2. INFRAESTRUCTURA DE REDES, SERVICIOS Y SEGURIDAD

Autor: Ing. Fernando Martínez Llamosas

2.1 INTRODUCCIÓN

Las redes de telecomunicaciones son aquellas que permiten el intercambio de información (uni- o bidireccionalmente) entre distintos dispositivos interconectados entre sí mediante la utilización de técnicas y tecnologías comunes a ambos equipos (protocolos de comunicación).

Además de las redes de datos de las cuales nos ocuparemos aquí, (con foco en las tecnologías principales que hacen posible la red internet), podemos señalar a la red de telefonía, tanto celular como fija, como casos de redes de comunicaciones en un principio orientadas a la transmisión de la voz, como así también a la red de radiodifusión (radio y tv) cuyos orígenes técnicos tienen cerca de un siglo y medio de historia.

De los ejemplos anteriores observamos que aquellas redes estaban orientadas a la intercomunicación de *un tipo* de dato en particular: voz (o audio en general), luego audiovisual. Sin embargo, actualmente las redes intercambian no solo estos mismos tipos de datos sino además una multiplicidad de otros que, en términos generales, son un flujo de datos digitales codificados, es por esto que a estas redes se las denomina genéricamente **redes de datos**.

2.2 CLASIFICACIONES DE LAS REDES DE DATOS

2.2.1 Según su extensión

Una primera clasificación habitual y útil de las redes de datos es según su extensión espacial, donde encontraremos las redes de área local (LAN) y las redes de área extendida (WAN). Como podemos inferir de sus nombres, las LAN son aquellas redes que interconectan dispositivos distribuidos en un área geográfica relativamente más próxima a aquellos que se vinculan mediante una WAN.

Ejemplos de LAN pueden ser una red hogareña que interconecta los diversos dispositivos electrónicos del hogar, la red de un edificio o conjunto de oficinas donde se interconectan diversos puestos de trabajo y equipos servidores, una escuela o campus, una red en un edificio fabril que interconecte maquinaria automatizada con sus equipos de control o monitoreo, o incluso una red que interconecte un conjunto de edificios dentro de una ciudad no muy extensa podría considerarse una LAN (o una variante un poco más extensa de esta denominada MAN: red de área metropolitana).

Por otro lado, una WAN es aquella red en que se vinculan puntos más remotos, siendo estos puntos interconectados no ya dispositivos de uso específico como en el caso de una LAN, sino puntos de interconexión entre redes LAN distantes entre sí,

proveyendo interconexión por ejemplo de distintas ciudades y países, donde las LAN contenidas pueden comunicarse con dispositivos geográficamente más distantes haciendo uso de las WAN que las vinculan entre sí. El caso paradigmático de WAN es la propia Internet que es la red de datos más extendida del planeta.

2.2.2 Según su dominio administrativo

De la clasificación anterior cuyo fundamento es de orden espacial habitualmente se corresponde con el hecho de que una LAN suele tener un dominio administrativo único dependiente de la organización o empresa interconectada, mientras que una WAN, por sus propios objetivos vinculares, implica la coordinación de las diversas instituciones administradoras de las múltiples infraestructuras tecnológicas que proporcionan la interconexión de redes. Es por esto que encontramos diversos organismos, en algunos casos consorcios de instituciones públicas y/o privadas, y en otros de orden estatal, dedicados a la organización, administración y gestión de distintos aspectos implicados en el funcionamiento de Internet: ejemplos son la administración y delegación del sistema de nombres de dominios (DNS) y administración y asignación de direccionamiento IP y sistemas autónomos (en nuestra región NIC.ar y LACNIC son las organizaciones que cumplen estos roles).

Existen además diversos consorcios y agrupaciones de diverso carácter de instituciones públicas y privadas del sector tecnológico que tienen como objetivo la coordinación en materia de desarrollo ya que puede entenderse con facilidad que la interoperabilidad tecnológica no centralizada y estandarizada es un punto clave de la industria de las comunicaciones globales.

2.2.3 Según su arquitectura

Se denomina arquitectura de red al conjunto de especificaciones de los componentes físicos, de su funcionamiento y configuración, sus principios y procesos operativos, y a los protocolos de comunicación utilizados para el intercambio de datos de una red.

Desde los comienzos de las redes de computadoras se diseñaron e implementaron una multiplicidad de arquitecturas, cada una con una orientación y objetivos particulares. Una de estas arquitecturas fue imponiéndose con el tiempo convirtiéndose hace más de 30 años en un estándar de facto, estamos hablando de la arquitectura de red basada en el modelo TCP/IP. Es la arquitectura que utiliza la red internet y la que encontramos implementada en prácticamente cualquier LAN en funcionamiento hoy en día, por esta razón es que es el modelo en cuyas características nos concentramos en el presente documento.

2.3 MODELO TCP/IP

El modelo de red TCP/IP es un conjunto de protocolos de comunicación para la creación de redes de datos, una característica fundamental de dicho modelo es su organización en un sistema de capas.

2.3.1 Modelo de capas TCP/IP

Capa de aplicación	Capa lógica
Capa de transporte (TCP)	
Capa de internet (IP)	
Capa de acceso a la red (física+enlace)	Capa física

Tabla 2.1 – Modelo de cpas TCP/IP

2.3.1.1 Capa física

La capa de acceso a la red del modelo, que constituye la capa física, es aquella que establece las características que han de cumplir las implementaciones tecnológicas utilizadas para enlazar equipos de red a un *nivel electrónico*, vinculando equipamiento mediante algún tipo de medio (por ejemplo: cables de cobre, cables de fibra óptica, radioenlaces), cabe aclarar que el modelo es aplicable independientemente de cuál sea la solución física-electrónica de vinculación siempre y cuando esta cumpla con los requerimientos del estándar.

Actualmente encontramos un abanico de opciones que posibilitan la interconexión de equipos a nivel de capa física del modelo TCP/IP, algunas de estas responden a normalizaciones y estándares definidos por entidades destinadas a estas tareas (por ejemplo, la IEEE) y otras de estas opciones son propietarias de empresas tecnológicas con equipos de I+D en busca de nuevas formas de mejorar las redes en esta capa. En muchas áreas del desarrollo científico-técnico, y en la electrónica y en las comunicaciones ocurre el fenómeno de que son instituciones privadas, aunque en general también con vínculos colaborativos con instituciones de investigación teórico-técnica como universidades, las que están a la vanguardia del desarrollo de nuevas tecnologías, que luego en su implementación y uso, y de acuerdo a su capacidad de dar respuesta satisfactoria a las diversas necesidades de conectividad terminan

imponiéndose como estándar de facto de la industria y muchas veces siendo recogidas y ajustadas en forma de estándares homologados.

Algunas de las soluciones más comunas actualmente en uso de tecnologías de capa de acceso a la red son:

2.3.1.1.1 Soluciones cableadas

- Ethernet (estandarizado como IEEE 802.3 y sus variantes)
    - Puede usar medios como cables de cobre (cable UTP) típicamente estos están acotados a distancia de un máximo de 100m y el 1 gbps de capacidad máxima.
    - Fibra óptica. Esta última destinada a vincular puntos de más distantes entre sí y que típicamente cumplen la función de vinculaciones troncales concentradoras de tráfico de múltiples usuarios.
    - También se utiliza esta solución de acceso a la red con FO para lo que se conoce FTTx (Fiber to the x : es decir llegar con fibra a algún tipo de usuario final, hogareño, empresarial, etc.) (LAN / MAN)
    - Su ámbito geográfico es siempre el de LAN en caso de la utilización de cables de cobre, y mediante fibra podría llegar cumplir con las condiciones para establecer un vínculo categoría WAN.
- DSL (típicamente en su versión asimétrica: ADSL)
    - Su medio habitual es el par de cobre que históricamente se utilizaba como acceso de telefonía fija. Actualmente se utiliza de manera heredada de una infraestructura existente y funcional pero no se espera un crecimiento de esta a futuro dadas sus limitaciones.
- MPLS
    - Es una tecnología comúnmente utilizada para el armado de WANs, clásicamente interconectando tendidos de FO.

2.3.1.1.2 Soluciones inalámbricas

- WIFI (estandarizado como IEEE 802.11 y sus variantes)
    - Su medio es el espectro radioeléctrico, transmitiendo ondas electromagnéticas moduladas, por eso por eso entra en la categoría de enlaces wireless (sin-cables en inglés)
    - Se suele utilizar para la creación de redes del tipo LAN, aunque hay casos en que se utilizan enlaces radioeléctricos para vincular puntos distantes que calificarían como una WAN. En la práctica estos vínculos suelen usar variantes propietarias del estándar WIFI que les agregan sus propias mejoras de industria o directamente soluciones propietarias de cierto fabricante no estandarizadas.

En resumen, estas soluciones tecnológicas (que es una lista de lo más habitualmente implementado en la actualidad, pero no es exhaustiva) son las que típicamente encontramos como modo de *conectarse físicamente* a una red, aunque la denominación de *físico* aquí pueda ser un poco contraintuitiva en el caso de las redes *wireless*. Estas distintas tecnologías de acceso físico pueden interconectarse sin necesidad de "subir" a la capa de lógica formando desde el punto de vista de los equipos que se están comunicando una única red física. Estas técnicas de interconexión entre distintas tecnologías de acceso a la red se denominan ***bridging***.

En los casos más típicos mencionados de soluciones de capa de enlace para LAN ethernet y WIFI encontraremos dispositivos *concentradores* que cumplen la función de vincular los nodos pertenecientes a esa misma red física (formando lo que se denomina un *dominio de broadcast*), el concepto importante aquí es que los nodos pertenecientes a un mismo dominio de broadcast podrán tener comunicación directa de capa física sin necesidad de que intercedan equipos intercomunicadores ubicados en el modelo TCP/IP en la capa superior (capa IP) en la jerga también se denomina a esto un ***segmento de red.*** Estos equipos que intercomunican distintos segmentos de red se denominan enrutadores o ***routers*** que funcionan en el primer nivel de la capa lógica interconectando distintos segmentos de una LAN, a una LAN con una WAN o a distintas WANs.

2.3.1.1.3 Seguridad en la capa física

A modo de introducir las primeras nociones de seguridad de redes podemos señalar que si bien existen técnicas de control acceso en el tráfico dentro de un segmento de red, en el nivel de capa de enlace, no es habitual su uso en la práctica (por su rigidez y complejidades en la administración cuando una red es de tamaño medio o grande) por lo que podemos inferir que la comunicación entre nodos de un mismo segmento de red es directa desde el punto de vista de la red y carente de controles, quedando bajo la responsabilidad de los usuarios de los nodos el uso que hacen de los datos que aportan y toman de la red. Este concepto constituye lo que en la esfera de seguridad de redes de datos denominamos **dominio de confianza**

2.3.1.1.4 Redes cableadas

De esto podemos deducir que para el caso de las redes cableadas el control sobre la conexión *física* a una red de esta capa está determinada en la práctica a la capacidad de acceder físicamente a un punto de conexión a la red (**switch** o puesto de red habilitado) (sin control por *access control list ACL a nivel concentrador*, que no son de uso generalizado en la práctica por imprácticos como fue indicado en párrafos anteriores).

Hay que señalar que existen soluciones técnicas orientadas a mitigar esta subordinación total al acceso físico de las instalaciones de red en lo que respecta a seguridad. En este sentido existen por ejemplo los protocolos IEEE 802.1X o los PPP y sus variantes, que en términos generales poseen mecanismos de autenticación a nivel de capa de enlace de quien trata de unirse al segmento de red y hacer uso de la red de datos. El segundo es ampliamente usado por los ISP para autenticar y proveer los parámetros de red necesarios para el acceso a sus usuarios. Sin embargo, desde el punto de vista estricto de seguridad de redes, no poseer las credenciales necesarias para la obtención de parámetros de configuración mitiga riesgos y dificulta un posible intento de uso malicioso de la red, pero el mero acceso físico a una red cableada sigue implicando cierto grado de compromiso de esta.

2.3.1.1.5 Redes inalámbricas

El acceso a las redes inalámbricas, como en el caso de las cableadas, está primeramente condicionada por la posibilidad de acceso al medio que esta utiliza para la transmisión de datos, pero, siendo como vimos que este medio es en este caso de las redes inalámbricas el espectro radioeléctrico, el cual no tiene (en principio) limitantes de orden espacial más que la sola distancia al concentrador (la distancia y los obstáculos físicos generan atenuación de la señal modulada hasta hacerla indistinguible del ruido electromagnético y es en este punto en que alcanzamos el límite de cobertura del nodo concentrador inalámbrico).

Es por esto que cualquier dispositivo con acceso al área de cobertura de un nodo puede escuchar (en la jerga *sniffear)* el tráfico entre clientes y concentrador (también denominado en las tecnologías wireless **punto de acceso**: *Access Point - **AP***). La manera de proporcionar seguridad a los datos circulantes es mediante el cifrado de dicha transmisión entre un determinado usuario y el AP, los mecanismos que ponen en práctica dicho cifrado estarán definidos en el protocolo particular utilizado. De la misma manera existen mecanismos de autenticación estandarizados que utilizan los AP para validar el acceso a un usuario como parte de la red inalámbrica, ejemplos prácticos de estos son típicamente los denominados WEP, WPA, WPA2 y dentro de estas variantes según los algoritmos criptográficos que utilicen.

Como en el caso de las redes cableadas, desde el punto de vista estrictamente de la seguridad de redes, la mera presencia de un dispositivo capaz de analizar el espectro radioeléctrico dentro del área de cobertura de una red inalámbrica dada ya implica un grado de compromiso de la misma, y por tanto en términos generales podemos aplicar una regla de pulgar donde las redes inalámbricas son menos seguras que una red cableada.

2.3.1.2 Capa lógica

Esta capa está compuesta en el modelo TCP/IP por tres capas: IP, TCP y Aplicación. Todas estas capas son en términos prácticos es un conjunto de soluciones de software con objetivos específicos. Mediante las capas IP y TCP (que clásicamente están implementadas en el sistema operativo del dispositivo y son transparentes a los usuarios una vez configurados) se proporciona una manera **uniforme** de que las aplicaciones hagan uso de la red sin tener que "conocer" la solución específica implementada en la capa física descrita anteriormente. Es haciendo uso de la capa IP que nos es posible interconectar distintos segmentos de red separados y que sin esta capa no podrían vincularse usuarios en uno de los segmentos con usuarios en el otro. Esta interconexión de segmentos de red distintos es el principio del *ruteo* entre redes.

La tarea de rutear entre distintas redes lógicas a nivel IP es llevada a cabo por el dispositivo de capa IP denominado **router de red** constituyéndose este en una denominada **puerta de enlace.**

Notamos entonces que toda la comunicación de un segmento hacia otros segmentos de red exteriores debe necesariamente pasar por los los puntos de enlace a otras redes que este primer segmento posea, así, estos puntos son lugares óptimos para aplicar políticas de seguridad en el control en el flujo de datos desde y hacia el segmento de red y los nodos participantes de este.

2.3.1.2.1 Seguridad en la capa lógica

Si en este punto de interconexión (aunque no siempre es, necesariamente, el mismo equipo de red) se realiza alguna aplicación de políticas restrictivas al tráfico de red entre segmentos (más allá del mero reenvío de los datos entre uno y otro) en función de sus características propias de la capa IP, TCP o de aplicación, estamos ante la técnica básica de seguridad de redes denominada *firewalling* (siendo el software que la realiza un ***firewall***).

Al aplicar un control de accesos entre distintos segmentos de red mediante un firewall estamos separando a ambos segmentos de red en distintos **dominios de confianza** concepto como ya vimos propio del ámbito de la seguridad de redes. Las comunicaciones posibles entre distintos dominios de confianza no son irrestrictas ya que está controlada por un firewall con políticas propias definidas y administradas por la organización que hace uso de las redes.

Si la información utilizada para el control de accesos entre redes está estrictamente restringida a información propia de los segmentos IP o TCP, estamos hablando de un firewall de red. Si el control del tráfico implica la "observación" y

eventual filtrado de la información circulante a nivel de las aplicaciones de usuario que están haciendo uso de la red, el firewall entra en la categoría de firewall de aplicación.

2.3.1.3 Capa de aplicación

La capa de aplicación es la que engloba aquellos protocolos, estándares o no, que hacen uso de la red para proporcionar servicios al usuario de esta (sean personas haciendo uso de aplicaciones de software (ej: un navegador web) u otros sistemas (ej: un software de backup automático por red). Como es propio del modelo de capas aplicado en TCP/IP los protocolos de la capa de aplicación comunican elementos pertenecientes a la misma capa de aplicación, típicamente siguiendo un esquema cliente-servidor, siendo tanto el software cliente, como el software servidor, ambos, parte de la capa de aplicación. A nivel de flujos de datos, la comunicación es siempre bidireccional (aunque puede variar las proporciones en un sentido y otro), la categorización entre cliente y servidor es más conceptual que técnica, siendo el servidor quien proporciona un servicio y el cliente quién hace uso de este. En ciertos casos es más fácil identificar estos roles: por ejemplo en un servicio de alojamiento de páginas web, el software web que contiene las páginas es el servidor, y el navegador web donde se visualizan estas es el cliente, que hace uso de las páginas alojadas en el servidor, el flujo principal de datos resulta el intuitivo: del servidor al cliente.
En otros casos estos roles son menos evidentes ya que el flujo principal de datos no es desde el servidor al cliente, ejemplo de esto podría ser un servidor de videoconferencias, donde cada usuario utiliza su software cliente para enviar sus datos de audio y video al servidor central, y este a su vez replica esta información enviándola a los demás participantes, quienes a su vez también están enviando su audio y video en el sentido contrario.

Cabe mencionar que hay una cierta cantidad de software de aplicación destinado a proporcionar servicios necesarios para contar con características avanzadas de la red por ejemplo el servicio de DNS o NTP.

Existe una gran cantidad de protocolos estándares de red pertenecientes a la capa de aplicación, cada uno diseñado con el objetivo de cumplir necesidades particulares, algunos ejemplos comúnmente usados son:

- HTTP (Hypertext Transfer Protocol) o su variante segura HTTPS
- FTP (File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- POP (Post Office Protocol)
- SSH (Secure Shell)

Sin embargo, existe una infinidad de software que hace uso de los servicios proporcionados por las implementaciones del modelo TCP/IP que utiliza la red para comunicarse utilizando un protocolo definido ad-hoc por los desarrolladores del

software en muchos casos estos protocolos son propietarios y su funcionamiento desconocido para quien utiliza las aplicaciones.

2.3.1.3.1 Seguridad en la capa de aplicación

La seguridad en la capa de aplicación es responsabilidad del protocolo de nivel de aplicación, la capacidad de protección (cifrado) de los datos que serán enviados a nivel de aplicación y la existencia de mecanismos de autenticación para establecimiento de una conexión a nivel cliente-servidor es una decisión de diseño de dicho protocolo. En general aquí entra en juego el balance entre la necesidad de proporcionar seguridad a la información circulante y la simplicidad de uso de los protocolos, ya que otra regla del pulgar es que, a mayor seguridad, mayor complejidad.

Ejemplo de esto es el protocolo HTTP, que es un protocolo basado en texto plano sin seguridad, es un protocolo ampliamente utilizado para proporcionar una gran cantidad de servicios. Pero cualquier agente intermediario en el proceso de comunicación por red utilizando este protocolo podría “mirar” el contenido y leerlo sin problemas (el usuario siempre podría cifrar los datos a enviar, pero esto no es un servicio del protocolo HTTP en sí).

El protocolo HTTPS es una variante de HTTP, orientado a proporcionar el mismo tipo de servicios o a ser usado en los mismos contextos pero que incorpora, como parte del mismo protocolo, mecanismos de autenticación de las partes a comunicarse y cifrado de los datos a ser transmitidos mediante un esquema de claves públicas y privadas.

2.4 SISTEMAS COLABORATIVOS

2.4.1 Introducción

Una red de datos puede interconectar sistemas informáticos con una multiplicidad de objetivos, aunque esencialmente estos implicarán siempre, y en alguna proporción particular determinada por el caso de uso, tanto el **intercambio de datos** como la **distribución de tareas** entre dos o más de los sistemas participantes de la red, en el caso de que estos sistemas interconectan software que funciona de manera más bien autónoma respecto de la intervención de los usuarios / operarios humanos, estaremos frente a la categoría de *sistemas de control* o de *sistemas distribuidos*, usos típicos de las redes de datos en el ámbito industrial.

En el caso de que la red de datos funcione también como medio para el intercambio de información, organización y distribución del trabajo y sus tareas, pero ya no de sistemas autónomos sino de personas que, mediante el uso de diversos

softwares orientados a apoyar el abordaje de tareas específicas de forma grupal, lleven adelante sus proyectos conjuntos y las tareas que los constituyen, estaremos en presencia de lo que se categoriza como un *sistema colaborativo*, también por extensión se denomina así, y también *groupware*, a cada uno de los softwares utilizados que en su conjunto constituyen este sistema.

Esta última definición viene a formalizar un uso que desde sus inicios tuvieron las redes informáticas de computadoras y que puede ser tan habitual y cotidiano en nuestros días que se pueda pasar por alto su pertenencia a esta categoría, tal es el caso por ejemplo del propio software para comunicación mediante **correo electrónico** método para el intercambio de información por antonomasia que hace uso de las redes de datos.

2.4.2 Categorías

Todo software colaborativo hará uso de la red de datos e involucrará a dos o más personas, pero a partir de aquí y según las características de las tareas o servicios que brinde podremos ubicarlo de distintas categorías:

- Comunicación asincrónica
  - Correo electrónico
  - Foros de discusión en línea
  - Redes sociales
- Comunicación sincrónica
  - Chats
  - Sistemas de videoconferencia
- Generación de contenido
  - Sistemas Wiki
  - Editores de texto con capacidad de edición grupal
  - Sistemas de almacenamiento compartido
- Coordinación de trabajo
  - Calendarios compartidos
  - Gestión de proyectos (task managers)
  - Flujo de proyectos (workflow)

Con excepción del software de gestión de proyectos y de workflow, que pueden estar más restringidos a ambientes donde el grado de apoyo en sistemas informáticos esté más desarrollado, el resto resultará al lector de un uso cotidiano y habitual, ya sea en el ambiente laboral, como en el educativo o como herramientas para proyectos personales con otras en colaboración con personas.

2.4.2.1 SaaS - Software como servicio

Más allá de los anteriores ejemplos puntualizados para las distintas categorías, que representan los casos clásicos de trabajo en red, la tendencia actual es que los nuevos sistemas que deben dar servicio o apoyo a las tareas de negocio sean pensados directamente como sistemas colaborativos, con la posibilidad de ser operados por múltiples actores que no deban estar geolocalizados en un único lugar de trabajo.

Esta tendencia ha hecho por un lado que los softwares utilizados estén cada vez más basados en el esquema de red cliente - servidor explicado anteriormente, y la tendencia actual es a tratar de que estos sistemas estén basados en tecnología de desarrollo web, es decir, que el cliente del sistema sea directamente accesible desde un navegador web, o de una aplicación de celular hecha a medida.

A lo anterior se suma la existencia de infraestructura de de redes de datos ya habitual en los lugares de trabajo, más el acceso ubicuo y de alta calidad a la red internet. Esto ha generado una tendencia cada vez mayor por parte de las empresas a tener interfaces a muchos de sus sistemas accesibles desde cualquier lugar con acceso a internet (involucrando las medidas de seguridad informática adecuadas), beneficiándose de la autogestión de sus clientes, o de la posibilidad de trabajo remoto de quienes desarrollan labores que pueden beneficiarse de estos sistemas.

Además, con esta masividad del acceso a internet de los usuarios departamentos enteros de empresas o instituciones que implican atención personalizada o telefónica han derivado en la atención en línea, como pueden ser el departamento de ventas, la asistencia al cliente postventa, muchas veces con estas tareas más o menos automatizadas y gestionadas mediante software colaborativo.

Esto implicó dos necesidades de las empresas e instituciones a de dedicar recursos de manera novedosa, por un lado, a poseer infraestructura de datacenters adecuados para brindar sus servicios (a usuarios internos: trabajadores, o externos: clientes), y por otro para la adquisición o el desarrollo de los software y sistemas que cumplieran con sus necesidades particulares de negocio.

Actualmente muchas empresas optan directamente por externalizar tanto el desarrollo del software como la infraestructura requerida para su funcionamiento, adquiriendo estos como un servicio brindado por otras compañías cuyo núcleo de negocio es desarrollar estos sistemas de gestión, vender el servicio de customización y de puesta y mantenimiento en línea de los servicios en su propia infraestructura. A este esquema se lo denomina **SaaS** *Software as a Service* que posee las ventajas reducción de costos a partir de la externalización para las empresas usuarias al ya no tener que poseer infraestructura, know how técnico, y desarrolladores propios. Y como es lógico las empresas prestadoras de estos servicios de software se benefician de la posibilidad de vender un servicio una multiplicidad de veces a empresas con necesidades similares.

Ejemplos clásicos de estos servicios pueden ser

- Portales de ventas
- CRM
- Portales de atención al cliente y help desk
- Gestión de cobros
- Email marketing y comunicación con clientes

2.4.2.2 Web Services y APIs

Una manera habitual de que tienen las empresas proveedoras de SaaS de proporcionar sus servicios es mediante el uso de los denominados Web Services a través del uso de APIs *Application Programming Interface* los cuales permiten hacer uso de funcionalidades genéricas para que empresas que las requieran dispongan de estas desde sus propios software mediante el uso de la red internet al proporcionar una interface de comunicaciones y un **protocolo de integración** para utilizar dicha interface por otro software que lo requiera.

Para ejemplificar mediante un caso típico puede pensarse en un software de facturación implementado localmente en la PC del cajero o en un servidor de la red local de la empresa, este podría hacer uso de un *Web Service* y su *API* provista por una empresa de cobros en línea para efectuar un cobro por tarjeta de crédito (o cualquier otro medio de ese tipo), y puede hacer uso también de otra funcionalidad de la misma API, o bien de otro *Web Service* de otra empresa de servicios online para realizar la facturación online ante la entidad AFIP.

2.4.2.3 Cloud computing

Un consecuencia técnico-empresarial particularmente importante derivada como de la masificación del acceso a internet en las últimas décadas y el surgimiento del modelo de provisión de servicios SaaS es el servicio de infraestructura informática en la nube *Cloud computing,* el cual permite la disponer de recursos computacionales: procesadores para cómputo, almacenamiento, conectividad de red, etc. donde desplegar el software utilitario a ser utilizado por la empresa u organización, accediendo a estos sin necesidad de la adquisición de hardware y el despliegue de una red compleja y de alta disponibilidad. De la misma manera si la empresa requiere proporcionar SaaS o un Web Service particular como parte de sus servicios puede desplegar estos en este tipo de infraestructura que se orientan a beneficiarse de una economía de escala en el reuso de sus recursos de hardware, software específico, y conocimientos técnicos particulares.

En el mercado actual los proveedores de cloud computing más comúnmente utilizados son

- AWS Amazon Web Services
- Google Cloud
- Microsoft Azure

Los cuales además proveen una amplia gama de SaaS.