e incluso de las líneas de comunicaciones que opera una empresa de telecomunicaciones.

Se activa en los casos en que se detecta que un problema o un incidente reside en un componente de red de un tercero.

Es importante cerrar bien los ANS con los proveedores de comunicaciones para que puedan incorporarse en los ANS propios que tengamos en el NOC.

4.4 Diferentes niveles de servicios

Los niveles de servicio se miden con los ANS. Se trata básicamente de un contrato o acuerdo por escrito entre un proveedor de servicios y sus clientes externos o internos, en el que se especifica qué servicios suministrará el proveedor y bajo qué estándares, para que dichos servicios sean de calidad.

Por ejemplo, un proveedor de servicios de red puede establecer en el ANS que tendrá una disponibilidad del 99,99%; sin embargo, si la disponibilidad real es menor a la estipulada, se estaría ante un incumplimiento del ANS. En ese caso, la empresa podría tener que ofrecer una compensación a sus clientes. Esto dependerá de las penalizaciones que hayan sido pactadas en el contrato.

El nivel de servicio de un NOC es ininterrumpido: la infraestructura completa debe permanecer operativa 24 horas al día, 7 días de la semana y 365 días al año (24x7x365).

¿Qué debe incluir un ANS?

Además de saber sobre el ANS y su significado, es importante conocer qué debe incluir y cómo podría aplicarse en algunas áreas. Al momento de acordar el nivel de servicio, estos son algunos de los puntos que debe incluir:

- Definición: se refiere a las características de la prestación del servicio.
- Provisión: es el tiempo que transcurre desde que se firma el contrato entre el proveedor y el cliente hasta la entrega o puesta en marcha del servicio contratado.
- Disponibilidad: abarca sistemas, comunicaciones y soporte técnico.
- Atención al cliente: describe el método que ha de seguir el cliente al momento de realizar consultas o reportar incidentes sobre la prestación del servicio.
- Tiempo de respuesta: es el tiempo mínimo con el que se compromete la empresa para solucionar un incidente. También se pueden medir los tiempos intermedios: desde el registro del incidente hasta el primer contacto, desde la asignación del incidente hasta que se resuelve.
- Mantenimiento: incluye el detalle de las condiciones sobre la reparación de equipos, el mantenimiento y posibles intervenciones que afecten al servicio.
- Penalizaciones: son compensaciones y garantías relacionadas con el incumplimiento del nivel de servicio.

- Casos en los que no se aplican los ANS: sería un caso extremo, ya que el NOC siempre debería brindar una alternativa para que el organismo público siga funcionando. No obstante, en el caso de un incidente de un tercero (por ejemplo, una línea de fibra que se ha roto al hacer una excavación para una carretera), donde no pueda hacerse nada para solucionar el problema, podría frenarse temporalmente la medición de los ANS (esto no quiere decir que el NOC se desvincule del problema: siempre tendrá que dar una solución de conectividad).

Creación y mantenimiento del ANS

Para la elaboración de los ANS de un NOC en el ámbito de la Administración pública (ya sea NOC propio o subcontratado), deben tenerse en cuenta los siguientes factores:

- Cultura de la Administración (ministerio/organismo público) orientada al servicio del ciudadano: la cultura de servicio es importante porque el proceso de los ANS se trata principalmente de realizar mejoras según las necesidades y los requerimientos de los ciudadanos o los funcionarios públicos.
- Definición de las partes que participan en el ANS: normalmente las partes que deben participar en el proceso de definición de los ANS de red serán: i) los elementos de red (equipo técnico de arquitectos de redes); ii) los grupos de administración de los servidores donde se alojan las aplicaciones (arquitectos de aplicaciones), y iii) los funcionarios públicos que brindan dichos servicios.
- Estipulación de los elementos del servicio, que debe incorporar lo siguiente:
 - Definición de las horas hábiles de soporte y de los procedimientos fuera de horario. Lo más normal respecto de un NOC para Administración pública es que sea 24x7.
 - Estipulación de prioridad, tipo de problema, tiempo máximo para comenzar a trabajar el problema, tiempo máximo para resolverlo, etc.
 - Requisitos de nivel de soporte geográfico (*in situ*, remoto, etc.).

En muchos casos, los elementos del servicio se agrupan (normalmente lo llamamos solución), y según el nivel de servicio que se le quiere dar al agrupamiento quedará directamente ligado al costo del servicio. Por lo general, habrá tres niveles de servicio: Platino, Oro y Plata (cuadro 1). Claramente, la opción que se elija repercutirá en el presupuesto del servicio del NOC.

- Definición del ANS para cada grupo: las distintas unidades organizativas dentro de la Administración pública de un país tendrán requisitos diferentes. Los requisitos más utilizados suelen ser disponibilidad y rendimiento. Los requisitos del Ministerio de Defensa o del Ministerio del Interior suelen ser mayores que los de otros organismos. El cuadro 2 muestra a modo de ejemplo cómo abordar los detalles de implementación y desarrollo en un país determinado.

CUADRO 1 Ejemplo de los tres niveles de servicio

Solución	Platino	Oro	Plata
Dispositivos	Routers redundantes para conectividad WAN	Router redundante para realizar copias de seguridad en el sitio central	Sin redundancia de dispositivo
WAN	Conectividad T1 redundante, varias portadoras	Conectividad T1 con copia de seguridad de <i>Frame Relay</i>	Sin redundancia WAN

Fuente: elaboración propia.

CUADRO 2 Ejemplo de implantación y desarrollo en un país determinado

Organismo público	Aplicaciones	Costo del tiempo de inactividad	Prioridad de problemas cuando desciende	Requisito de servidor/red
Min. de Justicia	Base de datos de sentencias	Alto	1	Redundancia más alta
Min. de Educación	Historial escolar	Medio	2	Redundancia de núcleo LAN
Min. de Obras Públicas	Servicio de contratación	Medio	2	Redundancia de núcleo LAN
Min. de Salud	Historial clínico	Alto	1	Redundancia más alta

Fuente: elaboración propia.

- Negociación del ANS: este apartado es importante porque la negociación del ANS no debe ser una herramienta que penalice al NOC sino que permita realizar mediciones y preparar planes de mejora en el tiempo. En este sentido, es muy importante si se decide crear un NOC (propio o subcontratado) a nivel país. Como se señaló en puntos anteriores, en este caso se tendrán que agregar los ANS. Todo lo que esté agregado podrá tener un precio; todo servicio que esté desagregado (adicionales) tendrá un sobrecosto.

ANS que debería implementar un NOC

En este apartado se enumeran los ANS más comunes que se implementan en un NOC. Claramente, durante la etapa de definición y diseño del NOC para el país podrán surgir ANS diferentes de los que se enumeran en esta sección. Los ANS nuevos supondrán un sobrecosto, ya que habrá que crear nuevos campos en la herramienta de ticketing, para que luego se pueda realizar su seguimiento y medición.

Se deben diferenciar los ANS que se implementan para incidentes, los problemas o la implantación de cambios en la red. Al final, todos van a incidir en la disponibilidad y el rendimiento de la red; sin embargo, no todos son tan cruciales.

Los ANS cuya implementación recomendaríamos para un NOC serían los ligados al rendimiento y la disponibilidad, a saber:

- Tiempo de respuesta desde la recepción del incidente: incluye dar de alta el incidente en la base de datos de incidentes (herramienta de ticketing). En este ANS se incluye el primer contacto que se tenga con el generador del incidente (siempre que fuera un funcionario público, un ciudadano, etc.; es decir, que sea externo al NOC).
- Tiempo en el que el incidente se escala: esto se mide cuando el incidente no se resuelve en el nivel actual y se escala al nivel superior. Este ANS es intermedio, y es una herramienta de mejora para el propio NOC, ya que permitirá mejorar su base de datos del conocimiento, formar en dichos problemas al nivel actual, etc. Pero al final redunda en un cumplimiento de los ANS de disponibilidad y rendimiento.
- Cierre del incidente: será el momento en que el incidente se cierra, habiendo completado las actividades necesarias (implantación de parches, generación de documentación, comunicación del cierre del incidente, actualización de la base de datos de incidentes, etc.).
- Rendimiento: debería ser una actividad proactiva del propio NOC, donde enviaría paquetes de *ping* de protocolo de control de mensajes de internet desde el NOC hacia los diferentes organismos públicos a los que dé servicio. Si se crean “grupos de disponibilidad” podrán sacarse promedios de todos los dispositivos con el grupo de disponibilidad para obtener resultados razonables.
- Disponibilidad: el método más común es abrir un ticket del problema y una medición denominada “Minutos de usuarios impactados” (*Impacted User Minutes*, IUM). Este método tabula la cantidad de usuarios (funcionarios públicos, ciudadanos, etc.) que han sido afectados por una interrupción y lo multiplica por la cantidad de minutos de la interrupción.
- Número de incidentes: es un ANS para activar planes de acción, automatizándolos, pero con un claro objetivo de reducirlo en el tiempo (o al menos mantenerlo, ya que el intrusismo en la red siempre existirá).

Prioridad del servicio

El NOC debería definir la prioridad del servicio, que tiene que estar marcada por el impacto en la actividad y la urgencia. La prioridad se define como la secuencia en la que se atienden los diferentes incidentes.

- Criterio de urgencia es la velocidad o el marco temporal en el que el incidente necesita obtener respuesta. Los criterios de urgencia se pueden clasificar de la siguiente manera:
 - Bajo: es una tarea rutinaria o con una alta disponibilidad de tiempo de la red. El recurso o recursos que atiendan el incidente aplicarán un procedimiento de cierre estándar.
 - Medio: es una actividad específica, o con una moderada disponibilidad de tiempo de la red. El equipo asignado utilizará el procedimiento estándar, aunque puede proporcionar una resolución parcial al problema hasta que se encuentre la resolución completa.
 - Alto: es una actividad anómala, con poca disponibilidad de tiempo de la red. El equipo proporcionará una respuesta inmediata, evaluará la situación urgentemente y podrá involucrar recursos asignados a otros incidentes. Puede activar el soporte de Nivel 4 del proveedor de la línea, del hardware o de cualquier componente de red.
- Criterio de impacto se refiere a la forma en que los servicios públicos están siendo afectados por los diferentes incidentes en la red. Los criterios de impacto se clasifican de la siguiente manera:
 - Bajo: se refiere a un incidente que produce una degradación leve del servicio y en un campo limitado. En este caso se aplicará el procedimiento de trabajo estándar.
 - Medio: es un incidente que produce una degradación moderada del servicio o su corte sectorizado. El equipo asignado aplicará el procedimiento estándar, pero al igual que antes, puede buscar una resolución parcial (*workaround*) hasta que el incidente se cierre definitivamente.
 - Alto: se define como un incidente que produce la interrupción general del servicio o su degradación significativa. El equipo asignado tendrá una respuesta inmediata, pudiendo involucrar otros recursos que estuvieran asignados a otro incidente.

La combinación de ambos criterios generaría el cuadro de prioridades, que se ejemplifica en el cuadro 3.

CUADRO 3 Prioridades estándar de mercado

		Impacto			Prioridad
		Alto	Medio	Bajo	
Urgencia	Alta	1	2	3	
	Media	2	3	4	
	Baja	3	4	4	

Fuente: elaboración propia.

Cuantificación de los ANS

Los ANS marcarán unos valores que serán los que el servicio tendrá que cumplir; a tal fin, el NOC tendrá que preparar su herramienta de ticketing para poder llevar a cabo el seguimiento y la presentación de informes de esos valores.

Como en los casos anteriores, el cuadro 4 que figura a continuación pretende servir de referencia como marco de actuación para cuando se trabaje el caso concreto. Cabe destacar que se puede incorporar algún ANS, así como variar la valoración.

CUADRO 4 Ejemplo de marco de referencia de actuación

Gestión de incidentes del NOC		Tiempo de respuesta	Tiempo de solución	Disponibilidad
Prioridad crítica		30 minutos	4 horas	24x7
Prioridad alta		1 hora	8 horas	24x7
Prioridad media		2 horas	16 horas	24x7
Prioridad baja		4 horas	24 horas	24x7
Gestión de cambios del NOC		Tiempo de respuesta	Tiempo de solución	Disponibilidad
Prioridad crítica		30 minutos	8 horas	24x7
Prioridad alta		2 horas	16 horas	24x7
Prioridad media		4 horas	32 horas	24x7
Prioridad baja		8 horas	64 horas	24x7
Gestión de problemas				
Eficacia en la solución de problemas	Lo deseable es que la solución del problema se resuelva de manera adecuada, de forma que no se repitan los incidentes producto de ese problema. Por ello, la aceptación de incidentes producto de un problema solucionado es de 5%.			
Gestión de cambios				
Tasa de cambios exitosos	Lo deseable es que los cambios realizados en la infraestructura de red sean exitosos, es por ello que la aceptación de los cambios debería estar por encima del 95%.			
Disponibilidad de la infraestructura				
Disponibilidad a lo largo del período	La disponibilidad de la red deberá estar por encima del 99,5%.			

Fuente: elaboración propia.

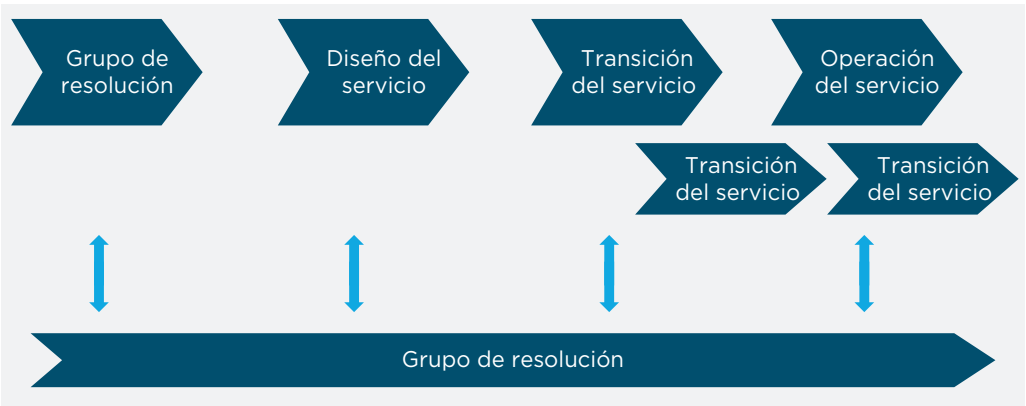
4.5 Servicio gestionado

Una vez que se definen los ANS y las prioridades del servicio, toca montar el servicio gestionado. ¿Cuál es el modelo de gobierno que tendrá el NOC y qué información suministrará a los organismos públicos o ministerios para que realicen su seguimiento?

Los servicios gestionados de un NOC se regulan con tres herramientas: i) los ANS; ii) el plan de calidad del servicio (*Service Quality Plan*, SQP), y iii) el informe de nivel de servicio (*Service Level Reporting*, SLR). La primera herramienta se abordó en apartados anteriores, las dos últimas se abordarán más adelante.

El ciclo de vida de un NOC es exactamente igual al de cualquier otro servicio gestionado en el mundo de la tecnología, y se detalla en el gráfico 9.

GRÁFICO 9 Modelo de servicio gestionado



Fuente: elaboración propia.

La fase de estrategia del servicio es la fase donde realmente se decide si el NOC será propio o gestionado por un tercero, así como las grandes líneas de lo que será el servicio a futuro (servicios que brindará) y para qué áreas se implementará (por ejemplo, toda la Administración pública, menos Defensa e Interior que por sus funciones requieren un servicio dedicado).

La fase de diseño del servicio es donde se define el catálogo de servicios, el nivel para cada uno de los componentes, el costo que puede asumirse, la definición de los ANS, la estipulación de información que se debe aportar a los diferentes organismos públicos, la definición de los gestores del contrato (cuando se externalice), la composición del equipo del NOC (cuando se haga con funcionarios), etc.

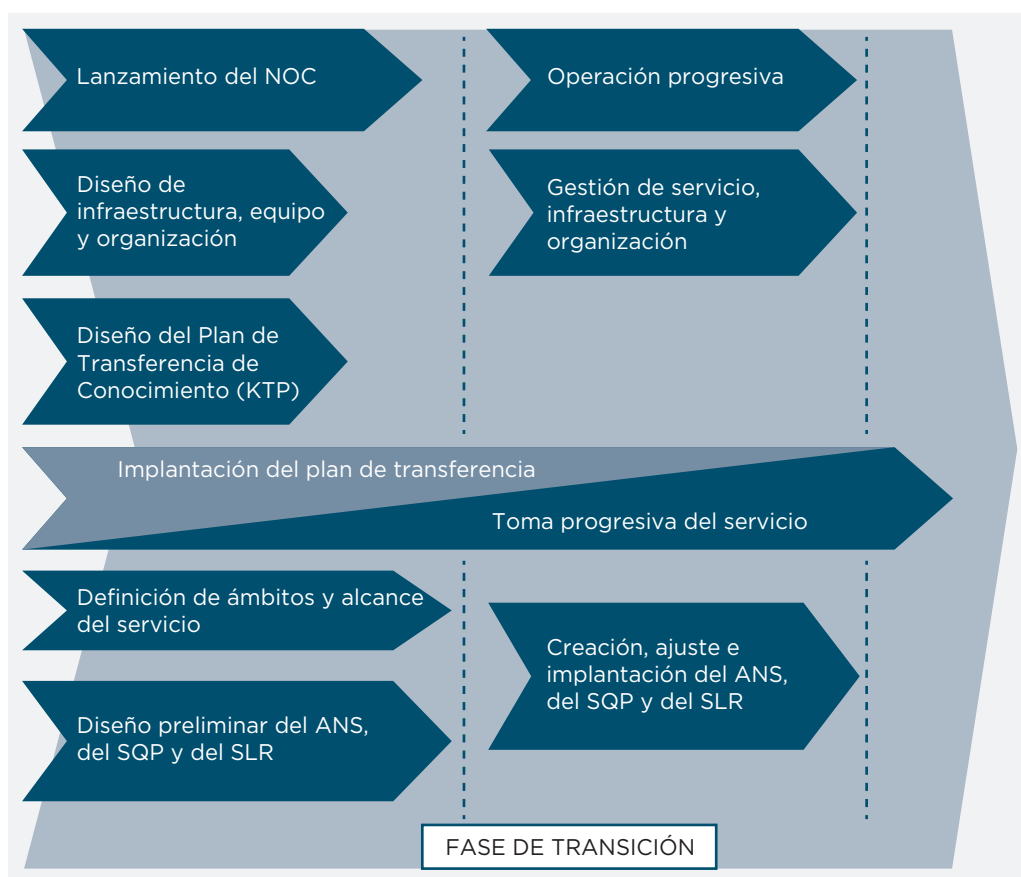
Por su parte, la fase de transición del servicio es clave para el funcionamiento del servicio que se suministre a futuro, y se tendrán dos visiones (que al final convergen): i) si lo teníamos desagregado (es decir, cada organismo tenía sus contratos con las operadoras y un equipo de técnicos para brindar servicio al organismo para el que trabajan), entonces, la estrategia que se decide es implementar un NOC para la Administración, gestionado por funcionarios (pero de manera centralizada), y ii) externalizarlo. En esta fase se establecerán todas las líneas maestras del servicio, y se implementará el plan de

calidad del servicio (de aquí en adelante, SQP) para poder efectuar planes de mejora. También, durante este periodo se implementan los ANS y se empiezan a medir (aunque no se aplican penalizaciones); se migrarán los elementos de red (cuando sea necesario); se formará al equipo del servicio en los procedimientos y en las herramientas, etc. Es decir, se establece el modelo organizativo y operativo del servicio.

A su vez, la fase de transición suele subdividirse en dos subfases. Se hacen todos los preparativos del servicio (procedimientos, herramientas, formación, etc.) y se comienza a proveer el servicio gradualmente (los ANS se miden pero no se aplican las penalizaciones; básicamente se miden para ver cómo va la fase de transición) (gráfico 10).

En la fase de operación del servicio se estará operando el NOC y la infraestructura asociada. Además, se estarán monitorizando las infraestructuras de los diferentes organismos públicos y ministerios, se resolverán los incidentes y problemas que

GRÁFICO 10 Fase de implementación del SQP y el SLR



Fuente: elaboración propia.

surjan en la red, y se aplicarán todos los cambios necesarios para que la red siga funcionando en un estado óptimo.

Entre la fase de transición y la de operación habrá que definir una etapa de estabilización del servicio, donde los ANS pueden estar suspendidos con el objetivo de conseguir la estabilización.

Al final del ciclo está la fase de devolución del servicio, que se hace efectiva en el caso de que se hubiera contratado a un tercero, se abriera una nueva licitación y la ganase un proveedor diferente al que estaba. Esta fase tiene que tomarse como un proyecto autónomo donde se sigan los pasos de la transición pero desde el punto de vista del que devuelve el servicio.

Plan de calidad del servicio

El plan de calidad del servicio (o SQP) del NOC se genera individualmente para cada cliente que se incorpora. En el caso que nos afecta, se generará un SQP por cada organismo público o ministerio que se incorpore al NOC.

El SQP tendrá que incorporar:

- La estructura del equipo del servicio que brinda el NOC.
- La organización del organismo público o ministerio en el marco del servicio con el NOC.
- Los procedimientos técnicos, de pruebas y de aceptación de incidentes, y los cambios o problemas.
- La gestión de la configuración de la documentación del servicio (esto es muy importante sobre todo en la fase de devolución).

A modo de guía, puede utilizarse el índice que figura a modo de ejemplo en la imagen 1, aunque podría complementarse con más apartados.

Informes de nivel de servicio

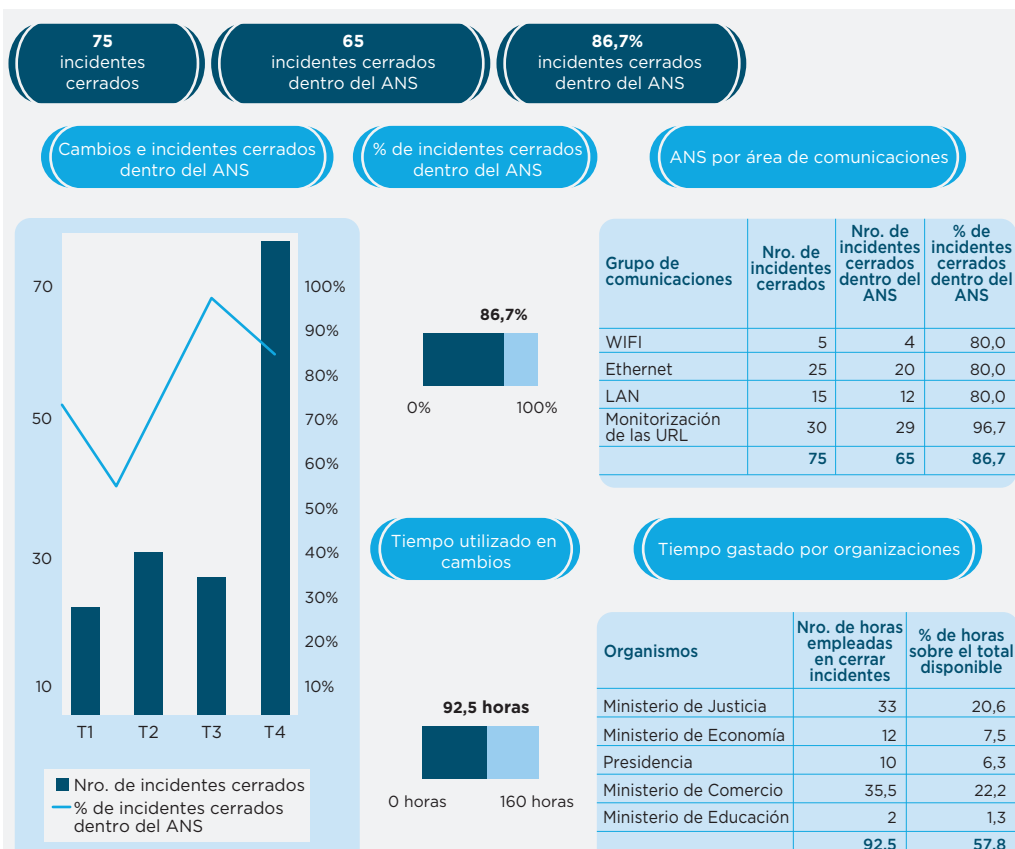
El informe de nivel de servicio (o SLR) comprende los informes que son necesarios para poder seguir el funcionamiento del servicio del NOC (gráfico 11). A su vez, tendrá que incluir todos aquellos indicadores que permitan hacer un seguimiento de los ANS que están incluidos en el contrato.

El SLR debe ser lo más automático posible. En el caso de un NOC de un país, debería incluir la información necesaria que debe entregarse en un periodo al ministerio/organismo público. Por otra parte, al estar automatizado, requiere que todos los indicadores necesarios estén dentro de la herramienta de ticketing, para que la fuente de

GRÁFICO

11

Ejemplo de un SLR



Fuente: elaboración propia.

datos sea única, y que haya un dato único, lo que evitará discusiones entre el operador del NOC y el ministerio/organismo público correspondiente. El hecho de que el operador del NOC utilice una herramienta para elaborar los informes de manera automatizada no impide que pueda haber vistas individualizadas, para que puedan entregarse a los diferentes ministerios/organismos públicos.

Los SLR también pueden servir como herramienta proactiva que permita detectar problemas antes de que los ANS se vean amenazados (por ejemplo, una tendencia de degradación de la red o del Nivel 1 de respuesta), lo que permite lanzar planes de acción para resolver este tipo de problemas.

¿Qué características tiene un SLR?

- Representa una colección personalizada de métricas sobre indicadores técnicos de la infraestructura que opere el NOC.

- Tiene una periodicidad (y plazo) de presentación que puede ser semanal (estadísticas de la semana anterior) o mensual (consolidación de todas las estadísticas del mes anterior), que es la más normal y extendida.
- Es un informe “*post mortem*”, pues analiza periodos pasados y con cuya información se elaboran planes de mejora continua.
- Se puede construir de manera agregada, teniendo una visión global del servicio del NOC a un país, pero también se puede generar de manera desagregada, para que cada ministerio/organismo público tenga su informe (esto es útil para dotar la partida presupuestaria de cada organismo público).
- Puede ser la herramienta de distribución del costo del NOC; si un ministerio/organismo público requiere más atención o tiene más incidentes, su costo será mayor a la hora de sufragar el costo del NOC.
- Siempre se define durante la fase de transición del servicio (véase el punto 4.6 de la imagen 1).

IMAGEN 1 Índice de un plan de calidad del servicio

1. INTRODUCCIÓN AL PLAN DE CALIDAD DEL SERVICIO (SQP):

- 1.1. Propósito del SQP
- 1.2. Ámbito del SQP
- 1.3. Control del SQP

2. PRESENTACIÓN DEL SERVICIO DEL NOC

- 2.1. Descripción del servicio
- 2.2. Objetivo y factores críticos de éxito
- 2.3. Ámbito del servicio

3. ORGANIZACIÓN DEL SERVICIO

- 3.1. Estructura de la organización del servicio
- 3.2. Roles, responsabilidades y obligaciones

4. GESTIÓN DEL SERVICIO

- 4.1. Gestión de incidentes
- 4.2. Gestión de problemas
- 4.3. Gestión de cambios
- 4.4. Gestión con el cliente (organismo público o ministerio)
- 4.5. Aspectos financieros y contractuales
- 4.6. Planificación, seguimiento e informes
- 4.7. Gestión del riesgo
- 4.8. Gestión de proveedores
- 4.9. Reuniones y correspondencia

5. GESTIÓN DE LA PRODUCCIÓN

- 5.1. Gestión de los incidentes/consultas
- 5.2. Gestión de mejoras/cambios
- 5.3. Gestión de peticiones
- 5.4. Gestión de la documentación
- 5.5. Gestión de la seguridad
- 5.6. Gestión de la disponibilidad
- 5.7. Gestión de versiones del software o el hardware de red

6. Planes de continuidad

- 6.1. Revisión y evolución de los planes de continuidad del negocio (redes redundantes, *workarounds*, etc.)
- 6.2. Pruebas de los planes de continuidad de negocio

Fuente: elaboración propia.

Es recomendable que un SLR incluya las siguientes métricas:

- Preguntas frecuentes del periodo: es una información útil tanto para el NOC como para el ministerio/organismo público. Si las preguntas frecuentes se repiten, podrían lanzar “píldoras formativas” al ministerio/organismo público para que se disminuya el tiempo empleado en el NOC en estas tareas (la automatización permitirá utilizar los recursos del NOC en aquellas tareas de mayor valor añadido, o por el contrario permitirá bajar el costo total del NOC). También puede ser una herramienta para formar al equipo de Nivel 1 en la resolución de incidentes.
- Listado de incidentes pendientes: serían todos aquellos incidentes que no tengan el estatus de “cerrado” en la herramienta (pudiéndose segmentar por los diferentes estados que se tengan en la herramienta; por ejemplo, “en progreso”, “pendiente de pruebas”, etc.).
- Tiempo de respuesta: es un dato importante, para conocer los tiempos de respuesta y de escalado de los diferentes niveles de soporte. Es muy importante para el responsable del servicio que los diferentes incidentes estén informados en la herramienta. Para que los informes sean lo más fiables posible, es necesario que cada técnico del NOC actualice la información de su incidente en la herramienta de ticketing.
- Cantidad de incidentes recibidos: este dato es importante básicamente por dos cuestiones: i) para saber que el servicio está dimensionado apropiadamente, y ii) para lanzar los planes de acción adecuados en cada momento. Cuantos más incidentes se vayan acumulando en el servicio, mayor será la sensación del organismo público de que las cosas no están funcionando como deberían.
- Estado de los ANS con respecto a los marcados en el contrato: es un punto básico si se aplican penalizaciones a los incumplimientos, y también para lanzar los planes de mejora continua.

El SLR siempre se define durante la fase de transición del servicio (véase el punto 4.6 de la imagen 1). Además, como ya se señaló, se trata de un informe “*post mortem*” que tiene como objetivo realizar un seguimiento diario de la infraestructura de red del NOC. Es una herramienta de monitorización.

Modelo de gobierno

El modelo de gobierno es la forma en que se estructura la relación y la comunicación entre el NOC y los diferentes organismos públicos, que comprende el modelo de escalado y comunicación de los problemas o incidentes, así como la periodicidad del seguimiento.

El modelo de gobierno en un país se podría organizar (al igual que el servicio) de manera agregada o desagregada.

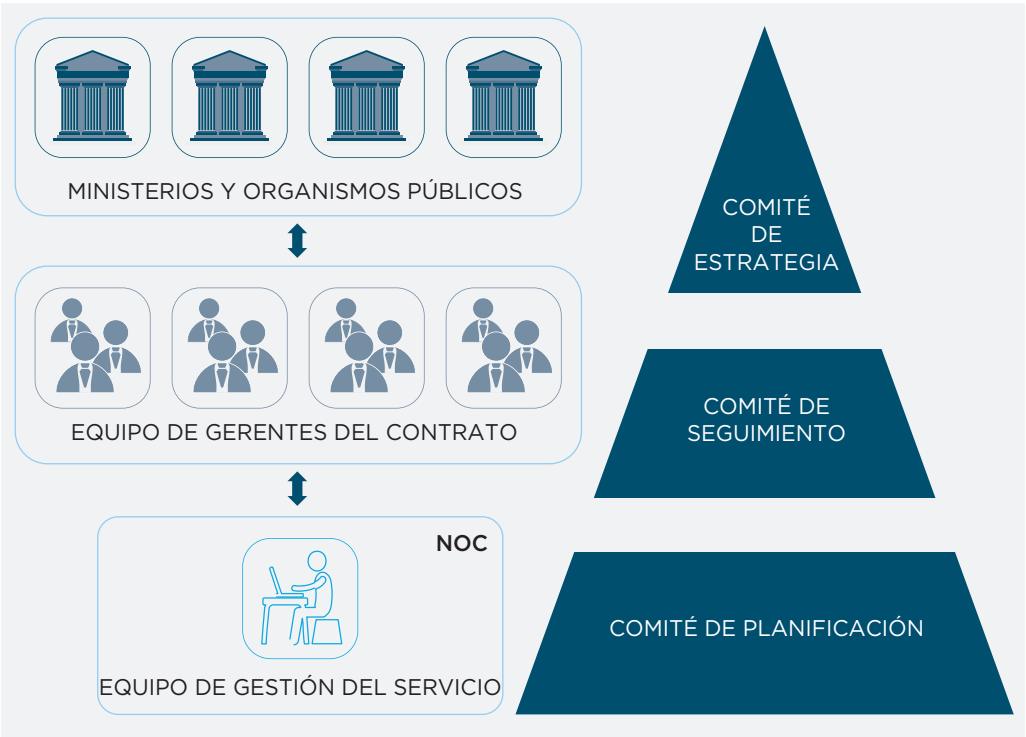
Modelo agregado de un NOC para un país

El modelo agregado es aquel que tiene una capa de funcionarios (equipo de gerentes del contrato; *Contract Managers*) entre los ministerios/organismos públicos y el NOC. Esta capa es la que canalizará toda la gestión del servicio, pero no los incidentes que encuentren los diferentes usuarios en los ministerios/organismos públicos. Son los garantes de que el contrato se cumpla en toda su extensión. A su vez, son responsables del seguimiento del servicio con el NOC y se reúnen periódicamente con los ministerios/organismos públicos para entregar la información del servicio individualizado para cada entidad (infografía 7).

Este modelo tendrá tres estamentos diferentes desde donde se gobierna el servicio:

- 1. Comité de planificación: el equipo de gerentes del contrato se reúne de manera individual con cada uno de los organismos públicos para discutir requerimientos

INFOGRAFÍA 7 Modelo de gobierno agregado



Fuente: elaboración propia.

y urgencias (desde luego que esta instancia aplica a los incidentes planificados, como son la actualización de alguna versión, la instalación de nuevo hardware de infraestructuras, etc.). Luego de dicha reunión, se tienen que priorizar todos los incidentes para una posterior reunión con el equipo de gestión del NOC y planificación de los trabajos definitivos. El equipo de gerentes del contrato también intentará planificar y hacer el seguimiento de los incidentes o problemas de red que todavía están abiertos, para lo cual el equipo del NOC tendrá que planificar dichas resoluciones.

Una vez cerrada la planificación de trabajo para el periodo siguiente, el equipo de gerentes del contrato tendrá que comunicárselo a los diferentes interlocutores en los ministerios/organismos públicos.

La periodicidad de las reuniones debería ser semanal hasta que el servicio esté maduro, y bisemanal cuando el servicio esté en marcha.

2. Comité de seguimiento: en este comité, el equipo de gestión del servicio del NOC se reunirá con el equipo de gerentes del contrato, donde se revisarán el SLR y los diferentes ANS de manera agrupada y de manera independiente, es decir, para cada uno de los organismos públicos.

Posteriormente, el equipo de gerentes del contrato tendría que presentar el seguimiento elaborado por el NOC con cada uno de los organismos públicos. Se verían el SLR y ANS individuales, así como el estado de cada uno de los problemas o incidentes.

La periodicidad de este comité debería ser mensual.

3. Comité de estrategia: sería el único comité conjunto, donde se incluirían a los ministerios/organismos públicos y se compartirían los retos, los planes de mejora implementados, las nuevas implantaciones, la ruta hacia donde tiene que ir derivando el servicio, etc.

La periodicidad de este comité sería trimestral (al principio) y semestral (cuando el servicio esté en marcha).

A modo de ejemplo, el gráfico 12 expone los participantes en los diferentes comités.

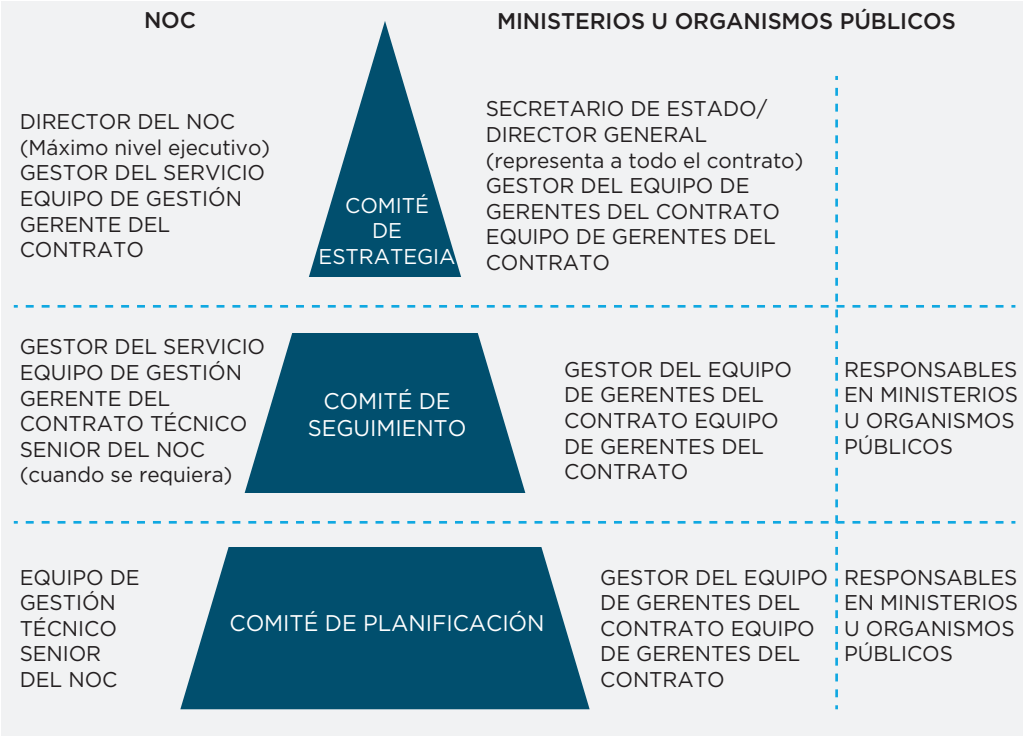
Modelo desagregado de un NOC para un país

El modelo desagregado es aquel en que cada uno de los organismos hace un seguimiento individualizado con el equipo de gestión del NOC (infografía 8).

En este caso, cada organismo público tiene que dotarse de un equipo que siga el contrato con el NOC.

Los comités son los mismos que en el apartado anterior. Tienen en común el comité estratégico, pero el comité de planificación y el comité de seguimiento actúan de manera independiente.

GRÁFICO 12 Participantes en los diferentes comités



Fuente: elaboración propia.

4.6 Herramientas del servicio

El uso de herramientas es básico para la gestión del servicio de un NOC. Las herramientas ya se describieron brevemente en la sección 4.2, pero aquí ahondaremos en su funcionamiento.

CUADRO 5 Pros y contras del modelo agregado

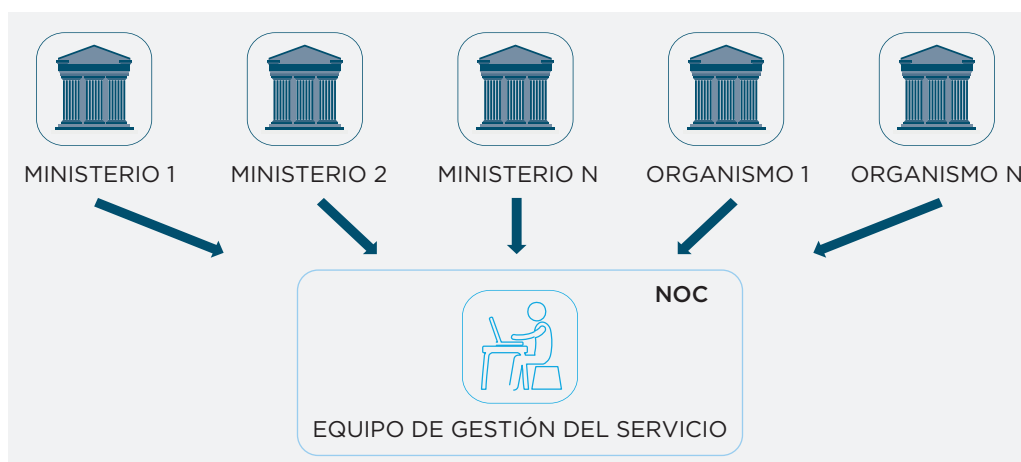
Pros	Contras
<ul style="list-style-type: none">• Unificación de todos los incidentes.• Economías a escala con la capa de funcionarios central: ahorro en costos.• Único canal para dar entrada a incidentes en el NOC (más económico).• Servicio estructurado y controlado.• Servicio más eficiente.• Planificación centralizada.	<ul style="list-style-type: none">• Pérdida de flexibilidad en los diferentes organismos.• Mayor impacto en la gestión del cambio.

Fuente: elaboración propia.

INFOGRAFÍA

8

Modelo de gobierno desagregado



Fuente: elaboración propia.

Herramienta de monitorización de la infraestructura de red

Se trata de una herramienta básica del servicio, que analiza la infraestructura de red en tiempo real, permitiéndonos anticipar problemas (cuando veamos degradación en el rendimiento) y recibir alertas.

El proceso de monitorización de red es donde se supervisan componentes de la red, servidores, firewalls, conmutadores, routers, etc. La herramienta recopila datos útiles de los diferentes componentes de la red, controlándola y administrándola. Se concentra en cuatro ámbitos:

1. Supervisión de errores.
2. Supervisión de las diferentes cuentas que tenga la organización.

CUADRO

6

Pros y contras del modelo desagregado

Pros	Contras
<ul style="list-style-type: none"> • Mayor flexibilidad para los organismos. • Mayor cercanía. 	<ul style="list-style-type: none"> • Nadie tiene el control de todos los incidentes. • Creación de estructura en cada organismo o ministerio: mayor costo económico. • El canal de atención del NOC tiene que ser mayor, ya que puede recibir incidentes de cualquier sitio. • Solo el NOC prioriza los diferentes eventos.

Fuente: elaboración propia.

3. Supervisión del rendimiento de la red.
4. Identificación de los activos (elementos de red, routers, switches, etc.)

En el caso de la red de un país, ministerio u organismo público, el software puede enviar avisos/señales (lo que en el sector se denomina “*ping*”) a diferentes puertos o componentes del sistema. Siempre se tiene en mente una monitorización de la red proactiva, lo que ayudará a encontrar soluciones a los problemas de red, evitando tiempos de inactividad o fallas.

El proceso de monitorización de la red se lleva a cabo en tres pasos:

1. PING: es una técnica básica pero eficiente, utilizada por el software de la red para probar su disponibilidad.
2. SNMP (protocolo simple de administración de red): monitoriza los dispositivos por separado dentro de una red por medio de la herramienta de monitorización.
3. SCRIPTS: cubren los vacíos (*gaps*) que no son cubiertos por la herramienta de monitorización.

Todos los mensajes generados por la herramienta de monitorización llegan a la consola del administrador de red, que tomará las decisiones adecuadas en función de la información que le esté suministrando la herramienta.

El software de monitorización de la red evalúa cómo funcionan las aplicaciones utilizando el acceso a la red. Supervisa principalmente tres cosas, a fin de asegurar el rendimiento de la aplicación (muchas veces creemos que tenemos un problema en la aplicación porque los tiempos de respuesta son altos, pero puede que tengamos un problema en la infraestructura de red):

1. Disponibilidad de la red para comprobar cómo está funcionando.
2. Utilización de la red y capacidad para examinar si está o no sobrecargada.
3. Rendimiento de la red para comprobar si los paquetes de datos llegan a destino a tiempo y con una velocidad constante.

Esta herramienta es capaz de generar patrones de destino, identificando patrones de rendimiento de la red. Si el rendimiento es deficiente, los administradores podrán determinar su causa en una fase inicial e implementar una solución para resolver el incidente.

Con la herramienta de monitorización se pueden crear mapas y paneles, que ayudan a visualizar la red en tiempo real. Se crean paneles de control personalizados, integrando los componentes de la red a través de objetos de mapa (gráficos de tráfico, íconos de estado, listas principales, etc.). También tiene que ser capaz de permitir que por defecto otro nodo se haga cargo del tráfico cuando un nodo principal de

red está inactivo o desconectado. Por otra parte, la herramienta debe generar informes detallados, de donde se puedan extraer estadísticas y gráficos con los datos de monitorización.

Dentro del apartado de herramientas de monitorización de la red, hay herramientas de software libre, como herramientas comerciales. Si el NOC es de un tercero, tendrá su propia herramienta de monitorización, con lo que solo deberá configurarse para el nuevo cliente (país, ministerio/organismo público).

Herramienta de ticketing

La herramienta de ticketing es imprescindible para la organización de un NOC. Una herramienta de ticketing permite registrar, organizar y priorizar los incidentes que suceden en un NOC.

La mayoría de los componentes de la herramienta de ticketing son soluciones web que cumplen en 100% con ITIL. También deberían cumplir con una serie de procesos ITIL, a saber:

- Gestión de incidentes.
- Gestión de problemas.
- Gestión de peticiones.
- Gestión de cambios.
- Gestión de los niveles de servicio (ANS).
- Gestión de versiones y despliegue.

El uso de esta herramienta no es de uso exclusivo del NOC, con lo que la inversión en la herramienta valdrá para gestionar el NOC, la tercerización de aplicaciones, el centro de atención, etc.

Si el servicio NOC es operado por un tercero, se le debe exigir que tenga una herramienta de ticketing para realizar el seguimiento del servicio NOC; además, tendrá que suministrar acceso para poder realizar el seguimiento de todos los incidentes que haya registrados para un ministerio/organismo público.

La herramienta tiene que ser configurable para incorporar incidentes que se recibían en el NOC mediante correo electrónico, teléfono o registro. El registro de incidentes puede ser realizado por un agente del centro de atención que abra el incidente al recibir una llamada telefónica de un funcionario público. Asimismo, puede ser creado por cualquier miembro del equipo de servicio del NOC, o cargado desde la aplicación web (en caso de existir).

Independientemente de los medios utilizados para la comunicación, la principal preocupación del ministerio/organismo público es recibir respuestas instantáneas y solucio-

nes rápidas, pero también esperan que se realice un seguimiento de sus consultas y que se los mantenga informados. Y aquí es donde entra en juego una herramienta de tickets.

Con este sistema de tickets, como ya se indicó, es más fácil priorizar, gestionar y realizar el seguimiento de los incidentes surgidos en el NOC. Además, ayudará al equipo del servicio del NOC a organizar el servicio, ya que este tipo de herramientas permite agrupar y categorizar los tickets para aplicar diferentes respuestas a cada solicitud.

La herramienta de ticketing se empieza a configurar en la fase de transición del servicio, ya que se tiene que configurar junto con los ANS contratados y con la metodología del gestor del NOC. El agrupamiento de incidentes es muy importante, ya que puede haber diferentes incidentes reportados por diferentes funcionarios públicos, pero que son parte del mismo problema (por ejemplo, el wifi del Ministerio de Economía de la calle tal no funciona). Agruparlo ayudará al equipo de gestión del NOC a cerrar muchos incidentes con una única solución.

Por otro lado, categorizar los incidentes tiene una importancia alta, ya que permitirá su solución en menos tiempo. Por ejemplo, si se ha producido un incidente con un router un tiempo atrás, y dicho incidente se categorizó correctamente, cuando ocurra un incidente parecido, se podrá aplicar la solución encontrada anteriormente. Además, se puede crear un ticket con toda la información generada meses atrás, para que el equipo del NOC pueda realizar una comprobación rápida, y según corresponda, avanzar con la aplicación o descartar posibilidades.

La herramienta de ticketing puede tener configurado un autoservicio, desde donde el funcionario público puede descargar algunas soluciones que podrían resolver el incidente en cuestión. El NOC es un área muy técnica y donde es preciso saber mucho para poder decidir si la solución es o no correcta. No se recomienda una extensa utilización del autoservicio, a menos que las soluciones hayan sido testeadas anteriormente y su complejidad de implementación no sea alta.

Por otra parte, la herramienta tiene que disponer de un módulo de presentación de informes que tendrá que configurarse en función de los ANS establecidos en el servicio del NOC. Esta es la información del servicio que se podrá extraer de manera rápida y que podrá ser agregada o desagregada. A su vez, la herramienta de ticketing debe ser fácilmente integrable con otras aplicaciones, debe permitir exportar información a una hoja de cálculo o a una presentación, y debe brindar acceso web al ministerio/organismo público para consulta sobre el avance de sus tickets.

Como en el caso de la herramienta de monitorización, existen softwares libres que pueden implementarse (con las limitaciones de funcionalidad que pueden llegar a tener), así como herramientas de mercado. Al igual que en el punto anterior, por la criticidad del servicio NOC que estamos gestionando, utilizaría herramientas de mercado si el NOC se implementase dentro de la Administración pública del país. Por el contrario, si el servicio de NOC se subcontrata, se tendrá que exigir al proveedor todo lo que se ha ido comentando en este apartado.

Repositorio de documentación

Esta es otra herramienta muy necesaria para la gestión eficiente de un NOC, con miras a que el servicio sea de calidad y tenga altos estándares de disponibilidad. Tan importante como el registro correcto de los tickets es documentar y archivar las soluciones o los parches implementados para resolver los diferentes incidentes del servicio.

Muchos fabricantes de herramientas de ticketing cuentan con una base de datos extendida donde se registra toda la documentación del servicio NOC. Dentro de este repositorio de documentación se encontrará toda la documentación sobre el funcionamiento del servicio NOC contratado, así como toda la documentación que se ha generado para la resolución de un incidente o problema.

Una vez más, lo ideal es que toda la documentación se adjunte al ticket abierto y categorizado. En caso de que la herramienta no incluyera el repositorio de documentación, habría que crearlo. Pero, como se señaló anteriormente, si la herramienta de ticketing es de mercado, lo más probable es que lo tenga incorporado.

Todo paso dentro del flujo de trabajo del NOC tiene que estar documentado; es decir, el recurso del NOC tiene que documentar correctamente las tareas que ha realizado, si el problema ha sido solucionado o si ha tenido que ser escalado al siguiente nivel. Con toda esa información en el repositorio del NOC, el servicio se torna más eficiente.

Un servicio “*post mortem*” añadiría la extracción del sistema de los tickets generados, y la utilización de la metodología de causa/raíz, para su aplicación a los planes de mejora. Este punto es primordial para tener un servicio de NOC proactivo, y no reactivo. Lo que hace la metodología de causa/raíz es extraer todos los tickets durante un periodo de tiempo, determinar cuál ha sido la causa/raíz de cada uno de los incidentes y considerar la posibilidad de agrupar los incidentes por solución. En el caso de que se encuentre un patrón común a los incidentes, se procede a documentar la solución e incorporarla al repositorio de documentación, por un lado, y a los planes de mejora, por el otro.

Los beneficios de la implantación y el uso de un repositorio de documentación son:

- Agilidad: respuesta rápida desde el centro de atención a usuarios si el incidente es parecido a alguna solución documentada, siempre y cuando lo permita el nivel de preparación y formación del centro de atención a usuarios.
- Asignación eficiente del incidente al técnico correspondiente: si el incidente tiene complejidad de resolución, se escalaría rápidamente al nivel adecuado sin pasar por los intermedios.
- Implantación del autoservicio: si los incidentes están bien categorizados y el servicio lleva tiempo funcionando, se pueden empezar a dejar soluciones en manos del funcionario público.

- Capacitaciones (presenciales o por plataformas de aprendizaje electrónico) para los funcionarios públicos: si el incidente se repite mucho con diferentes funcionarios, se puede dar una “píldora formativa” para que no se abran tantos incidentes.

Herramienta de *business intelligence*

La inteligencia artificial (IA) puede ser aplicada a un servicio NOC. Sin embargo, no existen soluciones desarrolladas, sino que el NOC tendrá que desarrollar y aplicar la IA para poder resolver y crear tickets.

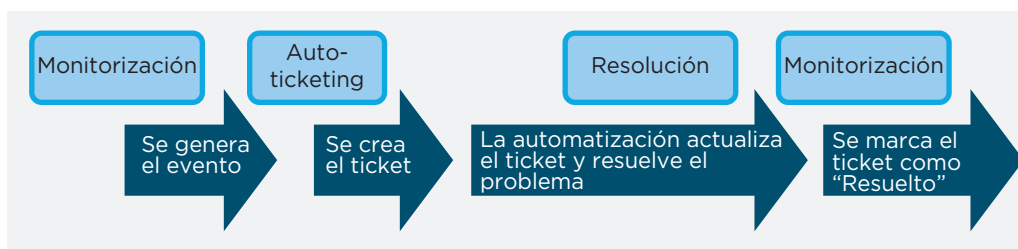
En este caso, se tendrían que identificar “disparadores de incidentes” (*triggers*) basados en alarmas identificadas. El sistema de IA realiza los controles adecuados. Si el control del ticket es verde, las notas de trabajo del ticket se actualizan y el ticket se cierra. En el caso de que fallase alguna verificación, el ticket pasaría a intervención manual. El proceso que se podría crear en el NOC se presenta en el gráfico 13.

En la monitorización de la infraestructura de red, si nuestro desarrollo de IA detecta algo para lo que ha sido programada, generaría un incidente, lo que a su vez generaría un ticket. Si el sistema tiene asignado el ID de resolución para ese tipo de incidentes, directamente resolvería el problema y actualizaría el ticket, cerrando el incidente de manera automática. Este sería el ideal de que todo fuera en automático, pero podrá haber variantes; por ejemplo, la resolución podría asignarse manualmente a un ingeniero de red (según los conocimientos y capacitación con la que cuente), quien luego de resolver el incidente, actualizará la herramienta de ticketing y lo cerrará.

Hay cinco categorías que pueden ser automatizadas, a saber:

1. El dispositivo ha dejado de responder a las peticiones.
2. Se ha perdido el agente de administración.
3. Se detecta un enlace defectuoso.

GRÁFICO 13 Modelo de gobierno desagregado



Fuente: elaboración propia.

4. Se registra una alta utilización de memoria o CPU.
5. Se detecta un servicio IP grande o un nodo inactivo.

Además, se pueden automatizar los cambios en la infraestructura de red. El ingeniero de red programa los cambios con un archivo CSV que consta de los parámetros que se necesitan cambiar, obtiene las aprobaciones y luego lo asigna al usuario de automatización para que lo ejecute a la hora programada. Hay una serie de tareas de cambio que para automatizarlas se pueden agrupar en tres categorías:

1. Cambios en el firewall estándar: ACL, ruta, NAT y configuración de la VPN.
2. Cambios de la LAN: modificación del puerto, VLAN, configuración troncal y canal ethernet.
3. Cambios en Load Balancer: renovación de certificado SSL, creación de listas VIP, etc.

Resulta evidente que la utilización de IA no puede darse al inicio del servicio del NOC, sino que tiene que incluirse como parte del SQP para incorporarla en los planes de mejora. Si el NOC es de nueva creación (en el caso de crearse en interno para dar servicio a un país), tendrá que pasar un tiempo hasta que se pueda implementar la IA, ya que se necesitará madurez en el servicio y experiencia. Si el NOC se contrata a un tercero, se podrán utilizar la metodología que se usó para algún otro cliente, habrá incidentes que serán parecidos y algo se podrá reutilizar. Claramente, desde el principio es difícil que puedan reutilizarse muchas cosas, se tendrán que ir incorporando a lo largo del servicio.

Esta herramienta también ayudará a generar algún informe que la herramienta de ticketing no genere de manera automática.

Base de datos con los recursos y su conocimiento

La tecnología avanza de manera muy rápida, los conocimientos que eran válidos deben actualizarse (certificaciones, formaciones, etc.), todo sumado a que el sector de las tecnologías tiene una gran movilidad (los recursos cambian de trabajo de manera bastante habitual). Todo ello hace que dispongamos de una base de datos de conocimiento por recurso. Esta base de datos nos ayudará a asignar correctamente las actividades al ingeniero de red adecuado, y a la resolución de incidentes de una manera ágil. El cuadro 7 presenta un ejemplo de base de datos y su conocimiento.

La base de datos puede categorizarse de acuerdo con los recursos y las certificaciones que tienen los ingenieros. Si tomamos el ejemplo de CISCO, cuenta con tres certificaciones principales para los entornos de red, a saber:

CUADRO 7 Ejemplo de base de datos y su conocimiento

	Routers y switches			Firewalls			Telefonia VoiP		
	Alta	Media	Baja	Alta	Media	Baja	Alta	Media	Baja
Ingeniero 1	JUNIPER NETWORKS	CISCO	Alcatel-Lucent Enterprise						
Ingeniero 2	CISCO	JUNIPER NETWORKS	Alcatel-Lucent Enterprise		paloalto FIREWALL	FORTINET			
Ingeniero 3							AVAYA	Alcatel-Lucent Enterprise	
Ingeniero N		CISCO	FORTINET	paloalto FIREWALL					

Fuente: elaboración propia.

1. CISCO CCDA (Cisco Certified Design Associate): sería la certificación con conocimientos básicos de los fundamentos de red.
2. CISCO CCNP (Cisco Certified Network Professional): se tienen conocimientos de redes LAN, WAN, grandes redes y redes de conexión telefónica (enrutadas o conmutadas).
3. CISCO CCIE (Cisco Certified Internetwork Expert): sería la certificación más alta y con mayor reconocimiento en el mercado.

Beneficios de la implementación de un NOC eficiente

La implementación de una buena infraestructura es clave para el desarrollo digital de un país, tal como se ha ido analizando a lo largo del estudio. Pero no solo vale contar con las infraestructuras instaladas, sino que hay que mantenerlas en funcionamiento. A tal fin, es básico haber implementado un centro de operaciones de red (*Network Operations Center*, NOC), ya que con ello se asegura el funcionamiento.

Hemos señalado la importancia de disminuir la brecha digital que existe entre América Latina y los países de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), y no se puede pensar en desarrollar digitalmente un país sin comunicaciones que funcionen.

Estamos en la era de la tecnología 5G, donde la menor latencia de las comunicaciones habilitará funcionalidades que no estaban hasta ahora operativas. La tecnología 5G habilitará (dará un salto cualitativo) internet de las cosas, Digital Twin, aprendizaje automático e inteligencia artificial. Asimismo, nos abrirá las puertas al comercio electrónico y permitirá vender productos más allá de nuestras fronteras. Para ello, resulta fundamental que las comunicaciones funcionen, y la herramienta para lograrlo es un NOC.

Una infraestructura de red en funcionamiento está democratizando el acceso a la tecnología, y si las comunicaciones llegan a más lugares (y no solo a las grandes ciudades), se estará cerrando la brecha digital que nos separa de los países de la OCDE.

Los beneficios de contar con comunicaciones que cubran la mayor parte del territorio nacional son, entre otros:

- Telemedicina: permite realizar consultas médicas a kilómetros de distancia, suministrando un servicio más completo al ciudadano.
- Aprendizaje electrónico: permite preparar cursos de formación en línea y que puedan cursar los ciudadanos en cualquier momento y en cualquier franja de edad. Incluso durante el confinamiento por la pandemia de COVID-19, esto permitió que muchos niños pudieran asistir a la escuela de forma remota.
- Interoperabilidad: permite la comunicación entre diferentes organismos públicos, y habilita la interacción del ciudadano con la Administración de manera digital.
- Crecimiento del tejido empresarial: las comunicaciones permitirán que las empresas puedan utilizar las capacidades de omnicanalidad que habilita la tecnología, pudiendo vender sus bienes o servicios a kilómetros de distancia.
- Formación digital: destinada a la población de los países, ya que solo en Europa hay una necesidad de cubrir una brecha de 1,6 millones de puestos de trabajo tecnológicos de cara a 2030. De impulsarse fuertemente la formación digital en los países, parte de esa brecha podría cubrirse desde América Latina. Además, esto incluye la ventaja del teletrabajo desde el hogar o la oficina para clientes que están a miles de kilómetros. Por ejemplo, se crearía una alternativa clara a la ofrecida por India, que hoy en día tiene problemas de incorporar recursos a los proyectos, teniendo, en algunos casos, un “*lead time*” de hasta cuatro meses.

En vista de los beneficios de las comunicaciones, debemos también valorar los beneficios que implica contar con un NOC eficiente, a saber:

- Una red operativa y en funcionamiento:
 - Que los datos, las comunicaciones, la información en general y las transacciones fluyan de manera constante por la red. Muy probablemente este sea el beneficio u objetivo principal de un NOC.
 - La monitorización constante de la red es la que nos permitirá asegurar que podemos reaccionar de manera inmediata ante cualquier incidente.
- Protección de la red ante incidentes:
 - La actualización del software de red permite protegerla contra ataques exteriores.
- Información en tiempo real:
 - Esto permite reaccionar e informar antes al ciudadano. Por ejemplo, si se cayera la red telefónica en un área de la ciudad o del país, se podrá informar por radio de forma anticipada y proactiva.

- Además, esta información estará suministrando datos del tráfico, de los ataques y, finalmente, del tiempo de uso de la red, lo que puede compartirse con la sociedad de manera periódica.
- Documentación de todos los incidentes generados en la red y de la forma en que se han solucionado:
 - Esto permitirá que cuando surjan incidentes parecidos, el tiempo de resolución sea menor.

