Métricas de calidad de servicios

Breve descripción:

En este componente formativo se determinará la importancia que tienen las métricas de calidad del “software” como herramienta fundamental con miras a cumplir los requerimientos implícitos y explícitos de los clientes, y que el producto entregado satisfaga las expectativas para la cual fue desarrollado, cumpliendo con las características puntuales para que las pruebas arrojen su resultado.

Abril 2024

Grupo de Ejecución de la Formación Virtual

Tabla de contenido

Introducción

Bienvenido al presente componente formativo, en el que se estudiarán las métricas de calidad de servicios. A través del siguiente video, podrá identificar la relevancia de este contenido.

Video 1. Métricas de calidad de servicios

Enlace de reproducción del video

Síntesis del video: Métricas de calidad de servicios
Video tutorial del experto donde se da una introducción a este componente formativo desde el interrogante: ¿Cuál cree que puede ser una buena estrategia para mantenerse competitivo y activo en el sector productivo?, además de tratar la

importancia de: realizar las pruebas de calidad de “software”; identificar las fallas en términos de accesibilidad, usabilidad, rendimiento y funcionalidad; la capacidad de integración de otras funcionalidades; las métricas de calidad de “software” como una herramienta fundamental para cumplir con los requerimientos de los clientes, de manera que el producto entregado cumpla con las expectativas para lo cual fue desarrollado. ¡Bienvenidos!

1. “Networking” y servicios de infraestructura

Seguramente ha escuchado los términos servicios de infraestructura y “networking”, pero, ¿a qué se refieren concretamente?

Según Icot (2021), el servicio de infraestructura IT es el conjunto de dispositivos y aplicaciones de “software” necesarios para que cualquier empresa opere (Párr.1).

Por otro lado, “networking” es la posibilidad que tienen múltiples usuarios con diferente ubicación geográfica, para trabajar en línea sobre una tarea específica de manera segura y eficiente, las 24 horas del día, los 7 días de la semana (24/7).

Es así como “networking” es una actividad que se ha venido extendiendo, debido a que las empresas requieren de personal en ubicaciones remotas, generando una cantidad de servicios derivados que son aprovechados por la industria debido a la reducción de costos de funcionamiento y a la automatización de procesos; es decir, las empresas ya no tienen que adquirir un “hardware” costoso para el funcionamiento de sus actividades económicas, porque existen muchas otras empresas que se dedican a prestar servicios en la nube.

“Networking” es un término muy robusto que involucra personas que se encuentran dispersas geográficamente, las cuales realizan actividades en conjunto para llevar a cabo un bien común, por lo que se requiere también de la agrupación de tecnología en “hardware” y “software” que intervienen en estas interacciones.

Los componentes “hardware” que poseen los servicios de infraestructura pueden ser utilizados por muchas empresas para ejecutar sus actividades comerciales y tener una continuidad en el negocio; este tipo de servicios hacen que las empresas no incurran en gastos elevados, adquiriendo tecnología y personal para su mantenimiento

o instalación, agilizando así una cantidad considerable de posibilidades de acceso a la información del negocio desde cualquier ubicación geográfica, gracias a sus bondades. Este método de trabajo es muy común actualmente, porque uno de los activos de mayor valor para las compañías es la información.

Los servicios de infraestructura que se ofrecen corresponden al "hardware" que una empresa podría adquirir para llevar a cabo sus actividades, pero por la versatilidad que representan estos servicios y la reducción de costo se delega o terceriza a empresas que se encargan de los mantenimientos y actualizaciones, como parte de la actividad de sus negocios.

Los servicios que se ofrecen en infraestructura se dividen en 4 elementos:

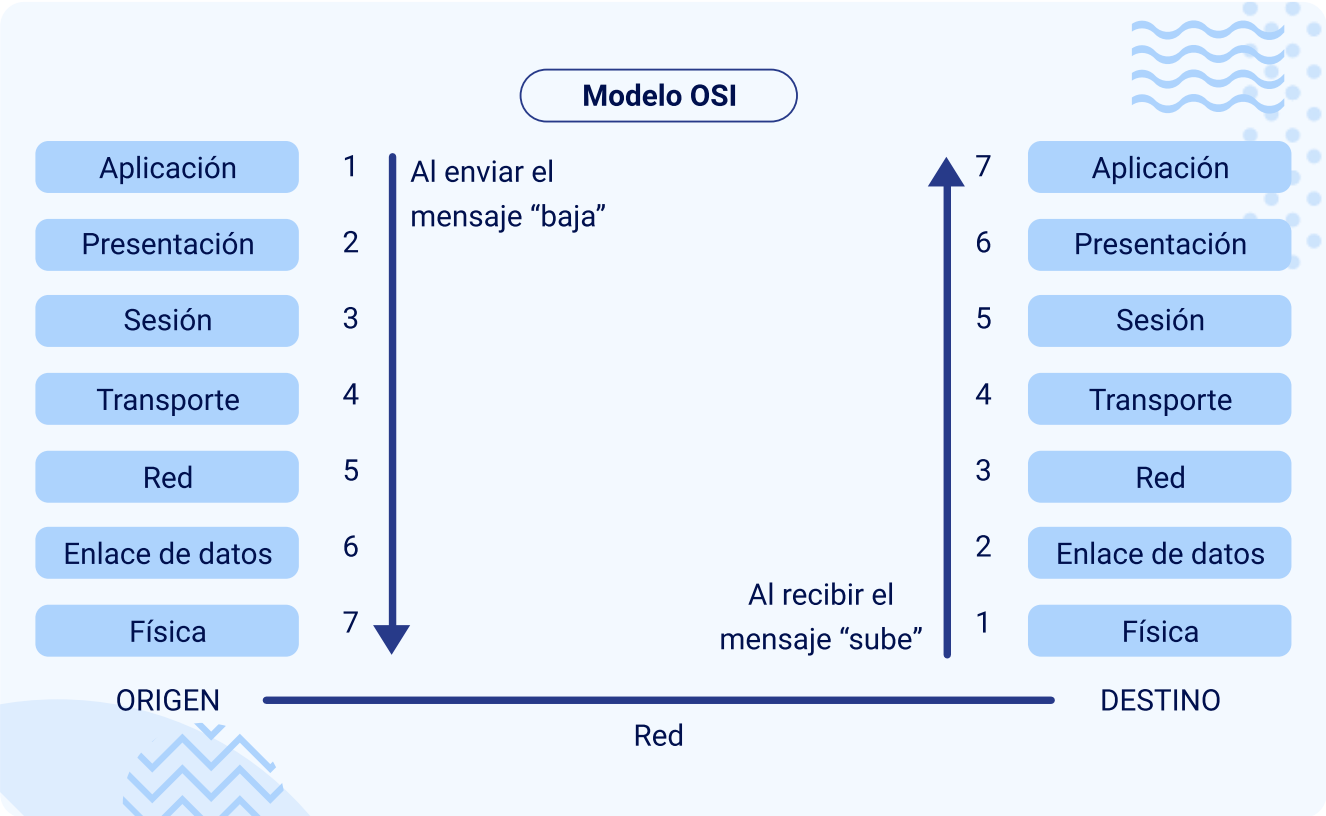
- **Almacenamiento:** el servicio de almacenamiento de información es de vital importancia para las empresas que requieran copia de seguridad en una locación diferente a aquella en la que, normalmente, funcionan, o para el funcionamiento de sus aplicativos.
- **Servidores:** los servicios de servidores reducen los costos para las empresas que los requieran, debido a que pueden realizar sus actividades comerciales con normal operación, evitando muchos costos en mantenimientos y actualizaciones.
- "**Networking**"**:** son dispositivos de interconexión que permiten un trabajo seguro por medio de switchs y conmutadores con conexiones seguras y rápidas entre los usuarios.
- **Seguridad:** la información contenida en dispositivos conectados a la red, hace parte importante en los activos de una empresa, de tal manera que se convierten en lo más preciado, porque contienen información crucial de

la actividad económica y de procesos clave para el desempeño. Asimismo, se adiciona la información personal y de los proveedores. La seguridad de la información se realiza con dispositivos “hardware” o “software” que la protegen de cualquier ataque.

1.1. Modelo de referencia OSI

Durante años, este modelo ha sido la base de las redes informáticas y el referente inicial para comprender los medios de transmisión con sus diferentes actores, lo que posibilita una comunicación exitosa entre máquinas y con un producto interpretado por las partes. Este modelo se divide en siete capas, las cuales se presentan en la siguiente figura.

Figura 1. Modelo de referencia OSI



De acuerdo con la figura anterior, en el modelo OSI encontramos las siguientes capas:

- **Capa física:** es la encargada de transmitir todo el flujo de "bits" sin procesar.
- **Capa de enlace de datos:** se encarga de definir el formato de los datos en la red.
- **Capa de red:** esta capa decide la ruta física por la que viajarán los datos.
- **Capa de transporte:** se encarga de la transmisión de los datos por medio de los protocolos TCP y UDP.
- **Capa de sesión:** es la capa que está pendiente de mantener la conexión entre puertos y sesiones.
- **Capa de presentación:** en esta capa se garantiza que los datos tengan un formato para ser interpretados, aquí se encriptan los datos.
- **Capa de aplicación:** en esta capa se establece la comunicación por medio de interfaces al usuario ocultando la complejidad del sistema.

Como se observa, los datos que transitan por los medios de comunicación son emitidos por un receptor y recibidos por otro receptor y están dirigidos por el concepto del modelo OSI.

Capas de presentación y aplicación

Las capas de presentación y aplicación, pertenecen al modelo OSI y se encuentran ubicadas en el lugar 6 y 7 cuando son receptores. Estas capas se encargan de trabajar y transformar la información al usuario.

La capa de presentación se encarga de garantizar que la transmisión sea entendida tanto por el emisor como por el receptor. Proporciona el formato a la información, reúne los formatos de presentación eligiendo sintaxis y semántica de lo que se está utilizando y puede conformar la información, transformando del formato de aplicación al de red y al contrario:

- **Formateo de datos:** es el proceso mediante el cual se interpretan dos códigos, por ejemplo: el código de caracteres decimales codificados en binario (EBCDIC), utilizado para representar los caracteres en la pantalla, y el código americano (ASCII) que tiene la misma función de dar forma a la información para visualizarla o imprimirla.
- **Cifrado de datos:** protección importante de la información durante la transmisión.
- **Compresión de datos:** por medio de técnicas algorítmicas busca patrones repetidos y los reemplaza por un token que es un patrón de "bit" mucho más corto.
- **Encriptación:** los datos se protegen con el proceso de encriptación.
- **Estructura de datos a transmitir:** Los protocolos presentes en esta capa de presentación son los siguientes:
  - ASN.1
  - MIME

Por su parte, la capa de aplicación se encarga de permitir a las aplicaciones de los usuarios, el acceso a las bondades de las otras capas.

Los usuarios interactúan directamente con la capa de aplicación; las que hacen este trabajo son las aplicaciones, escondiendo la complejidad del sistema al usuario.

En esta capa, existen algunos protocolos involucrados, que son interesantes nombrar:

- **FTP**: FTP (“File Transfer Protocol”), protocolo de transferencia de archivos que, como su nombre lo indica, realiza la transferencia de archivos.
- **DNS**: DNS (“Domain Name Service”), corresponde al servicio de nombres de dominio.
- **DHCP**: DHCP (“Dynamic Host Configuration Protocol”), o protocolo de configuración dinámica de anfitrión.
- **HTTP**: HTTP (“HyperText Transfer Protocol”), para acceso a páginas web.
- **NAT**: NAT (“Network Address Translation”), para traducción de dirección de red.
- **POP**: POP (“Post Office Protocol”), para correo electrónico.

1.2. IPv4 e IPv6

Según Cisco, una dirección IP se emplea para identificar a un dispositivo en una red IP. La dirección se compone de 32 “bits” binarios, que pueden dividirse en una porción correspondiente a la red y otra correspondiente al host, con la ayuda de una máscara de subred (Párr.6).

Cuando se menciona IPv4 e IPv6, se hace referencia a las versiones que se ofrecen del famoso protocolo de Internet (“Internet Protocol Next Generation” - IPng). En este sentido, el direccionamiento IPv6 es la versión más reciente y aún tiene poco

uso, aunque lentamente se está introduciendo a los hogares y a las compañías. Esta versión 6 del protocolo, presenta cambios relevantes frente a la versión 4.

La IPv4 está diseñada de la siguiente forma:

- Dirección de 32 “bits”.
- Direcciones desde la 0.0.0.0 hasta la 255.255.255.255.
- Organización en 4 octetos, separados por puntos en nuestros computadores (192.168.0.99).

Si traducimos la IP anterior a su código binario tendremos:

192.168.0.99 = 11000000.10101000.00000000.1100011.

La transición al nuevo protocolo no debería afectar en nada el funcionamiento, gracias a su compatibilidad, porque está diseñado para solucionar múltiples problemas presentados en la versión 4, por ejemplo, la carencia de direcciones en el mercado mundial y el limitado direccionamiento requerido por los dispositivos. El protocolo versión 6 permite la entrada a nuevas redes de alto desempeño como ATM, “Gigabit Ethernet”, etc.

Actualmente, hay millones de computadores y otros dispositivos conectados al Internet, por lo que las direcciones previstas por las compañías ISP han escaseado, teniendo en cuenta que hace algunos años se liberó el último paquete de direcciones con lo que se dio fin a las conjugaciones de las mismas. Por esta razón se considera que el IPv4 ya cumplió un ciclo de vida de más de 30 años.

Hace unos años era impensable que podríamos conectar a Internet cualquier tipo de producto, servicio o forma de comunicación, así como aplicaciones de control.

Debido a estas necesidades llegó la versión 6 del mismo protocolo de Internet, para solventar estos requerimientos.

Se ha venido identificando que, debido a la alta demanda de conexión a Internet, se ha requerido mayor cantidad de direcciones que se clasifican como privadas y públicas.

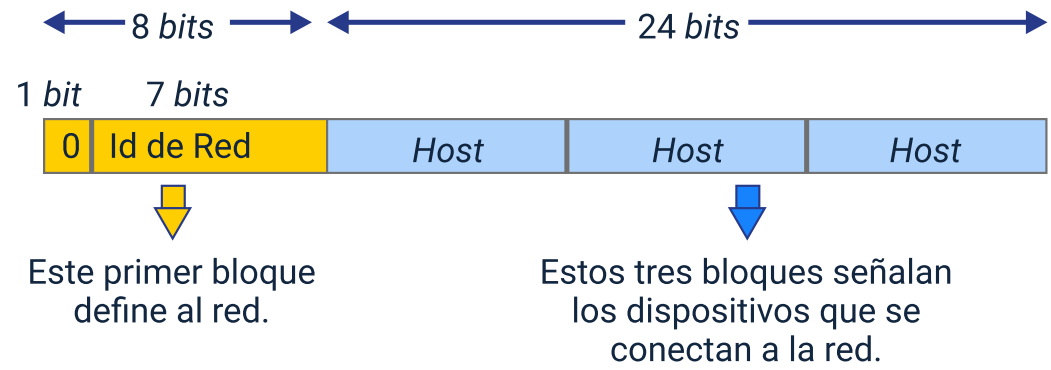
Direcciones privadas

Las direcciones IP privadas se encuentran en un esquema local; exactamente se refieren a las direcciones que asigna un router, de manera manual o automática, por medio de un protocolo llamado DHCP y que, en su conjunto hacen una red LAN. Tienen la característica de ser privadas porque son direcciones que no son visibles ante Internet, debido a que permiten la navegación a través de un dispositivo que sí tiene asignada una dirección pública vista en Internet.

Estas direcciones están dispuestas en rangos o clases, como se presenta a continuación:

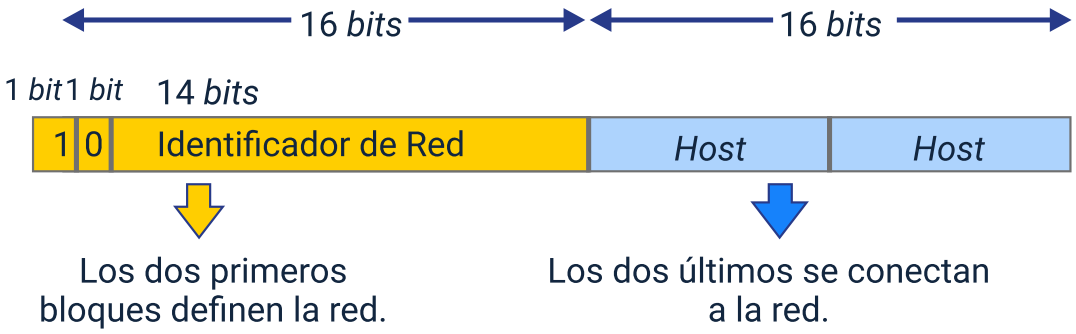
- **Clase A**: se utiliza por empresas de gran tamaño por la capacidad de conectar una cantidad considerable de equipos a la red; se pueden crear hasta 126 redes y conectar 16.777.214 dispositivos. El rango está comprendido entre: 10.0.0.0 a 10.255.255.255.

Figura 2. Clase A



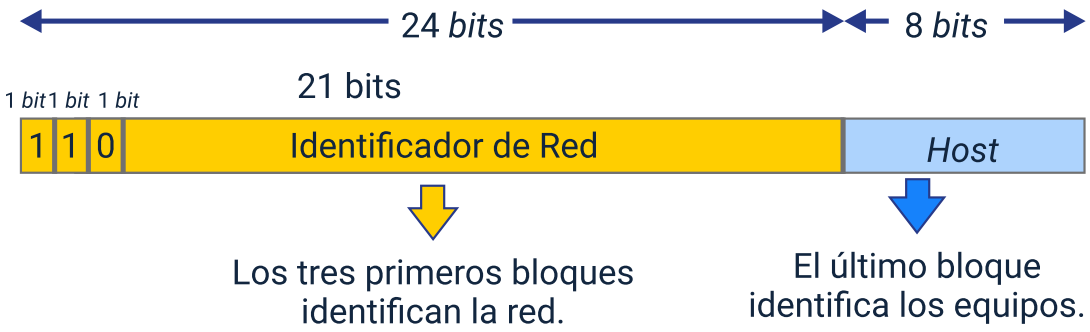
- **Clase B**: la clase B se utiliza en redes de tamaño medio, en la que se derivan más redes que la clase A (alrededor de 16.384 redes), pero con menos cantidad de dispositivos (65.534). El rango se define entre 172.16.0.0 a 172.31.255.255

Figura 3. Clase B



- **Clase C**: la clase C se conoce en las redes comunes y se conecta a 2.097.152 redes, pero con menor cantidad de dispositivos conectados a ella (alrededor de 254). El rango se encuentra desde 192.168.0.0 a 192.168.255.255

Figura 4. Clase C



Estas direcciones, independiente de la clase, deben ser únicas dentro de una red local, de tal manera que no exista otro dispositivo con la misma dirección IP. En caso de que llegara a suceder se generaría un conflicto de direcciones bloqueando a ambos dispositivos en la LAN.

Las direcciones IP privadas pueden estar repetidas, pero en diferentes redes; por ese motivo no habrá conflictos, porque las redes están separadas; también, es posible tener dos direcciones iguales, pero en distintas ciudades.

Direcciones públicas

Como ya se había indicado, también se presentan direcciones públicas, pero, ¿cómo funcionan?, ¿cuáles son sus características?, ¿presentan clases para su uso?

A continuación, respondemos cada uno de estos interrogantes.

¿Cómo funciona?

Una dirección pública se asigna a un equipo que está expuesto directamente a internet, por ejemplo, los routers que instalan las empresas prestadoras de servicio de

internet (ISP), los servidores que alojan información para acceder de manera remota, los servidores web, entre otros.

¿Cuáles son sus características?

Estas direcciones públicas presentan las siguientes características:

- No se pueden repetir, son únicas.
- Son asignadas por los proveedores de Internet (ISP).
- Se les conoce como IP dinámicas, porque cambian en determinado tiempo o cuando se reinicia el dispositivo de conexión (router).
- Existen direcciones IP públicas fijas o estáticas, en caso ser necesario. Cuando se quiere realizar el cambio de IP pública dinámica a estática se necesita contactar al proveedor para que se efectúe dicho cambio.

¿Cuál es la clasificación?

Las direcciones IP públicas también está denominadas por rangos, que corresponden a los rangos excluidos de las IP privadas. En este tipo de dirección el rango inicia en 1. … hasta 191. ….

De acuerdo con lo anterior, las clases de la IP pública se fijan así:

- Clase A: 1.0.0.0 a 126.255.255.255.
- Clase B: 128.0.0.0 a 191.255.255.255.
- Clase C: 192.0.0.0 a 223.255.255.255.

En la siguiente tabla, se pueden identificar las diferencias entre las direcciones públicas y privadas.

Tabla 1. IP privada vs. IP pública

IP privada	IP pública
Es asignada por un dispositivo (router) a los aparatos que se conectan al punto de enlace.	Es asignada por el proveedor de Internet ISP; en este caso la dirección va al dispositivo que conecta al exterior o router.
Los rangos se encuentran entre 10.0.0.0 a 192.168.255.255.	Las direcciones IP públicas también están denominadas por rangos y corresponden a aquellos que no están en las IP privadas (de 1… hasta 191).
Clase A: 10.0.0.0 a 10.255.255.255. Clase B: 172.16.0.0 a 172.31.255.255. Clase C: 192.168.0.0 a 192.168.255.255.	Clase A: 1.0.0.0 a 126.255.255.255. Clase B: 128.0.0.0 a 191.255.255.255. Clase C: 192.0.0.0 a 223.255.255.255.

De acuerdo con lo estudiado hasta el momento, se comprende que el protocolo IPv6 se creó para proporcionar direcciones IP a todos los dispositivos. Pero, en este sentido, es posible preguntarse: ¿cuántos dispositivos se podrían conectar con esta versión? A continuación, se presentan las características de este nuevo protocolo:

- Proporcionar IP fijas a todo tipo de dispositivos.
- Aumenta la cantidad de direcciones.
- Se utilizarán 128 “bits” de manera hexadecimal con menor espacio.
- Las direcciones se compondrán de 8 secciones cada sección con 16 “bits”.
- Las direcciones que se obtendrán: de 0:0:0:0:0:0:0:0 a ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.
- Las direcciones de los equipos o host se visualizarán con 128 ceros y unos.
- Con el nuevo protocolo IPv6 y los 128 “bits” se redireccionará un total de: 2128 = 340.282.366.920.938.463.463.374.607.431.768.211.456 hosts.

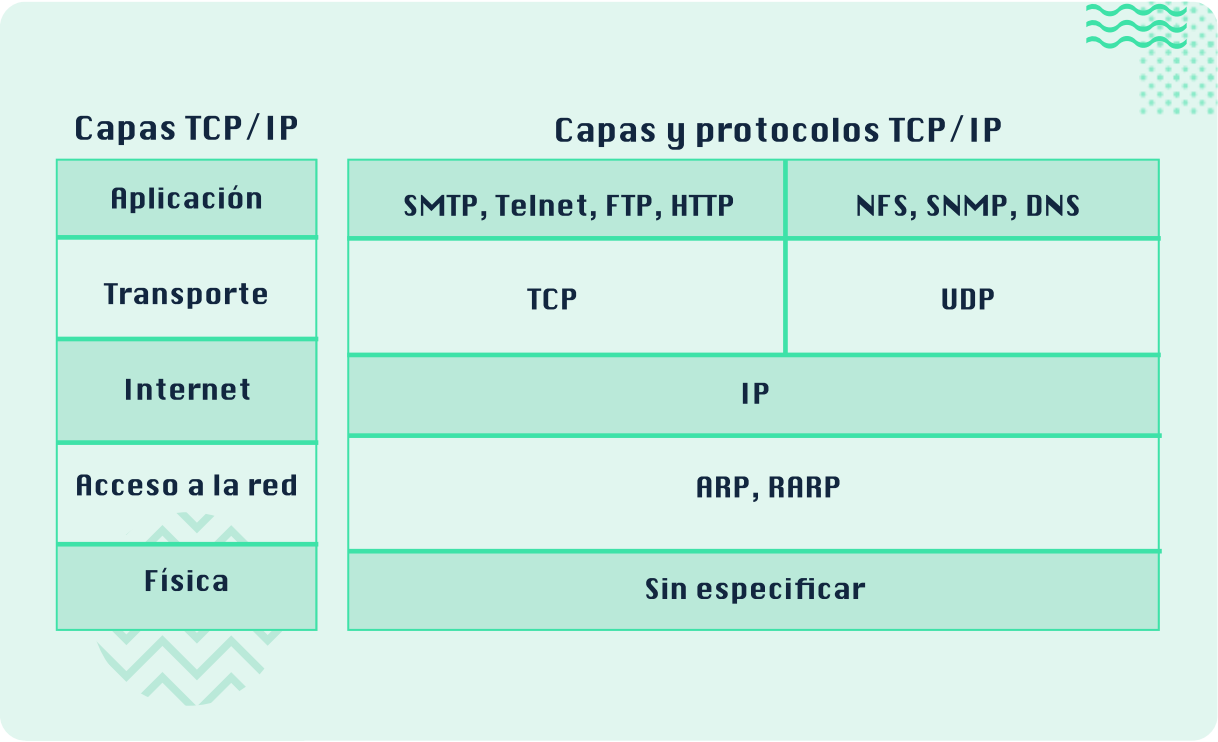
- Con este protocolo se podrán instalar los servidores que se quieran sin limitación debido a su capacidad.

TCP/IP

El protocolo de comunicación TCP/IP (protocolo para el control de transmisión / protocolo de Internet), es el más común y usado en el mundo para conectar los dispositivos con el exterior.

A continuación, se presenta la forma en la que se conforma este protocolo.

Figura 5. Protocolo TCP/IP



2. Alta disponibilidad

"High Availability" (HA) es la característica que tiene una arquitectura tecnológica que determina el grado con el que los servicios TI están activos o disponibles para ser usados por el cliente final. Por lo tanto, la alta disponibilidad garantiza que los sistemas estén disponibles, a pesar que existan fallos en las tecnologías que los soportan.

Una alta disponibilidad se mide en términos de porcentaje del tiempo que un sistema está disponible. En la siguiente tabla se presentan las categorías de los sistemas según su disponibilidad:

Tabla 2. Categorías de los sistemas según su disponibilidad

T disponibilidad	No Hay disponibilidad	Falla anual	Falla semanal
97 %	3 %	7,3 días	3 horas 22 minutos
92 %	8 %	3,65 días	1 hora, 41 minutos
99 %	1 %	17 horas, 30 minutos	20 minutos, 10 segundos
90 %	10 %	8 horas, 45 minutos	10 minutos, 5 segundos
99 %	1 %	52,5 minutos	1 minuto
99,777 %	0,223 %	5,25 minutos	6 segundos

Existen dos formas de activar la alta disponibilidad y mantener los servicios en operación: Activo-Activo y Activo-Pasivo.

En conclusión, se puede decir que el término redundancia se vincula a la implementación de alta disponibilidad, específicamente, mediante la implantación de, al menos, un dispositivo adicional que se emplea como respaldo (según el modelo activo-pasivo) o balanceador de carga (en el caso activo-activo).

Cuando se ofrecen servicios de alta disponibilidad (Higth Availability - HA), se puede suponer, en primer lugar, que se hace referencia al backup de los datos. Por lo tanto, este es el primer concepto que se debe excluir, debido a que la alta disponibilidad no conlleva copia de la información, de manera que se considera importante tener claridad en su significado.

Otro término fundamental es redundancia de "hardware", ¿qué significa?, ¿cuál es su objetivo?, ¿qué se logra? A continuación, responderemos estas preguntas.

¿A qué hace referencia?

Se relaciona con un componente del sistema duplicado. Considera que los proveedores de servicios en la nube ofrecen dichos servicios operando dentro de los Centros de Procesos de Datos (CPD), también conocidos como "Data Centers", y las máquinas en algún momento terminan fallando, porque tienen un tiempo de vida estimado muy difícil de garantizar.

¿Cuál es el objetivo?

El objetivo general no es evitar estos fallos, sino impedir que estas fallas no afecten a los usuarios, empresas o clientes con quienes se tienen contratos de servicios TI en la nube.

¿Cómo se logra?

Se logra duplicando el dispositivo de manera que cuando falle la máquina, los servicios que dependen de ese "hardware" sean trasladados de forma automática a un dispositivo que no esté afectado. De tal forma, que cuando dos dispositivos están publicados, se puede decir que están redundados.

2.1. Métricas de niveles de servicio

El funcionamiento del "hardware" sin fallas es la base para dotar a un sistema con alta disponibilidad; para ello, es imprescindible saber cómo presentar este valor según la norma IEEE 762/2006, que suministra el método del cálculo de este indicador para sistemas eléctricos, pero que se aplica también a todo sistema electrónico.

En esta norma se mencionan algunos indicadores:

- Fiabilidad.
- Disponibilidad.
- Tiempo medio entre paradas (MTBF, Mid Time Between failures).
- Duración de las paradas (MTTR, o Mid Time to Repair).
- Número de paradas por mantenimiento.
- Tiempo total perdido por mantenimiento.

En los casos MTTR y MTBF, aunque se refieren a paradas por falla, también se emplea para cualquier motivo por el que se detiene el servicio.

Para realizar estos cálculos se necesita tener los servicios con los siguientes datos:

- Servicio que se ha parado.

- Motivo de la parada (mantenimiento, actualización, falla, etc.).
- Duración de la parada (en minutos o segundos).

2.2. Clústeres

Cuando la HA es Activo-Activo, se puede tener mejor desempeño porque existe un balanceo de cargas; a este tipo de “agrupación” se le denomina clúster, nombre que se le da a un sistema compuesto con más de una unidad de procesamiento que trabajan de manera unificada hacia el mismo objetivo. Estas máquinas tienen en común que realizan las mismas tareas, debido a que tienen la misma configuración y sistemas informáticos para trabajar de forma simultánea.

La técnica del clúster se puede aplicar a:

- Máquinas virtuales.
- Contenedores.
- Arquitectura de computación.
- Redes.
- Computación en la nube.
- Banco de datos.

El nodo es el nombre que se atribuye a cada computador o unidad de procesamiento (máquina virtual, o contenedor) agregado a un clúster, sea virtual o físico.

En un clúster, los nodos se interconectan gracias a una tecnología o infraestructura de red, generalmente, una que ya es conocida por la empresa, con lo que se facilita el mantenimiento del sistema y control de los costos.

Cada nodo desempeña la misma función que los demás nodos, siendo posible suprimir o adicionar nodos cuando sea necesario, aún si el clúster se mantiene en funcionamiento sin interrupciones, de tal forma que estas operaciones de agregar o quitar no perjudican el proceso, ya que las tareas se distribuyen automáticamente sin ocasionar problemas.

Existen dos tipos de clústeres o motivos que se configuran:

- **Clúster de alto desempeño (High Performance Computing Cluster)**
  El objetivo es resolver problemas que requieren de mucho procesamiento concurrente (simultáneo); se realiza en un tiempo útil, cumpliendo la expectativa del usuario. Para lograr buenos resultados, se usa la técnica de balanceo de carga ("Load Balancing"), que consiste en repartir las tareas de manera similar o equilibrada entre los nodos.
- **Clúster de alta disponibilidad ("High Availability Computing Cluster")**
  Su principal objetivo es mantener el sistema en funcionamiento, es decir, está centrado en saber responder automáticamente a fallos sin afectar la continuidad de la prestación del servicio. Se requiere dotar al clúster de herramientas de control y monitoreo de fallas en la interconexión o en los nodos, redundancia de sistemas, sistemas sustitutos o de respaldo, entre otros.

Para que el sistema sea escalable, es importante saber que no existe límite de nodos que se puedan operar en un solo clúster; esta información es relevante cuando las empresas están en proceso de crecimiento continuo.

2.3. Computación en la nube

La migración de información a la nube es un paso obligado para particulares y empresas que tienen un alto nivel de infraestructura y cuentan con equipos de servidores, aplicaciones, redes, etc. Todo esto implica un largo y, a veces, complejo proceso de migración, que consiste en una serie de pasos para lograr una identificación, planificación, ejecución y evaluación de migración de servicios de TI locales a servicios en la nube.

Todo proyecto de implementación de servicios en la nube debe estar basado y dirigido por un plan estratégico hacia la migración, el cual varía según múltiples factores, teniendo en cuenta que para el abanico de productos TI no existen estrategias definidas.

Una de las ventajas de la infraestructura "cloud" es permitir combinar servicios que consoliden las necesidades de la organización. En el "cloud computing" es normal trabajar con las fórmulas de las 6 Rs para identificar diferentes estrategias de migración que se utilizan, según las características del proyecto TI.

2.4. Continuidad del negocio

Es importante que las empresas siempre tengan en cuenta los riesgos o amenazas que puedan tener en sus sistemas, redes, y datos. Desafortunadamente, no solo los desastres naturales están latentes en el día a día de una empresa, sino que también deben estar preparadas para delitos en la propiedad y fallas en la seguridad cibernética, dos riesgos de gran importancia. Se invita a analizar el siguiente caso:

El sector de la salud es muy regulado y una falla en la seguridad cibernética puede significar la afectación para muchas personas. En algunos países una situación

similar implica auditorías ante las entidades regulatorias; por ejemplo, en los Estados Unidos se debe notificar al Departamento de Salud y Servicios Humanos inmediatamente.

Por ello, es fundamental que, al realizar un plan, se tengan en cuenta las regulaciones pertinentes al sector de la industria en el que se encuentre la organización. Cuando se considera realizar un respaldo de información, se necesita plantearlo a gran escala. Una de las soluciones más importantes para asegurar que la información y los sistemas puedan recuperarse con pérdidas mínimas, es la implementación de múltiples centros de datos ubicados estratégicamente en diferentes regiones, o lo que se impone por estos días, una solución en la nube.

En este mundo tan competitivo y de rápida evolución tecnológica, muchas organizaciones dependen de aplicaciones de terceros para sus diferentes dependencias, como contabilidad, informática, mercadotecnia digital y recursos humanos.

Es importante que el plan de contingencia y continuidad de negocio, tenga en cuenta que las aplicaciones de terceros pueden disolverse o dejar de prestar servicios esenciales; por lo tanto, las empresas deben tener bajo la manga una lista de alternativas de proveedores adjunto a su plan de contingencia y, en caso de ser necesario, migrar la información para minimizar su dependencia en un solo proveedor.

Las empresas que preparan y organizan su contenido en la nube deben estar un paso adelante en caso de desastres. Entonces, ¿cómo se podrían preparar para enfrentar una situación extrema?

La gestión de contenido empresarial (ECM), es una aplicación diseñada para realizar de manera digital contenido y procesos de una compañía, con lo cual las

empresas pueden tener continuidad en sus procesos durante situaciones complejas. El personal puede tener acceso a sus labores empresariales desde cualquier lugar del mundo, lo que actualmente es una necesidad latente, transformándose en una tendencia empresarial. De esta manera, la empresa puede continuar con todos sus procesos.

Es así, que tener un plan de continuidad apoyado con un sistema de ECM es una opción que puede soportar las actividades empresariales en caso de fallos o de catástrofes:

- Permite acceder a las labores de la empresa desde cualquier parte, garantizando la continuidad del negocio.
- Proporciona controles de versiones de los documentos con lo que se garantizan documentos actualizados.
- Los servicios en la nube garantizan, sin necesidad de tener un lugar físico, que el negocio y los procesos tengan normal continuidad.
- La automatización de procesos importantes asegura la estandarización, consistencia y continuidad para generar una tranquilidad en los usuarios y garantizar el correcto funcionamiento.

Por otra parte, los valores del Objetivo de Punto de Recuperación (RPO, por sus siglas en inglés) y Tiempo Objetivo de Recuperación (RTO, por sus siglas en inglés), se deben incluir en el análisis de riesgos de negocio y se deben exponer los pasos para alcanzar estos valores dentro del plan. Es importante recordar que toda estrategia toma un tiempo estimado para la implementación, por lo que no se descartan estrategias que estén dentro de los parámetros de RPO y RTO.

Entonces, mantener varias de las opciones de servicio operando (clúster activo-activo) es una de las estrategias más rápidas, porque si una parte del servicio falla, la otra estará activa. La medida más suave es tener un sistema que se active manualmente como respaldo (también conocido como espera pasiva) en términos de RPO; la duplicación en tiempo real de la información (funcionalidad que comúnmente se incluye en las soluciones en la nube), se puede realizar una restauración de los datos de hasta segundos atrás, mientras una copia de un momento específico (snapshot) puede no estar al día y no llenar los requisitos para su RPO.

Entonces, ¿cómo se definen el RTO y el RPO?

- **RPO**

  Objetivo de Punto de Recuperación (“Recovery Point Objective”), se refiere a la copia de seguridad de los datos dentro del marco de una catástrofe. Establece un tiempo desde la última copia de seguridad directamente relacionada a la cantidad de datos que la empresa puede perder en caso de un desastre. RPO significa la pérdida tangible de datos, entre la copia de seguridad y el incidente.

- **RTO**

  Tiempo Objetivo de Recuperación (“Recovery Time Objective”), es el tiempo máximo que una empresa define para recuperar sus procesos; en los casos en los que se ha sufrido algún inconveniente de cualquier índole, que haya generado la suspensión de las operaciones. Entonces, el RTO es el tiempo requerido para solucionar el incidente, en el que se reanuden todas las operaciones con normalidad.

Sin importar la actividad económica que tenga la empresa, en un inesperado desastre, los datos corren un alto riesgo de perderse. En el plan de continuidad del negocio y en el de una recuperación ante desastres, se requiere saber cuánto tiempo se va a estar sin servicio, cuánto tiempo tardarán los procesos en restaurarse y qué datos se pueden llegar a perder, antes de recuperar la continuidad operacional.

3. Tipos de pruebas de servicio

Las pruebas de “software” son importantes en el ciclo de vida y en el desarrollo del mismo “software”; generan tranquilidad al equipo desarrollador por un trabajo confiable y, por supuesto, al usuario final que es quien utilizará el producto; es necesario asegurar la funcionalidad, el rendimiento y la experiencia del usuario. En este sentido, las pruebas, sean manuales o automatizadas, tienen el objetivo de garantizar la calidad de un producto antes de salir al mercado, por lo que se expone a diversos “test” para evitar problemas y ahorrar dinero a la empresa, previniendo posibles inconvenientes con sus clientes, porque si los problemas trascienden al entorno de producción, con seguridad su solución resultará más costosa.

Según IBM (s.f.), la prueba de “software” es el proceso de evaluación y verificación de un producto o aplicación de “software” para saber si hace lo que se supone que debe hacer. Los beneficios de las pruebas incluyen la prevención de errores, la reducción de los costos de desarrollo y la mejora del rendimiento (Párr.1).

Existen dos tipos de pruebas: funcionales y no funcionales; dentro de las funcionales se podría decir que existen unas subpruebas como las unitarias, de componentes, de humo, integración, cordura y aceptación. De otra parte, dentro de las no funcionales se encuentran las pruebas de carga, de estrés, de volumen, de configuración, de usabilidad, de seguridad, de resistencia, de escalabilidad, de recuperación y de mantenibilidad. Cada prueba de “software” expone la aplicación para examinarla a fondo y tomar decisiones oportunas en caso que se detecte un error desde el código hasta la experiencia del usuario.

A continuación, se tomará la prueba Performance que corresponde a la prueba de rendimiento del navegador Google Chrome. Esta herramienta es muy útil para los

desarrolladores de “software”, y se encuentra incorporada dentro de los navegadores Chrome y Mozilla.

“Performance testing”

La prueba “performance testing” es del tipo no funcional; identifica la velocidad, estabilidad y escalabilidad de una aplicación de “software”, es por eso que estas pruebas realizan la comprobación del rendimiento de la aplicación en los diferentes puntos de referencia del sistema y de la red, como la utilización de la CPU, la velocidad de carga de la página, el control de tráfico máximo, la utilización de recursos del servidor, etc. En estas pruebas de rendimiento, hay varios tipos de pruebas, como pruebas de carga y pruebas de esfuerzo.

Hoy en día, todas las empresas se han volcado a la era digital, por lo que se ha convertido en algo fundamental medir y rastrear el rendimiento de la prestación de servicios, especialmente, las métricas que arrojan los resultados provenientes del tiempo de actividad de los sistemas, de inactividad, debido a eventos inesperados y de la rapidez y eficiencia con que se restablecen los procesos; un pequeño fallo puede causar la parálisis de procesos vitales que presentan pérdidas económicas en millones de pesos para una compañía.

MTTR, MTBF, MTTF y MTTA son las siglas de las métricas de gestión de incidentes más importantes. En el marco de los servicios de TI, estas métricas permiten llevar un plan estratégico y una organización efectiva de los recursos para garantizar la solución de fallos causados por “hardware” y “software” (Gupta, 21).

Conozcamos cada una de ellas:

Tiempo medio de reparación (MTTR)

Es el tiempo medio que se tarda en recuperar un daño físico o lógico desde que llega el primer aviso de fallo, sin que se incluyan los retrasos en el sistema de alertas. Se involucra el apagado provocado por una interrupción hasta que el sistema vuelve a estar disponible al 100 %. MTTR es un excelente indicador para medir la velocidad de la recuperación del sistema general.

En este caso, la R no siempre se relaciona con la reparación, aplica para recuperación, respuesta o resolución. Estas métricas tienen relación entre sí, pero también tienen diferencias puntuales, por lo que hace parte de las buenas prácticas identificar qué MTTR se utilizará.

MTTR normalmente se usa en ciberseguridad para medir la eficacia del equipo en la evasión de ataques que está sufriendo el sistema. Se utiliza para medir el tiempo que se utiliza para resolver un problema por completo del sistema, incluyendo el tiempo invertido en detectar, identificar y resolver el problema hasta asegurarse que no vuelva a ocurrir. Se emplea para medir la solución de problemas imprevistos, pero no para solicitudes de servicio.

Tiempo medio entre fallos (MTBF)

Es una métrica muy importante, porque genera un aviso a los usuarios para realizar un mantenimiento preventivo contra un fallo o para reemplazar algún "hardware" antes que ocurra una parada del sistema, que pueda perjudicar la operación; si al realizar un mantenimiento preventivo, se observa que el MTBF ha mejorado, se plantea un parte positivo en la fiabilidad del "hardware". El aumento de MTBF es una clara manifestación de efectividad de los procesos de mantenimiento.

Este indicador corresponde al tiempo promedio que transcurre desde la solución de un problema hasta la siguiente vez en que se vuelve a ocasionar. El MTBF mide la disponibilidad y confiabilidad, es decir, entre mayor es el número de MTBF, más confiable es el sistema.

Tiempo medio para fallar (MTTF)

Se refiere al tiempo que transcurre de una falla irreparable de un sistema. MTTF mide la confiabilidad de los sistemas no reparables y mide el tiempo que funcione el sistema antes de que falle por completo.

Esta métrica es importante para identificar la vida útil de los dispositivos reemplazables y no reemplazables, como teclados, baterías, teléfonos de escritorio, ratones, etc. Los datos históricos sobre el MTTF de cada tipo de "hardware", permiten al personal de TI tomar medidas de obsolescencia de manera escalonada.

Esta métrica se usa para identificar el ciclo de vida de un sistema, control de versiones y cuándo planificar las revisiones del sistema.

Como se observa, cada una de estas métricas tiene una aplicación particular según la incidencia o fallo que un sistema puede presentar; pero, ¿cómo se calculan? A continuación, se presenta cómo calcular cada una de ellas.

¿Cómo calcular el MTTR?

MTTR es una métrica de gestión de incidentes que los equipos utilizan para estar al día con las reparaciones, se debe procurar mantener el número de MTTR lo más bajo posible, optimizando la eficiencia de los equipos que ejecutan los procesos de reparación.

MTRR es igual al tiempo total dedicado a las reparaciones durante un período determinado, dividido en el número de reparaciones.

Veamos el siguiente ejemplo:

Consideremos que hubo 6 fallas en un sistema y que el mantenimiento requerido para recuperarlo a la operatividad completa tomó 3 horas, que son 180 minutos. Entonces, el MTTR sería: MTTR = 180/6 = 30 minutos.

Esto es igual a que el MTTR de una organización es de 30 minutos, siendo este el tiempo promedio que la organización dedica a cada tiempo de inactividad.

¿Cómo se calcula el MTBF?

Consideremos que un sistema funciona perfectamente durante 13 horas. Durante este período, ocurren 3 fallas que causan un tiempo de inactividad total de 1 hora. Entonces, el MTBF se calcula así:

(13-1)/3

Este resultado nos indica que ocurre una falla en el sistema cada 4 horas, lo que origina que el sistema quede “off”, con lo cual se generan pérdidas para la empresa. El acompañamiento de esta métrica puede reducir el tiempo de inactividad.

MTBF es igual al tiempo de actividad operativo total entre fallas, dividido en el número total de fallas.

¿Cómo se calcula el MTTF?

MTTF es la principal métrica de confiabilidad de un “hardware” no reparable, por lo que el propósito es ampliar la vida útil del activo. Un MTTF más corto conlleva a repetidas interrupciones y tiempos de inactividad.

MTTF es igual a las horas totales de funcionamiento, dividido en el número total de fallas.

Veamos el siguiente ejemplo:

Consideremos que se observan tres sistemas idénticos hasta que todos fallan. El primer sistema duró 14 horas, el segundo 16 horas y el tercero 12 horas.

Entonces, MTTF se calcula así:

$$MTTF = (14 + 16 + 12) / 3$$

El resultado se interpreta que, en promedio, este tipo de sistema debe ser reemplazado cada 14 horas para evitar tiempos de inactividad más prolongados y daños posteriores.

¿Cómo se calcula el MTTA?

Esta métrica se emplea para monitorear la capacidad de respuesta, es decir, si un equipo se demora en su respuesta y sufre de estrés por alerta, MTTA contribuye a resaltar el problema.

MTTA es igual al tiempo total transcurrido entre la alerta y el reconocimiento, dividido en el número total de incidentes.

Veamos el siguiente ejemplo:

Hubo 5 incidentes en una empresa y tomó un total de 30 minutos de tiempo entre la alerta y el reconocimiento de todos los incidentes, entonces, el MTTA se calcula así:

$$MTTA = 30 / 5 = 6$$

La respuesta a la métrica MTTA es de 6 minutos, por lo cual la organización debe trabajar en reducir este tiempo para optimizar su proceso de resolución.

3.1. Gestión del proceso de pruebas

La gestión de pruebas soporta el ciclo de vida de una prueba (diseño, recopilación, verificación, activación, corrección y compartición), a la vez que reutiliza pruebas en múltiples programas. Es una parte clave del proceso global de elegibilidad y titularidad, comprendiendo que la elegibilidad se revaloriza de forma permanente, debido a los cambios en las circunstancias, reglas o tasas que tienen lugar a lo largo del tiempo.

La gestión de pruebas proporciona las siguientes características:

- **Traducción rápida de la legislación y la política**

  Herramientas de usuario de negocio para una traducción rápida de la legislación y la política, en una estructura de pruebas y unos requisitos de verificación.
- **Auditorías**

  Auditorías, históricos, seguridad y corrección de pruebas preconstruidas.
- **Flujos de trabajo**

  Flujos de trabajo preconstruidos que supervisan la validez de las verificaciones, e inician el proceso de nueva verificación.
- **Preconstruidas**

  Herramientas preconstruidas de gestión de pruebas, para la mejora de la productividad del asistente social.

- **Experiencia de usuario**

  Una experiencia de usuario coherente a lo largo del ciclo de vida, como por ejemplo, admisión, verificación, activación, corrección y compartición entre programas.

- **Visualización**

  La visualización de pruebas centra la atención del usuario en tareas pendientes, tales como la verificación y la activación.

- **Espacio de trabajo**

  Espacio de trabajo y flujos de trabajo de gestión de pruebas compartidas, para incorporar revisiones específicas de programa.

Estos procesos de aseguramiento de calidad de "software", normalmente se caracterizan por el análisis en pruebas estáticas y dinámicas, pero, ¿cuáles son las diferencias entre estas pruebas?

- **Pruebas estáticas**

  Se enfocan en la calidad de la documentación del proyecto, realizando revisiones periódicas.

- **Pruebas dinámicas**

  Precisan la ejecución del "software" para examinar la calidad del código con el que fue creado y verificar el cumplimiento con las especificaciones del sistema.

Cuando se efectúan pruebas dinámicas a un producto de "software", se piensa, normalmente, que se hace referencia a la ejecución del "software" y a la verificación de una serie de incidencias, al contrario de los productos robustos, se recomienda una metodología de pruebas que se ajuste a la metodología de desarrollo del "software".

Para desarrollos basados en la metodología RUP o métodos tradicionales, se recomienda implementar una metodología de pruebas totalmente viable, considerando que estas metodologías están orientadas a la documentación y formalización de todas las actividades realizadas. Si la firma desarrolladora realiza un acompañamiento del proceso bajo los lineamientos basados en metodologías ágiles, se estudiará la conveniencia de iniciar las actividades que tengan que ver con el proceso de pruebas formales.

Los procesos de pruebas que se realizan correctamente contienen 5 etapas:

a) Planeación de pruebas.
b) Diseño de pruebas.
c) Implementación de pruebas.
d) Evaluación de criterios de salida.
e) Cierre del proceso.

Se profundizará en la primera etapa.

Planeación de pruebas

En esta etapa se realizan las primeras pruebas que generan un entregable denominado Plan de pruebas, el cual debe considerar los siguientes aspectos:

- **Alcance de la prueba**

  Se identifica qué funcionalidades del producto serán probadas durante el transcurso de la prueba. El listado de funcionalidades se realiza con base en el estudio de riesgos realizado previamente, teniendo en cuenta variables como la falla de una funcionalidad o la posible falla de una de estas. Con este análisis se obtiene información adicional, para determinar,

además del detallado, la urgencia con la que las funcionalidades deben probarse.

- **Tipos de prueba**

  Es fundamental seleccionar los tipos de prueba que se pueden emplear para determinada aplicación, debido a que no es posible utilizar todos los tipos de prueba; por eso es indispensable que el encargado plantee las preguntas necesarias para identificar las pruebas correctas que se deberán implementar. Dentro de estos posibles tipos de pruebas se encuentran las de estrés, de rendimiento, de carga, de usabilidad, de regresión, entre otros.

- **Estrategia de pruebas**

  Por medio de un análisis de riesgos, se determina en qué funcionalidades del aplicativo se centrará nuestra aplicación; asimismo, en la estrategia de pruebas se indicarán los ciclos que se aplicarán y la intensidad o profundidad a realizar en cada nivel de prueba definido.

- **Criterios de salida**

  Las partes involucradas en el proceso, definen los entregables y la profundidad con la que se realizará una prueba, así como a qué funcionalidades se le realizarán las pruebas. Los criterios de salida se definen para cada nivel de pruebas; algunos de estos criterios son los siguientes:

  - Porcentaje de funcionalidades de alto riesgo probadas con éxito.
  - Número de defectos críticos y/o mayores aceptados, etc.

- **Diseño de pruebas**

  Cuando se haya definido el plan de pruebas, se debe realizar el examen de toda la documentación referente al sistema para empezar con el diseño de casos de pruebas; los entregables importantes podrían ser los siguientes:

  - Casos de uso.
  - Historias de usuario.
  - Arquitectura del sistema.
  - Diseños.
  - Manuales de usuario.
  - Manuales técnicos.

  En el diseño de los casos se deben tener en cuenta los casos positivos y negativos. En los casos de pruebas negativas, dejan evaluar el comportamiento ante situaciones atípicas y permite verificar la robustez del sistema.

- **Implementación y ejecución de pruebas**

  Cuando se ejecutan las pruebas en el sistema, se debe indicar la creación de datos de prueba para realizar los casos diseñados. Estos se pueden ejecutar de manera manual o automatizada. Cuando se detecte un fallo en el sistema se debe documentar y registrar en una herramienta indicada para ello; una vez el defecto se corrige, se valida nuevamente en el proceso de depuración, para hacer la verificación de la corrección. Así, se necesita hacer un proceso de regresión para verificar que dicha corrección no genere otro tipo de errores.

- **Evaluación de criterios de salida**

  La evaluación de criterios de salida se requiere para determinar si es posible dar por terminado el ciclo de pruebas; para ello, se necesita comparar, al final del proceso, las métricas obtenidas con las métricas esperadas; si estas métricas esperadas no son nada similares con las obtenidas, entonces, no es posible continuar con el proceso.

- **Cierre del proceso**

  En la planeación no se dedica mucho tiempo a esta parte del proceso. Se deben cerrar las incidencias reportadas, se verifica si los entregables diseñados han sido entregados y aprobados y, finalmente, se realizan y aprueban los documentos de soporte de prueba.

3.2. Normas y estándares

Normalmente, las aplicaciones son construidas por empresas desarrolladoras o terceros, y los contratantes de estos servicios confían en que el desarrollo que están adquiriendo tenga las condiciones de calidad; esto considerando que usualmente no tienen los medios para auditar el sistema que se les está entregando, por lo cual no pueden argumentar defectos en el proceso. Para este efecto se han establecido normas y estándares, que regulan estos servicios.

Los estándares de calidad de “software” hacen parte de la ingeniería de “software”, utilización de estándares y metodologías para el diseño, programación, prueba y análisis del “software” desarrollado, con el objetivo de ofrecer una mayor contabilidad, mantenibilidad en concordancia con los requisitos exigidos, con esto se eleva la productividad y el control en la calidad de “software”, parte de la gestión de

la calidad se establecen a mejorar su eficacia y eficiencia (Párr.1). Arciniega (2018) indica que:

Así, estos estándares de calidad del "software" ofrecen una mayor confiabilidad y concordancia con los requisitos exigidos. Pero, ¿cuáles son las normas que rigen la calidad del "software"?

- **ISO 12207 – Modelos de ciclos de vida del "software"**

  Este estándar se concibió para clientes de "software", así como para desarrolladores y proveedores. Indica una serie de procesos desde la recopilación de requisitos hasta la culminación del "software".

  El estándar comprende 17 procesos los cuales son agrupados en tres categorías principales:

  - De apoyo.
  - De organización.
  - De organización.

  La ISO 12207 agrupa las actividades que se pueden llevar a cabo durante el ciclo de vida del "software" en cinco procesos principales, ocho procesos de apoyo y cuatro procesos organizativos.

- **Norma ISO/IEC 9126 de 1991**

  Esta norma evalúa los productos de "software", indica la calidad y la forma de uso, las características de calidad del desarrollo y las métricas aplicadas, es decir, facilita la evaluación del producto. Esta norma se define en un marco conceptual basado en factores como la calidad del proceso y la calidad del producto del "software" que contribuye a mejorar la calidad

en el uso. Según la ISO/IEC 9126, la calidad en uso es la perspectiva del usuario de la calidad del producto "software" cuando se emplea en un ambiente específico y contexto específicos. Mide la extensión en la que los usuarios pueden conseguir sus metas en un ambiente particular, en vez de medir las propiedades del "software" en sí mismo.

3.3. Herramientas de pruebas

Una de las herramientas de prueba es la de performance o rendimiento, que hace referencia a la evaluación del rendimiento, valga la redundancia, de un sistema que está sujeto a manipulación por parte del usuario para que este arroje un resultado; las pruebas performance que se realizan se refieren a los tiempos de respuesta y estabilidad de los recursos que se utilizan en cuanto a "hardware" y a la utilización de los recursos de red, aplicando una carga de trabajo. En general, estas pruebas se diseñan para verificar la velocidad, la solidez, la confiabilidad y el tamaño de la aplicación; cuando se realiza este proceso se involucran algunos indicadores como:

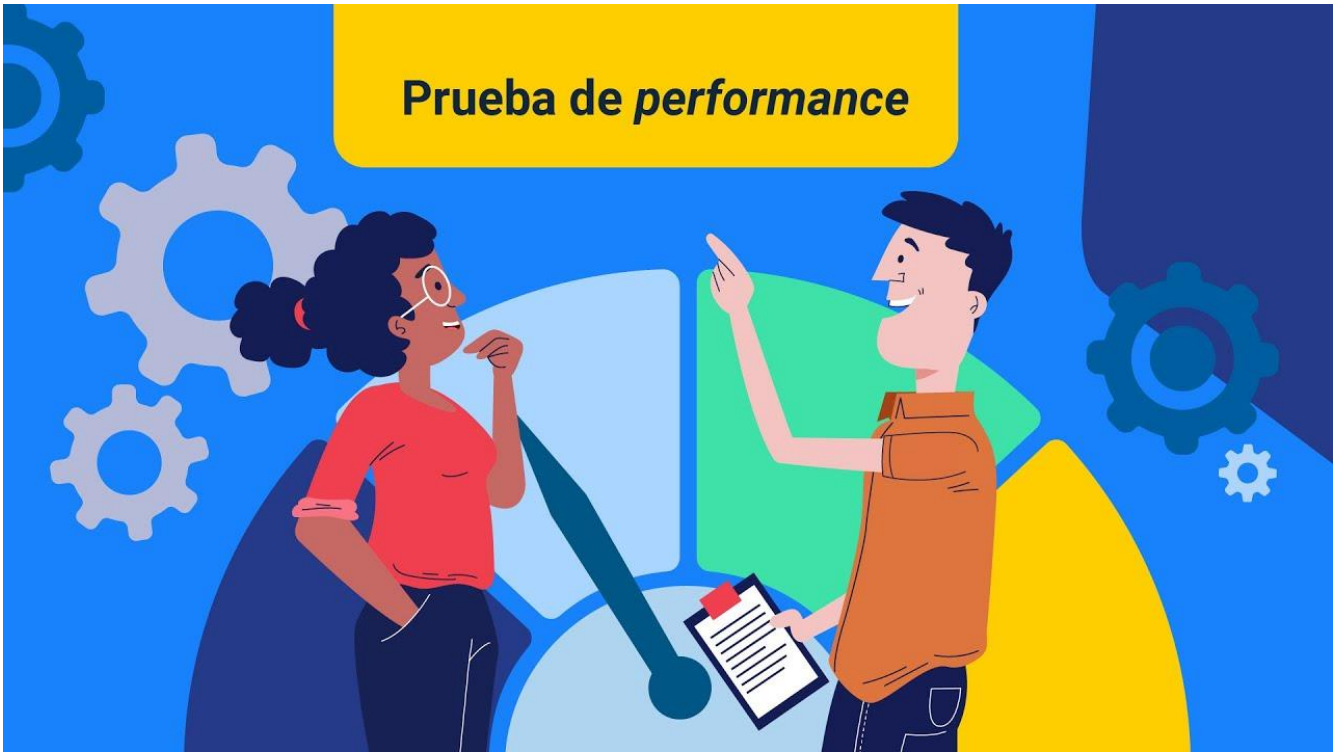
- Tiempos de respuesta del navegador, la página y la red.
- Tiempos de procesamiento de solicitudes del servidor.
- Volúmenes de usuarios simultáneos aceptables.
- Consumo de memoria del procesador, número y tipo de errores que se pueden encontrar con la aplicación.

Las pruebas de performance verifican las pruebas de velocidad, la solidez, la confiabilidad y el tamaño correcto de una aplicación. Hay muchos indicadores, como el navegador, los tiempos de respuesta de la página y la red, el tiempo de procesamiento

de consultas del servidor, la cantidad de usuarios conectados al tiempo, el consumo de memoria de la CPU y la cantidad y tipo de errores al usar alguna aplicación.

En el siguiente video se presenta la prueba de performance mediante el navegador de Google Chrome:

Video 2. Prueba de performance

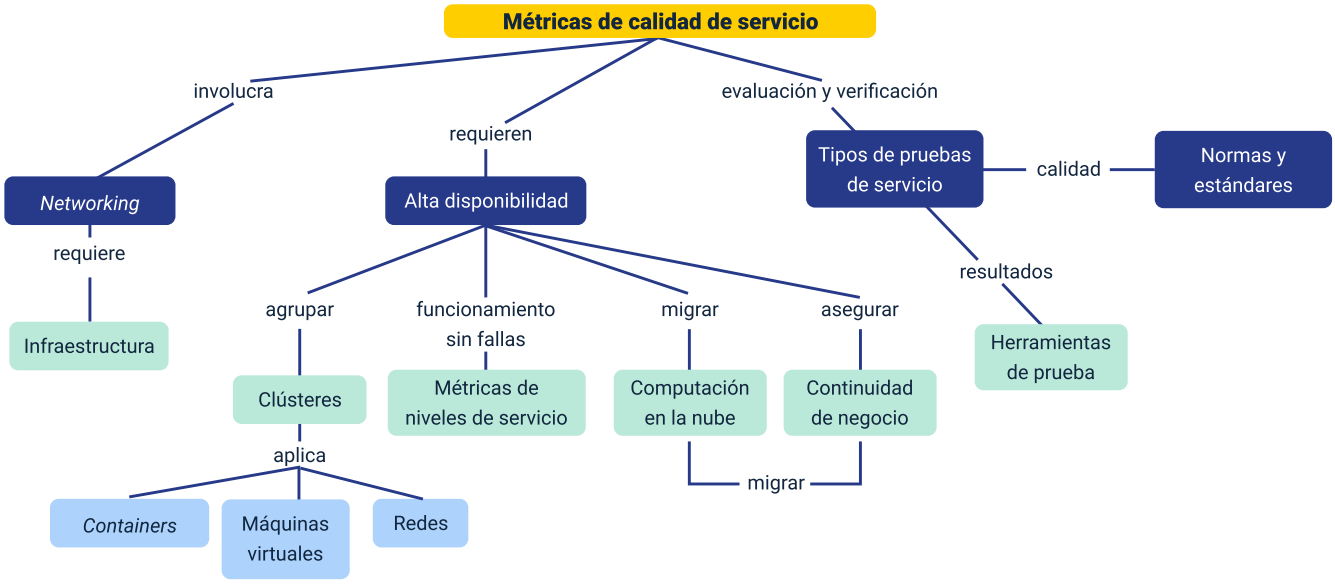


Enlace de reproducción del video

Síntesis del video: Prueba de performance
Video tutorial del experto donde se explica cómo usar el panel de rendimiento o performance de Google Chrome desde las “tools”, que proporciona un análisis del rendimiento del tiempo de ejecución, se practica como usar el panel de rendimiento

de Chrome, en términos del modelo Raid las habilidades que aprenderán son útiles para analizar las fases de respuesta, animación e inactividad de la aplicación. El tutorial inicia con el uso de las herramientas de desarrollo de Jank.

Síntesis


Métricas de calidad de servicio
involucra
requieren
evaluación y verificación
Networking
requiere
Infraestructura
Alta disponibilidad
agrupar
funcionamiento sin fallas
migrar
asegurar
Clústeres
aplica
Containers
Máquinas virtuales
Redes
Métricas de niveles de servicio
Computación en la nube
Continuidad de negocio
migrar
Tipos de pruebas de servicio
calidad
Normas y estándares
resultados
Herramientas de prueba

Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
IPv4 e IPv6	Mastering IT. (2020). Un resumen completo del modelo #TCPIP (Todas sus capas en menos de 7 minutos) [video]. YouTube.	Video	https://youtu.be/1pB2kan_AFk

Glosario

Capa: capa compleja que permite conectividad y elige una ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas (Todo de Redes. 2021).

Interoperabilidad: capacidad de comunicación entre distintos sistemas con distintos datos en distintos formatos de modo que la información pueda ser compartida, accesible desde distintos entornos y comprendida por cualquiera de ellos (Ecityclic, 2019).

"Performance testing": reúnen todas las pruebas que verifican la velocidad, la solidez, la confiabilidad y el tamaño correcto de una aplicación. Examina varios indicadores, como el navegador, los tiempos de respuesta de la página y la red, el tiempo de procesamiento de consultas del servidor, la cantidad de usuarios simultáneos aceptables diseñados, el consumo de memoria de la CPU y la cantidad/tipo de errores que se pueden encontrar al usar una aplicación.

Red de datos: infraestructuras o redes de comunicación que se han diseñado específicamente para la transmisión de información mediante el intercambio de datos. Las redes de datos se diseñan y construyen en arquitecturas que pretenden servir a sus objetivos de uso. Las redes de datos, generalmente, están basadas en la Comunicación de paquetes y se clasifican de acuerdo con su tamaño, la distancia que cubre y su arquitectura física (EcuRed, 2021).

Referencias bibliográficas

Arciniegas, A. (2018). Normas y estándares de calidad para el desarrollo de “software”. http://fcaenlinea.unam.mx/anexos/1728/Unidad_2/u2_act2_1.pdf

Cisco. (2023). Configuración de direcciones IP y subredes únicas para nuevos usuarios. https://www.cisco.com/c/es_mx/support/docs/ip/routing-information-protocol-rip/13788-3.html

Gupta. A. (2021). ¿Qué son MTTR, MTBF, MTTF y MTTA? Motadata. https://www.motadata.com/es/blog/incident-management-metrics

IBM. (s.f.). ¿Qué es una prueba de “software”? https://www.ibm.com/ar-es/topics/software-testing

Icot. (2021). Infraestructura IT https://www.icot.es/infraestructura-it/

Créditos

Nombre	Cargo	Centro de Formación y Regional
Milady Tatiana Villamil Castellanos	Responsable del Ecosistema	Dirección General
Olga Constanza Bermúdez Jaimes	Responsable de Línea de Producción	Centro de Servicios de Salud - Regional Antioquia
José Luis Bastidas Pérez	Experto Temático	Centro de Teleinformática y Producción Industrial - Regional Cauca
Ana Catalina Córdoba Sus	Evaluadora Instruccional	Centro de Servicios de Salud - Regional Antioquia
Blanca Flor Tinoco Torres	Diseñador de Contenidos Digitales	Centro de Servicios de Salud - Regional Antioquia
Luis Jesús Pérez Madariaga	Desarrollador Fullstack	Centro de Servicios de Salud - Regional Antioquia
Edgar Mauricio Cortés García	Actividad Didáctica	Centro de Servicios de Salud - Regional Antioquia
Laura Gisselle Murcia Pardo	Animador y Productor Multimedia	Centro de Servicios de Salud - Regional Antioquia
Andrés Felipe Guevara Ariza	Locución	Centro de Servicios de Salud - Regional Antioquia
Luis Gabriel Urueta Álvarez	Validador de Recursos Educativos Digitales	Centro de Servicios de Salud - Regional Antioquia
Jaime Hernán Tejada Llano	Validador de Recursos Educativos Digitales	Centro de Servicios de Salud - Regional Antioquia
Margarita Marcela Medrano Gómez	Evaluador para Contenidos Inclusivos y Accesibles	Centro de Servicios de Salud - Regional Antioquia

Nombre	Cargo	Centro de Formación y Regional
Daniel Ricardo Mutis Gómez	Evaluador para Contenidos Inclusivos y Accesibles	Centro de Servicios de Salud - Regional Antioquia