ESPECIALIDAD FORMATIVA

GESTIÓN DE REDES DE VOZ Y DATOS

IFCM0310

UF1876: Gestión de recursos, servicios y de la red de comunicaciones

* Bibliografía usada en este documento:
UF1876: Atención a usuarios e instalaciones de aplicaciones cliente, Autor: J. A. Jiménez Toro, EDITORIAL ELEARNING S.L. Edición: 5.0
Capturas de pantalla y textos electrónicos de varias web únicamente para ilustrar la actividad educativa

Luis Orlando Lázaro Medrano

Contenido

1 Incidencias producidas en asignación, uso servicios y recursos de comunicaciones

1.1. Alarmas y alertas. Significado

En todas las redes comunicaciones se producen incidencias de diversa índole que perjudican a los usuarios de la red, este perjuicio puede afectar al rendimiento de los recursos o servicios de la red. Estas incidencias pueden ser divididas en dos tipos:

- ⇨ Anomalías: define un comportamiento extraño o mal funcionamiento que afecta al rendimiento de un componente de la red pero no provoca un fallo en el componente. Las anomalías provocan unas pérdidas de rendimiento en los componentes afectados y el origen es debido a varios factores como puede ser:
  - Mal uso de un componente: los usuarios utilizan un componente de una forma correcta o en un uso para el cual no está diseñado.
  - Seguridad deficiente: las políticas de seguridad utilizadas por los usuarios son ineficaces, pueden provocar accesos no autorizados a un componente y utilizarlo para su provecho.
  - Mala configuración: la configuración de un componente no es óptima, provocando un funcionamiento anómalo.
- ⇨ Fallos: define un error grave que provoca una pérdida de funcionamiento del componente, los factores expuestos anteriormente pueden provocar un fallo, otros factores pueden ser:
  - Fallo hardware: error en el hardware interno del componente provocado por una sobrecarga de tensión, rotura de un componente, golpe físico, incendio, etc.
  - Fallo software: error que provoca que un determinado software deje de funcionar, pueden ser provocados por errores de programación, fallos de diseño en el software, etc.
  - Ataques informáticos: en este apartado podemos incluir, virus, troyanos, DDOS, etc., que utilizan algún error de seguridad en el sistema o aprovechan alguna vulnerabilidad, como un Zero Day, en el componente.

Las anomalías de funcionamiento deben ser controladas y resolverlas lo antes posible para que no conviertan un error grave que provoque un fallo y deje de funcionar un determinado recurso o servicio.
Un corte en el funcionamiento de un servicio, puede provocar pérdida económicas en la empresa proveedora. Una correcta monitorización de todos los componentes de la red puede detectar posibles anomalías en el funcionamiento de la red, analizando los datos y realizando las posibles actuaciones para resolver la situación.
Para controlar las posibles anomalías y fallos en la infraestructura de red, requiere una buena monitorización de los componentes de la red que permite realizar un control de su funcionamiento. Para detectar posibles errores en la red tenemos disponibles las alertas y alarmas.

ALERTAS	ALARMAS
Detecta un posible error en el sistema, tomando las medidas necesarias para resolverlo y que no derive en un error de mas gravedad.	Detecta un fallo grave en el sistema que puede provocar un daño grave en el funcionamiento de un componente de la red.

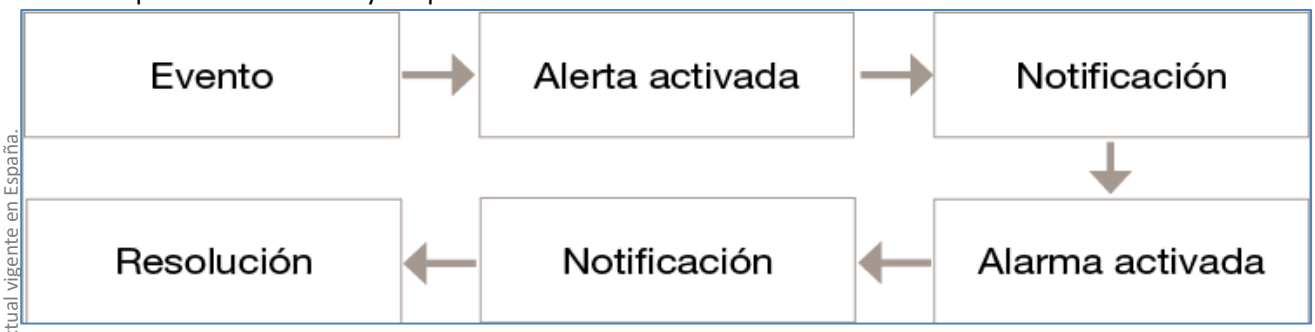
La principal diferencia entre las alertas y las alarmas es la gravedad del evento que ha servido para activarlo.
Una alerta conlleva un estado de precaución para vigilar el evento activador, se debe resolver la alerta aunque no lleve una prioridad alta la resolución. En una alarma la acción prioritaria sea resolverla, porque a diferencia de una alerta, el evento que ha provocado la alarma sí está causando un daño en el funcionamiento de la red.
Por ejemplo una excesiva subida en el tráfico de la red a un determinado nivel activará una alerta y cuando se produzca una sobrecarga en la red por el exceso de tráfico activará una alarma.
Las alertas son producidas en un estado anterior a las alarmas, pero pueden derivar en una alarma, sino se toman las medidas oportunas. Una alerta es activada cuando se produce un determinado evento en la red que puede provocar un fallo, con un alerta el administrador puede prevenir que ese evento genere en un daño mayor.

Las herramientas de monitorización permiten definir tanto alertas como alarmas, el administrador deberá configurar qué eventos activan las alertas o alarmas. Por ejemplo, un administrador desea monitorizar el espacio libre disponible en un disco duro, define una alerta cuando el espacio libre llega al 90% de la capacidad y la alarma es definida cuando no exista espacio libre en el disco duro.
En algunos sistemas existen las prealertas que definen un estado anterior de la alerta, que se activa cuando se produce algún evento considerado perjudicial y que pueden producir un funcionamiento anómalo, tomando las primeras medidas para evitar que derive en una alerta.
Cuando se activa una alarma o alerta, el administrador puede definir una serie de notificaciones que serán enviadas por diversos medios como:

- ⇨ Correo electrónico.
- ⇨ SMS.
- ⇨ Mensajería.

El administrador o personal correspondiente, recibirá una notificación cuando se activa una alarma o alerta, teniendo conocimiento de que alerta o alarma y cuál es el evento que la ha activado, que permitirá realizar las acciones más adecuadas para solventar el error o anomalía que se ha producido.
Cuando el administrador recibe una notificación de una alerta activada, deberá analizar los datos recibido.
Existen herramientas que permiten ejecutar determinados comandos de forma automática cuando una alarma o alerta es activada, el administrador puede configurar una serie de comandos que son ejecutados cuando es activada una alerta o alarma. Estos comandos tienen como objetivo resolver el incidente producido, si el comando no ha solucionado puede enviarse una notificación al administrador para resolver la situación.
El proceso que se sigue cuando una alerta es activada es el siguiente:

Por ejemplo, un administrador crea una alerta asociada a un evento especifico, también configura una notificación que estará asociada a la alerta, esta notificación deberá tener una serie de datos, como la dirección de correo del administrador donde enviar la notificación. Cuando se produce el evento la alerta es activada y es enviada la notificación al administrador con los datos correspondientes que podrá ponerse a trabajar para resolver el problema.
Como se ha explicado anteriormente, el administrador puede configurar una serie de comandos que serán ejecutados cuando se active una determinada alarma, esta acción se realizará después de activar la alerta.
Aunque los comandos resuelvan el problema, la notificación tendrá que enviarse para que el administrador tenga conocimiento de la alerta, de los comandos ejecutados y si estos comandos han tenido éxito o no han resuelto el problema, en este caso el administrador tendrá que tomar las medidas oportunas para solucionarlo.
En el caso de una alarma el proceso que se sigue es un poco diferente, para un determinado evento suelen asociarse primero una alerta y después una alarma.



Como se ha explicado anteriormente, la principal diferencia entre la alerta y alarma es la gravedad del evento que las activa. Una alerta activada induce al administrador un estado de precaución, realizando un control del evento producido y aplicar una serie de acciones para solventar el incidente, el evento no produce daños graves en el sistema pero en potencia el evento producido puede convertirse en un incidente de mayor gravedad.

En caso de persistir el problema, esa alerta puede convertirse en una alarma, que significa que se ha producido un daño grave en el sistema y el administrador debe tomar medida más determinantes, dando prioridad a la alarma. Igual que en las alertas, una alarma debe tener una notificación asociada.
Hay determinados escenarios donde por motivos de tiempo la transición entre una alerta y una alarma es muy corta, también debemos tener en cuenta si es necesario tener para un mismo evento una alerta y una alarma. Por ejemplo, en fallos hardware es más importante tener una alerta bien configurada que avise cuando el hardware tenga indicios de fallar y el administrador si cree conveniente sustituya el hardware, antes que deje de funcionar. Un fallo de hardware que significa que deje de funcionar puede provocar un gran perjuicio a la empresa, si el administrador desea configurar una alarma para un hardware debe ser para indicar que una situación de corte de funcionamiento es inminente, para que el administrador tenga tiempo para solucionar esa situación.
También las alarmas pueden tener una serie de comandos que son ejecutadas cuando es activada, estos comandos deben ser seleccionados para resolver o ayudar en el proceso de resolución del incidente.
Cuando se activa una alarma o una alerta el principal objetivo es resolver el incidente, los pasos a seguir son:

- Obtener información: cuando un administrador recibe una notificación, incluye información sobre el incidente, pero es conveniente obtener toda la información de otras fuentes. El administrador debe saber a qué componente a afectado el incidente producido.
- Aislar el componente: esta acción impide que el incidente se propague por la red.
- Análisis de información: con el incidente controlado se debe analizar la información obtenida y buscar la causa del incidente y que soluciones existen para resolver el fallo.
- Prueba de solución: la solución escogida debe probarse en el entorno de trabajo y comprobar si es una solución óptima, si la solución no es funcional deberá escogerse otra de las posibles soluciones.
- Resolución: si la solución es correcta y el sistema funciona de forma correcta, se ha conseguido el objetivo principal que es resolver el incidente que ha activado la alarma.

Obtener información
Existen diferentes fuentes de información para que el administrador pueda conocer la causa del incidente, entre las que tenemos:

- Ficheros log: en los componentes software existen una serie de archivos donde se almacena la actividad del software, en los componentes hardware, mediante su firmware, también existen este tipo de ficheros.
- Usuarios: otra fuente de información son los usuarios del sistema, que pueden proporcionar información, como los síntomas que ellos perciben.
- Gráficas: existen herramientas que monitorizan diversos parámetros del sistema mediante un conjunto de gráficas, observando el comportamiento de esas gráficas el administrador puede obtener información muy útil.

Aislar el componente
Con el componente localizado la siguiente tarea es aislar el componente para que el incidente pueda afectar a otros componente, el administrador podrá trabajar de forma más segura sin que sus acciones no perjudiquen al resto de componente de la red. Para realizar esta tarea se pueden existir diversos procedimientos como:

- Desconexión de la red: para aislar el incidente una forma fácil es desconectarlo de la infraestructura de red, si el incidente afecta a u dispositivo hardware esta opción es la más aconsejable.
- Cerrar servicios: si el fallo proviene de un componente que ofrece un servicio, un corte temporal del servicio permite que el fallo no perjudique a otros servicios, mientras el administrador puede trabajar de forma más segura en el componente donde ha surgido el incidente.

Análisis de la información
Con la información obtenida y el aislado, el administrador debe realizar un análisis de la información obtenido para descubrir la causa del fallo que ha provocado el evento que ha activado la alarma.
Descubierta la causa será más fácil conocer que soluciones hay disponibles, dependiendo de la causa

existirán una o varias soluciones, anteriormente se ha mostrado diversos tipos de fallos. El administrador deberá escoger que solución será la más adecuada.

Prueba de solución

La solución escogida debe ser probada antes de utilizarla en un entorno de producción, esta solución deberá cumplir una serie de requisitos de funcionamiento que el administrador ha configurado. Para probar la solución se deberá crear una entorno de pruebas y que sea los mas fiel al entorno de producción. Entre las diferentes pruebas que existen tenemos:

- Prueba de carga: comprueba que el componente que su funcionamiento soporta la carga de trabajo exigida.
- Prueba de seguridad: comprueba que la seguridad del componente es la adecuada.
- Prueba de funcionalidad: comprueba que las funciones del componente son las mismas que tenia anterior al fallo.

También debe cumplir con una serie de requisitos impuestos tanto por el administrador como por el cliente y la empresa. La solución seleccionada debe obtener un funcionamiento óptimo del componente.
Si la solución no cumple con algunos requisitos o no pasa alguna de las pruebas, esa solución no es la correcta y se debe escoger otra de las soluciones disponibles.

Resolución

Para la resolución existen diversos procedimientos. El primer paso es obtener todo la información disponible y realizar un exhaustivo análisis para proceder con las acciones más adecuadas, entre las que se puede encontrar.

- Reemplazo del componente: si no hay posibilidad de reparación, tendrá que instalarse un nuevo componente. En otros casos, el problema es que el componente no es el adecuado para el entorno de trabajo, con lo que el reemplazo se realiza por otro componente de otro fabricante o un modelo superior del mismo fabricante, que se ajuste a las necesidades del entorno de trabajo.
- Actualización o instalación: en algunos escenarios el problema es un fallo software, que puede ser un error en el diseño, error de programación, agujero de seguridad, etc. Que puede ser reparado con la instalación de un parche o una actualización a una versión superior.
- Cambio en la configuración: una mala configuración del componente puede provocar un mal funcionamiento e incluso un corte en el funcionamiento, la configuración debe estar optimizada al entorno de trabajo. Un cambio en la configuración puede ser la solución al problema surgido.
- Cambio en el diseño: toda infraestructura de red debe tener un diseño acorde con la carga de trabajo que va a soportar y los servicios que va a proporcionar. Los componentes (hardware y software) debe ser los adecuados y estar situado en su lugar, de acuerdo a un diseño (topología) seleccionado para el entorno de producción. Un mal diseño puede provocar que los componentes no funcionen de forma adecuada y no soporten la carga de trabajo.

1.2. Herramientas específicas y técnicas de detección de incidencias en sistemas de comunicaciones

Para la detección de forma óptima de las incidencias de una infraestructura de red, un administrador debe utilizar una herramienta que facilite esta gestión. Con las herramientas de monitorización se pueden configurar una serie de alertas y alarmas asociadas determinados eventos que se produzcan en un componente de la red, también existen herramientas específicas para la detección de incidencias.
Una primera clasificación de herramientas de detección de incidencia basada en la forma de detectar las incidencias:

- ⇨ **Detección manual:** las incidencias son detectadas y generados por personal de la empresa. Este tipo de herramientas permiten generar una incidencia rellenando datos relativos a la incidencia en un formulario, también permiten realizar las gestiones para la resolución. Para este tipo de herramienta lo habitual es recibir un aviso de un usuario y un operador generar la incidencia con una serie de datos, en caso necesario la tramita a otro departamento para su resolución.
- ⇨ **Detección automática:** este tipo de herramientas comprueban si ocurren determinadas incidencias, estas herramientas proporcionan una serie incidencias definidas por defecto que pueden ser aumentadas por incidencias definidas por el administrador. También permiten definir diversos flujos de trabajo en función de las incidencias.

Existen herramientas que detectan incidencias de cualquier tipo y otro tipo de herramientas que están especializado un determinada categoría de incidencias.
Existen diversas categorías de incidencias, entre las que tenemos:

- **Incidencias hardware**: relacionado con el fallo de algún componente hardware.
- **Incidencias software**: relacionado con el algún fallo de funcionamiento en el software, sin importar el tipo de software de la incidencia.
- **Incidencias de seguridad**: en esta categoría se incluye cualquier evento producido por un fallo de seguridad en el sistema, ya sea seguridad física, como una acceso no autorizado a las instalaciones de la empresa, como seguridad lógica, como un ataque informática.
- **Incidencias de usuario**: cualquier incidencia relacionada con el funcionamiento del sistema desde el punto de vista del usuario, como puede ser instalación de un software o ayuda con un determinado servicio.

La resolución de cada categoría de incidencia y los recursos son diferentes, también la gravedad generada suele ser diferentes, aunque todas las incidencias pueden provocar daños graves, pero no es lo mismo la detección de una incidencia hardware que una incidencia de usuario. El administrador deberá dar prioridad a aquellas incidencias potencialmente más graves.
En el módulo anterior, UF1875, se mostró una herramienta para generar incidencia y controlar el proceso de resolución denominada GLPI, explicando ejemplo de incidencia gestionado por esta herramienta.
En la gestión de incidencia requiere una serie de herramientas adicionales que son:

- Gestión de inventarios: para gestionar las incidencias se debe conocer los componente (software y hardware) que pertenecen en la infraestructura de red, este tipo de herramientas permiten gestionar un inventario con los componente de la red.
- Mapa de red: permite conocer la topología de red para localizar los componentes donde se ha producido la incidencia.
- Obtención de datos: para conocer la incidencia producida se deben recoger datos, existen múltiples formatos para de obtener datos, como gráficas, log, CSV, etc. Herramientas como Cacti o un visor de fichero log permiten obtener datos sobre la incidencia producida.
- Gestión de alarmas: permite configurar alarmas, o alertas, en diferentes componentes de la red, las herramientas de monitorización, como Nagios, permiten realizar esta función.
- Generación de incidencias: permite generar una incidencia mediante un formulario y gestionar el proceso de resolución. Como ejemplo de este tipo de herramientas tenemos GLPI.

Dependiendo de la infraestructura de red, es posible que sean necesarias otro tipo de herramientas, pero las mostradas anteriormente se pueden considerar esenciales.
Una herramienta de detección de incidencia debe disponer de las siguientes funcionalidades:

- Detección de cambios en los inventarios: cualquier cambio en los componentes de la red debe ser actualizado, para evitar que se produzcan incidencias en componentes no registrados.
- Realización de acciones ante incidencia: ante determinadas incidencia se pueden programar determinadas acciones, como realizar una copia de seguridad o notificar una incidencia a un técnico.
- Emisión de alarmas: cualquier alarma activada por una incidencia debe ser registrada por la herramienta y comenzar el flujo de trabajo que tenga configurado.
- Elaboración de informes: este tipo de herramientas debe generar informes sobre su actividad que recoja información como; alarmas activadas o incidencias generadas.

Teniendo en cuenta estas funcionalidades la gestión como la detección de incidencia se realizarán de forma óptima mejorando el tiempo de respuesta y ahorrando en recursos de la empresa.
Para la gestión se debe tener en cuenta los recursos disponibles y maximizar su rendimiento, priorizando los incidentes y asignándole más recursos. Para saber que incidentes son prioritarios podemos tener en cuenta el **Principio de Pareto**.
El principio de Pareto, también conocida como la regla 80-20, en la gestión de incidencia indica 80 por ciento de los incidentes son localizados en el 20 por ciento de los componentes. Esto significa que hay unos pocos componentes donde ocurren muchas incidencias, si enfocamos nuestros esfuerzos y recursos en esos componentes eliminaremos muchas posibles incidencias.

Ante una incidencia existen diversas estrategias de actuación, las dos más utilizadas son:

- ⇨ Estrategia reactiva
- ⇨ Estrategia proactiva

Estrategia reactiva

Este tipo de estrategia actúa cuando un incidente ha ocurrido y la respuesta que se ejecuta se basa en la información de los datos de incidencias pasadas. Para realizar esto, es necesario disponer de una base de conocimiento donde almacenar de forma organizada toda la información de los incidentes ocurridos y las soluciones implementadas. Esta base de conocimiento es un requisito imprescindible para poder aplicar esta estrategia y si no existe, deberá implementarse dentro de la herramienta de gestión de incidencias.
Para utilizar esta estrategia se puede escoger entre dos enfoques:

- ⇨ Enfoque cualitativo: se utilizan los datos históricos disponibles realizando un estudio informal y considerando diversos aspectos como:
  - Servicio con más incidencias.
  - Servicios con más recursos asignados para la resolución de incidencias.

  Esto permitirá conocer los servicios más "débiles" ante las incidencias y tomar las medidas oportunas para solucionarlos. Esto conllevaría una mejora de rendimiento de los servicios influyendo en la satisfacción de los clientes.
- ⇨ Enfoque cuantitativo: hace uso de los datos almacenados en la base de conocimiento, realizando un estudio estadístico de los datos. Este estudio estadístico hace uso del concepto de variabilidad provocado por:
  - Causas comunes: identifica las causas propias de una actividad y aparecen de forma aleatoria. Por ejemplo se tenemos un servicio de correo electrónico es posible que surja problemas con el spam que causara diversas incidencias, el correo electrónico y el spam son algo indisoluble, aunque se tomen medidas para evitar el spam.
  - Causas especiales: con aquellas provocadas por motivos concretos y provocan grandes variaciones en los resultados. Son las primeras causas que se deben estudiar porque supondrán una mejora de calidad en el rendimiento del sistema.

  Aquellas actividades cuya variabilidad esta fuera de un límite de tolerancia específicos no tendrán una calidad aceptable, serán objeto de estudio para conocer su incidencias asociadas. El objetivo de esta técnica es conocer el grado de ocurrencia de determinadas incidencias, estudiando una serie de variables que permitirán conocer las causas de una incidencia. Para conocer que incidencias son detectadas se utilizan gráficos de control, hay dos tipos gráficos que son utilizados.
  - Gráficos de control de variables.
  - Gráficos de control de atributos.

  Los gráficos de control solo detectan incidencias pero no la causa y posibles soluciones, se deben utilizar otras herramientas para conocer esa información. El enfoque cuantitativo permite conocer que incidencias se resuelven de forma eficiente y que incidencia no son resueltas de forma eficiente.

Estrategia proactiva

Este tipo de estrategias consiste en actuar antes de que una incidencia ocurra, analizando la información disponible. Esta estrategia puede complementarse con una estrategia reactiva cuando esta última esta implementada de forma óptima.
Procesos con información valiosa para prevenir incidencias, entre los procesos a vigilar tenemos:

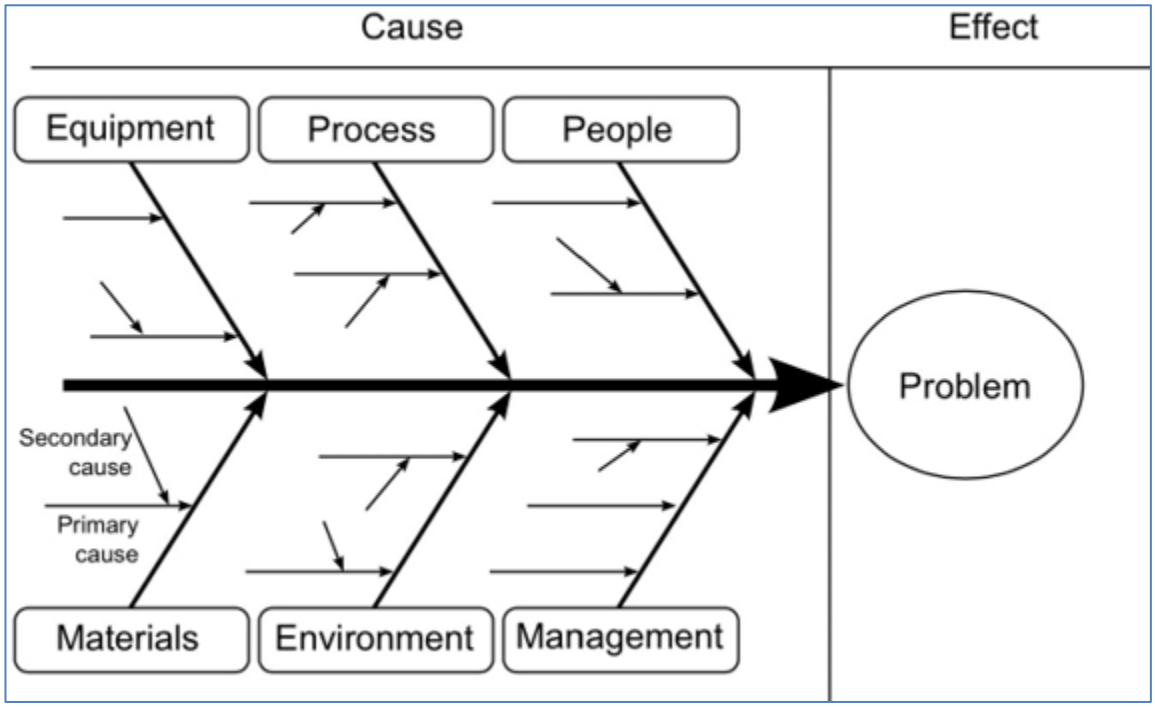
- ⇨ Capacidad: aquellos están relacionados con la capacidad de un componente, un exceso en la capacidad provocar una incidencia.
- ⇨ Disponibilidad: están relacionados con el funcionamiento de un componente, cuando un determinado componente no está disponible provoca un incidencia en el sistema.
- ⇨ Seguridad: están relacionados con la seguridad del sistema y la red.
- ⇨ Cambios: un cambio hardware o software como un cambio de configuración pueden provocar incidencias.
- ⇨ Eventos: determinados ocurrencias que se producen en la red pueden generar una incidencia.

Las actividades relacionadas con los puntos expuestos anteriormente pueden generar incidencias, esto debe ser tenido en cuenta para tomar las acciones oportunas para evitar la generación de una incidencia. Cuando es detectado un proceso o actividad que puede provocar una incidencia, empieza un proceso de gestión con los siguientes pasos:

1. Identificar la causa.
2. Posibles soluciones y alternativas.
3. Implementación de la solución y comprobación de su eficacia.

Para el paso de identificar la causa se analiza la actividad que ha motivado la incidencia, para realizar este análisis existen distintos métodos como:

- ⇨ 5-Why: esta técnica consiste en realizar 5 preguntas, cinco "por qué", que cuestionen la respuesta anterior.
- ⇨ Diagrama causa-efecto: es un método basado en tres puntos.
  - Plantear los síntomas del problema.
  - Realizar sesiones de brainstorming donde descubrir los factores realizados con la incidencia.
  - Construcción de un diagrama, denominado de espina de pez, donde se muestran los factores descubiertos y el impacto que produce en la causa de la incidencia.



En la estrategia reactiva podemos realizar un conjunto de tareas que se realizan como parte de la respuesta al incidente generado, existen múltiples tareas y algunas de ellas solo disponible para un tipo de incidente, entre las tareas más genéricas tenemos:

- ⇨ Recepción de informes sobre la incidencia.
- ⇨ Tramitación y escalado de una incidencia.
- ⇨ Relevo de los sistemas y procesos de negocio afectados.
- ⇨ Elaboración de un plan de respuesta ante el incidente.
- ⇨ Ejecución medida de contención y mitigación para controlar el daño producido.
- ⇨ Elaboración de documentación sobre el proceso de resolución.

Para la estrategia proactiva existen una serie de tareas que permiten estar mejor preparado ante posibles incidencias, estas tareas permitirán detectar la incidencia potenciales en la infraestructura de red, entre las tareas a ejecutar tenemos:

- ⇨ Análisis de alertas y alarmas.
- ⇨ Actividades de sensibilización.
- ⇨ Actividades de entrenamiento.
- ⇨ Evaluaciones de seguridad.
- ⇨ Análisis y optimización de los procesos de trabajo.

- ⇨ Evaluaciones de los componentes de la red.
- ⇨ Establecimiento de políticas de seguridad.

Como se ha indicado anteriormente las estrategias reactivas y proactivas son complementarias, aunque la estrategia proactiva es la más útil porque previene de posibles incidencias pero la prevención no es total y siempre una buena estrategia reactiva permitirá paliar las consecuencias de una incidencia.
Cuando una estrategia reactiva está correctamente implementada es considerada como madura, debe ser acompañada de una estrategia proactiva.

1.3. Procedimientos de diagnóstico y reparación de la incidencia

Cuando surge una incidencia en la infraestructura de red comienza una operativa por parte de la empresa para solucionar los errores producidos, también denominado plan de gestión de incidencias. Esta operativa debe ser especificada por la empresa teniendo en cuenta una serie de aspectos como pueden ser:

a) Tiempo de respuesta para resolver la incidencia.
b) Recursos disponibles por parte de la empresa.
c) Importancia del componente afectado por la incidencia.

Este proceso debe estar perfectamente documentado identificando el personal, su responsabilidad y los roles asignado, como todos los procesos involucrados en la operativa.
Un aspecto que se debe tener en cuenta es la diferencia entre una incidencia y un problema. Una incidencia es un evento que provoca un mal funcionamiento de un componente de la red, como un determinado servicio no funciona. Un problema es un hecho que ocasión o podría ocasionar una incidencia, un problema es la causa raíz de una o varias incidencias. La operativa de gestión de incidencia de una empresa debe descubrir el problema que ha causado la incidencia, eliminando el problema las incidencias generadas no volverán a ocurrir.
La empresa especifica una operativa para resolver una incidencia que deberá tener una serie de pasos definidos, el primero será realizar un diagnóstico de la incidencia que permite conocer qué tipo corresponde.
Una clasificación de la incidencia es muy útil, tener definida un esquema de clasificación de incidentes permitirá a la empresa conocer de forma rápida que problema ha causado la incidencia, aunque en algunos casos es muy difícil clasificar un incidente. Tener un esquema de clasificación puede ahorrar mucho tiempo en el proceso de resolución porque antes tendremos identificada la incidencia y más rápido se podrán tomar decisiones para el proceso de resolución. Para realizar una buena clasificación cada incidente debe ser valorado en función de varios puntos, entre los cuales tenemos:

- ⇨ Tipo: cada incidente puede ser englobado en un categoría atendiendo a sus aspectos funcionales.
- ⇨ Severidad: mide el daño potencial que puede generar el incidente.
- ⇨ Prioridad: permite conocer la importancia del incidente y la rapidez con que debe ser solucionado.
- ⇨ Coste: cuantificación de los costes que produce la incidencia.

Cualquier incidente en función de los datos obtenido estará dentro de un apartado en la clasificación, que permitirá planificar de un forma óptima los siguientes pasos en el proceso de resolución. El esquema de clasificación debe ser definido por la empresa en función de sus características.

Existen una serie de normas ISO donde definen como implementar un procedimiento para la gestión de incidencias. Por ejemplo, existe la norma ISO27001 que define un procedimiento para gestionar incidencias de seguridad.

Una vez realizado el diagnóstico de la incidencia, se ha obtenido información de la incidencia y se ha clasificado, el siguiente paso es proceso de reparación. El proceso de reparación consiste es seleccionar las posibles soluciones, realizando un estudio de viabilidad de cada una de ellas, teniendo en cuenta los siguientes factores:

- ⇨ Recursos disponibles.
- ⇨ Coste estimado.
- ⇨ Prioridad de la incidencia.
- ⇨ Tiempo de respuesta.

En algunos casos, como una incidencia en un servicio al cliente, se debe tener en cuenta otros factores como el SLA firmado con el cliente, donde puede existir cláusulas donde definen tiempo de respuesta

máximo o una disponibilidad garantizada. En este caso, las cláusulas del SLA donde se especifica el nivel de servicio serán más determinantes que otros factores de la empresa.
Las posibles soluciones serán clasificadas en función del cumplimiento de los factores expuestos, la solución seleccionada será aquella que pase con más nota el estudio de viabilidad. La solución seleccionada en primer lugar deberá ser probada en un entorno de prueba para comprobar si resuelve la incidencia. La solución escogida será la correcta si cumple unos determinados puntos:

- ⇨ La solución deberá resolver la incidencia sin afectar a otros componentes del sistema.
- ⇨ La solución implementada debe proporcionar un rendimiento similar o mejor en el sistema, comparado con el rendimiento antes de producirse la incidencia.
- ⇨ La carga de trabajo del sistema no debe aumentar al implementar la solución.

Resumiendo, la solución implementada será la correcta si resuelve la incidencia y el sistema funciona igual o mejor que antes. Si la solución no cumple con algún punto no se considera la mejor solución y se deberá escoger la siguiente solución.
Para comprobar la solución se deberá realizar una serie de pruebas en el entorno de pruebas antes de ponerla en funcionamiento en un entorno de producción. Esto es muy importante, la solución debe ser probada de forma exhaustiva para que no produzca fallos cuando sea trasladada al entorno de producción.
Entre las pruebas que pueden ser utilizadas, tenemos:

- ⇨ Pruebas de rendimiento.
- ⇨ Pruebas de seguridad.
- ⇨ Pruebas de carga y estrés.

Si la solución implementada no pasa alguna prueba o los datos obtenidos en las pruebas son peores comparado con el funcionamiento antes de la incidencia, la solución no es la correcta y se deberá probar la siguiente de la clasificación.
Con una solución implementada que resuelva la incidencia y pasadas todas las pruebas a las que ha sido sometida, deberá implementarse en el entorno de producción y ponerla en funcionamiento. Aunque ha sido probada en un entorno de pruebas con unas condiciones muy similares al entorno de producción, los administradores o personal responsables deben tener una especial vigilancia en aquellos componentes afectados por la incidencia y comprobar su correcto funcionamiento. Esta vigilancia debe durar un periodo corto de tiempo, suficiente para comprobar que la solución implementada no causa problemas en la infraestructura de red.
Con la solución implementada en el entorno de producción y funcionando correctamente, debe documentarse todo el proceso que se ha seguido y añadirlo en la base de conocimiento de la empresa, entre los datos que debemos indicar en la documentación tenemos:

- ⇨ Síntomas de la incidencia.
- ⇨ Descripción de la incidencia.
- ⇨ Causa de la incidencia.
- ⇨ Solución y alternativas.
- ⇨ Implementación de la solución y pruebas.
- ⇨ Tiempo de respuesta y recursos empleados.

La documentación del proceso de resolución es muy útil y permite obtener información que puede ser utilizada para otras incidencias que ocurran en el futuro, ahorrando tiempo en el proceso de resolución y en recursos utilizados.
La operativa utilizada por la empresa para resolver una incidencia debe ser evaluada para conocer si es eficiente. Cuando la operativa ha sido aplicada y la incidencia ha sido resuelta de forma satisfactoria se deben realizar ciertas preguntas como:

Evaluación de la operativa
¿El tiempo de respuesta ha sido bueno?
¿Los recursos disponibles han sido suficiente?
¿La comunicación entre los departamentos que han participado en la operativa ha sido correcta?
¿La operativa ha sido ejecutada sin problemas?

El resultado del proceso de la evaluación de la operativo permitirá conocer si son necesarios pequeños cambios en los procesos de la operativa o cambios más profundos, también si la el resultado ha sido positivo no debe introducirse cambios en la operativa.

1.4. Tipos de incidencias

Antes se ha mencionado que cualquier incidencia que ocurra en un sistema debe ser clasificada en un esquema que ha sido definido por la empresa, esta clasificación nos permitirá orientar los esfuerzos para dar resolución al tipo asignado según su clasificación. Este esquema de clasificación definido por una empresa no tiene que ser igual que otro esquema de clasificación de otra empresa, aunque habrá tipos genéricos que son incluidos en todos los esquemas, habrá otros que serán específicos de la empresa.
Existen diversos tipos de incidencias y cada uno de ellos se diferencia de los otros en:

- ⇨ Síntomas: cada tipo de incidencia provocan una serie de síntomas que permiten darnos cuenta que algo está pasando: bajada de velocidad, rendimiento bajo, comportamiento anómalos, caída de servicio, etc. Estos síntomas también nos dan pista de las posibles causas que han provocado la incidencia.
- ⇨ Daño: el tipo de incidencia influye en el daño que pueda producir, aunque todos los tipos de incidencia puede provocar daños graves, el daño potencial de una incidencia tiene relación con tipo y algunos tipos provocan un daño mayor que otros.
- ⇨ Recursos: dependiendo del tipo serán necesario unos recursos diferentes, algunos tipo requieren personal cualificado para su resolución y otro no es necesarios, otro tipo requiere recursos hardware y otros software.
- ⇨ Complejidad: cada tipo de incidencia tiene una complejidad, aunque otros factores en la incidencia aportan complejidad, la complejidad afecta a otros factores como el tiempo de respuesta, más complejidad involucra un mayor tiempo de respuesta.

Pueden existir otros factores para diferenciar los tipos de incidencia, pero los expuestos serían los más habituales. Aunque la empresa puede definir sus propios tipos de incidencia, hay un conjunto de tipos de incidencias genéricas que existen en toda infraestructura de red, estas incidencias son:

- ⇨ Incidencias de hardware.
- ⇨ Incidencias software.
- ⇨ Incidencias de usuario.
- ⇨ Incidencias de seguridad.
- ⇨ Incidencias de red.
- ⇨ Incidencias físicas.

Incidencias hardware

Cualquier problema surgido en un componente hardware de la red puede provocar una incidencias de este tipo, generalmente la causa está relacionada con la rotura o mal funcionamiento de un componente hardware y la solución a implementar es la sustitución del hardware. Muchas veces el coste de la reparación del hardware es mayor que la sustitución. Otra posible causa es que el hardware no es adecuado para la carga de trabajo que soporta y es sustituido por otro de mayor potencia. Este tipo de incidencia no tiene una complejidad excesiva, solo hay que realizar un proceso de sustitución y configuración del hardware.
El tiempo de respuesta no debe ser muy alto, aunque en algunos casos la sustitución del hardware suele demorarse por la no disponibilidad del hardware de sustitución y debe pedirse a un proveedor externo.

Incidencias software

En este caso, se refiere a cualquier problema surgido en las aplicaciones instaladas en el sistema, como:

a) Sistemas operativos.
b) Software de servidor (web, correo electrónico, ftp, base de datos, aplicaciones, etc.).
c) Aplicaciones de escritorio (ofimática, clientes de correo, clientes de mensajería, navegadores web, etc.).
d) Aplicaciones multimedia (visores de imágenes, editores de vídeo, reproductores, etc.).
e) Aplicaciones de seguridad (cortafuegos, antivirus, etc.).
f) Aplicaciones de gestión (programas de contabilidad, gestión de clientes, ERP, CRM, etc.).
g) Firmware.

Cualquier aplicación instalada en el sistema puede tener un mal funcionamiento, existen múltiples incidencias de este tipo, como ejemplo:

- ⇨ Bloqueo de la aplicación.
- ⇨ Cortes en el funcionamiento.
- ⇨ Lentitud de ejecución.
- ⇨ Errores en la interfaz gráfica de la aplicación.

Como este tipo de incidentes abarca un conjunto muy variado de aplicaciones las posibles causas son también muy variadas.

Incidencias software (causas)	Errores en la programación o en el diseño de la aplicación
	Errores en la configuración de la aplicación
	Fallos de dependencias
	Instalación no correcta
	Fallos de librerías
	Sistema operativo no soportado

En muchos casos, una reinstalación de la aplicación o una actualización soluciona el incidente, en otros casos la incidencia se resuelve con un ajuste en la configuración. En tipo de incidente tiene muchas posibles causas, algunas específicas para un tipo de aplicación, muchas soluciones.

La obtención de información desde múltiple fuentes y un buen análisis, permitirá conocer la causa y escoger la solución adecuada de la forma más rápida posible. La experiencia del equipo responsable de la resolución y disponer de una buena base de conocimiento son un requisito muy importante para el éxito en el proceso de resolución.

Tanto la complejidad como el tiempo de respuesta dependerán mucho del incidente ocurrido y el tipo de aplicación que ha afectado. Hay aplicaciones más complejas que otras y eso influye en el tiempo de respuesta.

Incidencias de usuario

Este tipo de incidencias afectan a los usuarios, cualquier problema que dificulte el trabajo del usuario en la infraestructura de red estará incluido en este tipo. También cualquier dificultad que encuentre el usuario utilizando los servicios proporcionados, esto se denomina ayuda o soporte de usuario.

Entre los incidentes que pueden surgir tenemos:

- ⇨ No conocer un determinado componente.
- ⇨ Servicio no funciona correctamente.
- ⇨ No usar correctamente un determinado recurso o servicio.
- ⇨ No saber instalar un determinado servicio o recurso.
- ⇨ Configuración incorrecta de un componente (hardware o software).

Habitualmente los usuarios pueden notificar incidencias al sistema que normalmente son registradas por un departamento específico de la empresa, servicio de atención al cliente, donde un operador atenderá al cliente registrando la incidencia en el sistema.

En muchas ocasiones, lo que empieza como una incidencia de usuario después de analizar la información obtenido puede derivar en otro tipo de incidencia, con lo que este tipo de incidencias están relacionadas con las demás incidencias. Las soluciones implementadas en este tipo de incidencias son muy diversas, en muchas ocasiones el operador de forma remota o dando instrucciones al usuario resuelve la incidencia y en caso no poder resolverla enviara un técnico.

Este tipo de incidencia no suelen ser muy complejas, siempre que no deriven a otro tipo de incidencias, y el tiempo de respuesta es corto porque suelen resolverse de forma remota, o el tiempo que tarde el técnico es desplazarse, que no suele ser mucho. Este tipo de incidencias son la más fáciles de resolver y no requieren muchos recursos en el proceso de resolución. En empresas con muchos usuarios, la gestión de este tipo de incidencias se asigna a un departamento, aunque lo normal es subcontratar este servicio a una empresa especializada en este tipo de funciones.

Incidencias de seguridad

Este tipo corresponde a cualquier problema surgido en la infraestructura de red debido a un fallo de seguridad en algún componente, generalmente software, permitiendo un acceso no autorizado a la infraestructura de red. Este tipo de incidencia son muy importante de monitorizar porque un fallo en la seguridad del sistema puede provocar acceso a componentes de la red por parte de atacante externo.
Entre las incidencias que podemos encontrar tenemos:

- ⇨ Vulnerabilidades.
- ⇨ Agujeros de seguridad.
- ⇨ Ataques informáticos (DOS, DDOS, zero day, man in the middle, etc.).
- ⇨ Virus informáticos (troyanos, gusanos, etc.).
- ⇨ Accesos no autorizados.

Una buena política de seguridad evita en gran parte este tipo de incidencia, entre las normas que pueden realizarse en la empresa tenemos:

- ⇨ Uso de contraseñas seguras.
- ⇨ Formación de los empleados en materia de seguridad informática.
- ⇨ Componentes actualizados.
- ⇨ Control de acceso a Internet.
- ⇨ Configuración correcta del software.

Las incidencias de seguridad pueden ser difíciles y se deben utilizar técnicas y herramientas específicas para localizarlas. En algunas ocasiones, no se presentan síntomas de bajadas de rendimiento en el sistema, debido a que intentan camuflarse para no ser detectado.
Para detectar las incidencias de seguridad podemos utilizar un conjunto de herramientas específicas en materia de seguridad, entre las cuales existen:

- ⇨ IDS/IPS.
- ⇨ Escáner de puerto.
- ⇨ Cortafuegos.
- ⇨ Antivirus.

Para resolver un incidente de este tipo los desarrolladores de software proporcionan parches de seguridad y actualizaciones que evitan o solucionan agujeros de seguridad descubiertos. Para estar al tanto de los agujeros de seguridad de software existen boletines de seguridad que informan de los últimos descubierto y si existe una parche que los soluciona, o que procedimiento realizar para evitar el agujero de seguridad.
La complejidad de este tipo de incidente es alta, requiere unos conocimientos específicos bastante altos por parte del personal y el proceso de detección de la incidencia puede ser bastante complejo.
Debido a esto el tiempo de respuesta puede ser alto, la detección del incidente y descubrir la causa puede requerir mucho tiempo, aunque implementar una solución no requiere mucho tiempo, generalmente consiste en aplicar un parche de seguridad o una actualización del componente afectado.

Incidencias de red

Problemas que surgen y perjudican el correcto funcionamiento de la red, entre las incidencias que podemos encontrar tenemos:

- ⇨ Cortes de comunicación.
- ⇨ Pérdida de velocidad.
- ⇨ Datos perdidos.
- ⇨ Tráfico de red excesivo.
- ⇨ Problemas de conexión.
- ⇨ Problemas con el ancho de banda.
- ⇨ Congestión de red.

Un aspecto diferenciador de este tipo de incidencia son los medios de transmisión (cables) cualquier problema en el medio perjudica seriamente en el rendimiento, existen herramientas específicas para chequear su funcionamiento.

En las redes se utiliza hardware específico como: routers, punto de acceso, DSLAM, tarjetas de red, etc., que un mal funcionamiento en ellos puede ser la causa del incidente, otras posibles causas que podemos encontrar son:

- ⇨ Mal uso de ancho de banda.
- ⇨ Configuración errónea en un componente hardware.
- ⇨ Ataque informático.
- ⇨ Uso incorrecto de los recursos de red.
- ⇨ Topología de red.

Las incidencias de red pueden estar relacionada con una incidencia de seguridad, porque un problema que surge en la red, como una congestión de red, la causa puede ser un ataque informático a la infraestructura de red de la empresa o un acceso no autorizado (usando un fallo de seguridad) de un atacante externo que ha conseguido el control de recursos de la red.

Respecto a la complejidad de este tipo de incidente, pueden surgir desde incidentes fáciles de resolver, como un cable mal conectado, a incidentes más complejos como una congestión de tráfico por un ataque informático. El tiempo de respuesta dependerá de la complejidad del incidente con un rango amplio de tiempo. Entre las soluciones que podemos encontrar:

- ⇨ Reparación o sustitución de medio del transmisión.
- ⇨ Modificación de la configuración de un componente.
- ⇨ Cambio de la topología de red.
- ⇨ Actualización de componentes.

Incidencias físicas

Representa aquellos problemas surgen en las instalaciones de la empresa, como puede ser:

- ⇨ Accesos no autorizados (robos en las instalaciones).
- ⇨ Accidentes (roturas, averías en las instalaciones).
- ⇨ Fenómenos meteorológicos (incendios, inundaciones, etc.).
- ⇨ Cortes de suministro eléctrico.

En este caso, los incidentes que se producen se podrían englobar dentro de algunas de las categorías anteriores. Por ejemplo, una inundación en las instalaciones puede provocar una caída de los servicios y rotura de hardware, con lo que se podría considerar como una incidencia hardware.

En algunas instalaciones, como instalaciones donde se almacenan los servidores de la empresa. La temperatura de ambiente es muy importante controlarla, a los componentes hardware las temperaturas altas perjudican su funcionamiento e incluso pueden provocar su rotura.

Este tipo de incidencia puede utilizar muchos recursos en proceso de resolución, y en la incidencia donde el daño ha sido alto son complejas de solucionar y el tiempo de respuesta será alto.

Entre las soluciones para incidencias de este tipo son muy variadas, como:

- ⇨ Sistemas de acceso (tarjetas de acceso, control de firma, tornos, sistemas biométricos, etc.).
- ⇨ Sistemas de vigilancia (cámaras, sensores, vigilante, etc.).
- ⇨ Control de temperatura.
- ⇨ SAI y generadores eléctricos de reserva.
- ⇨ Sistemas antiincendios, cámaras ignifugas.

1.4.1. Responsabilidad de la operadora

Un servicio es ofrecido a los clientes a través de un red de comunicaciones, la empresa que gestiona esta red se denomina operadora de comunicación o de telecomunicaciones.

Un proveedor ofrece una serie de servicio a sus clientes a través de la red que proporciona la operadora, el servicio que ofrece la operadora es ofrecer su red para que los proveedores puedan dar servicio a sus clientes. Una operadora puede ser de dos tipos:

- ⇨ Operadora con red: Es una operadora con red propia, ha realizado en un ámbito geográfico un despliegue de líneas de transmisión, proporcionando cobertura de comunicación en una zona geográfica, también disponen de la infraestructura necesaria para realizar la comunicación por sus líneas.

Tener una red propia necesita muchos recursos económicos para el despliegue inicial como para el mantenimiento, son empresas con una gran estructura organizativa compleja para funcionar correctamente.

- ⇨ Operadora virtual: No tienen red propia y necesitan alquilar la red a un operador con red, existen dos tipos de operadora virtuales que se diferencian en la infraestructura que poseen:
  - Revendedores: no poseen infraestructura y depende completamente, solo proporcionan labores comerciales todo los demás depende de un operador con red.
  - Completos: poseen infraestructura propia, como la gestión de la comunicación o departamento técnico, solo necesitan la red de otro operador. Esto proporciona cierto grado de independencia.

Las funciones de cada tipo de operador son las mismas, aunque en los operadores virtuales deben derivar todos los aspectos de la red de comunicación al operador propietario.

El operador tiene un contrato de uso tanto con los proveedores de servicio como con los clientes, aunque este contrato tiene diferentes cláusulas, la principal diferencia es la garantía que proporciona a los servicios, que es bastante más alta a los proveedores que los clientes particulares.

- ⇨ Proveedores de servicios: es un contrato de tipo de empresarial donde especifica las condiciones del servicio, denominado SLA, donde se especifica las características técnicas contratadas.
- ⇨ Clientes particulares: utilizan la red del operador para diferentes servicios como teléfono fijo o móvil, internet o televisión. Se especifican unas características básicas y soporte básico.

Cuando surge una incidencia en la red, el operador es responsable si la causa se ha generado en su red o en su infraestructura, si el operador proporciona determinados equipos a sus clientes y surge un incidencia en el equipo, el operador deberá repararlos.

La operadora dispone de un departamento de soporte técnico, donde se atenderá la incidencia y se asignarán recursos para resolver las incidencias en sus redes.

Otras responsabilidades de la operadora serán:

- ⇨ Garantizar una velocidad mínima: En el SLA debe especificarse la velocidad mínima, que puede alcanzar el 100% de la velocidad contratada, aunque lo normal es que corresponda a un porcentaje bastante menor, para clientes particulares suele ser del 10% de la velocidad contratada.
- ⇨ Acceso a la red: El accedo a la red siempre debe estar disponible, es responsabilidad de la empresa que sus clientes siempre puedan acceder a su red.
- ⇨ Mantenimiento de su infraestructura de red: La operadores deberán dedicar los recursos necesarios para mantener correctamente su infraestructura de red para que los servicios prestado tengan un rendimiento óptimo.
- ⇨ Soporte técnico adecuado: Toda operadora debe disponer un departamento de soporte técnico, mediante un SAT (servicio de atención telefónico) u otro tipo, donde unos operadores registrarán las incidencias de sus clientes e iniciará el proceso de resolución.
- ⇨ Seguridad en la red: El operador se debe encargar de la seguridad de sus redes, evitando cualquier problema causado por un fallo de seguridad, también que la comunicaciones de sus clientes sean seguras y no tengan interferencias u otros problemas

El operador no se hace responsable de los componentes o redes en las instalaciones de los clientes, tanto proveedores o clientes, aunque el operador puede ofrecer un soporte extra (de pago) donde se encargarán de las instalaciones de los clientes. Donde los técnicos de la operadora se desplazarán a las instalaciones de un cliente para resolver las incidencias que surjan.

El operador solo ofrecerá servicio en aquellas zonas geográficas donde tenga cobertura, ya sea mediante su propia red o alquilando la red de otro operador.

El operador no da soporte a servicios de empresas de terceros, solo de los servicios que ellos proporcionan.

Si el servicio es proporcionado por un operador virtual, existen unas cuantas diferencias respecto al operador de red propia. El operador virtual debe disponer de un servicio de soporte técnico a sus clientes, denominado SAU (Servicio de Atención al Usuario), se encargará de la gestión de la incidencia y todas las tareas relacionadas. La operadora derivara todas las incidencias que corresponden a la infraestructura de red al operador que le alquilan la red.

Si el operador es del tipo completo, dispone de sus propias equipos, deberá disponer de un equipo técnico que resuelva las incidencias que se produzcan en sus equipos. La comunicación entre el operador virtual y el operador con red, nunca la deberá realizar el cliente, la gestión corresponde al operador virtual.

1.4.2. Incidencias de usuario

La mayoría de las incidencias que ocurren en la red afectan de forma directa o indirectamente a los usuarios, afectando a los servicios que utilizan, también los usuarios tiene otra serie de incidencias relacionadas con el uso o instalación de un servicio o recursos, necesitando ayuda para utilizar correctamente el servicio o recurso.

En algunas ocasiones, los usuarios suelen ser los primeros en detectarlos y por ese motivo debe tener algún canal para notificar las incidencias que detectan.

La empresa proveedora de los servicios proporciona una serie de canales de comunicación para atender a sus clientes, estos canales pueden ser:

- ⇨ SAT (Servicio de Atención Telefónico): instalaciones de la empresa donde una serie de operadores reciben llamadas telefónicas de los clientes, registrando las incidencias que notifican los usuarios.
- ⇨ Correo electrónico: la empresa dispone de una o varias cuentas de correos electrónico donde recibir las incidencias que han detectado por los usuarios.
- ⇨ Chat: otro canal utilizado es mediante un chat con un operador de la empresa.
- ⇨ Twitter: últimamente las empresas disponen de una cuenta de Twitter para estar en contacto con sus usuarios, donde pueden notificar diferentes problemas.
- ⇨ Herramienta de gestión de incidencias: mediante una aplicación informática, normalmente una aplicación web, pueden registrar una incidencia rellenando un formulario con los datos correspondiente. Ejemplos de este tipo de herramientas tenemos: GLPI, OTRS, RT:Request.

En todos los canales, una serie de operadores de la empresa registrarán la incidencia y comenzarán el proceso de resolución.

Las incidencias de los usuarios podemos dividirlas en varias categorías:

- ⇨ Soporte
- ⇨ Problemas
- ⇨ Facturación y parte comercial

Soporte

Este tipo de incidencia está relacionada con el uso de los servicios que proporciona una empresa a sus usuario, donde podemos encontrar diferentes problemas:

- ⇨ Instalación del servicio o de algún componente (hardware o software) necesario.
- ⇨ Configuraciones.
- ⇨ Uso del servicio.
- ⇨ Fallo del servicio.
- ⇨ Dudas sobre el servicio o algún componente.

La empresa que proporciona un operador recibe las incidencias de los usuarios, analiza la información que proporciona e intenta resolverla, en caso de no poder resolverlas por no tener los conocimientos o recursos necesarios para resolverlas, realiza el proceso de derivar la incidencia a otro departamento más especializado.

Las incidencias el operador las recibe por diversos canales de comunicación que proporciona la empresa, como puede ser: SAT, correo electrónico, chat y Twitter.

La comunidad de usuarios de un servicio pueden proporcionar otros métodos para resolver dudas, principalmente son dos métodos:

- ⇨ Foros: es una aplicación web con una estructura donde un usuario puede dejar un mensaje que podrá ser leído por el resto de usuario y responder, creando un hilo de conversación. Los foros permiten diferentes funcionalidades como categorías o temas. Los foros son muy utilizados en Internet para resolver dudas.
- ⇨ Wiki: página web con estructura para crear, modificar un texto compartido entre varias personas, es muy utilizado como base de conocimiento de un determinado tema, donde mostrar información de forma organizada sobre un tema. El ejemplo más famoso es Wikipedia.

Estos dos métodos tienen como ventaja su bajo coste, hay empresas que proporcionan estos métodos, sobre todo pequeñas empresas, para dar soporte a sus usuarios.

Problemas

En este caso, las incidencias producidas son debidas a problemas que surgen con el servicio utilizado por el usuario y provoca que no funcione de forma correcta.
En muchas ocasiones, el usuario necesita algún tipo de componente hardware o software para utilizar un servicio, estos componentes son proporcionados por la empresa proveedora. Cualquier problema en estos componentes son incluidos en esta categoría.
Entre los incidentes tenemos:

- ⇨ Fallo en el componente proporcionado por la empresa.
- ⇨ Bajo rendimiento del servicio.
- ⇨ Velocidad del servicio inferior a la contratada.
- ⇨ Corte del servicio.

Los canales de comunicación para notificar este tipo de incidencias por parte de los usuarios son los mismos expuestos en el punto anterior.
La empresa dispone de recursos que permiten conocer los distintos problemas que surgen en un servicio, sin necesidad de esperar una notificación por parte de un usuario, ahorrando tiempo en el proceso de resolución.

Facturación y parte comercial

Fuera del ámbito técnico de los servicios, existen otros aspectos donde el cliente puede encontrar problemas. Los dos principales son, la facturación que incluye todo los relacionado con el coste económico en función del uso del servicio, y la parte comercial que incluye aspectos como la venta del servicio y las condiciones.
Entre los incidentes que podemos encontrar:

- ⇨ Fallos en el pago de un servicio.
- ⇨ Facturas erróneas.
- ⇨ Alta de un servicio no contratado.
- ⇨ Datos del usuario incorrectos.
- ⇨ Condiciones del servicio no son las contratadas.

Este tipo de incidencias no técnicas son resueltas por departamentos específicos, normalmente denominado departamento comercial y facturación, que dispone la empresa y donde utilizan recursos específicos. Si la empresa dispone de un SAT, hay determinados operadores asignados a estas incidencias, con una formación y conocimientos específicos a las incidencias que tramitan.

1.4.3. Incidencias del proveedor del servicio

Una empresa proporciona una serie de servicios a una serie de clientes y la empresa recibe una cantidad económica u otro tipo de contraprestación por parte de sus clientes.
Para obtener un nivel de satisfacción por parte del cliente en el uso del servicio, la empresa debe vigilar varios aspectos del servicio como:

- ⇨ Disponibilidad: el servicio debe estar siempre disponible, la empresa debe utilizar todos los recursos disponibles para cumplir este punto.
- ⇨ Rendimiento: el servicio debe funcionar de forma óptima y con una calidad aceptable para que los clientes puedan hacer uso del servicio sin problemas.
- ⇨ Seguridad: el servicio debe garantizar que ninguna otra persona pueda utilizar este servicio y tener un grado de privacidad en el trabajo que realiza el cliente en el servicio. La empresa debe garantizar que los datos de los clientes no sean utilizado para otros fines que no sean los estipulados en el contrato con el cliente.
- ⇨ Soporte: la empresa debe proporcionar una canal para ayudar a los clientes en el uso de servicio.
- ⇨ Tiempo de respuesta: cuando surge una incidencia, el proveedor activa la operativa para resolver la incidencia y esto conlleva un tiempo, que debe ser el mínimo posible, esto se denomina tiempo de respuesta.

Estos puntos deben estar especificados en un contrato con el cliente donde se especifican tanto unas características técnicas como económicas (pago por el servicio).
La empresa puede incluir un valor umbral mínimo en algunos puntos del servicio para ofrecer un nivel de garantía mínimo, dependiendo si un contrato para un cliente empresarial o particular, la garantía será diferente.
Por ejemplo, para una empresa la garantía de disponibilidad puede estar en el 100% (siempre está disponible) o tiempo de respuesta máximo garantizado (el incidente deberá estar resuelto como máximo en un número de horas determinado). En cambio para un cliente particular es posible que no tenga la disponibilidad garantizada o no disponga de un tiempo de respuesta máximo, aunque posiblemente el proveedor del servicio disponga de soporte de pago que permita mejorar esas condiciones.
Entre las incidencias que pueden ocurrir que son responsabilidad del proveedor del servicio tenemos:

- ⇨ Fallo en los componentes del proveedor
- ⇨ Mal rendimiento del servicio
- ⇨ Corte en el servicio
- ⇨ Fallo de acceso al servicio
- ⇨ Fallo en la instalación del servicio
- ⇨ Fallo de facturación
- ⇨ Gestión comercial errónea

Para algunos servicios los proveedores deben proporcionan algunos componentes (software o hardware) para que los clientes usen un servicio, estos componentes son mantenidos por el proveedor y cualquier incidencia debe ser reparada por ellos.
Dependiendo de la incidencia, es gestionada por uno o varios departamentos que pueden ser:

- ⇨ Técnico: compuesto por personal que se encarga del mantenimiento y resolver las incidencias de un sus servicio y componente, dispone de una serie de recursos para ejecutar su funciones.
- ⇨ Facturación: muchos servicios son de pago y el cliente debe pagar una cantidad económica por usar un servicio. Este departamento se encarga de la gestión del cobro de los servicio y la emisión de una factura a los clientes con el coste del servicio y otro tipo de información.
- ⇨ Comercial: compuesto por personal que se encarga de la parte comercial del servicio, como el alta o baja de un servicio, la contratación de un servicio extra (como un soporte de pago) o la comunicación con el cliente ofreciendo productos de la empresa.

La comunicación del proveedor con sus clientes utiliza unos recursos específicos que pueden ser propios del proveedor o subcontratados a una empresa especializada, entre los recursos tenemos:

- ⇨ Servicio de atención al cliente
- ⇨ Centro de llamadas

Servicio de atención al cliente

Se encarga de la comunicación con el cliente, proporciona diversos canales para que el cliente pueda ponerse en contacto con el proveedor, para diversas tareas como:

- ⇨ Incidencias.
- ⇨ Dudas sobre el servicio.
- ⇨ Quejas.
- ⇨ Alta o baja de un servicio.
- ⇨ Fidelización de clientes.

Puede disponer de sus propias instalaciones para realizar estas tareas o subcontratar a una empresa especializada.
Centro de llamadas
También denominado como Call Center, está compuesto por unas instalaciones donde un conjunto de operadores reciban vía telefónica llamadas de los clientes exponiendo sus problemas y dudas. Estos operadores pueden ser de distintos departamentos (técnico, facturación o comerciales) generando incidencias de su tipo.
Entre las funciones de un operador tenemos:

- ⇨ Resolver incidencias.
- ⇨ Rellenar partes de incidencias.

- ⇨ Resolver dudas.
- ⇨ Notificar incidencias.
- ⇨ Ayudar al cliente a resolver una incidencia.
- ⇨ Derivar una incidencia a otro departamento.
- ⇨ Realizar el escalado de una incidencia.
- ⇨ Gestionar una incidencia.
- ⇨ Vender servicios del proveedor.

Los centros de llamadas están incluidos dentro de los servicios de atención al cliente y son muy utilizados por grandes empresas, tienen un coste económico alto, existiendo empresas especializadas que proporcionan centro de llamadas a las empresas.

En los centros de llamadas, los operadores utilizan una serie de herramientas específicas para realizar sus tareas, generalmente cuando se recibe una llamada comienza un proceso denominado operativa que se encarga de determinar los que el operador debe decir y hacer para resolver el problema del cliente. Esta operativa depende del problema del cliente y permiten ahorrar tiempo en el proceso de resolución.

En los centros de llamadas es donde habitualmente se realiza la gestión de las incidencias producidas en los servicios del proveedor. El proveedor de servicio requiere de una red de comunicación para proporcionar una serie de servicios, si alquila la red a otro operador todas las incidencias relativas a la red de comunicaciones deben ser resueltas por el operador de la red de comunicación.

2 Instalación de aplicaciones de comunicaciones en equipos terminales

2.1. Terminales de comunicaciones

Los operadores proporcionan un serie de dispositivos hardware para poder acceder a su red comunicaciones, estos dispositivos depende del tipo de red y de la tecnología utilizada. Cada tipo de red utiliza un hardware especifico y solo puede ser utilizado para acceder a esa red, dentro de un tipo de red puede utilizar diferentes tecnologías y cada tecnología necesita un hardware especifico.
Dentro de los tipos de redes de comunicaciones tenemos:

- ⇨ Telefonía fija
- ⇨ Telefonía móvil
- ⇨ Internet
- ⇨ Televisión
- ⇨ Satélite

Este tipo de redes de comunicación son las más utilizadas, aunque existen otras. Cada tipo de red proporciona una serie de servicio utilizando una serie de tecnologías y un medio de transmisión. Los medios de transmisión se dividen en dos:

- ⇨ Físicos: la comunicación se transmite mediante un cable, existiendo diferentes tipos.
  - o Cable coaxial.
  - o Fibra óptica.
  - o Par trenzado.
- ⇨ Inalámbrico: la comunicación se transmite mediante una serie de ondas por el aire.

Un cliente utiliza una serie de servicios de uno o varios proveedores de servicios, para acceder a esos servicios debe utilizar una red de comunicaciones proporcionada por un operador. El operador pone a disposición del cliente un dispositivo hardware para acceder a su red de comunicaciones y poder dichos servicios.

El hardware de acceso proporcionado por el operador está configurado para acceder a su red y generalmente proporciona un serie de funcionalidades extras. También el hardware de acceso puede ser adquirido por el cliente en otro lugar, en este caso el cliente debe configurarlo para tener el acceso a la red de comunicación.
Este hardware comparado con el proporcionado por el operador, tiene un coste económico mayor aunque proporciona mas funcionalidades.
Existen diversas tecnologías que pueden ser implementadas en una red de comunicaciones por el operador, el hardware de acceso debe tener la capacidad de usar esas tecnologías.

RED	TECNOLOGÍAS	SERVICIOS
Telefónica	xDSL, VoIP, RDSI, FTTH, HFC	Internet, correo electrónico, llamadas de voz, televisión a la carta.
Móvil	GSM, 3G, 4G, HSDPA	Llamadas de voz, Internet, SMS, correo electrónico.
Inalámbrica	Wifi, Bluettooth, NFC, RFID	LAN,Voz, compartir datos, control de acceso.
Satélite	DVB-S2, DAB, DBS	Televisión, radio, Internet, llamadas de voz.
Televisión	PAL, TDT	Televisión, Internet, teletexto.

Como se muestra en la tabla las redes de comunicación tiene algunos servicios que son comunes en varias redes, como Internet.

2.1.1. Tipos y características

Cada hardware de acceso tiene que cumplir una serie de requisitos para utilizar la red comunicación. Existen diferentes tipos de hardware de acceso para una red y dependiendo de la tecnología de acceso que se utilice, tendrá sus propias características.

Una primera distinción seria si el tipo medio de comunicación.

- ⇨ Cableado: utiliza algún tipo de cable para el acceso, el dispositivo debe tener un conector compatible con el tipo de cable.
- ⇨ Inalámbrica: la transmisión es realizada por medio de la emisión de señales, el dispositivo necesita un componente que permita emitir y recibir señales, este componente se denomina antena. Dependiendo de la red de comunicación existen diversos tipos de antenas (omnidireccionales, planas, yagi, parabólicas, etc.).

Dependiendo del medio las características del hardware de acceso son diferentes, aunque existen hardware de acceso por proporciona un interfaz para diversos tipos de conexión, como cableado e inalámbrico.

Una lista de hardware de acceso sería la siguiente.

HARDWARE	RED	SERVICIOS
Teléfono	Telefónica, móvil, fibra, cable, satélite	Llamadas voz
Módem	Telefónica, móvil	Internet, teléfono
Router	Telefónica, fibra	Internet, teléfono, televisión...
Cablemodem	Cable	Internet, teléfono, televisión...
Mifi	Móvil, inalámbrica	Internet
Decodificadores	Televisión, satélite	Televisión
Terminal IP	Telefónica, cable, fibra, móvil	VoIP

En la actualidad hay una gran concentración de servicios hacia Internet, servicio como la televisión o teléfono se está migrando hacia Internet con tecnologías como VoIP para el teléfono e IPTV para televisión. Posiblemente en un futuro no muy lejano con aumento de velocidad y ancho de banda en tecnología como la fibra óptica, todos los servicios serán emitidos por Internet.

Algunos de los dispositivos hardware han sido vistos anteriormente, en el módulo 1874, donde se describían hardware de red.

Teléfono

Es un dispositivo para realizar llamadas de voz, permitiendo el envío de señales tanto analógicas como digitales para codificar la voz. Este tipo de dispositivo puede ser de dos tipos dependiendo del tipo de señal que emite.

- ⇨ Analógica: son los teléfonos tradicionales ofrecen un servicio de transmisión de voz y algunos servicios adicionales, dependiendo de la operadora.
- ⇨ Digital: con la llegada de nuevas tecnologías como RDSI o ADSL que permiten utilizar señales digitales para codificar la voz. Los dispositivos digitales tiene una apariencia similar a un teléfono analógico aunque pueden ofrecer otro tipo de servicios como videollamadas. La calidad de la señal de voz es superior a la conseguida con la analógica aunque consume más recursos. En España, haya varios operadores de comunicaciones, como Vodafone y Orange, que ofrecen teléfono de forma digital.

El teléfono es utilizado en múltiples redes, aunque sigue siendo muy utilizado en la red telefónica tradicional (par de cobre), pero también es utilizado en otro tipo de redes como fibra o cable, y principalmente es

utilizado para servicios de voz. En la actualidad con el auge de la telefonía móvil se está implementado de forma masiva la red móvil, aumentando el uso de terminales móviles en detrimento de teléfonos fijos. De hecho, en la actualidad el número de teléfonos móviles supera al de teléfonos fijos.
El uso de terminales móviles más avanzados denominados teléfonos inteligentes o smartphone ha conseguido gran aumento en el uso de otro tipo de servicio, aparte de servicio de voz, como puede ser internet. En la telefonía móvil, el uso de los servicios de voz está disminuyendo de forma muy importante.
Para el acceso a internet mediante una red móvil, utiliza diversas tecnologías como 3G o 4G que proporcionan una alta velocidad que permiten utilizar otros servicios distintos de las llamadas de voz.
Las operadoras están dando más importancia en sus tarifas al tráfico de datos (Internet) que a tráfico de voz.
Debido al aumento de estos terminales, ha aumentado el uso de otros servicios, como el uso de internet y otros como: mensajería instantánea, redes sociales, correo electrónico y videollamadas.
Estos servicios no son implementados en la telefonía analógica, en la telefonía digital algunos de estos servicios si pueden ser implementados aunque no son muy demandados.
Otro tipo de terminales más específicos es el teléfono satélite, que realiza la comunicación mediante satélites de comunicación en órbita geoestacionaria. Este tipo de terminal es utilizado en aquellas zonas donde no hay cobertura de otro tipo de red, normalmente en zona remotas, como zonas montañosas.
Este tipo de teléfono es utilizado principalmente para llamadas, aunque puede integrar otros servicios como un GPS, muy útil para las zonas donde es utilizado. Debido a sus características son teléfonos caros, con una buena duración de batería y muy robustos, están preparados para soportar temperaturas extremas, resistencia a choques y agua.

Módem

Cuando solo existía la red telefónica mediante el par de cobre, para acceder a Internet era necesario un dispositivo que permitiera convertir una señal digital (ordenador) en señal analógica (línea telefónica), este dispositivo se denomina módem y permitía el acceso a Internet. En la actualidad, para el acceso a Internet por red telefónica no es utilizado siendo sustituido por otros dispositivos. Aunque en las redes móviles se sigue utilizando para conexión a internet desde un ordenador.
Este tipo de dispositivo solo proporciona la función de conexión y no incluyen otro tipo de funcionalidad.
Los móviles se pueden diferenciar en diversas categorías, dependiendo de la conexión tenemos:

- ⇨ Internos: son instalados dentro de otro dispositivo para acceder a Internet y dependen de este dispositivo para funcionar (no son autónomos).
- ⇨ Externos: son dispositivos autónomos que son conectados al dispositivo para acceder a internet mediante un tipo de conexión, habitualmente se utiliza una conexión USB.

Son utilizado con diferentes tecnologías como 3G, ADSL o RDSI.
Otro aspecto importante de los módem es que necesitan un proceso de conexión/desconexión para su funcionamiento.

Router

Es un dispositivo para acceder a internet mediante redes de telefonía (par de cobre o fibra) incorporando un módem para ADSL. Se puede considerar que es el sucesor del módem y es el dispositivo de acceso utilizado por las operadoras de comunicaciones para dar acceso de Internet a sus clientes. Las funcionalidades que permite dependen del firmware que tenga instalado el router.
Dependiendo del router, puede incluir múltiples funcionalidades como:

- ⇨ Conexiones Ethernet: un router permite conectar varios dispositivos, habitualmente cuatro dispositivos, mediante puertos de Ethernet. Permite gestionar el acceso a Internet de varios equipos y configurar una red entre ellos.
- ⇨ Wifi: este tipo de dispositivos incluyen una antena, para conexiones inalámbricas tipo Wifi, esta conexión permite la comunicación inalámbrica a distintas velocidades (estándar 802.11). Dependiendo del soporte existen diversos tipos como a/b/g/n que implementan diversos tipos de velocidades. También permite encriptar este tipo de conexiones utilizando diversos protocolos (WEP, WPA, WPA2, etc.)

- ⇨ Puertos USB: en algunos router incluye una serie de puertos USB, habitualmente uno o dos, donde conectar otros dispositivos como disco duros o impresoras y ampliar la funcionalidades del router, como:
  - FTP: permite almacenar fichero, pudiendo subir y descargar archivos desde un cliente de FTP.
  - NAS: permite tener almacenar datos que son compartidos en una red utilizando diversas tecnologías.
  - Samba: permite compartir datos con máquinas con Windows.
  - Servidor de impresión: permite gestionar los trabajos de una impresora en red.
- ⇨ Firewall: prácticamente todos los router modernos incluyen un cortafuego para controlar el acceso a la red, especificando un conjunto de reglas.
- ⇨ DNS: permite especificar DNS utilizado para el acceso a Internet, en router de gama alta permite tener más opciones como un servidor de DNS.
- ⇨ DHCP: incluye un servidor un DHCP para la asignación de direcciones IP a los equipos de la red.
- ⇨ VPN: permite realizar conexiones utilizando esta tecnología.
- ⇨ QoS: permite ejecutar diversos mecanismos para garantizar el rendimiento de la red.

Esto es una pequeña lista de las funcionalidades que puede incluir un router, dependiendo del firmware y el hardware que incluye, las funcionalidades soportadas serán más amplias.

A diferencia de los módem no necesitan un proceso de conexión desconexión, solo es necesario suministrarle electricidad y encenderlos, el router siempre estará conectado y proporcionando acceso a Internet.

La velocidad de acceso dependerá de la tecnología utilizada para la conexión, principalmente son dos tipos:

- ⇨ Tecnologías xDSL: conjunto de tecnologías que permiten la transmisión analógica (líneas de teléfono de par de cobre) de datos digitales.
- ⇨ Fibra óptica: este tipo de tecnología permite transmisiones a gran velocidad y con pocas interferencias. Los router que soportan esta conexiones tienen las misma funcionalidades que los router de ADSL a diferencia de la conexión para acceder a la red de comunicaciones.

Terminales IP

Estos dispositivos permiten realizar comunicación de voz mediante datos digitales, son el sucesor de las llamadas de voz tradicionales. Esta comunicación se realiza mediante las mismas tecnologías para acceder a Internet, como ADSL o Cable.

Los terminales IP tienen una apariencia parecida a los teléfonos aunque su funcionamiento e instalación son diferentes. Para su funcionamiento necesita una dirección IP de Internet, igual que un ordenador, y utiliza una serie de tecnologías como VoIP. Esta tecnología permite el uso diversos protocolos como:

- ⇨ SIP
- ⇨ H.323
- ⇨ IAX
- ⇨ IAX2
- ⇨ MGCP
- ⇨ Jingle
- ⇨ WeSip
- ⇨ Skype
- ⇨ CorNET-IP

Estos protocolos ofrecen una serie de servicios que pueden ser:

- ⇨ Llamadas de voz.
- ⇨ Videoconferencias.
- ⇨ Mensajes de texto.

También existen terminales de VoIP que utilizan redes de telefonía móvil utilizando una conexión de datos.

Igual que los teléfonos tradicionales, los terminales VoIP necesitan un número de teléfono para realizar las comunicaciones con otros teléfonos, ya sean IP, móviles o tradicionales. Este número es proporcionado por un proveedor de servicios que se encarga de la conexión y transmisión utilizando una conexión a Internet.

Se ha comentado los terminales IP como teléfonos digitales, pero existen otros tipos de terminales IP, que son los siguientes:

- ⇨ Softphone
- ⇨ VoIP con teléfono analógico
- ⇨ Teléfono Wifi
- ⇨ Empresarial

Softphone

Aplicación informática instalada en un PC que permite realizar llamadas de voz y solo requiere conexión internet para su funcionamiento.
En caso de querer comunicaciones con otros teléfonos analógicos o móviles requiere el pago de una tarifa, existen diferentes empresas que ofrecen este servicio. En cambio, para la comunicación entre dos softphone suele ser gratuito.
Es posible realizar llamadas a otros teléfonos sin pagar una tarifa, pero para esto necesitaríamos un hardware específico para montar una centralita digital o PBX, también se necesita una línea de teléfono (con su número) y una conexión a Internet.
Últimamente están surgiendo aplicaciones para Smartphone para realizar llamadas VoIP, son aplicaciones softphone para el móvil, utilizando la conexión Wifi o la conexión de datos del móvil para realizar las llamadas.

VoIP con teléfono analógico.

Un teléfono tradicional (analógico) puede ser usado para realizar llamadas por VoIP, necesita un adaptador telefónico denominado ATA.
Este tipo de adaptador está compuesto por un conjunto de conectores para teléfonos analógicos y un conector Ethernet que permite conectarlos a una LAN, también puede disponer de un puerto WAN.
El adaptador ATA convierte los paquetes de datos de Internet en señales analógicas para el teléfono y viceversa, es necesario contratar un servicios de VoIP a un proveedor para su funcionamiento.

Teléfono Wifi

Estos dispositivos permiten realizar llamadas mediante una conexión Wifi, simplemente es un teléfono VoIP pero inalámbrico que se conecta al router que da acceso a Internet mediante una conexión inalámbrica.

Empresarial

Con la tecnología actual, una empresa puede sustituir una estructura telefónica analógica por estructuras digitales, como cualquier empresa tiene acceso a Internet y un número de teléfono, se puede realizar el cambio. Para esto necesitaría:

- ⇨ Centralita PBX: hardware con una serie de conexiones donde se podrían conectar los teléfonos analógicos, teléfonos IP y ordenadores con softphone. Esta conexión se realiza mediante una serie de puertos analógicos, para teléfonos, y puertos Ethernet.
- ⇨ Acceso a Internet.
- ⇨ Línea telefónica, si no quieres línea de teléfono, realizarlo todo por Internet, hay que contratar un proveedor de VoIP para que te asigne un número.
- ⇨ Opcionalmente, teléfonos (analógicos/digitales) y softphone.

Con estos elementos tenemos todo el sistema telefónico de forma digital, esto conlleva una serie de ventajas:

- ⇨ Con los softphone, un ordenador se convierte en teléfono digital permitiendo realizar llamadas y recibirlas.
- ⇨ La centralita PBX permite crear extensiones telefónicas, se podrán derivar las llamadas a cualquier dispositivo (teléfonos y softphone).
- ⇨ Gestión de las llamadas telefónicas.
- ⇨ Contestador automático.
- ⇨ Llamadas en espera.
- ⇨ Envío de SMS.
- ⇨ Sistema IVR.

Por último, un aspecto a tener en cuenta en los sistemas de VoIP es que la señal de voz debe codificarse y decodificarse para la transmisión por la red. Para esto se utiliza un software denominado códec que permite garantizar una calidad en la señal de voz y que esta consuma el menor ancho de banda.
Existen varios códec que proporciona distintas calidades de señal y compresiones, hay que tener en cuenta que la calidad de señal de voz es directamente proporcional a la cantidad de datos que necesita transmitir, calidad más alta más datos trasmite.

CableModem

Son dispositivos que sirven para dar acceso a redes de comunicación por cable. Este tipo de redes originalmente son utilizadas para la transmisión de señal de televisión, habitualmente denominada televisión por cable. En la actualidad también proporcionan servicio de teléfono e Internet.
Las operadoras de este tipo de redes utilizan como medio de transmisión cable coaxial, lo normal es utilizar una infraestructura híbrida de fibra óptica y coaxial (HFC). Dentro de una zona geográfica pequeña, como un barrio o una calle, existe una infraestructura de un cable coaxial que es compartida por todos los clientes de la zona, en zonas con gran densidad demográfica se instalan varios cables. Esta es una de las características, y de críticas, de la red por cable que es la idea de línea compartida.
La operadora solo pueden ofrecer sus servicios en aquellas zonas donde tengan su red por cable instalada, y por ese motivo este tipo de redes suelen tener menos cobertura que las redes de telefonía (par de cobre).
A diferencia de otras tecnologías como ADSL (utilizando redes de telefonía), las redes de cable proporcionan más velocidad y unas características técnicas superiores. Las características técnicas de un cablemodem son similares a las que proporciona un router, la principal diferencia es el conector para el acceso a la red, al utilizar un cable coaxial.
El funcionamiento técnico tanto del cablemodem como de la red está especificado por un estándar, existen dos posibilidades.

- DOCSIS: es el estándar surgido en Norteamérica, utilizado también en Sudamérica.
- EURODOCSIS: es la versión europera, cuya principal diferencia es el ancho de banda de los canales de cable, 8 Mhz para Norteamérica y 6 Mhz para Europa.

Actualmente está implantada DOCSIS 3.0 que apareció en 2006, existe una última versión DOCSIS 3.1 que apareció a principios de 2014, todavía no está muy implantada. Esta última versión consigue igualar en prestaciones a la redes de fibra óptica. El organismo de regular las especificaciones DOCSIS se llama CableLabs que es un consorcio de empresa de cables.

2.1.2. Sistemas operativos y lenguajes de programación específicos para terminales

Toda red de comunicaciones está compuesta por un conjunto de dispositivos hardware de diferentes tipos como pueden ser:

- Ordenadores.
- Router.
- Impresoras.
- Switch.
- Bridge.
- Gateway.
- Teléfonos.
- Centralitas.
- Etc.

Todo dispositivo debe tener un software que lo gestione, dependiendo del dispositivo tenemos:

- Firmware: software que funciona a bajo nivel, que permite gestionar un determinado hardware, es utilizado en hardware de comunicación (router, switch), impresoras o teléfonos.
- Sistema operativo: software compuesto por un conjunto de componentes que permiten gestionar hardware y proporciona una serie de servicios a distintas aplicaciones informáticas. Utilizado principalmente en ordenadores, existen sistemas operativos específicos para un determinado hardware como teléfonos o router.

El sistema operativo proporciona más funcionalidades que un firmware y este último está mas asociado a un determinado hardware.

Respecto a los sistemas operativos, en el ámbito de las redes de comunicaciones podemos considerar dos categorías, en función de los específicos que sean, tenemos:

Categorías de sistemas operativos	Genérico: Linux, Windows, MacOsX
	Específicos: Cisco IOS, JunOS, RouterOS, OpenWrt, DD-WRT, Android, IOS

Los sistemas operativos genéricos son utilizados principalmente en ordenadores, tanto para usuarios (portátiles, sobremesa, netbook, etc.) como para un uso más profesional (servidores o estaciones de trabajo). Los sistemas operativos específicos están adaptados para hardware determinado, algunos de ellos disponible para hardware de una empresa (Cisco, IOS).
Sistemas como Windows, MacOSX y Linux están prácticamente en todas las redes de comunicaciones, este tipo de sistemas operativos se encuentran principalmente en:

- ⇨ Ordenadores personales: son los dispositivos que utilizan los usuarios de la red y permiten utilizar los servicios de un proveedor a través de la red de una operadora. Aquí se pueden incluir sobremesa, portátil, netbook, ultraportátil y cualquier dispositivo para un usuario común.
- ⇨ Servidores: utilizados por las empresas para ofrecer servicios a sus usuarios, son ordenadores con unas características especificas, en función del o los servicios que proporcionan, entre esas características tenemos.
    - Redundancia: algunos componente se encuentran duplicados para en caso de fallo no afecte al funcionamiento del servidor.
    - Potencia: dependiendo del servicio que ofrezcan y a cuantos usuarios, pueden soportan una gran carga de trabajo, deben ser potentes para cumplir con su tarea.
    - Temperatura: son dispositivos que pueden producir mucho calor, deben estar correctamente refrigerado mediante una serie de ventiladores internos y otros sistemas de refrigeración externa.
    - Disponibilidad: los servicios que proporciona un servidor siempre deben estar activos, una de las características que debe disponer un servidor es tener los mecanismos adecuados para conseguir una alta disponibilidad.

Los sistemas operativos anteriormente citados, tienen versiones para ordenadores personales y para servidores.

Sistema Operativo	Versiones
Windows	*Personal:* XP, 98, Vista, 7 y 8. *Servidor:* 2003, 2008, 2008 R2, 2012, Small Bussines, Essential Bussines, Home.
MacOSX	*Personal:* Cheetah, Puma, Jaguar, Panther, Tiger, Leopard, Snow Leopard, Lion, Mountain Lion, Maverick. *Servidor:* OS X server.
Linux	*Personal:* Fedora, Ubuntu, OpenSuse, Elementary OS… *Servidor:* Debian, Red Hat, Ubuntu Server, CentOS…

En este apartado, también podemos incluir otro sistemas operativos cuyo uso es mas minoritario como pueden ser: Unix y sus variantes o la familia de sistemas BSD (OpenBSD, netBSD, FreeBSD).
Existen un conjunto de sistemas operativos específicos, normalmente suelen estar asociado a hardware de comunicaciones y de seguridad, como router o firewall, aunque algunos pueden ser instalado en PC normal.
Este tipo de sistema operativo suele estar desarrollado por una empresa para sus propios productos, esto proporciona una serie de ventajas.

- ⇨ Optimización: está diseñado para un hardware específico y permitiendo adaptar el sistema a las especificaciones del hardware.
- ⇨ No necesita instalación.

- ⇨ Aprovecha los recursos del hardware.
- ⇨ Consumo bajo.

Estos sistemas proporcionan una interfaz web para acceder a sus funcionalidades y una línea de comandos para ejecutar comandos.

Cisco IOS

Desarrollado por la compañía Cisco System y utilizado en sus productos como router, switches, firewall, etc. Es un sistema operativo multitarea que permite realizar tareas de encaminamiento, conmutación de paquetes o control de tráfico.
Este sistema operativo incluye una interfaz de línea de comandos (CLI) que proporciona un conjunto de comandos, también incluye una interfaz de web donde el usuario puede administrar el dispositivo.
La empresa Cisco proporciona dispone de un conjunto de software que utiliza Cisco IOS que permite ser utilizado en la amplia gama de producto, enfocándose en múltiples ambientes como: seguridad, movilidad o enrutamiento.

Router OS

Desarrollado por la empresa Mikrotik que desarrolla hardware de red como router, switches y firewall, también desarrolla su propio sistema operativo para sus productos.
Router OS está basado en GNU/Linux he implementa diversas funcionalidades para empresas proveedoras de servicios, es muy utilizado en pequeñas y medianas empresas ISP. Existe una versión específica para switch denominada SwitchOS.
Existen diversas versiones de Router OS incluyendo una versión para PC, esta versión se puede descargar e instalar de forma gratuita.

JunOS

Es un sistema operativo de la empresa Juniper Networks dedicada a sistemas de redes y seguridad, proporciona diverso hardware como Gateway, router, firewall, VPN o IDS.
Es un sistema operativo basado en FreeBSD. La empresa proporciona un SDK que permite realizar personalizaciones del sistema. JunOS incluye un CLI y una interfaz de web de usuario. El sistema operativo dispone de las siguientes características:

- ⇨ Modularidad.
- ⇨ Enrutamiento.
- ⇨ Seguridad.
- ⇨ Políticas de control.
- ⇨ Cumple con los estándares.

OpenWRT y DD-WRT

Son distribuciones de Linux basadas en el firmware del dispositivo Linksys WRt54G, que en la actualidad soporta múltiples dispositivos de varias marcas. Estos sistemas permiten añadir funcionalidades no soportadas por el firmware original de los dispositivos soportados. Aunque algunas marcas incluyen estos sistemas preinstalados, como la marca Buffalo con DD-WRT, requiere una instalación manual en el dispositivo, borrando el firmware original del dispositivo. Este proceso depende del dispositivo, aunque como norma general para un usuario medio no presenta una gran dificultad.
Los dos sistemas proporcionan un CLI y una interfaz web para la gestión, los dos sistemas principalmente presentan diferencias técnicas y en los dispositivos soportados.

Con el auge de los teléfonos móviles y en especial de los Smartphone, han surgido una serie de sistemas operativos específicos para estos dispositivos.
Aunque existen múltiples sistemas operativos para móviles, hay dos que son los más utilizados:

- ⇨ IOS: sistema operativo especifico para los productos de la compañía Apple y desarrollado por la misma compañía, que engloba a móviles como tablets.
- ⇨ Android: sistemas operativo desarrollado por la empresa Google que utilizado por diferentes marcas en múltiples dispositivos, como móviles, tablet, televisores, ordenadores, etc.

Los dos sistemas proporcionan unas funcionalidades parecidas a un Smartphone; algunas funcionalidades son proporcionadas por el sistema y otras mediante la instalación de software, algunas de estas funcionalidades son:

- Reproducción de contenido multimedia.
- Organizador de tareas.
- Correo electrónico.
- GPS.
- Agenda de teléfono.
- Navegador Web.
- Mensajería instantánea.
- Redes sociales.

Las diferencias entre los dos sistemas radican principalmente en la interfaz de usuario y en algunas funcionalidades más especificas.

IOS

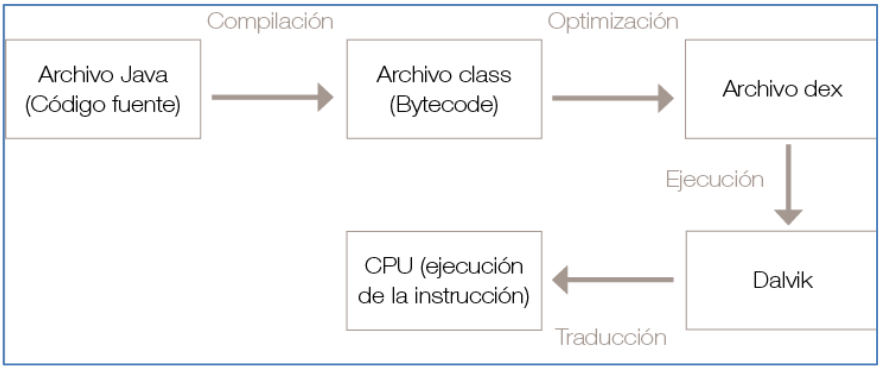
Sistema operativo desarrollado por Apple para el teléfono móvil de la compañía -iPhone-, aunque en la actualidad es usado en otros productos de la compañía como: ipodtouch, Ipad y Apple TV.
IOS está basado en una variante propia de BSD denominada Darwin BSD, este sistema es tipo Unix, está escrito en objective-C, C y C++. Este sistema proporciona una núcleo hibrido denominado XNU que es software libre, este núcleo también es utilizado en Mac OS X. Este núcleo compuesto por componentes de un micronúcleo Mach y código procedente de FreeBSD.
XNU es un kernel híbrido y posee características de los núcleos monolíticos y los micronúcleos. Intentando hacer un mejor uso de las dos tecnologías, como la capacidad de pasar mensajes de los micronúcleos, permitiendo una mayor modularidad y que grandes porciones del SO se beneficien de la protección de memoria. Asimismo, permite mantener la velocidad de los núcleos monolíticos para desempeñar determinadas tareas.
Interfaz de usuario de IOS versión 7
Una característica de IOS es la asociación perfecta con el hardware, como Iphone. Como la empresa que desarrolla el sistema es la misma que fabrica el hardware, este sistema está muy optimizado para ese hardware, necesitando menos recursos para un funcionamiento óptimo.

Mach es componente principal de XNU, “proyecto de diseño de sistemas operativos iniciado en la Universidad Carnegie Mellon con el objetivo de desarrollar un micronúcleo”. El objetivo de Mach es crear un sistema operativo para la computación distribuida, proporcionando características como:

- Multitarea.
- Hilos.
- Soporte a multiprocesadores.
- Protección y seguridad de memoria.

Android

Sistema operativo desarrollado por Google basado en un kernel de Linux y está enfocado a teléfonos móviles y tablets, aunque es utilizado en otros dispositivos como ordenadores o media center. Está desarrollado en C, principalmente en el kernel, y Java para la interfaz de usuario, el sistema es ejecutado en una máquina virtual denominada Dalvik que permite ejecutar aplicaciones programadas en Java.



La máquina virtual Dalvik proporciona una serie de características:

- ⇨ Aumento de rendimiento en dispositivos móviles.
- ⇨ Necesita poca memoria.
- ⇨ Consumo bajo.
- ⇨ Posibilidad de ejecutar múltiples máquinas virtuales.
- ⇨ Utiliza bytecode.

A diferencia de IOS, Android es gratuito, cualquier empresa puede instalarlo en sus dispositivos, esto característica ha conseguido que Android sea implementado en múltiples dispositivos, desde la gama baja hasta la gama alta.

Otra característica de Android debido al carácter libre del sistema, es el gran ecosistema de ROM de la comunidad, que son modificaciones del sistema operativo desarrolladas por una comunidad. Existen múltiples ROM, algunos para un único dispositivo y otras soportan múltiples dispositivos.

Entre la ROM más famosas, que soportan muchos dispositivos, tenemos Cyanogenmod y MIUI.

Existen un conjunto de sistemas operativos que tienen una cuota de implantación menor que los expuestos anteriormente.

NOMBRE	DESCRIPCIÓN
Windows Phone	Sistema desarrollado por Microsoft utilizado principalmente por Nokia y algunos modelos de otras empresas como Samsung o HTC.
BlackBerry OS	Sistema desarrollado por la empresa RIM para sus propios dispositivos denominados BlackBerry, proporciona un servicio propio de correo que es muy utilizado en ambientes profesionales o empresariales.
Tizen	Sistema desarrollado principalmente por Samsung y utilizado en varios de sus modelos. Está basado en el código de otro sistema denominado Meego, se puede considerar su sucesor.
Firefox OS	Sistema desarrollado por Mozilla basado en HTML5 con un núcleo de Linux, en la actualidad soporta pocos modelos.
Sailfish OS	Es un sistema operativo para dispositivos móviles desarrollado por la empresa finlandesa Jolla Ltd, en base al código fuente del proyecto Mer, la versión 5 de la biblioteca de desarrollo Qt y el protocolo de comunicación para servidores de visualización Wayland. Existe un modelo (Jolla) con el sistema operativo preinstalado y puede ser instalado en otros dispositivos.
Ubuntu touch	Sistema operativo basado en Linux desarrollado por la compañía Canonical, utiliza un interfaz denominada Unity que puede utilizarse en ordenadores, tablet o teléfonos.

A partir de la versión Android 4.4 la máquina virtual Dalvik es sustituida por ART que permite eliminar la máquina virtual del sistema, mejorando el desempeño del sistema.

Todo dispositivo hardware requiere algún tipo de software para funcionar, este software está compuesto por una serie de líneas de código desarrolladas en un lenguaje de programación.

Podemos tener dos categorías de lenguajes en función de los ámbitos donde son utilizados:

- ⇨ Propósito general: son lenguajes de programación que pueden ser utilizados en diversos ámbitos, ejemplo de este tipo de lenguaje son java o python.
- ⇨ Específicos: diseñado y utilizado para un ámbito específico como; web, inteligencia artificial, redes o base de datos. Ejemplo de lenguaje de este tipo pueden ser PHP, ASP, Scheme, Perl, SQL o Erlang o Scala.

Para utilizar un lenguaje en determinado ámbito puede hacer uso de librería como el uso de framework, como ocurre con Python con Django o Ruby onRails.

Respecto a los lenguajes utilizados en el ámbito de la redes de comunicaciones, existen diversos lenguajes utilizados, algunos como Erlang han sido creado por un empresa como Ericsson que se dedica a las telecomunicaciones, otros más genéricos como C, C++ o Java que utilizado en diversos terminales de comunicación, Perl es otro lenguaje muy utilizado en redes y proporciona muchas librerías. También hay lenguajes muy utilizados en software de comunicación como python.

Framework: “un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular que sirve como referencia, para enfrentar y resolver nuevos problemas de índole similar.”

A continuación se muestra una tabla con algunos lenguajes utilizados en redes.

USO	LENGUAJE	FUNCIÓN
Open-WRT, DD-WRT	C/C++	Al utilizar un kernel de Linux, está desarrollado principalmente por estos lenguajes.
Android	Java	Desarrollo del sistema operativo y aplicaciones.
IOS	Objective-C	Desarrollo del sistema operativo y aplicaciones.
Administración de Cisco	Perl	Este lenguaje proporciona la librería Net::Telnet::Cisco que permite interactuar con los router Cisco.
WhatsApp	Earlang	Servicios de mensajería instantánea muy utilizada generando mucho tráfico de red. Este servicio está desarrollado por este lenguaje.
Twitter	Scala	Otro servicio de envío de mensajes, muy utilizado en internet que genera mucho tráfico de red, este lenguaje permite gestionar múltiples peticiones concurrente de forma óptima.
Microsoft	Visual Basic Scripts (VBS)	En entornos Windows, VBS permite desarrollar scripts utilizados para diversas tareas, esto es muy utilizado en redes Windows.
Google, Amazon	Python	Este es un lenguaje muy utilizado en el ámbito de las redes, google en varios servicios utiliza python, como Google App Engine. Amazon también utiliza python, como su AWS o EC2.

Las empresa que desarrollan hardware de comunicaciones, anteriormente se han visto algunos, suelen dispone de un pequeño lenguaje de scripts utilizado para tareas de administración. Por ejemplo tenemos:

- ⇨ TCL/Expect (Cisco): Lenguaje de scripts incluido en su sistema IOS.
- ⇨ WBT (Juniper): Lenguaje de scritps para JunOS.

El ámbito de estos lenguajes se subscribe a sus dispositivos hardware.

Un lenguaje de programación puede ser categorizado por múltiples factores, como:

- ⇨ Implementación: dependiendo de cómo se ejecuten tenemos dos categorias:
  - Compilados: realiza un proceso donde el lenguaje de programación es traducido a otra lenguaje entendible por la máquina (lenguaje máquina). Este proceso es realizado por un compilador.
  - Interpretados: el proceso para generar el lenguaje máquina se realiza conforme vaya siendo necesario en la ejecución. Este proceso es realizado por un interprete.
- ⇨ Paradigma de programación: forma en que resuelve un lenguaje un problema, existen múltiples paradigmas como:
  - Imperativo.
  - Declarativo.
  - Orientado a objetivos.
  - Funcional.
  - Orientada a aspectos.
  - Dirigidas a eventos.
- ⇨ Sistema de tipos: Todos los lenguajes permiten declarar variable donde almacenar información, esto pueden ser de dos tipos en función de cuando se realiza la comprobación de tipo: estático, donde la comprobación se realiza en la compilación y dinámico donde la comprobación se realiza en la ejecución. También existen lenguajes que utilizan una combinación de ambas.
- ⇨ Tipos de datos: Cuando hay una variable tiene asignado un tipo de datos, si el lenguaje no permite cambiar el tipo de dato, es denominado tipo fuerte, si el lenguaje permite cambiar a otro tipo de dato, es denominado tipo débil.

C/C++

Lenguajes muy robustos utilizados en diversos ambientes, C es un lenguaje imperativo y estructurado, que utiliza un tipo dato débil y estático. En cambio C++, es un lenguaje orientado a objetos e imperativo, con un

tipo de dato fuerte y estático. Ambos lenguajes son compilados y el lenguaje C++ es considerado como una extensión de C.
El kernel de Linux esta desarrollado en gran parte en C y este kernel es utilizado en múltiples dispositivos hardware de red, C++ son utilizado en mucho software de red, debido a que es muy rápido en la ejecución es muy utilizado en el desarrollo de sistemas complejos.

Java

Es el lenguaje más utilizado, entre sus características tenemos:

- ⇨ Paradigmas: orientado a objeto e imperativo.
- ⇨ Tipo de datos: fuerte y estático.

Utiliza una máquina virtual que es donde se ejecutan las aplicaciones, esto permite que sea multiplataforma. La máquina virtual es utiliza por otro lenguajes como Groovy o Scala, siendo compatible con esos lenguajes.
Este lenguaje proporciona múltiples librerías que lo hacen ser apto para cualquier uso y existen varios framework que facilitan el desarrollo de aplicaciones en ciertos ámbitos.

Perl

Es un lenguaje interpretado muy utilizado en ámbito de la administración de redes, permite generar pequeños programas denominado script que permiten realizar pequeñas tareas de forma muy eficiente. Es un lenguaje muy robusto que toma ciertas características de C.
Sus características son:

- ⇨ Paradigmas: funcional, imperativa y orientado a objetos.
- ⇨ Tipos de datos: dinámico.

Perl toma características de la programación en Shell, creación de scripts, y posee algunas estructuras muy útiles como las expresiones regulares. Es un lenguaje que es utilizado en rango de pequeño de ámbitos, es especialmente útil en aquellos problemas donde el tratamiento de grandes cantidades de datos. Es utilizado en varios servicios de Internet donde se generar una gran cantidad de tráfico de datos.

Python

Lenguaje interpretado y multiplataforma utilizado en múltiples ámbitos, que genera un código muy limpio y organizado.
Sus características:

- ⇨ Paradigmas: imperativo, orientado a objetos y funcional.
- ⇨ Tipo de datos: débil y dinámico.

Lenguaje utilizando en múltiples servicios de Internet y en software de redes, mediante el uso de librerías y el framework es utilizado en prácticamente todos los ámbitos de la informática. Es un lenguaje que puede comunicarse con otros lenguajes de una forma cómoda.
Muchas empresas de Internet utilizan este lenguaje de forma intensiva, como ejemplo tenemos: Google, Amazon. Ebay o Yahoo.

Objective-C

Lenguaje desarrollado por Apple para ser utilizado en sus productos, como el Iphone. Este lenguaje está basado en parte en C, se considera un superconjunto de C, y como este es un lenguaje compilado.
Sus características:

- ⇨ Paradigmas: orientado a objetos.
- ⇨ Tipos de datos: fuerte y estático.

Este lenguaje solo está disponible en los sistemas de Apple, solo puede ser instalado en Mac X OS, permitiendo desarrollar aplicaciones para los sistemas de Apple, IOS y Mac X OS.

Erlang

Desarrollado por empresa de telecomunicaciones Ericsson y está diseñado específicamente para las telecomunicaciones.
Sus características:

- ⇨ Paradigma: funcional y concurrente.
- ⇨ Tipo de datos: dinámico y fuerte.

Este lenguaje tiene otra serie de características que lo hacen ideal para el ámbito de las redes: desarrollo de aplicaciones distribuidas, escalable, aplicaciones en tiempo real, diseñado para ser concurrente y tolerante a fallos.
Es un lenguaje que aunque ha sido desarrollado por una empresa y es utilizado en sus productos, posee una licencia libre que permite ser utilizado por otras empresas y producto sin ningún perjuicio. Aunque es utilizado por operadora de telecomunicaciones de forma interna, existen diversos aplicaciones como servidor de mensajería, herramienta de análisis de rendimiento, servidor de aplicaciones web, etc.
En la actualidad es conocido por ser el lenguaje de desarrollo de la aplicación de mensajería WhatsApp.

Scala

Lenguaje que utiliza la máquina virtual de Java que tiene un soporte total a la programación funcional, su proviene de juntar las palabras lenguaje y escalable.
Sus características:

- ⇨ Paradigma: funcional, orientado a objetos e imperativo.
- ⇨ Tipo de datos: fuerte y estático.

Scala al utilizar la máquina virtual de Java permite tener una integración con Java. Podemos desarrollar un proyecto con Java y algunos componentes con Scala, o al contrario.
Como se ha indicado anteriormente, Scala es un lenguaje diseñado para ser escalable que significa que este lenguaje permite adaptarse sin perder calidad de servicio a un crecimiento de la carga de trabajo. Aunque es un lenguaje relativamente modernos (2003) es utilizado en aplicaciones web varias con alta carga de trabajo como Twitter o Foursquare, con lo que demuestra que este lenguaje es utilizado en aplicaciones donde la escalabilidad es un factor clave.

Visual Basic Scripts (VBS)

Es un lenguaje interpretado desarrollado por Microsoft utilizado en sus sistemas Windows, es una variación de lenguaje Visual Basic y permite generar scripts.
Sus características:

- ⇨ Paradigma: interpretado (scripting).
- ⇨ Tipo de datos: débil y dinámico.

Este lenguaje es utilizado como herramienta de automatización de tareas mediante el desarrollo de scripts.

Se han visto algunos lenguajes utilizados en el ámbito de las redes de comunicación, algunos de ellos son utilizados en software instalado en los dispositivos de redes, como C/C++ o Erlang, otros son utilizados en software de redes, como Python o Scala y otros son utilizado en terminales móviles, como Java o Objective-C.
Para que un lenguaje puede ser utilizado en el ámbito de las redes y ser utilizado en terminales de comunicaciones, debe tener un serie de características que en ámbito de la redes es muy aconsejable que cumplan, ya sea por medio de librerías o como por diseño propio del lenguaje. Estas características son:

- ⇨ Concurrencia
- ⇨ Escalabilidad
- ⇨ Tiempo real

Concurrencia

Es la propiedad de gestionar o ejecutar múltiples tareas de forma simultánea. Por ejemplo, permite que un dispositivo ejecute varias conexiones o un software gestionar múltiples mensajes simultáneos.
El cumplimiento de esta propiedad mejorará el rendimiento de un dispositivo o software al poder realizar múltiples tareas simultáneas. Como desventaja tenemos, que la concurrencia es difícil de programar y requiere una especial atención para que no se produzcan bloqueos en la aplicación. La concurrencia está relacionada con la programación paralela, donde es muy importante la comunicación de la diversas tareas y el acceso coordinado a los recursos disponibles que comparten todas las tareas.
Un ejemplo donde es muy importante la concurrencia es la aplicación WhatsApp que recibe millones de mensajes de forma simultánea y debe gestionar de forma óptima para que no provoque caídas en el servicio.

Escalabilidad

Es la propiedad que indica la habilidad de una aplicación a adaptarse a un aumento, sostenido o inesperado, de la carga de trabajo sin perder rendimiento. Esta propiedad es muy importante a tener en cuenta en aquellos escenarios donde no se puede controlar la carga de trabajo de un servicio.
Si un servicio no es escalable, cualquier aumento significativo puede provocar una caída en el servicio. Si el servicio es escalable, cualquier aumento puede ser solucionado asignándole más recursos. Una buena escalabilidad de un aplicación influye en poder asignarle más recursos en tiempo de ejecución sin que afecte a su redimiendo. En el caso de una red, esta es mas escalable cuando su capacidad puede ser aumentada sin afectar al rendimiento y sin provocar cortes en el funcionamiento.
Existen dos tipos de escalabilidad en función de cómo se aumenta la capacidad y como afecta en su conjunto:

- Escalabilidad vertical: Un sistema escala verticalmente o hacia arriba, cuando al añadir más recursos a un nodo particular del sistema, este mejora en conjunto.
- Escalabilidad horizontal: Un sistema escala horizontalmente si al agregar más nodos al mismo, el rendimiento de este mejora.

Tiempo real

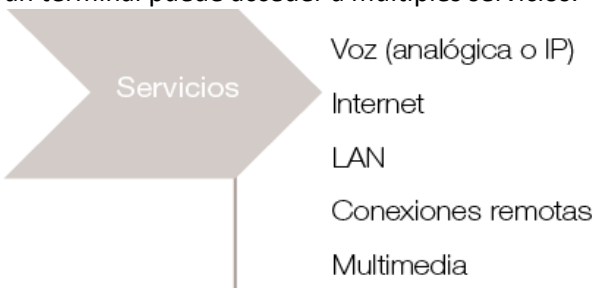
En cualquier comunicación, un retardo que se produzca provocara una caída de rendimiento. El tiempo que se produce entre la emisión y la recepción debe ser el menor posible, este tiempo se denomina tiempo de interacción. Otro aspecto es que cualquier reacción que se produzca ante un determinado eventos debe producirse en tiempo de ejecución.
Un lenguaje que permite desarrollar aplicaciones en tiempo real, es idónea para un escenario de comunicación. Una aplicación en tiempo real debe responder dentro de un plazo determinado, los menor posible, para que la comunicación no se resienta.
Un sistema en tiempo real debe cumplir varias características:

- Determinismo: Es la capacidad de determinar con una alta probabilidad, cuanto es el tiempo que se toma una tarea en iniciarse. Esto es importante porque los sistemas de tiempo real necesitan que ciertas tareas se ejecuten antes de que otras puedan iniciar.
- Responsividad: Es el tiempo que tarda una tarea en ejecutarse una vez que la interrupción ha sido atendida.
- Confiabilidad: El sistema no debe solamente estar libre de fallas pero más aún, la calidad del servicio que presta no debe degradarse más allá de un límite determinado.

Escenarios donde una ejecución en tiempo real es un factor clave son las videoconferencia o llamadas telefónicas, donde cualquier retardo produce una pérdida de calidad en la comunicación.

2.1.3. Servicios específicos para terminales

Cualquier terminal puede acceder a un conjunto de servicios, en función del tipo de terminal. Estos servicios necesitan una determinada aplicación para acceder, unos requisitos hardware y una configuración para un acceso que permite usar el servicio con una buena calidad.
Dependiendo del servicio se utiliza un determinado terminal, aunque con la implantación de las comunicaciones digitales un terminal puede acceder a múltiples servicios.



Voz

Voz: el terminal utilizado para este servicio es el teléfono, ya sea analógico o digital, o un ordenador en el caso de la telefonía digital, utilizando un softphone. Este servicio puede utilizar múltiples tipo de redes:

- ⇨ Par de cobre: es la red tradicional donde se he proporcionado este servicio. La comunicación puede realizarse de forma analógica mediante un terminal tradicional de teléfono o mediante tecnologías tipo XDSL que utiliza una señal digital mediante comunicación analógica.
- ⇨ Cable coaxial: el ancho de banda y las velocidades son mayores, utiliza señales eléctricas para la transmisión, igual que en el par de cobre. Este servicio se puede acceder directamente con un teléfono analógico o mediante internet utilizando telefonía IP.
- ⇨ Fibra óptica: la señal es digital, la transmisión digital se realiza mediante pulsos de luz, en vez de utilizar pulsos eléctricos, la comunicación digital proporciona muchas ventajas respecto al comunicación analógica, como mayor ancho de banda o velocidad.

Los servicios de voz pueden tener unas funcionalidades extras que complementan las funciones de voz, en la telefonía digital estas funcionalidades pueden ser aumentadas con otros servicios.
Entre las funcionalidades tenemos:

- ⇨ Contestador: consiste en un mensaje de voz que se iniciara si la llamada no es contestada, configurando su activación después de un número de tonos de llamada.
- ⇨ Llamada en espera: mantener una llamada mientras estas atendiendo otra llamada.
- ⇨ Extensiones: compartir un mismo número de teléfono, entre varios terminales, cada terminal se le añade un número que lo identifique (extensión). Necesita una centralita para gestionar las extensiones.
- ⇨ Llamadas entre varios: permite realizar una comunicación entre más de dos personas.

Hay un serie de servicios que solo pueden realizarse con terminales IP y utilizando tecnologías tipo VoIP.
Entre los que tenemos:

- ⇨ Videoconferencias: permite unir voz con imagen.
- ⇨ Utilizar un ordenador como un terminal de comunicaciones mediante el uso de softphone.
- ⇨ SMS.

Para utilizar un servicio de voz es necesario tener asignado un número de teléfono que permitirá identificar a cliente, también se denomina abonado. Permitiendo que el cliente reciba llamadas a ese número como otro tipo de servicios telefónico, también permite que el cliente pueda realizar llamadas a otro cliente.
El número debe ser proporcionado por un operador de telefonía, pagando una determinada tarifa por el servicio. Todos los operadores de telefonía deben utilizar una red de comunicación para la transmisión y todos los clientes están comunicados entre sí independientemente del operador que utilicen.
Respecto a tecnologías de telefonía IP, el servicio utiliza tecnologías de Internet para proporcionar un servicio de voz. Un operador debe asignar un número de teléfono si el cliente quiere comunicaciones con la telefonía tradicional, para comunicaciones con telefonía IP no es necesario utilizar un número, depende del operador.
Existen protocolos para telefonía IP como SIP que permite las comunicaciones entre terminales IP, este protocolo permite servicios de voz a través de Internet.
Para utilizar terminales IP en algunos casos, dependiendo de las funcionalidades, es necesario el uso de una centralita telefónica, PBX, que es un dispositivo hardware que está conectado a una red telefonía que proporciona el servicio de telefonía a conjunto de equipo, anteriormente se ha descrito el concepto de centralita.
En España existe una serie de regulaciones, como el rango numérico para la asignación de números de teléfono, que son gestionadas por la CMT, Comisión del Mercado de las Telecomunicaciones, que es un organismo que regula el sector de telecomunicaciones.

Internet:

Internet: este servicio está teniendo un auge y suele estar asociado con otros servicios, como telefonía.
Podemos definir Internet con un conjunto de dispositivos que están comunicados a través de múltiples redes y repartidas por todo el mundo. Internet se le denomina como “la red de redes” por su concepto de estar en todo el mundo.

Para que esa variedad de redes, con sus dispositivos hardware/software y tecnologías, puedan comunicarse, utilizan una serie de tecnologías que permite abstraerse de los características de las redes y centrarse en cómo realizar la comunicación. Estas tecnologías son múltiples como:

- ⇨ TCP/IP.
- ⇨ HTTPS.
- ⇨ HTTP.
- ⇨ DNS.
- ⇨ Etc.

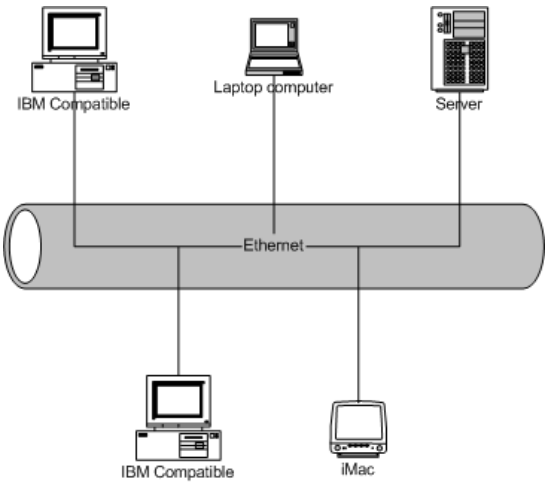
Esto permite tener un conjunto amplio de servicio. De hecho, están migrando servicios que habitualmente se dan con otras tecnologías al ámbito de Internet, como ejemplo telefonía o televisión.
Para el acceso a Internet como requisito se necesita un dispositivo que permite la conexión entre el hardware que disponemos; ordenador, portátil, tablet, televisión…etc, a la red de comunicación que proporcionara el acceso a Internet. Este dispositivo se denomina router y dependerá de la tecnología utilizada para acceder a Internet, existen diferencias entre un router ADSL y un router para fibra óptica.
Internet proporciona un conjunto de servicios que utilizan un serie de tecnologías y protocolos:

SERVICIO	PROTOCOLOS	DESCRIPCIÓN
Email	IMAP, SMPT, POP3	Correo electrónico, enviar y recibir mensajes de correos, con las posibilidad de añadir documentos adjuntos, es necesario la utilización de un servidor de correo.
Web	HTTP, HTTPS, SSL	Navegación por internet a través de páginas web que presentan la información con un formato específico, es necesario el uso de un servidor Web.
Mensajería	HTTP, XMPP, Hangouts	Envío y recepción de mensajes cortos a través de internet, disponible a través de servicios como Whatsapp, Telegram, Facebook Messenger o Google+.
Monitorización	SNMP, CMIP, RMON	Permite gestionar y vigilar un dispositivo tanto hardware como software y realizar diversas acciones sobre él.

Existen muchos más servicios, como FTP, VPN o cloudcomputing, que utilizan diversos protocolos. En la actualidad todos los servicios disponibles están convergiendo a Internet y en un futuro todos los servicios serán accedidos a través de Internet

LAN

LAN: una red de área local o LAN es un conjunto de dispositivos conectado en un área geográfica muy limitada, todas las empresas tienen una LAN en sus instalaciones, también los usuarios particulares.
Este tipo de red se considera una red privada, donde los dispositivos suelen estar conectados a través un dispositivo switch para la comunicación entre los dispositivos. En redes pequeñas se utiliza un router para la comunicación.
La estructura de la red o topología de red indica como están conectados los diversos dispositivos disponibles de la red, existen diversos tipos de organizaciones que pueden ser utilizadas. El estándar utilizado que especifica diversos aspectos técnicos de la red es Ethernet, existen otras alternativas pero en la actualidad casi no se utilizan.



Para acceder a una red pública, como Internet, es necesario que la red disponga de un dispositivo de acceso, un router o cable módem son los encargados de proporcionar el acceso.
Existen múltiples servicios que pueden que pueden ser utilizado en una LAN, en función del ámbito tenemos.

- ⇨ Locales: son servicios que son utilizados dentro de LAN, como DHCP.
- ⇨ Exteriores: son servicios que requieren de acceso a Internet para su utilización, como una VPN.
- ⇨ Mixtos: son servicio que pueden utilizarse de forma interna o a través de Internet, como un DNS.

Entre los servicios que pueden utilizarse en una LAN tenemos:

- ⇨ VPN (red privada virtual): permite una conexión segura desde una LAN a través de una red pública como Internet. Este tipo de tecnología permite enviar datos desde el terminal de una LAN a otro terminal de una LAN utilizando Internet para la comunicación, estableciendo una conexión segura y privada, comportándose como si los dos terminales estuvieran en la misma red LAN.
- ⇨ Radius: es un protocolo de red que proporciona una autenticación centralizada, permitiendo la autorización y gestión de las conexiones de los usuarios a los servicios de red.
- ⇨ LDAP: "protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también se considera una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas".
- ⇨ DHCP: protocolo que asigna direcciones IP a los dispositivos disponibles en la red.
- ⇨ DNS: sistema jerárquico que asocia nombres a los dispositivos de la red con una dirección IP, estos nombres son utilizados tanto dentro de red local como para Internet.

Existen muchos más servicios que pueden ser utilizados en una LAN por los dispositivos de la red.

Conexiones remotas

Conexiones remotas: en algunas ocasiones es necesario acceder a terminal desde otro dispositivo porque no tenemos acceso físico a él. Este tipo de conexión que es realizada sin tener acceso físico al sistema se denomina conexiones remotas y permiten gestionar un dispositivo.
Existen diversos protocolos o servicios que proporciona conexiones remotas, estas conexiones pueden realizar dentro de la misma LAN o fuera de ella, utilizando Internet para acceder. Las conexiones remotas pueden ser de dos tipos:

- ⇨ Conexiones por terminal: se accede al equipo mediante un terminal donde ejecutar diversos comandos que serán aplicados en el equipo remoto.
- ⇨ Conexiones gráficas: permite acceder al escritorio de un equipo de forma remota, permitiendo trabajar como si estuviéramos delante del equipo.

SERVICIO	DESCRIPCIÓN
SSH	Utilizado para acceder a un terminal, sin sistema gráfico, donde ejecutar comandos, muy utilizado en sistemas Linux.
Terminal server	Utilizando un software especifico en un máquina permite la ejecución de aplicaciones de forma remota, muy utilizado en Windows.
Teamviewer	Aplicación que permite conexiones remotas gráficas, está compuesto por una aplicación cliente que es ejecutada en el equipo remoto y desde otro equipo podemos acceder al equipo remoto.
VNC	Utiliza una estructura cliente-servidor para acceder a un equipo remoto independiente del sistema operativo que se utiliza.

Las conexiones remotas son muy utilizadas para la gestión de incidencias en un equipo, como requisitos tenemos que el equipo debe tener acceso a la red local o a Internet si la conexión se realiza desde otra LAN, también deben conocerse las credenciales de un usuario con acceso a la equipo remoto.
Otro aspecto para algunos servicios es el tema de la seguridad, algunos servicios remotos tiene los datos encriptados, como SSH o teamviewer, para que solo el emisor y el receptor puedan ver el contenido de los datos transmitidos y permitiendo una comunicación privada.

La mayoría de las aplicaciones utilizan una estructura de cliente-servidor, donde una aplicación cliente es instalado en el equipo donde se realiza el acceso y otra aplicación servidor es instalado en el equipo remoto. La aplicación cliente envía una serie de acciones realizadas en equipo de acceso y son recibidas en la aplicación servidor que las aplica en el equipo remoto.

Multimedia

Multimedia: otro de los servicios que pueden acceder los terminales es la visualización de contenido multimedia, donde podemos considerar:

- ⇨ Televisión: mediante un conjunto de canales de televisión que ofrecen diversos contenidos como:
  - Noticias.
  - Deportes.
  - Películas.
  - Temática especifica: existen canales que solo ofrecen un tipo de contenido como: animales, de cocina, historia, etc.
- ⇨ Películas y series: se puede ver este tipo de contenido mediante una programación que indica a la hora de emisión o mediante streaming que al cliente escoger la hora cuando desea ver el contenido.
- ⇨ Música: permite escuchar en un terminal mediante streaming las canciones que desea el cliente.

Igual que en los servicios anteriores, estos pueden ser ofrecidos a través de Internet mediante una red de comunicación. Aunque también es muy utilizado otro tipo de acceso como la red de satélite, que mediante una antena parabólica el cliente puede acceder al contenido de televisión.

El servicio por satélite es de pago, también se denomina pago por visión, para visualizar el contenido es necesario la instalación de una antena parabólica que tenga una determinada orientación y un dispositivo hardware que permite decodificar la señal de televisión y otros servicios en la televisión, este dispositivo se denomina decodificador y permite tanto gestionar las cadenas disponibles como ver las películas disponibles.

Otro servicios que está en auge es el video bajo demanda, que permite a un usuario el acceso a contenido multimedia de forma personalizada, este acceso puede ser realizar de dos formas.

- ⇨ En tiempo real, el usuario visualiza el contenido que está siendo transmitido en una cadena en ese momento.
- ⇨ Descarga: el usuario descarga el contenido a su propio dispositivo, ordenados, DVD, tablet, etc., para que pueda visualizarlo cuando quiera el usuario.

Estos servicios utilizan Internet para la transmisión, existen varios proveedores de este servicio y el usuario deberá pagar una cuota mensual por el servicio o un pago por contenido visualizado.

Dentro de los servicios multimedia está en auge la técnica de streaming para transmisión de contenido a cualquier terminal, ordenadores, portátil, televisión, telefonía móvil o tablet, estos dos últimos está creciendo mucho este servicio, generalmente el contenido que se consume es audio o video.

El streaming es una técnica de distribución de contenido mediante una red de computadoras, ya sea una red local como Internet. Esta técnica hace uso de buffer de datos donde va almacenando el contenido que se va descargando en el terminal del usuario, mientras este visualiza el contenido, evitando que se produzcan cortes en la visualización.

El streaming, depende del contenido que trasmite, puede utilizar bastantes recursos y es necesario un buen ancho de banda como velocidad para que el usuario visualice el contenido sin que se produzca cortes y tenga que esperar a que descargar más datos en el buffer.

Para un correcto funcionamiento la técnica del streaming utiliza diversas tecnologías.

- ⇨ Códec: son aplicaciones que se encargar de decodificar el contenido multimedia de un determinado archivo, existen diversos códec como MP3 o Vorbis para el audio.
- ⇨ Bitstream: cuando transmite un contenido de audio o vídeo, deben ser empaquetados en una secuencia de byte dentro de un contenedor. Existen diversos contenedores como FLV o AVI.
- ⇨ Transporte: el streaming utiliza una arquitectura cliente-servidor, para la comunicación entre el cliente y el servidor se utiliza un protocolo de transporte específico para esta tarea, como ejemplo tenemos MMS o RTP.
- ⇨ Control: El cliente puede interactuar con el servidor utilizando un protocolo específico como MMS o RTPS.

El streaming se utiliza para diversos programas que permiten enviar contenido multimedia a una aplicación cliente, como ejemplo de estas aplicaciones tenemos Real Player que dispone de diversas soluciones o VLC como aplicación más sencilla para transmitir contenido multimedia.
También existen empresas que ofrecen servicios de streaming de contenido multimedia, como video o audio, entre las cuales están:

NOMBRE	SERVICIO
Filmin	Plataforma que proporciona streaming de cine y series.
Youtube	Plataforma de streaming de vídeo.
Netflix	Proporciona un servicio streaming de películas y series mediante el pago de un cuota mensual.
Amazon	Plataforma de streaming de vídeo, series y audio, dispone de un hardware KindleFire, que es una tablet que permite acceder al contenido de manera mas fácil.
Spotify	Servicio de streaming de música mediante el uso de una aplicación disponible en diversos sistemas.

2.1.4. Aplicaciones de cliente, gestión y configuración

Para utilizar los servicios proporcionados por diversas empresas es necesaria una serie de aplicaciones clientes que permiten usar esos servicios. Estas aplicaciones pueden ser:

- ⇨ Genéricas: el servicio no obliga al uso de una determinada aplicación, existiendo varias alternativas.
- ⇨ Específicas: el servicio obliga a utilizar una determinada aplicación para el uso del servicio.

La instalación de una aplicación cliente debe tener diversos factores como:

- ⇨ Dispositivo hardware donde se va instalar: Portátil, ordenador, tablet o movil.
- ⇨ Sistema operativo: Windows, Linux, IOS, Android, etc.
- ⇨ Versión del sistema operativo.
- ⇨ Arquitectura del hardware. ARM, x86, x64.

La aplicación a instalar en un teléfono móvil con Android no es la misma aplicación que para un portátil con Windows. La aplicación debe tener soporte para el sistema operativo, versión, dispositivo y arquitectura, en muchas ocasiones el soporte de la aplicación se circunscribe a determinados sistemas operativos.
Toda aplicación instalada en el equipo del cliente, necesita una configuración adecuada para utilizar de forma óptima un servicio, normalmente con la configuración por defecto que incluye la aplicación, aunque algunas veces requiere una configuración personalizada. Una determinada aplicación también puede requerir una cierta configuración en el sistema operativo o en otras aplicaciones del sistema, como en el cortafuegos.
La configuración de una aplicación no debe ser fija, deberá adaptarse en función de entorno donde se ejecuta y si los requisitos cambian, es posible que necesite ser modificada.
Una aplicación después de la instalación requiere una gestión, debe realizarse una serie de tareas entre las cuales tenemos:

- ⇨ Debe estar actualizada, en caso necesario aplicar los parches de seguridad que recomienda la empresa desarrolladora de la aplicación.
- ⇨ Monitorizar su uso para comprobar que los usuarios están utilizando de forma correcta y evitar errores.
- ⇨ Aquellas aplicaciones que incluyan gestión de usuario, comprobar que los usuarios tienen los permisos adecuados conforme a su perfil.
- ⇨ Controlar la seguridad de la aplicación, si requiere el uso de contraseña. Los usuarios deben tener contraseñas que sean seguras.

Los servicios que son proporcionados a un cliente necesitan de una aplicación que facilita su uso. Una pequeña lista de servicios y aplicaciones se muestra a continuación.

SERVICIO	DESCRIPCIÓN	APLICACIONES
Web	Navegación por páginas web.	Firefox, Opera, Chrome, Safari, Edge.
Correo electrónico	Envío y recepción de mensajes de correo electrónico.	Outlook, Thunderbird, Evolution.
Almacenamiento en la nube	Servicio que permite almacenar archivos en la nube, de forma deslocalizada, permitiendo la sincronización con nuestro dispositivo.	Dropbox, Box, Onedrive, Copy, Google Drive, SpiderOak, SparkleShare.
Acceso a Internet	Los sistemas operativo proporciona una herramienta de configuración de redes (gestor de redes) para el acceso a Internet.	El gestor de redes que proporciona el sistema operativo.
Mensajería	Servicio para el envió de de mensajes cortos.	Telegram, WhatsApp, Line.
Redes Sociales	Servicio utilizado para la comunicación con otras personas a través de Internet.	Facebook, Tuenti, Google +, Linkedin.
Conexión remota	Permite acceder a un dispositivo de forma remota.	SSH, Teamviewer, VNC, Escritorio remoto, Terminal server.

Para poder utilizar un servicio, como los mostrados en la tabla anterior, debemos utilizar una aplicación especifica o aplicación cliente. Algunos servicios proporcionan una página web desde donde poder usar el servicio, sin necesidad de instalar un cliente, aunque lo habitual es que la empresa desarrolladora ofrezca uno. La instalación de una aplicación dependerá del sistema operativo, aunque existen diversos métodos de instalación.

- ⇨ Paquete de instalación: El proveedor del servicio proporciona la aplicación en un formato específico para ser instalada. En Windows son paquetes msi, en Linux hay varios formatos como rpm o deb.
- ⇨ Instalador: es una herramienta que se integra con la aplicación y facilita la instalación en el sistema, por medio de un asistente que guía paso a paso el proceso de instalación.
- ⇨ Tienda virtual: este método es muy utilizado en aplicaciones móviles y consiste en un servicio, parecido a una tienda, donde aparecen las aplicaciones disponibles de forma organizada. El usuario simplemente deberá seleccionar la aplicación, pagar si es necesario, y esta será instalada en su dispositivo.
- ⇨ Web: Algunos servicio pueden ser usados mediante un navegador Web o instalando algún plugin en el navegador. No es necesaria la instalación en el sistema, solo un navegador Web.

Toda aplicación debe ser gestionada para conocer si el rendimiento es óptimo, esta gestión puede realizarse con las herramientas de gestión mostradas en el módulo uf1875 o realizar una gestión mas sencilla a través de una serie de tareas como:

1. Comprobar si hay actualizaciones de forma periódica.
2. Los usuarios deben tener los permisos necesarios para utilizar la aplicación.
3. Proporcionar información a los usuarios de la aplicación.
4. Realizar copias de seguridad de las aplicaciones.
5. Comprobar el correcto funcionamiento de la aplicación.
6. Registrar todas las incidencias producidas en la aplicación y resolverlas lo antes posible.

Respecto a la configuración de una aplicación:

1. La configuración debe estar adaptada al entorno donde se encuentra y al uso.
2. Configurar de forma adecuada los componentes (hardware o software) que puedan influir en el funcionamiento de la aplicación, como sistema operativo, cortafuego, antivirus o router.
3. La configuración debe ser probada.
4. La configuración debe conseguir que la aplicación tenga el mejor rendimiento y que no perjudique al resto de componentes del sistema.

Una aplicación proporciona uno o varios archivos de configuración donde ver sus opciones, también esta configuración puede ser modificada de forma gráfica, las aplicaciones suelen incluir un apartado de configuración.

Por último, existen herramientas que son gestores de configuraciones que permiten controlar la configuración de un conjunto de aplicaciones y aplicar modificaciones en caso necesario, ejemplo de este tipo de herramientas son Puppet o Chef. También existen herramientas que proporciona un panel de

control mediante una interfaz web donde realizar configuraciones de una serie de servicios y aplicaciones, como otras gestiones. Un ejemplo de este tipo de herramienta es Webmin.

2.2. Implantación y configuración de aplicaciones en terminales

En un dispositivo o en una red se necesita una serie de aplicaciones que deben ser configuradas de forma óptima. Cuando se realiza la implantación y configuración de aplicaciones en un conjunto de dispositivos de una forma organizada se denomina despliegue. Como requisitos para realizar:

- ⇨ Los dispositivos deben estar conectados a una red, puede ser a una red local o a través de Internet.
- ⇨ Los dispositivos deben estar accesibles, cualquier herramienta de seguridad, como un cortafuegos, debe estar configurado para permitir el acceso.
- ⇨ Los dispositivos donde realizar el despliegue de aplicaciones deben tener el mismo sistema operativo.

Los dispositivos pueden tener el sistema operativo instalado y solo se instalaran las aplicaciones, también pueden realizarse un despliegue de sistema operativo con un conjunto de aplicaciones instaladas. En este caso, los dispositivos no deben tener un sistema instalado.

Existen aplicaciones que facilitan el despliegue de aplicaciones de forma remota y en red, este tipo de aplicaciones utilizan una estructura de cliente-servidor.

- ⇨ Servidor: almacena las aplicaciones que van a ser instalados y las configuraciones asociadas, también deben estar añadidos en la aplicación de despliegue todos los dispositivos que controla y que puede instalar aplicaciones.
- ⇨ Cliente: software que recibe las aplicaciones y permite a la aplicación de despliegue

El despliegue para implantar aplicaciones sigue el siguiente proceso:

Preparación

Hay que preparar el sistema donde se va instalar las aplicaciones, suponemos que se utiliza una herramienta para las tareas a realizar:

- ⇨ Escoger qué aplicaciones son necesarias en función de los servicios a utilizar y los requisitos de los clientes.
- ⇨ Configurar la red para la implantación.
- ⇨ Instalar y configurar la herramienta de despliegue.
- ⇨ Configurar la seguridad de la red para permitir el despliegue.

Instalación

La red y la herramienta de despliegue están configuradas para instalar las aplicaciones, en este paso se utilizará la herramienta de despliegue para la instalación remota de aplicaciones a los clientes. Las tareas a realizar:

- ⇨ Configurar las aplicaciones a instalar en función de los requisitos.
- ⇨ Seleccionar los clientes donde se van a instalar.
- ⇨ Comprobar que la aplicación ha sido instalada de forma correcta y ejecutar la aplicación para comprobar su correcto funcionamiento.
- ⇨ Informar a los usuarios de los cambios en el sistema.

Gestión

Después de la instalación con éxito de la aplicación, debe realizar una serie de tareas de forma periódica para comprobar el correcto funcionamiento de la aplicación. Las tareas a realizar son:

- ⇨ Comprobar si existen actualizaciones de la aplicación y en caso afirmativo instalarlas.
- ⇨ Comprobar si hay errores en el funcionamiento.
- ⇨ Registrar las incidencias de los usuarios con la aplicación y ejecutar los procedimientos necesarios para resolver las incidencias.
- ⇨ Generar documentación, que puede ser:
  - Manuales de uso: explicando cómo usar la aplicación.
  - Guía de usuario: información útil para el usuario.

- Informes de incidencia: información sobre las incidencias producidas y su resolución.

Una herramienta de gestión, como las vistas en el módulo anterior (por ejemplo Nagios) proporciona ayuda para monitorizar las aplicaciones y descubrir los errores en el funcionamiento, aunque algunas tareas como gestión de actualizaciones o generar documentación no está dentro de sus funcionalidades.

2.3. Pruebas de aplicaciones y servicios instalados

Todas las aplicaciones deben ser probadas antes de ser ejecutadas en un entorno de producción, igual que los servicios disponibles para un cliente. La empresa proveedora del servicio debe realizar una serie de pruebas antes de que un servicio esté disponible.
Las pruebas están compuestas por un proceso de verificación que consiste en evaluar la aplicación o servicios si cumplen con las especificaciones que previamente han sido definidos.
Si el resultado de una prueba no es satisfactorio, puede ser por dos motivos:

- ⇨ Por un fallo que define la incapacidad del sistema o componente de realizar la función requerida con el rendimiento especificado.
- ⇨ Por un error que especifica que el resultado obtenido es diferente al resultado esperado.

Este último punto es importante tener en cuenta. En muchas ocasiones una aplicación no produce un error en su forma más clásica -corte de funcionamiento-, sino que el resultado al realizar una tarea en la aplicación no es el esperado.
Por ejemplo si la aplicación tiene una opción para imprimir un archivo y la utilizamos, el resultado debe ser un conjunto de hojas con el contenido del archivo, si el resultado es que las hojas salen en blanco, no cumple con esa funcionalidad.
Si una prueba tiene éxito es que ha encontrado un error o un fallo en la aplicación. En función de cómo se ejecutan tenemos:

- ⇨ Pruebas manuales.
- ⇨ Pruebas automáticas.

Prueba o test: una actividad en la cual un sistema o uno de sus componentes se ejecuta en circunstancias previamente especificadas, los resultados obtenidos son registrados para una posterior evaluación de algún aspecto.
Otro aspecto a destacar, es la elección de buenos casos de prueba.
Caso de prueba: es un conjunto de entradas, condiciones de ejecución y resultados esperados para un requisito que se quiere comprobar en particular.

Todas las pruebas deben tener una serie de casos de prueba que permiten comprobar si la prueba ha sido exitosa o no. Los casos de prueba dependen del tipo de prueba que se realiza, para escoger un buen caso de prueba debe tenerse en cuenta a que tipo de prueba está asociado.
Se pueden realizar muchos casos de prueba para determinar que un requisito es completamente satisfactorio. Con el propósito de comprobar que todos los requisitos de una aplicación son revisados, debe haber al menos un caso de prueba para cada requisito a menos que un requisito tenga requisitos secundarios. En ese caso, cada requisito secundario deberá tener por lo menos un caso de prueba.
Un caso de prueba está compuesto por:

- ⇨ Variable de entradas.
- ⇨ Variables salidas.

En algunas ocasiones los casos de prueba son documentados, siguiendo una estructura determinada divida en tres partes:

INTRODUCCIÓN	ACTIVIDADES	RESULTADOS
Identificador	Configuración	Salida esperada
Creador	Inicialización	Salida obtenida
Versión	Finalización	Resultado
Propósito	Acciones	Severidad
Dependencias	Descripción de los datos de entrada	Evidencia
		Seguimiento
		Estado

Dependiendo del enfoque o la técnica utilizada en las pruebas tenemos tres categorías: caja blanca, caja negra y aleatorio.

Caja blanca

Caja blanca: es un enfoque estructural y se centra en los detalles internos de la aplicación (estructura de la aplicación), analizando la ejecución de la aplicación y estudiando todos los procesos internos. Por esta razón, este enfoque está muy ligado al código fuente de la aplicación.

Las pruebas que utilizan este tipo de enfoque son utilizadas en el proceso de desarrollo de la aplicación. Las pruebas deben diseñarse en función del código de la aplicación, si el código cambia deben modificarse las pruebas.

Los casos de prueba deben probar la mayor cantidad de código, el objetivo de los casos de prueba es dar la mayor cobertura al código, si es alta significa que gran parte de la aplicación tiene su correspondiente caso de prueba.

Existen diversos tipos de cobertura, existen los siguientes tipos:

- ⇨ Cobertura de sentencias. Se trata de generar los casos de prueba necesarios para que cada sentencia o instrucción del programa se ejecute al menos una vez.
- ⇨ Cobertura de decisiones. Consiste en escribir casos suficientes para que cada decisión tenga, por lo menos una vez, un resultado verdadero y, al menos una vez, uno falso (incluye a la cobertura de sentencias).
- ⇨ Cobertura de condiciones. Se trata de diseñar tantos casos como sea necesario para que cada condición de cada decisión adopte el valor verdadero al menos una vez y el falso al menos una vez (no incluye cobertura de condiciones).
- ⇨ Criterio de decisión/condición. Consiste en exigir el criterio de cobertura de condiciones obligando a que se cumpla también el criterio de decisiones.
- ⇨ Criterio de condición múltiple. En el caso de que se considere que la evaluación de las condiciones de cada decisión no se realiza de forma simultánea, se puede considerar que cada decisión multicondicional se descompone en varias condiciones unicondicionales.
- ⇨ Criterio de cobertura de caminos. Se recorren todos los caminos (impracticable).

Entre las pruebas que utilizan este enfoque tenemos:

- ⇨ Pruebas unitarias: comprueban el correcto funcionamiento, de una parte concreta de la aplicación, como una función, cada prueba comprobará una parte del código de forma independiente.
- ⇨ Pruebas de integración: se realizan después de las pruebas unitarias, consiste en realizar pruebas sobre un conjunto de elementos que componen un determinado proceso en la aplicación.
- ⇨ Pruebas de sistema: comprueban el correcto funcionamiento de la aplicación en su conjunto, comprobando el correcto de todas las funcionalidades de la aplicación. Este tipo de pruebas debe tener en cuenta los requisitos especificados para la aplicación sometida a pruebas.
- ⇨ Pruebas de aceptación: conjunto de pruebas que realiza el cliente para validar el producto.
- ⇨ Pruebas de regresión: se encarga de asegurar que toda la aplicación sigue funcionando después de que se hayan realizado cambios. Consiste en una batería de pruebas que son ejecutadas periódicamente y de forma automática.

Caja negra

Caja negra: en este caso se centra en las funcionalidades de la aplicación o servicio, sin importar los procesos que se ejecutan internamente.

Para realizar este tipo de pruebas, se escoge una función específica para la que fue diseñada la aplicación y hay que comprobar que realiza dicha función de forma correcta. Para realizar esto se introducen una serie de valores de entradas y conocemos los valores de salida que debe proporcionar la aplicación. Si con los valores de entradas introducidos el resultado son los valores de salida esperados, esa funcionalidad es correcta, si el resultado son valores de salida distintos a los esperados, esa funcionalidad no es correcta.

Este tipo de pruebas necesitan unos casos de prueba que cumplan con unos criterios específicos. Para elegir unos buenos casos de prueba, debe cumplir que:

- ⇨ Reduce el número de otros casos necesarios para que la prueba sea razonable. Esto implica que el caso ejecute el máximo número de posibilidades de entrada diferentes para así reducir el total de casos.

- ⇨ Cubre un conjunto extenso de otros casos posibles, es decir, no indica algo acerca de la ausencia o la presencia de defectos en el conjunto específico de entradas que prueba, así como de otros conjuntos similares.
- ⇨ Cada caso debe cubrir el máximo número de entradas.

Existen diversas técnicas para identificar casos de pruebas buenos, estas técnicas son:

- ⇨ Particiones o clases de equivalencia.
- ⇨ Análisis de valores límite.
- ⇨ Conjetura de errores.

Participaciones o clases de equivalencia

Es un método que trata el dominio de valores de entrada dividido en un número finito de clases de equivalencia que cumplan la siguiente propiedad: la prueba de un valor representativo de una clase permite suponer «razonablemente» que el resultado obtenido (existan defectos o no) será el mismo que el obtenido probando cualquier otro valor de la clase. El proceso a seguir es el siguiente:

- ⇨ Identificar clases de equivalencia.
- ⇨ Crear casos de prueba correspondiente.

Para identificar una clase de equivalencia se sigue los siguientes pasos:

1. Identificación de las condiciones de las entradas del programa, es decir, restricciones de formato o contenido de los datos de entrada.
2. A partir de ellas, se identifican clases de equivalencia que pueden ser:
   - ⇨ De datos válidos.
   - ⇨ De datos no válidos o erróneos.
3. Existen algunas reglas que ayudan a identificar clase:
   - ⇨ Si se especifica un rango de valores para los datos de entrada, se creará una clase válida y dos clases no válidas.
   - ⇨ Si se especifica un número finito y consecutivo de valores, se creará una clase válida y dos no válidas.
   - ⇨ Si se especifica una situación del tipo «debe ser» o booleana (por ejemplo, «el primer carácter debe ser una letra»), se identifican una clase válida («es una letra») y una no válida («no es una letra»).
   - ⇨ Si se especifica un conjunto de valores admitidos y se sabe que el programa trata de forma diferente cada uno de ellos, se identifica una clase válida por cada valor y una no válida.
   - ⇨ En cualquier caso, si se sospecha que ciertos elementos de una clase no se tratan igual que el resto de la misma, deben dividirse en clases menores.

El último paso del método es el uso de las clases de equivalencia para identificar los casos de prueba correspondientes. Este proceso consta de las siguientes fases:

- ⇨ Asignación de un número único a cada clase de equivalencia.
- ⇨ Hasta que todas las clases de equivalencia válidas hayan sido cubiertas por (incorporadas a) casos de prueba, se tratará de escribir que cubra tantas clases válidas no incorporadas como sea posible.
- ⇨ Hasta que todas las clases de equivalencia no hayan sido cubiertas por casos de prueba, escribir un caso para una única clase no válida sin cubrir.

Análisis del valor límite (AVL)

La experiencia indica que los casos de prueba que exploran las condiciones límite de un programa producen un mejor resultado para detectar defectos. El AVL es una técnica de diseño de casos de prueba que complementa a la de particiones de equivalencia. Las diferencias son las siguientes:

- ⇨ Más que elegir «cualquier» elemento como representativo de una clase de equivalencia, se requiere la selección de uno o más elementos tal que los márgenes se sometan a prueba.
- ⇨ Más que concentrarse únicamente en el dominio de entrada (condiciones de entrada), los casos de prueba se generan considerando también el espacio de salida.

Conjetura de errores

Se enumera una lista de posibles equivocaciones típicas que pueden cometer los desarrolladores y de situaciones propensas a ciertos errores.

- ⇨ El valor cero es una situación propensa a error tanto en la salida como en la entrada.
- ⇨ En situaciones en las que se introduce un número variable de valores, conviene centrarse en el caso de no introducir ningún valor y en el de un solo valor. También puede ser interesante un lista que tiene todos los valores iguales.
- ⇨ Es recomendable imaginar que el programador pudiera haber interpretado algo mal en la especificación.
- ⇨ También interesa imaginar lo que el usuario puede introducir como entrada a un programa.

Pruebas aleatorias

En este tipo de pruebas se utilizan una serie de modelos, normalmente de tipo estadísticos, que representan las posibles entradas al programa para crear a partir de ellos los casos de prueba.
Las pruebas simulan posibles datos de entradas con la secuencia y frecuencia que podrían aparecer con el uso real de la aplicación. Si el proceso de generación se ha realizado correctamente, se crearán eventualmente todas las posibles entradas del programa en todas las posibles combinaciones y permutaciones.
Para la generación de pruebas se utiliza un tipo de herramienta específica denominada generadores automáticos de casos de prueba.
Las pruebas pueden necesitar una serie de documentos, existe un estándar, IEEE 829, que especifica una serie de documentos relacionado con el diseño de las pruebas.
Los documentos que especifica el estándar son:

- ⇨ Plan de pruebas: señalar el enfoque, los recursos y el esquema de actividades de prueba, así como los elementos a probar, las características,las actividades de prueba, el personal responsable y los riesgos asociados.
- ⇨ Especificación de diseño de las pruebas: especificar los refinamientos necesarios sobre el enfoque general reflejado en el plan e identificar las características que se deben probar con este diseño de pruebas.
- ⇨ Especificación de caso de prueba: definir uno de los casos de prueba identificando por una especificación del diseño de las pruebas.
- ⇨ Especificación de procedimiento de prueba: especificar los pasos para la ejecución de un conjunto de casos de prueba o, más generalmente, los pasos utilizados para analizar un elemento software con el propósito de evaluar un conjunto de características del mismo.

2.4. Redacción de guías de usuario

Cualquier aplicación informática debe proporcionar una serie de documentación, uno de los documentos mas importante y que siempre viene incluido con la aplicación es la guía de usuario.
Una guía de usuario de un aplicación es un documento, generalmente elaborado por el equipo desarrollador de la aplicación, destinado a ayudar al usuario en el manejo de la aplicación. Este documento muestra un conjunto de información de la aplicación como:

- ⇨ Opciones de la aplicación: muestra las opciones disponibles de la aplicación, explicando su significado y para qué sirven.
- ⇨ Funcionalidades: muestra todas las funciones que dispone la aplicación.
- ⇨ Uso de aplicación: enseña al usuario como utilizar la aplicación y pequeños trucos para facilitar su uso.
- ⇨ Problemas mas frecuentes: indica los problemas que habitualmente pueden surgir y las posibles soluciones.
- ⇨ Ayuda con la instalación y configuración de la aplicación.

La guía de usuario está indicada para aquellos usuarios que están empezando a utilizar la aplicación, aunque puede realizarse para usuario con un nivel mas alto, para facilitar la tarea de conocimiento y uso de la aplicación.
En una guía se suelen utilizar un conjunto de recursos, como:

- ⇨ Imágenes: generalmente capturas de pantalla de la aplicación.

- ⇨ Ejemplos: que permitirán practicar con la aplicación.
- ⇨ Esquemas o diagramas: utilizados para explicar como realizar un determinado proceso en la aplicación.

Para algunas aplicaciones pueden generarse diversas guías de usuario dependiendo del tipo de usuario, por ejemplos:

- ⇨ Guía para el desarrollador.
- ⇨ Guía para el administrador.

Es muy común este tipo de guía para determinados aplicaciones, la primera guía permite a un usuario generar código para la aplicación, la segunda guía está incluida en aquellas aplicaciones que tenga gestión de usuarios y explicara como utiliza el usuario administrador en la aplicación, este usuario tendrá todos los privilegios en la aplicación.

Otras guías que pueden incluirse, aunque son menos habituales son:

- ⇨ Guía para plugin o extensiones: indica cómo programar un plugin para la aplicación.
- ⇨ Guía para API: explica cómo utilizar la API de la aplicación.

Una guía de usuario está compuesta de múltiples secciones, dependiendo de la aplicación pueden ser el número y tipo de secciones, aunque suele existir un conjunto de secciones comunes, como pueden ser:

- ⇨ Portada y título.
- ⇨ Página de derechos de autor.
- ⇨ Índice.
- ⇨ Contenido de la guía.
- ⇨ Instalación de la aplicación en diversos sistemas operativo.
- ⇨ Problemas frecuentes.
- ⇨ Bibliografía y enlaces de ayuda.
- ⇨ Glosario.

Otras secciones que pueden incluir es una serie apéndices donde se explica algunas funcionalidades mas especificas, ejercicios o un resumen de cada capítulo con los datos más significativos.

Para la elaboración de una guía de usuario habitualmente se emplean programas ofimáticos que son más fáciles de utilizar. Permite utilizar diversos opciones para añadir diversos recursos como imágenes o índices.

Otra opción para la elaboración es utilizar Latex que es un lenguaje de sistemas orientado a la elaboración de documentos técnicos; principalmente utilizado en el ambiente universitario. Proporciona un conjunto de herramientas muy potente y la calidad del resultado es muy alta. Como desventaja tiene que necesita un periodo de aprendizaje más elevado que para los programas ofimáticos.

Una opción que últimamente está siendo utilizada por empresas desarrolladoras para la elaboración de guías de usuarios para sus productos son las Wikis. Una wiki es un sitio web con un organización donde cada página web puede incluir contenido de diversos formatos (texto, imágenes, vídeo o audio) siguiendo una estructura fijada. Existen diversas herramientas que permiten crear wikis de manera fácil.

Las ventajas de una wiki es su estructura de página web que facilita la lectura, como desventaja tenemos que requiere una serie de conocimientos técnicos.

Antiguamente las guías de usuario venían impresas con la aplicación, pero en actualidad es difícil ver guías impresas. El formato más utilizado para distribuir guías es el formato PDF y estas guías suelen estar disponibles en la página web de la empresa desarrolladora.

Resumen

Concepto de Anomalía y Fallo
Concepto de Alerta (advertencia) y Alarma
Tipos de Incidencias: Hardware, Software, Seguridad y Usuario
En la gestión de incidencias utilizamos herramientas: GLPI (inventario y ticket), Mapa de Red (topología para localizar elementos) y Nagios (monitorización, alarmas…)
Principio de Pareto
SAT (Servicio de Atención Telefónico) instalaciones de la empresa donde una serie de operadores reciben llamadas telefónicas de los clientes, registrando las incidencias que notifican los usuarios.
En los lenguajes de programación un tipo de datos (números, textos, fechas…) es débil cuando puedes cambiar el tipo asociado a una variable. Es decir, asignas que la variable Cantidad es numérica y luego puedes cambiarlo a texto, eso no proporciona ninguna integridad…
Conceptos de Concurrencia (más de una tarea a la vez), Escalabilidad (adaptarse a la carga de trabajo sin perder rendimiento) y Tiempo real (Muy poco tiempo entre emisión y recepción)
Concepto de Prueba de Caja Blanca (Como funciona, pruebas interiores) y Caja Negra (Funciona si o no, pruebas exteriores)