COMUNICACIONES UNIFICADAS

Ing. José Joskowicz
josej@fing.edu.uy
Instituto de Ingeniería Eléctrica, Facultad de Ingeniería
Universidad de la República
Montevideo, URUGUAY

Agosto 2009
Versión 8

Tabla de Contenido

1 Introducción

Las Comunicaciones Unificadas (UC, por sus siglas en Inglés) pueden definirse genéricamente como una plataforma de aplicaciones que mejoran la productividad individual, grupal y organizacional permitiendo y facilitando la administración y el control integrado de diversos canales de comunicación, redes, sistemas y aplicaciones de negocios [1].

Los componentes de las Comunicaciones Unificadas incluyen aplicaciones de presencia, mensajería instantánea, telefonía IP, conferencia de audio, conferencia web o colaboración de datos, mensajería unificada, movilidad y/o video conferencia, todo accesible a través de una única interfaz de cliente, o embebida dentro de una interfaz de aplicación.

Según la Empresa consultora Frost & Sullivan, en 2008 algunos cientos de empresas tenían ya implementaciones de comunicaciones unificadas, cada una con algunas centenas de usuarios. Sin embargo, se prevé un rápido crecimiento, como se muestra en la Figura 1.1 [2].

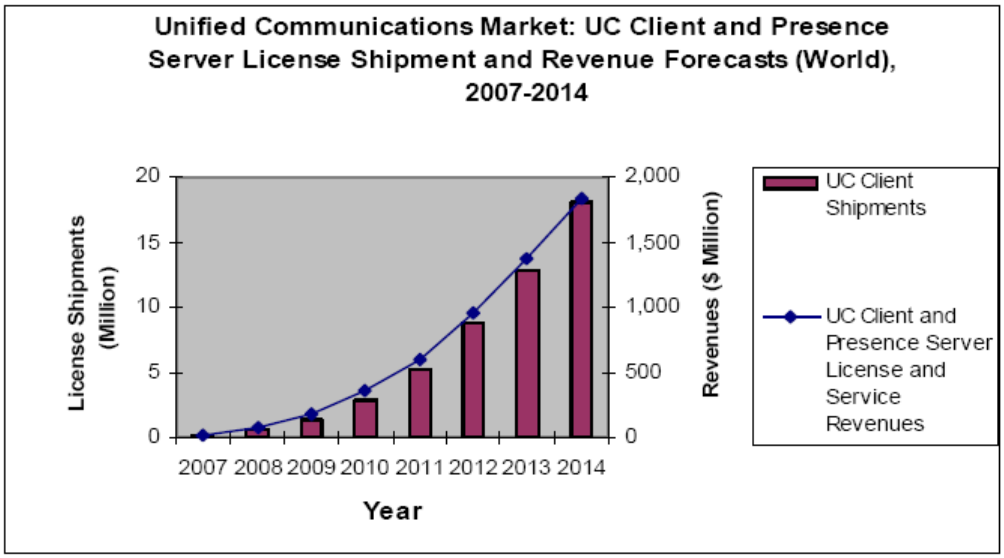

Figura 1.1

Hasta el año 2006 solo unas pocas empresas proveedoras de tecnologías disponían de soluciones completas de “comunicaciones unificadas”. Sin embargo, entre el 2007 y el 2008, la mayoría de las empresas proveedoras de tecnología incorporaron las comunicaciones unificadas a sus líneas de productos. El mercado ha comenzado, por otra parte, a generar interés y demanda sobre este tipo de aplicaciones. Se espera que este tipo de tecnologías sea de rápido desarrollo y adopción en los próximos años, estando ya “embebida” en diversas plataformas de telecomunicaciones y productos de software. En una encuesta realizada en 2009, el 22% de las empresas respondieron que ya han implementado tecnologías

de comunicaciones unificadas, mientras que el 39% tienen planes de implementar estas tecnologías dentro de los próximos 12 o 24 meses [3]. Según esta misma encuesta, los principales motivadores consisten en integrar los diversos mecanismos de comunicación, mejorar la eficiencia, el servicio a los clientes y permitir la movilidad de los empleados.

Las comunicaciones unificadas son posibles gracias a la integración de diversas tecnologías, las que se han dado en forma gradual desde hace ya más de una década. La primera etapa en la integración se ha dado en la transmisión a distancia, la que está directamente relacionada con gastos mensuales, ya sean fijos, o por utilización. Bajar estos costos, incide directamente en los costos operativos de las Empresas. Las primeras aplicaciones de integración se correspondieron con el tráfico de canales de voz sobre enlaces de datos a distancia (WAN). En paralelo se desarrollaron tecnologías que permiten la sincronización, en el escritorio, de ciertos eventos telefónicos con las aplicaciones informáticas. Inicialmente este tipo de tecnologías se desarrollaron para los sectores de centros de llamadas (Call Centers), y fueron conocidas como “CTI” (Computer Telephony Integration). La VoIP fue ganando terreno, llevando su incorporación también a las redes de área locales (LAN), sustituyendo en algunos casos los teléfonos analógicos y digitales por teléfonos IP, ya sean de hardware o de software. Finalmente, estas tecnologías se están integrando a las aplicaciones de escritorio corporativas, incluyendo el correo electrónico, la mensajería instantánea, procesadores de texto e incluso sistemas del tipo CRM, ERP y aplicaciones de gestión empresarial.

A continuación se detallarán diversos aspectos relacionados a las comunicaciones unificadas, explicando la tecnología utilizada, los beneficios obtenidos y los nuevos desafíos que se plantean respecto a la seguridad de la información al utilizar estas tecnologías. Finalmente se presentan algunos aspectos relativos a la gestión de proyectos de implementación de comunicaciones unificadas.

2 Convergencia en la WAN

La integración de las redes de voz [4] y las redes de datos [5] en la WAN (es decir, en los enlaces a distancia entre varios puntos de la misma empresa) es un concepto que tiene ya varios años, y el principal móvil ha sido históricamente el ahorro económico.

En la actualidad la gran mayoría de las empresas con varias sucursales disponen de enlaces de datos, utilizando diversas tecnologías. Estos enlaces, generalmente tienen un costo fijo mensual, independientemente de su utilización. Es por tanto razonable tratar de incluir en estos enlaces la mayor cantidad de información posible, incluyendo conversaciones de voz.

Diversas tecnologías han sido desarrolladas para permitir el tráfico de voz sobre enlaces WAN. A continuación se mencionan las más conocidas.

2.1 Routers con "placas" de voz

Los equipos ruteadores ("routers") fueron diseñados originalmente para interconectar dos o varias redes de área local (LAN) a través de enlaces de datos "a distancia" (WAN). Generalmente tienen incorporados algoritmos de "ruteo" de varios protocolos (incluido casi siempre el protocolo IP), y soportan una gran variedad de protocolos de WAN (Frame Relay, enlaces punto a punto, etc.)

Muchos de estos equipos soportan actualmente "placas de voz", con señalización FXS, FXO, E&M, E1, etc. como se muestra en la Figura 2.1.

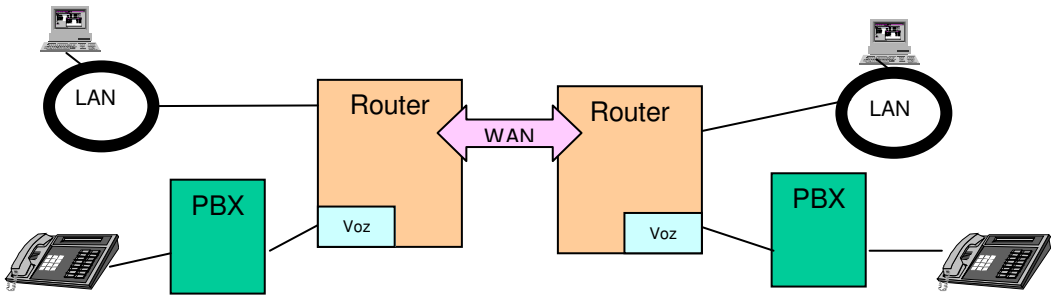

Figura 2.1

Interfaces de Voz:

FXS
Esta interfaz "simula" una línea urbana, a la que se puede conectar un teléfono analógico. También es posible conectar un puerto de línea urbana de una PBX.

FXO
Esta interfaz "simula" un teléfono, a la que se puede conectar una línea urbana. También es posible conectar un puerto de interno de una PBX.

E&M
Esta interfaz se conecta a PBX, con señalización E&M

T1 / E1
Esta interfaz provee canales telefónicos a través enlaces digitales T1 (24 canales) o E1 (30 canales), típicamente con señalización CAS (Channel Associated Signaling) o ISDN PRI.

En cualquiera de los casos, la voz es empaquetada y enviada al enlace WAN en conjunto con los datos. El tipo de enlace WAN puede ser IP, Frame Relay, ATM, etc. La calidad de la voz depende del protocolo del enlace y de varios factores, como ser, algoritmos de compresión, tecnología utilizada, ancho de banda, etc.

2.2 PBX con "Gateways" IP

Muchas PBX soportan actualmente la incorporación de Gateways IP. Estos Gateways conectan la PBX directamente a la LAN, e implementan la conversión de la voz a paquetes IP y viceversa (ver Figura 2.2).

Los paquetes de voz que salen del Gateway son enviados por el Router, a través de la WAN, hasta el Gateway de la otra PBX.

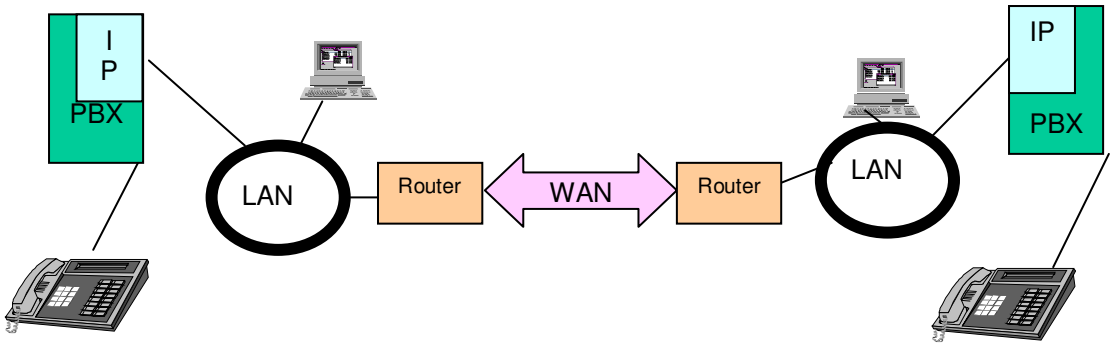

Figura 2.2

Es de hacer notar que en estas configuraciones se requiere que el Gateway marque los paquetes de voz como "prioritarios" y que el router respete ésta priorización. Esto es muy importante debido a la diferencia de velocidades de transmisión que típicamente existen entre la LAN y la WAN. Mientras que en la LAN es usual disponer de velocidades de 100 Mb/s, en la WAN, ésta velocidad no sobrepasa generalmente 1 Mb/s y muchas veces se dispone velocidades menores a 0.1 Mb/s (por ejemplo 64 kb/s). Esto indica una relación de velocidades de 1 a 100 o a 1000.
Por ésta razón, los routers implementan colas de datos: Los paquetes recibidos de la LAN son encolados para ser enviados a la WAN. Dado que la LAN tiene una velocidad mucho mayor que la WAN, las ráfagas de paquetes recibidos desde la LAN pueden tener que esperar tiempos "largos" hasta ser enviados a la WAN. Esto perjudica especialmente a los paquetes de voz y video, que requieren demoras de punta a punta muy pequeñas.
Para evitar estos problemas, es posible "marcar" los paquetes, tanto a nivel IP como a nivel Ethernet, indicando la prioridad del mismo. Los routers preparados para aplicaciones de voz, soportan varias colas de datos, y los envíos a la WAN se realizan por orden de prioridad.
Los estándares más comunes son DiffServ (para IP) y 802.1p para Ethernet [6].

Por otro lado, cuando la velocidad de acceso a la WAN es pequeña, los tiempos que demoran en ser enviados los paquetes no son despreciables. Por ejemplo, un paquete de 1.500 bytes, transmitido a 32 kbps demora 375 mseg en ser transmitido (1,5x8/32). Los paquetes de voz, aún siendo priorizados, deberán esperar a que pase el paquete de datos, por lo que se introducen demoras muy apreciables en el sistema. Previniendo esto, algunos protocolos de WAN pueden "fragmentar" los paquetes IP grandes, en varios paquetes de WAN más pequeños, de manera que entre cada fragmento del paquete original se puedan insertar paquetes de voz. En el caso de Frame Relay, los mecanismos de fragmentación están normalizados, según la recomendación FRF-12 ("Frame Relay Fragmentation Implementation Agreement")

2.3 "Gateways" IP independientes

Estos equipos se utilizan cuando se dispone de PBX y routers que no soportan la incorporación de Gateways IP. Son equipos independientes, que disponen de las interfaces telefónicas clásicas (FXS, FXO, E&M, etc.) y son capaces de paquetizar la voz sobre IP (ver Figura 2.3).

Es muy importante que estos equipos puedan "marcar" a los paquetes que generan como "prioritarios", ya sea a nivel de IP, Ethernet, o ambos. Es también muy importante que los routers respeten la priorización, según las "marcas" realizadas por los "gateways".

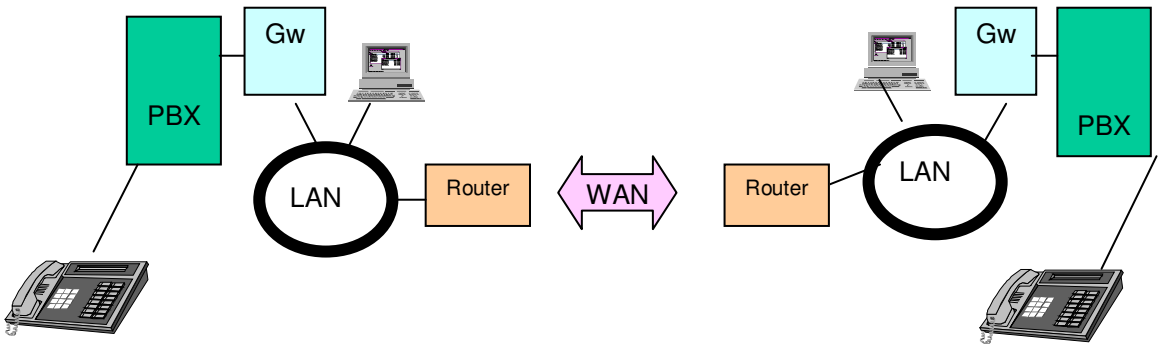

Figura 2.3

3 Convergencia en el Escritorio

La unificación de las redes de voz y datos a nivel del "escritorio" comprende varias tecnologías. La tecnología llamada "CTI" (Computer Telephony Integration) permite vincular la telefonía con las aplicaciones informáticas. Sobre esta tecnología se han desarrollado diversos tipos de aplicaciones. Se destaca su uso en ambientes de Call Center, y más recientemente, como plataforma tecnológica para las denominadas "Comunicaciones Unificadas".

3.1 CTI

La tecnología de CTI (Computer Telephony Integration) fue concebida manteniendo las redes de voz y las de datos separadas, pero permitiendo integrar ambos sistemas. Esto se logra a través de vínculos de datos entre los servidores informáticos y las centrales telefónicas, tal como se esquematiza en la Figura 3.1..

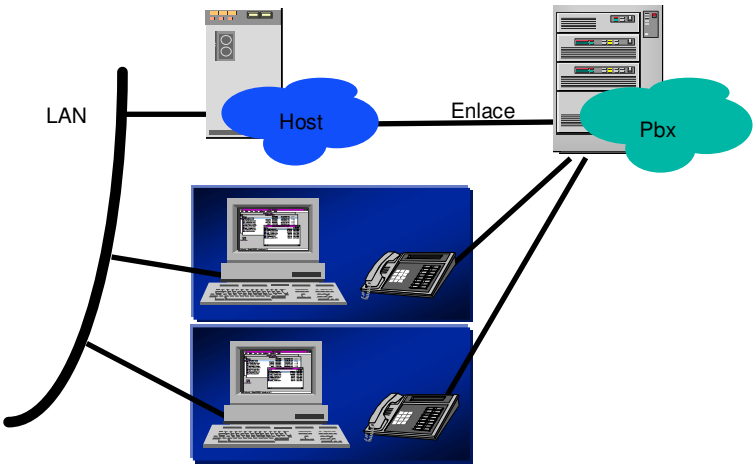

Figura 3.1

Las tecnologías de CTI permiten mantener los teléfonos de escritorio, ya sean TDM (analógicos o digitales) o IP, pero "controlados" desde aplicaciones informáticas. Estas aplicaciones informáticas pueden integrarse con funciones telefónicas, permitiendo realizar "screen popups" cuando llega una llamada, y controlando las funciones de los teléfonos desde el computador.

La tecnología de CTI permite "sincronizar" la recuperación de datos en las aplicaciones de los PCs con el ingreso de cada llamada. Por ejemplo, si se dispone de la facilidad de identificación del abonado llamante, es posible, utilizando funciones de CTI, desplegar en la pantalla del PC los datos del llamante antes de atender la llamada, de manera que se pueda saludar a quien llama por su nombre, o se conozca el historial del llamante sin necesidad de preguntar su identificación.

Las tecnologías de CTI son ampliamente utilizadas, desde hace ya varios años, en ambientes de Call Center, dónde es importante minimizar los tiempos de cada

llamada, y brindarle a las telefonistas la máxima información posible referente al cliente.

Estas tecnologías están teniendo actualmente creciente difusión en ambientes corporativos, asociados a la integración de las aplicaciones de escritorio y sistemas de presencia. Con este tipo de integraciones, el correo electrónico, las herramientas de oficina y la mensajería instantánea se "integran" a la telefonía, permitiendo por un lado actualizar el estado de presencia en función de la actividad telefónica, y por otro, iniciar llamadas desde aplicaciones de escritorio, en forma automática y a través del teléfono habitual.

CTI es conocido también como "RCC", o "Remote Call Control", entiendo por éste concepto a las tecnologías que permiten realizar el control de las llamadas y los teléfonos desde aplicaciones externas.

Las tecnologías de CTI están basadas en arquitecturas del tipo "cliente – servidor". Un "Servidor de Telefonía" se vincula con la PBX mediante un enlace dedicado a tal fin. Originalmente estos enlaces se implementaban sobre comunicaciones seriales (RS-232 por ejemplo). Actualmente se realizan a través de la red IP. En el "Servidor de Telefonía" se instalan programas que dialogan con las PBX, y "publican" servicios para los usuarios de la red de datos. Éstos servicios permiten controlar los dispositivos telefónicos (por ejemplo, los teléfonos) desde aplicaciones informáticas. Existen varios "estándares" de CTI entre los que se destacan:

- TAPI (Telephony API): Es utilizada en ambientes Microsoft. Las bibliotecas necesarias para su uso se distribuyen como parte de los sistemas operativos Windows
- JTAPI (Java Telephony API)
- CSTA (Computer Supported Telecommunications Applications)
- ECMA TR/87
- Protocolos propietarios (como por ejemplo "MLink" de Nortel, "ASAI" de Avaya, etc.)

3.1.1 Microsoft TAPI

Las bibliotecas **TAPI** de Microsoft contienen un conjunto de funciones de telefonía, que pueden ser utilizadas desde aplicaciones desarrolladas en C, C++, .net o cualquier otro lenguaje de programación que pueda llamar a funciones de Microsoft. La arquitectura es del tipo "Cliente-Servidor", como se esquematiza en la Figura 3.2. En el Servidor residen los componentes "Telephony Service" (de Microsoft) y el denominado "Telephony Service Provider" (TSP), que es el responsable de mantener el vínculo con la PBX, implementando el protocolo adecuado (el que puede ser propietario). Los clientes se comunican con el servidor a través de las funciones de TAPI locales.

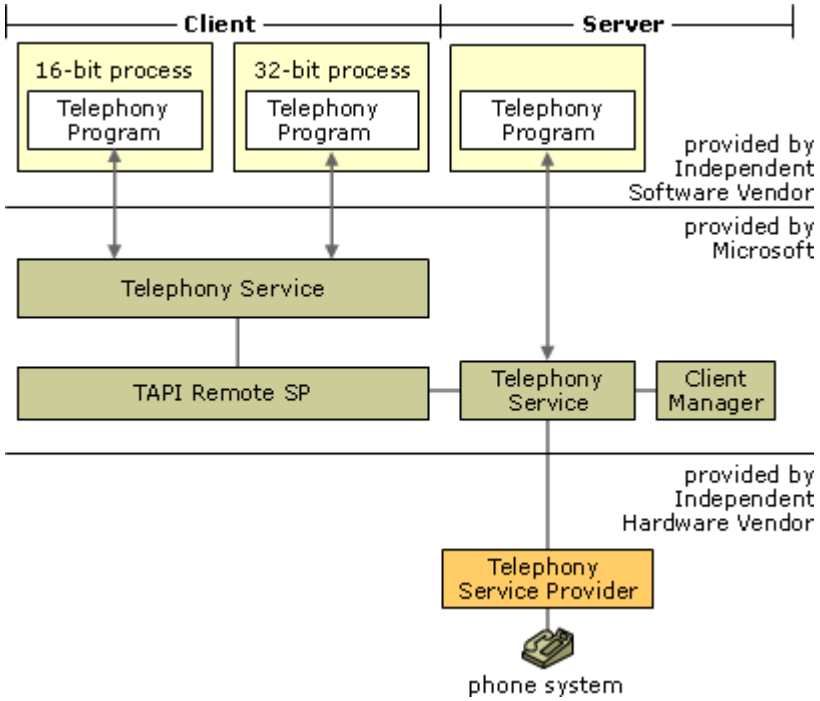

Figura 3.2

3.1.2 JAVA JTAPI

La especificación de JTAPI (Java Telephony API) fue desarrollada en forma conjunta por diferentes empresas, de computación y telecomunicaciones (Sun, Avaya, Nortle, Intel, IBM, entre otras). La primera versión de JTAPI data de 1996, y la más reciente, la versión 1.4, de 2001. El modelo de JTAPI se muestra en la Figura 3.3. JTAPI es una capa por encima del motor de tiempo real de Java (Java Run-Time), y accede remotamente a al servidor de telefonía, donde residen APIs de telefonía (como TAPI). JTAPI dispone de un conjunto completo de funciones y eventos de telefonía, que pueden ser utilizadas desde aplicaciones JAVA.

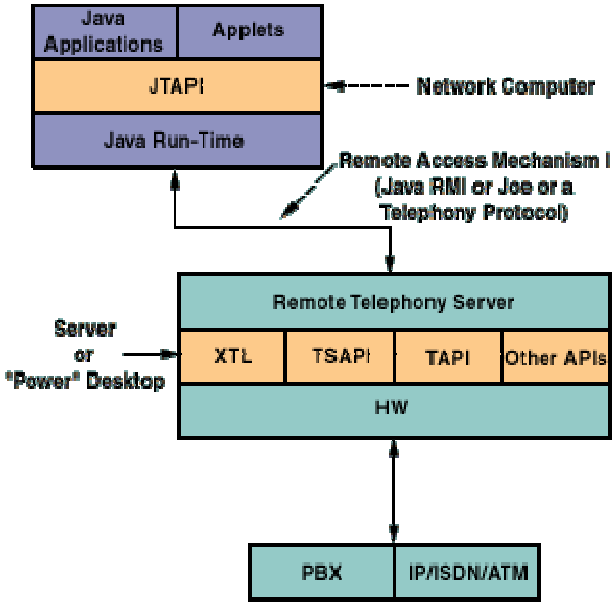

Figura 3.3

3.1.3 CSTA

CSTA (Computer Supported Telecommunications Applications) proporciona una capa de abstracción para las aplicaciones de telecomunicaciones que requieran usar tecnologías de CTI. La primera versión fue publicada en 1992, y es conocida con “Fase I”. La actual “Fase III” fue publicada en 1998, y ha tenido varias actualizaciones posteriores. En 2000 CSTA fue estandarizada por la ISO en las recomendaciones ISO/IEC 18051, ISO/IEC 18052, ISO/IEC 18053 y ISO/IEC 18056.
El modelo de CSTA es similar a los anteriores, conectando el dominio informático con el de la PBX a través de un “Switch Link”, tal como se ilustra en la Figura 3.4. CSTA utiliza ASN.1 ("Abstract Syntax Notation One"), una metodología para representar estructuras de datos desarrollada por la ITU. ASN.1 consiste en un lenguaje declarativo, y ciertas reglas de codificación para traducir el código ASN.1 en un flujo de bytes que se puedan ser fácil y eficientemente transmitidos. Al estar normalizado, se garantiza que la codificación y la decodificación de los mensajes es realizada de la misma manera.

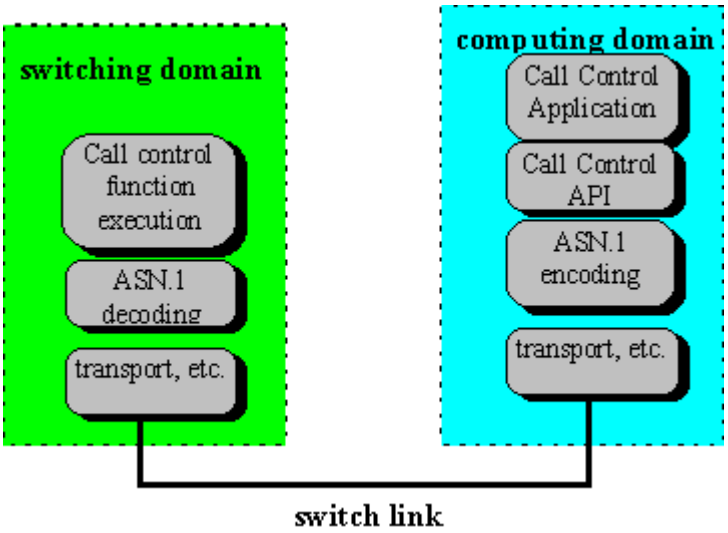

Figura 3.4

CSTA tiene un conjunto completo de funciones, incluyendo:

- 26 funciones de control de llamadas ("Call Control", como "Make Call", Answer call", etc.)
- 6 funciones asociadas a las llamadas ("Call Associated", como "Send User Data", etc.)
- 19 funciones lógicas ("Logical Device features", como "do not disturb", "forwarding", etc.)
- 23 funciones asociadas a los dispositivos físicos ("Physical Device" como escribir en los displays de los teléfonos, etc.)
- 5 funciones de intercambio de capacidades ("Capability Exchange", como "feature discovery", etc.)
- 4 funciones de consultas ("Snapshot features" como consultar las llamadas establecidas en un dispostivo, etc.)
- 3 funciones de monitorización ("Monitor features", como subscribirse a notificaciones de eventos, etc.)
- 17 funciones de voz ("Voice Services", como detección de DTMF, etc.)
- Otras funciones de ruteo, funciones de mantenimiento, administración, etc.

El modelo de llamada entrante en CSTA es el presentado en la Figura 3.5.

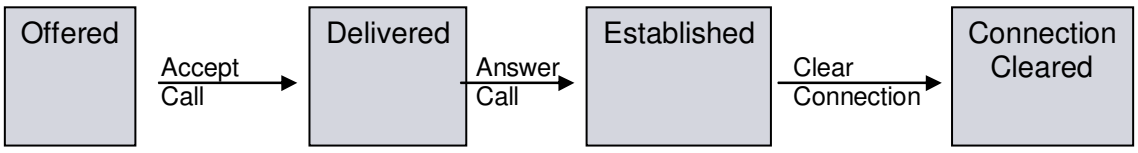

Figura 3.5

El modelo de llamada saliente (por ejemplo “Make Call”) en CSTA es el presentado en la Figura 3.6.

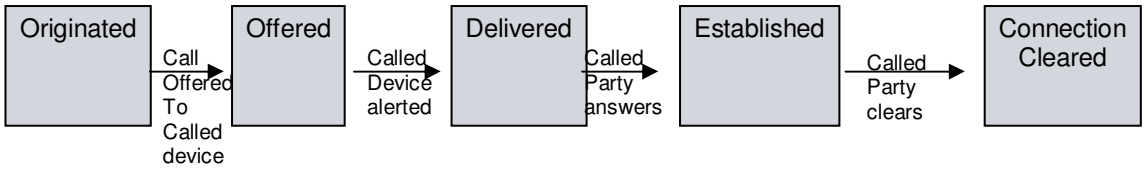

Figura 3.6

Adicionalmente, CSTA soporta el control y notificación de interacciones no telefónicas, como por ejemplo mensajería instantánea, correo electrónico y Chat. Esto permite utilizar un mismo modelo para la atención de contactos multimedia, ya sean de voz, texto, etc.

3.1.4 ECMA TR/87

Entre los estándares, ECMA (European Computer Manufacturer's Association) TR/87 se destaca por estar siendo adoptado por diferentes aplicaciones, entre ellas “Microsoft Office Communicator”. Este protocolo fue estandarizado por la ISO en la recomendación ISO/IEC TR 22767, en agosto de 2005 [7].
Este estándar utiliza el protocolo SIP (ver [6]) y lo adapta para ser utilizado como transporte para notificar los eventos telefónicos de CSTA. Los eventos telefónicos son embebidos, extendiendo el protocolo CSTA, dentro de mensajes con formato SIP. Por ejemplo, un mensaje SIP TR/87 tiene un formato como el siguiente:

```
INFO sip:SignalingISBEL@isbel.com.uy:5060;maddr=192.168.1.175
contact:     <sip:cavallone@isbel.com.uy:1554;maddr=192.168.1.248;transport=tcp;ms-received-
cid=A400>
via: SIP/2.0/TCP 192.168.1.248:9639;ms-received-port=1554;ms-received-cid=a400
max-forwards: 70
from: "Claudio Avallone" <sip:cavallone@isbel.com.uy>;tag=fe92afa496;epid=df4c4f0f01
to: <sip:SignalingISBEL@isbel.com.uy>;tag=af01a8c0-13c4-46f3f24e-167cfc9b-2f52
call-id: 1d8f7fcfb3d54d6b8d0066edd39ccd27
cseq: 6 INFO
user-agent: LCC/1.3
content-disposition: signal;handling=required
content-type: application/csta+xml
content-length: 279


<?xml version="1.0" ?>
- <MakeCall xmlns="http://www.ecma-international.org/standards/ecma-323/csta/ed3">
     <callingDevice>tel:121;phone-context=dialstring</callingDevice>
     <calledDirectoryNumber>tel:ESN 330</calledDirectoryNumber>
     <autoOriginate>doNotPrompt</autoOriginate>
</MakeCall>
```

El cabezal es un comando SIP, del tipo “INFO” El cuerpo del mensaje se corresponde con un formato XML, donde se detalla el tipo de operación telefónica a realizar (“Make call” en el ejemplo anterior).

La Figura 3.7 (tomada de [7]) ilustra el proceso de intercambio de mensajes para iniciar una llamada desde una aplicación, utilizando TR/87. Se puede observar como todos la mensajería CSTA se incluyen dentro de métodos “INFO” de SIP.

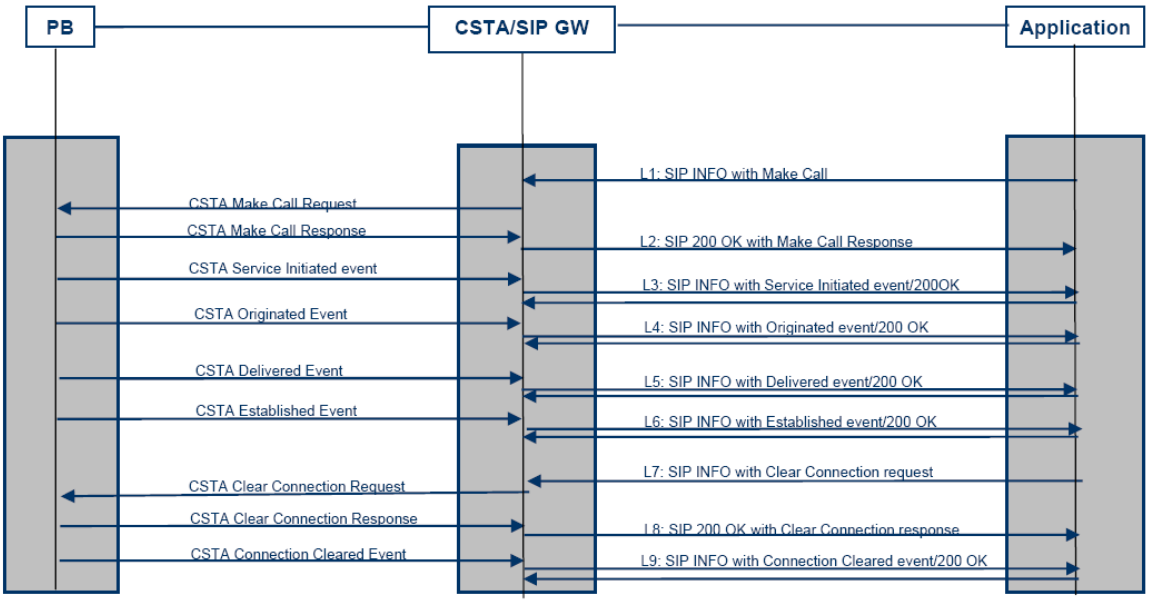

Figura 3.7

4 Comunicaciones Unificadas

Las comunicaciones unificadas son un resultado directo de la convergencia de las telecomunicaciones y las aplicaciones. Diferentes formas de comunicación han sido históricamente desarrolladas, promocionadas y distribuidas como aplicaciones independientes. La convergencia de todas las formas de comunicación sobre redes IP y sobre plataformas estandarizadas de software han permitido el desarrollo de un nuevo paradigma, cambiando la manera en que los individuos y las organizaciones se comunican.

Las Comunicaciones Unificadas reducen la "latencia humana" en los procesos de negocios. Si bien los diferentes métodos de comunicación (voz, mensajería instantánea, etc.) pueden ser utilizados en forma individual e independiente, la unificación entre todos ellos ayuda a mejorar la productividad y la eficiencia, permitiendo disminuir los tiempos necesarios para contactar a otras personas, u obtener respuestas a las necesidades en forma más rápida.

Las Comunicaciones Unificadas pueden definirse genéricamente como una plataforma de aplicaciones que mejoran la productividad individual, grupal y organizacional permitiendo y facilitando la administración y el control integrado de diversos canales de comunicación, redes, sistemas y aplicaciones de negocios [1].

Los componentes de las Comunicaciones Unificadas incluyen aplicaciones de presencia, mensajería instantánea, telefonía IP, conferencia de audio, conferencia web o colaboración de datos, mensajería unificada (un lugar común de almacenamiento de correo de voz, correo electrónico y fax), movilidad y/o video conferencia, todo accesible a través de una única interfaz de cliente, o embebida dentro de una interfaz de aplicación.

4.1.1 Componentes de las Comunicaciones Unificadas

4.1.1.1 Escritorio Convergente

Utilizando Comunicaciones Unificadas se obtiene un escritorio "unificado" o "convergente" ("Converged Desktop"). Este concepto apunta a consolidar las interfaces informáticas y telefónicas, manteniendo ambas, pero permitiendo un alto grado de integración y unificación. Mediante la utilización de técnicas de CTI, integradas o embebidas en las aplicaciones de escritorio, es posible:

- **Recibir notificaciones de llamadas telefónicas en el escritorio**: Mediante la presentación de pantallas emergentes ("screen popups"), la información de las llamadas entrantes se despliegan de manera similar a la recepción de un nuevo correo electrónico, o de un mensaje instantáneo (ver Figura 4.1).

Figura 4.1

- **Controlar el teléfono desde el escritorio**: Las llamadas pueden ser atendidas u originadas desde las aplicaciones de escritorio, integrando la libreta de direcciones corporativa. Mediante “un clic” sobre el nombre de la persona es posible iniciar una llamada, a su interno, a su celular, a su trabajo, etc. (ver Figura 4.2).

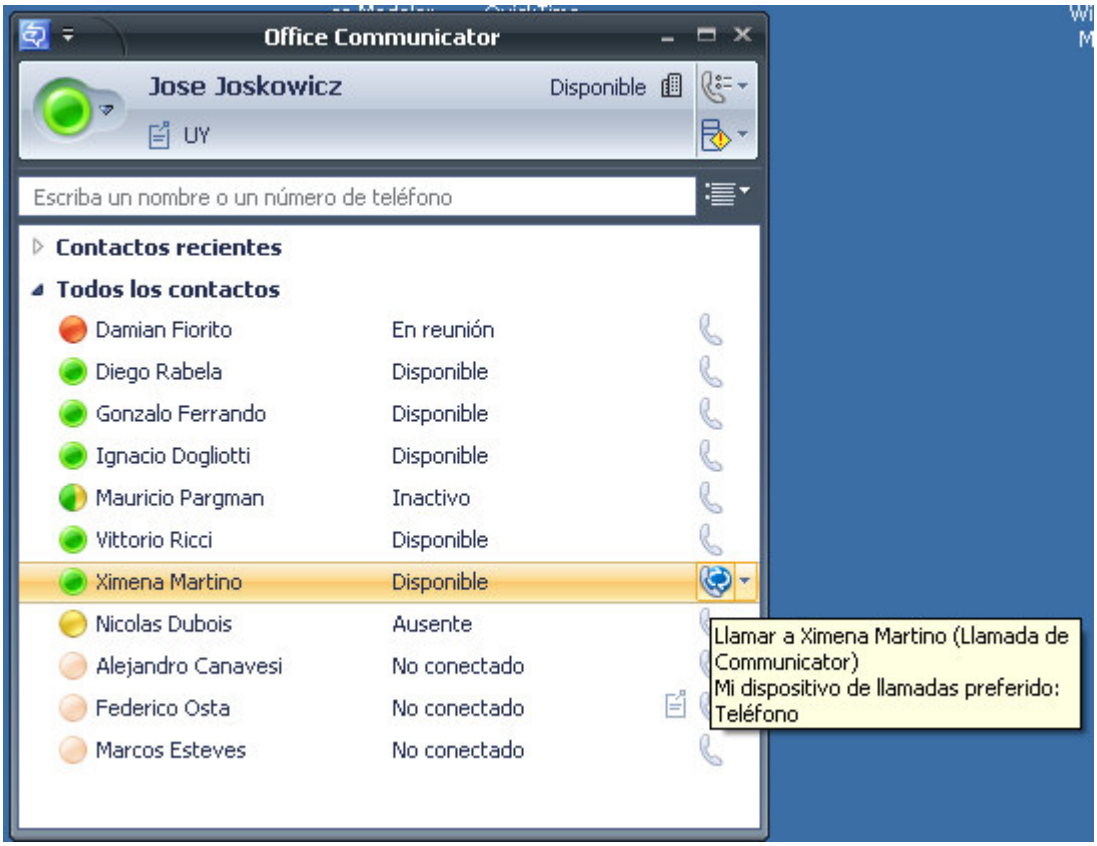

Figura 4.2

- **Activar desvíos "inteligentes" de llamadas**: En forma integrada al calendario de reuniones, o al estado de presencia, es posible activar desvíos de llamadas, al correo de voz, al celular, etc. (ver Figura 4.3).

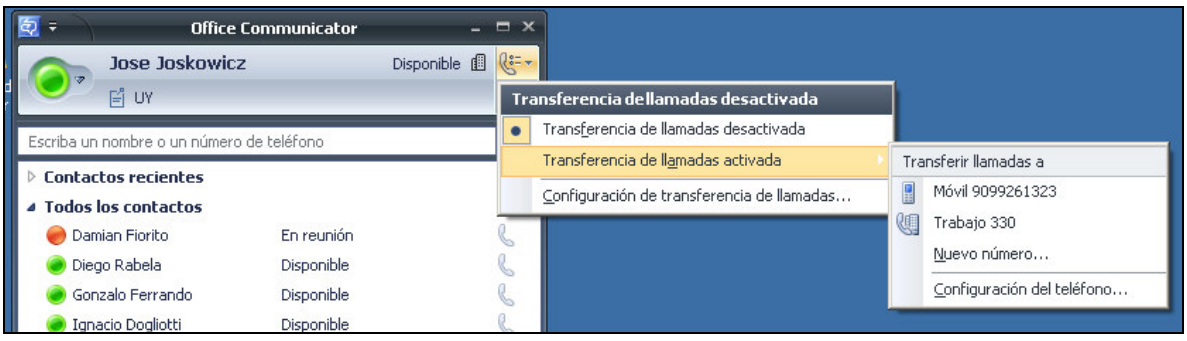

Figura 4.3

- **Combinar los sistemas de mensajería instantánea y presencia a las actividades telefónicas**: Automáticamente el estado de presencia se cambia a "Al teléfono" cuando se está en una llamada. Adicionalmente, con

una llamada establecida, se puede iniciar una sesión de mensajería instantánea para intercambiar archivos, o compartir el escritorio (Ver Figura 4.4).

Figura 4.4

4.1.1.2 Presencia

La "presencia" es una indicación del estado de disponibilidad de una persona para comunicarse con otras. Los sistemas de presencia basan su desarrollo en las recomendaciones del RFC 2778 [8] donde se definen las siguientes entidades:

- **Presentity:** Una entidad descrita por su información de presencia. Generalmente esta "entidad" es una persona, y su estado se mantiene en un servidor de presencia.
- **Watcher:** Quienes solicitan información de presencia de otras personas al servidor de presencia
- **Fetcher:** Un "watcher" que solicita el estado actual de presencia de algún "Presentity" a través del servidor de presencia
- **Subscriber:** Un "watcher" que solicita notificaciones del servidor de presencia cuando algún "presentity" cambia de estado.
- **Poller:** Una clase especial de "Fetcher" que solicita los estados de presencia en forma regular.

En el contexto de las Comunicaciones Unificadas, diversos tipos de aplicaciones pueden conocer y presentar el estado de presencia de las personas. Típicamente la presencia es indicada en sistemas de mensajería instantánea. Sin embargo, el estado de presencia puede ser muy útil en otro tipo de aplicaciones. En los clientes de correo electrónico, conocer el estado de presencia del remitente brinda la posibilidad de decir en el mismo momento el medio por el cual contestar su solicitud. Si la persona está presente y disponible, puede ser más eficiente llamarlo que responderle en forma escrita. Aplicaciones de procesadores de texto y planillas electrónicas, así como aplicaciones de gestión (CRM, ERP, etc.) también pueden mostrar el estado de presencia de las personas involucradas en el documento o proceso, mejorando de esta manera la comunicación organizacional cooperativa (ver Figura 4.5).

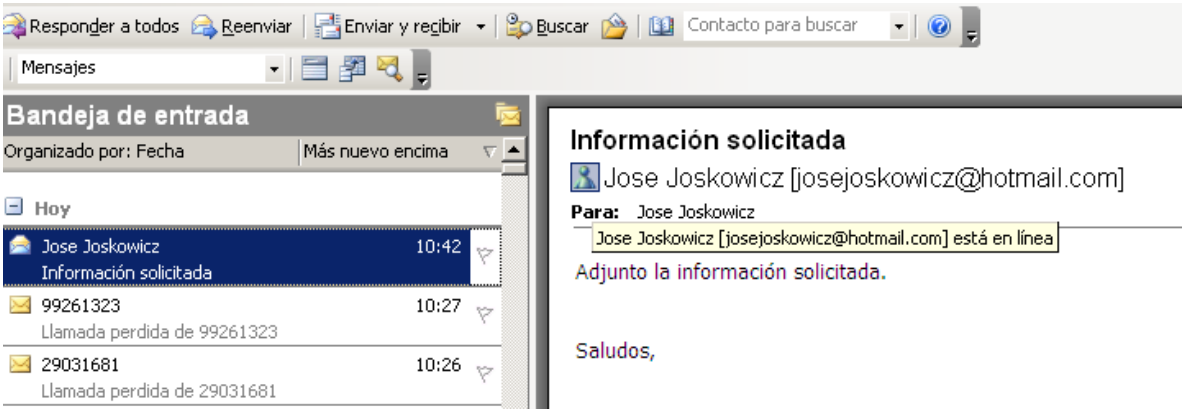

Figura 4.5

4.1.1.3 Mensajería Instantánea

Originalmente los sistemas de mensajería instantánea fueron definidos para entregar mensajes de texto cortos y simples en forma inmediata a otros usuarios que estén contactados en línea. Con el tiempo los sistemas fueron mejorados para soportar intercambios de archivos, conversaciones de voz y video, y otras funciones. La definición estandarizada de estos sistemas se corresponde con el RFC 2778.

En 2004, el RFC 3860 [9] estableció un perfil común para las aplicaciones de mensajería instantánea, denominado CPIM (Common Profile for Instant Messaging). Este perfil común indica, por ejemplo, el uso de un sistema de direcciones basado en el formato del mailto:. En este caso el formato es im: [to] [headers]. CPIM establece, adicionalmente, el formato requerido para los mensajes de presencia y mensajería instantánea.

Por su parte, el RFC 3920 [10], también de 2004, define un protocolo llamado XMPP (eXtensible Messaging and Presence Protocol) [11], utilizado para intercambiar mensajes XML en tiempo casi real. Este protocolo es utilizado para aplicaciones de mensajería instantánea y chat, estandarizados en el RFC 3921 [12]. Los tipos de presencia definidos son los siguientes:

- **Unavailable:** La entidad no está disponible para las comunicaciones
- **Subscribe:** Quien envía el mensaje desea subscribirse al estado de presencia del destinatario**.**
- **Subscribed:** Quien envía el mensaje permite al destinatario subscribirse a su estado de presencia
- **Unsubscribe:** Quien envía el mensaje se des subscribe
- **Probe:** Quien envía solicita conocer el estado de presencia del destinatario
- **Error:** Ocurrió un error al procesar un mensaje.

Un intercambio de mensajes instantáneo puede tener un formato similar al siguiente:

```
<message   from='juan@example.com'
           to='maria@example.net'
           type ='chat'
           xml:lang='sp'>

       <body>
           Hola, ¿como estas?
       </body>
</message>

<message    from='maria@example.net'
            to='juan@example.com'
            type ='chat'
            xml:lang='sp'>
       <body>
           Bien, gracias!
       </body>
</message>
```

Los mensajes pueden tener un tipo ("type"), entre las siguientes opciones: chat, error, groupchat, headline o normal. También pueden tener un asunto ("Subject"), un cuerpo ("body") y un "hilo" ("thread"), el que permite identificar todos los mensajes de una misma sesión de mensajería instantánea.

Los sistemas de mensajería instantánea han tenido un enorme éxito para la comunicación informal interpersonal. Es por ello que su incorporación al ámbito corporativo sea un camino casi natural.

4.1.1.4 Conferencias

Las conferencias multipartitas existen desde hace tiempo en el ambiente corporativo. Sin embargo, los conceptos de Comunicaciones Unificadas aplican a los sistemas de conferencias, permitiendo la integración con los sistemas de presencia, mensajería instantánea, calendarios, PBX, etc.

El RFC 4245 [13] publicado en 2005 describe los lineamientos para construir aplicaciones que soportan conferencias de manera interoperable, basados en SIP. Los requerimientos básicos descritos en ésta recomendación incluyen, entre otros:

- **Descubrimiento:** Soportar el descubrimiento automático de servidores de conferencias basados en SIP.
- **Creación de Conferencias:** Crear y especificar las propiedades de conferencias, ya sean "ad-hoc" o programadas. Las conferencias iniciadas desde el escritorio convergente cumplen con las definición de conferencias "ad-hoc"
- **Terminación de Conferencias:** Terminar las conexiones establecidas en una conferencia. Debe incluir la capacidad de pasar la conferencia a una comunicación básica punto a punto cuando queden únicamente dos participantes.

- **Manipulación de Participantes:** Invitar o desconectar participantes a una conferencia. Cuando sea necesario, debe permitir el anonimato de los participantes.
- **Información de Estado:** Mantener una base de datos que registre varios aspectos referentes a la conferencia. Los aspectos a registrar incluyen la información de los participantes, quien es el moderador actual, información acerca de cada sesión, etc.
- **Migración de Roles:** Debe ser posible cambiar los roles en la conferencia dinámicamente
- **Conferencias Asociadas:** Poder crear conferencias asociadas y apartadas entre participantes de la conferencia principal, y con participantes que no estén en la conferencia principal.

4.1.1.5 Colaboración

El concepto de Colaboración involucra a múltiples personas trabajando en conjunto para lograr un objetivo común.

Diversas herramientas de colaboración forman parte de las Comunicaciones Unificadas. Entre ellas, se destacan:

- **Vistas compartidas:** Permiten compartir documentos o el escritorio de una o varias personas entre varias personas. Entre las herramientas de vistas compartidas se incluye la pizarra electrónica.
- **Navegación Web compartida:** Permite que los participantes de una conferencia multimedia puedan navegar en forma conjunta por páginas de Internet. Esto complementa las vistas compartidas, con aplicaciones que realizan esta función de los navegadores de Internet de cada participante, no mediante una vista compartida del navegador de uno de los participantes.
- **Transferencia de Archivos:** Permite que un usuario envíe un archivo a uno o varios colaboradores.

5 Seguridad en las comunicaciones unificadas

En todas las empresas, las redes de voz y datos transportan “información”. Esta información es valiosa para las organizaciones, al punto que se considera uno de sus “activos” que, al igual que otros activos importantes para el negocio, tiene valor para la organización y consecuentemente necesita ser protegido apropiadamente.

Dentro de una corporación o empresa, la información puede existir en muchas formas. Puede ser impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o medios digitales, mostrada en videos, o hablada en conversaciones. En muchos de estos aspectos, las redes corporativas y las comunicaciones unificadas participan activamente. Asegurar la información, incluye, por lo tanto, asegurar las redes por dónde la misma es transmitida.

Muchos componentes tecnológicos son utilizados en las redes corporativas asociados a los aspectos de seguridad. Sin embargo, todos ellos tienen como objetivo proteger *la información*, y no los componentes informáticos en si mismos. Tomando esto en cuenta, es natural ver a los aspectos de seguridad de estos componentes tecnológicos enmarcados dentro de los planes más genéricos de “seguridad de la información”. Los planes de seguridad de la información generalmente se implementan mediante un Sistema de Gestión de la Seguridad de la Información (SGSI). En general, los objetivos de un SGSI son asegurar la continuidad del negocio y minimizar el daño ante un incidente de seguridad. En forma genérica, se establecen 3 objetivos de seguridad de la información [5]:

- **Confidencialidad**
  Procurar que la información sea accesible sólo a las personas autorizadas a acceder a su utilización.

- **Integridad**
  Asegurar la exactitud y la completitud de la información y los métodos de su procesamiento.

- **Disponibilidad**
  Asegurar que los usuarios autorizados tengan acceso a la información y los recursos asociados cuando lo requieran.

Varios actores pueden potencialmente amenazar los sistemas de seguridad de una organización. Entre ellos podemos mencionar “insiders”, o personal interno, competidores, o “hackers” en general. Las amenazas explotan posibles vulnerabilidades a la infraestructura que soporta la información.

Una **amenaza** es una condición del entorno del sistema de información con el potencial de causar una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). Las amenazas son, por tanto, el conjunto de los

peligros a los que están expuestos la información y sus recursos tecnológicos relacionados.

Una **vulnerabilidad** es una debilidad de un sistema, aplicación o infraestructura que lo haga susceptible a la materialización de una amenaza.
El **riesgo** puede verse como la probabilidad de que una amenaza en particular explote una vulnerabilidad
Un **ataque** no es más que la concreción o realización de una amenaza.

La política de seguridad y el análisis de riesgos deben identificar las vulnerabilidades y amenazas, y evaluar los correspondientes riesgos. Los riesgos pueden ser:

- **Mitigados**: Mediante la implementación de los correspondientes controles
- **Transferidos**: Por ejemplo tomando un seguro
- **Eludidos**: Cambiando la forma de hacer las cosas, o prescindiendo del activo amenazado.
- **Aceptado**: Luego de evaluado, decidir que no es conveniente tomar acciones.

En general, es sumamente importante ser concientes de las vulnerabilidades y amenazas a las que está expuesta la información, de manera de mitigar, transferir, eludir o aceptar el riesgo. Muchas veces, la decisión de cuanto dinero vale la pena invertir para eliminar o bajar el riesgo de una amenaza no es sencillo. En [14] puede verse un estudio genérico de la “rentabilidad” de las medidas de seguridad.

Las tecnologías de las comunicaciones unificadas, y en particular la Voz y Video sobre IP presentan nuevas vulnerabilidades y amenazas, las que se describirán brevemente a continuación.

5.1 Vulnerabilidades de los protocolos

Los protocolos utilizados en las tecnologías de VoIP son mayoritariamente estándar. Esto tiene la gran ventaja de permitir la interoperabilidad entre equipos de diversas marcas y fabricantes. Como contrapartida, el conocimiento público de estos protocolos los hace más vulnerables a ataques. A continuación se presentan algunas vulnerabilidades de los protocolos utilizados en VoIP:

5.1.1 Reescritura de cabezales

Varios protocolos (como H.323 o SIP) permiten que los usuarios manipulen los datos de los cabezales de los mensajes y reemplacen información dentro de los mismos. Un usuario malicioso podría de esta manera redirigir una llamada o un flujo de información de audio o video a un destino diferente al original.

En H.323 un usuario malicioso podría interceptar el setup inicial y modificar los paquetes del protocolo H.225 enviados del usuario final al gatekeeper, cambiando la dirección IP del origen a la del usuario malicioso. El resto de los mensajes serán respondidos, por tanto, hacia el usuario malicioso.

En SIP este proceso es aún más sencillo, debido a que los paquetes SIP son textuales, no binarios como lo son en H.323. Un usuario malicioso podría interceptar los mensajes de registro ("REGISTER") y cambiarlos para poner su propia dirección IP como origen del registro. El servidor de registro responde al usuario malicioso, aceptando la solicitud. El usuario malicioso le devuelve a su vez la respuesta al usuario original, sin embargo queda el usuario malicioso como el destino registrado. Ni el servidor de registro ni el usuario final se percatan de la maniobra. Sin embargo, cualquier llamada hacia el usuario final será en realidad dirigida hacia el usuario malicioso, como se muestra en la Figura 5.1

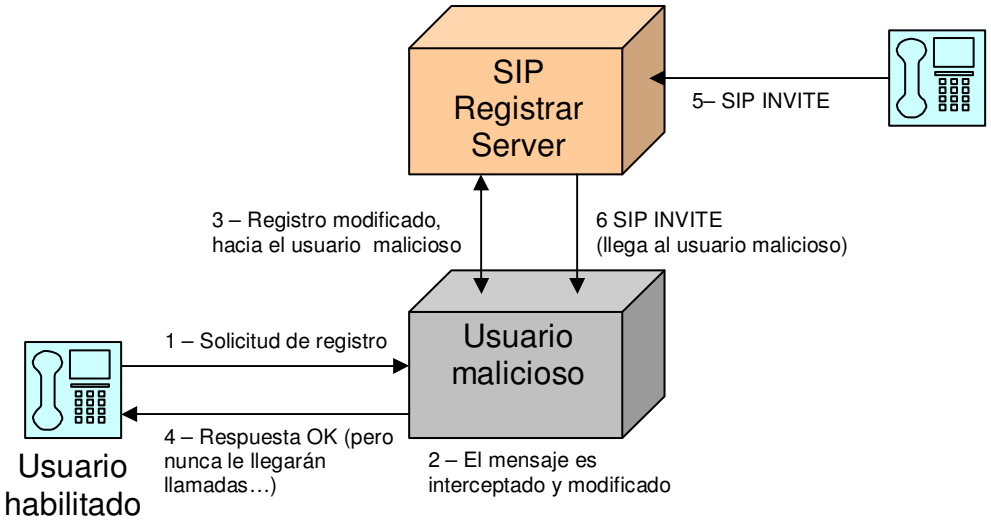

Figura 5.1

5.1.2 Denegación de servicio

Las aplicaciones que procesan los mensajes de señalización pueden tener "bugs" o problemas al intentar interpretar mensajes que deliberadamente tienen campos incorrectos. Esto puede causar errores, desde desbordes de memorias hasta reinicios. Inundando a un equipo con este tipo de paquetes puede causar su salida de servicio. Si el equipo es un Gateway o Proxy, esto puede afectar a toda la compañía**.**
En H.323 esto puede lograrse modificando ciertos campos binarios de los paquees H.225, insertando valores no válidos o mayores a los máximos admitidos.

En SIP estos ataques son sencillos. Los largos de los campos no están especialmente definidos en SIP. Un usuario malicioso podría incluir campos con valores excesivamente altos, mayores a los soportados por algunos equipos. Esto puede causar desbordes de memorias o variables internas, y generar reinicios en

los equipos. Por ejemplo, un mensaje SIP modificado podría tener el siguiente aspecto:

```
INVITE sip:pepe@fing.com SIP/2.0
Via:aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
    aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
    aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa...
Max-Forwards: 70
To: Pepe <sip:pepe@fing.com>
From: Alicia <sip:alicia@abc.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.montevideo.com
CSeq: 314159 INVITE
Contact: <sip:alicia@pc33.montevideo.com>
Content-Type: application/sdp
Content-Length: 142
```

El receptor de este mensaje podría tener problemas al interpretar el campo “Via”, el que normalmente tiene valores con pocos caracteres. En este caso, el valor de este campo no tiene el formato esperado, y además tiene muchos más caracteres que cualquier mensaje “normal”. Cambios similares se podrían hacer incluyendo caracteres normalmente “no soportados”, cambiando el formato de los campos, etc. Si los receptores no son lo suficientemente robustos, el procesamiento de este tipo de alteraciones puede generar interrupciones en el servicio.

Otro tipo de ataques del tipo “denegación del servicio” en SIP consiste en el envío de mensajes de finalización de llamadas (“BYE”). Esto es sencillo de hacer, y basta con interceptar un mensaje cualquier en el establecimiento de una llamada SIP, para capturar el Call-ID de la llamada. Con este valor, es posible armar un mensaje del tipo “BYE” y enviarlo hacia el usuario final, como se muestra en Figura 5.2

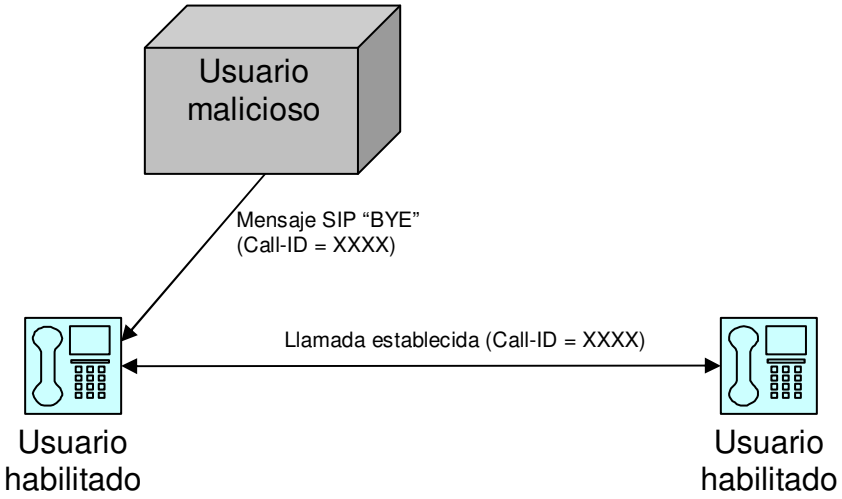

Figura 5.2

5.1.3 Intercepción de medios

Conocido como "Eavesdropping"[1] o "Packet Sniffing"[2] consiste en ganar acceso al audio y/o video de ciertas conversaciones, las que luego pueden eventualmente ser grabadas. Este tipo de ataques pueden darse en llamadas o conferencias. Una manera de realizar esto es simplemente obtener copias de todos los paquetes de cierta terminal, por ejemplo utilizando técnicas de "port mirroring" en los switches de datos. Si bien algunos sistemas de grabación de audio IP funcionan exactamente de esta manera, la realización no autorizada de estas configuraciones son consideradas un ataque, o un incidente de seguridad.
Algunos terminales tienen la posibilidad de realizar una duplicación del medio enviando una copia de los paquetes RTP enviados y recibidos hacia cierto destino. Esto está pensado para sistemas de grabación. La intercepción y manipulación de los paquetes de señalización pueden alterar la dirección destino de estas copias del medio, enviándolas hacia usuarios maliciosos.

En conferencias, existen otros mecanismos para ganar acceso a las mismas. Si un usuario malicioso captura los paquetes de registro de un usuario habilitado en la conferencia (por ejemplo, un "INVITE"), puede registrar el Call-ID. Luego puede enviar un paquete SIP del tipo "UPDATE" solicitando que el medio (audio/video) de la misma sea re-dirigido a su propia dirección IP. Esto puede hacerse fácilmente, cambiando el campo "c" dentro del cuerpo SDP del mensaje SIP.

5.1.4 Envío no permitido de datos

Las aplicaciones de escritorio pueden manejar señalización y flujos de audio o video. Manipulando apropiadamente el medio, es posible utilizar el flujo RTP para enviar datos, archivos o programas, permitiendo de esta manera quebrar las restricciones de seguridad en lo que respecta a la bajada o intercambio de archivos.

5.1.5 SPIT (Spam over Internet Telephony)

La popularización de VoIP está dando lugar a nuevos tipos de "Spam". SPIT es una nueva forma de spam para el envío de propagandas, ofertas o promociones a usuarios finales. Haciendo uso de vulnerabilidades de los protocolos, es posible enviar mensajes de voz en forma masiva con propagandas a sistemas de mensajería unificada, o interceptar conversaciones establecidas para introducir sobre las mismas mensajes publicitarios.

[1] "Eavesdrop" se traduce como "Escuchar indiscretamente". Un "eavesdropper" es una persona indiscreta, o que escucha indiscretamente.
[2] "Sniffer" proviene de la palabra "Sniff", que se traduce como "olfatear" o "husmear"

5.1.6 Degradación de calidad

Capturando y modificando los paquetes RTCP, es posible enviar informes falsos acerca de la calidad de servicio. Esto puede causar que los equipos reserven mayor ancho de banda del necesario, generen falsas alarmas, y en algunos casos, que se dejen de cursar llamadas a través de la red IP.

5.2 Seguridad en los protocolos

A los efectos de mejorar los aspectos de confidencialidad, varios de los protocolos admiten cierto grado de encripción o cifrado. Tal es el caso de SIP o RTP, por ejemplo.

5.2.1 Seguridad en SIP: SIPS

El protocolo SIP es textual, sencillo de comprender, y si se accede a los mensajes, son sencillos de modificar. Por este motivo, existen diferentes opciones para cifrar la mensajería SIP, tales como SSL (Secure Sockets Layer) o TLS (Transport Layer Security), estandarizado en el RFC 4346 [15]. SIP TLS es también conocido como SIPS (Secure SIP), y es una de las técnicas mayoritariamente utilizada. El uso de SIPS requiere que todas las partes involucradas en la señalización lo soporte, y pueden existir problemas de desempeño, ya que son necesarios tiempos adicionales para la cifrado y descifrado de los mensajes.

En forma complementaria, existen mecanismos para autenticar el acceso a los sistemas SIP, por ejemplo a los servidores de registro. En la recomendación original de SIP, el mecanismo sugerido de autenticación es similar al usado para sesiones HTTP, basado en MD5. En este escenario, la clave de acceso al servidor de registro es encriptada con MD5 (Message Digest 5). Nuevas formas de cifrado más seguras, como AES (Advanced Encryption Standard), están comenzando a ser utilizadas. Sin embargo, estos mecanismos no están completamente estandarizados.

5.2.2 Seguridad en RTP: SRTP

Adicionalmente al uso de TLS para asegurar la señalización, es posible cifrar el medio, a través del protocolo SRTP (Secure RTP), estandarizado en el RFC 3711 [16]. Cuando se implementa SRTP, los paquetes RTP y RTCP son cifrados en la fuente, antes de ser enviados a las capas inferiores de comunicación y descifrados en el destino antes de ser enviados a las capas superiores. Para ello se utilizan técnicas de cifrado AES. Las claves de cifrados utilizados para los protocolos RTP y RTCP son derivadas de una “clave maestra”. Esta clave maestra debe ser compartida entre los usuarios, y puede ser obtenida de una entidad externa de administración de claves de cifrado, utilizando los protocolos MIKEY, ZRTP, KEYMGT entre otros.

6 Gestión de proyectos de comunicaciones unificadas

Además de los desafíos propios que presenta llevar adelante cualquier tipo de proyecto de tecnología, los proyectos que involucran la implementación de comunicaciones unificadas tienen sus características y desafíos particulares. Muchas veces estos proyectos involucran también el diseño y la implementación de tecnologías de VoIP. Las particularidades de la gestión de proyectos de implementación de VoIP pueden verse en [6], y no serán discutidas en esta sección, donde se asume como un proyecto independiente.

Las ventajas de las comunicaciones unificadas se centran en la mejora de la productividad y la reducción de los tiempos de latencia en la toma de decisiones. El análisis de ROI (Retorno de la Inversión) debe siempre ser realizado, como en todo proyecto. Sin embargo, cuando los motivadores principales tienen que ver con el aumento de la productividad, los ahorros a veces son difíciles de justificar. Los siguientes aspectos pueden ser considerados en el cálculo de ROI de un proyecto de comunicaciones unificadas:

- **Mejoras en la productividad**. Cada uno de los grupos funcionales donde sean implantados sistemas de UC experimentarán mejoras en su productividad. Esto se puede evaluar considerando el tiempo por día que se invierte en buscar a personas, esperar por una respuesta, o no tener la información apropiada a tiempo.
- **Ahorros en viajes**. Las herramientas de comunicaciones unificadas permiten realizar reuniones virtuales, compartir pizarras, y otra serie de funciones que en muchos casos pueden reemplazar las reuniones presenciales. Una estimación del ahorro de costos en viajes aporta directamente al cálculo del ROI en un proyecto de comunicaciones unificadas.
- **Reducción del tiempo de cierre de negocios.** Mediante el acceso a los expertos de manera sencilla, o al intercambio fluido de información, es posible bajar el tiempo de cotizaciones y en definitiva de ciclo de ventas. Este aspecto puede tener un impacto importante en el ROI de un sistema de comunicaciones unificadas.
- **Reducción en costos telefónicos:** Mediante mecanismos alternativos de comunicación es posible reducir los gastos telefónicos. Estos mecanismos incluyen la mensajería instantánea, el correo electrónico, y los “Bridges” de conferencias, que permiten recibir llamadas en lugar de realizarlas para armar una conferencia.
- **Mejoras en la administración:** Al unificar sistemas, es posible disminuir costos de administración, gestión y soporte.

Los proyectos de comunicaciones unificadas pueden tener problemas técnicos de implementación, ya que se trata generalmente de proyectos de integración entre aplicaciones y sistemas telefónicos de tecnología emergente. Es de esperar que, aún siguiendo las mejores prácticas, algunos problemas se presenten al momento

de la implementación. La etapa de diseño es, como en todo proyecto, fundamental para el éxito.

Según las prácticas reconocidas del PMI (Project Managment Institute), un proyecto puede ser dividido en diversos procesos, tal como se ilustra en la Figura 6.1 [17]. Cada uno de estos procesos, que conforman el ciclo de vida de un proyecto, tiene sus particularidades, y aplican ciertas áreas de conocimiento.

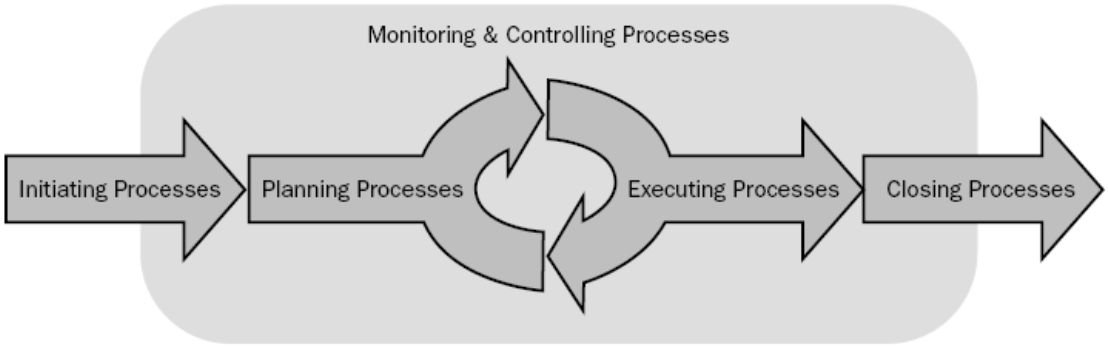

Figura 6.1

Es de notar que el comienzo del proyecto se da mucho antes de comenzar implementación, que es parte del proceso de ejecución. Las etapas previas a la implementación son tanto o quizás más importantes que la implementación. A continuación se presentan las actividades típicamente realizadas en cada proceso del proyecto, con foco en lo específico de las tecnologías de comunicaciones unificadas.

6.1 Iniciando un proyecto de UC (Procesos de Iniciación)

Durante esta fase del proyecto, se desarrollan las siguientes actividades:

- Desarrollo del “caso de negocio”
- Determinar el ROI (Retorno de la inversión)
- Establecer el alcance del proyecto, a alto nivel
- Identificar a los grupos de interés (“stakeholders”) y determinar sus necesidades y expectativas
- Identificar las restricciones conocidas
- Crear un “Project charter”, o acta de inicio del proyecto

En los proyectos de UC no es fácil determinar el ROI, como ya fue mencionado. Las reducciones de costos en lo que respecta a los aspectos “blandos”, como son el aumento de la productividad y la disminución de los tiempos en tomas de decisiones pueden ser estimadas para el cálculo del ROI. También pueden ser estimadas las reducciones en gastos de telefonía y en viajes. Aspectos como educación a distancia pueden ser relevantes en cierto tipo de empresas. En cualquier caso, el caso de negocio debe ser presentado, y si se hace

apropiadamente, seguramente se logre una justificación también económica del proyecto. Existen varias firmas consultoras y proveedores de tecnología que han realizado estimaciones de ROI para proyectos de comunicaciones unificadas, en diferentes escenarios, y pueden ser utilizados como base para el cálculo de un proyecto particular [18] [19] [20].

6.2 Planificando un proyecto de UC (Procesos de Planificación)

Durante esta fase del proyecto, se desarrollan las siguientes actividades:

- Definición de un alcance detallado
- Estimación detalla del presupuesto y asignación del presupuesto
- Creación de la Estructura de Desglose del Trabajo (WBS)
- Identificación del camino crítico
- Desarrollo de los diversos planes de gestión del proyecto
- Identificación y cuantificación de riesgos

En los proyectos de UC, al igual que en diversos proyectos de tecnología, es importante establecer el grado de ayuda o contrataciones externas deseado. Esta ayuda externa, típicamente tercerizada en Empresas y/o Consultores especializados, puede incluir alguna, varias, o todas las fases del proyecto (por ejemplo, desde el diseño hasta la implementación). Sin embargo, en cualquier caso, los clientes finales, quienes finalmente utilicen la tecnología, deberán ser involucrados, para poder lograr el éxito del proyecto.

Los riesgos en los proyecto de UC son variados, y deben ser identificados lo antes posible en la etapa de planificación. Entre los riesgos comunes se encuentran:

- Dependencia de la VoIP, con los riesgos de esta tecnología
- Problemas de seguridad
- Problemas de integración entre aplicaciones de diferentes proveedores
- Problemas técnicos de una tecnología emergente

Los riesgos técnicos más importantes están relacionados a las integraciones esperadas entre las aplicaciones y los sistemas. En algunos casos, éstos proyectos incluyen la integración de las aplicaciones específicas a las UC (por ejemplo, la integración desde el CRM o el ERP propio de la Empresa). En estos casos es posible que sea necesario realizar desarrollos de software específicos, los que deben ser incluidos como parte del proyecto. Sin embargo, estos desarrollos de software serán, seguramente, un proyecto en sí mismo, con su propio ciclo de vida. Dado que las comunicaciones unificadas son una tecnología reciente, existe aún poca experiencia por parte de los desarrolladores de software al respecto. Esto se convierte en un riesgo potencial importante, que debe ser evaluado y tenido en cuenta desde el inicio del proyecto. Adicionalmente, deberá ser considerado si para este tipo de proyectos se requiere o no un ambiente de desarrollo y pruebas separado del ambiente de producción. Si así fuera el caso,

también este ambiente deberá ser previsto como parte de los requisitos del proyecto.

6.3 Ejecutando un proyecto de UC (Procesos de Ejecución)

Como parte de la etapa de ejecución, se realizan generalmente las siguientes actividades:

- Determinación y asignación de el o los equipos de trabajo asignados al proyecto
- Realizar y gestionar los contratos de sub contratistas, incluyendo los contratos de hardware, software y servicios.
- Implementación, de acuerdo al alcance detallado realizado en el proceso de planificación

La etapa de ejecución es, sin dudas, sumamente importante. Sin embargo, la etapa de ejecución no suple, en ningún caso, la planificación. En caso de tener varios sub contratos, es de suma importancia mantener el control de los mismos, tener claros los límites de responsabilidades, y saber gestionar cualquier tipo de problemas que se presente entre éstos. Los proyectos de UC tienen impacto, generalmente, sobre diversos departamentos y grupos de trabajo. Los alcances de cada parte involucrada que debe aportar al proyecto deben estar bien establecidos y correctamente administrados para garantizar el éxito del proyecto. Entre estos grupos se incluye al departamento de IT, al de seguridad de la información, al departamento de telefonía, y a las gerencias que utilicen la tecnología resultante del proyecto, entre otros.

6.4 Controlando un proyecto de UC (Procesos de Monitoreo y Control)

Durante las etapas de planificación y ejecución es habitual que surjan problemas, o que se materialicen los riesgos. Es por tanto muy importante en todo proyecto mantener un proceso de monitoreo y control permanente.

Como parte de este proceso, generalmente se realizan las siguientes actividades:

- Monitorear y controlar el avance general del proyecto
- Realizar la verificación y control de que se esté cumpliendo con el alcance definido
- Realizar un control de costos
- Realizar controles de calidad
- Tareas relativas a reportes de avances
- Mantener los riesgos monitoreados y controlados. En casos que corresponda, gestionar la implementación de las medidas correctivas previstas

- Administrar a los sub contratos
- Realizar un control integral de cambios

Los procesos de monitoreo y control en proyectos de UC deben tener especial cuidado en lo que respecta a la gestión de riesgos. Siendo ésta una tecnología emergente, es posible que se presenten inconvenientes no previstos y se deban tomar acciones correctivas o de mitigación apropiadas. Los problemas de integración o de "frontera" entre diversos sectores son frecuentes, y muchas veces difíciles de prever en la etapa de planificación. También problemas no previstos de seguridad de la información pueden presentarse.

6.5 Finalización del proyecto de UC (Procesos de Cierre)

Los procesos de cierre generalmente incluyen las siguientes actividades:

- Obtener la aceptación de los interesados
- Finalizar los sub-contratos
- Des-asignar a los equipos de trabajo y recursos del proyecto
- Documentar las lecciones aprendidas
- Archivar la documentación para referencias futuras

Una vez cerrado el proyecto, es recomendable realizar un análisis del éxito del mismo, evaluando las mejoras de la productividad y eventualmente la reducción de costos obtenidas en la operación, así como el grado de satisfacción de los usuarios. Hacer visibles estas mejoras ayudará a conseguir presupuesto para nuevas ampliaciones o futuros proyectos de tecnologías relacionadas.

Glosario

AES	Advanced Encryption Standard
API	Application Programming Interface
ASN.1	Abstract Syntax Notation One
CAS	Channel Associated Signaling
CPIM	Common Profile for Instant Messaging
CRM	Customer Relationship Management
CSTA	Computer Supported Telecommunications Applications
CTI	Computer Telephony Integration
ECMA	European Computer Manufacturer's Association
IP	Internet Protocol
ISDN	Integrated Services Digital Networks
ITU	International Telecommunications Union
JTAPI	Java TAPI
LAN	Local Area Network
MD5	Message Digest 5
PBX	Private Branch Exchange
PMI	Project Managment Institute
PRI	Primary Rate Interface
RCC	Remote Call Control
RFC	Request For Comment
ROI	Return On Investment
SIP	Session Initiated Protocol
SGSI	Sistema de Gestión de la Seguridad de la Información
SPIT	Spam over Internet Telephony
TAPI	Telephony API
TDM	Time Division Multiplexing
TSP	Telephony Service Provider
UC	Unified Communications
VoIP	Voice over IP
WAN	Wide Area Network
WBS	Work Breakdown Structure
XML	eXtended Markup Language
XMPP	eXtensible Messaging and Presence Protocol

Referencias

[1] Unified Communications Solutions – A practical Business and Technology Approach
ISBN 978-0-9801074-1-78, Nortel Press

[2] World Unified Communication Market, N481-64 (November 2008), Frost & Sullivan

[3] Unified Communications: Holding its own in tough economic times. Steven Taylor and David DeWeese (Webtutorials, June 2009)

[4] "Conceptos de Telefonía Corporativa", Versión 08, José Joskowicz (Julio 2009)

[5] "Redes de Datos", Versión 05, José Joskowicz (Agosto 2008)

[6] "Voz Video y Telefonía sobre IP", Versión 08, José Joskowicz (Agosto 2009)

[7] "ISO/IEC TR 22767:2005 Technical report - Information technology — Telecommunications and information exchange between systems — Using CSTA for SIP phone user agents (uaCSTA)", 15 de agosto de 2005

[8] RFC 2778 A Model for Presence and Instant Messaging
M. Day et al, February 2000

[9] RFC 3860 Common Profile for Instant Messaging (CPIM)
J. Peterson, August 2004

[10] RFC 3920 Extensible Messaging and Presence Protocol (XMPP): Core
P. Saint-Andre, Ed., October 2004

[11] XMPP Standars Foundation
http://xmpp.org/

[12] RFC 3921 Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence
P. Saint-Andre, Ed., October 2004

[13] RFC 4245 High-Level Requirements for Tightly Coupled SIP Conferencing
O. Levin et al, Novembre 2005

[14] La rentabilidad de las medidas de seguridad de la información
Vicente Aceituno Canal, e.Security, septiembre 2004 – No 1, pp 36-37.
(Reproducido parcialmente en
http://www.seguridaddelainformacion.com/seg_10.htm)

[15] RFC 2778 The Transport Layer Security (TLS) Protocol Version 1.1
T. Dierks, E. Rescorla, April 2006

[16] RFC 3711 The Secure Real-time Transport Protocol (SRTP)
M. Baugher et al. March 2004

[17] A guide to the Project Management Body of Knowledge (PMBOK guide, 4th edtion)
PMI, 2008

[18] The Total Economic Impact™ Of Microsoft Unified Communications Products and Services
Forrester Consulting, October 2008

[19] Unified Communications ROI, A White paper
Vanguard Communications Corp., July 2007

[20] How Enterprises Can Reduce costs and boost ROI, White paper
Cisco, C11-460470-00, 03/2008