Luis Orlando Lázaro Medrano

ESPECIALIDAD FORMATIVA

Operación en sistemas de comunicaciones de voz y datos

IFCM0110

UF1348: Monitorización y resolución de incidencias en la interconexión de redes privadas con redes públicas

* Bibliografía usada en este documento:
UF1848: Monitorización y resolución de incidencias en la interconexión de redes privadas con redes públicas, Autor: Pedro Mora Pérez, EDITORIAL ELEARNING S.L. Edición: 5.1
Capturas de pantalla y textos electrónicos de varias web únicamente para ilustrar la actividad educativa

Luis Orlando Lázaro Medrano

Contenido

1. Procedimientos de monitorización en dispositivos de interconexión de redes

1.1. Herramientas de monitorización en dispositivos de interconexión de redes

Introducción

Dos de las herramientas principales para detectar alarmas usadas son MDM Multiservice Data Manager) NMS (Network Management System) de Nortel para detectar problemas en Red a nivel de líneas sobre equipos Passport / DPN y (Network Node Manager) de HPOV HP Open view que nos avisa de cambios de estado en equipos mediante SNMP (Simple Network Management Protocol).
Netcool de Omnibus es una herramienta que se está implantando desde hace algún tiempo y nos sirve también para monitorizar tanto la Red como los routers mediante la combinación de ambos tipos de alarma, las alarmas tanto de NMS como de los equipos llegan a una colectora que compara los datos que le llegan con una Base de Datos y el resultado final filtrado es mostrado por Netcool en el terminal del centro a quien pertenezca la gestión de esa línea.
Netcool incorpora también algunas herramientas de diagnóstico y pruebas desde la propia consola de alarmas.
El Sistema de gestión es una plataforma multivendedor, donde se integran diversas herramientas comerciales.
Entre ellas podemos destacar: Openview, Netcool, Oracle, MDM.
Desde el punto de vista de los elementos gestionados, puede decirse que el sistema integra 2 entornos diferentes:
–Ámbito Multiservicio, dentro de este entorno se supervisan las alarmas procedentes de los equipos en domicilio de cliente -pertenecientes a servicios MS-, bien a través de los traps que envían los propios equipos bien a través de las alarmas de los puertos de acceso (Passport, DPN) donde se conectan los routers.
–Ámbito IP, dentro de este entorno se supervisan las alarmas procedentes tanto de los routers de servicios IP, como de los equipos de acceso o de los equipos de core de la red IP. Dentro de este entorno están configurados monitores (ISM) que permiten realizar un seguimiento de la calidad de la Red.
La supervisión de alarmas de ambos entornos ha sido consolidada en un punto de entrada única (Consola Única), con objeto de facilitar las tareas de operación a los administradores de routers, evitando el tener 2 consolas abiertas para aquellos operadores que tenga servicios mixtos (MS e IP)

1.1.1. Descripción

Las herramientas de monitorización de red, son imprescindibles para cualquier entorno de comunicaciones, ya que su principal función es la búsqueda de componentes defectuosos o lentos, para avisar a los administradores de red, de dichos eventos mediante la generación de alarmas por las herramientas de monitorización.
Prácticamente la totalidad de las herramientas disponibles, poseen un amplio catálogo de eventos generadores de alarmas.
A diferencia de otros sistemas de monitoreo, como por ejemplo de intrusos, los sistemas de monitoreo en equipos de interconexión de red, buscan problemas en los diferentes dispositivos, para ir en busca de problemas causados por fallas o sobrecargas en servidores, o en la infraestructura de red.
La aparición de las diferentes herramientas de monitoreo, se ha hecho posible gracias a diversos procesos que se han generado en los diferentes ejecutivos del mundo de las TI, y su evolución gracias a la llegada de protocolos más avanzados de visualización de tráfico, como por ejemplo, netflow, jflow, Cflow, Sflow, IPFIX o Netstream.
Todo este desempeño, ha originado el propósito de estas herramientas de monitorización, para tener una perspectiva del todo, para poder clasificar los diferentes eventos que afectan a la operativa de una infraestructura de comunicaciones o servicio de negocio.
Estas herramientas de monitoreo, en su primera generación, mostraban elementos a través de una serie de colores.
Estas aplicaciones propietarias eran aptas para monitorear dispositivos activos e inactivos.

El código de colores era:
–En verde: todo está funcionando bien.
–En amarillo: se detectó que hay algún problema temporal que no afecta la disponibilidad, sin embargo, se deben realizar ajustes para no perder la comunicación.
–En naranja: el problema se ha hecho persistente y requiere pronta atención para evitar afectaciones a la disponibilidad.
–En rojo: el dispositivo se encuentra fuera de servicio en este momento y requiere acciones inmediatas para su restablecimiento.

En una 2ª generación de estas herramientas de monitoreo, realizaban un análisis exhaustivo muy profundo con el objetivo de poder evaluar independientemente, todos los componentes internos de cada dispositivo a gestionar por la herramienta de monitoreo.
Para analizar tal cantidad de elementos, estas herramientas de 2ª generación, se apoyaban en utilidades como por ejemplo analizadores de tráfico o sniffers, cuyas funciones son recolectar información de tráfico de la red y generar informes conforme a los parámetros recopilados.
Todas estas funciones, se gestionan desde una consola central.
Por último en una 3ª generación, estas herramientas analizaban todos los componentes de forma exhaustiva y de un extremo a otro, orientado al servicio.
En esta generación de herramientas de monitorización, son capaces de proporcionar información sobre problemas en las comunicaciones de la red, como por ejemplo cuellos de botella o problemas de latencia, que puedan existir a lo largo de todos los componentes del servicio.
En esta generación, cada dispositivo sabe cuándo informar a cada dispositivo sin que afecte a la operativa que está realizando, ya que de otra manera, estaría afectando al rendimiento, generando una sobrecarga de información y así, poder gestionar todos los dispositivos de una forma más eficiente.

El potencial de estas nuevas herramientas de la 3ª generación son:
–Predicciones de desempeño.
–Modelado de escenarios (simulación y emulación).
–Análisis y planeación de capacidad.
–Funcionalidades de ajustes a las configuraciones.
–Mediciones de impacto al negocio (calidad, salud y riesgos en los servicios prestados).
–Experiencia del usuario.
En definitiva, una buena herramienta de monitorización, sus principales funcionalidades deben de cubrir aspectos tales como:
–La administración remota de la herramienta, a través de navegadores, aplicaciones de Windows, etc.
–Notificaciones de las alarmas o eventos que se produzcan, a través de la visualización de la consola, por correo electrónico, por sms, o por medio de cualquier dispositivo que sea útil y de gran uso para recibir la información de la herramienta.
–Poseer una amplia gama de sensores, que posean capacidades para dar cobertura a un amplio abanico de elementos a gestionar.
–Poseer la posibilidad de poder administrar múltiples ubicaciones, desde tan solo una Tener localizado única instalación
–Ofrecer soporte para todos los protocolos de obtención de datos, que mejore los métodos comunes de operación de estas herramientas.

1.1.2. Uso

Los usos de las herramientas de monitorización, tienen su esencia en las redes multiservicios y red IP, donde las herramientas de gestión de fallos o de monitorización (por ejemplo Netcool), junto con la plataforma de hardware que lo sustenta, hacen la operativa de estas herramientas, en los diferentes servicios de la red.
Para afrontar las nuevas demandas en los usos de las herramientas de monitorización, es posible hacer unas nuevas implementaciones o modificaciones en estas herramientas, para mejorar y optimizar el funcionamiento de las mismas.

Podemos tener un ejemplo claro con el sistema Netcool.
–Unificación el criterio de tratamiento de las alarmas.
–Inclusión de nuevos campos en las alarmas de NetCool que enriquecen la información proporcionada.
–Supresión de campos no empleados en las alarmas de NetCool.
–Redistribución de las funciones de los servidores de gestión y de la redundancia de los mismos.
Los usos más comunes para la obtención de una correcta información del ancho de banda y del consumo de los equipos de red, es imprescindible para gestionar con eficiencia las redes, podrían ser:
–Evitan cuellos de botella con respecto al ancho de banda y en relación a los servidores.
–Localización de los dispositivos que están consumiendo ancho de banda.
–Proporcionar una mejor calidad en el servicio, gracias al servicio de proactividad que proporciona las herramientas de monitorización.
–Optimización de la carga en el ancho de banda y en el procesamiento de hardware, que se ajuste a un escenario real.
–Tener localizados todos aquellos puntos o dispositivos, que usan el ancho de banda, dónde se usan y cómo se están utilizando.
–Evitar estrangulamientos de ancho de banda y de rendimiento de servidor
–Proporcionar una mejor calidad de servicio a sus usuarios de manera proactiva
–Reducir costos comprando el ancho de banda y el equipo necesario basándose en cargas efectivas
–Incrementar ganancias evitando pérdidas causadas por fallos de sistemas no descubiertos
–Ganar tranquilidad: mientras PRTG no se comunique mediante correo electrónico, SMS, radio localizador, etc. se puede estar seguro que todo esta funcionando correctamente y de esta manera se puede dedicar a otros negocios importantes.

Estos usos de las herramientas de monitorización y gestión de fallos, facilita enormemente la resolución de problemas de manera proactiva, antes de que dichas amenazas se conviertan en un verdadero problema real para la infraestructura subyacente de comunicaciones y para el negocio que se sustenta bajo dicha infraestructura.

1.1.3. Funciones principales

A continuación, se va a proceder a realizar una descripción de la funcionalidad, los criterios de utilización y una ejemplificación de la herramienta de monitorización de red, para tener una ida profunda de este tipo de herramientas.
En este punto también haremos un estudio de nivel medio-alto sobre este tipo de herramientas, ya que son de vital importancia conocerlas a fondo para la resolución de incidencias en redes telemáticas.
–Gestión. Es la planificación, organización, supervisión y control de los elementos de comunicación para garantizar un nivel de servicio aceptable.
–Objetivos. Que la utilización de los recursos se aproxime al 100%, mejorando la disponibilidad y los recursos.
–Métodos de Gestión. Conjunto de herramientas, aplicaciones y metodologías que permiten gestionar una red.

Existen dos métodos básicos para la gestión:
–Monitorización de la red. Consiste en obtener información de los elementos que componen la red.
–Control de la red. Actúa sobre dichos elementos.

Métodos de Monitorización:
–Sondeo (Polling). Consiste en acceder de forma periódica a la información de los elementos gestionados. Es sencillo pero supone mucho tráfico.
–Notificaciones (Event Reporting). Son los elementos quienes envían notificaciones ante determinados eventos. Los elementos son más complejos.
–Mixtos. Sondean un grupo de elementos, y notifican al gestor cuando ocurre algún evento.

–Gestión integrada. Por lo general se va a disponer de un único sistema de gestión para todos los elementos gestionados, que nos va a facilitar los datos mediante una interfaz sencilla y única.

Para ello todos los elementos de la red, independientemente del fabricante, modelo, etc., deben facilitarnos los datos y responder a nuestras consultas de igual forma.
El protocolo empleado para gestionar equipos en Internet es SNMP (Simple Network Management Protocol)

1. Gestión en internet: SNMP

Modelo de Información

Para referenciar los distintos recursos de un sistema remoto para gestionarlo, utilizaremos el protocolo SNMP.
Protocolo que funciona sobre IP, con lo que podremos utilizar cualquier red IP (pública o privada) para gestionar dichos equipos.
Una de las preguntas importantes en este sentido sería por ejemplo la siguiente:
¿Cómo obtendremos los distintos recursos del sistema remoto? Para ello utilizaremos un método común a todos los sistemas para nombrar los objetos: Object Identifier (OID).
Se creará un Árbol de OIDs, que sigue una arquitectura jerárquica y está definido por una serie de números enteros, no negativos, separados por puntos (dependiendo del orden dentro de dicho árbol).

1.2. Modelo de Gestión SNMP

Protocolo SNMP

El protocolo SNMP o “Simple Network Management Protocol” es, como su nombre indica, un protocolo sencillo para la gestión de redes, es decir, que nos permitirá gestionar los distintos equipos de red (configurar y consultar parámetros) de una forma sencilla.
Para ello se sirve del protocolo UDP, ya que básicamente haremos consultas, y el elemento consultado nos enviará la respuesta.
Existe otro método de funcionamiento; mediante Traps, es decir, cuando el elemento gestionado sufra algún cambio, nos enviará una notificación, indicando qué es lo que ha ocurrido, sin necesidad de que nosotros le hayamos preguntado.
Las consultas se harán a través del puerto 161, y cuando el equipo gestionado nos quiera enviar un trap, lo hará al puerto 162 del sistema gestor (o equipo de gestión).
Los mensajes SNMP seguirán siempre el siguiente formato:
–Versión SNMP. La versión SNMP que estamos utilizando.
–Community. La Comunidad SNMP (o clave SNMP) con la que vamos a hacer la consulta.
–PDU SNMP. En ella se indica si el mensaje es de petición, de respuesta, o de trap, así como los datos de la consulta/respuesta/trap.

Operaciones SNMP

Para poder consultar/configurar los distintos parámetros, se emplearán distintos tipos de PDUs:
–GetRequest. El gestor realiza una petición de valores específicos de la MIB del agente.
–GetNextRequest. Solicitamos el valor siguiente al que enviamos.
–GetResponse. El agente devuelve los valores solicitados en la consulta del gestor.
–SetRequest. El gestor asigna un valor a una variable del agente.
–Traps. El agente nos notifica que ha ocurrido algún evento.

Control de Acceso

Este control de acceso se utiliza para limitar quién puede acceder o modificar parámetros por SNMP un determinado agente.
Existen una política de autenticación y una política de autorización:
–Autenticación. Para ello se utiliza la community snmp, que sería algo así como una clave.
–Autorización. Dependiendo de la “clave” (o community) que utilicemos, podremos tener acceso a toda o a una parte del árbol de MIBs, y si este acceso es de escritura o de sólo lectura.

A esto se le llama vista.
Este control de acceso también se puede limitar por IPs, es decir, podremos filtrar desde que IPs se nos pueden hacer consultas desde un sistema gestor, así como la community que deben emplear.

Herramientas y aplicaciones utilizadas. Características

MRTG: Multi Router Traffic Grapher

MRTG o Multi Router Traffic Grapher es una herramienta para monitorizar la carga de tráfico en los enlaces de una red.
MRTG genera páginas HTML que contienen gráficos PNG, que nos muestran el estado del tráfico de forma activa.
Básicamente MRTG es un script escrito en Perl, que se encarga de leer vía SNMP variables de los distintos elementos de la red a monitorizar.
Posteriormente, mediante una rutina escrita en lenguaje C representa dichas medidas en gráficos, que se insertan en páginas Web, para ser visualizados con cualquier explorador de Internet.
Esta Web incluirá cuatro gráficas para cada medida; una diaria, una semanal, una mensual y una anual, pudiéndose así observar las evoluciones con distinta precisión.
MRTG está diseñado para mostrar el tráfico, tanto de entrada como de salida, de los distintos interfaces de los equipos.
Aun así podremos editar el fichero de configuración y añadir gráficas para cualquier variable de los equipos, tales como uso de CPU, memoria libre/ocupada, número de conexiones establecidas, etc.
Al igual que otras herramientas de monitorización de tráfico de red, este protocolo utiliza el protocolo de administración de redes SNMP, para gestionar y recolectar información proveniente de los dispositivos (habitualmente routers), los cuales están vinculados a colectoras que gestionan dichos dispositivos.
Debido a la ingesta información que se genera, hay que distinguir la información de entrada y salida que se generan en dichos dispositivos, para poder clasificar esta información y tratarla posteriormente para la generación de informes, como resultado.
También, se pueden utilizar aplicaciones en lugar de consultar un dispositivo que utilice SNMP, utilizando 2 valores que se corresponderían con la entrada y salida del dispositivo. Para ello se utiliza normalmente Scripts que monitorean la máquina local.

Funcionamiento

MRTG, utiliza un “demonio”, el cual es “invocado” por las tareas pertinentes para la recolecta de información, ejecutando los scripts incluidos en la configuración.
Esta recolecta de información, esta aplicación la realiza cada 5 minutos.
Las últimas versiones, a diferencia de las primeras versiones, almacenan la información en una base de datos, gestionada por RRDtool, a partir de la cual se generan los informes y gráficas, de forma separada las una de las otras.

Netcool

Dos de las herramientas principales para detectar alarmas usadas en los centros de gestión Personalizados son MDM (Multi service Data Manager) NMS (Network Management System) de Nortel para detectar problemas en Red a nivel de líneas sobre equipos Passport / DPN y (Network Node Manager) de HPOV HP Open view que nos avisa de cambios de estado en equipos mediante SNMP (Simple Network Management Protocol).
Las principales características que presenta Netcool Network Management son:
–Un conjunto de herramientas de monitorización de red, que proporcionan descubrimiento de red, gestión de incidencias, supervisión y configuración.
–Permite la generación de informes de red, complejos y diversos de topologías heterogéneas y homogéneas, cuyos informes y visualización, están centralizados.
–Mecanismos de supervisión y descubrimiento de la red.
–Gestión de incidencias y errores en los dispositivos SNMP gestionados.
–Proporciona la funcionalidad idónea que dan un soporte eficaz a la gestión de despliegue y cambios en la configuración de red.

Netcool incorpora también algunas herramientas de diagnóstico y pruebas desde la propia consola de alarmas.
–La capa Netcool es la capa superior del Sistema de Gestión. Es ésta la que proporciona el interfaz de cara al usuario. En ella se realizan diversas tareas:

- ·Consolidación de alarmas.
- ·Recolección.
- ·Duplicación.
- ·Correlación.
- ·Enriquecimiento.

–Como se ha comentado anteriormente el sistema, y como consecuencia de su desarrollo, integra dos subsistemas independientes (MS, IP) en uno solo. Por esta razón, se puede dividir en dos niveles:

- ·Nivel de Recolección.
- ·Nivel de Presentación.

–El objeto de la capa de presentación es doble; por un lado consolida las alarmas de los entornos IP y MS. De este modo el operador al conectarse a este nivel -que se ha denominado Consola Única- puede tener en una misma lista de eventos, alarmas de ambos entornos.
Por otro lado esta capa de presentación atiende las peticiones de todos los operadores que se conectan al sistema.

Herramientas de la Consola Netcool

En el menú Tools de la consola de Netcool, aparecen diferentes herramientas algunas de ellas útiles para el tratamiento de las incidencias, y otras para actualizar o corregir posibles errores en la Base de Datos que tiene el Sistema de Gestión de Interlan con los datos de todos los routers que actualmente están en gestión. Las primeras herramientas que aparecen en el menú son el ping y el telnet, en ambas te pide como valor la IP de gestión, o el nemónico.

Históricos

Te pide como valor el nemónico del router (Name of the host), y dibuja una gráfica que representa el valor que se seleccione de la lista Tipo de histórico:
–CpuUsage: Representa el uso de CPU.
–MemoryUsage: Representa el uso de memoria.
–LanCollisions: Representa las colisiones LAN
–FencBenc: Representa el Fenc y el Benc
–FrameRelayErrors: Representa los errores en la FR
–BWinPVC: Tráfico de entrada por PVC
–BWoutPVC: Tráfico de salida por PVC

Herramientas y aplicaciones utilizadas

HP Openview

–La Gestión de routers se implementa a través de un conjunto de herramientas de HP Openview: OV Operations y Network Node Manager. El router es gestionado a través de 2 procedimientos complementarios:

- ·Interrogación periódica desde la colectora al router en cuestión.
  En este caso la comunicación es bilateral (primero la colectora pregunta al router, y a continuación este contesta). Se deduce de aquí un requerimiento importante del Sistema de Gestión: “es necesario que haya conectividad permanente entre la colectora y el router gestionado”.
- ·Envío de traps SNMP (Simple Network Management Protocol) desde el router a la colectora ante determinado tipo de eventos.
  En este caso la comunicación es unilateral (el router envía un paquete UDP a la colectora)

MDM

–Dentro del Sistema de Gestión hay integradas 2 máquinas: mdmgestion y mdmgestion2 (una backup de la otra) cuya función es recibir las alarmas de los Passport y DPN de acceso.
–En estas máquinas se ha instalado un software propietario de Nortel. De todas ellas nos centraremos en la parte de Gestión de Fallos.
–La gestión de fallos de los puertos de los Passports a los que se conectan los routers (Equipos en Domicilio de Cliente) se realiza a través del servicio gmdr de la máquina que es quién consolida todas las alarmas recibidas.

ORACLE

–Un elemento esencial en la plataforma de Supervisión es la Base de Datos Oracle.
–Dada la importancia de este elemento se ha dotado de Redundancia a varios niveles.: A nivel físico y a nivel lógico
–Esta Base de Datos realiza diversas funciones:
·Histórico de eventos de netcool .Estos eventos son volcados desde la Consola Única a través de un gateway que se ejecuta en el cluster de base de datos. Se almacena en la base de datos REPORTER.
·Repositorio de todas las mediciones de CPU y memoria que se realizan desde NNM y que son volcadas de forma periódica a la Base de Datos. Se almacena en la base de datos NNM
·Inventario de los equipos de gestión. Es lo que se denomina BDSG (Base de Datos del Sistema de Gestión). Se almacena en la base de datos REPORTER.
El contenido de BDSG es el elemento de la Base de Datos ya que si se pierde la gestión de los routers pues no habría:
–Enriquecimiento de alarmas
–Personalización de alarmas por grupo de gestión

Perfomance viewer y Data viewer

Estas son herramientas del software MDM (Multiservice Data Manager), que se realizan para realizar monitorizaciones gráficas de la Red Multiservicio.
El Data Viewer, solo se podrá encontrar en las últimas versiones de MDM, ya que es la aplicación más moderna de las 2.
Performance Viewer, a pesar de ser más antiguo, sigue siendo muy usado en el ámbito de los centros de soporte remoto, y en las últimas versiones de MDM se ha recuperado o se ha añadido al Data Viewer.

1.2. Pruebas de monitorización

En las pruebas de monitorización, podemos extraer información muy valiosa, sobre el proceso del sistema de monitorización en sí, para comprobar la efectividad de los diferentes tests a realizar (esto dependiendo de la herramienta de monitoreo que se vaya a implementar).

A continuación, se va a mostrar una serie de pruebas de monitorización, que resultarán del todo imprescindibles para la comprobación de los distintos servicios en los dispositivos de la sede de cada cliente o de una corporación.

Prueba de obtención de información del equipo

Este test controla si existen diferencias entre la configuración actual del equipo y la provisionada en el inventario.
El resultado aparece diferenciado en dos partes. En la parte superior de la pantalla aparece la parte provisionada en el inventario, y la inferior la configuración actual del equipo.
Los Datos Sede, mostrarán la información del puerto de la sede del cliente.
En el caso de que la sede del cliente esté diversificada, mostrará los datos de ambas sedes (principal y secundaria).

Prueba de consultar tráfico

Este test controla la existencia de tráfico en la sede del cliente, tanto en el puerto como en sus vlan´s. El test consulta varias veces el tráfico de la sede, una cada intervalo dado, accediendo a los contadores de paquetes de entrada y de salida de los puertos y vlans.
Entre una y otra ejecución, se muestra el resultado en tablas, comparando las diferencias de tráfico, y un reloj indicando el tiempo que falta para la próxima repetición.
1.En el caso de que la sede NO sea diversificada:
De cada consulta se obtienen dos tablas:
·La primera tabla avisa si el puerto está “Activo” o “Inactivo”:
Un puerto se considera “Activo” cuando se observa tráfico entrante (los paq. entrantes aumentan de una consulta a otra) en alguna de sus vlan’s.
En cualquier otro caso, se considera “Inactivo”.
Así, si el puerto se detectara “Inactivo” aparecería en rojo.
·La segunda tabla muestra el tráfico tanto en el puerto como en las vlan’s:
Si los contadores del puerto (paquetes de entrada y paquetes de salida) aumentan de una iteración a otra se considera que hay tráfico, y se indica con el mensaje “Hay Tráfico”.
Si algún contador, tanto el de paquetes de entrada como el de paquetes de salida no aumenta entonces es un error, y se indica con el mensaje de “No hay Tráfico” en rojo.
De la misma manera que en los puertos, en las vlans debe de haber tráfico en sus contadores de paquetes de salida y de paquetes de entrada, si no lo hay en alguno es un error y se indica con el mensaje “No hay Tráfico” en rojo.

2.En el caso de que la sede sea diversificada:
De cada consulta se obtienen tres tablas:
·La primera tabla avisa cuál de los dos puertos es el “activo” y cuál el “inactivo”.
La situación correcta es que uno de los dos se encuentre “Activo” y el otro “Inactivo”.
Si los dos estuvieran a la vez activos o inactivos, se indicaría en rojo.
·La segunda y tercera tabla, muestran el tráfico de puerto y vlan’s de cada sede (principal y secundaria).
La situación deseada es que en el puerto Activo, haya tráfico tanto en el puerto como en las vlan’s; y que en el puerto Inactivo no haya tráfico de puerto (si lo hay es por tráfico saliente de broadcast) y no haya tráfico en las vlan’s.
Si en el puerto activo no se observa tráfico en alguna vlan se indica en rojo “No hay tráfico”, indicando que es un error y señalando en rojo el contador de paquetes de entrada y/o paquetes de salida que no ha aumentado.

Prueba de ping desatendido

Este test ejecuta una serie de comandos “ping” programados. Cuando se accede a él, se pueden indicar algunos parámetros.
Los parámetros son:
–IP del router: dirección IP del router del circuito.
–Máscara de Subred: subred a la que pertenece la IP del router.
–IP auxiliar del Switch: dirección IP auxiliar de SWITCH, perteneciente a la mismasubred que la dirección IP del router, que se configura en este equipo expresamente para este test.
–Vlan: vlan del circuito sobre la que se ejecuta el ping. Es un desplegable que muestra todas las vlan que pertenecen al circuito (incluida la vlan 90).
–Número de repeticiones: con esta opción se indica el número de veces que se va a repetir el ping desatendido.
–Tiempo entre repeticiones: es el tiempo transcurrido entre cada ping que se ejecuta.
–Fecha fin ejecución: esta opción permite indicar la fecha en que finaliza el test.
Hasta la fecha de fin de ejecución el switch no para de enviar ping hacia el router.
–Tamaño del Payload: tamaño de la trama del ping.

–ICMP Ping: opción para ejecutar un ping de nivel de red ICMP.
–TCP Ping: opción para ejecutar un ping de nivel de transporte TCP. Hay que indicar el puerto TCP por el que se realiza el ping.
Una vez se han introducido los parámetros, al pulsar sobre el botón “aceptar” tiene lugar el test.
El resultado del test contiene una estadística de tiempos de los ping que se han ejecutado, tiempo mínimo, máximo y medio, la suma de todos los tiempos, y el porcentaje de paquetes perdidos.
El resultado del test es correcto cuando el número de los paquetes transmitidos es igual al número de paquetes recibidos.

Prueba de Conectividad

El test “Test de Conectividad” consiste en comprobar la conectividad de los equipos de un circuito. El test realiza la comprobación de la conectividad en dos pasos, en primer lugar el test ejecuta un ping sobre una vlan del circuito desde el Switch hacia el router y comprueba si se ha transmitido correctamente.
En segundo lugar, si el circuito está compuesto por conversores de medio, se comprueba el estado de las conexiones de los equipos que lo forman, conexión SWITCH-conversor de medios maestro, conexión conversor de medios maestro-conversor de medios esclavos y conversor de medios esclavo-router, indicando si se produce algún error de conexión.
IP del router: dirección IP del router del circuito.
–Máscara de Subred: subred a la que pertenece la IP del router.
–IP auxiliar del Switch: dirección IP auxiliar de SWITCH, perteneciente a la misma subred que la dirección IP del router, que se configura en este equipo expresamente para este test.
–Vlan: vlan del circuito sobre la que se ejecuta el ping. Es un desplegable que muestra todas las vlan que pertenecen al circuito (además de la vlan 90)
–Tamaño del Payload: tamaño de la trama del ping.
–Timeout: tiempo máximo de espera de respuesta del ping.
–ICMP Ping: opción que indica que es un ping de nivel de red (Opción por defecto).
–TCP Ping: opción que indica que es un ping de nivel de transporte sobre el protocolo TCP.
UDP Ping: opción que indica que es un ping de nivel de transporte sobre el protocolo UDP.
En el caso de que el circuito esté formado por conversores de medios Intelnet es necesario indicar un parámetro adicional:
–IP auxiliar del Conversor: dirección ip auxiliar del conversor de medios utilizada para comprobar la conectividad de estos equipos.
Esta dirección IP tiene que pertenecer al mismo rango que la ip del router.
La ventana de resultado muestra el resultado de la ejecución del ping y el estado de las conexiones de los equipos en el circuito. Si se ha producido un error de conectividad se indica en qué punto del circuito se ha producido el error.
La vista de resultado presenta variaciones en función de los distintos tipos de circuitos que existen: circuitos simples y circuitos diversificados (circuitos que poseen dos sedes, Sede Principal y Sede Secundaria).

Además existen circuitos que utilizan conversores de medios y otros que no lo utilizan.
En el caso de que el circuito no disponga de conversores de medios (el Switch está conectado directamente al router) el resultado se muestra en una vista donde solo aparecen las conexiones entre el switch y el router:
–UDP Ping: opción para ejecutar un ping de nivel de transporte UDP. Hay que indicar el puerto UDP por el que se realiza el ping.
Cuando el circuito presenta errores de conectividad, el test muestra (en el dibujo del circuito) en color rojo las conexiones que no transmiten tráfico y un mensaje que indica el motivo por el que se produce el error.
Existe dos errores que ocurren con bastante frecuencia en el test de conectividad: ‘No se envían o transmiten paquetes’ y ‘El enlace está caído’.
El error ‘No se envían o transmiten paquetes’ se debe a que por ese tramo del circuito no se transmite tráfico pero la configuración del circuito es correcta.

El error 'El enlace está caído' se produce cuando se detecta que una de las interfaces de la conexión está caída.
En la siguiente vista se presenta un caso habitual de circuito con sede diversificada en el que una sede transmite correctamente y otra sede no transmite (es una sede de respaldo).
El test detecta que no hay tráfico en una sede y marca el enlace que no funciona.
La otra sede transmite correctamente y muestra el resultado del ping.
En el caso de que el test detecte un error de enlace caído en algún punto del circuito de la sede, el mensaje de error 'Tipo de error' de la vista cambia a 'El enlace está caído'.

Prueba Consultar alarmas

Este test permite realizar una consulta de las alarmas de un circuito.
Al acceder al test, le aparecerá un dialogo que le solicitará la introducción de la fecha o rango de fechas entre las que desea consultar las alarmas.
Una vez introducida la fecha o rango de fechas, aceptar para ejecutar el test.
Las alarmas se mostrarán resaltadas en distintos colores, dependiendo de su severidad.

Prueba de Obtener datos del circuito

Este test permite obtener los datos de un circuito (vía SNMP).
Al ejecutarlo, aparecerá un esquema del circuito, que podrá variar en función del circuito sobre el que se esté realizando el test.
Para visualizar los datos de los distintos elementos del circuito, debe hacer clic sobre los mismos. Los datos, aparecerán bajo el esquema del circuito.

Prueba de Obtener datos del puerto

Este test permite obtener los datos de los puertos de acceso de un circuito.
En los resultados del test, se puede observar el estado de los puertos, al igual que el de las vlans asociadas a los puertos.
En caso de que se detecte algún error, se mostrará un aviso en color rojo, indicando la posible causa.

1.2.1. Tipos de prueba

Existen multitud de tipos de pruebas en entornos de monitorización, pudiendo identificarse fácilmente en clasificaciones más o menos genéricas.
A continuación, se va a realizar un breve resumen sobre los tipos de pruebas o también denominados tests de operación, que pueden ser invocados, por los diferentes test o herramientas disponibles en la monitorización de una infraestructura de comunicaciones.
–Consulta de la información del circuito guardada en el inventario del HPSA.
–Consulta de la configuración del circuito en los equipos de red y su comparación con la información existente en el inventario.
–Consulta de los contadores de tráfico de los puertos y VLANs asociados a un circuito.
–Chequeo de la auto-negociación de los conversores de medios (mediante el chequeo de la tabla de MACs de los puertos de acceso).
–Chequeo del tráfico descartado en la VLAN 4095 en el puerto de acceso del switch.
–Lecturas consecutivas de un comando del tipo port show XXX ejecutado cada 2 minutos, para ver el incremento de los contadores de tráfico y errores.
–Información de VLANs bloqueadas en el puerto del switch.
–Direcciones MAC conocidas por el puerto del switch.
–Consulta de la información de los conversores de medios via SNMP:
·Estado de los puertos.
·Configuración de los puertos (full duplex, negociación, etc).
·Contadores de tráfico cursado y errores.
–Realización de un bucle entre el conversor maestro y el esclavo para comprobar la conexión entre ellos.
–Realización de pings desde el switch a los conversores de medios y al router para comprobar el estado del enlace en cada uno de sus tramos. Esta prueba conlleva la modificación de la configuración del switch y de los conversores de medios (actualmente solo soportado en los conversores Telnet).

–Realización de pings desde el switch al router de cliente utilizando las pruebas desatendidas, para comprobar posibles pérdidas de paquetes.
Estos tipos de pruebas, se verán condicionados por el tipo de acceso a cada circuito.
A continuación, voy a mostrar otros tipos de pruebas remotas o también denominados test remotos, que normalmente se suministran a los operadores de telecomunicaciones.
–VLAN asociadas al puerto del cliente, rate limit configurado, velocidad de la conexión, QoS, etc.
–Información de los contadores de tráfico cursado, tráfico erróneo, etc.
–Lecturas consecutivas de un comando del tipo port show XXX ejecutado cada 2 minutos, para ver el incremento de los contadores de tráfico y errores.
–Información de VLANs bloqueadas en el puerto del switch.
–Tráfico unicast y multicast cursado en el puerto.
–Direcciones MAC conocidas por el puerto del switch.
–Información de los conversores de medios via SNMP:
·Estado de los puertos.
·Configuración de los puertos (full dúplex, negociación, etc…).
·Contadores de tráfico cursado y errores.
–Alarmas asociadas a los elementos involucrados en el circuito (esta información se recopilará del sistema de gestión de fallos):
·Alarmas actuales de los puertos del switch y de los conversores.
·Histórico de alarmas de las últimas 24 horas.

Estos tipos de pruebas de monitorización, se lleva a cabo su implementación en 3 fases diferentes:
–Interfaz Web GUI:
·Implementación de la Web GUI de acceso a la herramienta para los operadores de Telecomunicaciones
·Definición de los grupos de usuarios y permisos de ejecución de los tests existentes
·Desarrollo de la páginas de ayuda on-line sobre los posibles tests a ejecutar y los posibles resultados de la ejecución.
–Flujos de consulta inventario:
·Modificación del modelo de datos para la implementación de vistas de inventario para la búsqueda de circuitos
·Implementación de las búsquedas avanzadas sobre los circuitos existentes en el inventario
–Flujos consulta parámetros provisión circuitos:
·Implementación de los flujos para la extracción de la información de provisión de los circuitos
–Flujos consulta información switches:
·Implementación de los flujos de consulta de los contadores de tráfico
·Implementación de los flujos de lecturas consecutivas y comparación de resultados
–Interfaz servicios web:
·Definición e implementación de los web services para la invocación remota de los tests permitidos.
·Configuración del módulo SOSA para la recepción de invocaciones de tests remotas
·Realización de las pruebas de integración.
–Tests conectividad
·Implementación de los tests de conectividad (ping hacia los routers)
·Implementación de las plantillas de configuración de interfaces IP en los switches.
–Flujos consulta información switches (II):
·Implementación de flujos de consulta de información en los equipos (Direcciones MAC conocidas por el puerto del switch, VLANs bloqueadas en el puerto del switch, etc)
–Pruebas desatendidas:
·Definición de las posibles pruebas desatendidas a realizar.
·Implementación de los flujos para la invocación de las pruebas y la posterior lectura de los resultados de la ejecución.
–Interfaz Netcool:
·Definición del interfaz y del sistema de gestión de fallo.

·Implementación del interfaz de acceso a las alarmas activas de Netcool (utilizando el plugin de Netcool)
·Implementación del interfaz de acceso al histórico de alarmas de Netcool (via JDBC)
–Flujos consulta conversores medios:
Desarrollo del plugin de acceso telnet a los conversores de medios de la marca Telnet e Inelcom
Implementación de los flujos de extracción de información de los conversores (mediante SNMP y Telnet cuando sea necesario).
Implementación de los flujos de configuración de interfaces IP en los conversores de medios para poder realizar pruebas de conectividad desde el switch de acceso

1.2.2. Selección, conexión y configuración de la herramienta

La selección de este tipo de herramientas de monitorización, es la de gestionar las diferentes alarmas producidas, identificarlas y aplicarles las diferentes herramientas implementadas del sistema.
La capa Netcool es la capa superior del Sistema de Gestión. Es ésta la que proporciona el interfaz de cara al usuario. En ella se realizan diversas tareas:
–Consolidación de alarmas.
–Recolección.
–De duplicación.
–Correlación.
–Enriquecimiento.
Como se ha comentado anteriormente el sistema, y como consecuencia de su desarrollo, integra 2 subsistemas independientes (MS, IP) en uno solo.
Por esta razón, se puede dividir en 2 niveles:
–Nivel de Recolección.
–Nivel de Presentación.
El objeto de la capa de presentación es doble; por un lado consolida las alarmas de los entornos IP y MS. De este modo el operador al conectarse a este nivel -que se ha denominado Consola Única- puede tener en una misma lista de eventos, alarmas de ambos entornos.
Por otro lado esta capa de presentación atiende las peticiones de todos los operadores que
–La Gestión de routers se implementa a través de un conjunto de herramientas de HP Openview: OV Operations y Network Node Manager.
–El router es gestionado a través de 2 procedimientos complementarios:
·Interrogación periódica desde la colectora al router en cuestión. En este caso la comunicación es bilateral (primero la colectora pregunta al router, y a continuación este contesta).
Se deduce de aquí un requerimiento importante del Sistema de Gestión: “es necesario que haya conectividad permanente entre la colectora y el router gestionado”.
·Envío de traps SNMP (Simple Network Management Protocol) desde el router a la colectora ante determinado tipo de eventos.
En este caso la comunicación es unilateral (el router envía un paquete UDP a la colectora)
En la configuración de la herramienta, tenemos la parte imprescindible de la gestión de los equipos, mediante el módulo de gestión SNMP.
A continuación, se va a proceder a dar los pasos necesarios para la configuración de la herramienta de monitorización, mediante el módulo de gestión SNMP.
Al seleccionar el enlace SNMP Mgmt, obtenemos varios enlaces del módulo de gestión SNMP.
Estos enlaces nos permiten realizar diferentes acciones:

Referentes a la compilación de Mibs

–Add Mib: Permite añadir al repositorio de la aplicación de Mibs un nuevo archivo de tipo Mib.
–Compile Mib: Permite compilar una Mib del repositorio de la aplicación.
–List Mibs: Lista las Mibs que han sido compiladas y, por tanto, se pueden asociar a un Element Model para su gestión.

Referentes a la gestión de Mibs compiladas

–Mibs Favorites: Permite seleccionar aquellas propiedades de una Mib a las que el usuario quiere tener acceso rápido.

–Common Props: Esta opción sólo está disponible para el Administrador. Permite seleccionar las propiedades que serán modificadas de forma masiva en los equipos que utilizan esta mib.

–Restrict access: Esta opción sólo está disponible para el Administrador. Permite fijar el acceso o no a cada una de las propiedades de una determinada Mib por parte de los distintos roles existentes.

–Backup Props: Esta opción sólo está disponible para el Administrador. Permite guardar en un fichero las propiedades de la que se desea realizar un "backup.

Agregar una MIB

Para poder compilar una Mib, se debe añadir antes el fichero que contiene su especificación (generalmente de tipo *.mib) en el repositorio de mibs que posee la aplicación.

La acción Add Mib permite realizar esta operación.

Como puede observarse, únicamente hay que introducir la ruta del archivo que se quiere añadir (se da la opción de buscarlo con el explorador) y una pequeña descripción para su mejor identificación en el repositorio.

Una vez introducidos los datos se pulsa el botón de Enviar para añadir el fichero Mib en cuestión.

Seguidamente se muestra una pantalla que muestra si la Mib que hemos añadido ya ha sido compilada o no y si la operación se ha ejecutado correctamente.

De estar indicado la casilla de compilado, es necesario ejecutar de nuevo la compilación de la Mib.

Existen Mibs, que dependen de la información que contengan otras Mibs, en este caso se deberá añadir primero la Mibs madre, de lo contrario la pantalla mostrara un error donde especifica que hace falta información.

Compilar una MIB

Una vez añadida una Mib al repositorio, ésta debe ser compilada para que se pueda asociar a los equipos que son susceptibles de ser gestionados por Snmp.

Como puede observarse, existe la opción de escoger la o las Mibs que se deseen compilar, mediante la tecla shift + cursor; así como chequear la casilla de SelectAll y ejecutar la acción de compilado sobre todas las Mibs existentes en el repositorio.

Se puede re-compilar Mibs que ya han sido previamente compiladas. Una vez seleccionada la(s) Mib(s) se pulsa el botón de Compile para compilarla.

Esta operación solo permite compilar Mibs compatibles con Snmp V.2, todas aquellas Mibs de Snmp V.3 no están soportadas por este compilador

La compilación masiva de Mibs, es independiente del orden de dependencia de cada Mibs, lo único importante es que existan todas las Mibs madres en el repositorio o directorio del que se está compilando.

Si falla la compilación se detiene el proceso y se informa por medio de un mensaje en la parte inferior de la pantalla.

Estas Mibs son genéricas y son válidas para todo tipo de equipos.

Solo en el caso de haber compilado una única Mib, se muestra la estructura de la misma, compuesta por carpetas y ficheros que pueden ser de tipo índice, demarcados por la letra i, además de las propiedades propias de la Mib indicada.

Para compilar la siguiente Mib, no es necesario volver a la lista de las Tools, basta con seleccionarla, desde la lista desplegable de la propia herramienta.

Las Mibs que existen en el repositorio de la aplicación, así como su estado (compilada o no compilada) el campo Compiled indica si la Mib ya ha sido o no compilada.

Existen Mibs asociadas a un Element Model, que el operador puede ver de pinchar en el icono de expansión ubicado a la izquierda del nombre de la Mib, y contraer cuando así lo desee.

Se da también la opción de eliminar el fichero del repositorio con el icono.

Si se va a eliminar una Mib compilada, se deberá tener en cuenta que dicho borrado afectará a todos los árboles de gestión snmp de los equipos que tengan asociada esa Mib.

El borrado de cualquier Mib no se efectuará satisfactoriamente de existir una asociación entre la Mib y algún elemento.
También se puede modificar la descripción de la Mib

1.3. Procedimientos sistemáticos de monitorización de equipos de interconexión de redes

En este sentido, los procedimientos sistemáticos de monitorización de equipos de interconexión de redes, en la herramienta de Netcool, pueden afectar gravemente a las alarmas mostradas por pantallas, así como a los campos mostrados por las mismas.
Por lo general no será necesario crear o modificar filtros o vistas porque cada grupo ya tiene sus vistas y filtros personalizados y cualquier modificación que se haga en los mismos puede afectar gravemente a las alarmas mostradas por pantalla así como a los campos mostrados por las mismas.
Cuando se realiza un cambio en un filtro o una vista, si ese filtro o vista está asignado a la ventana de eventos de un usuario de NetCool, todos los usuarios del grupo de Operaciones que se conecta con dicho usuario tendrán la vista o el filtro modificado la próxima vez que se conecten.
Esto implica que si el cambio realizado no se ha efectuado correctamente podemos estar haciendo que un grupo entero no esté monitorizando un conjunto de alarmas que están llegando a NetCool.
En el caso, de que los filtros y vistas deban de ser modificados, a continuación se va a explicar los procedimientos sistemáticos para llevarlo a cabo, y que la operativa de monitorización de equipos, se lleve de forma eficiente.

Modificación / Creación de filtros

Los filtros se deben modificar desde la ventana de eventos de NetCool seleccionando la opción “Edit Filter” dentro del menú “Edit”.
Al seleccionar dicha opción se nos abre el filtro que tenemos configurado para nuestro usuario.
No se recomienda modificar directamente la plantilla que tiene nuestro usuario por defecto, sino guardar esta plantilla con otro nombre y realizar las modificaciones sobre esta copia.
Una vez que se compruebe el correcto funcionamiento de la nueva plantilla se puede reemplazar la anterior.
Los filtros creados por el usuario desde el editor de filtros son almacenados en el directorio del usuario unix con la extensión ‘.elf’.
Los filtros vienen representados en una estructura de árbol en la que se unen condiciones lógicas (“Condition”) mediante operaciones lógicas (“Leading Logical”).
La limitación de representación gráfica que tiene la herramienta de modificación/creación de filtros impide que de una operación lógica cuelgue más de dos elementos (puede tener 1 ó 2).
De una operación lógica pueden colgar dos condiciones lógicas o una condición y una operación lógica, dos condiciones o una única condición.
Para añadir una nueva condición a un árbol formado por dos condiciones y una operación lógica es preciso añadir una nueva operación lógica y a continuación la nueva condición.
En la parte superior izquierda del editor de filtros aparece la representación en árbol del filtro, mostrándose en la parte inferior izquierda la codificación de dicho filtro y en la parte derecha las características del elemento seleccionado (condición, operación lógica o negación).
El elemento seleccionado aparece dentro de un recuadro rojo.

Condición

Una condición se añade en el editor de filtros pulsando el botón “Condition”. En la parte derecha de la ventana se nos permite seleccionar las características de la condición. Los campos a rellenar son:
1.Condition Type: que puede tomar los valores de “Simple” o “Complex”. Indican la complejidad de la condición. Se recomienda usar el valor “Simple”.
2.Columm: Presenta un menú desplegable en el que aparecen todos los campos que contiene una alarma para que seleccionamos el campo sobre el que queremos aplicar la condición.
3.Operador: Indica la operación que se va a aplicar sobre el campo de la alarma seleccionado.
A continuación viene un campo vacío en el que se introduce el valor o la cadena con la que se va a comparar el contenido del campo de la alarma seleccionado.

Dentro de dicha cadena existe la posibilidad de emplear expresiones regulares, formadas por caracteres normales y metacaracteres.
Los metacaracteres que se pueden emplear son los siguientes:
–* : valida cero o más repeticiones del carácter o patrón de caracteres introducidos anteriormente. p.e.: 'goo*' valida las cadenas 'my godness', 'my goodness' pero no 'my gdness'.
–+ : valida una o más repeticiones del carácter o patrón de caracteres introducidos anteriormente. p.e.: 'goo+' valida las cadenas 'my goodness', my gooodness' pero no 'my godness'.
–? : valida cero o una repetición del carácter o patrón de caracteres introducidos anteriormente. p.e.: 'goo?' valida las cadenas 'my godness', 'my goodness' pero no 'my gooodness' ni 'my gdness'.
–$: valida el final de una cadena. p.e: 'end$' valida 'the end' pero no 'ending'.
–^ : valida el comienzo de una cadena. p.e: '^severity' valida la cadena 'severity 5' pero no 'the severity'.
–. : valida un único carácter. p.e: 'b.at' valida 'baat' o 'bBat' o 'b4at' pero no 'bB4at'.
–[abad] : valida cualquier carácter incluido entre los corchetes o un rango de caracteres si vienen separados por el carácter '-' (como [0-9]). p.e: ^[A-Za-z]$ valida cualquier cadena que contenga únicamente letras mayúsculas o minúsculas.
–( ) : indica que el conjunto de caracteres incluidos entre los paréntesis se tratarán como un patrón de caracteres. p.e: A(boo)+Z validará las cadenas 'AbooZ', 'AboobooZ' y 'AbooboobooZ' pero no 'AboZ' ni 'AboooZ'.
–| : valida uno de los caracteres o uno de los patrones de caracteres situados a cualquiera de los lados de la barra vertical (|). p.e: A(B|C)D valida 'ABD' y 'ACD' pero no 'AD' ni 'ABDC' ni 'ABBD' ni 'ACCD'.
–\ : La barra invertida indica que el metacaracter que viene a continuación de la barra será tratado como un carácter regular. p.e: \[[0-9]*\] validará cualquier cadena que contenga un abrir-corchete seguido de un número de dígitos o espacios seguidos por un cerrar-corchete.
Es importante destacar que si se utiliza la operación "Equal To" el campo en cuestión de la alarma debe ser exactamente igual que la cadena que se indique a continuación para cumplir la condición (con espacios y todo).
Suele ser más recomendable utilizar "Like" o "Not Like" que lo que hace es buscar en el campo de la alarma el patrón que se indique a continuación.

Operaciones Lógicas

Las operaciones lógicas pueden ser "OR" o "AND".
Una alarma pasará un filtro que esté formado por un OR con dos condiciones colgando de él cuando cumpla al menos una de las dos condiciones.
En el siguiente ejemplo en la ventana de eventos se verán todas las alarmas que vengan del equipo llamado "gesti12m" y todas las alarmas que vengan del equipo llamado "sinter":
En el caso de que el filtro tenga un AND con dos condiciones colgando para que la alarma pase el filtro debe cumplir las dos condiciones.
En el siguiente ejemplo se mostrarán por la ventana de eventos todas las alarmas cuyo origen sea un nodo cuyo nombre contenga las letras "nsg" y cuyo identificador no sea como "PRUEBAIVNC":
Para poder añadir una operación lógica a nuestro filtro, es preciso pulsar el botón "Leading Logical" o el botón "Trailing Logical' y se añade la operación.
A continuación debemos seleccionar en la parte derecha de la ventana si la operación se tratará de un OR (seleccionando la opción "logical OR") o un AND (seleccionando la opción "logical AND").
Siempre existirá la posibilidad de cambiar un OR por un AND modificando esta opción en la definición de la operación lógica.

Negación

A parte de las operaciones lógicas OR y AND existe la operación "NOT" que consiste en la negación de todas las operaciones lógicas y condiciones que cuelguen a la derecha del NOT. De un NOT puede colgar una condición o una operación lógica, pero nunca pueden colgar más de una rama del árbol.

En el filtro del siguiente ejemplo se mostrarán por la ventana de eventos aquellas alarmas que no contengan en el campo Summary de la alarma el texto “No se llega por ping” ni el texto “Recyoerado: Caída LDP”:
Un NOT se añade pulsando el botón “Negate” del editor de filtros. Es preciso que el filtro contenga una condición o una operación lógica para poder añadir un NOT.

1.3.1. Elementos a monitorizar

Los elementos a monitorizar en las herramientas de gestión y monitorización de eventos, suponen el pilar fundamental en el que se sustenta la creación y la base de los fundamentos de la creación de este tipo de herramientas.
Los elementos a monitorizar, pueden provenir de eventos del sistema (desde VPO, NMS, correlados en Omnibus), por lo que vamos a describir cada uno de los eventos que se generan, así como las alarmas provenientes de dichos elementos gestionados desde la aplicación de monitorización.

Eventos provenientes desde VPO

Alarma de caída de interfaz ethernet (SNMP Link Down Ethernet)
Alarma que nos indica la caída o recuperación de un puerto ethernet del router.
Se asocia a un problema en la parte LAN del equipo gestionado, o bien a un problema en el propio puerto.
Esta alarma proviene de router con tecnología Teldat o Bay Networks.
Alarma de caída de interfaz token ring (SNMP Link Down Token Ring)
Alarma que nos indica la caída o recuperación de un puerto Token Ring.
Se asocia a un problema en la parte LAN del equipo gestionado, o bien a un problema en el propio puerto.
Esta alarma proviene de router con tecnología Teldat o Bay Networks.
Alarma de caída de interfaz ethernet cisco (SNMP Link Down Cisco Ethernet)
Alarma que nos indica la caída o recuperación de un puerto ethernet de un router Cisco.
Se asocia a un problema en la parte LAN del equipo gestionado, o bien a un problema en el propio puerto.
Esta alarma proviene de router con tecnología Cisco.
Alarma de caída de interfaz token ring cisco (SNMP Link Down Cisco Token Ring)
Alarma que nos indica la caída o recuperación de un puerto Token Ring de un router Cisco.
Se asocia a un problema en la parte LAN del equipo gestionado, o bien a un problema en el propio puerto.
Esta alarma proviene de router con tecnología Cisco.
Alarma de pérdida de conectividad (IL_Node_Down,IL_Node_Up)
Alarma que nos indica cuando la aplicación NNM falla o vuelve a contactar al realizar el sondeo periódico sobre el router. El sondeo es cada 5 minutos.
Alarma de reinicio de router cisco (Cisco_Reload)
Alarma que indica el reinicio de un router Cisco. El evento llega a VPO antes de suceder el reinicio.
Alarma de reinicio de router (SNMP_Cold_Start)
Alarma que indica el reinicio de un router. El evento llega cuando se está reinicializando.
Alarmas de enlace sin backup (IL_linea_Down, IL_linea_Up)
Notifican la caída de un enlace FrameRelay extremo-extremo cuando no existe ningún tipo de backup asociado al enlace.
Alarmas de enlace con backup RDSI
Son varios eventos que informan de cambios de estado del enlace y del backup RDSI asociado al mismo.
Alarmas de enlace con backup CVPPLUS
Son varios eventos que informan de cambios de estado del enlace y del backup CVPPLUS asociado al mismo.
Alarmas routers de segundo nivel
Son eventos que informan sobre el estado de la conectividad entre el equipo de Primer Nivel y el de Segundo Nivel.

Eventos provenientes de NMS

Alarma de bloqueo de componente (0000 1000)
Alarma que indica el bloqueo de un componente en un Passport.
El bloqueo de un componente puede producir la pérdida de conexión de uno o varios enlaces.
Componente: EM/Passport LP/X Tarjeta/Puerto

SEV=major Ejemplos: EM/PSABL3 LP/3 E1/0
CAUSE: operationalCondition CO: The component is locked RAW: oos
Alarma de error de protocolo frame relay (7007 1000)
Alarma que se habilita cuando el número de errores del procedimiento LMI dentro de los últimos eventos, supera el límite errorEventThreshold.
Las transmisiones de datos asociadas a la conexión quedan suspendidas. Es una alarma de Passport.
Componente: EM/Passport FRUNI/XXXX Ejemplos: EM/PLLB01 FRUNI/8323 LMI
SEV=critical CAUSE: commProtocolError RAW: oos
Alarma de pérdida de trama (7011 5000)
La habilitación de la alarma significa que el enlace ha sufrido pérdida de trama durante más de dos segundos.
El borrado de la alarma se produce cuando se detecta la desaparición del estado LOF durante más de diez segundos. Es una alarma de Passport.
Componente=PASSPORT LP/X E1/Y O DS1/Y
SEV=Critical Ejemplo= EM/PMVEL4 LP/7 E1/3
TYPE: communications CAUSE: lossOfFrame RAW: istb
Alarma de indicación remota de alarma (7011 5001)
Alarma que indica la recepción desde el extremo remoto de la señal RAI (remote alarm indication).
Se indica inmediatamente a su recepción, y permanece por lo menos durante un segundo.
El borrado de la alarma se produce cuando se deja de recibir el indicador.
Es una alarma de Passport.
En este caso, el extremo remoto sufre una alarma de pérdida de trama (7011 5000)
Componente=PASSPORT LP/X DS1/Y o E1/Y
SEV=minor Ejemplo=EM/PMLLA1 LP/2 E1/0
TYPE: communications CAUSE: localTransmissionError RAW: istb
Alarma de señal de indicación de alarma (7011 5002)
Si esta alarma se habilita significa que en el enlace se ha detectado una indicación de señal de alarma durante más de dos segundos.
Cuando esta condición de alarma desaparece durante más de 10 segundos, se produce el borrado de la alarma. Es una alarma de Passport.
El extremo remoto presenta la alarma de pérdida de señal, es decir, una alarma 7011 5003.
Componente=PASSPORT LP/X DS1/Y O E1/Y
SEV=critical RAW: insv Ejemplo=EM/PMPEN4 LP/1 E1/3
TYPE: communications CAUSE: remoteTransmissionError
Alarma de pérdida de señal (7011 5003)
Alarma que indica pérdida de señal (Loss of signal, LOS) en el puerto correspondiente, durante más de dos segundos.
El borrado de la alarma se produce cuando desaparece esa condición durante más de diez segundos. Es una alarma de Passport.
Alarma de indicacion de alarma remota de multitrama (7011 5004)
Si se habilita esta alarma en un determinado puerto E1, se indica que en ese enlace de datos se ha presentado una condición de indicación de alarma remota de multitrama durante un tiempo mayor que dos segundos.
La interfaz del extremo remoto ha perdido el alineamiento de multitrama.
El borrado de esta alarma se producirá cuando desaparezca la condición de alarma durante más de diez segundos. Es una alarma de Passport.
Alarma “multiframe red” (7011 5005)
La aparición de esta alarma en un puerto E1 indica la presencia del estado Multiframe red para ese enlace de datos durante más de dos segundos.
La alarma desaparece con la desaparición de esta condición durante más de diez segundos. Es una alarma de Passport.
Alarmas de servicio en DPN

Alarma que debe indicar la caída o recuperación de un circuito asociada a un problema detectado mediante el sistema de gestión NMS en un nodo del tipo DPN
Eventos correlados en Omnibus
Los eventos correlados en Omnibus y mostrados a los administradores del servicio Interlan atienden a una serie de objetos finales que están especificados a continuación:
–Interfaz LAN
–Conectividad de router de Primer Nivel.
–Conectividad de router de Segundo Nivel.
–Enlace extremo-extremo sin backup.
–Enlace extremo-extremo con backup RDSI o CVPPLUS.

Interfaz LAN

Este evento final solo se correla entre eventos originados por los routers, por lo tanto, provienen de VPO.
Este evento final refleja el estado actual de los interfaces LAN de los routers.
Conectividad de router de Primer Nivel
El evento final de Conectividad de un router es el resultado de la correlación de varios eventos. Por una parte los eventos provenientes en VPO:
–Alarma de Pérdida de Conectividad.
–Alarma de Reinicio de Router Cisco.
–Alarma de Reinicio de router.
Y por otro lado, las alarmas de red:
–Todas las alarmas provenientes de NMS.
Básicamente la correlación realizada, permite dejar reflejado cual es el problema en todo momento:
–Si se ha producido un Reinicio de Router Cisco, este marcará el texto final del evento, eliminando todas las demás alarmas posteriores.
–Si se produce una Alarma de Reinicio de router, marcará el texto final del evento para indicar que el problema fue un reseteo.
–Si se produce una Alarma de Pérdida de Conectividad, solo marca el texto del evento final en caso de que no exista ninguna otra alarma.
–Si se producen Alarmas desde NMS, solo marca el texto del evento final en caso de que no exista ninguna otra alarma.
Conectividad de router de Segundo Nivel
Al igual que el evento de Conectividad de router de Primer Nivel, para los routers de Segundo Nivel, el evento que los Administradores del servicio verán, se basa en los eventos provenientes de VPO, concretamente los expuestos en el punto.
Enlace extremo-extremo sin backup
Los eventos finales son producto de la correlación entre los eventos de VPO:
–Alarma de Pérdida de Conectividad.
–Alarma de Reinicio de Router Cisco.
–Alarma de Reinicio de routers.
–Alarma de Enlace sin backup.
Y por otro lado, las alarmas de red:
–Todas las alarmas provenientes de NMS.
Básicamente la correlación realizada, permite dejar reflejado cual es el problema en todo momento:
–Si se ha producido un Reinicio de Router Cisco, este marcará el texto final del evento, eliminando todas las demás alarmas posteriores.
–Si se produce una Alarma de Reinicio de router, marcará el texto final del evento para indicar que el problema fue un reseteo.
–Si se produce una Alarma de Enlace sin backup, se visualiza el evento, siempre que no haya un Reinicio de router Cisco.
–Si se produce una Alarma de Pérdida de Conectividad, solo marca el texto del evento final en caso de que no exista ninguna otra alarma.

–Si se producen Alarmas desde NMS, solo marca el texto del evento final en caso de que no exista ninguna otra alarma.

Enlace extremo-extremo con backup
Los eventos finales son producto de la correlación entre los eventos de VPO:
–Alarma de Pérdida de Conectividad.
–Alarma de Reinicio de Router Cisco.
–Alarma de Reinicio de routers.
–Alarma de Enlace con backup RDSI o CVPLUS.
Y por otro lado, las alarmas de red:
–Todas las alarmas provenientes de NMS.
La diferencia con el evento anterior, es que este evento no desaparece del browser de eventos, aunque vengan eventos que especifiquen la causa, ya que no solo aportan información acerca del enlace sino también del backup.

1.3.2. Herramientas a utilizar

Herramientas de la consola NETCOOL

En el menú Tools de la consola de Netcool, aparecen diferentes herramientas algunas de ellas útiles para el tratamiento de las incidencias, y otras para actualizar o corregir posibles errores en la Base de Datos que tiene el Sistema de Gestión de Interlan con los datos de todos los routers que actualmente están en gestión.
Las primeras herramientas que aparecen en el menú son el ping y el telnet, en ambas te pide como valor la IP de gestión, o el nemónico.

Históricos

Te pide como valor el nemónico del router (Name of the host), y dibuja una gráfica que representa el valor que se seleccione de la lista Tipo de histórico:
–CpuUsage: Representa el uso de CPU.
–MemoryUsage: Representa el uso de memoria
–LanCollisions: Representa las colisiones LAN
–FencBenc: Representa el Fenc y el Benc
–FrameRelayErrors: Representa los errores en la FR
–BWinPVC: Tráfico de entrada por PVC
–BWoutPVC: Tráfico de salida por PVC

Net Config

Te pide como valor el nemónico del router (Name of the host), y según la opción seleccionada en la lista VpoInterlanNetConfig te indica lo siguiente:
–Addresses: Muestra la colectora en la que está dado de alta el equipo, así como los interfaces que tiene el equipo y las direcciones IP, máscara de red y dirección de red, de cada uno.
–Routing Table: Muestra la tabla de rutas del equipo (Destination, Gateway, Type, Mask, Interface)
–ArpCache: Muestra la tabla de arp del router.
–SystemInfo: NO ESTA OPERATIVA.

Net Diag

Te pide como valor el nemónico del router (Name of the host).
Dentro de esta opción esta la tool Rping, en la que el equipo necesita un agente snmp que soporte el ping remoto.

Telnet genérico

Realiza un telnet al equipo, pero el valor que puedes indicar para realizar la conexión pueden ser IP, NRI o NEMÓNICO

Consulta routers – Prueba

No necesita ningún dato, te muestra una lista con los routers que hay dados de alta en BBDD. (Tarda bastante en salir la lista completa).

Devices.sh

Te pide como valor la IP del router, y te muestra una lista de los interfaces que tiene el equipo. (Hay que poner la dirección IP, con nemónico no funciona).

Herramientas NMS

nri.don
Te pide como valor el NRI. En el caso de Passport, te muestra el módulo y el Fruni correspondientes al NRI indicado, y en el caso de DPN, te muestra el módulo y el PI y PO correspondientes al NRI indicado.

nricv
Te pide como valor el NRI. En el caso de passport, te indica el modulo, Fruni y CID del NRI introducido, así como una tabla con los dlci´s que tiene el circuito y los NRI enfrentados. Y el caso de DPN, te indica velocidad del cto, el modulo, el PI, PO, CID...

cid
Te pide como valor el CID, y te indica el cliente al que pertenece dicho CID.

lmi
Te pide como valor el Passport y el FRUNI, ó el DPN y el PI/PO. Te muestra el estado del lmi.

pref.mac
Te pide como valor el NRI, módulo DPN PI/PO o modulo PP FRUNI.
Te muestra el modulo, la velocidad de la línea y estado del lmi, y según la opción que se indique te realiza las siguientes pruebas:
–Con la opción -p analiza el cto. y realiza las siguientes pruebas:
·En el caso de DPN:
›Sin nivel 2 pero con ctos.: Lanza B2R
›Sin nivel 2 y sin ctos.: Lanza B3
·En caso de PP:
›En caso de FR no realiza bucles por poder tener BIR
›En caso de LMI caído: lanza un ppdelta 10,2 al framer para ver si hay tráfico.

asignafr.don
Te pide como valor el Passport y el FRUNI, o el DPN y el PI/PO, y te indica la asignación FR del puerto.

nri.red
Te pide como valor el NRI. Esta macro es para localizar y mostrar la red con origen en un NRI.
Se muestran datos del destino de cada DLCI (puerto, CID, nombre cliente).
–En FR de Passport indica:
·La velocidad de la línea (V35 y HSSI)
·Los time-slots y el ancho de banda (E1 canalizada)
–En FR de DPN indica:
·La velocidad de la línea
–En el resto de DPN indica:
La velocidad de la línea en el nuevo formato de FR

Bucles
Te pide como valor el NRI, o el modulo y el FRUNI o ATMIF, y sirve para realizar bucles en Passport, según las opciones que se indiquen (externalloop, manual, card):

–externalloop: realiza un bucle externo
–manual: realiza un bucle manual o b2l
–card: realiza bucle a la placa
·d: se visualiza el bucle
·stop: se para el bucle

chkADSL
Te pide como valor el NRI y el DLCI del extremo correspondiente al router Central, y se muestra el estado de los distintos tramos que hay entre el NRI del router Central y el último tramo de la Pasarela ATM-FR.

Todo.jul
Te pide como valor el NRI y nos devuelve el estado de la línea y si tiene o no respaldo

Ppdelta
Te pide como valor el módulo DPN PI o modulo PP FRUNI y el dlci conde queremos hacer las tomas, también se pueden modificar el número de tomas que queremos hacer y cada cuanto tiempo.

Nos mostrará el tráfico que tiene el dlci en esas tomas.

Consulta a BBDD

Datos Router
Te pide como valor el NRI, IP o nemónico según lo que se seleccione en la lista Conectar como.
Te indica los datos que existen en BBDD para ese equipo. (País, provincia, población, calle, contacto, teléfono, nombre, cliente_id, customer_id).
Situación router
AL igual que Datos router, te pide como valor el NRI, IP o nemónico según lo que se seleccione en la lista Conectar como. Te da datos del equipo (IP, Nemónico, colectora asignada, NRI, si esta dado de alta en BBDD, si esta dado de alta en VPO).
Consulta Backup RDSI
Muestra los nemónicos de los routers, origen y destino, de un enlace Frame Relay extremo-extremo, así como el nemónico del router que acepta la llamada de backup RDSI junto con los números RDSI del llamante y del llamado. (Origen, RDSI_OR, RDSI_DEST, Remoto, Receptor).
Además de sacar información por pantalla, lo guarda en el fichero /tmp/USUARIO.CBD
Consulta de Backup RDSI Completa
Te muestra lo mismo que el anterior, y además, muestra los DLCIs y los NRIs en los extremos origen y remoto y el NRI que hace de backup CVPPLUS al extremo remoto cuando existe esta posibilidad. (NRI_OR, DLCI_OR, NRI_DEST, DLCI_DEST, CVPPLUS).
Consulta de Backup CvpPlus
Muestra, únicamente, los nemónicos de los routers, origen y destino, de un enlace Frame Relay extremo-extremo que poseen CVPPLUS.
También muestra los DLCIs y los NRIs en los extremos origen y remoto y el NRI que hace de backup CVPPLUS al extremo remoto. (Origen, NRI_OR, DLCI_OR, NRI_DEST, DLCI_DEST, destino, CVPPLUS).
HP Openview
–La Gestión de routers se implementa a través de un conjunto de herramientas de HP Openview: OV Operations y Network Node Manager.
El router es gestionado a través de 2 procedimientos complementarios:
·Interrogación periódica desde la colectora al router en cuestión.
En este caso la comunicación es bilateral (primero la colectora pregunta al router, y a continuación este contesta).
Se deduce de aquí un requerimiento importante del Sistema de Gestión: “es necesario que haya conectividad permanente entre la colectora y el router gestionado”.

·Envío de traps SNMP (Simple Network Management Protocol) desde el router a la colectora ante determinado tipo de eventos. En este caso la comunicación es unilateral (el router envía un paquete UDP a la colectora)

MDM
–Dentro del Sistema de Gestión hay integradas 2 máquinas: mdmgestion y mdmgestion2 (una backup de la otra) cuya función es recibir las alarmas de los Passport y DPN de acceso.
–En estas máquinas se ha instalado un software propietario de Nortel. De todas ellas nos centraremos en la parte de Gestión de Fallos.
–La gestión de fallos de los puertos de los Passports a los que se conectan los routers (Equipos en Domicilio de Cliente) se realiza a través del servicio gmdr de la máquina que es quién consolida todas las alarmas recibidas.

ORACLE

–Un elemento esencial en la plataforma de Supervisión es la Base de Datos Oracle.
–Dada la importancia de este elemento se ha dotado de Redundancia a varios niveles.: A nivel físico y a nivel lógico.
–Esta Base de Datos realiza diversas funciones:
·Histórico de eventos de netcool .Estos eventos son volcados desde la Consola Única a través de un gateway que se ejecuta en el cluster de base de datos. Se almacena en la base de datos REPORTER.
·Repositorio de todas las mediciones de CPU y memoria que se realizan desde NNM y que son volcadas de forma periódica a la Base de Datos. Se almacena en la base de datos NNM.
·Inventario de los equipos de gestión. Es lo que se denomina BDSG (Base de Datos del Sistema de Gestión). Se almacena en la base de datos REPORTER.

El contenido de BDSG es el elemento de la Base de Datos ya que si se pierde la gestión de los routers pues no habría:
–Enriquecimiento de alarmas.
–Personalización de alarmas por grupo de gestión.

Perfomance viewer y data viewer

Estas son herramientas del software MDM (Multiservice Data Manager), que se realizan para realizar monitorizaciones gráficas de la Red Multiservicio.
El Data Viewer, solo se podrá encontrar en las últimas versiones de MDM, ya que es la aplicación más moderna de las 2.
Performance Viewer, a pesar de ser más antiguo, sigue siendo muy usado en el ámbito de los centros de soporte remoto, y en las últimas versiones de MDM se ha recuperado o se ha añadido al Data Viewer.

1.3.3. Pasos a seguir

Los pasos a seguir en los procesos sistemáticos de monitorización de equipos de interconexión de datos, pasan por una construcción de filtros y vistas.
En función de estos filtros y vistas construidos y aplicados, se irá recibiendo las líneas de eventos que nos interesen a partir de los campos de las alarmas que vayan sucediendo.
Por lo tanto, los pasos a seguir en el proceso de sistematización en la monitorización de equipos de interconexión de redes, tenemos por un lado al constructor de filtros y las vistas de los mismos.

Filter builder

Qué es el constructor de filtros
El constructor de filtros es una herramienta que permite al operador crear peticiones gráficas complejas sobre el estado de los objetos gestionados, de modo que se muestre en un event list únicamente un subconjunto de las alertas almacenadas en el sistema, definido por la selección implementada en el filtro.

Cómo iniciar el constructor de filtros

El constructor de filtros se puede iniciar de cuatro formas distintas:
–Desde la lista de eventos pulsando sobre el botón “Edit” del filtro seleccionado.
–Desde la ventana de cajas de monitorización, pulsando sobre el botón en el que aparece el nombre del filtro.
–Desde un fichero de filtro ya guardado (*.elf), haciendo doble click sobre él.
–Desde el conductor, pulsando sobre el botón “Filter Builder”.

Ejemplo de construcción de filtros

Lo primero que necesitamos saber es que tipo de alarmas queremos filtrar.
Por ejemplo vamos a crear un filtro que nos muestre las alarmas recibidas con código de equipo.
Esto es necesario para evitar alarmas de Passport sobre equipos no gestionados, bajas, errores en Base de datos, imaginad que se da de alta una línea nueva en un centro del que no tenemos gestión o no sabemos que existe, el Passport detectaría que no hay conectividad, y daría el circuito como caído, en el campo Node nos aparecería el Passport que lo ha detectado (por ejemplo PALGE1), esto es demasiado genérico, hay demasiadas líneas que dependen de PALGE1, es posible que en el campo node alias aparezca el nri que tiene el problema, pero si no lo hace no tendremos suficientes datos para tratar la avería, esto no quiere decir que debamos ignorar las alarmas de este tipo, pero nos permitirá distinguir las alarmas que tenemos en gestión de las que no.
–Abrimos el constructor de filtros.
–Damos un nombre al filtro, en este caso no nulos.
–Pulsamos el botón Condition.
–A la derecha tenemos varias expresiones, marcamos en expresión type complex (simple filtra partes del texto, por ejemplo todos los que empiecen por una cadena, complex identifica el nombre entero).
–En el menú de colums seleccionamos Passport (filtarr campo Passport)
–En las condiciones not equal a Node.
–Guardamos el filtro en .omnibus con extensión .elf
–Vamos a la ventana del constructor y grabamos también.
La próxima vez que arranquemos el constructor tenderemos la opción de este filtro, también podemos usarlo ahora, pero si no lo grabamos desaparecerá al salir.
Este filtro comprueba que todas las alarmas que se muestran tengan código de equipo.

View builder

Qué es el constructor de vistas
Es la herramienta que utiliza Omnibus para definir el formato de presentación de la información: es decir, los campos de una alarma y en qué orden se muestran estos al operador.
Cómo iniciar el constructor de vistas
El constructor de vistas se puede iniciar de tres formas distintas:
–Desde la lista de eventos pulsando sobre el botón “Edit” de la vista seleccionada.
–Desde el conductor, pulsando sobre el botón “Constructor de vistas”.
–Desde un fichero de vistas ya existente (*.elv), haciendo doble click sobre él.
Ejemplo de construcción de vistas
Una vez definidos los filtros (que queremos que nos muestre) debemos seleccionar las vistas (como queremos que nos lo muestre).
Por defecto nos muestra los siguientes campos (vista por defecto).
Node: Equipo que detecta la alarma
Alert Key: Código de alarma
Summary: Descripción de la Alarma.
Last Ocurrente: Hora a la que ocurrió el último evento (caída, recuperación).
Count: Numero de eventos recibidos de esa alarma.

1.3.4. Resultados del proceso

Los resultados de los diferentes procedimientos sistemáticos de monitorización, se formalizan en forma de eventos o alarmas, que son generadas a causa de un suceso o sucesos en la operativa de los elementos gestionados.

1.3.5. Listas de comprobación

Para la construcción de indicadores válidos y fiables que generen eventos de alarma de los elementos gestionados, debemos de asegurarnos de su validez y fiabilidad.
La existencia de propuestas en este sentido, genera unos esquemas de procedimientos sistemáticos de monitorización, como pueden ser por ejemplo resumibles en 7 puntos, que se deberían de considerar a modo de comprobación o de lista de comprobación.
Existen otras propuestas compuestas de 4 pasos, más recientes, donde se especifica una serie de procesos a seguir para la construcción de buenos indicadores que generen a modo de comprobación o de lista de comprobación una buena manera de medir los procedimientos sistemáticos de monitorización.
Para la elaboración de indicadores válidos y fiables, que conformen unas buenas listas de comprobación de procesos sistemáticos de monitorización, los siguientes procesos:
1.Selección de indicadores potenciales:
·Valorar la evidencia que justifica la importancia del indicador.
·Valorar la capacidad de medir y la frecuencia del indicador, frente a problemas que son identificados por el indicador.
·Valorar y clasificar los elementos modificables que identifica el indicador en relación a los casos problemáticos que han sido detectados.
2.Diseño y establecimiento de estándares y herramientas eficaces de medición.
3.Establecimiento de pruebas de fiabilidad en casos o controles por parte de los indicadores, en relación a la sensibilidad, especificidad y predicción de los indicadores en referencia a los casos problemáticos.
4.Simulación en entorno donde se valore la aplicabilidad y utilidad de los indicadores diseñados.
Los elementos gestionables, supervisados por una serie de indicadores, los cuales han conformado una serie de listas de comprobación, tendrían su representación de la monitorización, en el concepto de pirámide de control, donde la relación de los servicios y procesos, se sustentarían en un plan de delegaciones, cuya base serían los controles automatizados, y como proceso de comprobación, las listas de comprobación, previamente elaboradas.

2. Procedimientos de diagnóstico averías en dispositivos de interconex. de redes

2.1. Tipos de incidencias en la interconexión de redes públicas y privadas

Incidencia	Descripción
Faltan datos para configuración equipo	Faltan los datos para configurar los equipos, no se han pasado por correo ni están en la base de datos.
Tramitación incompleta	La información existente es errónea porque los datos no son correctos para realizar la provisión del servicio.
Pte de anular	Hay que anular el pedido porque el cliente ya no lo quiere.
Pte de anular y retramitar	Hay que anular el pedido porque alguno de los datos no son los correctos y no se puede solucionar sobre el mismo pedido por lo que hay que retramitar otro con los datos correctos.
Pte soporte a comercial	Durante la provisión surgen problemas que implican conceptos facturables y para seguir adelante es necesario que el comercial comente al cliente estos problemas y se tome una decisión de si se sigue con la provisión (aportando el comercial la información necesaria para ello) o se toma una solución alternativa.
Avería de línea	La línea está instalada y no se ha conseguido que funcione después de que routers y el técnico que está realizando la instalación han estado en contacto con el grupo de Gestión de Circuitos de Acceso.
Elemento de red	Se utilizará para indicar problemas en nodos de red.
Incidencia en multienlace	Se utilizará para indicar problemas en los elementos que controla el grupo de Supervisión de Circuitos.
Pte soporte a coordinación	Es necesario que coordinación aclare algún dato del pedido.
Retenida cliente	Cliente retiene la instalación por alguna causa (obras, no lo quiere todavía, etc.) y no tiene fecha prevista de cuando se puede realizar el trabajo.
Demanda aplazada	Cliente retiene la instalación por alguna causa (obras, no lo quiere todavía, etc.) y tiene fecha prevista de cuando se puede realizar el trabajo o hay un plan de fechas acordado con el cliente para realizar las instalaciones. Cambios de domicilio, traslados exteriores y traslados interiores con y sin fecha acordada. Altas de Backup de Acceso y cambios de velocidad con fecha acordada.
Incidencia de aplicación	Por problemas de base de datos.
Pte backup extremo a extremo	Sólo se debe utilizar en las modificaciones en las que se dé de alta el Backup Extremo a Extremo, la RDSI la hemos pedido nosotros, no está instalada la línea de Backup de la fase implicada no la del remoto y se ha estado en contacto con el grupo de Gestión de Circuitos de Acceso.
Pte de stock	Falta el material que está tramitado para poder realizar la instalación.
Pte proyecto	Falta proyecto técnico por parte de Soporte a Ventas de la dirección Comercial.
Pte soporte ingeniería	Abierto soporte a Ingeniería de Servicios de la dirección de Marketing.
Pte de circuito	Se va a realizar la instalación del router y se confirma entre routers, el técnico desplazado que está realizando la instalación, el cliente y el grupo de Gestión de Circuitos de Acceso que no se encuentra la línea (UTR/TR1) en el lugar dónde se debe instalar el router. Altas de Backup de Acceso y cambios de velocidad en los que después de haber hablado con el grupo de Pruebas de Aceptación se ha indicado que no hay fecha acordada.
Pendiente de generar	YA NO SE DEBE UTILIZAR, todos los problemas de generación se deben enviar a Control de Configuración (CC) para que se resuelvan en el mismo día. Sólo en el caso de que CC indique que en ese día no se puede hacer la generación se pondrá en incidencia.
Pte de host	YA NO SE DEBE UTILIZAR, cuando se haya instalado y configurado el router, aunque el otro extremo de la comunicación no esté instalado.
Cortes coordinados	YA NO SE DEBE UTILIZAR, se debe usar DEMANDA APLAZADA o PTE de CIRCUITO (según corresponda).
En obra	YA NO SE DEBE UTILIZAR, se debe usar RETENIDA POR CLIENTE o DEMANDA APLAZADA (según corresponda).

2.1.1. Clasificaciones

En esta clasificación, generalmente se establece el tipo de incidencia, con una clasificación multinivel, con varias dependencias entre niveles, todo está correlacionado.

El número total de niveles, dependerá en gran medida de la diversidad en la tipificación de las incidencias, que necesitemos clasificar, según nuestros criterios para su correcta gestión y resolución.

Existe una multitud de ocasiones, donde al producirse una incidencia, no se establece adecuadamente su clasificación, en el momento de registrarla, por lo que si esto sucede, en el momento del cierre de la misma, es necesario su correcta clasificación.

Como hemos indicado en un párrafo más arriba, la clasificación multinivel con dependencias entre niveles, según el granulado de la tipificación de las incidencias que hagamos, podemos clasificarlas en los siguientes tipos de incidencias, con correlación entre sí.

Alarma de caída de interfaz ethernet (SNMP Link Down Ethernet)
Alarma que nos indica la caída o recuperación de un puerto ethernet del router. Se asocia a un problema en la parte LAN del equipo gestionado, o bien a un problema en el propio puerto.
Esta alarma proviene de un router con tecnología Teldat o Bay Networks.

Alarma de caída de interfaz token ring (SNMP Link Down Token Ring)
Alarma que nos indica la caída o recuperación de un puerto Token Ring. Se asocia a un problema en la parte LAN del equipo gestionado, o bien a un problema en el propio puerto.
Esta alarma proviene de router con tecnología Teldat o Bay Networks.

Alarma de caída de interfaz ethernet cisco (SNMP Link Down Cisco Ethernet)
Alarma que nos indica la caída o recuperación de un puerto ethernet de un router Cisco. Se asocia a un problema en la parte LAN del equipo gestionado, o bien a un problema en el propio puerto.
Esta alarma proviene de router con tecnología Cisco.
Alarma de caída de interfaz token ring cisco (SNMP Link Down Cisco Token Ring)

Alarma que nos indica la caída o recuperación de un puerto Token Ring de un router Cisco. Se asocia a un problema en la parte LAN del equipo gestionado, o bien a un problema en el propio puerto.
Esta alarma proviene de router con tecnología Cisco.

Alarma de pérdida de conectividad (IL_Node_Down, IL_Node_Up)

Alarma que nos indica cuando la aplicación NNM falla o vuelve a contactar al realizar el sondeo periódico sobre el router.
El sondeo es cada 5 minutos.

Alarma de reinicio de router cisco (Cisco_Reload)

Alarma que indica el reinicio de un router Cisco.

Alarma de reinicio de router (SNMP_Cold_Start)

Alarma que indica el reinicio de un router.
El evento llega cuando se está reinicializando.

Alarmas de enlace sin backup (IL_linea_Down, IL_linea_Up)

Notifican la caída de un enlace FrameRelay extremo-extremo cuando no existe ningún tipo de backup asociado al enlace.

Alarmas de enlace con backup

Son varios eventos que informan de cambios de estado del enlace y del backup asociado al mismo.

Alarmas routers de segundo nivel
Son eventos que informan sobre el estado de la conectividad entre el equipo de Primer Nivel y el de Segundo Nivel.

Dentro de la funcionalidad de generación de eventos en un sistema de gestión de incidencias, tenemos eventos correlados, que atienden a una serie de objetos finales dentro de las redes telemáticas, que están especificados a continuación, para completar el proceso de detección y generación de alarmas.
–Interfaz LAN.
–Conectividad de router de Primer Nivel.
–Conectividad de router de Segundo Nivel.
–Enlace extremo-extremo sin backup.
–Enlace extremo-extremo con backup.

Interfaz LAN

Este evento final solo se correla entre eventos originados por los routers.
Son los eventos descritos en alarma de caída de interfaz ethernet (snmp Link Down Ethernet), alarma de caída de interfaz token ring (snmp link down token ring), alarma de caída de interfaz ethernet cisco (snmp link down cisco ethernet) y alarma de caída de interfaz token ring cisco (snmp link down cisco token ring)
Este evento final refleja el estado actual de los interfaces LAN de los routers.

Conectividad de router de Primer Nivel

El evento final de Conectividad de un router es el resultado de la correlación de varios eventos:
–Alarma de Pérdida de Conectividad
(Alarma de pérdida de conectividad (il_node_down,il_node_up))
–Alarma de Reinicio de Router Cisco
(Alarma de reinicio de router cisco (cisco_reload))
–Alarma de Reinicio de routers.
(Alarma de reinicio de router (snmp_cold_start))

Conectividad de router de Segundo Nivel

Al igual que el evento de Conectividad de router de Primer Nivel, para los routers de Segundo Nivel, el evento que los Administradores del servicio verán, se basa en los eventos provenientes de VPO (El equipo que centraliza todas las alarmas generadas por NMS y son filtradas , concretamente las alarmas de routers de segundo nivel.
–Enlace extremo-extremo sin backup.
Los eventos finales son producto de la correlación entre los eventos de VPO:
–Alarma de Pérdida de Conectividad.
(Alarma de pérdida de conectividad (il_node_down,il_node_up))
–Alarma de Reinicio de Router Cisco.
(Alarma de reinicio de router cisco (cisco_reload))
–Alarma de Reinicio de routers.
(Alarma de reinicio de router (snmp_cold_start))
–Alarma de Enlace sin backup.

(Alarmas de enlace sin backup (il_linea_down, il_linea_up))
–Y por otro lado, las alarmas de red:
Todas las alarmas provenientes de NMS.

Básicamente la correlación realizada, permite dejar reflejado cual es el problema en todo momento:

–Si se ha producido un Reinicio de Router Cisco, este marcará el texto final del evento, eliminando todas las demás alarmas posteriores.
–Si se produce una Alarma de Reinicio de router, marcará el texto final del evento para indicar que el problema fue un reseteo.
–Si se produce una Alarma de Enlace sin backup, se visualiza el evento, siempre que no haya un Reinicio de router Cisco.
–Si se produce una Alarma de Pérdida de Conectividad, solo marca el texto del evento final en caso de que no exista ninguna otra alarma.
–Si se producen Alarmas desde NMS, solo marca el texto del evento final en caso de que no exista ninguna otra alarma.

2.1.2. Ejemplos

A continuación, vamos a mostrar un proceso de apertura de boletín Sirio, para el tratamiento y gestión de una incidencia, de la naturaleza que sea. Comentar que este ejemplo no muestra ningún dato o caso real, por motivos de clasificación de datos sensibles, bajo la protección de la LOPD.

Por lo tanto, se va a explicitar una plantilla de cómo proceder para la apertura de la plantilla para la apertura de un boletín Sirio, mediante la herramienta de gestión de incidencias Vantive.

En la barra de herramientas tenemos un botón “Crear Boletín Sirio”, (el cuarto empezando por la derecha) solamente pulsando encima de él te crea el boletín.

Automáticamente nos aparecerá una pantalla con todas estas pestañas:
–Boletín.
–Datos de Cliente.
–Otros Datos.
–Franqueo.
–Informaciones.
–Paradas.
–Prefranqueos.
–Conformidad / disconformidad Cliente.
–Envíos/ Cesiones/ Devoluciones.
–Mensajes.

Boletín SIRIO

Datos más relevantes relativos a un boletín SIRIO:
–Estado Apertura: Estado en el que se encuentra el boletín con respecto a SIRIO. Puede tomar los valores ‘Solicitado’, ‘Aceptado’ o ‘Rechazado’.
–Modo Apertura: Modo en que se ha realizado la apertura del boletín. ‘Manual’, tras pulsar el Botón ‘Modo Manual’, el usuario introduce el Nº de serie SIRIO manualmente. ‘Automático en otro caso.
–Nº Serie SIRIO: Número de serie dado por SIRIO al boletín.
–Origen: Origen del boletín.
–Nº que Reclama: Contiene el número administrativo del objeto reclamante, o bien un número de RDSI
–NRI: Número de Red Iberpac del circuito

–Servicio: Código y descripción del servicio del boletín, que será distinto dependiendo del Tipo de servicio.
· FR: IBERPAC FRAME RELAY o CIRCUITOS DIGITALES PUNTO A PUNTO.
· X25: IBERPAC X.25
·ADSL: GIGAADSL

Normalmente este campo aparecerá cumplimentado, de no ser así deberemos cumplimentarlo nosotros.
–Fecha Registro: Fecha de registro del boletín.
–Manifestación: Código y descripción del síntoma de la avería. Será el diagnóstico (que también dependerá del Servicio), lo que le ocurre al circuito: cortes, avería total del servicio, MODEM no sincroniza, etc.
–Estado: Estado en el que se encuentra el boletín. Se visualiza el estado que maneja SIRIO así como su descripción simplificada, que puede ser 'Arrancado', 'Parado', 'Prefranqueado', 'Franqueado' y 'Confirmado'.
–Ir al expediente: Botón para abrir el expediente al que está asociado el boletín.
–Nº Reiteraciones: Número de veces que el cliente ha reiterado la resolución de un boletín sin que éste estuviera franqueado.
–Observaciones: Texto libre para introducir cualquier observación. Pruebas de los equipos, no cursa b2l, b3...luces de la utr, etc.

Datos de Cliente

En esta pantalla se recogen de forma detallada aquellos datos relacionados con el cliente que pueden ser de utilidad durante la tramitación del boletín.

Los DATOS CLIENTE detallan la localización física de la sede del cliente que suscita la Incidencia.

Estos datos se rellenaran automáticamente por la aplicación.

Después de rellenar todos los campos que sean obligatorios y grabar todos los datos, se enviará el boletín pulsando el botón "Solicitud de Apertura"

Otros Datos

En esta pantalla se muestran datos relacionados con el boletín que tienen una importancia menor en el desarrollo del boletín.

Sí es importante la sección de puntos de control, ya que el desarrollo de un boletín depende, en la mayoría de ocasiones, del centro que posee el control del mismo.
–Control: Código y descripción del terminal que tiene actualmente el control del boletín
–Remoto Receptor: Primer centro por el que pasó el boletín
·Si en el control aparece: DT. La avería no se ha enviado a ningún sitio, la seguimos teniendo nosotros.
·Si en control aparece: 9200-Operaciones IU. La avería ha llegado al Centro de soporte correspondiente.
·Si en control aparece: GRI. Desde el Centro de soporte han pasado la avería al departamento correspondiente, transmisión, unidades móviles.

Estos datos se rellenaran automáticamente por la aplicación.

Franqueo

En esta pantalla se muestran los datos referentes al franqueo de un boletín.
–Causa: Causa de la Avería.
–Localización: Localización de la Avería.
–Área Resp.: Área de responsabilidad causante de la avería.
–Descripción: Pequeña descripción del franqueo.

Estos datos serán rellenados por los técnicos al solucionar la avería.

Informaciones

En esta pantalla se muestran la Informaciones que han sido dadas de alta a lo largo del ciclo de vida de un boletín.
Nosotros podremos mandar una información cuando creamos que sea necesario, ya sea porque el circuito este caído, porque continúen los cortes, porque recupera la línea, etc.

Ejemplo:

El circuito esta incomunicado desde hace bastante tiempo y reiteramos la avería (botón de la barra de herramientas Reiteración de Boletín), nosotros podemos enviar una información.

New---Description: donde solicitamos información de la avería, informando de la reiteración del boletín porque es urgente, etc.

Visitas

Cuando se abra un boletín para un circuito ADSL deberemos crear una 'visita con diagnóstico'.
Pulsaremos en New y grabaremos. Automáticamente aparecerá una X en el cuadrado de Solicitud.

Cuando se franquee la avería deberemos rellenar la pestaña 'Código de:'. Para ello desplegaremos la lista y elegiremos la que más se adecue a la resolución de la incidencia.

Paradas

Esta pantalla muestra una relación de las paradas y arranques que se han producido a lo largo del ciclo de vida de un boletín.

Conformidad/ Disconformidad Cliente

En esta pantalla se muestran las conformidades o disconformidades de un cliente, en relación a la resolución de una avería
–Estado Serie: Estado en el que se encuentra el boletín. Se visualiza el estado que maneja SIRIO así como su descripción simplificada, que puede ser 'Arrancado', 'Parado', 'Prefranqueado', 'Franqueado' y 'Confirmado'.
Si la avería ya ha sido franqueada en el estado aparecerá: FRANQUEADO.
Código Conf./Disconf: Descripción de la conformidad/disconformidad del cliente.

Una vez franqueada la avería, nosotros deberemos confirmar o no el franqueo dependiendo si el circuito está bien o sigue teniendo problemas.
–Cliente conforme con franqueo: Cuando el circuito este correctamente.
–Confirmada por el sistema automáticamente: una vez franqueada la avería si antes de 8 horas no es confirmada, automáticamente el sistema la confirmará.

Cuando tú confirmas el franqueo al grabarlo el estado que antes estaba FRANQUEADO pasa a CONFIRMADO.
–El resto de códigos son para rechazar el franqueo.

Cuando tú rechazas el franqueo al grabarlo el estado que antes estaba FRANQUEADO pasa a ARRANCADO.

Información: Se pondrá una breve descripción tanto si se confirma el franqueo, como si se rechaza (el porqué del rechazo, si sigue teniendo cortes, si el circuito sigue incomunicado, si tiene lentitud, etc.).

2.2. Herramientas de diagnóstico y notific. incidencias en dispositivos de interconex. de redes

Herramientas hardware

Las herramientas hardware ayudan a identificar los problemas del funcionamiento.

Voltímetros digitales

El voltímetro digital (medidor de voltios-ohmios) es la herramienta electrónica de medida general más básica.

Está considerada como algo estándar para cualquier técnico informático o electrónico y puede revelar muchas más cosas que la cantidad de tensión en los extremos de una resistencia.

Los voltímetros pueden determinar si:
–El cable es continuo (no tiene cortes).
–El cable está transmitiendo.
–Dos partes del mismo cable están tocándose (y pueden producir cortocircuitos).
–Una parte expuesta de un cable está tocando otro conductor, como una superficie metálica.

Una de las funciones más importantes del administrador de la red es comprobar la tensión de funcionamiento del equipamiento de la red.

La mayoría del equipamiento electrónico funciona a 220voltios AC.

Pero no todas las tomas de corriente lo cumplen.

El funcionamiento durante períodos prolongados a baja tensión puede generar problemas en el equipamiento electrónico.

Tensiones bajas suelen producir errores intermitentes. Por el contrario, tensiones muy altas pueden causar un daño inmediato en el equipamiento.
En los lugares de reciente construcción, es indispensable hacer las comprobaciones oportunas sobre la tensión en cada una de las tomas de corrientes, para comprobar si están dentro del rango permitido, y así evitar enchufar ciertos dispositivos, que puedan causarles daños irreversibles. Reflectómetros del dominio temporal (TDR).

Los reflectómetros del dominio temporal (TDR, Time-Domain Reflectometer), envían pulsos como los de un radar a través de los cables para localizar cortes, cortocircuitos o imperfecciones.

El generador y localizador de tonos como herramienta de diagnóstico y notificación de incidencia

Generador de tono y localizador de tono

Los generadores de tono y los localizadores de tono son pequeños dispositivos manuales utilizados para identificar los pares de hilos.

El receptor de tonos/detector de traza modelo TR02 es un instrumento de mano de reducidas dimensiones que, mediante la identificación de los tonos emitidos por un cable, permite seguir su recorrido o traza sin cortar el recubrimiento aislante.

Consta de un amplificador y un parlante con un robusto cono de mylar de gran resistencia a la humedad.

Se utiliza con los instrumentos modelos CA7024, CA7026 o CA7028 funcionando en modo transmisor de tonos, conformando así un método muy rápido y eficiente para determinar el recorrido de un conductor o su localización.

El equipo se enciende y activa como receptor oprimiendo un botón.

Mediante un control se puede ajustar el volumen del parlante al nivel deseado.

También posee un conector de audio para enchufar un auricular común que inhibe el funcionamiento del parlante.

De esta forma el operador obtiene una señal clara y puede trabajar en una oficina sin molestar al personal de la misma.

Características
–Determinar la traza de los cables.
–Detectar roturas en los cables.
–Encontrar cables ocultos en paredes, tuberías y paneles.

El reflectómetro de dominio temporal como herramienta de diagnóstico y notificación de incidencia

La principal función del reflectómetro de dominio temporal, es la detección de fallos en los cableados metálicos, como pueden ser los cableados de par trenzado de alambre, los coaxiales, junto con otros tipos de cableados, usando igualmente, otro tipo de OTDR, para el cableado de fibra óptica.

Es un instrumento electrónico que simplemente caracteriza y detecta anomalías en el cableado subyacente.

Los fundamentos propios del dispositivo, consiste en la emisión de un pulso muy corto en el tiempo.

Su modo operando, consiste en que dicho pulso no regresará al OTDR, si el conductor del cableado, es de una impedancia uniforme y su conector está bien terminado.

En este escenario normal y de correcto funcionamiento de la red y de las terminaciones de los conectores, tiene su lectura en la absorción del pulso en la terminación final del OTDR, además de no reflejar una señal de regreso al equipo electrónico.

En caso contrario, donde existe una impedancia discontínua, junto con una mala terminación de los conectores, generará una serie de ecos por cada discontinuidad, que se reflejará de vuelta al equipo electrónico TDR.

La interpretación del resultado del pulso medio de entrada/salida, como fruto del resultado de los aumentos y disminuciones de impedancia en relación al pulso original, teniéndose en cuenta la velocidad de una impedancia dada como prácticamente constante, se representa como una función del tiempo.

En resumidas cuentas, esta función del tiempo, puede ser leída como una función de longitud del cable.

Indicación de corto

Para verlo de forma simple, consideremos el caso trivial donde el extremo final del cable se cortocircuita (es decir, se termina en una impedancia de cero ohmios).

Cuando la orilla creciente del pulso se lanza a través del cable, el voltaje en el punto que lanza los pulsos alcanza un valor instantáneo dado, y el pulso comienza a propagarse a través del cable.

Cuando el pulso alcanza el corto, no se absorbe ninguna energía en el extremo final.

En vez de eso, un pulso opuesto se refleja hacia atrás.

Cuando el reflejo opuesto alcanza el punto de lanzamiento, el voltaje en este punto aumenta bruscamente, señalando que hay un corto en el final del cable.

Esto es, el TDR no tiene indicación de que hay un corto al final del cable hasta que el pulso emitido haya viajado por el cable -aproximadamente a la velocidad de la luz- y el eco haya vuelto a la misma velocidad.

Tras este tiempo de ida y vuelta, el corto puede ser detectado por el TDR.

Conociendo la velocidad de propagación de la señal en el cable, se obtiene de esta manera la distancia a la que se produce el corto.

Indicación de circuito abierto

Algo parecido ocurre si el extremo distante del cable es un circuito abierto (termina en una impedancia infinita).

En este caso, el reflejo del extremo distante se polariza idénticamente al pulso original y añade lo cancelando anteriormente.

Así que, tras una demora de viaje de ida y vuelta, el voltaje en el TDR salta bruscamente a dos veces el voltaje inicialmente aplicado.

Una terminación perfecta teórica en el extremo distante del cable, absorbería enteramente el pulso aplicado sin causar ningún reflejo.
En este caso, sería imposible determinar la longitud del cable. Afortunadamente, las terminaciones perfectas son muy raras y casi siempre se produce algún pequeño reflejo.

La magnitud del reflejo se denomina “coeficiente de reflexión”; que puede ser relacionado con la proporción de la impedancia nominal del sistema contra la impedancia verdadera en cada discontinuidad.

Uso
Como se ha aprendido hasta ahora, una de las características que aprovecha el TDR, son las sensibilidades a las variaciones de la impedancia, dando lugar a múltiples aplicaciones para este dispositivo electrónico.

Entre ellas, podemos destacar la verificación de las características de la impedancia, la ubicación de los empalmes y conectores del cableado, asimismo, las pérdidas de potencia asociadas a un medio cableado, ya sea de par trenzado de alambre, coaxial o de fibra óptica.

De esta forma, analizando las variaciones de impedancia, así como las diferentes discontinuidades del cable, detectadas en forma de eco, podemos realizar la lectura de las anomalías provocadas en el cableado, y estimar su longitud, ubicación del empalme, así como los conectores.

Son aparatos imprescindibles para la conservación y mantenimiento de las líneas de telecomunicaciones, incluyendo las nuevas aplicaciones para TDR, el aislamiento de los únicos puntos de fallo.

El certificador de cableado como herramienta de diagnóstico y notificación de incidencia

Redes de comunicaciones
Certificadores y Comprobadores de cableado estructurado

Son instrumentos necesarios, para el aseguramiento y fiabilidad de una instalación de cableado estructurado.

Para el cumplimiento del aseguramiento y fiabilidad de una instalación, los elementos o componentes pasivos, deben de regirse por una serie de normas estrictas y muy bien definidas, para el correcto cumplimiento de los parámetros necesarios de transmisión, para un correcto funcionamiento de la red.

A medida que las aplicaciones y servicios requeridos por los usuarios de estas redes, se hacen más exigentes en cuestión de velocidad y capacidad de transmisión, los parámetros de requerimiento a la hora de confeccionar el cableado correcto, junto con sus elementos pasivos, dependiendo de la categoría de cableado.

Según se va aumentando la velocidad, la cantidad de parámetros se hacen extensibles a estos requerimientos, haciéndose imprescindibles los mismos, a medida que la velocidad del enlace aumenta.

Esto se hace necesario, ya que en un determinado tipo de cableado, como puede ser de tipo 10 mbps de categoría 4, se hace imprescindible cambiar ciertas capacidades parásitas propias del tipo de cableado, por otras capacidades y valores, que hagan de estas y de por ejemplo la diafonía, críticas para los nuevos requerimientos.

Por ello, en velocidades más grandes, se requiere estos tipos de cambios, para que estas capacidades y por tanto la diafonía, no sean un punto crítico a la hora de establecer las capacidades necesarias en cuestión de velocidad, requeridas por las aplicaciones y recursos de los usuarios.
Uno de los errores típicos consiste en unir los 4 pares, siguiendo el esquema 1, 2, 3, 4, 5, 6, 7, 8 con 1, 2, 3, 4, 5, 6, 7, 8.

Esta unión provoca un destrenzado de dos pares, lo que supone que en una transmisión real se provoque una diafonía excesiva.

Todos ellos se deben medir en el enlace de transmisión de datos.

Cada parámetro puede depender de las características estructurales de construcción del cable, conectores, etc.
Esta unión provoca un destrenzado de dos pares lo que supone que en una transmisión real se provoque una diafonía excesiva y la red caiga.

Redes de comunicaciones

El efecto no es crítico cuando la red funciona a 10 Mbits (Ethernet), pero cuando utilizamos ese enlace o latiguillo para una red de 100 Mbits (Fast Ethernet), el resultado es que la diafonía provoca una caída del segmento al que está conectado la red o peor, una caída de toda la red.

Los 8 hilos de un cable de datos van trenzados dos a dos, siguiendo el esquema 1, 2, 3, 4, 5, 6, 7, 8 con 1, 2, 3, 4, 5, 6, 7, 8. Esta situación crea un par 3,4 y uno 5,6 que no existen en realidad, o lo que es lo mismo, se están destrenzando el par 3,6 y el 4,5.

Este destrenzado tiene una longitud igual a la del latiguillo, o del enlace horizontal, dependiendo dónde se realiza esta conexión. Esto provoca campos electromagnéticos que generan una diafonía en pares adyacentes, especialmente entre el 4,5 y el 3,6.

La transmisión se interrumpe cuando trabajamos en Fast Ethernet, ya que la tasa de colisiones aumenta hasta que ésta ya no es soportada por la red, y como consecuencia cae.

Estas colisiones no son generadas por ningún equipo, sino por el cable y la diafonía generada de un par sobre otro.

Es importante notar que eléctricamente están unidos.

Sin embargo, cuando hay una transmisión real en Fast Ethernet, este enlace fallará ya que la diafonía que se provoque debido al destrenzado de pares generará colisiones.

Otro ejemplo es la atenuación, o las pérdidas de retorno, parámetros de crucial importancia que necesitan comprobarse en cada latiguillo, cada enlace de la instalación.

El fallo de un parámetro en cualquier enlace de la instalación puede suponer, especialmente en Fast Ethernet y Gigabit Ethernet, que la red falle.

Cuando una empresa instaladora acomete la instalación de una red de datos debe comprobar que eléctricamente es correcta, para lo cual puede utilizar un comprobador de cableado estructurado como por ejemplo un Fluke 620, que comprueba longitud, mapa de cableado y si hay pares divididos (la causa más importante de diafonía).

Una vez que toda la instalación ha sido realizada y que se ha comprobado que eléctricamente es correcta, es necesario asegurar que el enlace de datos (todos y cada uno de los enlaces) cumple con los parámetros de transmisión apropiados para las aplicaciones que correrán por encima del enlace, o lo que es lo mismo certificar la instalación de cableado de datos.

Para ello es necesario utilizar un certificador de cableado estructurado.

Los latiguillos se tienen que hacer siguiendo criterios según normativas y con componentes adecuados para la instalación donde se vayan a usar; si no es así, puede haber caídas o ralentizaciones de la red, cuando todos los PC's, impresoras, servidores, etc., funcionan correctamente.

Para comprobar eléctricamente es necesario certificar todos los enlaces de datos:

"No se puede abordar la solución de problemas en la red si la instalación de cableado no está certificada por una herramienta de Certificación de Cableado Estructurado para la Categoría apropiada".

Esta afirmación puede parecer un tanto drástica, pero la realidad así lo confirma. Estos equipos comprueban todos los parámetros de transmisión y los eléctricos. Los hay de varios tipos, según la categoría hasta la que lleguen.

Hay certificadores de hasta categoría 5 (Ethernet y Fast Ethernet y medidas en F.O.) como el DSP-100 o DSP-2000 con precios entre 2500 y 4000 euros, o certificadores de hasta categoría 6 (Ethernet, Fast Ethernet y Gigabit Ethernet, y certificación de fibra óptica).

En resumen: la correcta instalación de las redes de datos es fundamental para que la red funcione sin problemas.

No se puede acometer la solución de problemas en redes de datos si la instalación física, o sea el cableado, no ha sido garantizado para las aplicaciones que corren por encima.

No se puede acometer la solución de problemas en redes de datos si la instalación física (el cableado), no ha sido garantizado o certificado para las aplicaciones que deben correr por él. (Garantizado por certificadores de cableado estructurado de Fluke).

Para acometer una instalación de datos se necesita un comprobador de cableado capaz de detectar problemas eléctricos como cortos, abiertos, longitud, mapa de cableado, y que pueda reconocer pares divididos (potenciales generadores de diafonía).

Para garantizar que la instalación de datos podrá correr aplicaciones como Ethernet, Fast Ethernet o superiores es necesario comprobar no sólo parámetros eléctricos sino parámetros de transmisión, para lo cual es crítico certificar todos los puntos de la instalación de datos, utilizando para ello los Certificadores t de categoría 5, 5e o 6.
Esto provoca campos electromagnéticos que generan una diafonía en pares adyacentes, especialmente entre el 4,5 y el 3,6.

La transmisión se interrumpe cuando trabajamos en Fast Ethernet, ya que la tasa de colisiones aumenta hasta que ésta ya no es soportada por la red, y como consecuencia cae.

Estas colisiones no son generadas por ningún equipo, sino por el cable y la diafonía generada de un par sobre otro.

Es importante notar que eléctricamente están unidos.

Sin embargo, cuando hay una transmisión real en Fast Ethernet, este enlace fallará ya que latiguillo para una red de 100 Mbits (Fast Ethernet), el resultado es que la diafonía provoca una caída del segmento al que está conectada la red o peor, una caída de toda la red.

2.2.1. Analizadores de protocolos

Los analizadores de protocolos, o comúnmente denominados “sniffers“, son herramientas especialmente útiles para los administradores de red.

Estas herramientas, capaces de detectar anomalías e incidencias en el comportamiento de las comunicaciones entre computadoras.

Son de especial utilidad, para la detección y clasificación de problemas, en los segmento de red, protocolos y aquellas máquinas, que están generando una serie de deficiencias en el comportamiento de la red.

Dado que por la red viajan multitud de paquetes, será necesario seleccionar aquellos que nos resulten de interés.

Ejemplificación de herramientas de software de diagnóstico

Wireshark

Es una herramienta gráfica utilizada por los profesionales y/o administradores de la red para identificar y analizar el tipo tráfico en un momento determinado.
En el argot IT se denominan analizadores de protocolos de red, analizadores de paquetes, packet sniffer o sniffer.

Wireshark permite analizar los paquetes de datos en una red activa como también desde un archivo de lectura previamente generado, un caso particular es generar un archivo con TCPDUMP y luego analizarlo con Wireshark.

A partir del año 2006 Wireshark es conocido como Wireshark1y hoy en día está categorizado como uno de los TOP 10 como sniffer junto a Nessus y Snort ocupando el segundo lugar entre estos.

Algunas de las características de Wireshark son las siguientes:

Disponible para UNIX, LINUX, Windows y Mac OS.

Captura los paquetes directamente desde una interfaz de red.

Permite obtener detalladamente la información del protocolo utilizado en el paquete capturado.

Cuenta con la capacidad de importar/exportar los paquetes capturados desde/hacia otros programas.

Filtra los paquetes que cumplan con un criterio definido previamente.

Realiza la búsqueda de los paquetes que cumplan con un criterio definido previamente.

Permite obtener estadísticas.

Sus funciones gráficas son muy poderosas ya que identifica mediante el uso de colores los paquetes que cumplen con los filtros establecidos.

Es importante tener presente que Wireshark no es un IDS (Intrusión Detection System) ya que no es capaz de generar una alerta cuando se presentan casos anómalos en la red.

Sin embargo, permite a los profesionales de IT analizar y solventar comportamientos anómalos en el tráfico de la red.

Estas aplicaciones permiten capturar una copia de los paquetes que circulan por la red para su análisis posterior.

Los más avanzados incluyen una interfaz gráfica capaz de mostrar los campos de los protocolos de comunicación de los distintos niveles, obtener estadísticas de utilización y facilitar considerablemente el posterior análisis de los datos capturados.

De este modo se facilita la detección de problemas, así como la depuración del software de red durante su fase de elaboración.

Por ejemplo, un administrador de red que detecte que las prestaciones de la red son bajas puede utilizar uno de estos analizadores para detectar qué segmentos de la red, protocolos y máquinas están generando más tráfico, y de esa forma llevar a cabo las acciones necesarias, o bien verificar el correcto funcionamiento de los diferentes dispositivos de red (hosts, servidores, routers, cortafuegos, NAT, etc.).

2.2.2. Herramientas «help-desk»

Las herramientas Help Desk, tienen por objeto el acceso y diagnóstico de información en los diferentes dispositivos de interconexión de redes, con el propósito único de facilitar las labores de detección y resolución de las posibles incidencias que se produzcan.

Estas herramientas son de especial utilidad en entornos operativos de soporte donde la operativa consiste en la supervisión, detección y resolución de incidencias.

Existen múltiples herramientas Help Desk en el mercado, pero a continuación se van a describir una serie de herramientas Help Desk en entorno operador, escenario idóneo donde abundan una multitud de

dispositivos de interconexión de redes, y donde estas herramientas se ponen a prueba para comprobar su rendimiento y funcionalidad.
El Kit HelpDesk tiene por objeto la centralización del acceso a toda la información necesaria para las labores que se lleva a cabo respecto al servicio GigADSL.

Gracias a este sistema, el acceso a esta información se lleva a cabo desde la plataforma SIGA, por lo que ya no es necesario utilizar los terminales de los sistemas de gestión propietarios a la hora de acceder a cada uno de los elementos de red.

Anteriormente, cada vez que se producía una incidencia en el servicio GigADSL, el operador debía recurrir a varios sistemas distintos (SIGA y cada uno de los sistemas de gestión propietarios de los distintos fabricantes) para obtener toda la información necesaria para realizar el diagnóstico del problema.

Esto conllevaba una ralentización del proceso de reparación de la avería, además de que requería por parte del operador el conocimiento de la operativa de los sistemas de los distintos fabricantes involucrados.

El Kit HelpDesk tiene por objetivo principal el ser un punto de entrada único para toda la información relativa al servicio, eliminando así la dependencia de multitud de terminales de los sistemas de gestión propietarios.

De esta forma se consigue que el operador acceda desde el SIGA a toda la información que necesita sobre una conexión sin más que introducir el número de teléfono del usuario, independientemente del fabricante de los elementos de red involucrados.

Esta unificación de la operativa de trabajo para los nodos de distintos fabricantes simplifica de manera importante el proceso de formación de los operadores, además de agilizar el proceso de diagnóstico y resolución de averías.

El desarrollo de este proyecto permite eliminar los terminales de los sistemas de gestión propietarios, con el consiguiente ahorro tanto en hardware como en licencias software.

Esto se debe al hecho de que el Kit HelpDesk SIGA unifica en la misma plataforma la gestión de todos los elementos de red, evitando por tanto, el tener que acudir a los terminales de las distintas plataformas propietarias para realizar las labores de supervisión y diagnóstico de averías del servicio GigADSL.

Una de las consecuencias de eliminar los terminales de los sistemas de gestión propietarios y realizar toda la gestión de forma centralizada, es que se unifica la operativa para los distintos fabricantes de nodos.

Es decir, al poder acceder a toda la información necesaria desde un mismo punto, se evita el depender de los sistemas implementados por cada fabricante de nodos, que son distintos entre sí.

Así, los operadores necesitan conocer únicamente un sistema, con el consiguiente ahorro en formación.

El tener un punto de entrada único para la gestión y la supervisión del servicio GigADSL permite que el procedimiento de atención al cliente, ante posibles fallos en la prestación del servicio, sea mucho más rápido y sencillo.

El operador dispone de toda la información relativa al servicio de forma centralizada y su obtención es mucho más sencilla.

Por todo ello, el grado de satisfacción de los usuarios del servicio GigADSL aumentará, ya que la solución a sus problemas será mucho más rápida y eficaz.

En este caso la herramienta está adaptada a los operadores de la Dirección General de Operaciones, requiriéndose un alto grado de conocimientos técnicos para utilizarla.

Operativa del HELP DESK nivel de operación

El HelpDesk Nivel de Operación es una herramienta adaptada a necesidades más avanzadas y que es útil cuando no se ha podido diagnosticar la avería en los niveles anteriores.
Está orientada a operadores con un alto grado de conocimientos técnicos.

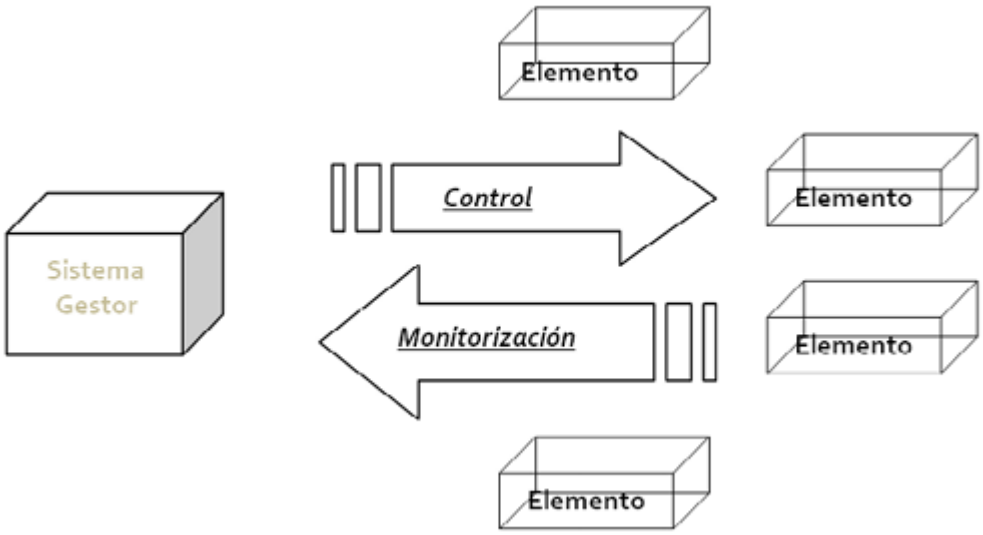
En este caso los operadores tienen acceso a casi todas las funcionalidades de la herramienta.

El objetivo fundamental del sistema es averiguar los valores de los parámetros que configuran una conexión para así poder encontrar la causa del fallo en la conexión.

La aplicación muestra la información concerniente a esa conexión presente en la Base de Datos de SIGA y la contenida en las bases de datos de los elementos de red.
Comparando estas dos informaciones, el operador es capaz de descubrir las discrepancias entre ambas, procediendo a solucionar el error y, por tanto, reparando la avería de la conexión.
El sistema también muestra información sobre el tráfico cursado.
Esta información se muestra tanto en forma textual como en forma gráfica, para que su análisis sea más sencillo e intuitivo.

2.3. Procedimientos de gestión de incidencias

Introducción a la gestión
Antes de adentrarnos en los diferentes objetivos de un Sistema de Gestión de Incidencias, se considera un requisito indispensable, hacer una pequeña introducción a la gestión misma de la incidencia, para conocer a vista general, ciertos aspectos que van correlacionados con los objetivos a definir en un Sistema de Gestión de Incidencias.
–Gestión. Es la planificación, organización, supervisión y control de los elementos de comunicación para garantizar un nivel de servicio aceptable.
–Objetivos. Que la utilización de los recursos se aproxime al 100%, mejorando la disponibilidad y los recursos.
–Métodos de Gestión. Conjunto de herramientas, aplicaciones y metodologías que permiten gestionar una red.
Existen dos métodos básicos para la gestión:
–Monitorización de la red – Consiste en obtener información de los elementos que componen la red.
–Control de la red – Actúa sobre dichos elementos.



En la gestión de incidencias, existen múltiples elementos gestionados por el sistema de gestión, cuya misión es la de facilitar y resultar intuitivo, la gestión de todos los elementos gestionados ya sea de manera remota o localmente, mediante una interfaz que integre todos los elementos a gestionar.

Por ello, vamos a nombrar de forma breve, esta forma de integración en la gestión de incidencias.
Gestión integrada. Por lo general se va a disponer de un único sistema de gestión para todos los elementos gestionados, que nos va a facilitar los datos mediante una interfaz sencilla y única.

Para ello todos los elementos de la red, independientemente del fabricante, modelo, etc. deben facilitarnos los datos y responder a nuestras consultas de igual forma.

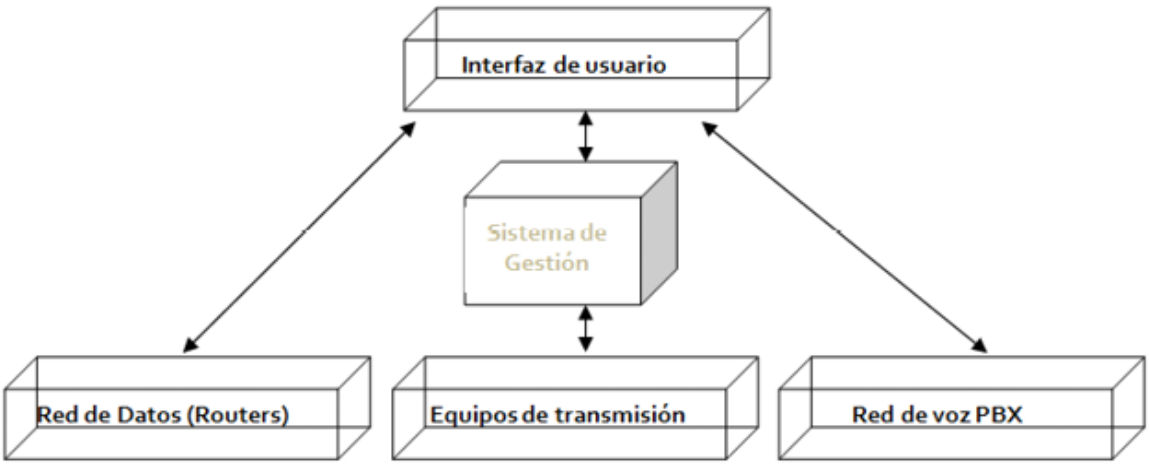
El protocolo empleado para gestionar equipos en Internet es SNMP (Simple Network Management Protocol).

Proceso de resolución

En primer lugar de las distintas fases del proceso de resolución de incidencias tenemos:

1.La identificación y selección del problema, cuyos objetivos fundamentales son:
·Definir el problema de una forma comprensible para el resto del equipo de soporte o encargado de su solución
·Definir el estado futuro deseado a alcanzar cuando se implante la solución al problema.

2.Percepción:
·Normalmente, se atienden con una necesidad extrema los asuntos urgentes, pero olvidándose de la proyección del problema.
·El sentimiento de frustración de extiende a todos los miembros.
·Surgen conflictos, debido a una percepción probablemente equivocada o difusa de la realidad.
·La desorientación se adueña de todos los miembros y de la organización.
·No existe claridad del problema.
·Sólo se perciben los efectos negativos del problema.
Las fases de percepción del problema (análisis, definición y aceptación del problema), deben de haber sido tratadas por completo, ya que si no es así, no se llegará nunca a ningún acuerdo sobre la solución o posibles soluciones al problema.
Para solucionar un problema, el primer paso a seguir, es identificarlo y describirlo adecuadamente, con el objetivo de poder separarlo realmente de problemas sintomáticos, de problemas estructurales o esenciales de la incidencia en sí.
La identificación de un problema, es el momento más importante y difícil sobre todas las fases del proceso de resolución de incidencias, teniendo de antemano ya el 50% del problema resuelto.



Objetivos del Sistema de Gestión
El sistema de gestión tiene por objeto:
–Gestionar de forma centralizada y proactiva las alarmas procedentes de los routers del servicio.
–Proporcionar un diagnóstico de la avería producida, correlacionando la información de las diversas fuentes utilizadas.
–Proporcionar información adicional del cliente afectado por una determinada alarma.
–Definir un entorno de operación.
–Recolectar valores de rendimiento de los routers para la generación posterior de informes.
–Integración con el sistema de ticketing corporativo.
–Generación de informes.

Se ha expuesto los diferentes objetivos que pueden tener un sistema de gestión de incidencias, de una forma generalizada y sentando las bases, para establecer las líneas estratégicas de un sistema de gestión de incidencias.

Los sistemas de gestión de incidencias, sirven para gestionar las diferentes incidencias que puedan suceder a causa de ciertos eventos internos, propios de la organización, o externos, que sean provenientes del entorno exterior.

La utilización de este sistema, permite la agilidad en la operativa de gestión de incidencias, con el firme objetivo, de obtener informes de operación, que resulten de vital importancia, para la medición de ciertos parámetros de calidad en el servicio, en la resolución de dichas incidencias, en los procedimientos establecidos inicialmente para afianzar la seguridad de los servicios, los contratos con terceros, el intercambio de información, etc.

Dentro de los sistemas de gestión de incidencias, en el ámbito de las redes telemáticas, en un entorno operacional, se pueden extraer de forma estructural, ciertos tipos de incidencias, que recogerían todas las fases en la gestión de incidencias, comenzando desde la parte comercial, pasando por el cliente, la infraestructura o circuitos, la gestión de pedidos y el resto de incidencias que puedan producirse en la provisión.

Por ello, me merece especial importancia, reflejar estos tipos de incidencias que pueden darse, en un entorno operacional de redes telemáticas, en el cual, es un factor clave una buena gestión de todas las clases de incidencias, dentro de las diferentes fases que pueden subdividirse las incidencias, en los sistemas de gestión de incidencias.

A continuación, se hace un repaso de algunos aspectos relacionados con la operativa que se sigue en el tratamiento de tickets o actividades en la identificación y descripción de las diferentes actividades en el tratamiento de las incidencias.

Como premisa de actuación en el proceso de identificación y descripción de las actividades, todos los técnicos asignados al área deberán entrar en el sistema, identificar las incidencias y describir las actividades del proceso, para su tratamiento completo, dentro de su ciclo de vida en el sistema de gestión de incidencias.
Periódicamente se hará un seguimiento para comprobar si se han realizado las modificaciones solicitadas y en caso de que no se hayan hecho se volverán a reclamar.

Cuanto antes de identifique y detecte una incidencia, menor será su impacto en la infraestructura subyacente y en definitiva para el conjunto de la red telemáticas que sustenta el negocio de la organización.

La crucial importancia, de monitorizar constantemente los recursos, para detectar de manera temprana al ser posible, potenciales incidencias, es para normalizar el servicio cuanto antes, para minimizar el impacto

negativo que causaría si se mantuviera el evento o suceso en cuestión durante un mayor tiempo de prolongación.
De todas formas, en el caso de que no resulte posible reducir a nulo el impacto de la incidencia, habría que reducir su impacto al mínimo posible.
El paso siguiente es analizar toda la información disponible para identificar las causas y factores contribuyentes asociados al incidente.
–Causa:
·Produjo el evento adverso.
·Su ausencia prevendrá o reducirá este incidente en circunstancias parecidas en el futuro.
–Factor contribuyente:
·No hubieran impedido el incidente pero contribuyen (tierra abonada).
·Su ausencia mejora la seguridad del sistema.
–Las herramientas más utilizadas para identificar las causas y los factores contribuyentes son:
·Diagrama de Ishikawa.
·Análisis Causa-Raíz: preguntas "por qué" en cascada.
·Análisis de barreras, cambios, procesos.
Todas las incidencias del servicio deben ser registradas y cada incidencia debe registrarse de forma independiente.
La información a registrar generalmente incluye:

Información del registro
Identificador único
Categorización
Urgencia, impacto y prioridad
Fecha y hora
Personal/grupo que registra la incidencia
Canal de entrada
Datos del usuario
Síntomas
Estado
CLs
Persona/grupo asignado para la resolución
Problema/know error asociado
Actividades realizadas para la resolución
Fecha y hora de resolución
Categoría del cierre
Fecha y hora del cierre

A parte de la información general que acabamos de ver, también es muy importante llevar un registro diario, con los siguientes parámetros:
–Nº de incidencias.
–Tipo / Clasificación.
–Segmento de cliente.
–Tareas en las que está.
–Servicio afectado.
–Carterización en Provisión.

Los datos a aportar son los siguientes:
1.Control de todos los pedidos en incidencia pendientes
·Segmento de cliente
·Tipo de incidencia
·Servicio afectado

2.Control de áreas que tienen que cerrar incidencias:
·Entradas y Salidas
·SLOs y SLAs,
·Tiempo medio en pendientes
·Nº pedidos superan niveles de calidad en incidencia
·Tipo de incidencia

3.Control de áreas que abren incidencias:
·Entradas y Salidas
·Pendientes
·Nº medio mensual de incidencias abiertas desde área que realiza la tarea
·Tareas en las que se han abierto las incidencias

4.Control de rotaciones de incidencias
·Nº incidencias están mal abiertas (por tarea y tipo)

5.Se realizará un registro semanal que tendrá los siguientes componentes
·Nº medio de incidencias abiertas al día
·Nº medio de incidencias cerradas al día
·Nº medio de incidencias pendientes
·Tiempo medio de incidencias abiertas pendientes

6.Todo ello, atendiendo a la siguiente clasificación:
·Por tipo de incidencia
·Por tarea
·Por segmento
·Por servicio
·Diferenciando carterizados en Provisión

Generalmente, la prioridad de una incidencia, va a determinar su tratamiento y su gestión de cara a su resolución.

La prioridad de la incidencia depende de:

–Rapidez: La urgencia que necesita la incidencia par ser resuelta en un tiempo óptimo.
–Impacto: Por norma general, se determina por usuarios afectados, aunque lo realmente importante es la criticidad de los servicios afectados por la incidencia, siendo lo realmente importante, el impacto adverso que tiene la incidencia en la infraestructura subyacente de la organización, causando efectos muy negativos para su negocio en general.

El equipo de soporte, debe de conocer las reglas en las cuales ha de basarse la priorización de las incidencias.
Resulta muy conveniente, que la herramienta de soporte utilizada, sea capaz de basarse en reglas, para la priorización de las incidencias.

Los incidentes sencillos, o de relativa sencillez, se tramitarán mucho antes que cualquier otro tipo de incidente.

Dependiendo de la prioridad, se asignarán los recursos necesarios para la resolución de la incidencia.

La prioridad de la incidencia, puede cambiar durante su ciclo de vida.

Ejemplo:
Se pueden establecer soluciones temporales a los incidentes, sin que tengan las más mínima repercusión en el restablecimiento del mismo, con unos niveles de calidad y servicio, más que aceptables, sin cerrar la incidencia.
Es conveniente establecer un protocolo para determinar, en primera instancia, la prioridad del incidente.
La priorización de una incidencia está relacionada con el impacto y la urgencia para los usuarios o clientes del servicio TI.
El impacto va relacionado con el grado de afectación sobre el servicio, mientras que la urgencia, establece el grado de priorización para poner en marcha el plan de intervención.
Cuando se recibe una incidencia el personal de soporte de primer nivel, en base a los síntomas, diagnostica la incidencia y la resuelve si está capacitado para ello.
Este diagnóstico inicial de las incidencias, dan lugar a múltiples tipos de incidencias, posibilitando al personal de soporte de nivel 1, poder gestionarlas por sí mismos, o con el departamento correspondiente.

Identificación

En todo proceso de identificación y detección de una incidencia, el problema o problemas que han originado dicha incidencia, deberán haber sido descritos de forma eficiente y eficaz, ya que si no resulta así, el resto de procesos que le siguen, podrían ser con un porcentaje alto de ineficacia, o en el peor de los casos, ineficaz totalmente debido a una mala descripción del problema que originó la incidencia.

Estos pasos son:
–Objetivo: Donde se quiere llegar. El estado deseado.
–Realidad: Donde se está ahora, en relación con el problema.
–Diferencia: Variación entre el objetivo y la realidad del problema.
–Tendencia: El alcance del problema..

La descripción del problema, debe de hacerse de una manera clara y práctica, una vez que el equipo encargado de plantearlo o describirlo, ha llegado a un consenso sobre la descripción del mismo.

Tener la descripción del problema suficientemente bien clara y argumentada, con todos los objetivos claros y el estado final deseado, el equipo debería haber llegado a un acuerdo, por el que el problema y su solución son importantes.

Una vez llegados a este punto, el equipo encargado de la solución al problema, puede asumir la responsabilidad de resolverlo, al quedar totalmente claro la descripción del mismo, estando en su total control del alcance y causas del mismo
La descripción del problema, debe de expresar la situación actual, con respecto del problema del que se adolece.

A mayor exactitud en la descripción del problema, mayores son las posibilidades de obtener una solución satisfactoria.
Para ello, es necesario, que el problema se exprese en términos concretos, explícitos y específicos.

En ciertas ocasiones, en la descripción de un problema, a menudo se sabe lo que se desea hacer, pero es necesario realizar un esfuerzo en poder traducir ese pensamiento para poder transmitirlo al equipo encargado de su resolución.

Esta parte del entendimiento y aceptación de la descripción del problema, es de vital importancia, para que el resto del equipo, posea la misma visión sobre la descripción del problema que les acontece.

El hecho de limitarse tan solo a preguntar y responder ante un problema, ya que no daría respuesta a una buena descripción del problema, sino quedaría sometido al arbitrio, intuición e inteligencia de aquel técnico de soporte.

Como es bien sabido, el planteamiento o descripción del problema, es la fase más importante en todo el proceso de resolución de incidencias en redes telemáticas, y en cualquier otro ámbito.

Monitoree los procesos más importantes y los márgenes deseables de eficiencia.

Cuando el equipo de soporte describe su problema presenta los antecedentes del estudio, las teorías en las que se basó y los supuestos básicos en los que se apoya el enunciado del problema.

Debe aclarar en particular qué personas, situaciones, materiales, factores y causas serán consideradas o no.

Un enunciado completo del problema incluye todos los hechos, relaciones y explicaciones que sean importantes en la investigación.

Hay que encuadrarlo en un enunciado descriptivo o en una pregunta que indique con claridad qué información ha de obtener el equipo de soporte para resolver el problema.

En consonancia con la descripción y análisis de una situación problemática, los siguientes aspectos determinarán la descripción del problema desde muchos aspectos a tomar en cuenta, como por ejemplo:
–Reunir los hechos en relación con el problema.
–Determinar la importancia de los hechos.
–Identificar las posibles relaciones existentes entre los hechos que pudieran indicar la causa de la dificultad.
–Proponer explicaciones de la causa de la dificultad y determinar su importancia para el problema.
–Encontrar, entre las explicaciones, aquellas relaciones que permitan adquirir una visión más amplia de la solución del problema.
–Hallar relaciones entre hechos y explicaciones.
–Analizar los supuestos en que se apoyan los elementos identificados

Una descripción bien indicada del problema apresura un proceso robusto de la acción correctiva.

Ayuda a identificar potenciales causas raíz y elimina prejuicios y ruido.

Descripción correcta del problema ahorra tiempo y esfuerzo haciendo que el equipo se concentre en identificación de causas raíz.

Usando herramientas tales como diagrama de pez (fishbone), el equipo puede probar causas raíz potenciales contra el problema declarado.
La causa raíz verificada debe constar todos los que y donde en la declaración del problema.

Monitoree los procesos más importantes y los márgenes deseables de eficiencia.

La información que se tomará en cuenta deberá: ser objetivamente medida con datos que reflejen con realidad el proceso; deberán ser parte de los objetivos primarios y estar directamente relacionados con necesidades de servicio.

Registro

Todas las incidencias del servicio deben ser registradas y cada incidencia debe registrarse de forma independiente.

La información a registrar generalmente incluye:

Como en todo registro, el proceso de documentación del registro, es donde se genera toda la documentación de partes de no conformidades, de inspección y de acción correctiva / preventiva o de comprobación, por el departamento correspondiente donde se genera.

Mientras aquella documentación relacionada con el sistema de calidad en la comprobación, serán archivados por este último. Será el encargado de la guardia y custodia de dicha documentación.

Por otro lado, todo aquellos partes o quejas / reclamaciones, informes de auditoría y altas de revisión o comprobación, perteneciente al proceso de comprobación de la reparación de la incidencia, será archivado por el área de calidad.

Esta fase de documentación en el proceso de gestión de incidencias, sirve como tales, para el mismo registro de incidencias, así como para establecer, aplicar y verificar todas aquellas acciones correctivas para tratar la incidencia.

Todo ello, debe de ser documentado mediante un procedimiento de documentación, de tales pasos.

Este procedimiento de documentación, no solo serviría como proceso para el tratamiento de las incidencias y recoger las reclamaciones a clientes y proveedores, sino que además, deberá recoger ciertos procesos del sistema de calidad, como por ejemplo, las sugerencias del personal propio, material en mal estado e incumplimiento de requisitos preestablecidos.

En el procedimiento debidamente documentado, deberá entenderse que se entiende por incidencia, los tipos que existen, las diferentes actuaciones y quienes son los responsables de las mismas.

La documentación de todas las distintas fases o procesos por los que se gestionan las incidencias, son de vital importancia.

La aprobación por parte de la alta dirección, no es un mero capricho del responsable de calidad, sino que establece una forma más segura de poner en marcha todos los procedimientos y pautas a seguir, para el tratamiento y gestión de las incidencias.
Antes de la aceptación del documento de procedimientos por parte de la alta dirección, dicho documento de procedimientos, ha sufrido importantes debates acerca de su desarrollo e implementación, teniendo en cuenta las diferentes opiniones del personal y de todos los responsables implicados.

Una vez tenidos en cuenta las diferentes opiniones del personal y de todos los responsables, el documento de procedimientos, se aseguraba su implicación y ejecución, junto con un nivel de detalle.

Finalmente, para que la documentación de procedimientos tuviera la difusión que le correspondía, debido a la gran implicación que se recogía en él, debía de estar suficientemente expuesto a todos el personal y responsables de la organización para su posterior consulta y seguimiento.

Esta difusión de la documentación, deberá estar regida a su vez, por un procedimiento también documentado, sobre la distribución de documentación por toda la organización.

Para todas las incidencias, deberán ser registradas y documentadas con detalle y extensión adecuados a la magnitud y criticidad de la incidencia, por medio de cualquiera de los medios de comunicación puestos a disposición para el tratamiento y gestión de incidencias.

Relación de formatos de documentación

Podemos establecer una relación a modo de introducción y guía, sobre los posibles formatos de los diferentes documentos, citando por ejemplo:
–Formato F01: para la apertura y formulación de incidencias.
–Formato F02: para la presentación de quejas, sugerencias y reclamaciones.
–Formato F03: para la obtención de resultados de los indicadores.
–Formato F04: para la solución de las incidencias.
–Formato F05: para el cierre de incidencias.

Priorización

Generalmente, la prioridad de una incidencia, va a determinar su tratamiento y su gestión de cara a su resolución.

La prioridad de la incidencia depende de:
–Rapidez: La urgencia que necesita la incidencia par ser resuelta en un tiempo óptimo.
–Impacto: Por norma general, se determina por usuarios afectados, aunque lo realmente importante es la criticidad de los servicios afectados por la incidencia, siendo lo realmente importante, el impacto adverso que tiene la incidencia en la infraestructura subyacente de la organización, causando efectos muy negativos para su negocio en general.

El equipo de soporte, debe de conocer las reglas en las cuales ha de basarse la priorización de las incidencias.

Resulta muy conveniente, que la herramienta de soporte utilizada, sea capaz de basarse en reglas, para la priorización de las incidencias

Es muy conveniente, que se deben de tener en cuenta factores adicionales como por ejemplo el tiempo de resolución y los recursos que haya disponible, ya que las incidencias más simples, se tramitan con más rapidez

Según la prioridad de la incidencia, se irán asignado los recursos disponibles para su resolución
Durante la vigencia, la priorización de la incidencia, puede cambiar notablemente durante la vida de la misma.

Uno de los ejemplos es que se pueden implementar soluciones temporales que restauren el servicio notablemente el servicio y que nos permite poder retrasar el cierre, hasta dar una solución óptima al incidente.

Es recomendable, el establecer un protocolo para determinar la prioridad del incidente.

La priorización de una incidencia está relacionada con el impacto y la urgencia para los usuarios o clientes del servicio TI.

El impacto se determina según el efecto que tiene sobre la operación del negocio o sobre el funcionamiento del servicio, mientras que la urgencia es determinada por la velocidad que se requiere para su resolución.

Diagnóstico inicial

Cuando se recibe una incidencia el personal de soporte de primer nivel, en base a los síntomas, diagnostica la incidencia y la resuelve si está capacitado para ello.

Este diagnóstico inicial de las incidencias, dan lugar a múltiples tipos de incidencias, posibilitando al personal de soporte de nivel 1, poder gestionarlas por sí mismos, o con el departamento correspondiente.

Por otro lado, cabe mencionar que una vez adentrados en la observación y búsqueda de las raíces del problema, en la mayoría de los casos, se tiene la sensación de que las causas del problema se expanden de una manera incontrolable en varias direcciones, resultando en un primer momento, como un gran obstáculo de una complejidad casi incontrolable.

En gran parte, por no decir la gran mayoría de los equipos de soporte, la tendencia es en hacer un proceso exhaustivo de todas las causas posibles, con el firme objetivo de establecer aquella o aquellas que han originado el problema del que se adolece.

Esto último, en muchos casos, puede ser contraproducente.

La mejor forma de hacer una limpieza de aquellas posibles causas que puedan interferir en el establecimiento de la causa o causas del problema, es ignorar o eliminar aquellas, en las que sus efectos son casi irrelevantes e imperceptibles.
Para ver, según el diagnóstico inicial, podemos encontrarnos con los siguientes tipos de incidencias.

Incidencias por Causas del Cliente

1.Retenida por cliente: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + Nombre y teléfono de contacto del cliente que retiene la instalación y la causa expresada de retención.

2.Demanda Aplazada: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + Indicar la persona y teléfono del contacto del cliente que retiene la instalación y la fecha programada en la que quiere realizar el trabajo.

En el caso de que se tratara de un Proyecto Especial donde se estableciera un plan de implantación con el cliente semanal o mensual, el Jefe de Proyecto de provisión podrá indicar entonces en la incidencia la fecha de fin de proyecto.

También se utiliza este tipo de incidencia para los cambios de router, indicando la fecha programada con el cliente.

Incidencias por Causas Comerciales

Tramitación Incompleta: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + [LITERAL] + Indicar los datos erróneos y la causa de por qué no son correctos.
Los literales serán:
–Incidencia tramitación: si sospechamos que hay un error en la tramitación.
–Incidencia sistema: si sospechamos que hay un error en la tramitación debido al sistema.

Soporte a Comercial: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + [LITERAL] + Indicar todos los datos posibles del problema y de la duda comercial que hay que aclarar con el gestor que atiende la cuenta del cliente, en función del literal conforme se específica abajo.

Los literales posibles son los siguientes:
–[CONFIRMAR ANULACIÓN]: Nº del pedido con el que se ha duplicado. Nombre del cliente y teléfono de contacto y causa por la que no lo quiere.
–[ACLARAR DOMICILIO]: Descripción de los datos de domicilio que faltan.
–[CONSULTA COMERCIAL]: Descripción de la incidencia.
–[FALTA COBERTURA]: Descripción de la conexión en la que no existe cobertura del proveedor de circuitos.

Incidencias por causas de provisión

Soporte a Coordinación: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + Indicar la información adicional que debe ser aclarada para poder finalizar el trabajo.

En definitiva, un análisis correctamente realizado, se debe de concentrar inmediatamente en el problema, no en sus efectos y supuestas causas que lo provocaron, estableciendo una trayectoria clara y lógica, desde el reconocimiento del problema, al punto donde ocurre, pasando al punto del establecimiento de las posibles causas del problema, y finalmente, llegando a la causa raíz que ha originado el problema verdaderamente.
–Incidencia Aplicación: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + Indicar el número de incidencia aportada desde la aplicación.
–Avería de línea: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + Indicar el número de avería proporcionados por el grupo de Gestión de Circuitos de acceso y Cortes en Red.
–Pendiente Soporte a Ingeniería: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto + (fecha en la que se abre la incidencia) + Indicar número del soporte proporcionado por Ingeniería de Servicios o por Soporte Técnico a la Gestión.
–Pendiente de Circuito: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + Indicar el teléfono y nombre de la persona del cliente, datos donde se debe de instalar la línea y los datos donde está la línea en ese momento.
–Cortes coordinados: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + Indicar el tipo de cambio que falta por realizar.
–Pendiente de Stock: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + Indicar el material que falta para la instalación.
–Elemento de RED: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + Descripción del problema localizado en Nodo de Red.
–Incidencia en Multienlace: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + Descripción del problema localizado.
–Faltan Datos para la configuración del equipo: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia) + Indicar los parámetros técnicos del cliente configurables en el router, que no se tienen y son necesarios.
–Pendiente de proyecto: (siglas del grupo que reporta la incidencia) + (nombre de la persona que reporta la incidencia) + (extensión o teléfono de contacto) + (fecha en la que se abre la incidencia)+ Indicar bajo que causa se encuentra el proyecto que se demanda.

Una vez expuestos las diferentes incidencias que se pueden dar, en relación a la causa de los problemas que originan las incidencias, en gran parte, por no decir la gran mayoría de los equipos de soporte, la tendencia es en hacer un proceso exhaustivo de todas las causas posibles, con el firme objetivo de establecer aquella o aquellas que han originado el problema del que se adolece.

Escalado

Las herramientas de Gestión del Servicio deben usarse para automatizar los tiempos de escalado y escalar la incidencia, según los protocolos establecidos.

En realidad, esta definición de las herramientas de gestión del servicio, en relación con los tiempos de escalado, nos viene a decir que, dependiendo del tipo de incidencia y transcurrido un tiempo establecido para su resolución, debe de pasar de un grupo de soporte a otro más especializado para resolverla.

No es en absoluto recomendable, el escalado de incidencias de manera automática, ya que puede generar tensiones entre los diferentes grupos de soporte, sin que un específico grupo, no haya trabajado nada con ella, y por lo tanto, llegarán incidencias sin documentar, incidencias resueltas en anteriores ocasiones etc.

Para un proceso de gestión de incidencias no muy maduro, el escalado de incidencias de manera automática, serviría muy bien en organizaciones que están empezando a prestar servicios, y que por supuesto aquellas incidencias, estén muy bien definidas, para que no haya ambigüedades ni lagunas en su documentación.

Para definir un proceso de asignación de incidencias con respecto a los tiempos de escalado, lo primero que hay que definir es:
–Qué tipo de incidencias van a ser resueltas y por cada grupo de soporte.
–Tener en cuenta la criticidad de la incidencia.

Un buen comienzo para establecer una serie de reglas predefinidas o una especie de matriz inicial, sería:

Tipo de Incidencia	Grupo de escalado	Criticidad	Tiempo de escalado
Refrigeración CPD	Operación CPD	Alta	0'
Impresoras	Soporte insitu	Baja	15'
Impresoras de maquetación	Soporte insitu	Alta	25'
Caída servicio de Windows	Microsoft	Alta	10'

Existen dos tipos de escalado:
–Funcional: El grupo de nivel 1, se ve incapacitado para resolver la incidencia, y la escala al grupo especializado de nivel 2 para su resolución.
–Jerárquico: en caso de que se den ciertas circunstancias (incidencias graves o críticas, riesgo de incumplimiento del SLA o SLO, dependiendo de los tiempos estimados de resolución), éstas se deben notificar a los responsables del servicio correspondientes.

A tenor del escalado que se realice, la incidencia que está escalada, sigue perteneciendo al grupo de nivel 1.

El grupo de nivel 1, es quién debe de hacer el seguimiento de la incidencia, gestionarla adecuadamente, para que sus tiempos de resolución no excedan los parámetros de calidad marcados en los SLAs y SLOs.

Este grupo de nivel 1, es quién debe de cerrar la incidencia cuando esté resuelta, además de ser los responsables de la interlocución con los usuarios finales con respecto a la misma.

A tenor de estos procedimientos de escalado, que se hacen necesarios para una correcta planificación de las intervenciones y niveles de escalado, para resolver la incidencia, se hace necesario igualmente, un conjunto de capacidades que puedan representarse como una planificación de escalado o de intervenciones.

La planificación de las intervenciones, son un conjunto de capacidades en relación a la comprensión de un plan trazado, con el firme objetivo de organizar, elaborar un plan, buscar estrategias y tomar decisiones al respecto.

Las acciones llevadas a cabo por la planificación, se articulan mediante una serie de procedimientos en los que la existencia de una mejor racionalidad y organización, en el conjunto de las actividades que hay que realizar, influyen directamente sobre el curso causal de estas actividades, con el fin de poder obtener unos resultados o una situación como deseable, mediante el uso eficiente de los medios y los recursos escasos o limitados.
La planificación, al ser un proceso que se desarrolla en un período de tiempo determinado y con la misión de definir la dirección del proceso de cambio de la actividad o conjunto de actividades, se va a ilustrar en un esquema, la planificación, desde su origen, pasando por la dirección del proceso de cambio, llegando a la situación deseada.
Como en todo servicio, estos se pueden desglosar en un número determinado de niveles operativos, los cuales no van a ser menos en la planificación de las intervenciones, resultando ser los siguientes:

Niveles operativos en la planificación de las intervenciones

1.Las políticas son las bases en las que se fundamentan los procesos de desarrollo, en dirección a la culminación de los objetivos marcados.

2.El plan es el instrumento del proceso y del sistema de planificación que concreta y materializa la visión, los principios, los objetivos, las políticas, las estrategias y las metas de desarrollo deseado y posible.

3.Los objetivos hacen referencia al fin o propósito de la situación futura deseable.

4.Las metas cuantifican los objetivos a través de indicadores e índices con los que se pretende evaluar su grado de cumplimiento.

5.Las estrategias se refieren a los caminos o direcciones sobre cómo lograr los objetivos, las políticas elegidas.

6.Los instrumentos son las diferentes herramientas que permiten evaluar y hacer el seguimiento del plan.

7.El programa materializa un conjunto de decisiones, cuyas directrices deben estar orientadas a solucionar los problemas, satisfacer las necesidades y conseguir los objetivos del plan.

8.El proyecto se percibe como un conjunto de acciones, orientadas a la solución de un problema o una necesidad, teniendo en cuenta los recursos disponibles debidamente programados en el tiempo y en el espacio. Los objetivos del proyecto concretan y materializan los objetivos del programa y a su vez los del plan de desarrollo.

9.Los recursos pueden ser de carácter humano, físico, económico, financiero, etc.

10.La actividad es un conjunto de tareas u operaciones interrelacionadas entre sí, enfocadas a la obtención de objetivos parciales y localizados dentro del proyecto y del plan de desarrollo.

Estas capacidades en relación a la planificación de las intervenciones en una situación dada a un problema existente, podemos clasificarlas en 4 bloques distintos:

1.Análisis de la información existente:
Aquí se trata de saber la información disponible de la que se tiene, la necesidad y la relevancia de dicha información disponible con respecto a la planificación de las intervenciones y si son importantes o meramente superfluas con respecto al fin que se persigue.

NIVELES DE CONTROL.

Nivel estratégico	⇨	Misión, visión, objetivos institucionales Titulares/órgano de gobierno	⇨	Planificación
Nivel Directivo	⇨	2º, 3º y 4º nivel (procesos)	⇨	Programación, presupuesto y supervisión.
Nivel Operativo	⇨	Operación	⇨	Acciones y tareas

Dentro del análisis de la información existente, podemos distinguir igualmente 2 partes bien diferenciadas:
·Una reflexión sobre las posibilidades de la información disponible

Aquí, podemos extraer las distintas combinaciones posibles entre las informaciones que disponemos, como se pueden combinar entre ellas, las relaciones existentes entre ellas, además de poder deducir los tipos de operaciones que se pueden llevar a cabo en la planificación de las intervenciones, junto con su sentido o coherencia.
·Reflexiones sobre los medios empleados, en relación a los fines. La relación de los datos disponibles con las preguntas formuladas al respecto.

En este apartado, podemos preguntarnos sobre como los datos de los que disponemos, puede responder eficazmente al problema que se nos plantea.

Como elegir los medios idóneos y necesarios con la información disponible, para dar respuesta al problema del que se adolece, para conseguir u obtener un fin en concreto, para responder a lo que el problema en si está pidiendo.
·Organización de la información disponible

La información, debe de ser estructurada en esquemas y diagramas con datos e incógnitas, es decir con datos que se saben y otros datos que no se saben.
·Exploración

Se trata de capacidades asociadas a examinar problemas equivalentes, modificar problemas y examinar problemas particulares.
·Concebir y estructurar un plan de resolución

En este apartado, consiste en razonar con una parte del plan o con toda, a raíz de los datos de los que disponemos, realizar prospecciones sobre los resultados posibles a obtener, probar estrategias previamente elaboradas o heurísticas.

La situación y problemática actual de los servicios, en relación a la resolución de incidencias en redes telemáticas, requieren una planificación previa de las intervenciones a realizar en los diferentes servicios que se presten.

En algunos casos, esta planificación de las intervenciones, requieren desplazamientos de los técnicos para revisar y solucionar los problemas que se hayan presentado.

Uno de los inconvenientes en algunos casos que pueden presentarse en la planificación de las intervenciones y en el cierre de una incidencia, es determinar si la intervención, es o no facturable.

A continuación, presento los conceptos según mi criterio que pueden ser facturables y los que no lo son.

Investigación y diagnóstico

Si la incidencia hace referencia a un fallo en el sistema, lo más probable es que se necesite investigar la causa del fallo. Las tareas más comunes dentro de esta actividad son las siguientes:

1.Establecer exactamente qué es lo que no funciona correctamente y para qué secuencia de acciones del usuario (casuística).

2.Establecer el impacto potencial de la incidencia.

3.Determinar si la incidencia está producida por la implantación de un cambio.

4.Buscar en la base de datos de conocimiento (base de datos de errores conocidos, registro de incidencias, etc.) posibles soluciones y/o workarounds.

–Se debería obtener información oportuna sobre la vulnerabilidad técnica de los sistemas de información que se están utilizando, evaluar la exposición de la organización ante tal vulnerabilidad y tomar las medidas adecuadas para hacer frente a los riesgos asociados.

Diagnóstico
–En base al estado del circuito, corresponde con una primera valoración de la causa de la incidencia
–Es muy importante realizar el diagnóstico rápidamente (10-15min) ya que es la prueba de que comenzamos a tratar la incidencia.

Problemática
–Peticiones de los clientes de dejar en observación los circuitos un largo período de tiempo – Localización de los clientes durante periodos festivos: fines de semana, vacaciones, etc.
–Solución: serie local (solo aperturas proactivas)

1.Estado observación por más de 12 horas: se cierra y se abre una nueva como proactiva para convertirla en local.

2.Provisión incompleta: se anula (si no es proactiva) y se reabre como proactiva para convertirla en local.

Solución: serie local (solo aperturas proactivas).
–Incidencia proactiva pero NO se puede contactar con cliente en dos horas: local.
–Si existe avería real, se cierra la incidencia local y se abre una nueva para tratarla.
–Si no existe avería real, se cierra la incidencia local y se abre una nueva para cerrarla indicando la causa adecuada.
–Abiertas por cliente y NO se contacta con él en dos horas.
–Se cierra dicha incidencia indicando ‘mala operación de cliente’.
–Abrimos una como ‘proactiva por rutina’ e indicamos el número de la incidencia anterior de la que procede.
Tras un proceso de investigación y diagnóstico exhaustivo, habrá procesos que tendrán que ser nuevamente filtrados, para poder encontrar la causa o causas reales que originaron el problema o incidencia.

Este nuevo proceso de filtrado, en aras de la verificación de la causa o causas reales al problema, es de suma importancia, para descartar indicios o fundamentos que anteriormente se pensaba que podrían establecerse como causa o causas reales del problema o incidencia.

En la verificación de la causa real se requiere de métodos eficientes para la captación de información, para el caso se recomienda la hoja de verificación o de registro.

La hoja de verificación es un formato construido especialmente para recabar datos, de tal forma que sea fácil el registro y el análisis de los mismos, lo que permitirá facilitar el análisis en la forma de cómo influyen los principales factores que intervienen en un problema específico

Áreas de aplicación
–Descripción de resultados de operación de inspección.
–Examen de artículos defectuosos (identificación de razones, tipos de fallas, áreas de procedencia, maquinaria, material u operador que participó en la elaboración).
–Confirmar posibles causas de problemas de calidad.
–Analizar o verificar operaciones y evaluar el efecto de los problemas de mejora.
–La hoja de verificación es un paso natural dentro de un análisis de Pareto y una estratificación para recabar datos o confirmar pistas de búsqueda.

Además indica de forma objetiva y permanente a la dirección cuales son los principales problemas, lo que orienta a la generación de planes para reducirlos.

Así mismo esta hoja sirve para evaluar los planes de mejora.

Es importante considerar que el uso excesivo de la hoja de verificación puede llevar a obtener datos sin ningún objetivo concreto e importante.

Para evitar esto, debe considerarse que cada hoja con la que se obtienen datos en una empresa, tenga un objetivo claro y de importancia.

A raíz del uso de una hoja de verificación y de la obtención de estos datos por parte de cada hoja, resulta de manera unánime, que las causas reales deben de verificarse con datos e información, con preguntas del estilo de:
–¿Cómo puede detectarse la influencia de esas causas potenciales? ¿Qué patrones esperas encontrar en los datos?
–¿Hay información actual que pueda ayudar a decidir las causas actuales de los problemas? ¿Es relevante esta información?
–¿Qué otra información o datos son necesarios? ¿Cómo pueden obtenerse?
–¿Quién recolectará la información y cuándo?
–¿Cómo será analizada y cuándo?

Otro punto importante, sobre la verificación de las causa reales, es verificar las conclusiones que se hayan sacado de todo el proceso de determinación de las causas de una incidencia.

Este proceso de verificación de las causas, interrelaciona la información y los datos obtenidos, junto con el proceso de extracción de conclusiones sobre toda la información y datos obtenidos, para después poder verificarlas con personas que conocen muy bien el proceso.

Podemos extraer las siguientes cuestiones, referentes a la verificación de las conclusiones sobre las causas y son:
–Las otras personas que conocen el proceso ¿Están de acuerdo con tus conclusiones? Si eso no es realmente así, ¿Qué otra información o datos son necesarios para apoyar o contradecir tus conclusiones?

A través de experimentación (o simulación), verificar si se ha encontrado, la causa raíz.

Ver si es posible generar y eliminar el problema a través de provocar y retirar la causa a propósito.

La verdadera causa raíz, debe de explicar todos los hechos y datos obtenidos hasta el momento.

Por último, el final de los pasos en el proceso de verificación de la causa real del problema, se hace hincapié en el desarrollo y verificación de la solución a la causa real del problema planteado.

Desarrollo y verificación de la solución a la causa real

Seleccionar entre soluciones alternativas para el problema, y confirmar a través de programas de pruebas, que las causas del problema, han sido eliminadas sin efectos colaterales no deseados.

Escoger y verificar acciones correctivas
–El equipo de soporte, debe de confirmar cuantitativamente que dichas acciones no producirán efectos secundarios no deseados, y que resolverán el problema.
–El equipo de soporte, debe de evaluar objetivamente, cada acción posible en relación con un criterio de decisión.
–El equipo de soporte, también debe de probar dicha acción correctiva y ver que eliminará el problema, conduciendo a pruebas de verificación.
–Se debe de establecer indicadores, que determinen la eliminación total del problema, para asegurarse de que el defecto ha sido del todo eliminado.
–La decisión de la acción correctiva, se hace a través del proceso de toma de decisiones.

A continuación, expongo la hoja de verificación, cuyo uso es muy valioso ya sea una vez identificado el problema, para corroborar los hechos y para verificar la efectividad de las acciones tomadas.

Hoja de verificación
Recabar información o datos de forma estructurada
Verificación de la distribución del proceso de operación
Verificación de ítems o errores defectuosos en el servicio
Verificación de las causas de los defectos o errores
Verificación de la localización de los defectos o errores
Uso valioso ya sea después de identificar el problema, para corroborar los hechos, así como para verificar la efectividad de las acciones tomadas

En el proceso de verificación de la causa real, en relación para corroborar los hechos y verificar la efectividad de las acciones tomadas, para escoger y verificar las acciones correctivas tomadas, hay una serie de criterios a cumplir, como son:
–El equipo de soporte, debe de asegurar de forma cuantitativa, que las acciones correctivas empleadas, resolverán el problema en todo su plenitud, no ocasionando efectos secundarios impredecibles.
–El equipo de soporte, debe de evaluar objetivamente cada acción correctora empleada, en relación con los criterios de decisión empleados en el proceso de verificación.
–El equipo, debe de probar que las acciones correctivas, eliminarán el problema, conduciendo eficazmente las pruebas de verificación oportunas y destinadas a tal fin.
–Establecer indicadores, que establezcan el 100% de confianza, del que el problema ha sido eliminado.

Resolución y recuperación

Cuando se detecta una solución potencial, ésta debería ser aplicada y testeada.
Asimismo, todas las acciones realizadas para resolver la incidencia deben registrarse en el historial de la misma.
Una vez comprobada la resolución, la incidencia se da por resuelta y se asigna al equipo de service desk para su cierre.

Todas las incidencias, poseen unos tiempos establecidos para su resolución, tiempos objetivos (SLO) y medios (SLA).

En caso de sobrepasar estos tiempos límites de resolución, el grupo correspondiente de servicios de operación, procederá a reclamar, siguiendo una serie de niveles preestablecidos de escalado para su reclamación, como son:
–Nivel 1 (SLO): Cuando una incidencia cumple el SLO establecido sin resolverse, se comunicará al área responsable de su resolución.
–Nivel 2 (SLA): Cuando una incidencia cumple el SLA establecido sin resolverse, se comunicará al área responsable de su resolución y al primer nivel jerárquico.
–Nivel 3 (N x SLA): Cuando una incidencia cumple N x SLA establecido sin resolverse, se comunicará al área responsable de su resolución, al primer nivel jerárquico y al segundo nivel jerárquico
–Nivel 4 (5 x SLA): Cuando una incidencia cumple 5 x SLA establecido sin resolverse, se comunicará al área responsable de su resolución, al primer nivel jerárquico, al segundo nivel jerárquico y al tercer nivel jerárquico

En una resolución de una incidencia, comprende varios elementos que deben de llevarse a cabo, como por ejemplo, dar el aviso, además de comprobar y anotar sobre una incidencia que estaba pendiente, ha sido reparada y comprobada por los supervisores del equipo de soporte.

En el proceso de comunicación de la reparación de una incidencia, tenemos varias vías para poder hacer efectiva dicha comunicación, como son:

Mediante observación directa del personal encargado de la reparación, y al término de la reparación, comunica al cliente dicha reparación y su resolución.

Siempre hacer un informe sobre la reparación y las comprobaciones realizadas y acciones tomadas, debidamente motivado que indique que está resuelta.

Otra forma de la comunicación de la reparación, es mediante correo electrónico o vía telefónica, aunque en ciertos clientes, no son los medios más adecuados de comunicación de la reparación de la incidencia. Este medio, resulta aceptable en pequeñas empresas o comercios.
En el proceso de comprobación de la reparación de una incidencia, el encargado del servicio que ha sufrido dicha incidencia, deberá comprobar in situ la resolución de la incidencia, debiéndolo comunicar al departamento o usuario que abrió la incidencia, indicándole que ha quedado resuelta.

Posteriormente, el encargado del servicio en cuestión, deberá de anotar la resolución de la incidencia en el registro oportuno a tal efecto, para su correspondiente asentamiento.

También, debe de ser comunicado el responsable de infraestructuras, si procede, para finalizar el tramo de aceptación y finalización de la incidencia.

En el caso, de una no conformidad con la reparación efectuada, se procederá a la apertura de una nueva incidencia, por no conformidad con la resolución adoptada en la incidencia.

Cierre

Antes de cerrar la incidencia el equipo de service desk debería validar lo siguiente:
–El usuario está satisfecho con la resolución de la incidencia.
–El cierre ha sido categorizado.
–Se han cumplimentado todos los datos necesarios.
–Decidir si es un problema recurrente. En este caso generar un problema.

Cuando se ha solucionado la avería, lo primero es aceptar el franqueo que nos envía el grupo de soporte que ha gestionado la incidencia.

Posteriormente tenemos que abrir la incidencia y tendríamos que franquear el boletín de la incidencia previamente abierta, para una vez conseguida que la incidencia haya sido pre franqueada, podamos optar a introducir las observaciones pertinentes en el campo Conformidad / Disconformidad Cliente, indicando las observaciones por parte del cliente sobre la resolución de la misma, y su conformidad con la resolución adoptada.

Por otro lado, en las observaciones de la línea, tendremos igualmente que generar el cierre, siempre y cuando se haya resuelto la incidencia que afectase a la línea, o si por el contrario no ha sido afectada, indicar en el franqueo del boletín, que esta infraestructura no ha sido afectada por la incidencia.

En el caso de que una vez introducido las debidas observaciones en el campo Disconformidad / conformidad del cliente, y las observaciones en el campo de la línea, el cliente no esté de acuerdo con la resolución adoptada, se procederá a realizar otro trámite.

Este trámite a adoptar por los motivos de no conformidad por parte del cliente, obviamente, no genera el cierre de la incidencia, sino que es reclamada por no ser reparada conforme al cliente, indicando en los campos pertinentes, que no ha sido reparada adecuadamente, según criterio del cliente, y se hacen los diagnósticos y procedimiento que se hayan establecido para la no conformidad por parte de cliente.

Una vez solucionada, esta parte de no reparación por causa de cliente, estamos en disposición de poder proceder al cierre de la incidencia, y así poder comunicárselo al grupo de soporte que ha estado haciendo el seguimiento desde un principio.

Flujo de procedimientos de gestión de incidencias

Componentes del Sistema de Gestión

El sistema de gestión podría descomponerse en los siguientes bloques:
1.Módulo de Gestión de Routers que recoge información de los routers a través del protocolo SNMP.
La Gestión de Routers se implementa a través de un conjunto de herramientas (podrían ser por ejemplo HP Openview, Vantage Point Operations y Network Node Manager).

El Router es gestionado a través de 2 procedimientos complementarios:
–Interrogación periódica desde la colectora al Router en cuestión. En este caso la comunicación es bilateral (primero la colectora pregunta al router, y a continuación este contesta). Se deduce de aquí un requerimiento importante del Sistema de Gestión: “es necesario que haya conectividad permanente entre la colectora y el Router gestionado”.
–Envío de traps SNMP (Simple Network Management Protocol) desde el router a la colectora ante determinado tipo de evento. En este caso la comunicación es unilateral (el router envía un paquete UDP a la colectora)

Se gestionan diferentes tecnologías (Cisco, Teldat, Riverstone, etc.).

Con objeto de poder abarcar todo un entorno operativo de los elementos gestionables o que se desean gestionar mediante sistema de gestión, se ha utilizado una arquitectura jerárquica de dominios de gestión.

Un dominio de gestión engloba el conjunto de routers que son gestionados desde una, solamente una, colectora.

A modo de ejemplo tenemos que los Routers correspondientes al Dominio de gestión A, reenviarán sus traps solamente a la Colectora A (Dominio de gestión A).

En la colectora se ha instalado el software que recibe los traps enviados desde el Router y los reenvía a la gestora, que es quién centraliza las alarmas de las diferentes colectoras.

La comunicación entre colectora y gestora se lleva a cabo mediante un software cliente-servidor.

En el diseño de la plataforma se han tenido en cuenta las siguientes premisas:
–El número límite de Routers por cada colectora no deberá ser superior a 1500 Routers.
–La gestora no presentará ningún límite en cuanto al número de colectoras que puede llegar a soportar. El límite vendrá establecido por el número de objetos en la base de datos de la gestora. El límite recomendado es de 15000 Routers por gestora
–A partir de 15000 Routers es necesario introducir una nueva gestora.

El número límite de routers por cada colectora, y aquel límite impuesto a cada gestora a la hora de introducir una nueva gestora, están pensados para la herramientas de HP Open View.

Una de las colectoras, serían un agente NNM, cuya gestora de dicha colectora, estaría a un nivel jerárquico superior, que es donde se centralizarían todas las colectoras, con todos los routers gestionables que deseamos que generen alarmas, en relación a una serie de causas, con unos determinados efectos.

Para terminar con el módulo de Gestión de Routers, es importante tener en cuenta, que es necesario tener en cuenta ciertas premisas con anterioridad a la inclusión de los routers, en el sistema de gestión de incidencias, como son:

Direccionamiento IP de gestión: todos los Routers presentan una dirección única para realizar la gestión (y será del rango de direcciones previamente establecido para estos casos).

Direccionamiento IP privado: los Routers al estar en casa del cliente presentan un direccionamiento privado del mismo. Este direccionamiento privado, primero no es accesible desde los sistemas de gestión.

Adicionalmente el Router requerirá una configuración adicional referente a la parte de gestión, en especial, la parte que hace referencia a la configuración SNMP.

La configuración SNMP, no está dentro del alcance de este libro, por lo que el alumno, para saber más, deberá consultar otras fuentes en internet, para determinar y comprender una configuración SNMP referente a la parte de Gestión de incidencias en relación a su interconexión con las colectoras.

2.Módulo de Gestión de Acceso a Red recolecta las averías producidas en los puertos de los Passport y DPN donde se conectan los routers.

Otra de las fuentes utilizadas por el Sistema de Gestión es la Supervisión de Accesos a Red.

Para ello se utiliza, normalmente, la herramienta de Nortel, Network Management System (NMS) que permite extraer información de una serie de equipos, destinados a dar acceso autorizado a una red determinada.

Existen un conjunto de servidores de primer nivel que se encargan de recibir de distintas áreas, los datos de supervisión (Alarmas).

Estos servidores de primer nivel están distribuidos por zonas geográficas, o estar distribuidos por cualquier otra línea estratégica corporativa, de las cuales resultan más idóneas a los requerimientos técnicos para generar alarmas:

En una distribución por zona geográfica, una posible distribución tradicional, podría resultar, como sigue a continuación:
–Norte
–Noroeste
–Nordeste
–Sur
–Centro
–Sudeste

Para el Sistema de Gestión de Incidencias existe una o varias máquinas, que reciben alarmas de los 6 nodos geográficos previamente mencionados (cardinales).

A través de estas máquinas se recogen todas las alarmas relacionadas con averías o problemas en la línea de acceso.

3.Módulo de Correlación de los Módulos anteriores; Gestión de Routers y de Acceso a Red. Este módulo, intenta relacionar ciertos aspectos gestionables del módulo de Gestión de Routers y de Gestión de Acceso a Red, e interrelacionarlos entre ellos, identificando las distintas correlaciones existentes entre ambos.

Una vez recibidas las alarmas en cada uno de los módulos anteriores; Gestión de Routers y Gestión de Red, se reenvían al módulo de Correlación de Alto Nivel (Por ejemplo Netcool).

En este módulo se realizan diversas tareas:
–Centralización de alarmas en un servidor (omnilan)
–Filtrado de alarmas
–De duplicación de alarmas
–Correlación de alarmas

De todas las tareas antes mencionadas, la de correlación de alarmas es la de mayor complejidad. Para implementarla se ha utilizado 2 productos del fabricante netcool:
–Object Server, es el que recibe, filtra y duplica las alarmas. Además es el que proporciona el interfaz a los diferentes usuarios del Sistema (administradores del Servicio) para que puedan visualizar sus alarmas.
–Impact Server, es el que lleva a cabo la correlación y es el que procesa el impacto de las alarmas recibidas.

A modo de ejemplo, una vez recibida en el object server una alarma de caída de un puerto en un passport, se procesa esta alarma en Impact y mediante el acceso al Inventario se añade a la alarma información diversa como, nombre del router, nombre del cliente afectado, teléfono de contacto, etc.

4.Módulo de Inventario que contiene una base de datos de diversa índole de todos los elementos gestionados.

El Sistema de Gestión es capaz de enriquecer los eventos que llegan al sistema.

Para ello era necesario disponer por un lado de un sistema de correlación, que en este caso sea Impact, y por otro, es necesario disponer de una base de datos de inventario.

Por tanto, dentro del Sistema de Gestión, se ha incluido un módulo que constituye el inventario de la planta de Routers que forman parte del Servicio.

Adicionalmente, hay que indicar que este Inventario es el punto de partida a la hora de realizar la provisión del Router en el Sistema de Gestión.

La información de la planta está organizada 6 tablas relacionadas:
–Router.
–Cliente.
–Backup.
–Gestion.
–Centro.

5.Módulo de la Integración con el sistema de ticketing corporativo

INDICADORES Y MÉTRICAS DE LOS PROCEDIMIENTOS DE GESTIÓN DE LAS INCIDENCIAS.

Indicadores y métrica
Nº total de incidentes
Desglose de incidentes por fase
Nº incidentes acumulados
Nº y % incidentes graves
Tiempo medio de resolución de incidentes
%incidentes en pro del tiempo de respuesta del SLA
Coste medio por incidente
Nº de incidentes reabiertos y su relación con el total
Nº y % categorizados incorrectamente
Nº y % asignados incorrectamente
% incidentes gestionados en el plazo acordado
Nº y % incidentes procesados por agentes del service desk
Nº y % incidentes resueltos de forma remota
Nº de incidentes clasificados por modelos
Desglose de incidentes por hora del día

Indicadores

Un indicador, debe de presentar una serie de aspectos que no deben de dar lugar a interpretaciones diferentes, por ello, se ha seleccionado los siguientes aspectos a tener en cuenta a la hora de diseñar un indicador:
–Selección del indicador.
–Denominación del indicador.
–Forma de cálculo.
–Forma de representación.
–Definición de responsabilidades.
–Definición de umbrales y objetivos.

2.3.1. Aislamiento y diagnóstico de incidencias

Dentro de un proceso de aislamiento y diagnóstico de incidencias, existe otro proceso de identificación y análisis de la solución, para ello, tenemos que analizar una serie de fases en el proceso de aislamiento, diagnóstico y resolución de incidencias.

En cada fase o etapa de cada fase en la resolución de incidencias, la discusión o el debate sobre el problema, pueden abrir o esclarecer nuevos caracteres que eran completamente desconocidos para el equipo de soporte y la organización, los cuales, obligan a redefinir el problema.

En la siguiente fase del proceso de resolución de incidencias, estamos en la del establecimiento de las posibles casusas.

En esta fase del proceso, realizamos una análisis de las posibles causas que hayan podido desembocar en la incidencia que se adolece, tratando siempre de eliminar aquellos riesgos o causas, que no aporten datos suficientes al problema en cuestión o bien, no existe una relación de causalidad – efecto con el problema en cuestión.

Este tipo de análisis, filtra las causas que no aportan utilidad ni clarifican las posibles causas del problema, delimitando el campo de acción y atención del equipo de soporte y a la organización, con respecto al problema.

En esta fase, es muy importante, establecer los criterios que se vayan a seguir para eliminar aquellas causas que no aporten nada sustancial a la incidencia.

Una vez establecidas e identificadas las posibles causas del problema, se procede a un segundo filtro sobre la idoneidad de las posibles causas que se han determinado como posibles del problema.

La fase de prueba de las posibles causas, resulta determinante filtrar nuevamente aquellas causas más probables, que proporcionen mayor información, y que estén más expuestas a ser la causa o causas efectivas del efecto negativo del problema generado.

Tras pasar la fase de la prueba de las causas más probables, establecemos la fase de verificación de la causa real del problema.

En la fase de verificación de la causa real del problema, nos aseguramos de que realmente la causa real del problema, pertenece directamente al curso causal de la incidencia, siendo esta, la causa real derivado de un riesgo distinto.

Las fases de planificación, comprobación y documentación, son las últimas fases del proceso de resolución de incidencias, donde se cierra la causa o causas reales que han provocado la incidencia, y su solución o soluciones, para solventar el problema.

En la identificación y análisis de las distintas fases del proceso de resolución de incidencias, cabe destacar un papel muy importante y predominante, sobre las herramientas básicas para la resolución de problemas.

A continuación, se va a describir básicamente una serie de herramientas básicas (a excepción del diagrama de Ishikawa, que será un apartado independiente y exclusivo para dicha herramienta) dentro del proceso de identificación y análisis del proceso de resolución de incidencias, las cuales serán muy útiles en la tarea.

Definición del problema

Para definir claramente un problema, es preciso y vital, invertir gran cantidad de tiempo y esfuerzo en mejorar la comprensión del problema, antes de ir directamente a él.

Para la comprensión del problema desde diferentes puntos de vista, es necesario pasar por una serie de criterios, que seguramente y con total probabilidad, mejoren nuestra percepción del mismo, definiéndolo y enmarcándolo dentro de su ámbito y alcance correcto.

Los criterios a seguir podrían ser:
1.Reformulación del problema: Los problemas, llevan implícitos una serie de palabras, que conllevan unos significados, los cuales desempeñan un papel importante a la hora de percibir el problema, es decir su ámbito y alcance.
2.Consideración y cuestionamiento de los supuestos: Como es bien sabido, casi todos, por no decir la totalidad de ellos, vienen con muchísimas hipótesis implícitas, lo cuáles muchos de ellos, puede ser erróneos e inducir a una posible solución del problema inadecuada o inexacta.

Uno de los primeros pasos a seguir para resolver y aclarar estás hipótesis erróneas, es hacerlas explícitas, incluso las hipótesis más obvias, es decir, todas aquellas que queden afianzadas por asunción. Esto aportará más claridad al problema.

Pensar en las formas o maneras de que un supuesto válido en concreto, podría no ser válido, podría llevarnos a darnos cuenta de que muchos de los supuestos malos, son auto-impuestos.

Por ello, pensar en sus formas no válidas y sus consecuencias, podría proporcionarnos un valor sorprendente, sobre aquellos supuestos auto-impuestos. Esto ayudará con poco de control, a despejar aquellos supuestos de este tipo.

3.Descomposición del problema hacia arriba: Tenemos que tener en cuenta, que cada problema, es una pieza más pequeña, de un problema de unas dimensiones mayores.

A veces, y con cierta frecuencia, se tiende a no observar el problema de una vista más general, tan solo se tiende a resolver el problema acotado, en vez de pensar de que puede ser parte este problema, o que intención hay detrás de este problema.

Otro enfoque aparte de pensar dicho problema como parte de algo más, las intenciones que hay detrás, es la utilización de términos con un significado de mayor alcance, es decir, más amplio que las propias palabras que definen el problema en sí.

Probablemente, esto nos proporcione una mayor visión más generalizada del problema, y nos ayude a determinar de que puede formar parte este problema, o descubrir sus intenciones, las cuales nos podrían servir como medio vehicular para llegar a un nivel del problema más amplio, del cual forma parte este " pequeño " problema.

En sintonía con lo anteriormente descrito, podemos percibir el problema, como una especie de síntoma o parte de un problema más profundo, del simplemente técnico o procedimental.

4.Descomposición del problema hacia abajo:

En contraposición con lo expuesto en el apartado anterior, la descomposición de un problema mayor en problemas más pequeños, puede proporcionar un conocimiento más profundo sobre el problema en sí.

Esta descomposición en problemas más pequeños, es especialmente útil, cuando nos sobrepasa un problema de ciertas dimensiones, que no sabemos manejar adecuadamente, y nos resulta muy desafiante.

Esta sería una buena forma de acatar el problema.

Al igual que en el apartado anterior, pero de forma contraria, nos resultaría muy útil, el empleo de palabras más estrictas para la definición del problema, ya que delimitaría el ámbito de actuación y lo reduciría drásticamente, reduciendo la vaguedad de los términos empleados de manera amplia.

5.Emplear múltiples perspectivas al problema:

El hecho de observar el mismo problema, desde muchas perspectivas diferentes, es uno de los grandes métodos a la hora de definir un problema y de su resolución, ya que te proporciona, diferentes caminos posibles, que de otro modo, hubieran pasado por alto, al emplear una visión restrictiva o acotada del problema en sí.

La clave está en encontrar diferencias y similitudes de las diferentes visiones o perspectivas que puedas imaginar.
6.Uso de un lenguaje efectivo:

Es bien sabido, que las construcciones del lenguaje son un activo muy importante para la elaboración apropiada de un problema, ya que se debe de asumir que existen multitud de soluciones al mismo problema.
El sentimiento de esperanza ayuda a tu cerebro a encontrar soluciones.

También es altamente recomendable y de hecho está demostrado, que los planteamientos positivos, no sólo a la hora de definir un problema en concreto, sino en general, son más motivadores y te ayudan a encontrar una solución u objetivo real, que está detrás del problema.

En toda descripción de un problema, existen una serie de elementos que deben de seguirse al paso, para poder completar con éxito el proceso de descripción del problema.

Monitoree los procesos más importantes y los márgenes deseables de eficiencia.

En el plano de los planteamientos o pensamientos negativos, requieren de más poder de convicción de las posibles soluciones u objetivos reales, es decir, mayor poder cognitivo para poder procesarlas adecuadamente.

Esto obviamente, no significa que al final del camino, por muy duro que parezca, se encuentra la solución u objetivo real, sino que es muy altamente probable esos pensamientos o planteamientos negativos, hagan fracasar tu línea o estrategia del planteamiento de definición del problema y no te ayudará a encontrar la solución real.

Una de las formas más poderosas de definición del problema, es decir su redacción, es continuamente hacer preguntas sobre qué acción o acciones podría tomar para lograr el objetivo u objetivos planteados.
Nuestro cerebro está diseñado para sobrevivir. Tan solo obviar el problema, o reducirlo a la mínima expresión, resultan excusas para no pensar.

1.Emplear una fuerte carga emotiva: De todo lo que llevamos visto para definir el problema, otro de los aspectos muy interesantes para verdaderamente encontrar un planteamiento para el problema.

El hecho de mantener un planteamiento o razonamiento verdaderamente excitante, estarás en una mejor posición de creatividad para poder afrontarlo con éxito, y si de lo contrario el problema es aburrido, encuentra la forma y el tiempo suficiente para añadirlo vigor, haciéndolo genuino e único, creando así una fuerte carga emotiva para tu cerebro, que realmente más tarde serás recompensado.

2.Invertir el problema: Es una de las técnicas más usadas, para intentar desatascar un problema.

Una de las opciones más adecuadas para generar planteamientos o soluciones al problema, sería pensar en cómo darle la vuelta al problema, por ejemplo si deseas ganar en algo o ser competitivo en algunos servicios, hay que pensar en todo aquello que te haga perder o no ser competitivo.

Esto último, es importante para comenzar a darle la vuelta al problema desde ese punto de vista contrario, ya que a priori puede parecer enrevesado y poco atractivo, pero puede ayudarte a obtener otra dirección de cuál es realmente el problema para conseguir definir el problema original y hacerte descubrir soluciones reales al problema originario.

Establecimiento de las posibles causas

Investigar las causas y circunstancias del problema, suele resultar más productivo que intentar solucionarlo inmediatamente.

Este planteamiento resulta muy útil ante problemas demasiados vagos en sí mismos.

El hecho de formularse preguntas uno mismo, sobre cuándo fue la última vez que funcionó el sistema, o cuanto se sabe del problema hasta el día de hoy, o bien los límites del problema.

El definir el problema y establecimiento de las posibles causas, reuniendo hechos constatables y formulándose preguntas parecidas a las anteriores, resulta ser un problema definido, que no es más que otra cosa que un problema a mitad de camino de ser resuelto de inmediato.

Un problema definido, no es en realidad otro problema más.

Para el establecimiento de las posibles causas de un problema en concreto, es investigar para descubrir las causas raíz del problema del que se adolece.

En una primera toma de contacto con el problema, tienden a aparecer como grandes obstáculos que no tienen unos límites claros.

Por ello, un análisis correctamente realizado, se debe de concentrar inmediatamente en el problema, no en sus efectos y supuestas causas que lo provocaron, estableciendo una trayectoria clara y lógica, desde el reconocimiento del problema, al punto donde ocurre, pasando al punto del establecimiento de las posibles causas del problema, y finalmente, llegando a la causa raíz que ha originado el problema verdaderamente.
Llegados a este punto del establecimiento de las posibles causas, podemos empezar a analizar la cadena causal de circunstancias que han originado la causa del problema.
Una vez adentrados en la observación y búsqueda de las raíces del problema, en la mayoría de los casos, se tiene la sensación de que las causas del problema se expanden de una manera incontrolable en varias direcciones, resultando en un primer momento, como un gran obstáculo de una complejidad casi incontrolable.
Partiendo de la composición sobre el funcionamiento de las pruebas de las causas más probables, estas, como premisa fundamental en aras de la calidad y eficiencia en la determinación y prueba de las causas más probables que generaron el problema o incidencia, deben de seguir unas pautas de buenas prácticas para conseguir esos objetivos específicos.
Otra de las formas para reducir las causas posibles, es ignorar o eliminar aquella o aquellas, en las que no existen datos disponibles, que puedan dar certeza al origen del problema o a una posible causas o causas del mismo.
Para no caer en realizar procesos excesivamente exhaustivos en todas las raíces de las posibles causas o establecimientos, resulta necesario tener en cuenta:
–La causa de un problema, más de una causa raíz que lo ha originado.
–La causa de un problema, contribuya de forma exponencial a la aparición de muchos problemas.
–Si no se soluciona la causa o causas raíces, es muy probable, que el problema vuelva a surgir en el tiempo.
–Uno de los métodos más eficaces contra el establecimiento de la causa o causas de los problemas, es la PREVENCIÓN.

Teniendo plenamente identificadas las partes más adecuadas e idóneas para llevar a cabo una investigación más exhaustiva para el establecimiento de la causa o causas de un problema, es posible analizar las causas raíz con mayor detalle e influencia, sobre el estado futuro y el actual.

Partiendo de la composición sobre el funcionamiento de las pruebas de las causas más probables, estas, como premisa fundamental en aras de la calidad y eficiencia en la determinación y prueba de las causas más probables que generaron el problema o incidencia, deben de seguir unas pautas de buenas prácticas para conseguir esos objetivos específicos.

A continuación, se expone unas recomendaciones de buenas prácticas para conseguir la eficiencia deseada en la determinación y prueba de las causas más probables del problema o incidencia.

Dentro de un sistema de gestión de incidencias, podemos extraer ciertas pautas de recomendaciones de buenas prácticas, para una correcta actuación dentro de los diferentes procesos que pueden llevarse a cabo en el tratamiento de las incidencias y en su gestión.

Para ello, se va a describir a continuación una serie de recomendaciones de buenas prácticas, en el ámbito de la gestión de incidencias, que cubren prácticamente la totalidad del alcance que una incidencia puede tener efectos negativos y maliciosos, para la propia organización que presta los servicios, como para el cliente gestionado.

Procedimientos y responsabilidades de operación

–Supervisión de los servicios contratados a terceros
–Planificación y aceptación del sistema
–Protección contra software malicioso y código móvil
–Gestión interna de soportes y recuperación
–Gestión de redes
–Utilización y seguridad de los soportes de información
–Intercambio de información y software
–Servicios de comercio electrónico

Pruebas de las causas más probables

Teniendo ya identificadas las partes de las posibles causas más probables del problema, estamos en disposición de realizar un análisis más exhaustivo y con más detalle sobre las causas raíz con mayor incidencia sobre el problema.

En este apartado, se va a exponer un método con el que se profundiza en el problema, hasta llegar a la causa o causas más probables del citado problema.

Hablamos de la técnica de los 5 porqués, donde consiste en simplemente preguntar ¿Por qué? o preguntas similares como ¿Qué? ¿Dónde? ¿Cuándo? ¿Quién? Al menos 5 veces para probar las causas más probables del problema.

A continuación, expongo una tabla identificativa a modo de ejemplo:

¿Por qué?	No podemos fabricar la cantidad suficiente de repuestos por hora
¿Por qué?	Pérdida de oportunidades de producción
¿Por qué?	Pérdida de tiempo
¿Por qué?	Pérdidas en el tiempo del ciclo
¿Por qué?	Cargar la máquina demasiado tiempo
¿Por qué?	El operador debe caminar al menos 1.5 M hasta llegar al material

Hay que tener en cuenta también que la técnica de “los 5 porqués” es solo uno de los métodos y está diseñada para realizar un análisis rápido de problemas relativamente sencillos.

Es posible que este enfoque no sea adecuado para problemas más complejos.

Si no obtiene una respuesta clara de manera rápida, es posible que deba optar por técnicas de resolución de problemas más avanzadas.

Aquí se ha expuesto la técnica de los 5 porqués, pero existen muchas otras técnicas que son muy útiles para conseguir el mismo objetivo, como por ejemplo, el análisis de Pareto, el análisis de modo de falla y el diagrama de Ishikawa, que más adelante entraremos en materia.
Una vez ya determinado el análisis más detallado (un análisis de causa raíz), el cual resulta más útil para determinar la causa real del problema, se procede a la prueba de la causa o causas de los problemas que el análisis de la causa raíz ha determinado con más realismo y detalle.

El funcionamiento de las pruebas de las causas más probables del problema, se puede ejecutar siguiendo una composición muy particular, como por ejemplo:

1.Utilización de un traceroute, para encontrar rutas reales entre 2 equipos de monitorización, que han sido utilizadas para ejecutar las pruebas de la causa del problema, mediante las correspondientes alarmas.

2.Diversas capturas de pantalla, para la prueba y comprobación sobre la causa del problema, con el objetivo de si aporta información útil al proceso.

3. El código fuente si está disponible, para la realización de las correspondientes pruebas.

4.Realización de comprobaciones relevantes, tanto anteriores a la monitorización, como después de la misma.

5.Un análisis detallado de la configuración del equipamiento utilizado en la red telemática.

6.Un análisis DNS, para comprobar si los nombres de dominio, se resuelven correctamente, en caso de que se tenga acceso al exterior de la red telemática.

Documentación de procedimientos operativos (documentar y mantener los procedimientos de operación)

–Control de cambios operacionales (controlar los cambios en los sistemas y en los recursos).
–Segregación de tareas (segregar las tareas y las áreas de responsabilidad).
–Separación de los recursos para desarrollo y producción (la separación de los recursos para el desarrollo, prueba y producción es importante para reducir los riesgos).

Prestación de servicios (Garantizar que los controles de seguridad sean implementados, operados y mantenidos por la parte externa)

–Monitorización y revisión de los servicios contratados (las auditorias se deberían realizar a intervalos regulares).
–Gestión de los cambios en los servicios contratados (mantenimiento y mejoras en las políticas de seguridad de información existentes, así como la reevaluación de los riesgos).
–Se requiere una planificación y preparación avanzadas para garantizar la adecuada capacidad y recursos con objeto de mantener la disponibilidad de los sistemas requerida.
–Deberían realizarse proyecciones de los requisitos de capacidad en el futuro para reducir el riesgo de sobrecarga de los sistemas.
–Se deberían establecer, documentar y probar, antes de su aceptación, los requisitos operacionales de los nuevos sistemas.

Planificación de capacidades

–Se debería monitorizar el uso de recursos, así como de las proyecciones de los requisitos de las capacidades adecuadas para el futuro con objeto de asegurar el funcionamiento requerido del sistema.
–Aceptación del sistema
–Se deberían establecer criterios de aceptación para nuevos sistemas de información, actualizaciones y versiones nuevas. Se deberían desarrollar las pruebas adecuadas del sistema durante el desarrollo y antes de su aceptación.
–Se requieren ciertas precauciones para prevenir y detectar la introducción de código malicioso y códigos móviles no autorizados.
–El software y los recursos de tratamiento de información son vulnerables a la introducción de software malicioso como virus informáticos, gusanos de la red, caballos de troya y bombas lógicas.
–Los usuarios deberían conocer los peligros que puede ocasionar el software malicioso o no autorizado y los administradores deberían introducir controles y medidas especiales para detectar o evitar su introducción.
–Se deberían establecer procedimientos rutinarios para conseguir la estrategia aceptada de respaldo para realizar copias de seguridad y probar su puntual recuperación.
–Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, de acuerdo con la política acordada de recuperación.
–La gestión de la seguridad de las redes, de la seguridad de las redes, las cuales pueden cruzar las fronteras de la organización, exige la atención a los flujos de datos, implicaciones legales, monitoreo y la protección de datos.
–Podrían ser necesarios controles adicionales con el fin de proteger la información sensible que pasa por las redes públicas.

Controles de red

Se deberían mantener y controlar adecuadamente las redes para mantener y controlar adecuadamente las redes para protegerlas de amenazas y mantener la seguridad en los sistemas protegerlas de amenazas y mantener la seguridad en los sistemas y aplicaciones que utilizan las redes, incluyendo la información y aplicaciones que utilizan las redes, incluyendo la información en tránsito.

Seguridad en los servicios de red

Se deberían mantener y controlar adecuadamente las redes para protegerlas de amenazas y mantener la seguridad en los sistemas y aplicaciones que utilizan las redes, incluyendo la información en tránsito.

Los medios deberían ser controlados y físicamente protegidos

Se deberían establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizadas.

Gestión de soportes extraíbles (establecer procedimientos)

–Eliminación de soportes (de forma segura con procedimientos formales).
–Procedimientos de utilización de la información (manipulación y almacenamiento).
–Seguridad de la documentación de sistemas (se debe proteger contra accesos no autorizados).
–Soportes físicos en tránsito (proteger los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte).
–Mensajería electrónica (proteger adecuadamente la información contenida en la mensajería electrónica).
–Sistemas de información empresariales (políticas y procedimientos con el fin de proteger la información asociada con la interconexión de sistemas).

Seguridad en comercio electrónico:

Se debería proteger la información involucrada en el comercio electrónico que pasa por redes públicas contra actividades fraudulentas, disputas por contratos y divulgación o modificación no autorizadas.

Seguridad en transacciones en línea

–Se debería proteger la información implicada en las transacciones en línea para prevenir la transmisión incompleta, enrutamiento equivocado, alteración, divulgación, duplicación o repetición no autorizada del mensaje.

Seguridad en información pública

Se debería proteger la integridad de la información que pone a disposición en un sistema de acceso público para prevenir modificaciones no autorizadas

Verificación de la causa real

En la verificación de la causa real se requiere de métodos eficientes para la captación de información, para el caso se recomienda la hoja de verificación o de registro.

La hoja de verificación, es un instrumento especialmente diseñado para la recopilación de datos, cuya función consiste en hacer fácil y ameno el análisis de dichos datos.

Esto facilita enormemente, el posterior análisis que deba de realizarse en aquellos factores principales, que influyan en un problema específico.

Tras un proceso de investigación y diagnóstico exhaustivo, habrá procesos que tendrán que ser nuevamente filtrados, para poder encontrar la causa o causas reales que originaron el problema o incidencia.

Las técnicas utilizadas para el aislamiento, diagnóstico y resolución de incidencias son las siguientes:

Hoja de recogida de datos

La Hoja de Recogida de Datos también llamada Hoja de Registro, Verificación, Chequeo o Cotejo.

Sirve para reunir y clasificar las informaciones según determinadas categorías, mediante la anotación y registro de sus frecuencias bajo la forma de datos.

Una vez que se ha establecido el fenómeno que se requiere estudiar e identificadas las categorías que lo caracterizan, se registran estas en una hoja, indicando la frecuencia de observación.

Lo esencial de los datos es que el propósito este claro y que los datos reflejen la verdad.

La hoja de recogida de datos, posee múltiples funciones, pero la más importante y esencial que le proporciona un verdadero potencial a estas hojas de datos, es su poder analítico y automático, a la hora de estructurar los datos, además de recopilarlos y organizarlos.

De modo general las hojas de recogida de datos tienen las siguientes funciones:
–De distribución de variaciones de variables de los artículos producidos (peso, volumen, longitud, talla, clase, calidad, etc.)
–De clasificación de artículos defectuosos.
–De localización de defectos en las piezas.
–De causas de os defectos.
–De verificación de chequeo o tareas de mantenimiento.

Una vez que se ha fijado las razones para recopilar los datos, es importante que se analicen las siguientes cuestiones:
–La información es cuantitativa o cualitativa.
–Cómo se recogerán los datos y en qué tipo de documentos se hará.
–Cómo se utilizará la información recopilada.
–Cómo se analizará.
–Quién se encargará de la recogida de datos.
–Con qué frecuencia se va a analizar.
–Dónde se va a efectuar.

Una secuencia de pasos útiles para aplicar esta hoja en un Taller es la siguiente:
1.Identificar el elemento de seguimiento. Ejemplo: la cantidad de fallas de las maquinas.
2.Definir el alcance de los datos a recoger.
3.Siguiendo el ejemplo anterior, la hoja de recogida de datos se puede usar para verificar todas las maquinas similares.
4.Fijar la periodicidad de los datos a recolectar (cada hora, diariamente, semanalmente, etc.)
5.Diseñar el formato de la hoja de recogida de datos, de acuerdo con la cantidad de información a recoger, dejando un espacio para totalizar los datos, que permita conocer: las fechas de inicio y término, las probables interrupciones, la persona que recoge la información, fuente etc.

Cabe indicar que este instrumento se utiliza tanto para la identificación y análisis de problemas como de causas.

Diagrama de pareto

Es una herramienta que se utiliza para priorizar los problemas o las causas que los genera.
El Dr. Juran aplicó este concepto a la calidad, obteniéndose lo que hoy se conoce como la regla 80/20.

Según este concepto, si se tiene un problema con muchas causas, podemos decir que el 20% de las causas resuelven el 80% del problema y el 80% de las causas solo resuelven el 20% del problema.

Procedimiento para elaborar el diagrama de Pareto:
1.Decidir el problema a analizar.
–Seleccionar los problemas que se desea investigar (Ejemplo: Objetos defectuosos.)
–Decidir los tipos de datos a analizar y como clasificarlos (Ejemplo: tipo de defecto, localización, proceso, máquina, etc.).
–Definir el método de recolección de datos.

2.Diseñar una tabla para conteo o verificación de datos, en el que se registre los totales.

3.Recoger los datos y efectuar el cálculo de totales.

4.Elaborar una tabla de datos para el diagrama de Pareto con la lista de ítems, los totales individuales, los totales acumulados, la composición porcentual y los porcentajes acumulados.

5.Jerarquizar los ítems por orden de cantidad llenando la tabla respectiva.

6.Dibujar dos ejes verticales y un eje horizontal.

Marque en el eje vertical izquierdo con una escala de cero hasta el total general (cantidad de ítems acumulados). A continuación marcar el eje vertical derecho con una escala de 0% hasta 100%.

Luego divida el eje horizontal en un número de intervalos igual al número de ítems clasificados.

7.Construya un gráfico de barras en base a las cantidades y porcentajes de cada ítem.

8.Dibuje la curva acumulada.
En esta curva, se marca los valores acumulados (Total acumulado o porcentaje acumulado) en la parte superior, junto al lado derecho de los intervalos de cada ítem, finalmente cuando se tenga todos los valores representados, se unen todos los puntos con una línea contínua, la cual dibujará la curva acumulada que nos interesa.

9.Escribir cualquier información necesaria sobre el diagrama (título, unidades, etc.) sobre los datos (periodo de tiempo, número total de datos, etc.)

Para determinar las causas de mayor incidencia en un problema se traza una línea horizontal a partir del eje vertical derecho, desde el punto donde se indica el 80% hasta su intercepción con la curva acumulada.

De este punto trazar una línea vertical hacia el eje horizontal.
Los ítems comprendidos entre esta línea vertical y el eje izquierdo (de cantidades acumuladas) constituyen las causas cuya eliminación resuelve el 80% del problema.

El histograma

El histograma, es un instrumento muy potente que nos sirve como forma de síntesis entre las cosas que ocurren o aquellos eventos relacionados entre sí.
El histograma, es una herramienta muy útil para mejorar procesos y servicios, ya que identifica aquellos patrones que dan lugar a la ocurrencia de dichas cosas o eventos.

El histograma se usa para:
–Obtener una comunicación clara y efectiva de la variabilidad del sistema.
–Mostrar el resultado de un cambio en el sistema.
–Identificar anormalidades examinando la forma.
–Comparar la variabilidad con los límites de especificación.

Procedimiento de elaboración:
1.Reunir datos para localizar por lo menos 50 puntos de referencia.
2.Calcular la variación de los puntos de referencia, restando el dato del mínimo valor del dato de máximo valor.
3.Calcular el número de barras que se usaran en el histograma (un método consiste en extraer la raíz cuadrada del número de puntos de referencia).
4.Determinar el ancho de cada barra, dividiendo la variación entre el número de barras por dibujar.

5.Calcule el intervalo o sea la localización sobre el eje X de las dos líneas verticales que sirven de fronteras para cada barrera.
6.Construya una tabla de frecuencias que organice los puntos de referencia desde el más bajo hasta el más alto de acuerdo con las fronteras establecidas por cada barra.
7.Elabore el histograma respectivo.

Los histogramas más fáciles de entender tienen no menos de 5 barras y no más de 12.
De acuerdo con la gráfica obtenida podemos apreciar distintos tipos de histograma: normal, bimodal, de dientes rotos o de peine, cortado y distorsionado.

Diagrama de dispersión

El diagrama de dispersión es una herramienta de análisis la cual representa en forma gráfica la relación existente entre dos variables pudiendo observar la dependencia o influencia que tiene una variable sobre la otra, permitiendo visualizar de forma gráfica su posible correlación.

Conocidos también como gráficos XY es una herramienta de análisis utilizado generalmente en el área de la gestión de calidad con el objeto de encontrar las relaciones de las causas que producen un efecto.

Tal y como hemos citado en la definición anterior el diagrama de dispersión nos indica la relación existente entre dos variables, y por lo tanto si traducimos estas dos variables a grupos de datos, podemos relacionar grupos de datos con el objeto de verificar o averiguar que existe una relación entre ambos y como es esta relación de forma aproximada.

Los diagramas de dispersión se emplean para:
–Observar el grado de intensidad en la relación entre dos variables, esta relación puede ser entre un efecto y una de las supuestas causas que lo producen o para ver la relación entre dos causas que provocan un mismo efecto.
–Visualizar rápidamente cambios anómalos.
–Analizar determinadas cuestiones mediante comparaciones.

Modo de aplicación
Los pasos a seguir para construir un diagrama de dispersión son:
1.Seleccionar las 2 variables que se van relacionar.
2.Establecer una hipótesis de la posible relación entre ambas.
3.Construir una tabla que nos relacione los valores de ambas variables por parejas. Si no disponemos de dichos datos será necesario realizar una toma.
4.Dibujar el diagrama poniendo una variable en cada uno de los ejes cartesianos (x,y) con una escala de valores que se ajuste a los datos que se dispone.
5.Representar en el gráfico cada par de valores por un punto.
6.Encontrar la correlación analizando la tendencia de la nube de puntos y la correlación entre las variables.

Hoy en día gracias a la informática disponemos de programas basados en hojas de cálculo como Excel, Numbers o Calc que te permiten realizar rápidamente un diagrama de dispersión con solo introducir los datos de las variables.
Interpretación del diagrama de dispersión

Una vez que hemos realizado el diagrama de dispersión la forma que adquiera la nube de puntos nos permitirá analizar la relación entre las 2 variables o grupos de datos, pudiendo obtener las siguientes figuras e interpretaciones:
–Correlación positiva - Se observa como la nube de puntos obtenida adquiere una forma de recta creciente, cuando los puntos de la nube se encuentra próximos a la recta se le conoce como fuerte, en el caso que se encuentren distantes a la recta es conocida como débil.

Por ejemplo la relación existente entre la altura y el peso de una persona es positiva a mayor altura mayor peso.
–Correlación negativa - Al contrario del caso anterior se observa como la nube de puntos obtenida adquiere una forma de recta decreciente, cuando los puntos de la nube se encuentra próximos a la recta se le conoce como fuerte, en el caso que se encuentren distantes a la recta es conocida como débil.
Por ejemplo la relación existente para los fumadores entre el número de paquetes de tabaco al mes y los años de vida es negativa dado que a mayor cantidad de tabaco fumado menor esperanza de vida.
–Correlación compleja - La nube de puntos obtenidas adquiere forma de curva, elipse u otra forma geométrica.
–Correlación nula - Se observa una distribución de la nube de puntos con una forma circular, indicándonos la no existencia de relación entre ambas variables.
Por ejemplo la relación existente entre el color de los ojos y el tamaño del pie es nula.

Análisis por estratificación

Este es un instrumento que nos permite pasar de lo general a lo particular en el análisis de un problema.

Se puede obtener información más útil estratificando los datos de defectos que se registran en cada turno de trabajo, y observar así si hay diferencias de un turno con respecto a otro.

Ello servirá de base para un análisis más profundo, en el turno donde se registre la mayor dispersión de los datos.

Herramientas

En este apartado, se va a describir brevemente una serie de herramientas para el diagnóstico y la resolución de incidencias en redes telemáticas, que interconectan redes privadas con redes públicas.
Estas son las que vamos a describir su función y concepto:
1.La herramienta NIMBA.
2.El perfomance viewer.
3.SIGA.
4.Vista trouble shooter.

La herramienta NIMBA
Con esta herramienta, podemos hacer test de diagnósticas a unos determinados circuitos, además de poder buscar datos sobre su localización, vlans, etc.
El poder de esta herramienta para realizar diferentes test sobre diferentes circuitos, junto con las opciones adicionales que posee, la convierte en una herramienta de extraordinaria potencia y alcance, para redes complejas y heterogéneas.

La herramienta perfomance viewer
Esta herramienta es de mucha utilidad, ya que proporciona gráficos de tráfico presentables al cliente, para poder monitorear en un determinado período de tiempo, el ancho de banda consumido o desde donde se está generando un alto tráfico.
Es una herramienta que se utiliza cuando el tráfico pasa a través de un equipo Passport. En el resto de tráfico como por ejemplo de LAN o punto a punto, se utiliza otras herramientas (MRTG).
En las gráficas que se presentan en esta herramienta, el parámetro RX, significa lo que envía el router y lo que recibe el Passport, y TX viceversa.

La herramienta SIGA
El HelpDesk Nivel de Red es una herramienta adaptada a necesidades más avanzadas y que es útil cuando no se ha podido diagnosticar la avería en los niveles anteriores.

Está orientada a operadores con un alto grado de conocimientos técnicos.
Este tipo de herramienta, se diagnostica por ejemplo el servicio de ADSL.

La herramienta vista TROBULE SHOOTER
Es una herramienta importante para los centros de gestión. Es una herramienta que funciona con las colectoras de los routers en el sistema de monitorización de equipamiento.

2.3.2. Los planes de contingencia

Introducción
1.Errores habituales en empresas.
2.Eventos que necesitan planes de continuidad.
3.¿Por dónde empezar?
4.Actividades principales en un BCP (Business Continuity Planning).
5.Clasificación de las operaciones de la empresa.
6.Análisis de impacto (Business Impact Analysis BIA).
7.Administración de la continuidad del negocio.
–Los intentos de ataque por Internet muestran un crecimiento anual del 64%.
–Una empresa media habrá experimentado 32 ataques a la semana durante los últimos seis meses.
–Dos de cada cinco compañías afectadas por un desastre se ven obligadas a cerrar en un plazo de 5 años.
–En los últimos 5 años han ocurrido más desastres a gran escala que en toda la historia reciente de las empresas.

Casi el 90% de los pequeños negocios no tienen un plan de continuidad.
–Sólo el 43% de las empresas que sufren un desastre se recuperan lo suficiente como para continuar funcionando.
–De las que reabren, sólo el 29% siguen operativas dos años después.
–El 93% de las empresas que pierden sus centros de datos durante más de 9 días, quiebran en el primer año después del desastre.
El 72% de todos los negocios se encuentra en una de estas situaciones:
–No tienen Plan de Continuidad de Negocio
–Si lo tienen, nunca lo han probado
–Si lo han probado, falló

Los mayores errores de las empresas

–Creer que la Seguridad de la Información y la Recuperación de Desastres son temas importantes, pero pensar que son importantes para que los administre otro.
–Pretender que desaparezca el problema simplemente ignorándolo.
–Usar la tecnología para reparar y no para prevenir.
–Ignorar el valor de la información y de la reputación de la empresa.
–Pensar: “eso no me pasará a mí”

No entender la relación entre Continuidad de Negocio y Plan de Recuperación de Desastres.
–Pensar que la Continuidad de Negocio y la Recuperación de Desastres es únicamente responsabilidad del departamento de informática.
–Diseñar estrategias de recuperación sin que se involucre la empresa
–Ver la Continuidad de Negocio y la Recuperación de

Desastres como un gasto y no como una inversión.
–Fallar al diseñar, desarrollar e implementar una Estrategia

Corporativa para la Continuidad de Negocio.

Eventos que necesitan planes de continuidad

–Factores de riesgo destacables:

·Desastres Naturales

·Fuego

·Fallo de alimentación
·Ataques terroristas: Después de los ataques del 11S ha dejado de ser una hipótesis lejana.

·Interrupciones organizadas o deliberadas

·Robo

·Fallo de Sistema o equipamiento

·Error humano

·Virus

·Sabotaje por parte de empleados

·Testeo: Un fallo en las pruebas de un nuevo sistema informático puede dar lugar a la pérdida irremisible de la base de datos de la empresa.

¿Por dónde empezar?

–Debemos saber qué queremos proteger. No pasarnos por exceso ni por defecto.

–Es imposible prepararse de forma adecuada para un desastre si se desconoce el impacto que una interrupción puede tener en la empresa.

–La Planificación de la Continuidad del Negocio (Business Continuity Planning BCP) es un método estándar por el que las empresas planean la continuidad de sus operaciones en caso de emergencia.

Un BCP implica varios pasos, que incluyen un Análisis de Impacto en el Negocio (Business Impact Analysis BIA) y un Análisis de Riesgos (Risk Assessment RA).

Actividades principales en un BCP

–BIA Completo (Business Impact Analysis)

–Desarrollar una estrategia de respuesta/recuperación

–Preparar Equipos y Listas de contacto

–Identificar el equipamiento crítico, fabricantes y documentación

–Documentar los planes

–Practicar los planes
Clasificación de las operaciones de la empresa

–Una parte fundamental de la planificación de continuidad de los procesos de la empresa es precisamente identificar y clasificar esos procesos u operaciones.

Estos procesos se pueden clasificar en:

–Críticos:

–Vitales:

–Sensitivos:

–No críticos:

Procesos críticos y vitales

–Críticos:

·Sus funciones no pueden ser ejecutadas a menos que sean reemplazadas por recursos idénticos.

·No se pueden utilizar métodos manuales.

·El coste de su interrupción es muy alto.

–Vitales:

·Sus funciones pueden ser ejecutadas manualmente durante un periodo corto.

·Tienen una mayor tolerancia a las interrupciones que los procesos críticos.

·Los costes de su interrupción son menores.

Procesos sensitivos y “no críticos”

–Sensitivos:

Sus funciones pueden ser ejecutadas manualmente durante un periodo relativamente largo.

Mientras se hace manualmente se requiere personal adicional.

El coste de su interrupción es medio.

–No críticos:
·Sus funciones pueden ser interrumpidas durante un periodo relativamente largo, con poco o ningún coste.

Análisis de impacto (BIA)

–El Análisis de Impacto da lugar a la distinción entre procesos críticos y no críticos en las funciones y actividades de la empresa.

–Para cada proceso crítico se asignan dos valores:

·Recovery Point Objective (RPO): La latencia aceptable de los datos que se deben recuperar. También podemos definirlo como la cantidad de datos cuya pérdida es tolerable.

·Recovery Time Objective (RTO): La cantidad de tiempo aceptable para restaurar la función.

Hemos visto lo importante que puede ser para una empresa la recuperación lo antes posible de los procesos de negocio y de la información relacionada.

Para la recuperación de la información es imprescindible contar con una estrategia de realización de copias de seguridad de la misma.

Entre las estrategias básicas tenemos:

–Copia de Seguridad Completa.

–Copia de Seguridad Incremental.

–Copia de Seguridad Diferencial.

–Combinación de alguna de las tres anteriores.

Administración de la continuidad del negocio
–Podemos definir la Administración de la Continuidad del Negocio (Business Continuity Management – BCM) como el proceso de gestión que identifica las amenazas potenciales para una organización, analiza el impacto de esas amenazas en los procesos de negocio y proporciona un marco para el desarrollo de la capacidad de respuesta que salvaguarde sus intereses.

BCM / BCP / DRP

–El BCM considera la administración de la continuidad del negocio como parte de un proceso.

–El BCP es un plan dirigido a los procesos del Negocio.

–El DRP es un plan específico para la tecnología de la Información.

Beneficios de BCM I

–Prever y mitigar el desastre de forma positiva, logrando mantener la continuidad de la empresa su reputación, credibilidad y la fidelidad del cliente.

–Recuperar en forma efectiva en el tiempo a la organización, reduciendo los impactos por el evento de la contingencia.

–Identificar las prioridades del negocio, alineándolas al BCM con la sinergia de la arquitectura de TI proporcionando a la organización elementos de competitividad en el ambiente de los negocios y de la industria.

–Contar con un voto de confianza por parte de los accionistas de la organización.

–Delimitar la severidad del daño y riesgos hacia la salud y bienestar de los empleados.

Beneficios de BCM II

–Minimizar la magnitud de la interrupción sobre los procesos críticos ante eventos inesperados.

–Contar con los elementos regulatorios y jurídicos para enfrentar juicios o demandas de terceros o gubernamentales.

–Contar con un BCM alineado a los estándares internacionales que permita cubrir los lineamientos solicitados por cada uno de ellos.

–Contar con personal entrenado para el manejo de crisis y recuperación de las operaciones.

–Asegurar que los registros vitales estén disponibles ante el evento de contingencia.

–Contar con la mayoría de los procedimientos probados.

–Minimizar la dependencia de los servicios informáticos ante el evento de la contingencia.

2.3.3. Procedimientos sistemáticos de resolución de incidencias

En los procedimientos sistemáticos de resolución de incidencias, están asociados a una serie de buenas prácticas dentro de un sistema de gestión de incidencias.

Como se ha podido estudiar en apartados anteriores referente a los sistemas de gestión de incidencias, junto con los procedimientos o fases que se incluyen en cada uno de ellos, en este apartado, se va a destacar especialmente, dentro de los procedimientos sistemáticas de resolución de incidencias, su seguimiento y la ficha de cumplimentación en el desarrollo de los procedimientos, junto con los documentos que se deben de acompañar con el check list.

Sistema de seguimiento

Organo responsable del seguimiento	Mecanismo /procedimiento para realizar el seguimiento	Periodicidad establecida	Indicador de seguimiento	Estandares establecidos

Documentos a incorporar en el check list

Documentos a incorporar en el Check-list	Si	No	No procede
Normativa de funcionamiento de la Comisión Coordinadora de resolución de incidencias (funciones)			
Normativa de funcionamiento de las Subcomisiones de la coordinadora de resolución de incidencias (funciones)			
Documento estandarizado para registrar las alteraciones y modificaciones entre lo planificado y lo realizado en el procedimiento de resolución de incidencias			
Canales de comunicación formales para hacer llegar las incidencias (web, buzón de sugerencias…)			
Protocolo de actuación ante las incidencias			
Registro del archivo histórico de las incidencias y resoluciones			
Procedimiento de reajuste y adaptación de los protocolos de actuación de las incidencias			

Etapas o fases en el desarrollo de los procedimientos de resolución de incidencias sistemáticos

Etapas o fases en el desarrollo del procedimiento	Cumple	No cumple
Existe algún órgano gestor (comisión coordinador del programa, subcomisiones) en donde se recogen las incidencias surgidas en el desarrollo de los procedimientos de resolución de incidencias.		
El órgano gestor da salida a las incidencias distribuyéndolas por destinatario (receptor, encargado de solucionarla).		
Existencia de protocolos de actuación para solventar incidencias.		
Emisión de la resolución.		
Notificación de la resolución adoptada al órgano gestor.		
Notificación a la persona o colectivo interesados en la resolución.		
Archivo tanto de la incidencia como de la resolución.		
Readaptar los distintos protocolos en base a las incidencias solventadas con objeto de mantener y mejorarlos continuamente.		
Total de incidencias solucionadas.		
Total de incidencias sin solventar.		
Procedimientos de recogida del nivel de satisfacción de la persona o colectivo hacedor de la incidencia para con la resolución adoptada.		

Gestión de incidencias en ITIL.

En la metodología ITIL, la gestión de incidencias, tiene por objetivo restablecer los servicios de TI lo antes posibles a los usuarios, es decir manejar el ciclo de vida de todos los incidentes con la eficiencia y eficacia que merece un buen proceso de restablecimiento del servicio en caso de falla o corte del servicio.

En ITIL v3, se establece las interrupciones del servicio y las solicitudes de servicio, donde estos últimos son atendidos por el proceso cumplimento de la solicitud, y no por el proceso de gestión de incidentes.

En esta nueva versión de ITIL, se han añadido nuevas funcionalidades como por ejemplo una interfaz entre la gestión de incidentes y la gestión de eventos, donde los casos más urgentes son denominados “Incidentes Graves”.

La gestión de incidencias en ITIL, se lleva a cabo mediante una serie de subprocesos los cuales paso a detallar a continuación:

–Soporte a gestión de incidentes: Provee los mecanismos necesarios para suministrar un soporte efectivo y eficiente.

–Registro y Categorización de incidentes: Registran y asignan prioridades a los incidentes, para que proporcionen soluciones efectivas e inmediatas.

–Resolución de incidentes por el soporte de nivel 1: Se trata de resolver el incidente en el tiempo acordado. De no ser posible, se acordará proporcionar una solución temporal y se transferirá la incidencia al grupo de nivel 2.

–Resolución de incidentes por el soporte de nivel 2: Consiste en resolver un incidente en el tiempo acordado. Si no es posible la resolución del problema, se establecerá una solución temporal y se transferirá la incidencia a un grupo de soporte especializado o proveedor externo. Si no es posible corregir el problema, este se registra y se pasa el grupo de gestión de problemas.

–Gestión de incidencias Graves: Se intenta solucionar incidentes graves. Estos incidentes deben de resolverse a la mayor urgencia, implantando si hace falta soluciones temporales para el restablecimiento temprano de los servicios.

–Monitorización y escalado de incidentes: Monitoriza el estado pendiente de las incidencias, para que se tomen medidas que minimizen los efectos adversos que tendrían para la infraestructura y servicios.
–Cierre y evaluación de incidentes: En este subproceso, se remite a control de calidad la incidencia, antes de emitir el cierre de la misma. Se asegura de que la incidencia ha quedado resuelta eficazmente y con los criterios de calidad que se requieren, además de haber recopilado la información suficiente para describir el ciclo de vida que ha tenido la incidencia con suficiente detalle.

–Información Proactiva a los usuarios: Consiste en informar a los usuarios tan pronto se conozcan las incidencias que se han producido. Esto ayuda enormemente a los usuarios a realizar operaciones, antes de la interrupción del servicio.

–Informe de gestión de incidentes: Servir la información obtenida de otros procesos de incidentes, para paliar incidencias parecidas, además de que sirvan para potenciar las mejoras.

En el proceso de gestión de incidencias en ITIL, podemos extraes igualmente ciertos términos que están directamente relacionados.

–Incidente: Es una interrupción de un servicio o bien una reducción de la calidad del mismo.

–Reglas de escalado de incidentes: Estas reglas establecen jerarquías de escalado y establecen la gravedad de las mismas, junto con sus períodos de resolución.

–Escalado por parte del usuario: Se produce porque el usuario ha experimentado fallos o cortes en el servicio, durante su restauración.

–Preguntas frecuentes de los usuarios: Proporciona información por parte del Service Desk para saber cómo operar en caso de fallos del servicio.

–Informe de gestión de incidentes: Provee información pertinente de las incidencias con respecto a la gestión de incidentes.

–Registro de incidente: Es un registro que se lleva a cabo de cada incidente ocurrido, desde que se produjo, hasta su resolución.

–Información sobre el estado de un incidente: Reporta el estado de un incidente.

–Preguntas sobre el estado de un incidente: Son preguntas generalmente sobre el estado de un incidente concreto.
–Notificación de fallos al servicio: Es una notificación de fallo del servicio, que puede tener su origen de múltiples sitios.

–Información Proactiva al usuario: Es información que resulta vital para los usuarios, con el objetivo de prepararse ante una inminente interrupción del servicio. En realidad es una indisponibilidad del servicio.

–Solicitud de apoyo: Es una solicitud dirigida a expertos en la resolución de una incidencia, como parte del proceso de gestión de la incidencia.

Organización de un centro de atención al usuario

Para cualquier empresa, el cliente es lo primero. Como sucede con todos los tópicos y frases hechas, a fuerza de repetirlos acabamos por olvidar la profunda realidad en que se basan.

La empresa necesita a sus empleados para que realicen las actividades y las tareas; los empleados necesitan a la empresa para que canalice el esfuerzo común, y todos -empleados y empresa- necesitan al cliente para permanecer en el mercado. Por ello, la tarea de atender al cliente es extraordinariamente útil e importante.

Las consecuencias más directas de este planteamiento para nuestro trabajo cotidiano son que tenemos que:

Ofrecer a los clientes, productos y servicios que respondan a sus necesidades de comunicación.

Ofrecer a los clientes productos y servicios con claras ventajas sobre los productos y servicios de la competencia.

Construir y desarrollar un estilo de atención eficaz y atractivo para que el cliente nos identifique con claridad, agrado y satisfacción.

La calidad orientada al cliente

Existen varias definiciones de Calidad de Servicio:

Es la capacidad para identificar y satisfacer las necesidades de los clientes.

Es la acumulación de experiencias satisfactorias del cliente cada vez que tiene un contacto con la empresa.
Es conseguir que el cliente valore mejor el servicio de lo que esperaba en un principio (es decir, que la realidad de un servicio supere las expectativas).

Sin embargo, la calidad de servicio tiene otro componente más: la relación que mantenemos con el cliente.

A través de esta relación también conseguimos que el cliente se sienta satisfecho cada vez que le prestamos un servicio.

Por lo tanto, la calidad de un servicio tiene dos dimensiones:

La de los procedimientos: hacen referencia a las medidas que se llevan a cabo para satisfacer las demandas y necesidades de los clientes.

Se relaciona con el servicio que se da y al hecho de que se presta de acuerdo con unas determinadas normas y procedimientos, todo ello en función de las necesidades del cliente y orientado a satisfacer sus expectativas.

La de las personas: hace referencia a cómo cada persona de la organización (utilizando sus actitudes, conocimientos y habilidades) se relaciona con el cliente para satisfacer sus necesidades.

De ello podemos deducir que la percepción del cliente es la que determina la calidad de un producto o servicio. Dicho en otras palabras:

La calidad de un servicio está orientada al cliente.

Si los procedimientos se adaptan a las demandas y necesidades de los clientes, y si los clientes están contentos con la relación que mantienen con nosotros, entonces hemos dado un servicio de calidad.

En definitiva: Es el cliente el que marca la calidad de un servicio

El punto de vista del cliente

Para saber cómo debemos atender a los clientes, sean externos o internos, de forma que se sientan satisfechos, es preciso tener muy en cuenta su punto de vista. En este sentido, hay que considerar tres aspectos fundamentales:

El cliente espera de nosotros una prestación de servicio concreta que debemos conocer.

El cliente necesita sentir que controla el servicio que recibe.

El cliente necesita sentir que se le está dedicando el tiempo necesario.
No debemos olvidar que las personas acuden a nosotros para conseguir una determinada prestación de servicios.

Además, podemos distinguir dos elementos en esa prestación de servicios:

El servicio básico: es el servicio esencial que solicita el cliente.

El servicio asociado: es todo aquello que rodea al servicio básico

Una vez realizada esa distinción, veamos cuáles son los elementos que aseguran una buena calidad de servicio:

Servicio básico:

–Satisfacción por la prestación: las características del servicio en sí mismo.

–Satisfacción por el suministro: la rapidez en la prestación del servicio, la disponibilidad de éste, el respeto a los plazos, etc.

Servicio asociado:

–Satisfacción por el acceso: cercanía de la empresa al cliente, comunicaciones, aparcamiento, posibilidad de contactar y ofertar el servicio por medio de fax, teléfono, amplitud de horarios, etc.

–Satisfacción por la relación: acogida, escucha, atención, interés en las necesidades del cliente, etc.

–Satisfacción por la información: claridad, rapidez, precisión, fiabilidad de ésta, calidad de la documentación.

–Satisfacción por los consejos: adecuación y pertinencia de las sugerencias.

–Satisfacción por el seguimiento: preocupación posterior por el cliente, por el resultado final del servicio, comunicación correcta con otros miembros de la empresa implicados en la prestación, recogida de información sobre la satisfacción del cliente.

–Satisfacción por el entorno: carácter agradable y funcional de las instalaciones, espacio disponible, comodidad del mobiliario, etc.

Independientemente de las características específicas de cada cliente, existen dos necesidades básicas que todo cliente tiene:

–La necesidad de controlar el servicio que recibe.
–La necesidad de sentir que se le está dedicando el tiempo que requiere.

El control de servicio

Los estudios efectuados indican que para conseguir una relación satisfactoria con nuestros clientes es importante que éstos sientan que controlan la situación, es decir, que conocen y dominan sin mayor esfuerzo el producto que han comprado o el servicio que reciben.

El tiempo de atención

Para la mayoría de nuestros clientes, el tiempo es un bien escaso y muy apreciado.

Nuestra propia experiencia nos dice que no nos gusta dedicarle a una gestión más tiempo del que consideramos estrictamente necesario.

Por eso, el cliente se sentirá agradecido si no le hacemos esperar y si le atendemos con agilidad y rapidez.

Tampoco debemos olvidar que rapidez y brevedad no significan mala atención.

La relación con el usuario o el cliente

Para que un cliente considere satisfechas sus necesidades y nuestro trabajo sea más satisfactorio para nosotros mismos debemos cuidar la actitud general que adoptamos en nuestra relación con él.

El interés y la tolerancia que mostremos, la empatía que comuniquemos y la autenticidad que transmitamos, así como la adecuación del entorno en el que recibimos al cliente permite que éste perciba calidad en la atención que se le presta.

Otro elemento fundamental en la calidad de la atención al cliente es el relacionado con las habilidades que mostramos en el momento de nuestra relación con él.

Estas habilidades nos permitirán cuidar los primeros momentos de contacto con él, establecer una buena comunicación, evitar la continua improvisación y comprobar que nuestra gestión ha sido eficaz.

Debemos estar preparados para resolver con éxito las dudas que el cliente tiene y transmitirle que somos los mejores profesionales para atender la necesidad que nos comunica, generando un buen clima y logrando que el cliente se sienta cómodo y comprendido.

Actitudes en el trato con el usuario o el cliente

Esta predisposición está influida por las creencias, experiencias y valores de la persona.

En el caso de la relación con un cliente deberemos tener en cuenta las actitudes de ambas partes: nuestras actitudes, sobre las que podemos actuar más directamente, y las actitudes del cliente, sobre las que podemos influir de forma más indirecta por medio de las nuestras.

La base para el análisis acerca de las actitudes que nos van a predisponer para un trato adecuado con el cliente pasa por intentar acercarnos a su propio punto de vista.

A la mayoría de nosotros no nos gusta esperar ni tener que realizar desplazamientos molestos e innecesarios; apreciamos cuando nos atienden con esmero y amabilidad y normalmente elegimos aquellos productos que nos ofrecen confianza, se adaptan mejor a nuestras necesidades y tienen un precio razonable.

Barreras en la relación con el usuario o cliente

A veces no existe una buena relación con un cliente o con otras personas y no entendemos por qué.

En algunas de estas ocasiones las causas se relacionan con barreras que aparecen entre esas personas y nosotros.

Aunque estas barreras son difíciles de eliminar, su conocimiento nos ayudará a comprender más de una situación en la que el entendimiento con el cliente se hace especialmente difícil.

Estas barreras son:

El estereotipo: es un cliché de pensamiento referido a características de una persona o grupo (étnico, laboral, social, etc.). Estos clichés distorsionan nuestra capacidad perceptiva y hacen que la misma información adquiera un distinto significado en función de a quién tengamos de interlocutor.

La actitud defensiva: bien hacia uno mismo, hacia el tema que se trata o hacia nuestro interlocutor.
La defensa psicológica: sirve para evitar que nos sintamos molestos o confundidos cuando la realidad no coincide con nuestras expectativas o nuestros actos.

Este sentimiento de molestia o confusión intentamos reducirlo a través de tres caminos:

–Negando la veracidad del hecho.

–Restando importancia al asunto.

–Evitando toda información que provoque ese sentimiento.

La proyección: significa atribuir a otras características de uno mismo, generalmente negativas.

La tendencia a inferir: significa inducir una cosa de otra muy rápidamente, sin obtener toda la información precisa.

Habilidades de comunicación con el usuario o cliente

La s diferentes habilidades que permiten una buena comunicación con el cliente, y que, por lo tanto, facilitan la satisfacción de éste con nuestro trabajo y nuestra empresa, se pueden organizar en función de las tres fases de atención al cliente:

1.La acogida.

2.El diálogo con el cliente.

3.El cierre.

Atención de reclamaciones

Algunas de las gestiones que se realizan en la atención al cliente requieren un tratamiento muy delicado, ya que están relacionadas con su insatisfacción.
respecto a productos o servicios.

La atención de reclamaciones, es uno de los momentos más importantes en el proceso de atención al cliente. El cliente que reclama, debe percibir que su reclamación es debidamente atendida, y que su insatisfacción respecto del servicio o producto contratado, es un tema de especial relevancia para la empresa proveedora de dicho producto o servicio.

Las reclamaciones podrían clasificarse de diversas formas, incluso en reclamaciones fundadas y reclamaciones sin fundamento que, como bien sabemos, también las hay.

Sin embargo, todas ellas deben ser tratadas de la misma manera, puesto que forman parte de la relación con el cliente.

En este sentido cabría decir que el cliente siempre tiene razón, aun cuando no la tenga.

Cualquier reclamación es legítima desde el punto de vista de cliente

Dicho de otra forma, en la atención a las reclamaciones, como en cualquier otro momento de la relación, debemos buscar en primer lugar la satisfacción del cliente.

Debemos tener también en cuenta que reclamar es una gestión desagradable que casi nadie hace por gusto.

Lógicamente, el cliente que reclama no suele ser un cliente feliz.

Con bastante frecuencia, el cliente se pone en contacto con nosotros en un estado de ánimo que varía desde la frustración hasta diversos grados de enfado, en función de su carácter y de su nivel de descontento.

Aunque sus palabras puedan ser más o menos desagradables.

El cliente que reclama no tiene nada personal contra nosotros

La reclamación, por ofensiva que pueda ser a veces su formulación, no debe considerarse jamás una ofensa para el profesional que la recibe, ni siquiera en aquellos casos en los que el origen de la queja sea un error nuestro.

Todos nos equivocamos, y la actitud positiva ante un error es reconocerlo y corregirlo para evitar que se repita.
Tener una segunda oportunidad de satisfacerle. Al atender adecuadamente la reclamación de un cliente recuperamos su confianza y evitamos perderlo y/o que realice comentarios negativos sobre nuestro trabajo o nuestra empresa.

Algo ha fallado en nuestro primer intento de satisfacer sus necesidades pero, por fortuna, podemos intentarlo de nuevo.

Convertir un cliente insatisfecho en un cliente satisfecho. Un cliente atendido adecuadamente en una reclamación suele hacer comentarios positivos sobre nuestra empresa y nuestro trabajo.

Por consiguiente, nos ayuda a ganar de forma indirecta varios clientes.

Detectar errores y deficiencias y, por tanto, corregirlos. Nos interesa estimular la expresión de los clientes descontentos y atender y escuchar atentamente lo que esas personas nos dicen, porque nos ayuda a propiciar mejoras en los servicios.

Proceso de atención de las reclamaciones

Atender reclamaciones es buscar una solución viable que satisfaga al cliente.

Este equilibrio merece la máxima atención. No debemos mostrarnos “cómplices del cliente”, pero tampoco “apegarnos a la rigidez normativa de la empresa”.

En estas situaciones nos encontramos ante un interesante juego, donde tienen mucha importancia nuestra capacidad para comprender cada situación y cliente y la iniciativa que podamos desarrollar en cada caso.

Cuando una persona reclama, está claro que su primer objetivo es conseguir que le demos una solución rápida y satisfactoria a su queja; pero también desea que le escuchemos y comprendamos los perjuicios causados.

Nuestro objetivo al atender una reclamación es que el cliente perciba:

Que le escuchamos con atención e interés.

Que le comprendemos.

Que vamos a darle una solución rápida, seria y satisfactoria.

Para cumplir este objetivo debemos seguir un proceso de atención a reclamaciones que se divide en 7 fases:
1.Recepción de la reclamación

En esta primera fase es recomendable:

No interrumpir al interlocutor. Dejar que el cliente hable y se exprese, sin intentar cortarle. Es difícil que nos escuche hasta que no haya dicho todo lo que quiere decirnos: con frecuencia, el cliente que va a reclamar prepara su discurso y, si le cortamos, se sentirá aún más irritado.

Esperar que baje su nivel de agresividad antes de tomar la palabra.

Escuchar atentamente y tomar notas, demostrando así que estamos atentos y nos interesa.

Intentar percibir las intenciones y el carácter del reclamante.

Tratar de ponerse en el lugar del cliente: sentir lo que él siente en ese momento.

Debemos intentar comprender su enfado y escuchar atentamente su reclamación. Es muy útil preguntar sobre lo que se juega el cliente en este asunto.

Reconducir el posible error del cliente. Tras los primeros instantes de conversación, puede darse el caso de que el propio cliente entienda que parte de la culpa del problema ha sido suya. Nunca debemos aprovechar esa situación para colocarnos en posición dominante e, incluso, reprocharle su error.

2.Verificación de la reclamación

Es fundamental asegurarnos que la información que el cliente nos está dando es correcta para enfocar adecuadamente la gestión de la reclamación. Por ello, deberemos:

Comprobar la veracidad de todos los datos que nos den. Estas verificaciones deben hacerse de forma rápida, procurando evitarle al cliente una espera larga.

Si después de las primeras indagaciones entendemos que la responsabilidad de los problemas reclamados es nuestra, deberemos actuar de la siguiente forma:

–Pedir disculpas por las molestias causadas
–Explicar brevemente las causas que han originado su problema: esto es importante ya que, normalmente, el cliente quiere saber qué fue lo que sucedió. Es más fácil que el cliente entienda -y hasta llegue a disculpar- un error concreto, que enfrentarse al manido argumento de fallos del sistema.

No debemos exagerar la autocrítica ni descender excesivamente en la explicación del fallo.

El cliente que reclama no necesita culpables (qué persona no informó suficientemente, qué aparato no funcionó, quién es el responsable último del problema, etc.); el cliente quiere, sobre todo, resultados y soluciones, y eso es lo que debemos proporcionarle.

3.Asumir nuestra responsabilidad.

Es contraproducente intentar eludir nuestra responsabilidad y la de la empresa ante una reclamación justa. Si usamos evasivas ante el cliente, éste pensará: “encima, se está riendo de mí”.

4.Reformulación de la reclamación

Tras las comprobaciones, es el momento de delimitar con el cliente las características exactas de la reclamación. Podemos seguir para ello, la siguiente estrategia:

–Exponer el problema con nuestras palabras:

·Emplear términos que quiten dramatismo.

–Exponer datos concretos y objetivos.

·Eliminar expresiones, calificativos y términos negativos.

·Evitar minimizar la queja.

5.Oferta de soluciones.

En este momento, pueden darse dos situaciones:

–No es posible solucionar la demanda del cliente: es conveniente hacérselo saber con amabilidad y evitar, así, que pierda el tiempo; de nada sirve demorar un problema si sabemos que no tiene arreglo.

Si el cliente vuelve a irritarse, aplicaremos otra vez la primera etapa del proceso de atención.
–Sí son posibles las soluciones: debemos ofrecerle al cliente una rápida y eficaz, especialmente cuando la responsabilidad es manifiestamente nuestra.

En este caso, pueden presentarse diversas opciones:

–La solución puede ser inmediata porque es sencilla y accesible.

–La solución no puede ser inmediata porque el problema es complejo: debemos explicar al cliente la situación y consultar al departamento o persona correspondiente. No debemos obligar al cliente a volver a reclamar. Si la reclamación no pertenece a nuestro ámbito, nos encargaremos nosotros mismos de dirigirla al departamento o persona correspondiente.

En los casos en los que la solución no es inmediata hay que estudiar muy bien el problema antes de decidir lo que se puede hacer:

–Podemos ofrecer una alternativa provisional que reduzca los perjuicios al cliente.
Podemos ofrecer una bonificación por la complejidad o imposibilidad de dar con otro tipo de solución.

6.Despedida

Para cerrar adecuadamente el proceso de diálogo con el cliente en una reclamación, debemos:

–Evitar que el cliente sienta que nos lo queremos quitar de encima cuanto antes: no debemos mostrar prisa o impaciencia.

–Disculparnos o lamentar la situación ocurrida, agradeciéndole la oportunidad de aclarar el problema: debemos hacer percibir al cliente que su queja no la consideramos un ataque para nosotros, frente al que nos defendemos, sino una oportunidad para complacerle.

–Despedirnos cortésmente.

7.Seguimiento de la solución elegida.

El final de una reclamación no siempre es cuando el cliente se despide y se marcha. Pueden darse dos posibilidades:

La queja se solucionó sobre la marcha: anotar los datos y características de la reclamación, ya que a partir de su estudio es posible establecer controles de calidad, detectar fallos de funcionamiento, etc.
Si muchos clientes se quejan del mal funcionamiento de determinado servicio o producto, es fácil que dicho producto/servicio presente alguna deficiencia de diseño que puede subsanarse.

La solución quedó pendiente o aplazada por cualquier motivo: tomar las medidas para solucionarla, bien personalmente bien a través del departamento correspondiente, y siempre de acuerdo con el compromiso que se le haya ofrecido al cliente.

Para finalizar este apartado de cómo se organiza un centro de atención al usuario, se resume las cualidades que debe de reunir dicho centro, para la prestación eficaz de servicios y que este orientado al cliente.

La calidad orientada al cliente

Existen varias definiciones de Calidad de Servicio:

Es la capacidad para identificar y satisfacer las necesidades de los clientes.

Es la acumulación de experiencias satisfactorias del cliente cada vez que tiene un contacto con la empresa.

Es conseguir que el cliente valore mejor el servicio de lo que esperaba en un principio (es decir, que la realidad de un servicio supere las expectativas).

Sin embargo, la calidad de servicio tiene otro componente más: la relación que mantenemos con el cliente.

A través de esta relación también conseguimos que el cliente se sienta satisfecho cada vez que le prestamos un servicio.

Por lo tanto, la calidad de un servicio tiene dos dimensiones:

La de los procedimientos: hacen referencia a las medidas que se llevan a cabo para satisfacer las demandas y necesidades de los clientes.

Se relaciona con el servicio que se da y al hecho de que se presta de acuerdo con unas determinadas normas y procedimientos, todo ello en función de las necesidades del cliente y orientado a satisfacer sus expectativas.

La de las personas: hace referencia a cómo cada persona de la organización (utilizando sus actitudes, conocimientos y habilidades) se relaciona con el cliente para satisfacer sus necesidades.
De ello podemos deducir que la percepción del cliente es la que determina la calidad de un producto o servicio. Dicho en otras palabras: La calidad de un servicio está orientada al cliente.

Si los procedimientos se adaptan a las demandas y necesidades de los clientes, y si los clientes están contentos con la relación que mantienen con nosotros, entonces hemos dado un servicio de calidad.

En definitiva, es el cliente el que marca la calidad de un servicio.