INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

UNIDAD ZACATENCO

DISEÑO Y ESTRUCTURA ADMINISTRATIVA DE LOS PROCESOS DE INFRAESTRUCTURA TECNOLÓGICA EN UN PROYECTO DE "CONTACT CENTER", APLICADO EN: IMPLEMENTACIÓN DE UNA SEDE ALTERNA DE OPERACIONES

T E S I S

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMUNICACIONES Y ELECTRÓNICA

P R E S E N T A

Carlos Alberto Reyes Martínez

DIRECTOR DE TESIS: **Dr. Jesús Enrique Urbano Noriega**

Ciudad de México Diciembre, 2016

INSTITUTO POLITECNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERIA MECANICA Y ELECTRICA

UNIDAD PROFESIONAL " ADOLFO LOPEZ MATEOS"

REPORTE TECNICO

QUE PARA OBTENER EL TÍTULO DE	INGENIERO EN COMUNICACIONES Y ELECTRÓNICA
POR LA OPCIÓN DE TITULACIÓN	MEMORIA DE EXPERIENCIA PROFESIONAL
DEBERA (N) DESARROLLAR	C. CARLOS ALBERTO REYES MARTÍNEZ

"DISEÑO Y ESTRUCTURA ADMINISTRATIVA DE LOS PROCESOS DE INFRAESTRUCTURA TECNOLÓGICA EN UN PROYECTO DE "CONTACT CENTER", APLICADO EN: IMPLEMENTACIÓN DE UNA SEDE ALTERNA DE OPERACIONES."

DISEÑAR E IMPLEMENTAR LA ADMINISTRACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA DE COMUNICACIONES Y COMPUTACIÓN, SU NORMALIZACIÓN Y SEGURIDAD DE LA INFORMACIÓN, EN UN CONTACT CENTER PARA DIFERENTES LÍNEAS DE NEGOCIO (SEGMENTO BANCARIO Y/O AEROLINEA), APLICANDOLO A LA IMPLEMENTACIÓN DE UNA SEDE ALTERNA DE OPERACIONES DE UN CONTACT CENTER.

- INTRODUCCIÓN A LOS CALL CENTER Y CONTACT CENTER.
- ESTRUCTURA Y OPERACIÓN DE UN CONTACT CENTER.
- INTRODUCCIÓN Y GENERALIDADES DE LA INFRAESTRUCTURA TECNOLÓGICA DE UN CONTACT CENTER.
- DISEÑO E IMPLEMENTACIÓN DE LA INFRAESTRUCTURA Y RECURSOS TECNOLÓGICOS PARA UNA SEDE ALTERNA DE CONTACT CENTER.
- ESTRUCTURA ADMINISTRATIVA DE LOS PROCESOS DE SEGURIDAD INFORMÁTICA.
- CREACIÓN DE UN PLAN DE CONTINUIDAD DE INFRAESTRUCTURA TECNOLÓGICA PARA EL NEGOCIO.
- REDUCCIÓN DE SOFTWARE DEL LICENCIAMIENTO MICROSOFT.

CIUDAD DE MÉXICO., A 22 DE NOVIEMBRE DEL 2016.

ASESOR

DR. JESUS ENRIQUE URBANO NORIEGA

ESCUELA SUPERIOR DE INGENIERIA MECANICA Y ELECTRICA
ESTADOS UNIDOS MEXICANOS
DEPARTAMENTO

ING. PATRICIA LORENA RAMIREZ RANGEL
JEFA DEL DEPARTAMENTO DE INGENIERÍA
EN COMUNICACIONES Y ELECTRÓNICA

Dedicatorias

Al IPN, ESIME y profesores

Agradezco infinitamente la oportunidad de abrirme las puertas de la mejor institución de México, siempre llevaré en alto el nombre del glorioso Instituto Politécnico Nacional. Así como llevar a la práctica los aprendizajes de los mejores maestros de ingeniería, y me comprometo a ser un gran ingeniero egresado de la gloriosa ESIME Zacatenco.

Al Ing. Enrique Urbano

Por ser un excelente guía para concretar el paso más importante de mi trayectoria en la ingeniería, agradezco infinitamente sus conocimientos.

Al Ing. Hugo Macias

Por su apoyo incondicional durante la trayectoria escolar, sus aprendizajes tanto escolares y de experiencia profesional, y forjarnos como grandes egresados e ingenieros de la ESIME.

A Cruz Sánchez

Todo el agradecimiento por llevarme al éxito principalmente es para ti, por ser la mejor madre y siempre apoyarme en mis triunfos y caídas, por aquellos momentos en los que he fallado siempre a impulsarme a ser el mejor y no darme por vencido, por darme segundas y terceras oportunidades, es triunfo es para ti, para la mejor madre que cualquier hijo envidiaría tener y por el gran amor infinito que te tengo, madre no es la que trae al mundo, es la que cría.

A Jesús Reyes

Por enseñarme a ser un gran hombre y padre de familia, el mejor ejemplo a seguir, el cual mantendré todas tus enseñas y se vuelvan perpetuas en el paso de los años, por demostrarme tu fortaleza no importando situaciones, ni edades, siempre serás el mejor.

A Violeta Reyes

Mi hermosa princesa, que me ha impulsado a ser el mejor y nunca dejarme fracasar en mis proyectos y propósitos, un motor de energía infinita que me impulsa que me hace desafiar

las leyes naturales, y siempre te impulsaré en lo más que pueda, en algunos años seré yo quien te vea triunfar y seguir siendo el padre más orgulloso, Te amo.

A Patricia Castro

La mejor persona que pude escoger como esposa, me has apoyado con los ojos cerrados y sin condiciones, gracias por compartir mis triunfos, y esta vida juntos agradezco este apoyo y tu valioso amor.

A Alberto Reyes

Por darme los mejores años de mi infancia y ese gran impulso a nunca darme por vencido, nunca ser conformista, siempre dar más del 100 %.

A Gustavo Reyes

Al Ingeniero que me inspiro a seguir este camino, por nunca dejarme vencer por mis propias tormentas y enseñarme a tomar los mejor de cada circunstancia, aún en decisiones precipitadas, gracias por todas tus enseñanzas y consejos.

A Guillermina Morales, Patricio Castro, Jahave Castro

Por apoyarme a alcanzar mis objetivos y permitirme ser un integrante de la familia, agradezco en demasía el apoyo y nuevas enseñanzas en la vida, siempre hay alguien en quien contar, sin pedir nada a cambio, sin condiciones.

A mis amigos

Por siempre estar en aquellos momentos importantes de mi vida, siempre valoraré su apoyo incondicional.

"La imaginación es más importante que el conocimiento."

Albert Einstein

|

"Si hay un secreto del buen éxito reside en la capacidad

para apreciar el punto de vista del prójimo y

Ver las cosas desde ese punto de vista así como del propio"

Henry Ford

"Si he visto más lejos ha sido porque he subido a hombros de gigantes."

Sir Isaac Newton

"Un experto es un hombre que ha cometido todos

los errores posibles en un campo muy pequeño"

Niels Bohr

Objetivo

Diseñar e implementar la administración de la infraestructura tecnológica de comunicaciones y computación, su normalización, procesos de seguridad de la información, en un Contact Center para diferentes líneas de negocio (Segmento bancario y/o Aerolínea), aplicándolo a la implementación de una sede alterna de operaciones.

Justificación

El proyecto está diseñado para la implementación de una nueva sede alterna, a solicitud de las áreas de negocio de operaciones de un Contact Center, quienes a su vez han recibido la petición de los clientes de las respectivas líneas de negocio, para tener un incremento en sus estaciones de trabajo y tener una opción estratégica de plan de continuidad de negocio en caso de presentarse una catástrofe. El trabajo abarca la configuración y diseño de la propuesta ofertada de infraestructura tecnológica, hasta la estabilización de los procesos administrativos de soporte y seguridad de la información, así como atender necesidades para operar las estrategias establecidas y funciones de negocio requeridas por el cliente.

Dentro de la solucion, se estructura los procesos para la administración de los recursos tecnológicos en un Contact Center, es necesario e imperante ir optimizando los procesos, con el fin de garantizar una alta disponibilidad para ofrecer un servicio de Contact Center, rentable, motivo por el cual está trabajo se enfoca, en estandarizar, diseñar e implementar procesos que cumplan este propósito.

Los principales puntos de interés, en los cuales se detecta áreas de oportunidad, son los siguientes:

- Reconocimiento e implementación de la infraestructura y recursos tecnológicos para una sede alterna, aplicado a la solicitud de negocio referida la propuesta entregada al cliente.
- Estandarizar los procesos de seguridad informática.
- Creación de un plan de continuidad de infraestructura tecnológica para el negocio.
- Reducción de software con licenciamiento.

Índice

Índice ilustraciones y tablas

Resumen

El proyecto se enfoca a diseñar y estandarizar los procesos de infraestructura tecnológica de un Contact Center para la implementación de una sede alterna, donde se iniciaran operaciones, en los cuales el propósito es enfatizar una proyección para la alta disponibilidad de los recursos tecnológicos, así como el cumplimiento de los estándares de seguridad de la información.

En general el proyecto explica los capítulos de la siguiente forma:

Capítulo 1. Introducción a los Call Center y Contact Center.

Capítulo el cual relata una breve historia del origen y evolución de los Call y Contact Center, así como la definición de ambos y una breve explicación del enfoque de negocio que tienen (CRM y BPO).

Capítulo 2. Estructura y operación de un Contact Center

En el segundo capítulo se explican las generalidades de operación del Contact Center, asimilando misión y valores, hasta los sectores de competitividad y los tipos de soluciones ofrecidas al cliente final, en las cuales se logra definir de acuerdo al sector social o económico en el cual se ofrecen cada una.

Capítulo 3. Introducción y generalidades de la infraestructura tecnológica de un Contact Center

El tercer capítulo describe las generalidades de los recursos tecnológicos principalmente utilizados para el funcionamiento de las soluciones multicanal ofrecidas para las líneas de negocio, que son el canal de contacto con los usuarios finales de cada cliente, se describe algunas de las tecnologías utilizadas por la arquitectura de IT del Contact Center.

Capítulo 4. Diseño e implementación de la infraestructura y recursos tecnológicos para una sede alterna de Contact Center.

El cuarto capítulo explica los procesos del Contact Center considerando la normalización de los procesos ya establecidos, así como complementar y diseñar procesos para mantener una alta disponibilidad de los recursos de infraestructura tecnológica, esto garantiza tener una nueva visión para prevenir y detectar fallas oportunamente, lo cual debe reflejarse una disminución de penalizaciones.

Estos procesos se implementan en una sede alterna de operaciones de un Contact Center el cual opera soluciones tecnológicas de la misma línea de negocio que la sede principal y una nueva línea de negocio.

Capítulo 5. Estructura administrativa de los procesos de seguridad informática.

Dentro de las necesidades de los clientes de las líneas de negocio a las cuales se les brinda un servicio multicanal, es importante mantener la confidencialidad de la información y seguridad de los clientes finales; por lo cual este capítulo se enfoca en mantener estos procesos, ya que es un pilar fundamental para la inclusión de nuevos clientes.

Capítulo 6. Creación de un plan de continuidad de infraestructura tecnológica para el negocio.

Derivado de la alta disponibilidad y la ventana de servicios ofrecida 24 horas x 365 días, para el caso de algunas líneas de negocio; surge la necesidad de crear un plan de continuidad de negocio, ya sea en caso de alguna catástrofe natural o alguna contingencia ocasionada por un tercero, permite al negocio operar en una sede diferente sin tener una alta afectación en tiempo, y reducir el impacto económico al no estar operando.

Capítulo 7. Reducción de software del licenciamiento Microsoft

El último capítulo está enfocando en generar un plan de acción para reducir el licenciamiento software corporativo, como es el caso de Microsoft, migrando a soluciones de tipo libre (freeware) que sean funcionales para las soluciones ofrecidas multicanal.

Abstract

The project focuses on designing and standardize the processes of technological infrastructure of a Contact Center for the implementation of an alternative site, where operations began, in which the purpose is to emphasize a projection for high availability of technology resources and the compliance with standards of information security. Overall, the project explains chapters as follows:

Chapter 1. Introduction to Call Center and Contact Center.

Chapter which tells a brief history of the origin and evolution of the Call and Contact Center, as well as the definition of both and a brief explanation of business approach with (CRM and BPO).

Chapter 2. Structure and operation of a Contact Center

In the second chapter generalities operating Contact Center explains, assimilating mission and values, to the sectors of competitiveness and rates offered to the end customer solutions, which is achieved defined according to the social or economic sector in which They are offered each.

Chapter 3. Introduction and overview of the technological infrastructure of a Contact Center

The third chapter describes the overview of technological resources primarily used for the operation of multichannel solutions offered to business lines, which are the channel of contact with the end of each client users, describes some of the technologies used for architecture IT Contact Center.

Chapter 4. Design and implementation of infrastructure and technological resources for an alternative site

The fourth chapter explains the processes of the Contact Center considering the standardization of established processes, as well as complement and design processes to maintain high availability of technology infrastructure resources, this will ensure a new vision to prevent and detect faults early, it which should be reflected a dewcrease in penalties.

These processes will be implemented in a new building of a Contact Center which technological solutions will be operating in the same line of business headquarters and a new line of business.

Chapter 5. Administrative structure of security processes.

Within the customer needs of the business lines which are provided with a multichannel service, it is important to maintain the confidentiality of information and safety of end customers; so this chapter focuses on keeping these processes, since it is fundamental for the inclusion of new customers pillar.

Chapter 6. Creating a continuity plan for business technology infrastructure.

Derived from high availability and window service offered 24 hours x 365 days, for some lines of business; arises the need to create a business continuity planning, whether in the event of a natural disaster or any contingency caused by a third party allows the business to operate in a different seat without a high involvement in time, and reduce the economic impact not operating.

Chapter 7. Reduce software licensing Microsoft

The last chapter is focusing on creating an action plan to reduce corporate software licensing, as in the case of Microsoft, migrating to free type solutions (freeware) that are functional for multi-channel solutions offered.

Introducción

Los Contact Center y los recursos de Infraestructura Tecnológica han cambiado la forma en que operan las organizaciones actuales. A través de su uso se logran importantes mejoras, ya que automatizan los procesos operativos, suministran una plataforma de información necesaria para la toma de decisiones y, lo más importante, su implantación logra ventajas competitivas.

Las Tecnologías de la Información han sido conceptualizadas como la integración y convergencia de la computación, las telecomunicaciones y la técnica para el procesamiento de datos, donde sus principales componentes son: la información, el equipamiento, el factor humano, la infraestructura, el software y los mecanismos de intercambio de información, los elementos de política y regulaciones; además de los recursos financieros. Los negocios tienden a tener una mayor dependencia de las Tecnologías de la Información (IT).

Las áreas de IT y las actividades en ellos desarrolladas han sido tradicionalmente vistos como un área de soporte al negocio, descuidando incluso muchas veces el uso de criterios racionales para medir su rentabilidad, eficacia y la calidad del servicio ofrecidos a toda la organización.

Tecnología juega uno de los principales pilares fundamentales para las estructuras empresariales de la gran mayoría de las empresas, ya que la comunicación con los clientes o allegados se logra a través de los medios de comunicación multicanal (teléfono, redes sociales, correo, etc.), en el caso particular para los Contact Center, los clientes logren contactar a sus proveedores o prestadores de servicios por el mayor numero de canales disponibles.

CAPÍTULO 1 Introducción a los Call Center y Contact Center

En este capítulo se describe los principales conceptos de un Call y Contact Center, así como la evolución que han ido tenido a la largo del tiempo este tipo de empresas, que presentan las soluciones de IT para el negocio, adicional se describe su enfoque de negocio en los sectores del CRM y BPO, y la definición de los mismos.

1.1 Estado del arte de los Contact Center

El origen de los call center se remonta al año 1876 en Estados Unidos, cuando Graham Bell, inventor del teléfono, creó la empresa Bell Telephone (posterior AT&T), el primer centro nacional de ventas por teléfono en la ciudad de Kansas. El incremento del uso del teléfono en EE.UU. hizo posible apreciar sus posibilidades en el ámbito empresarial. De esta manera, muchas empresas encontraron en este nuevo método vinculado a la telefonía una excelente oportunidad y una innovadora forma de relacionarse con sus clientes. Las compañías comenzaron a publicar su número de teléfono en anuncios de prensa y a recibir llamadas de sus clientes, con lo cual apareció la función del operador telefónico, empleado contratado única y exclusivamente para atender el teléfono. A medida que el volumen de llamadas fue creciendo, las empresas fueron incorporando un equipo de personas para dar ese servicio, ver **Figura 1.1**.

Figura 1.1. Uso de llamadas de entrada y salida de un call Center

Posteriormente, con la revolución tecnológica, aparecen centrales dedicadas exclusivamente a desarrollar esta función, con herramientas que gestionan el flujo de llamadas y sistemas automáticos de atención al cliente, como las que es posible observar hoy en día. La experiencia estadounidense es llevada a Europa; los primeros call center aparecen en los años 70, de la mano de multinacionales norteamericanas com.o IBM, AMEX, 3M, Rank Xerox y Kodak que implementan allí la experiencia que tuvieron en Estados Unidos y que años después fue llevada al resto del mundo.

En la actualidad, la industria de los call center emplea en el mundo a un número cercano a los 8 millones de trabajadores, distribuidos en 4,8 millones de posiciones, de las cuales Estados Unidos representa el 55%, equivalente al 2% de su fuerza laboral, seguido por el Reino Unido, Alemania y Francia. A nivel planetario, factura alrededor de US$180 billones al año. Existen estimaciones aproximadas acerca de la fuerza de trabajo que posee el sector en diversos países. La complejidad de la industria, donde hay muchas empresas que realizan esta actividad internamente, dificulta pesquisar con precisión la cantidad de trabajadores del rubro. Se calcula que en EE.UU. alcanzarían a ser entre 2,5 y 6,5 millones de empleados (Moss, Salzman y Tilly, 2004); en Europa serían alrededor de 750 mil (Datamonitor, 2004), sólo en Francia cerca de 200 mil (Novethinc, 2005), en México 190 mil (Instituto Mexicano de Telemarketing, 2005) y por último en Centroamérica y el Caribe llegarían a cerca de 24 mil (empresa Avaya). **[1]**

Los call centers iniciaron su existencia básicamente como nuevas funciones que ejercían las empresas interesadas en las ventas por teléfono o bien la atención a sus clientes (ejemplo típico: las compañías de aviación). Poco tiempo después, este servicio fue ofrecido como outsourcingG1 por nuevas empresas que se dedicaban íntegramente a desarrollar las diversas prácticas del call center. Estas nuevas empresas han sido las propulsoras de la internacionalización de la industria. La difusión y adaptabilidad de la tecnología necesaria para la implementación de un call center permitió que se adoptara en naciones de desarrollo medio. **[1]**

1.2 Evolución de los Contact Center en México

México es un jugador líder en el sector de TI (Tecnologías de la información) y BPO (Business Process Outsourcing), siendo el sexto mejor destino a nivel mundial para la localización de servicios globales (tercerización de servicios de TI, BPO, contact center y call center, entre otros).
Entre los principales proveedores en México, se enlistan en la **Tabla 1.1**:

Tabla 1.1. Principales proveedores de Contact Center en México

Empresa	Posiciones	Certificaciones	Año de Fundación
Teleperfomance	14400	ISO 27000 ,COPC, ISO 9001/2008, TOPS y Best	1996
Atento México	10500	ISO 9000, ISO 27000,COPC, ITIL	1999
TELVISTA	5825	ISO 9000, MGCIC/NECC,ITIL, PCI	1998
Teletech México	5000	Six SigmaISO 9000 1982 MDY Contact Center & BPO 4,500 COPC, ITIL, ISO9001,Six Sigma	1997
Bconnect Services S.A de C.V	3500	ISO 9000, ISO 27000,COPC, MGCIC/NECC,ITIL, OHSAS 180001:2007	1995
Axtel	3400	ISO 9000, MGCIC/NECC	1995
AMATECH S.A. de C.V	3000	ISO 9000, ISO 27000,COPC, ITIL	2000
Digitex	2576	ISO 9000, ISO 27000,COPC, ITIL, ESR	2009
EFICACIA	2526	Atención Telefónica 2,500 MGCIC/NECC, ESR	1996

[Ver Anexo 1, Certificaciones]

Algunos clientes que utilizan el servicio de Contact Center en México:

BBVA Bancomer
Telefónica Movistar
Interjet
American Express
Volaris
Metlife
Terra
HSBC
Banco Wallmart
Telcel
ACE Banamex
Mejor Compra TV
Nextel
Santander
Gayosso
Seguros Monterrey
L'oreal
Sodexo
Sony
Toyota
Verifone
Lexmark
Afore XXI **[1]**

1.3 Definición de Call Center

Call center del inglés puede traducirse como centro de llamadas. Se trata de la oficina o empresa donde un grupo de personas capacitadas prestan sus servicios para brindar algún tipo de atención o servicio telefónico **[1]**.

Los trabajadores de un call center pueden realizar llamadas (para tratar de vender un producto o un servicio, realizar una encuesta, etc.) o recibirlas (para responder a las dudas de los clientes, tomar pedidos, quejas y sugerencias). El call center se especializa en una de las dos tareas (realizar o recibir las llamadas) mientras otros cumplen con ambas funciones.

El Call Center, se destina a establecer comunicaciones con los clientes, proveedores, socios u otros grupos. Su función está determinada por cada empresa, es frecuente que un mismo call center lleve a cabo ambas tareas.

La industria del call center presenta algunas diferenciaciones. Existen empresas que desarrollan estos servicios internamente, dedicadas a atender únicamente a sus propios clientes (**inhouse***). Por otro lado, están las empresas dedicadas a la atención de clientes de terceros, es decir, a proveer servicios de outsourcing de call center a otras compañías. El outsourcing se desarrolla a su vez en dos modalidades: cuando los servicios son prestados dentro de las instalaciones de la empresa cliente, se habla de **insourcing***; en el outsourcing propiamente tal, en cambio, el servicio es

desarrollado en el establecimiento de la empresa de call center proveedora. A su vez, los call center que proveen servicios externos pueden hacerlo en el mercado interno (**inshore***), y/o bien exportar servicios hacia el extranjero (**offshore***). La **Figura 1.2** ilustra esta clasificación.

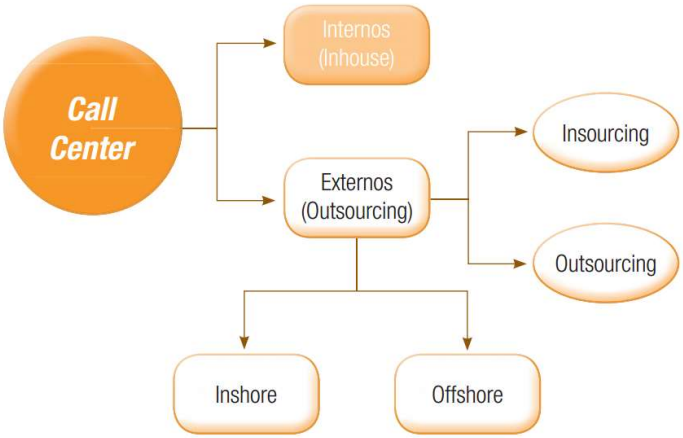


Figura 1.2. Soluciones generales de un Contact Center

1.4 Definición de Contact Center

Se define como un centro de atención multicanal, donde las interacciones o solicitudes que se produzcan entre la empresa y el cliente pueden provenir de cualquier canal o medio de comunicación (teléfono, chat, e-mail, web, fax, videollamada), ver **Figura 1.3**. Esto permite la centralización de toda la información de todos los canales de comunicación en una sola solución de Contact Center.

Es importante destacar que el Contact Center puede ser operado por la propia compañía o por un tercero (servicio de Outsourcing) en una empresa externa. Existen empresas conformadas que se dedican a ofrecer este tipo de soluciones, con la infraestructura tecnológica necesaria y el personal capacitado para comercializar la prestación de este servicio.

Figura 1.3. Soluciones mullticanal de un Contact Center

1.5 Definición de CRM, Gestión de Relaciones con el Cliente

El CRM (Customer Relationship Management), o "Gestión de Relaciones con el Cliente" es un modelo de negocios cuya estrategia está destinada a lograr identificar y administrar las relaciones en aquellas cuentas más valiosas para una empresa, trabajando diferentemente en cada una de ellas de forma tal de poder mejorar la efectividad sobre los clientes **[2].**

Los objetivos de las soluciones CRM son:

- Maximizar la información del cliente
- Identificar nuevas oportunidades de negocio
- Mejora del servicio al cliente
- Procesos optimizados y personalizados
- Mejora de ofertas y reducción de costos
- Identificar los clientes potenciales que mayor beneficio generen para la empresa.
- Fidelizar al cliente, aumentando la retención de clientes

Para implementar una herramienta CRM se deben considerar los cuatro pilares básicos en una empresa:

- Estrategia:

La implementación de herramientas CRM debe estar alineada con la estrategia corporativa y con las necesidades tácticas y operativas de la misma, **ver Figura 1.4**.

- Personas:

La aportación tecnología no es suficiente, los resultados llegarán con el correcto uso que hagan de ella las personas. Se debe gestionar el cambio en la cultura de la organización buscando la satisfacción del cliente, mejorando el clima laboral.

- Procesos:

Es necesaria la definición de nuevos procesos para optimizar las relaciones con los clientes, consiguiendo procesos más eficientes y eficaces. Cualquier implementación de tecnología converge en los procesos de negocio, haciéndolos más rentables y flexibles.

La cual en cada caso será diferente en función de las necesidades y recursos de la empresa.

El CRM es definido como un enfoque empresarial por el cual se puede conocer la conducta de los clientes e influir en ella por medio de una comunicación congruente, para aumentar su nivel de captación, retención y rentabilidad. Es una estrategia utilizada por muchas empresas para incrementar la satisfacción de sus clientes y optimizar la rentabilidad de sus negocios **[2]**.

Conceptualmente, la metodología para desarrollar un proyecto CRM contemplará las siguientes etapas:

- Definición de objetivos y visión del proyecto CRM
  Tecnología:

Es necesario definir una visión ("cómo será la organización tras la implementación del proyecto") así como unos objetivos globales del proyecto para así poder focalizar en estos objetivos y poder hacer un seguimiento de los mismos. La definición ha de ser desarrollada tras un análisis para conocer tanto los puntos fuertes y débiles de la organización, siendo crítico este análisis inicial para el desarrollo posterior del proyecto.

Estos objetivos deben ser bastantes concretos. Es decir, los objetivos serían por ejemplo "disminuir la tasa de pérdida de clientes en un x%" en lugar de "mejorar las relaciones con los clientes".

- Definición de la estrategia CRM

Tras haber definido la visión y objetivos, es indispensable definir una estrategia para alcanzar los objetivos.

En esta estrategia es clave la definición del posicionamiento en cada uno de los segmentos de clientes de la organización, analizando las competencias actuales y necesarias así como un calendario para su implementación.

- Cambios organizacionales, en los procesos y en las personas

Es necesario modificar la estructura organizativa y los procesos para conseguir una empresa centralizada en el cliente. Los procesos han de ser nuevamente definidos para mejorar su eficacia y eficiencia dando prioridad a los que más impacto tengan en la satisfacción del cliente. En este punto, la tecnología será clave.

Es necesario introducir los valores de organización orientada al cliente en la cultura corporativa. Este es uno de los elementos críticos en el éxito de un proyecto CRM: la "pasión por el cliente" integrada en la cultura de la organización.

- Información

Definición de las correctas prácticas para la gestión de la información.

Esta es una parte muy importante para el desarrollo de la "inteligencia de clientes" (customer intelligence) y consiguiendo de esta manera conocer más a los clientes, inicialmente para el desarrollo de una estrategia completa CRM basada en el conocimiento de los clientes y el desarrollo de productos y servicios a su medida.

Igualmente es importante también la recogida de información para la mejora de los procesos así como para la puesta en marcha de sistemas de mejora continua.

- Tecnología

En este punto es muy importante destacar que es totalmente necesario conocer exactamente las necesidades de negocio que se tienen para poder escoger la solución tecnológica mejor adaptada a las necesidades concretas.

Problemático es escoger soluciones para las necesidades como escoger una solución que tras su implementación se detecta claramente que es insuficiente para las necesidades de la organización **[3].**

- Seguimiento y control

Como cualquier proyecto importante, se han de definir unos indicadores KPI (Key Performance Indicators) que sirvan para el control de los resultados así como la toma de decisiones en consecuencia con esos objetivos.

Es importante destacar que aunque tengamos un plan global de desarrollo del proyecto es muy importante dar pasos cortos y seguros.

El CRM se apoya en nuevas tecnologías para lograr una acelerada toma de decisiones administrativas y aumentar la utilidad de la información recopilada, obteniendo un mejor conocimiento sobre clientes potenciales.

Figura 1.4 Referencia a los recursos de los cuales están compuesto el CRM

1.5.1 Contact Center con orientación CRM

CRM es la estrategia de negocio, soportada por una herramienta tecnológica como es el software, por la cual una empresa pretende apalancar en el conocimiento de sus clientes para crear relaciones más rentables basadas en la aportar valor añadido a sus productos o servicios que finalmente beneficien a sus clientes **[3].**

El Contact Center debe apoyar los siguientes objetivos de la estrategia CRM:

- Adquisición
- Retención
- Crecimiento
- Conocimiento

1.5.2 Retención de clientes

- Resolver en el primer contacto
  - Disponibilidad de información en línea: sobre facturación, órdenes de servicio, información del cliente, quejas y reclamos, información de producto y políticas.

  - Conocimiento del operador: constante entrenamiento, aprendizaje de nuevas habilidades.

  - Empoderamiento: enfoque solución, procedimientos flexibles.

- Maximizar el acceso
  - Acceso multicanal: telefónicos (**IVR**,** fax por demanda, **Inbound*** y **Outbound***) y virtuales (email, chat, call back).
  - Cola universal, Virtual Hold
  - Combinación de autoservicios (Internet e IVR) y soporte para el agente (**CTI**** y **Call Manager***).
  - Programación de turnos y agentes: inferior a la demanda, superior a la demanda.
  - Horarios y accesos telefónicos (combinación de números locales y nacionales)
  - Nuevos requerimientos de capacitación para asesores con capacidad de atención multicanal.

Las estrategias de retención de clientes en el Call Center son: Identificar, clasificar y personalizar al cliente **[3]**.

1.5.3 Adquisición y crecimiento de clientes

- Pre llamada
  - Generar y calificar prospectos
  - Convertir las preguntas sobre productos y servicios en potenciales procesos de venta (marcar cliente como potencial).
- Durante el tiempo de la llamada
  Inbound (Llamadas de entrada)
  - Identificar y clasificar al cliente según valor y oportunidad
  - Sistema de soporte de decisión para sugerir alternativas de solución o venta
  - Formar al agente con habilidades potenciales

  Outbound (Llamadas de salida)

  - Calidad de base de datos, atractiva oferta continua, estrategia para realizar contacto.
  - Efectividad
- Después de la llamada
  - Acciones Correctivas
  - Auditorías de gestión

1.5.4 Conocimiento de clientes

La información sobre la interacción con el Contact Center, se recopila lo siguiente **[3]**:

- Inquietudes y Dudas sobre el producto/servicio

- Problemas con el producto/servicio
- Características deseables sobre el producto/servicio
- Comportamiento en el canal
- Expectativas de trato
- Retroalimentación a campañas o iniciativas
- Alertas de deserción

- Tipos de análisis y reportes

- Identificar y clasificar razones para que un cliente decida no cancelar su deuda o no compre el producto.
- Identificar y clasificar áreas de insatisfacción del cliente dentro del Contact Center
- Identificar y clasificar oportunidades de mejoramiento del producto
- Identificar y clasificar información no disponible o errada.

- Medios y Herramientas

- Agente/Operador: incentivo a ideas aplicadas que mejoren la relación con el cliente.

1.6 Definición de BPO

El Business Process Outsourcing (BPO) se conoce en español como "Externalización de Procesos de Negocios". Se refiere a la subcontratación de funciones de procesos de negocios mediante proveedores de servicios internos o externos a una empresa. Normalmente, el objetivo de dicha subcontratación va unida a la reducción de costos y recursos por parte de la empresa contratante.

El BPO es muy recurrente para empresas que quieren maximizar la eficiencia de sus operaciones, sin tener que emplear grandes volúmenes de recursos. De esta forma, es posible rentabilizar procesos y conseguir un mayor beneficio, estableciendo relaciones de colaboración con otras empresas. Estos acuerdos son totalmente negociables entre ambas partes, aunque la empresa que subcontrata suele definir y revisar constantemente los parámetros de calidad.

Se entiende como la delegación de uno o más procesos de negocio, intensivos en el uso de tecnologías de la Información, a un proveedor externo, quien a su vez posee, administra y gerencia los procesos seleccionados, basado en métricas definidas y medibles **[4]**.

El BPO ayuda a minimizar costos de tipo fijo como el de personal, de espacio físico y equipamiento. La empresa subcontratada asumirá estos gastos y a mejorar y automatizar procesos en los cuales cuentan con mayor experiencia. De esta manera, reducen costos operativos y se convierten los costos fijos en variables en la cuenta de resultados.

El BPO puede ayudar a lanzar nuevas líneas de negocio al mercado de forma rápida. Subcontratando, se eliminan gastos de estructura y se gana en flexibilidad y capacidad de adaptación a cambios en el entorno. Se minimizan los costos en nuevas tecnologías eliminando inversiones en software y actualizaciones, sin renunciar a estar a la última. Mejoras en la calidad del servicio y se podrá evaluar objetivamente el cumplimiento las negociaciones previas.

CAPÍTULO 2 Estructura y operación de un Contact Center

De la visión que proporciona, los conceptos del CRM y BPO, se generaliza una estructura y forma de operación de un Contact Center, de esta forma puede determinar el tipo de soluciones a ofrecer, y en los sectores que se pueden aplicar comparado con el beneficio que presenta al cliente y/o usuario.

2.1 El Contact Center como solución de Tecnología

El Contact Center día a día se conecta con millones de consumidores con marcas líderes. De esta forma, se contribuye a que importantes empresas atiendan las crecientes demandas de sus clientes al tiempo que se mejora su eficiencia.

Se logra esto por medio de experiencias que generan valor a los clientes y las compañías. Estas experiencias se logran a través de un modelo único que combina personas, soluciones y canales.

El Contact Center debe mantenerse como el proveedor líder en soluciones, servicios y relaciones con clientes más importantes a nivel mundial. La fuerte presencia y capacidad operativa, permite mantener la operación de los clientes en mercados locales, así como ofrecer soluciones "**Nearshore***".

Un equipo, altamente motivado, es el motor fundamental que habilita nuestro modelo de negocios, siendo la mayor ventaja competitiva. Esto se refleja en la posición que actualmente tiene el propósito de ser la mejor empresa del sector CRM/BPO.

Un contact center es el punto de contacto entre el cliente y la empresa a través de medios de comunicación como la vía telefónica, el correo electrónico, el chat y la comunicación multimedia por Internet. Es la evolución del call center, donde solo existe un único punto de contacto: la línea telefónica **[5]**.

2.2 Misión, valor fundamental

Misión:

Contribuir al éxito de los clientes garantizando una mejor experiencia y apoyo en sus requerimientos de información y soluciones.

Valor Fundamental:

La cultura corporativa refleja la misión, valores y principios rectores. Éstos, determinan el comportamiento como compañía, enfatizan el trabajo en equipo, la innovación e inspiran a los colaboradores a trabajar con total dedicación a favor de nuestros clientes

2.2.1 Valores: compromiso, integridad y confianza

Compromiso:

Comprometido con el éxito de nuestros clientes.

Integridad:

Actuando con integridad, fiel a los valores corporativos, defendiendo creencias y asumiendo la responsabilidad de las acciones.

Confianza:

Garantizando la confianza, transparencia y respeto en las relaciones con todos los grupos de interés (clientes, empleados, proveedores, sociedad y accionistas).

2.3 Principios Rectores

Trabajo como un equipo, entendiendo las necesidades locales de los clientes pero con apoyo de las capacidades y escala multinacional.

Fomento de un espíritu emprendedor e innovador

Eficiencia, agilidad y enfoque en crear valor para nuestros clientes.

Agregando pasión en todo, con la ambición de siempre lograr metas y el deseo de ser mejores.

Disciplina financiera y operacional.

Construir un gran lugar para trabajar.

2.4 Sectores de competitividad

Telecomunicaciones

El sector de telecomunicaciones se encuentra en epicentro y a la cabeza de la revolución digital. Hoy más que nunca, las empresas de telecomunicaciones demandan un modelo diferenciado de compromiso con el cliente que les permita ofrecer atención a través de diversos canales digitales, mejorando así su satisfacción y reduciendo costes.

Diseñar estrategias innovadoras basadas en inteligencia de procesos empresariales y de clientes de alto nivel destinadas a fidelizar a los clientes y mejorar la eficiencia empresarial, ayudando a las compañías de telecomunicaciones a triunfar en un mercado cada vez más competitivo y maduro.

Servicios bancarios, financieros y aseguradoras

El sector financiero es uno de los pilares más importantes de la economía mundial, sin embargo, como todos los sectores, tendrá que adaptarse a un ambiente en constante evolución y crecimiento. La internacionalización y el panorama tecnológico de los últimos veinte años han cambiado por completo el escenario del sector financiero. La digitalización de la economía y el drástico cambio del perfil del cliente han transformado la forma de captar, atender y retener a los clientes en este sector.

En consecuencia, uno de los grandes retos para el sector financiero consiste en brindar acceso a la creciente oferta de productos financieros de una manera más eficiente a un mayor número de personas, garantizando a la vez la seguridad en la transferencia de información.

Salud

El sector salud mundial evoluciona con las estructuras demográficas y los niveles de vida de las distintas regiones, que exigen más servicios y de mejor calidad. En concreto, el acceso a servicios e información sobre salubridad a través de canales digitales, constituye una de las tendencias que más está afectando al sector. Ejemplos de ello son la consolidación del expediente clínico electrónico, la atención virtual y la vigilancia y atención simultáneas al paciente a través de la red, que generan mayor demanda por parte de los pacientes y de los profesionales de la salud.

Tecnología

La industria tecnológica es un pilar estratégico de la economía mundial que, a través de la innovación, transforma las industrias y propicia nuevos modelos transaccionales y de negocio. Los responsables de TI de las empresas se han convertido en los nuevos estrategas corporativos, mientras que tecnologías como el cómputo en la nube, Big Data y los medios sociales configuran el futuro de dichas empresas.

Son los actores de este sector los que deben colocarse a la cabeza de la innovación para evitar ser obsoletos y perder competitividad.

Comercio minorista y electrónico

Los hábitos de compra han cambiado y están altamente influenciados por internet y el auge del comercio electrónico. La conectividad ha cambiado la forma en que compramos y vendemos, y la forma en que vivimos y contamos nuestra experiencia. Las marcas están obligadas a maximizar las oportunidades y a reducir el número de competidores que surgen con estas nuevas formas de atraer clientes.

Existen más de 100 000 millones de compradores online en todo el mundo. Como en otros sectores, las ventas por internet ya representan más de la mitad de las ventas totales. Este tipo de interacción prioriza aspectos como la privacidad de los datos de carácter personal, el uso de dispositivos y plataformas y la innovación.

Bienes de consumo

El sector de bienes de consumo afronta varios retos debido a la proliferación de nuevos reglamentos en materia de consumo, el aumento de los impuestos y la generalización de problemas relacionados con la globalización y el impacto medioambiental. Un ejemplo de ello son las tendencias reguladoras en el ámbito de la alimentación y las bebidas que incluyen una revisión

minuciosa de aspectos como la composición nutricional, la restricción de productos químicos y conservantes y la presentación de datos específicos en el envase. Esto afecta a todo el sector y puede tener una gran repercusión para la atención al cliente y la eficiencia de los procesos de negocio. La clave del éxito está en mantener una buena estrategia de marketing y un excelente servicio de atención al cliente que permita una relación rentable y beneficiosa.

Gobierno

Como parte del entorno digital, los gobiernos y las administraciones públicas están obligados a prestar servicios públicos más eficientes y rentables a través del canal de comunicación más conveniente para los ciudadanos.

Los gobiernos y administraciones eficientes mejorarán el nivel de vida de la población mediante el suministro de procesos administrativos eficientes y la adopción de nuevas tecnologías.

Un Contact Center es un socio estratégico en la modernización de procesos emprendida por la administración pública para responder a las crecientes demandas de comunicación de los ciudadanos. Con los años, se han desarrollado soluciones a medida para la implementación de servicios administrativos electrónicos que ayudan a las instituciones públicas a interactuar y atender mejor a los ciudadanos.

Hotelería y turismo

El sector de hotelería y turismo es uno de los pilares de la economía mundial y ha registrado un crecimiento continuo durante las dos últimas décadas. Los ingresos que genera el sector lo colocan en el cuarto lugar por detrás del sector minorista y el sector público. Actualmente es un sector en expansión y una pieza clave para el progreso socioeconómico.

La ampliación de los destinos y la diversificación de la oferta han contribuido a su estabilidad. Además, se trata de un sector que ha sabido reaccionar positivamente al mundo digital para capitalizarlo a su favor. La compra de servicios online rebasa la venta tradicional, obligando a las compañías a invertir en nuevas tecnologías y en atención al cliente digital.

El servicio de atención al cliente es fundamental para el sector de hostelería y turismo, ayudando a grandes compañías a convertir servicios intangibles en experiencias integrales para esta industria tan exigente y en constante evolución. Convirtiendo la información en datos concretos y estratégicos para la toma de decisiones y esto genera un aumento de la lealtad y la satisfacción de los clientes finales.

Servicios Públicos

El sector de servicios públicos es uno de los que más rápido está evolucionando en el mundo. Debido en gran medida al proceso de la liberación y el desarrollo de la tecnología en los últimos 20 años, este sector opera en mercados altamente competitivos y cada vez más maduros. Por lo tanto, la atención al cliente y los índices de fidelidad se han convertido en factores competitivos decisivos frente a indicadores más tradicionales.

Comunicación y medios

Los medios de comunicación tradicionales están migrando hacia plataformas digitales. El consumo y producción de contenidos aumenta en espacios online y disminuye en formatos físicos.

Los sistemas de alta demanda y multiplataforma permiten personalizar la selección del contenido que debe tener un diseño interoperable, inmediato e interactivo.

La era digital obliga a los medios de comunicación tradicionales a romper paradigmas y apostar por nuevos modelos de negocio, plataformas y formatos de contenidos, expandiendo las experiencias de los usuarios a nuevos terrenos cada día.

Logística y transportes

Los gastos logísticos generan un déficit en las empresas producto de errores en la planificación, la gestión de inventarios, el almacenamiento, el transporte y la distribución. En países emergentes, los gastos logísticos suelen representar un gasto de las ventas.

Automotriz

La tecnología, la globalización, las nuevas formas de consumo y los hábitos de las nuevas generaciones han significado un cambio de paradigma para el mercado automotriz.

Fabricantes y proveedores se encuentran en un punto en el que la demanda de movilidad en las grandes ciudades está cambiando drásticamente. Por un lado, se cuenta con la influencia de la generación Y, con sus grandes expectativas, su conciencia medioambiental y su tendencia a depender menos del coche y más de los medios de transporte que ofrecen países desarrollados, como el transporte público y los carriles bici.

Por otro lado, están los consumidores con mayor poder adquisitivo que buscan nuevas experiencias y demandan automóviles más inteligentes. En última instancia, los fabricantes se ven obligados a innovar a través de la tecnología y de los nuevos esquemas de comercialización para responder a un mercado cambiante y competitivo.

Farmacéutica

El ecosistema de salud a nivel mundial afronta retos sumamente complicados. En concreto, el sector farmacéutico requiere innovación y desarrollo para garantizar la disponibilidad de los recursos que la población mundial necesita. Hoy más que nunca, este sector sufre una presión constante en términos de eficiencia, gastos y regulación. Al mismo tiempo, es un sector en constante crecimiento; según las previsiones, para 2017 el volumen de ventas del mercado de medicamentos habrá registrado un aumento del 21 % comparado con 2012.

Como resultado de estas tendencias, el consumidor demanda modelos más atractivos para acercarse a los productos y servicios que brinda el sector. El Contact Center ayuda a los laboratorios farmacéuticos a satisfacer esta demanda a través de experiencias integrales para sus consumidores, diseñadas para elevar el grado de satisfacción durante su interacción a través de los múltiples canales de comunicación.

2.5 Soluciones disponibles para esta industria: bancaria y aerolínea

En lo particular del proyecto se enfoca en las soluciones tecnológicas y de negocio ofertadas para los segmentos, bancarios y aerolíneas, pero derivado de la gran de demanda y el auge de centralizar los servicios en Contact Center, las soluciones a mencionar son aplicables para los sectores de competitividad que han sido revisados en el apartado **2.4** de este trabajo.

2.5.1 Ventas

Incrementar la conversión comercial garantizando la satisfacción, retención y lealtad de los clientes.

Esta robusta solución, incluye todas las etapas del proceso comercial; desde la identificación de prospectos, hasta las acciones de post-venta, maximizando oportunidades de negocio y entregando experiencias excepcionales a los clientes.

Apoyados sobre la plataforma de inteligencia de negocio y análisis; diseñar innovadoras estrategias que aceleran los procesos comerciales e incrementan los índices de conversión a costos eficientes. Para lograr esto, operamos y gestionamos nuestros procesos en tiempo real, lo que permite mayor control sobre las operaciones y la toma de decisión durante el ciclo de venta.

De igual manera, integrar y gestionar todo el proceso administrativo de la venta a través del canal adecuado para cada tipo de oferta; ya sea por teléfono, SMS (Short Message Service-Servicio de Mensajes Cortos), chat, e-mail, VPA (Virtual Personal Assistance) y/o cualquier combinación de estos de forma independiente o integrada para tener un enfoque más holístico **[4]**.

Canales Adicionales:

Puerta a Puerta (PaP): Venta activa de los productos o servicios de nuestros clientes. Los consultores van directamente al entorno del consumidor.

Punto de Venta (PdV): Promoción de los productos y/o servicios de nuestros clientes por medio de dinámicas de activación; degustación de productos, promociones, distribución de promocionales, gestión de anaqueles o venta directa en el punto de venta o de consumo.

SERVICIOS ADICIONALES

Canales:
- Plataformas de Omni y Multi Canal

Servicios de Valor Agregado:

-Monitoreo e interacción en rede sociales
- Inteligencia en Bases de Datos
- Encuestas

Automatización:
- Tele-mensajes
- IVR "Interactive Voice Response"
- Localización
- Verificación
- Calificación
- Documentos electrónicos

2.5.2 Atención a clientes

Principal canal de comunicación y relacionamiento entre una empresa y sus clientes.

El servicio de Atención al Cliente gestiona las llamadas recibidas y activas proporcionando información y atendiendo sugerencias, peticiones y reclamaciones relativas a los productos/servicios durante todo el ciclo de vida del cliente a través de múltiples canales.

Servicios orientados a la tipología de cliente: B2C (Business to Consumer), B2B (Business to Business), segmentación por perfiles (masivo, VIP, etc.).

Además, podrá incluir actividades de retención de clientes, consideradas valiosas fuentes de beneficios adicionales al negocio así como de información que aportarán valor a la empresa y le ayudarán en la toma de decisiones.

SERVICIOS ADICIONALES

Canales:
- Chat
- E-mail
- SMS
- APV (Atención Personal Virtual)

Servicios de valor añadido:
- Inteligencia de datos
- Encuestas
- Monitorización e interacción en Redes Sociales

Automatización:
- IVR
- Servicio de atención especial para sordos
- Documentos electrónicos

2.5.3 Soporte Técnico

Asistencia técnica inmediata al primer contacto.

Realizar el diagnóstico, análisis y resolución remota de problemas técnicos con rapidez y a través de diferentes canales de atención, reduciendo los costes y garantizando la satisfacción del cliente.

Para garantizar la resolución desde el primer contacto con el cliente (FCR – First Call Resolution), promoviendo su mayor satisfacción y evitando costes innecesarios, realizar la gestión de todos los procesos de soporte técnico de su empresa con la mayor calidad del mercado.

Como un único punto de contacto y cumpliendo con exigentes niveles de servicio SLA's (Service Level Agreemen- Acuerdo de Nivel de Servicio), resolvemos problemas, suministramos información técnica y efectiva sobre dudas en la instalación, uso y mantenimiento de productos y/o servicios, así como la gestión de los servicios de campo y centros de reparación.

SERVICIOS ADICIONALES

Canales:
- Chat
- E-mail
- SMS
- APV (Atención Personal Virtual)

Servicios de valor añadido:
- Encuestas
- Monitorización e Interacción en Redes Sociales

Automatización:
- IVR
- Servicio de atención especial para sordos
- Documentos electrónicos

2.5.4 Gestión de Reclamaciones

Comprensión y cumplimiento de las expectativas de los clientes de una forma oportuna con los más elevados niveles de calidad **[5]**.

Abordaje estratégico y ejecución de la gestión de reclamaciones que incluye prevención, recepción, análisis y tratamiento de reclamaciones en todos los canales y niveles de complejidad.

Prevención y gestión de los procesos de reclamaciones en todos los segmentos del mercado, en especial en aquellos sectores con más volumen, proporcionando asistencia y soluciones a las demandas de los clientes finales y las entidades reguladoras. El objetivo es reducir el número de reclamaciones y su repetición, incrementando la satisfacción del cliente.

- Procesos especializados
- Integración multicanal centrada en el comportamiento del cliente
- BPM social, gestión automática de la carga de trabajo, plataforma multicanal, interfaz con el software del cliente (CRM)
- Gestión del conocimiento, IVR inteligente

2.5.5 Servicios Presenciales / "Trade Marketing"

Integración experta de canales y tecnología para la entrega de mejores experiencias para el consumidor en los puntos de venta.

La solución de "Trade Marketing" apoya a las empresas en la ejecución de estrategias en los puntos de venta (POS) de acuerdo a las características de perfil del comprador y del canal más adecuado. Adaptar a la estrategia y necesidades de ventas y mercadotecnia de cada compañía.

Basados en un enfoque consultivo, definir la mejor estrategia Omni y/o Multi Canal para cada situación; actividades comerciales, atención a clientes, investigación, monitoreo de calidad y mercadeo. Analizar a detalle el perfil, la segmentación, el mercado objetivo, los indicadores y los procesos de los clientes para ofrecerles las mejores experiencias.

Utilizar tecnología móvil y las herramientas más sofisticadas para administrar equipos de trabajo, incrementando su productividad en tiempo real, de forma consistente, única y personalizada.

Un ejemplo de este tipo de soluciones es el Contact Center "Atento", que mantiene sus operaciones para líneas de negocio, desde el sector bancario, aerolíneas y servicios de telefonía, dando servicio a miles de usuarios diariamente en múltiples países, **ver Figura 2.1.**

Figura 2.1. Presencia de Atento en el mundo

2.5.6 Cobranza

Recobro de deuda temprana o tardía en un amplia variedad de segmento de productos

Servicio especializado en el recobro de impagados con experiencia en distintos sectores y productos que aúna el recobro de deuda reciente (amistosa) con deuda tardía (más de 60 días), a través de un modelo de retribución 100% variable para el pago a los agentes, y del uso de las más avanzadas herramientas que soportan una operación rentable y productiva.

- Solución end-to-end con procesos expertos e innovadores.

- Operación Centralizada y estructura de inteligencia dedicada, identificando el mejor momento de llamada y el mejor canal de contacto.

- Profesionales especializados en el nivel operacional, planificación y gestión.

- Análisis de datos, proporcionando la eficiencia de la estrategia multicanal.

2.5.7 "Back Office"

Garantía de productividad y calidad

Gestionar de manera eficiente todos los servicios administrativos y de soporte encaminados a ofrecer la mejor solución y mayor rentabilidad en su negocio **Back Office***. Contempla la

automatización de actividades rutinarias y repetitivas, realizando la gestión de información y procesos de negocio de gran volumen, como gestión de reclamaciones, análisis de crédito y riesgo, seguros y atención "post" complementaria a otros productos como SAC, Ventas y Soporte Técnico.

Actuar en diferentes sectores del mercado con conocimientos específicos de los procesos de cada uno de ellos, y a través de un abordaje consultivo, hacemos el mapeo y optimización de los mismos.

Proveer herramientas para automatización y control de productividad, como software Workflow BPM (Business Process Management), segmentación, priorización y distribución de procesos (Workload) y ECM (Electronic Content Management).

SERVICIOS ADICIONALES

Servicios de valor añadido:
- Inteligencia de datos
- Encuestas
- Monitorización e interacción en Redes Sociales

Automatización:
- IVR
- Servicio de atención especial para sordos
- Documentos electrónicos

CAPÍTULO 3 Introducción y generalidades de la infraestructura tecnológica de un Contact Center

El capítulo se enfoca en describir los componentes y arquitectura de la infraestructura tecnológica, equipos de comunicación y principales tecnologías en las cuales se fundamente su funcionamiento, así mismo se detalla para poder enfocar los conceptos y sea más comprensible el capítulo que está diseñado en las mejoras a los procesos de IT.

3.1 Soluciones de arquitectura IT para un Contact Center

Los Contact Center se comunican con los usuarios de diversas maneras, y dependiendo de qué lado inicie la comunicación se puede definir el tipo de Contact Center.

Se tiene un Inbound Contact Center cuando la comunicación es iniciada por el cliente. En estos sistemas el cliente buscará comunicarse con un representante de determinada compañía para obtener asistencia técnica o de emergencia, resolver dudas de facturación, entre otros.

Cuando el Contact Center es quien inicia la comunicación, se tiene un Outbound Contact Center. En la mayoría de casos la comunicación con el cliente se realiza solamente por medios telefónicos, tendiendo a tener una menor complejidad que en el caso anterior.

Son muchas las empresas que buscan implementar un Inbound Contact Center para mejorar las relaciones con sus clientes. Como ejemplo se podría considerar el caso de una Aerolínea que mediante sus diferentes canales de atención pueda resolver las inquietudes de los clientes sobre diversos vuelos y promociones así como un método eficiente de reserva y compra de boletos.

3.1.1 Call Center con arquitectura TDM (Time Division Multiple Access)

La multiplexación por división de tiempo es una técnica para compartir un canal de transmisión entre varios usuarios. Consiste en asignar a cada usuario, durante unas determinadas "ranuras de tiempo", la totalidad del ancho de banda disponible

La multiplexación por división de tiempo (Time Division Multiple Access o TDM) es una técnica que permite la transmisión de señales digitales y cuya idea consiste en ocupar un canal (normalmente de gran capacidad) de transmisión a partir de distintas fuentes, de esta manera se logra un mejor aprovechamiento del medio de transmisión. El Acceso múltiple por división de tiempo (TDMA) es una de las técnicas de TDM más difundidas.

Este modelo es una infraestructura de hardware sencilla donde el núcleo era una central PBX con la inteligencia para poder derivar la llamada entrante de un cliente a un pool de agentes (ACD-Automatic Call Distributor), **ver Figura 3.1**. Es la solución más simple para atención de clientes; sin embargo, algunos factores como el manejo de las colas de espera y reportes de gestión del sistema, lo convierte en un sistema con muchas limitaciones **[6]**.

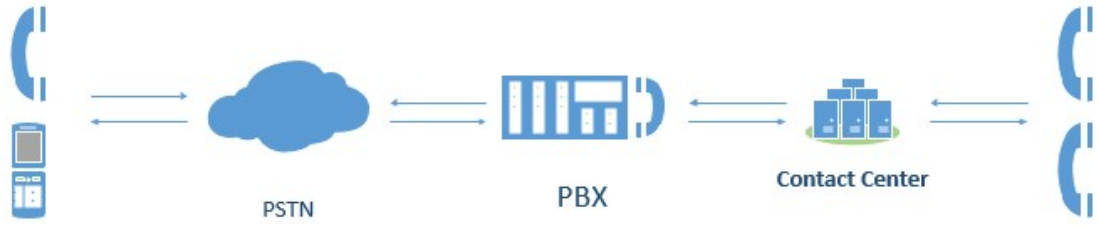


Figura 3.1. Arquitectura TDM de un Contact Center

3.1.2 Call Center con arquitectura CTI (Computer Telephony Integration)

Posteriormente se buscó la convergencia de voz y datos en los Contact Centers, obteniéndose así el modelo Computer Telephony Integration (CTI). En este modelo se cuenta con una mayor cantidad de elementos, siendo el principal, el Servidor CTI, que se encarga de enviar a los agentes del Call Center la información de los clientes en el momento que se produce la llamada.

Este modelo supera las limitaciones del modelo anterior; sin embargo no brinda facilidad para integrar mejoras, no pudiendo cubrir la necesidad naciente de atender nuevos canales de comunicación, **ver Figura 3.2**.

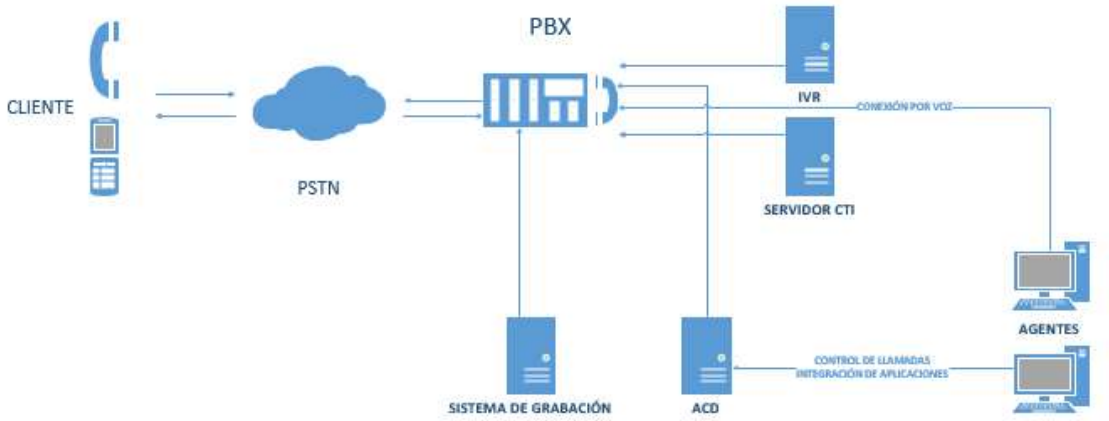


Figura 3.2. Arquitectura CTI de un Contact Center

3.1.3 Call Center con arquitectura IP

Debido al uso masivo de Internet y del comercio electrónico, la atención telefónica era cada vez la opción menos llamativa, al incrementarse la demanda de atender todos los canales de comunicación y poder ofrecer nuevas soluciones. Los clientes exigían nuevas vías de interacción con las organizaciones, y estás se vieron en la necesidad de habilitar nuevos canales de atención.

Los modelos de Call Center eran en ese momento muy rígidos, no se podían implementar nuevas mejoras fácilmente; es así que surge la necesidad de transformar estos modelos empleando tecnología IP para alcanzar la flexibilidad deseada, **ver Figura 3.3**. Este nuevo modelo permite, entre otras cosas, integrar los nuevos canales de atención, pasando a ser llamado Contact Center **[7].**

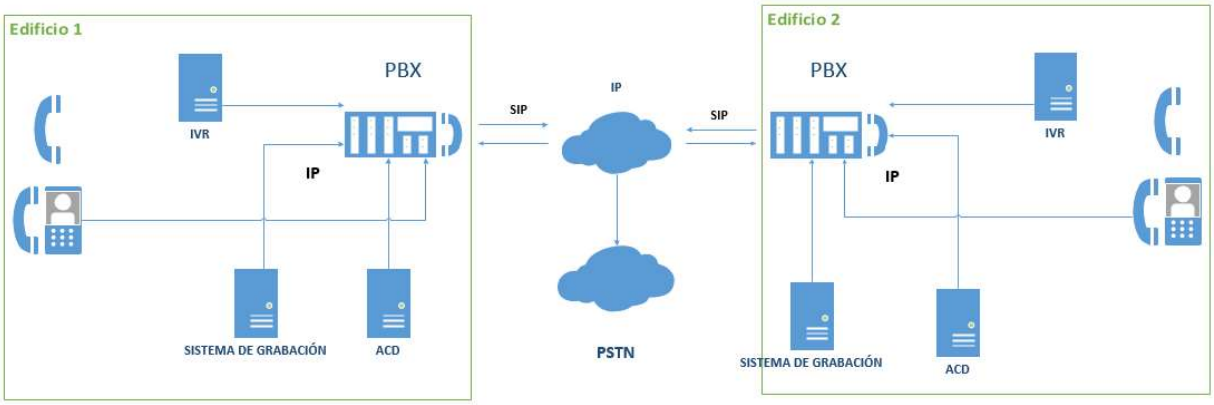


Figura 3.3. Arquitectura IP de un Contact Center

3.1.4 Contact Center Robusto

El Contact Center IP aprovecha los beneficios de las comunicaciones IP, incluyendo el hecho de que las comunicaciones de voz y de datos pueden ser enviados de manera eficiente a cualquier agente que tiene acceso a una conexión IP (banda ancha) por lo tanto la eliminación de la necesidad de la centralización del Contact Center, se vuelve ampliamente distribuida, se puede lograr a través de múltiples locaciones **[7]**.

Surgieron nuevas consideraciones en el diseño de los Contact Centers. Se requería de una plataforma de alta confiabilidad y disponibilidad que además realice el balanceo de carga entre los equipos responsables de las actividades críticas. Es así, como surge el Contact Center Robusto que, consiste en un sistema redundante que garantiza el funcionamiento de la plataforma en caso de fallas o sobrecarga. En algunos casos y dependiendo del servicio, puede llegar a requerirse un balanceador de cargas, **ver Figura 3.4**.

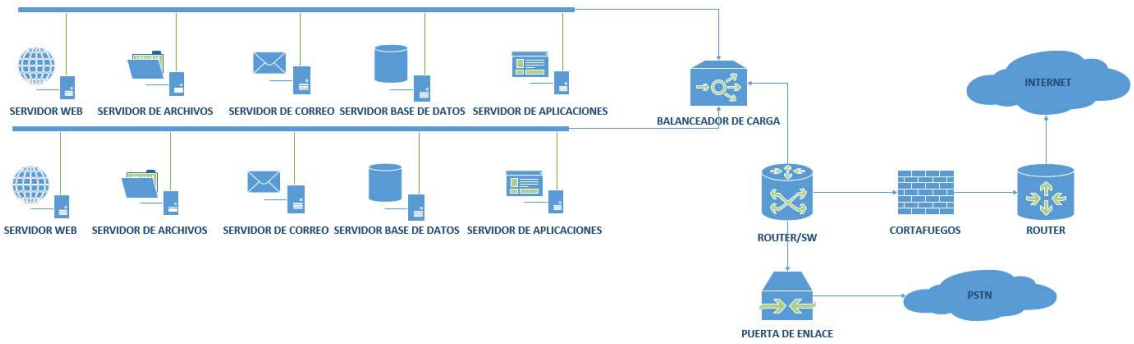


Figura 3.4. Arquitectura IP de un Contact Center Robusto, mostrando la redundancia

3.2 Infraestructura física del Contact Center

3.2.1 Estaciones de trabajo o posiciones de operador

Son los lugares de operación donde se ubican los agentes telefónicos para realizar su trabajo de interacción con los clientes. Este puesto debe constar de un cubículo, un PC, un teléfono y diadema. Para esto es necesario establecer el cableado que se utilizará en la organización.

El cableado de red de voz y datos debe soportar más de 100 Mbps y los equipos activos también deben soportar estas velocidades, aunque lo recomendable actualmente es un cableado que soporte VoIP (voice over IP- Voz sobre IP), así como el correspondiente cableado de energía eléctrica, de acuerdo a los estándares internacionales.

Esta característica del cableado permitirá ahorrar nodos en el mismo, ya que por una sola vía se tendrá voz y datos; o bien utilizar nodos dobles, teniendo algún respaldo en lugares críticos que así lo ameriten, **véase en la Figura 3.5** la distribución de las estaciones de trabajo de operaciones.

Figura 3.5. Distribución física de la infraestructura de un Contact Center

3.2.2 Cuarto de telecomunicaciones (MDF o Site)

"Main Distribution Frame" o "Marco de Distribución Principal" (en ocasiones denominado Site) es una estructura de distribución de señales para conectar equipo de redes y

telecomunicaciones a los cables y equipos que corresponden al proveedor de servicios de telefonía, Internet, entre otros.

El MDF es un punto final dentro de la central telefónica local donde el equipo y las terminaciones de bucles locales son conectados por un jumper. Todos los pares de cable de cobre que proveen de servicios a través de líneas telefónicas llegan al MDF y son distribuidos hacia los equipos dentro de la central, tales como repetidores y los routers utilizados por los proveedores de los servicios. Asimismo, los cables de los IDFs, es decir, de estructuras intermedias de distribución de señales, también deben terminar en el MDF **[8].**

Se define como el espacio dónde se ubican los equipos de telecomunicaciones comunes al edificio. Los equipos de esta sala pueden incluir centrales telefónicas (PBX), equipos informáticos (servidores), Centrales de video, etc. Sólo se admiten equipos directamente relacionados con los sistemas de telecomunicaciones, **véase en la Figura 3.6** los gabinetes donde se colocan los equipos de comunicación dentro del SITE o IDF.

Objetivos principales de un MDF/SITE:

- Establecer un cableado.
- Permitir la planeación e instalaciones.
- Establecer un criterio.
- Interconexión de los equipos de comunicación del edificio
- Se reciben los enlaces de comunicación de los proveedores
- Se colocan gabinetes para servidores o equipos de monitoreo

Figura 3.6. Cuarto de comunicaciones

3.2.3 Intermediate Distribution Frame (IDF)

"Intermediate Distribution Frame" o "Cuadro de Distribución Intermedia", es un cuarto con **rack*** de cables que interconecta y administra las telecomunicaciones entre el tráfico de un MDF y dispositivos de red. Los cables de una red en un edificio viajan a través de IDFs individuales conectados todos a un MDF o un SITE

Este tipo de cuarto aislado es de manera similar a la estructura de un SITE o MDF pero en menor escala, por lo donde regularmente se conectan Switches de comunicación hacia el SITE o MDF, esta conexión se pueda realizar mediante cable UTP o fibra óptica (FO). Los switches de comunicación abastecerán las estaciones de trabajo de los agentes. En la **Figura 3.7** se tiene la interconexión de varios IDF hacia el MDF.

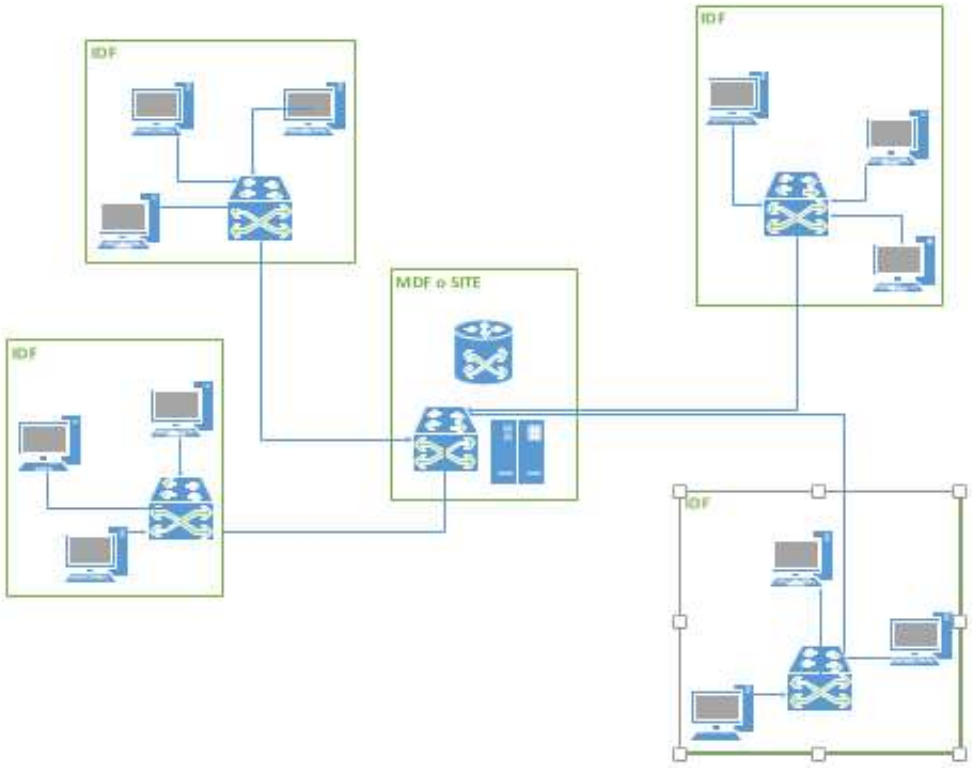


Figura 3.7. Diagrama de interconexión de un IDF hacia un SITE

3.3 Servidores

Un servidor o server, es un ordenador de alto rendimiento (high performance), que está al servicio de otros ordenadores. El servidor atiende y responde a las peticiones que le hacen los otros ordenadores. Los otros ordenadores, que le hacen peticiones, serán los "clientes" del servidor.

Un servidor, como la misma palabra indica, es un ordenador o máquina informática que está al "servicio" de otras máquinas, ordenadores o personas llamadas clientes y que le suministran a estos, todo tipo de información. A modo de ejemplo, imaginemos que estamos en nuestra casa, y tenemos una despensa. Pues bien a la hora de comer necesitamos unos ingredientes por lo cual vamos a la despensa, los cogemos y nos lo llevamos a la cocina para cocinarlos **[9].**

Precisamente se llaman servidores porque sirven cosas y están al servicio de otros ordenadores. Por ejemplo si se tiene un correo electrónico, se recibe de un servidor de correo electrónico, si se desea ver una página web, se recibe de un servidor web y así otros muchos servicios.

El modelo o arquitectura que siguen los servidores es el de cliente-servidor, es decir el cliente/s pide y el servidor proporciona los recursos o servicios, **ver Figura 3.8**.

Los servidores se utilizan para gestionar los recursos de una red. Por ejemplo, un usuario puede configurar un servidor para controlar el acceso a una red, enviar/recibir correo electrónico, gestionar los trabajos de impresión, o alojar un sitio web.

Un servidor debe estar siempre encendido, ya que si se apaga deja de dar servicio a las dependencias que lo utilizan. Cuando un servidor falla (se apaga o tiene errores) hace que los demás usuarios de la red tengan problemas, porque no disponen de los servicios que proporciona ese servidor. Dependiendo del servicio/rol que tiene el servidor, tiene que disponer de software (Roles) específicos capaces de ofrecer esos servicios.

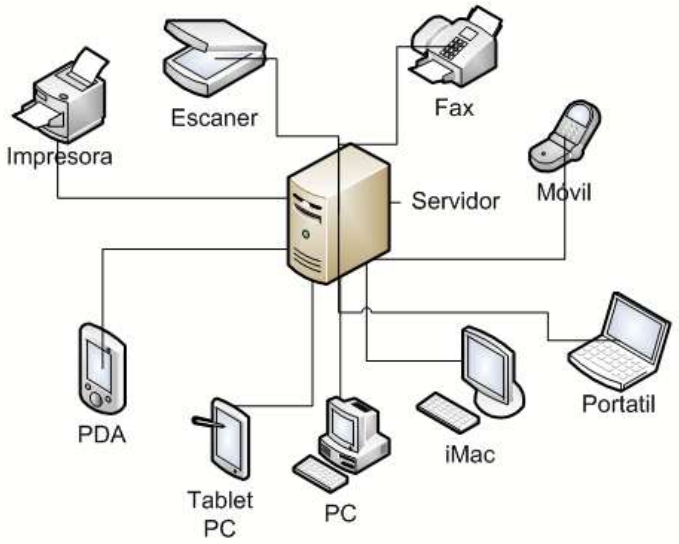


Figura 3.8. El servidor y los servicios/clientes que abastece

3.3.1 Servidor de Correo Electrónico o Mail Server

Es un ordenador dentro de una red que funciona como una oficina de correo virtual. Transfiere y almacena los mensajes de correo electrónico a través de una red.

Estos servidores tienen programas capaces de almacenar correos para los usuarios locales y con un conjunto de reglas definidas por el usuario que determinan cómo el servidor de correo debe reaccionar ante el destino de un mensaje específico la **Figura 3.9** muestra el icono de representación de un servidor de correo dentro de la herramienta Visio de Microsoft, software utlizado para realizar diagramas de red.

Normalmente estos servidores se dividen en otros 2 diferentes, una para el correo entrante y otro para el saliente:

Los servidores POP3 (Post Office Protocol- Protocolo de Oficina de Correo) retienen los mensajes de correo electrónico entrantes hasta que el usuario compruebe su correo y entonces los transfieren al equipo.

Los servidores SMTP (Simple Mail Transfer Protocol- Protocolo para Transferencia Simple de Correo) administran el envío de los mensajes de correo electrónico a Internet. El servidor SMTP administra el correo electrónico saliente y se utiliza en combinación con un servidor POP3 o IMAP de correo electrónico entrante.

Figura 3.9. Reconocimiento en un diagrama de red y de un servidor de correo

3.3.2 Servidor FTP

FTP (File Transfer Protocol- Protocolo Para la Transferencia de Archivos). FTP utilizan para realizar una transferencia segura de archivos entre ordenadores (envío de archivos de un sitio a otro). Los FTP garantiza la seguridad de los archivos y control de su transferencia, ver **Figura 3.10** de la representación de un Servidor FTP en Visio .

Por defecto FTP no lleva ningún tipo de encriptación permitiendo la máxima velocidad en la transferencia de los archivos, pero puede presentar problemas de seguridad, por lo que muchas veces se utiliza SFTP que permite un servicio de seguridad encriptada.

En este caso el cliente 1 envía una petición al servidor FTP para que le envíe un archivo al cliente 2. El servidor se lo envía y el cliente 2 lo recibe. Todo este proceso se realiza mediante un programa llamado FTP instalado en el cliente 1 y en el 2. El servidor dispondrá de otro programa (software) que se encargará de la recepción y el envío.

Este tipo de servidores se utilizan para subir archivos de páginas web a los servidores web, archivos de imágenes, videos, para hacer respaldo (backup o copias de seguridad), etc.

Figura 3.10. Reconocimiento en un diagrama de red y de un servidor FTP

3.3.3 Servidor Web o Web Server (ISS)

ISS (Internet Information Services- Servicios de información de Internet), es un servidor web y un conjunto de servicios para el sistema operativo Microsoft Windows. Originalmente era parte del Option Pack para Windows NT. Luego fue integrado en otros sistemas operativos de Microsoft destinados a ofrecer servicios, como Windows 2000 o Windows Server 2003. Windows XP Profesional incluye una versión limitada de IIS. Los servicios que ofrece son: FTP, SMTP, y **HTTP/HTTPS*.**

Almacena los archivos de una web del tipo HTML (HyperText Markup Language- Lenguaje de Marcas de Hipertexto) y los proporciona a los clientes que los solicitan haciendo la transferencia de los

archivos a través de la red mediante los navegadores. Los archivos HTML incluyen texto, imágenes, videos, etc., pero que sólo los navegadores pueden visualizar.

El servidor envía el archivo HTML al navegador del cliente para que lo pueda visualizar. El servidor, el navegador y la comunicación a través de la red seguirán unas normas llamadas "protocolo HTTP", **veáse la Figura 3.11** la representación de visio del servidor ISS.

Figura 3.11. Reconocimiento en un diagrama de red y de un servidor web

3.3.4 Servidor DHCP

"Dynamic Host Configuration Protocol" o "Protocolo de Configuración Dinámica de Host/Cliente", es un servidor que usa protocolo de red de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres.

Cuando un cliente se conecta a un servidor, éste tiene que identificar a cada cliente y lo hace con una dirección IP. Es decir, cuando desde uan casa se entra en una página web, se le identifica por una serie de dígitos que son la IP. Esta dirección IP son 4 pares de números y es única para cada cliente. Así el protocolo TCP/IP permite que cuando se conecta a internet se asigne una dirección IP que identifica a cada usuario. Por otro lado, DHCP es un protocolo de asignación dinámica de host que permite asignar una IP dinámicamente a cada cliente cuando este se conecta con el servidor que le da acceso a internet. Esto significa que si nos conectamos el lunes a internet, nuestra IP, que nos asigna Telefónica, puede ser 82.78.12.52. En cambio, si se conecta el jueves nuestra IP podría ser 212.15.23.88.

3.3.5 Servidor SIP

SIP (Session Initiation Protocol-Protocolo de Inicio de Sesiones). Se encargan de gestionar el establecimiento de las llamadas telefónicas por internet. Los SIP almacenan la dirección IP donde deben acceder para realizar la comunicación con un usuario. No transmite ni audio ni video, solo establece la comunicación.

La sintaxis de sus operaciones se asemeja a las de HTTP y SMTP, los protocolos utilizados en los servicios de páginas Web y de distribución de e-mails respectivamente. Esta similitud es natural ya que SIP fue diseñado para que la telefonía se vuelva un servicio más en Internet, véase en la **Figura 3.12**, el funcionamiento y el flujo de la información para SIP.

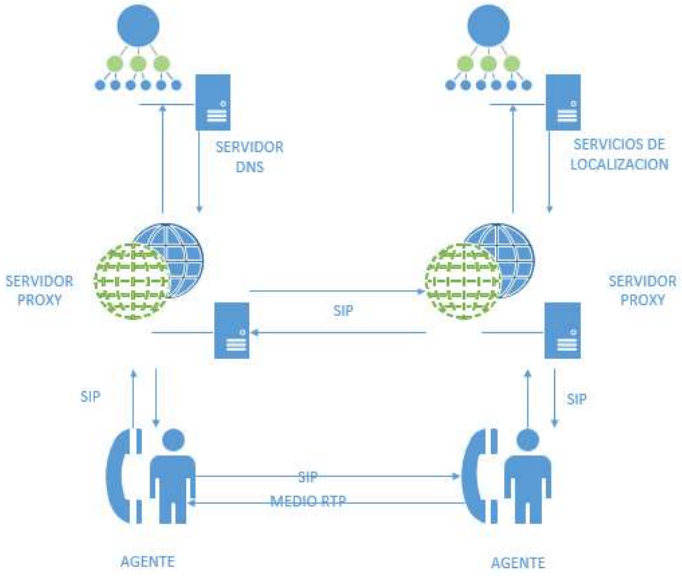


Figura 3.12. Arquitectura principal del funcionamiento de los servicios SIP

3.3.6 Servidores Cloud, Servidores en la "nube"

La computación en la nube, conocida también como servicios en la nube, informática en la nube, nube de cómputo o nube de conceptos (del inglés cloud computing), es un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es Internet.

Realmente estos servidores lo único que hacen es dejarte o alquilarte un espacio del servidor. La mayoría se utilizan para almacenar grandes cantidades de información en el servidor y tenerla protegida fuera de nuestro ordenador. Muchas empresas alquilan servidores cloud (en la nube) para tener en ellos toda la valiosa información de la empresa, utilizándola cuando quieran y realizando el propio servidor copias de seguridad, **ver Figura 3.13**.

Figura 3.13. Arquitectura de solución del funcionamiento de conexión a la nube

3.3.7 Cluster de Servidores

Un clúster de servidores es la agrupación de varios servidores dedicados a la misma tarea, Hay veces que un solo servidor se queda pequeño para toda la demanda de los clientes y es necesario más. En estos casos se agrupan en lo que se conoce como Cluster de Servidores**, ver Figura 3.14 [10]**.

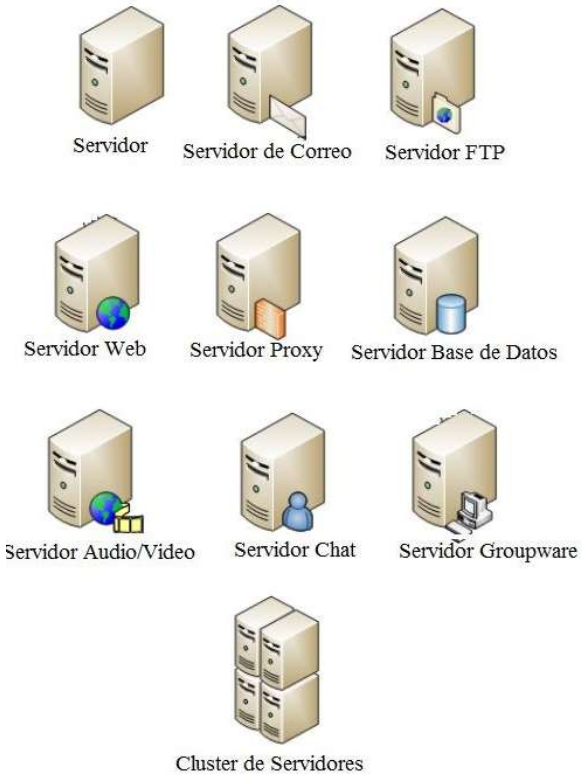


Figura 3.14. Servidor Cluster

3.3.8 Servidor de Base de Datos (BBDD)

Da servicios de almacenamiento y gestión de bases de datos a sus clientes. Una base de datos es un sistema que nos permite almacenar grandes cantidades de información. Por ejemplo, todos los datos de los clientes de un banco y sus movimientos en las cuentas.

Además estos servidores realizan tareas como el análisis de los datos, el almacenamiento, la manipulación de datos, y otras tareas específicas, véase en la **Figura 3.15**, la representación de un servidor de Base de Datos.

Figura 3.15. Reconocimiento en un diagrama de red y de un servidor de base de datos

3.3.9 Servidor de Dominio (DNS)

DNS (Domain Name System- Sistema de Nombres de Dominio), es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante es "traducir" nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente **[10]**.

El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

Los controladores de dominio almacenan datos y administran las interacciones entre el usuario y el dominio, como los procesos de inicio de sesión, la autenticación y las búsquedas de directorio, al igual se pueden regular para una red corporativa los permisos por usuario, en los cuales se establecen las restricciones por perfil de jerarquía que debiesen tener.

Esta configuración del servidor de dominio, así como la gestión de permisos se pueden realizar a través del rol de Active Directory (Directorio Activo), **ver Figura 3.16**.

Figura 3.16. Solución ofrecida por Microsoft para un Servidor de Dominio

3.3.10 Servidor de archivos (FileServer)

Un servidor de archivos es un tipo de servidor que almacena y distribuye diferentes tipos de archivos informáticos entre los clientes de una red de computadoras.

Su función es permitir el acceso remoto de otros nodos a los archivos que almacena o sobre los que tiene acceso. Desde el punto de vista del cliente de red de un servidor de archivos, la localización de los archivos compartidos es transparente, es decir, en la práctica no hay diferencias perceptibles si un archivo está almacenado en un servidor de archivos remoto o en el disco de la propia máquina.

Para robustecer esta solución de servidor se pueden utilizar roles apropiados dentro del servidor como lo son "File Server Resource Manager" o "Administrador de Recursos de Servidor".

3.3.11 Servidor de impresión

Un "servidor de impresión", o "Print Server" como también se lo conoce, es un servidor que se puede configurar, y de este modo hacer accesible cualquier impresora que conectemos a él desde todas las impresoras que sean parte de la red, es decir que básicamente permitirá a las computadoras en una red acceder a una misma impresora y poder distribuirlas mediante colas de impresión, este tipo de soluciones se pueden integrar con proveedores externos o software que sea capaz de realizar contabilidad de impresión e integraciones con el Directorio Activo del servidor DNS.

3.3.12 Servidores virtuales o Hyper-V

Se conoce como servidor virtual a una partición dentro de un servidor que habilita varias máquinas virtuales dentro de dicha máquina por medio de varias tecnologías.

Los servidores dedicados virtuales (SDV) usan una avanzada tecnología de virtualización, que le permite proveer acceso y la capacidad de reiniciarlo cuando desee, igual que un servidor dedicado. Con la posibilidad de instalar sus propias aplicaciones y controlar completamente la configuración de su servidor, los SDV representan una alternativa económica y eficiente para aquellos que desean disfrutar los beneficios de un servidor dedicado pero aun no poseen el presupuesto para hacerlo.

Cada SDV tiene asignado un límite del uso de la CPU (Central Processing Unit- Unidad Central de Procesamiento) y la memoria RAM (entre otros) que es dedicado sólo el de dentro del servidor. Así, cada uno de los SDV, funcionan independientemente dentro del mismo servidor físico; es decir que actúan como jaulas dentro de un mismo equipo. Por ejemplo, si uno de ellos está mal administrado y trabaja en forma sobrecargada, no afectará el funcionamiento del resto.

Hyper-V ofrece una infraestructura con la que es posible virtualizar aplicaciones y cargas de trabajo con objeto de alcanzar una serie de metas empresariales dirigidas a mejorar la eficacia y reducir costos, por ejemplo:

- Establecer o ampliar un entorno de nube privado. Hyper-V le ayuda a adoptar o ampliar el uso de recursos compartidos, así como a adaptar dicho uso en función de los cambios en la demanda, a fin de prestar unos servicios de TI más flexibles y a petición.

- Aumentar el uso del hardware. Al consolidar los servidores y las cargas de trabajo en un menor número de equipos físicos de mayor potencia, se puede reducir el consumo de recursos como la energía y espacio físico.
- Mejorar la continuidad empresarial. Hyper-V sirve para minimizar el impacto del tiempo de inactividad de las cargas de trabajo, tanto si está programado como si no.
- Establecer o ampliar una infraestructura de escritorio virtual (VDI). Una estrategia de escritorio centralizado con VDI contribuye a aumentar la agilidad empresarial y la seguridad de los datos y, al mismo tiempo, simplifica el cumplimiento de normas y la administración del sistema operativo y las aplicaciones del escritorio. Implemente Hyper-V y el host de virtualización de Escritorio remoto en el mismo equipo físico para poner a disposición de los usuarios escritorios virtuales personales o grupos de escritorios virtuales.
- Aumentar la eficacia de las actividades de desarrollo y prueba. Puede usar máquinas virtuales para reproducir diferentes entornos informáticos, sin necesidad de adquirir o mantener todo el hardware que, de otro modo, sería necesario.

3.4 Equipos de telefonía y configuraciones

3.4.1 Conmutador Telefónico (PBX)

Un PBX, es en realidad cualquier central telefónica conectada directamente a la red pública de telefonía por medio de líneas troncales para gestionar además de las llamadas internas, las entrantes y salientes con autonomía sobre cualquier otra central telefónica. Este dispositivo generalmente pertenece a la empresa que lo tiene instalado y no a la compañía telefónica, de aquí el adjetivo Privado a su denominación **[11].**

PBX es el acrónimo de Private Branch eXchange o Private Business eXchange. Identifica a las centrales privadas que se utilizan en las organizaciones o empresas para interconectar sus internos y para conectarse a la red telefónica a través de líneas externas. En los internos puede haber teléfonos, fax, módems y cualquier otro aparato capaz de conectarse a una línea telefónica. Inicialmente, la ventaja principal de las centrales privadas era el ahorro generado al evitar la utilización de la telefonía pública para llamadas internas. Posteriormente, con la popularización de los equipos, comenzaron a ofrecerse servicios adicionales que no estaban presentes en las redes telefónicas tradicionales como conferencia entre grupos, desvió de llamadas. En los últimos 15 años el concepto de conmutación de paquetes se fue imponiendo por sobre el concepto de conmutación de circuitos, dado que las empresas ya utilizan redes de conmutación de paquetes para el intercambio de datos y que la disponibilidad de Internet ha crecido al punto de considerárselo un servicio como cualquier otro. Es por ello que han surgido, entonces, las centrales telefónicas con capacidades de VoIP (Voz sobre IP). Existe, además, una tendencia que lleva a las empresas pequeñas a no querer generar su propia central telefónica, ya que los costos de comprar, mantener y administrar una central son elevados. Ha surgido a partir de esto el concepto de una central virtual (Centrex). Estas centrales están ubicadas en las oficinas del proveedor de telefonía y son gestionadas por el mismo proveedor, de modo que las empresas solo pagan por el servicio y no tienen que comprar y mantener el hardware de la central **[11]**.

Una central privada realiza como mínimo tres funcionalidades básicas:

- Establecer conexiones entre dos teléfonos. Esto implica establecer la relación entre un número y una línea, asegurarse de que la línea no este ocupada, etc.

- Mantener esas conexiones activas durante el tiempo que los usuarios lo deseen.
- Proveer información para contabilidad, como medición de las llamadas y tarifación.

Además de estas funcionalidades básicas, las centrales privadas suelen ofrecer una gran cantidad de características adicionales, que dependen del fabricante y el modelo de la central en cuestión. En los casos de las funcionalidades más complejas, la central ofrece la posibilidad de conectarse con un equipo adicional que es el que provee las características en sí. Las capacidades adicionales más comunes son:

- **Llamada en espera**, permite que cuando un interno se encuentra ocupado, sea notificado de que hay otra llamada esperándolo. Una vez notificado, el usuario puede poner en espera a la llamada actual para atender la segunda llamada.
- **Desvió de llamadas** es la capacidad de desviar todos los llamados que se dirijan a un determinado interno a otro teléfono. Según la central de la que se trate, puede limitarse a otro interno o puede permitirse un desvío a un número externo.
- **Transferencia de llamadas** es la capacidad de transferir un llamado a otro interno. Esta transferencia puede realizarse con un anuncio intermedio.
- **Conferencia** es la capacidad de vincular tres o más internos (o externos) entre sí, de manera que se realiza una conferencia telefónica. La cantidad máxima de participantes en una llamada de conferencia varía según el tipo de central.
- **Preatendedor** es el servicio que permite que los usuarios externos que realicen una llamada puedan discar el número del interno con el que se quieren comunicar y sean transferidos directamente sin tener que pasar por una operadora.
- **Discado directo a extensión** es la característica que permite que una empresa tenga más números telefónicos asignados que líneas externas reales, de manera que a cada interno le corresponda una numeración de la **PSTN***, si bien no se cuenta con esa cantidad de líneas. Para ello, el proveedor de telefonía debe anunciarle a la central cuál es el número que se ha discado, de modo que la central pueda realizar la transferencia correctamente. 5 Este tipo de conexiones se realizan generalmente a través de conexiones de tipo E1/T1 que permiten la utilización de canales de voz y canales de control entre la central telefónica pública y la privada.
- **Conteo de llamadas** es la capacidad de almacenar información sobre las llamadas realizadas y su duración. Esta característica suele utilizarse para realizar la tarifación.
- **Auto discado** es la capacidad de **discar*** un número y automáticamente dejar un mensaje en ese número, sin la participación de una persona.
- **Rellamado automático** es la capacidad de avisarle a un usuario que llamó a un número que estaba ocupado, que el número está disponible. Esta solución se puede realizar mediante la integración de un proveedor externo, ejemplo, la solución Virtual Hold.

3.4.1.1 Interactive voice response (IVR)

Es el servicio que permite a un usuario navegar a través de distintos menú de información utilizando reconocimiento de voz, o de tonos. Suelen utilizarse para servicios de soporte o de información, proveyendo a los usuarios de los datos necesarios para comunicarse con el operador correcto, o directamente para obtener la información deseada sin la intervención de un operador. Dada la complejidad que puede llegar a tener este servicio, muchas veces se requiere un equipo adicional. Se puede ejemplificar el funcionamiento de un IVR de la siguiente forma: en el Centro de Atención al Cliente del banco "ABC" se recibe un gran número de llamadas para realizar consultas

referentes a saldos bancarios. El cliente desea saber en este tipo de consultas el saldo de su cuenta bancaria, para verificar si se han hecho los depósitos o retiros correspondientes. El agente del Centro de Llamadas le solicita su número de cuenta, y una clave personal para evitar brindar información confidencial a personas no autorizadas. Los datos son ingresados por el agente en su ordenador, el que le indica en la pantalla el dato solicitado. El agente le informa al cliente su saldo y la conversación termina.

Este tipo de consultas rutinarias pueden ser automatizadas mediante un IVR. Este equipo dispone de interfaces que le permiten reconocer dígitos DMTF (Dual-Tone Multi-Frequency- El Sistema de Marcación por Tonos), en algunos casos también puede reconocer comandos hablados, es capaz de reproducir frases pregrabadas (completas o combinadas) y hablar texto.
De esta manera, el IVR puede solicitar al cliente que digite su número de cuenta y clave o PIN a través del teclado de su teléfono. Los datos son reconocidos por el IVR, el que realiza una consulta al sistema informático del Banco, verificando los mismos y recuperando el saldo del cliente. El saldo es hablado, componiendo la frase "Su saldo es de – Cinco - mil - Quinientos - Cuarenta - y - Ocho – pesos - con - treinta - y - cinco - centésimos". Si el sistema de IVR está bien diseñado y si las frases son bien grabadas, la voz resultante puede llegar a ser de muy alta calidad de una pronunciación muy amigable, **ver Figura 3.17** para ver la interconexión entre el PBX e IVR.

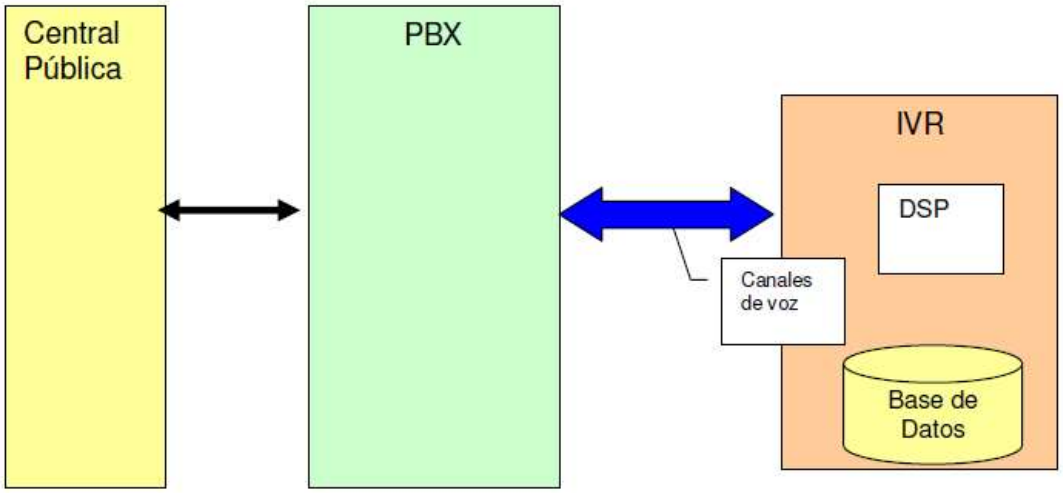


Figura 3.17. Diagrama de funcionamiento de un PBX

3.4.1.2 Distribución automática de llamados (ACD Automatic Call Distribuitor)

Es la capacidad de distribuir llamados entrantes a un grupo de internos. Utilizada principalmente en centros de atención o de venta, en los cuales la persona que llama no requiere hablar con un operador en particular, sino con el que éste disponible lo antes posible.

A continuación se enumeran las funcionalidades y beneficios más importantes de un ACD:

- Aplica inteligencia de negocio al tráfico de llamadas entrantes, asignando las llamadas a colas y distribuyéndolas de forma efectiva a los agentes en espera.

- Agiliza la administración de llamadas con tres algoritmos de enrutamiento: circular, lineal y de agentes a grupos de trabajo.
- Incluye mensajes de aviso de espera, que se emiten a intervalos programados para llamadas en espera y a clientes en una cola.
- Soporta un número ilimitado de supervisores.
- Permite una mejor interacción con el cliente y tiempos de aprendizaje reducidos, al proporcionar una supervisión discreta de la actividad de los agentes para garantizar la calidad.

Con esta solución profesional, las pequeñas y medianas empresas pueden mejorar de forma decisiva tanto sus servicios de atención telefónica y de bienvenida, como los relacionados con éstos. A continuación enumeramos aspectos importantes:

- Un ACD mejora de los niveles de servicio al cliente y tiempos de respuesta.
- Permite la reducción de niveles de llamadas no atendidas.
- Acelerar los tiempos de respuesta a las llamadas.

3.4.1.3 DISA

DISA (Direct Inward System Access- Sistema Interno de Acceso Directo), permite atender las llamadas con un mensaje vocal que invita a digitar el interno deseado. Si el llamante digita un interno, la llamada es dirigida en forma automática (sin intervención de una operadora) al interno deseado. Si no se digita ningún interno, la llamada es dirigida en forma automática a un lugar predeterminado (usualmente la telefonista). Esta facilidad es también llamada "Operadora Automática" o "Automatic Attendant", y no requiere de ningún servicio especial por parte del operador telefónico.

3.4.1.4 DID

El servicio de DID o Direct Inward Dial, Discado Directo Entrante, permite acceder desde la red pública directamente a un interno de la PBX. Para ello, la red pública provee a la empresa de un número abreviado (usualmente de 4 dígitos), al que le puede seguir cualquier número de interno de la PBX. Por ejemplo, si el número abreviado es 1234 y el número de interno es 555, desde la red pública se podrá discar 1234555, y la llamada será dirigida en forma automática al interno 555, sin intervención de la telefonista ni de ningún mensaje. En el servicio DID, por el contrario, el número deseado (incluido el interno) se digita en forma completa, sin pausas y sin esperar mensajes. La central pública recoge todo el número, y mediante un protocolo de señalización con la PBX, le reenvía los últimos números correspondientes al interno. La PBX a su vez le informa a la central pública el estado del interno solicitado (libre, ocupado, fuera de servicio, etc.). La llamada es establecida en el momento en que el interno contesta.

3.4.1.5 CTI

Las facilidades de CTI (Computer Telephony Integration- Integración de Telefonia Computarizada) permiten integrar los sistemas telefónicos e informáticos. A través de vínculos de

datos entre los servidores informáticos y las PBX es posible integrar, a nivel de señalización y control, el teléfono con las aplicaciones informáticas.

Desde las aplicaciones es posible controlar al teléfono (atender, cortar, conectarse (login), desconectarse (logout), no disponible, etc.)

Asimismo, permiten "sincronizar" la recuperación de datos en las aplicaciones de los ordenadores de los agentes con el ingreso de cada llamada. El grado de "integración" de los servicios de Internet en los Centros de Contactos es cada vez mayor, comenzando con la recepción de solicitudes vía e-mail, hasta la atención en vivo, con aplicaciones multimedia sobre Internet. Dentro de las funciones de los Centros de contactos se destacan:

- Email routing: Los correos electrónicos enviados por los clientes a cuentas genéricas (por ejemplo soporte@empresa.com) son automáticamente procesados y presentados a los agentes.

- Chat o mensajería instantánea: Los clientes pueden solicitar el inicio de una conversación escrita por medio de sistemas de "mensajería instantánea". La solicitud es encolada y distribuida a los agentes

- Web Collaboration o colaboración en Internet: Los clientes que navegan por las páginas corporativas pueden solicitar asistencia en línea.

- Video: Permite que el cliente y el agente establezcan una llamada de voz y video.

- Redes Sociales: La comunicación por Facebook, Twitter y otras redes sociales es necesaria para poder garantizar la atención a los clientes.

3.5 Sistemas de grabación

Existen contactos telefónicos que implican el establecimiento de compromisos recíprocos entre el agente y la persona que lo contacta. Para aquellos clientes del Call Center que por razón de su actividad requieren esta capacidad es necesario realizar la grabación de llamadas cursadas y su almacenamiento y custodia para cuando la situación lo amerite. Esta facilidad tecnológica protege al Cliente del Call Center de reclamos posteriores permitiéndole determinar exactamente los componentes adquiridos y la aceptación de los mismos.

Esta tecnología consiste en una grabación digitalizada de las conversaciones del agente en comunicaciones salientes y entrantes, en discos duros de PC's y directorios a elección, según diversos criterios.

Es imprescindible para control de personal, supervisión de calidad de atención, rendimiento y resguardo de información. Es también un recurso de capacitación y perfeccionamiento que permite detectar defectos y errores, manteniendo registros de desempeño en archivos digitales de audio.

Algunos beneficios de esta tecnología es poder escuchar a los agentes al dirigirse a los clientes: conocer su tono de voz, sus errores, aciertos, entre otras variables de interés. De esta manera se conoce dónde se debe reforzar mediante capacitación, dónde a través de correctivos y dónde amerite despido.

Los sistemas de grabación pueden activarse automáticamente, por programa o por un comando del operador.

Ejemplos del uso de esta función son:

- Control de calidad de la atención de los clientes por parte del operador.
- En aquellos casos donde el CALL CENTER es utilizado para recibir pedidos, reclamos, dar órdenes (pagos, transferencias bancarias, etc.), emergencias, etc, para resolver posibles conflictos

La **Figura 3.18** muestra las siguientes funciones de grabación de llamada, en la cual se le puede denominar "grabación por troncal", la cual consiste en colocar los equipos de grabación en espejo a los enlaces de comunicación o de algún puerto de algún de un Switch donde se conectan las extensiones analógicas de los operadores, y estar grabando todo el tráfico que pasa por estos medios. El sistema de grabación tiene la capacidad de discriminar los protocolos y puertos específicos para grabar solo las llamadas telefónicas, este tipo de grabación puede llegar a tener un eficiencia del 97 %, variando de acuerdo al proveedor contratado para el sistema.

Por ejemplo en el caso del proveedor NICE, permite la grabación por extensión puntual convergida por la compra de licenciamiento previo, la cual se configura puntualmente en el equipo interesado a grabar.

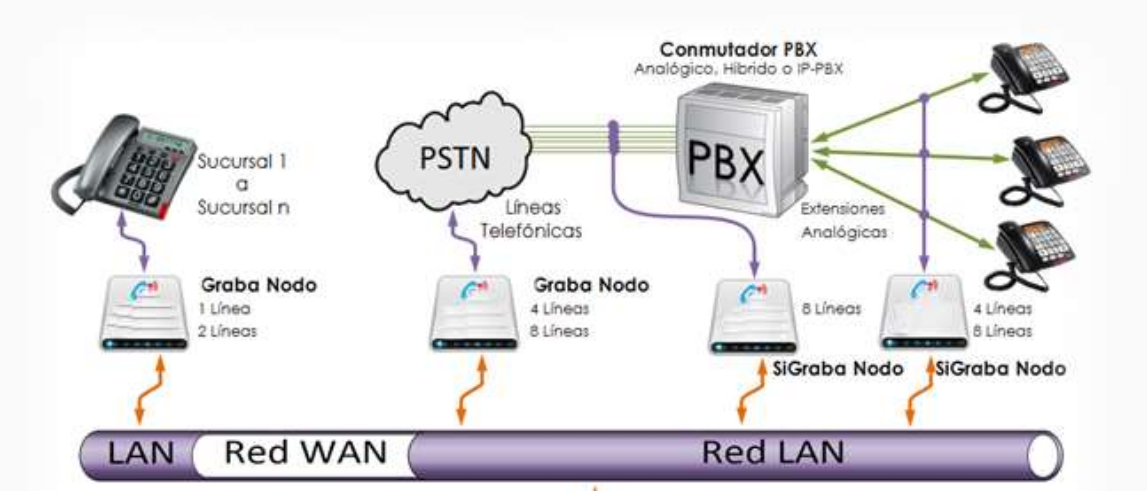


Figura 3.18. Diagrama de conexión de sistema de grabación

3.6 Sistemas de marcadores predictivos

Es como un verdadero robot telefónico, que disca un número telefónico indicado, evitando al agente este trabajo.

Un servidor de administración de listas distribuye registros de llamadas a la aplicación de la gente a petición de este. Utilizando una interfaz el agente obtiene una vista previa de la información del cliente a ser contactado e inicia la llamada saliente. Una vez finalizada o durante la llamada, el agente puede actualizar la información de la gestión o actualización de datos del cliente, la **Figura 3.19**, muestra el ejemplo de una solución de marcación predictiva.

3.6.1 Marcación progresiva

Cuando los contactos se establecen por medio de llamadas originadas en el Contact Center es un factor muy importante y crítico el tiempo asociado con la marcación telefónica. Para disminuir estos tiempos, evitar errores y detectar situaciones de contacto no efectivo:

- No contesta
- Ocupado
- Atendieron
- Contestador Automático
- Fax
- Teléfono dañado

Esta utilización, que representa un aumento de la eficiencia en el proceso de establecimiento del contacto, se traduce en beneficios tangibles para el Cliente del Contact Center al aumentarse el número de contactos efectivos por unidad de tiempo y por lo tanto, dando la posibilidad de aumentar la eficiencia de los agentes.

El modo progresivo garantiza que un agente este disponible para todas las llamadas de clientes activos. El servidor efectúa activamente las llamadas salientes, activa la detección de progresión de todas las llamadas y transfiere las llamadas conectadas a agentes disponibles.

3.6.2 Marcación predictiva

En este modo se activa un algoritmo predictivo. El servidor supervisa la actividad de los agentes, recoge estadísticas y predice el tráfico futuro de llamadas. En este modo de marcación, el servidor puede efectuar más llamadas que agentes disponibles haya en el grupo. En este caso pueden abandonarse algunas llamadas establecidas. El algoritmo se basa en dos parámetros de optimización:

- Tasa de sobre-llamada

El número de llamadas realizadas se calcula a partir del porcentaje de llamadas establecidas que no se han transferido a un agente libre.

- Factor de ocupado

El número de llamadas realizadas depende del porcentaje especificado para el tiempo de ocupado del agente.

El marcador predictivo apoya a los Contact Center en la realización de las llamadas salientes para aquellas empresas que tengan un alto número de llamadas por realizar. Por lo tanto genera acciones consecuentes, sin intervención del agente. Con esta aptitud consigue varios beneficios:

- Reducción de Tiempos.
- Eliminación de acciones improductivas a cargo del agente.

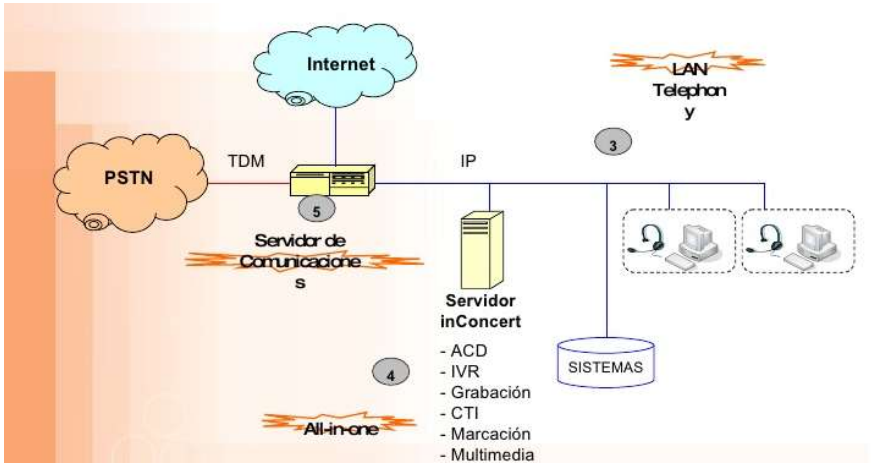


Figura 3.19. Ejemplo de solución de Marcador Predictivo Inconcert

3.7 Switch

Un switch o conmutador es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una LAN (Red de Área Local) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3 [Ver Anexo 3-Eterneth) **[15].**

En la actualidad las redes locales cableadas siguen el estándar Ethernet, donde se utiliza una topología en estrella y donde el switch es el elemento central de dicha topología, **ver Figura 3.20.**

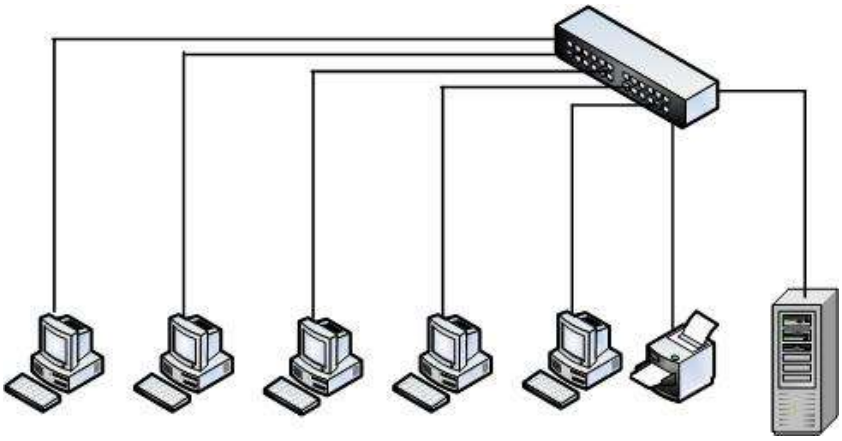


Figura 3.20. Topología en estrella de las redes locales en la actualidad

La función básica de un switch es la de unir o conectar dispositivos en red**.** Es importante tener claro que un switch **no** proporciona por si solo conectividad con otras redes, y tampoco proporciona conectividad con Internet, para ello es necesario un router, **véase en el apartado 3.8**.

Como se observa en la **Figura 3.21**, la existencia de la red local permite:

- **Compartir archivos**. Un equipo de la red habilita la compartición de archivos y el resto de equipos pueden acceder a dichos archivos a través de la red.
- **Compartir impresoras**. Todos los equipos de la red pueden utilizar la misma impresora.
- **Compartir la conexión a Internet**. Todos los equipos pueden acceder a Internet a través de router de acceso, que está conectado en la red.

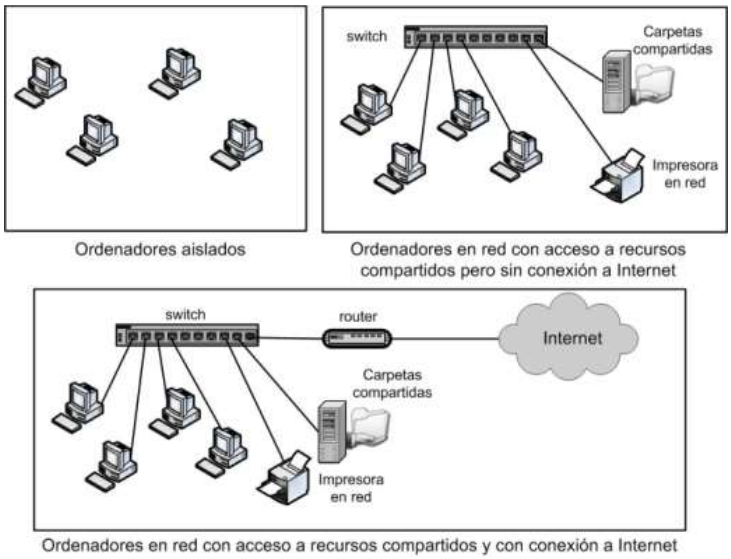


Figura 3.21. Como se puede utilizar un Switch

3.7.1 Características básicas de los switches

3.7.1.1. Puertos

Los puertos son los elementos del switch que permiten la conexión de otros dispositivos al mismo. Como por ejemplo un PC, portátil, un router, otro switch, una impresora y en general cualquier dispositivo que incluya una interfaz de red Ethernet. El número de puertos es una de las características básicas de los switches.

El estándar Ethernet admite básicamente dos tipos de medios de transmisión cableados: el cable de par trenzado y el cable de fibra óptica**.** El conector utilizado para cada tipo lógicamente es diferente así que otro dato a tener en cuenta es de qué tipo son los puertos. Normalmente los switches básicos sólo disponen de puertos de cable de par trenzado (cuyo conector se conoce como RJ-45) y los más avanzados incluyen puertos de fibra óptica (el conector más frecuente aunque no el único es el de tipo SC), **ver Figura 3.22**.

Figura 3.22. Switch con puertos RJ-45 y SC

3.7.1.2 Velocidad

Dado que Ethernet permite varias velocidades y medios de transmisión, otra de las características destacables sobre los puertos de los switches es precisamente la velocidad a la que pueden trabajar sobre un determinado medio de transmisión. Podemos encontrar puertos definidos como 10/100, es decir, que pueden funcionar bajo los estándares 10BASE-T (con una velocidad de 10 Mbps) y 100BASE-TX (velocidad: 100 Mbps). Otra posibilidad es encontrar puertos 10/100/1000, es decir, añaden el estándar 1000BASE-T (velocidad 1000 Mbps). También se pueden encontrar puertos que utilicen fibra óptica utilizando conectores hembra de algún formato para fibra óptica. Existen puertos 100BASE-FX y 1000BASE-X**.**

Por último, los switches de altas prestaciones pueden ofrecer puertos que cumplan con el estándar 10GbE, tanto en fibra como en cable UTP.

3.7.1.3 Puertos modulares: GBIC y SFP

La mayor parte de los switches de gamas media y alta ofrecen los llamados puertos modulares. Estos puertos realmente no tienen ningún conector específico si no que a ellos se conecta un módulo que contiene el puerto. De esta forma podemos adaptar el puerto al tipo de medio y velocidad que necesitemos. Es habitual que los fabricantes ofrezcan módulos de diferentes tipos con conectores RJ-45 o de fibra óptica. Los puertos modulares proporcionan flexibilidad en la configuración de los switches.

Existen dos tipos de módulos para conectar a los puertos modulares: el primer tipo de módulo que apareció es el módulo **GBIC** (*Gigabit Interface Converter*) diseñado para ofrecer flexibilidad en la elección del medio de transmisión para Gigabit Ethernet. Posteriormente apareció el módulo **SFP** (*Small Form-factor Puggable*) que es algo más pequeño que GBIC (de hecho también se denomina **mini-GBIC**) y que ha sido utilizado por los fabricante para ofrecer módulos tanto Gigabit como 10GbE en fibra o en cable UTP, **ver Figura 3.23.**

Figura 3.23. Puertos modulares SFP y GBIC

3.7.2 Power Over Ethernet

Power Over Ethernet (*Alimentación eléctrica por Ethernet*), también conocido como PoE, es una tecnología que permite el envío de alimentación eléctrica junto con los datos en el cableado de una red Ethernet. La primera versión de esta tecnología se publicó en el estándar IEEE 802.3af en 2003 y en el año 2009 se publicó una revisión y ampliación en el estándar IEEE 802.3at**.**

La tecnología PoE permite suministrar alimentación eléctrica a dispositivos conectados a una red Ethernet, simplificando por tanto la infraestructura de cableado para su funcionamiento. Un dispositivo que soporte PoE obtenien tanto los datos como la alimentación por el cable de red Ethernet**.**

Los dispositivos que utilizan esta característica son puntos de acceso inalámbricos Wi-Fi, cámaras de video IP, teléfonos de VoIP, switches remotos y en general cualquier dispositivo que esté conectado a una red Ethernet, que no tenga un consumo energético muy elevado y que su ubicación física dificulte la instalación de cableado.

3.7.3 Conmutación

La función básica que realiza un switch se conoce como conmutación y consiste en trasferir datos entre los diferentes dispositivos de la red. Para ello, los switches procesan la información contenida en las cabeceras de la trama Ethernet.

Sin entrar mucho en detalle en el funcionamiento de Ethernet se puede decir que Ethernet es una tecnología de transmisión de datos para redes locales cableadas que divide los datos que se tiene que transmitir en tramas y a cada trama se le añade una determinada información de control llamada cabecera. Dicha cabecera contiene la dirección MAC (Media Access Control- Control de Medio de Acceso) tanto del emisor como del receptor.

Los switches guardan en una tabla las direcciones MAC de todos los dispositivos conectados junto con el puerto en el que están conectados, de forma que cuando llega una trama al switch, dicha trama se envía al puerto correspondiente.

3.7.3.1 Gestión y configuración

La función básica que llevan a cabo los switches, que es la conmutación de tramas Ethernet, no necesita ninguna configuración manual. Una de las características incluídas en el estándar Ethernet (concretamente en la especificación IEEE 802.3u) es la autonegociación. Esta función permite que se establezca un diálogo entre el switch y cualquier equipo que se conecte a uno de sus puertos para que "negocien" los parámetros de la comunicación de forma transparente al usuario.

Sin embargo, las funciones avanzadas que ofrecen algunos modelos (como por ejemplo, la configuración de redes **VLAN**[**]) sí requieren una configuración manual. A los switches que proporcionan mecanismos de configuración y gestión se les conoce como switches gestionables.

El acceso a la configuración de dichos switches se puede hacer, o bien por un puerto especial de configuración, o por un servicio web interno que proporciona el propio switch. En el primer caso, es necesario conectar un PC a dicho puerto y acceder mediante algún software específico (como por ejemplo un programa de terminal de comandos). En el segundo caso basta con utilizar un navegador web en algún PC conectado en un puerto Ethernet del switch. El acceso a la interfaz de configuración del switch requiere que se configure en el mismo una dirección IP dentro del rango de la red donde esté conectado, **ver Figura 3.24.**

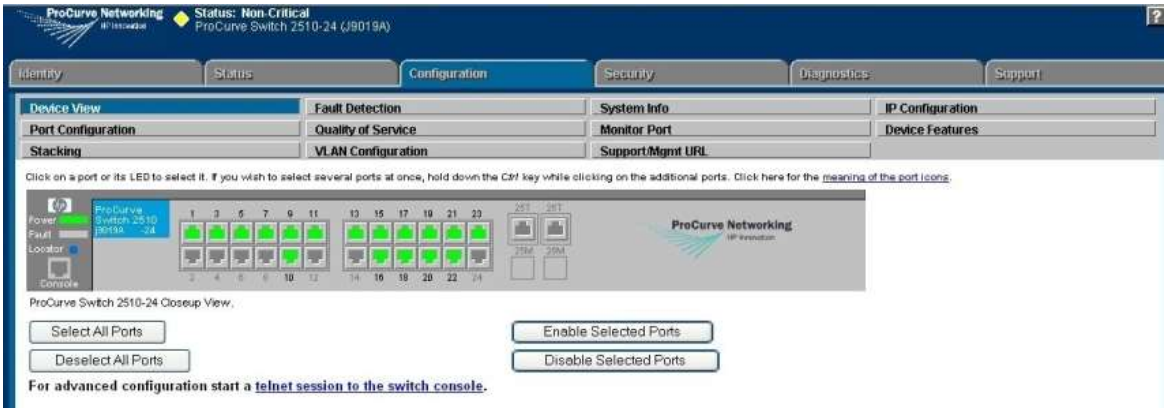


Figura 3.24. Pantalla de configuración de un switch gestionable

Algunas de las características que suelen incluir los switches gestionables son:

- Gestión de VLAN
- Monitorización de puertos (Port Mirroring)
- Agregación de enlaces (Link Aggregation / Port Trunking)
- Seguridad IEEE 802.1X
- Control de bucles: Spanning Tree

3.7.4 Switches de Nivel 3 y Nivel 3 / 4

Los switches de gama alta utilizados en el troncal de redes Ethernet de mediana y gran envergadura suelen ofrecer capacidades de enrutamiento de paquetes IP. A este tipo de switches se le conoce como switches de nivel 3. Un switch de nivel 3 realiza todas las funciones de

conmutación de un switch pero además proporciona funciones de enrutamiento IP. Esta característica es especialmente útil para switches que utilicen VLAN y necesiten comunicar algunas de sus redes LAN virtuales. Además, pueden existir switches que ofrezcan características relacionadas con funciones del nivel 4, como control de puertos. A estos switches se le conoce como switches de nivel 3 / 4.

3.7.5 Arquitectura de las redes Ethernet

Las redes actuales basadas en Ethernet siguen una topología en estrella donde el elemento central es el switch. En los casos en los que el número de equipos supera la capacidad del switch, es posible ampliar dicha capacidad conectando otro switch a la red. En este caso, la topología sigue siendo en estrella, **ver Figura 3.25**.

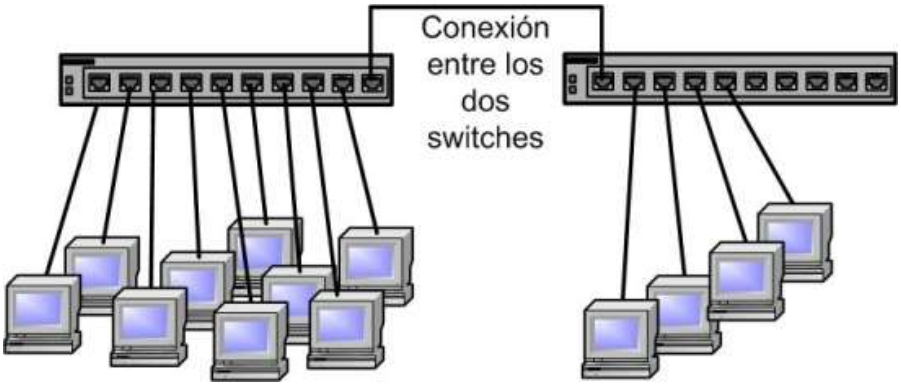


Figura 3.25. Ampliación de la capacidad de la red con dos switches

Cuando el número de dispositivos de la red es alto, normalmente se sigue una cierta estructura jerárquica donde lo normal es que haya dos o tres niveles jerárquicos. En este caso la estructura de la red se corresponde a una topología en árbol. En las siguientes figuras se pueden ver dos ejemplos de redes Ethernet con dos y tres niveles jerárquicos respectivamente, **ver figuras 3.26, 3.27**.

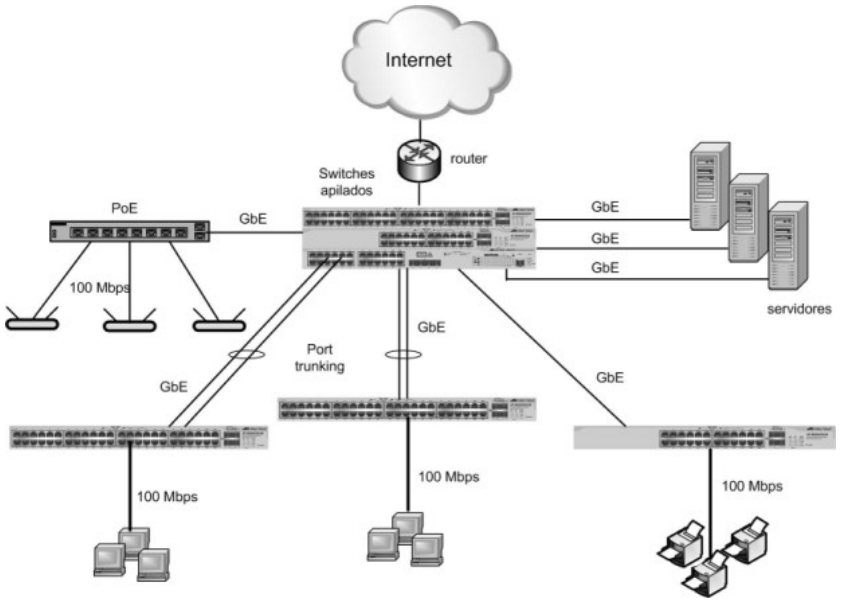


Figura 3.26. Red local con estructura jerárquica de switches con 2 niveles

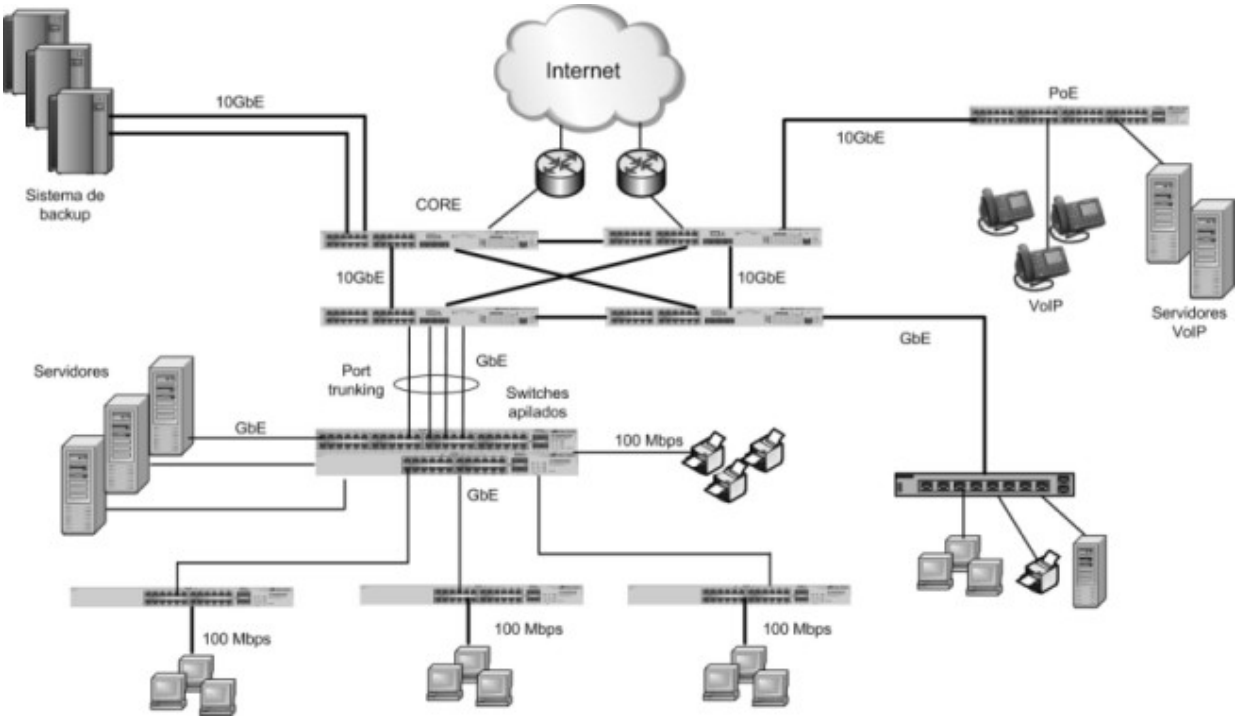


Figura 3.27. Red local con estructura jerárquica de switches con 3 niveles

3.7.6 Switch troncal / switch perimetral

El término switch troncal se refiere a los que se utilizan en el núcleo central (core) de las grandes redes. Es decir, a estos switches están conectados otros de jerarquía inferior, además de servidores, routers **WAN***, etc. Por otro lado el término**s** Switch perimetral se refiere a los utilizados en el nivel jerárquico inferior en una red local y a los que están conectados los equipos de los usuarios finales, **ver Figura 3.28**.

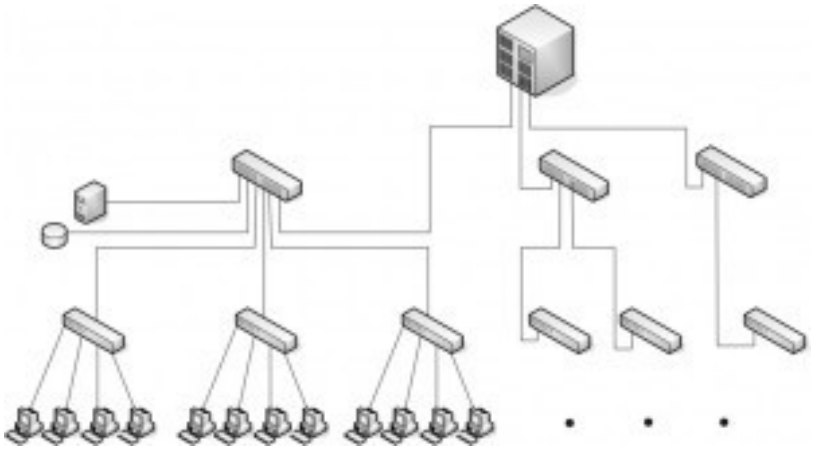


Figura 3.28. Ejemplo de conexión de un Switch troncal

3.7.6 Tipos de Switch, gestionable y no gestionable

El término gestionable (managed**)** se refiere a los switches que ofrecen una serie de características adicionales que requieren de configuración y gestión. Por el contario los switches no gestionables (unmanaged) suelen ser los que ofrecen funcionalidades básicas que no requieren procedimiento de configuración o gestión.

En base a todo lo anterior se ofrece la clasificación propuesta, seguida de la explicación de las características de cada tipo.

3.7.7 Tipos de switches

Se tienen los siguientes tipos de switches que dependen de su funcionalidad y aplicación a utilizar

- Desktop
- Perimetrales no gestionables
- Perimetrales gestionables
- Troncales de prestaciones medias
- Troncales de altas prestaciones

3.7.7.1 Switches desktop

Este es el tipo de switch más básico que ofrece la función de conmutación básica sin ninguna característica adicional. Estos switches no requieren ningún tipo de configuración, ya que utilizan el

modo de *autoconfiguración* de Ethernet para configurar los parámetros de cada puerto, **ver Figura 3.29**. Las características más habituales en este tipo son:

- Número de puertos: 4 -8 puertos RJ-45.
- Configuración de los puertos: normalmente admiten 10BASE-T y 100BASE-TX tanto en modo half-dúplex como full-dúplex. Su configuración se lleva a cabo por negociación mediante la característica de *autonegociación* que proporciona el estándar IEEE 802.3**.**
- Los switches más actuales de este tipo pueden incluir la característica *Auto MDI/MDI-X*.

Figura 3.29. Foto de un switch más básico

3.7.7.2 Switches perimetrales no gestionables

Este tipo de switches se utilizan habitualmente para constituir redes de pequeño tamaño de prestaciones medias. No admiten opciones de configuración y suelen tener características similares a los switches desktop pero incrementando el número de puertos y ofreciendo la posibilidad de montaje en rack 19''**, ver Figura 3.30**.

- El número de puertos de este tipo de switch puede ser típicamente de 4, 8, 16 o 24 puertos.
- Suelen ser puertos 10/100 RJ-45 que admiten *autonegociación* y *Auto MDI/MDI-X*. Existen algunos modelos con puertos 10/100/1000.
- En algunos casos pueden presentar puertos adicionales de rendimiento superior al resto de puertos.
- Existen modelos no gestionables que proporcionan *Power Over Ethernet* (**PoE**).
- Preparados para su montaje en rack de 19''.

Figura 3.30. Switch perimetral no gestionable

3.7.73 Switches perimetrales gestionables

Este tipo se utiliza para la conexión de los equipos de los usuarios en redes de tamaño medio y grande, y se localizan en el nivel jerárquico inferior. Es necesario que estos switches ofrezcan características avanzadas de configuración y gestión, **ver Figura 3.31**.

Sus características más habituales son:

- EL número de puertos fijos que ofrecen oscila entre 16 y 48 puertos.
- Existen modelos con puertos 10/100 y otros con puertos 10/100/1000, todos con soporte *Auto MDI/MDI-X*.
- Incluyen puertos adicionales de mayores prestaciones o puertos modulares (GBIC **o** SFP) para la conexión con un switch troncal.
- Características avanzadas de configuración en el nivel 2 como *Port Trunking*, *Spanning Tree*, *IEEE 802.1x*, *QoS, VLAN*, soporte de tramas *Jumbo*, etc.

Figura 3.31. Switch perimetral gestionable

3.7.7.4 Switches troncales de prestaciones medias

Este tipo de switches están diseñados para formar el núcleo o troncal de una red de tamaño medio. Proporcionan altas prestaciones y funcionalidades avanzadas. Una de las principales diferencias con los switches perimetrales es que ofrecen características de nivel 3 como enrutamiento IP, **ver Figura 3.32**. A continuación se exponen sus características más representativas:

- Características avanzadas de configuración de nivel 2 similares a los switches perimetrales gestionables.
- Habitualmente ofrecen entre 24 y 48 puertos fijos 10/100 con conector RJ-45 con algunos puertos modulares adicionales para Gigabit Ethernet y 10GbE para cable y fibra. Existen también modelos con puertos de altas prestaciones 10/100/1000 o incluso puertos 10GbE.
- Permiten expandir sus capacidades mediante la apilación de switches.
- Niveles 2/3. Además de cubrir funciones de conmutación avanzadas del nivel 2 también proporcionan funciones de enrutamiento y gestión en el nivel 3.

Figura 3.32. Switches troncales de prestaciones medias

3.7.7.5 Switches troncales de altas prestaciones

La principal característica de este tipo, además de su alto rendimiento, es su alta modularidad. El formato habitual es de tipo *chasis* donde se instalan los módulos que se necesitan. Se utilizan en grandes redes corporativas o de campus, e incluso se utilizan por los operadores para constituir sus redes metropolitanas, **ver Figura 3.33**.

Sus principales características son:

- Altamente modulares mediante un chasis con un número variable de slots donde se insertan módulos con los elementos requeridos. Normalmente suelen admitir la inserción de módulos "en caliente" (*hot swappable*) de forma que no hay que desconectar el switch para realizar dicha operación, garantizando así una alta disponibilidad.
- Niveles 2/3/4. Además de cubrir funciones de conmutación avanzadas del nivel 2 también proporcionan funciones de enrutamiento y gestión en los niveles 3 y 4.
- Admiten módulos con todos los tipos de puertos, tanto de cobre como de fibra con velocidades 10/100/1000 Mbps hasta 10Gbps.
- Características avanzadas de configuración y gestión en el nivel 2.
- Enrutamiento en el nivel 3 (IPv4 e IPv6).

Figura 3.33. Switch troncal de altas prestaciones

3.8 Router

El término router se podría traducir como enrutador o encaminador. Desde el punto de vista de las telecomunicaciones, un router es un dispositivo de red utilizado para unir redes y encaminar datos entre ellas, permite el conocimiento de varias redes entre sí, sin importar pertenezcan al mismo segmento de red, **ver Figura 3.34 [16]**.

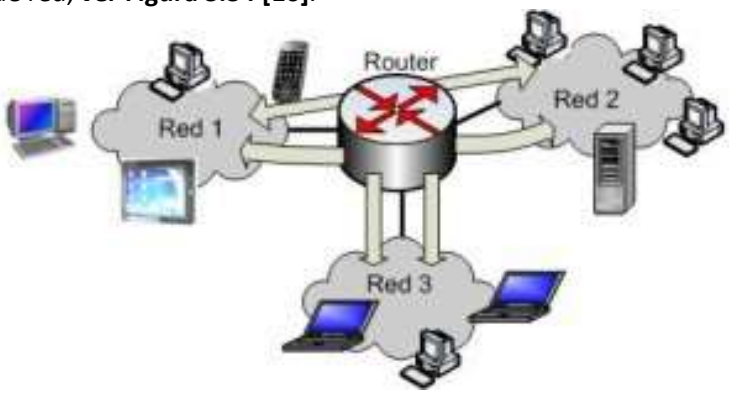


Figura 3.34. Router uniendo tres redes

Unir redes es la función básica asociada a un router. Sin embargo la evolución de las redes y de Internet ha hecho evolucionar también a los routers añadiendo cada vez más funcionalidades a los mismos. En la actualidad podemos clasificar los routers en dos grandes grupos:

3.8.1 Tipos de router

3.8.1.1 Routers de acceso

Cada nodo intermedio de una comunicación debe conocer dónde ha de enviar el paquete que ha recibido.

Son routers utilizados para unir dos redes, normalmente la red de un operador de telecomunicaciones con la red de su cliente, ya sea residencial o corporativo, y ya sea para proporcionar acceso a Internet o proporcionar acceso a otras redes de datos, **ver Figura 3.35**. En este tipo de routers la función de "enrutamiento" es más o menos simple porque solo tienen que intercambiar datos entre dos redes. Por el contrario, suelen incorporar otras funciones adicionales como cortafuegos, NAT, proxy, balanceo de carga en el tráfico de datos de los puertos, Wi-Fi **[12]**.

Figura 3.35. Routers de acceso profesional de la serie 2800 de Cisco

3.8.1.2 Routers de distribución

Son routers que están conectados a más de dos redes. Este tipo de routers sí mantiene como principal función la de "enrutar" datos entre las diferentes redes a las que están conectados y deben estar preparados para procesar una gran cantidad de información. Utilizan algoritmos de enrutamiento para optimizar la búsqueda de las rutas más óptimas para los datos que manejan. Ver **Figura 3.36.**

Figura 3.36. Router de distribución Juniper cuya principal función es encaminar datos

En la figura siguiente hay representadas tres redes aisladas entre sí. Las dos primeras son redes cableadas cuyo dispositivo de interconexión es un switch. La tercera es una red inalámbrica cuyo dispositivo de interconexión es un punto de acceso inalámbrico. En todas ellas se ha indicado la dirección IP de cada dispositivo. La máscara de subred para todos los dispositivos sería 255.255.255.0, por tanto, cada red física tiene un rango de direccionamiento diferente, es decir, utilizan redes lógicas diferentes, **ver Figura 3.37**. [Ver anexo 4- Máscaras de red y CDIR).

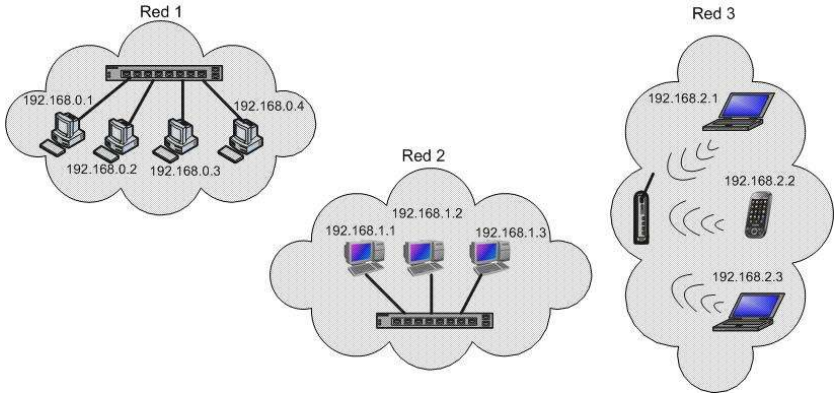


Figura 3.37. Tres redes aisladas

El rango de direccionamiento o red lógica de cada red, utilizando la nomenclatura CIDR sería:
Red 1 192.168.0.0 / 24
Red 2 192.168.1.0 / 24
Red 3 192.168.2.0 / 24

Ahora supongamos que queremos interconectar todos los dispositivos de esas tres redes. Existen dos posibles soluciones.

La primera es formar una única red que interconecte todos los dispositivos de las tres redes. En este caso, habría que cambiar las direcciones de dos de las redes para que todos los dispositivos pertenecieran a la misma red lógica, **ver Figura 3.38**.

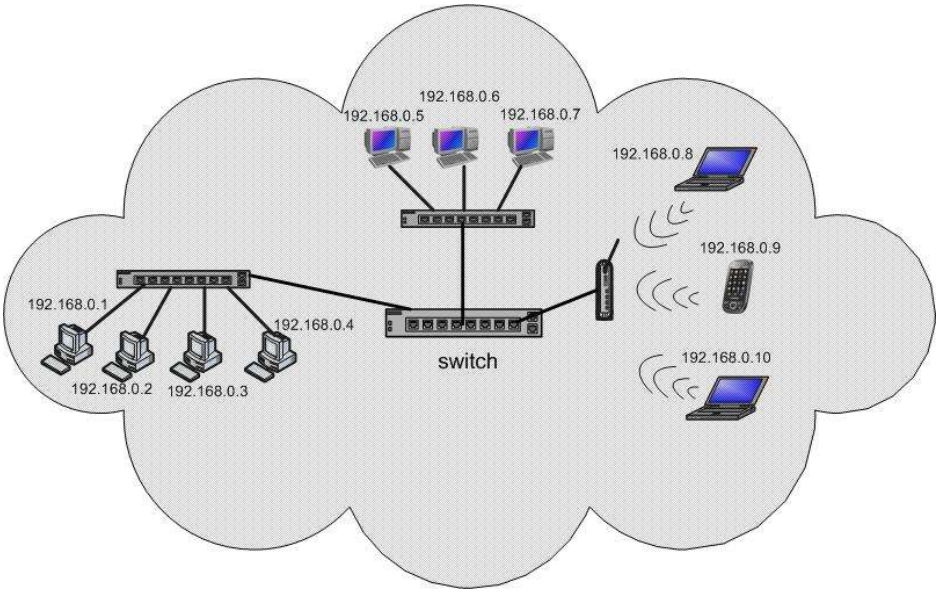


Figura 3.38. Fusión de las 3 redes cambiando las direcciones IP de los equipos y redes 2 y 3

Véase que el dispositivo de interconexión utilizado en este caso es un switch. Lo que se ha hecho por tanto, no es unir tres redes, sino fusionar tres redes en una sola red más grande. Utilizando un solo rango de direcciones, el 192.168.0.0 / 24, que es el que se utiliza para la red 1.

La segunda solución es unir las tres redes pero manteniendo la identidad de cada red. En este caso, el dispositivo de interconexión necesario es un router, **ver Figura 3.39**.

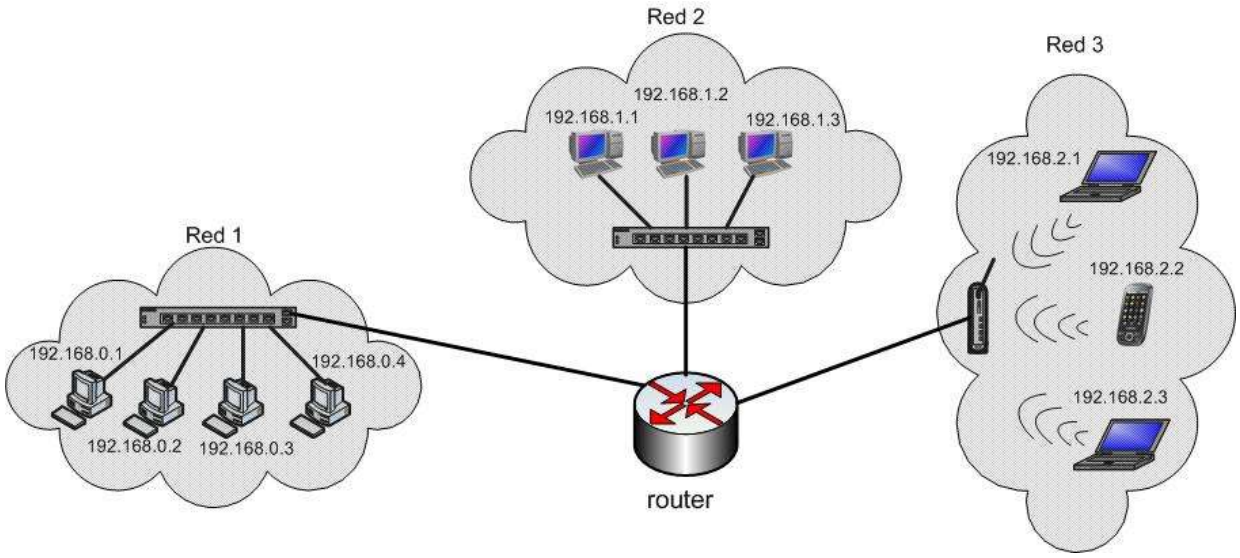


Figura 3.39. Unión de las tres redes manteniendo el direccionamiento de cada red

Véase, que en la segunda solución, los dispositivos de cada red pertenecen a su propia red lógica, diferente para cada red. El router será capaz de redirigir el tráfico de datos entre las diferentes redes pero cada red mantiene su identidad y su propio rango de direcciones.

Una creencia muy extendida es que los routers sólo se usan para conectar redes separadas físicamente, en edificios, ciudades o incluso países diferentes, sin embargo esto no siempre es así. Dentro de la red de una misma empresa se pueden tener diferentes redes lógicas por cuestiones organizativas, de seguridad o de gestión del propio tráfico de red, de forma que dos equipos conectados a la misma red física pueden pertenecer a redes lógicas diferentes**.**
Como se observa, el router de la figura ha unido las tres redes pero sin que cada red pierda su identidad, es decir, su rango de direccionamiento.

3.8.2 Funcionalidades del Router

Los routers, además de su función como encaminadores del tráfico de red, pueden proporcionar muchas otras funcionalidades. A continuación se describe brevemente algunas de ellas:

- **Adaptación de los datos entre diferentes tecnologías de transmisión**. El caso más típico son los routers residenciales que unen las redes residenciales con las redes de los operadores de telecomunicaciones para proporcionar servicios de conexión a Internet. Estos routers son capaces de intercambiar datos entre la red del usuario residencial que utiliza tecnologías típicas de redes locales (Ethernet y Wi-Fi) y la red de acceso del operador, que utilizará tecnologías de última milla como ADSL, cable (HFC) o fibra óptica (FTTH).
- **Proporcionar los parámetros de configuración de red**. Esta función se lleva a cabo mediante un servicio llamado **DHCP** y que simplifica mucho la conexión de un dispositivo a la red ya que todos los parámetros de red se configuran de forma automática **Filtrado de datos**. El filtrado de datos se lleva a cabo principalmente por cuestiones de seguridad.

- **Traducción de direcciones de red**. En la actualidad y debido a la escasez de direcciones IP prácticamente todas las redes utilizan un mecanismo de traducción de direcciones de red conocido como NAT (Network Address Translation) que permite el uso de direcciones privadas en redes conectadas a Internet. Esta función es implementada en muchos casos por routers, especialmente en los routers residenciales.

Otras características que pueden implementarse en los router actualmente:

- Punto de acceso inalámbrico (Wi-Fi)
- Redirección de puertos
- Servidor proxy
- Balanceo de carga/tráfico
- Gestión de conexiones VPN

3.9 Puntos de Acceso Inalámbrico (Access Point, AP)

Un punto de acceso inalámbrico (WAP o AP por sus siglas en inglés: Wireless Access Point) en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos **[12]**.

Son los encargados de crear la red, están siempre a la espera de nuevos clientes a los que dar servicios. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) y la LAN cableada.

El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, mediante una antena inalámbrica, **ver Figura 3.40**.

Figura 3.40. Funcionamiento de un Access Point

3.10 Sistemas de seguridad

3.10.1 Firewall

Un cortafuegos (Firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados **[13].**

En general el firewall debe controlar lo siguiente

- Todo el tráfico desde interior a exterior y viceversa debe pasar por el Cortafuegos/Firewall.
- Bloqueo de todos los accesos físicos a red propia excepto el del Cortafuegos
- El Cortafuegos permite sólo trafico autorizado definido por las políticas de seguridad de la organización
- Cada tipo de Cortafuegos permite distintos tipos de control
- Debe ser inmune a intrusiones

3.10.1.1 Tipos de cortafuegos

Nivel de aplicación de pasarela

Aplica mecanismos de seguridad para aplicaciones específicas, tales como servidores FTP y **Telnet***. Esto es muy eficaz, pero puede imponer una degradación del rendimiento.

Cortafuegos de capa de red o de filtrado de paquetes

Funciona a nivel de red (capa 3 del modelo OSI, capa 2 del stack de protocolos TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (capa 3 TCP/IP, capa 4 Modelo OSI), como el puerto origen y destino, o a nivel de enlace de datos (no existe en TCP/IP, capa 2 Modelo OSI) como la dirección MAC. [Ver anexo 2- Modelo OSI).

Cortafuegos de capa de aplicación

Trabaja en el nivel de aplicación (capa 7 del modelo OSI), de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si trata de tráfico HTTP, se pueden realizar filtrados según la URL a la que se está intentando acceder, e incluso puede aplicar reglas en función de los propios valores de los parámetros que aparezcan en un formulario web. Un cortafuegos a nivel 7 de tráfico HTTP suele denominarse proxy, y permite que los ordenadores de una organización entren a Internet de una forma controlada. Un proxy oculta de manera eficaz las verdaderas direcciones de red.

Cortafuegos personal

Es un caso particular de cortafuegos que se instala como software en un ordenador, filtrando las comunicaciones entre dicho ordenador y el resto de la red. Se usa por tanto, a nivel personal.

3.10.1.2 Políticas de un cortafuegos

Hay dos políticas básicas en la configuración de un cortafuegos que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

• Política restrictiva: Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafu egos obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten. Esta aproximación es la que suelen utilizar las empresas y organismos gubernamentales.

• Política permisiva: Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado. La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por omisión.

3.10.1.3 Topologías de un Firewall

Cortafuegos básico de borde

- Un equipo actúa como cortafuegos, conectando red interna con la externa, **ver Figura 3.41**
- Ofrece todas las funcionalidades de Cortafuegos más (opcionalmente) todos los servicios adicionales
- Si se ve comprometido, todo el sistema se compromete

Alternativas:

- Router con filtrado de paquetes
  - Opción más simple, pero menos potente
  - Escasas posibilidades de monitorización
- Equipo dedicado
  - Sistema estándar con 2 interfaces de red
  - Todas las conexiones pasan a través de él
  - Puede integrar los Proxi precisos

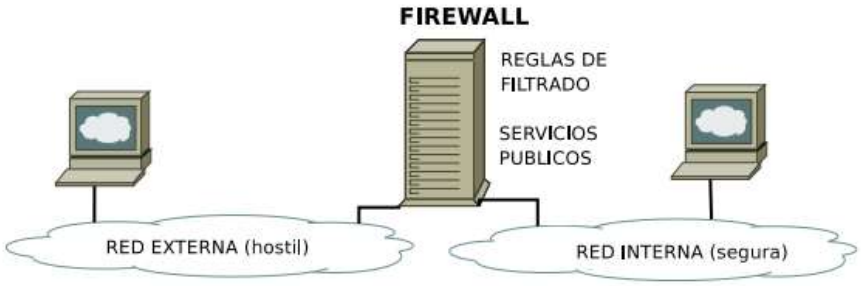


Figura 3.41. Funcionamiento de un Firewall básico de borde

Host oculto (screened host)

- Ofrecer los servicios (internos y externos) en una única maquina ubicada en el interior, **ver Figura 3.42**.
- Alojará a los Proxies de aplicación usados por la red interna.
- Alojará los servicios ofrecidos al exterior en el esquema anterior estaban en el Cortafuegos o repartidos en la LAN interna.
- Elemento potencialmente vulnerable por ser el único accesible desde el exterior
- Única máquina accesible desde el exterior (host bastión)
- Elemento potencialmente vulnerable por ser el único accesible desde el exterior.
- Administración delicada (es la base de la seguridad de este esquema)

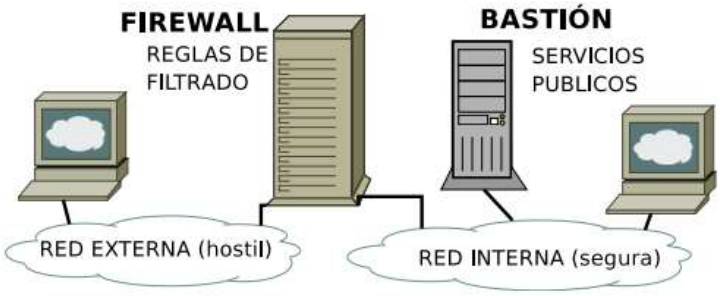


Figura 3.42. Funcionamiento de un firewall de hosts oculto

Host inseguro (untrusted host)

- Variante del anterior, el host bastión con los servicios hacia el exterior se ubica fuera de la red protegida, **ver Figura 3.43**.
- Cortafuegos no tiene efecto sobre ´el

Características:

- Ofrece los servicios públicos sin debilitar la red interna.
- Configuración y administración delicada

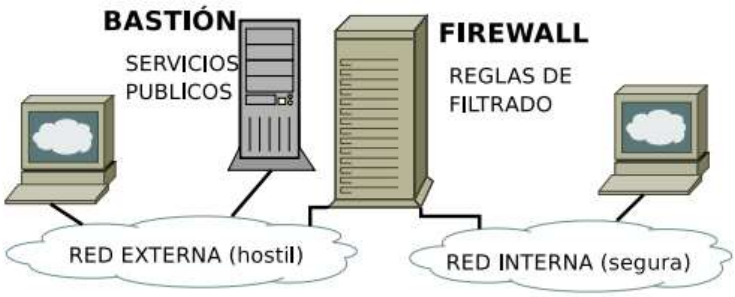


Figura 3.43. Funcionamiento de un firewall de hosts inseguro

3.10.1.4 Red de Perímetro/Zona Desmilitarizada(DMZ)

En seguridad informática, una zona desmilitarizada (Demilitarized Zone) o red perimetral es una zona segura que se ubica entre la red interna de una organización y una red externa, generalmente en Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que en general las conexiones desde la DMZ solo se permitan a la red externa -- los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, Web y DNS. Y es precisamente estos servicios alojados en estos servidores los únicos que pueden establecer tráfico de datos entre el DMZ y la red interna, **ver Figura 3.44**.

- Objetivo: aislar los servicios al exterior para evitar acceso a la red protegida.
- Host inseguro se sitúa detrás del Cortafuegos, pero en una red aislada
- Cortafuegos con 3 interfaces.
- Incrementa seguridad, fiabilidad y disponibilidad del host inseguro.
- Los equipos internos siguen sin poder confiar en ese host.
- Dentro de la DMZ (zona desmilitarizada) pueden ubicarse más de 1 host.
- DMZ define una red de servicios públicos

DMZ suele incluir:

- Proxies de aplicación para la red interna.
- Sistemas que requieran acceso controlado desde el exterior

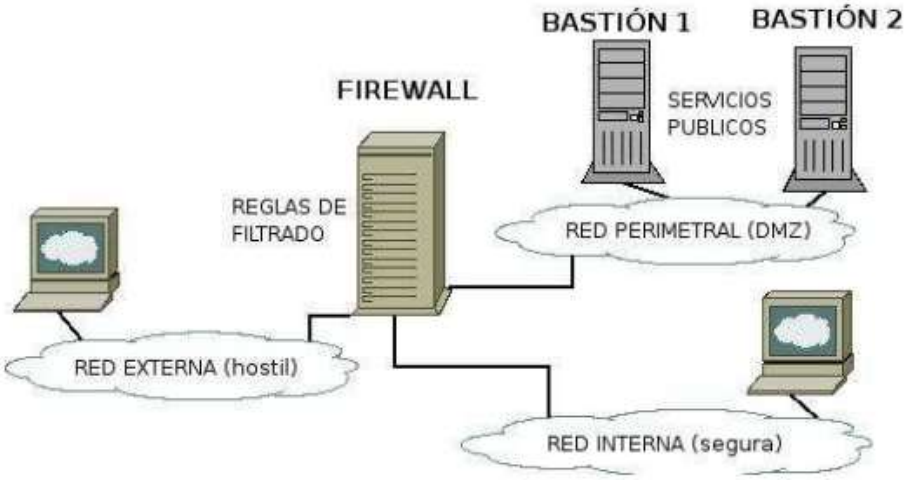


Figura 3.44. Funcionamiento de una DMZ

3.10.1.5 VPN

VPN es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet, mediante un proceso de encapsulación y de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada.

Una red privada virtual (RPV), en inglés: Virtual Private Network (VPN), es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones **[14].**

Básicamente existen cuatro arquitecturas de conexión VPN:

- VPN de acceso remoto

Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas), **ver Figura 3.45**.

- VPN punto a punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se

conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha.

- VPN over LAN

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

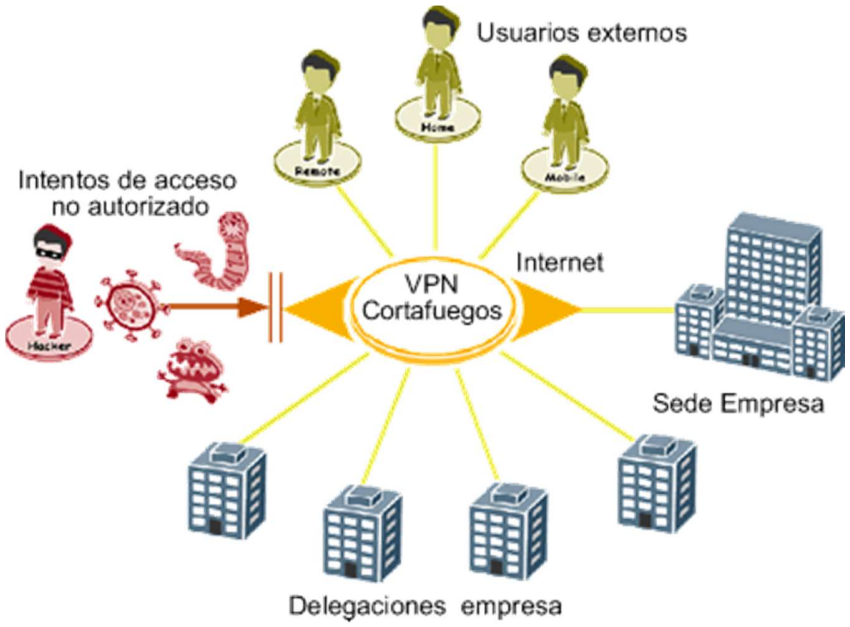


Figura 3.45. Funcionamiento de una VPN

3.10.2 Antivirus

Los antivirus son programas cuyo objetivo es detectar y/o eliminar virus informáticos. Nacieron durante la década de 1980. Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, ha hecho que los antivirus hayan evolucionado hacia programas más avanzados que no sólo buscan detectar virus informáticos, sino bloquearlos, desinfectarlos y prevenir una infección de los mismos, y actualmente ya son capaces de reconocer otros tipos de malware, como spyware, rootkits, etc.

Un virus es una especie de programa informático; una secuencia de instrucciones codificadas en un lenguaje de programación específico (código malicioso), creada intencionadamente con un fin concreto (gastar bromas, recopilar y enviar información a terceras personas o empresas, robar información sensible o simplemente bloquear la red o causar daños en los equipos); que suelen introducirse en los equipos informáticos de manera involuntaria (sin el consentimiento del usuario) **[15]**.

Básicamente, un antivirus compara el código de cada archivo con una base de datos de los códigos (también conocidos como firmas o vacunas) de los virus conocidos, por lo que es importante actualizarla periódicamente a fin de evitar que un virus nuevo no sea detectado. También se les ha

agregado funciones avanzadas, como la búsqueda de comportamientos típicos de virus (técnica conocida como Heurística) o la verificación contra virus en redes de computadores. Normalmente un antivirus tiene un componente que se carga en memoria y permanece en ella para verificar todos los archivos abiertos, creados, modificados y ejecutados en tiempo real. Es muy común que tengan componentes que revisen los adjuntos de los correos electrónicos salientes y entrantes, así como los scripts y programas que pueden ejecutarse en un navegador web (ActiveX, Java, JavaScript).

Métodos de contagio

Existen dos grandes grupos de propagación: los virus cuya instalación el usuario en un momento dado ejecuta o acepta de forma inadvertida, o los gusanos, con los que el programa malicioso actúa replicándose a través de las redes. Dentro de las contaminaciones más frecuentes por interacción del usuario están las siguientes:

• Mensajes que ejecutan automáticamente programas (como el programa de correo que abre directamente un archivo adjunto).

• Ingeniería social, mensajes como: «Ejecute este programa y gane un premio».

• Entrada de información en discos de otros usuarios infectados.

• Instalación de software que pueda contener uno o varios programas maliciosos.

• Unidades extraíbles de almacenamiento (USB). Seguridad y métodos de protección Los métodos para contener o reducir los riesgos asociados a los virus pueden ser los denominados activos o pasivos. Tipos de vacunas

• Sólo detección: Son vacunas que sólo actualizan archivos infectados sin embargo no pueden eliminarlos o desinfectarlos.

• Detección y desinfección: son vacunas que detectan archivos infectados y que pueden desinfectarlos.

• Detección y aborto de la acción: son vacunas que detectan archivos infectados y detienen las acciones que causa el virus.

• Comparación por firmas: son vacunas que comparan las firmas de archivos sospechosos para saber si están infectados.

• Comparación de firmas de archivo: son vacunas que comparan las firmas de los atributos guardados en tu equipo.

• Por métodos heurísticos: son vacunas que usan métodos heurísticos para comparar archivos.

• Invocado por el usuario: son vacunas que se activan instantáneamente con el usuario.

• Invocado por la actividad del sistema: son vacunas que se activan instantáneamente por la actividad del sistema operativo.

3.10.2.1 DLP (Prevención de Pérdida de Datos, Data Loss Prevention)

Una solución de prevención de pérdida de datos (PPD) es un sistema que está diseñado para detectar potenciales brechas de datos/ transmisiones de datos y prevenirlos a través de monitoreo,

detección y bloqueo de información sensible mientras está en uso (acciones de extremos) en movimiento (tráfico de red) y en reposo (almacenamiento de datos). En incidentes de filtración de datos, información sensible es divulgada a personal no autorizado, ya sea para intenciones maliciosas o un por un error inadvertido. Dichos datos sensibles pueden venir en la forma de información de compañías, propiedad intelectual (PI), información financiera, datos de tarjetas de crédito y otra información dependiendo del negocio y la industria **[15]**.

Los términos "pérdida de datos" y "filtración de datos" están cercanamente relacionados y son comúnmente usados indistintamente, a pesar de que son diferentes en cierto sentido. Los incidentes de pérdida de datos se convierten en incidentes de filtración de datos en los casos donde el medio que contenga información sensible sea perdido y subsecuentemente adquirido por un grupo no autorizado

Tipos de sistemas

- **Información en movimiento**

Típicamente, es una solución de software o hardware que es instalada en el puerto de egreso de una red cerca del perímetro. Analiza el tráfico de red para detectar información sensible que está siendo enviada violando las políticas de seguridad de información.

- **Información en uso**

Dichos sistemas corren en estaciones de trabajo de usuarios o servidores en la organización. Como los sistemas basados en red, los sistemas basados en extremos pueden direccionar comunicaciones internas y externas y, en consecuencia, pueden ser utilizados para controlar el flujo de información entre grupos o usuarios(pared china). También pueden controlar comunicaciones vía email o mensajería instantánea antes de que sean almacenados en el registro corporativo, de esta manera, una comunicación bloqueada (una que nunca se haya enviado y por lo tanto no se le aplican reglas de retención) no será identificada en una situación de descubrimiento legal subsecuente. Los sistemas de extremo tienen la ventaja de poder monitorear y controlar el acceso físico a dispositivos (dispositivos móviles con capacidad de almacenamiento de datos) y en algunos casos pueden acceder a información antes de ser encriptada.

- **Identificación de datos**

Las solucuines incluyen varias técnicas para identificar información confidencial o sensible. Algunas veces confundida con descubrimiento, la identificación de datos es un proceso por el cual las organizaciones utilizan tecnología PPD para determinar qué buscar y en que datos buscar (en movimiento, en reposo o en uso).

Los datos son clasificados como estructurados o no estructurados. Datos estructurados residen en campos fijos dentro de un archivo como una hoja de cálculo, mientras que los datos no estructurados se refieren a texto en formato libre como documentos en archivos PDF. Se estima que el 80% de datos no son estructurados y el 20% son estructurados. La clasificación de datos se divide en análisis de contenido, concentrado en datos estructurados, y análisis contextual que busca en el lugar de origen, la aplicación o el sistema que generó los datos.

- **Detección de filtración de datos**

Algunas veces, un distribuidor de datos provee información sensible a un conjunto de grupos terceros. Un tiempo después, una parte de los datos es encontrada en un lugar no autorizado (en internet o en la computadora de un usuario). Entonces, el distribuidor tiene la obligación de investigar si la filtración de datos vino de uno o más grupos terceros o si fue juntada independientemente para otros propósitos.

- **Datos en reposo**

"Datos en reposo" se refiere a información vieja almacenada ya sea, en la computadora de un cliente, en una red de almacenamiento o un servidor de datos o incluso en un sistema de respaldo, como un CD o un casete. Está información es de gran preocupación para las empresas e instituciones gubernamentales simplemente porque mientras más tiempo estén esos datos almacenados y sin utilizarse, pueden ser obtenidos por individuos no autorizados a tenerlos.

3.10.3 Antispam

'Spam' entonces es la palabra que se utiliza para calificar el correo no solicitado enviado por Internet. La mayor razón para ser indeseable es que la mayoría de las personas conectadas a la Internet no goza de una conexión que no les cueste, y adicionalmente reciben un cobro por uso del buzón. Por lo tanto el envío indiscriminado de este tipo de correo ocasiona costos al lector. Contrario al 'correo basura' o Junk Mail que recibimos en nuestros buzones ordinarios (físicos, en papel!), el recibo de correo por la red le cuesta a un buen número de personas, tanto en la conexión como en el uso de la red misma. El correo físico no tiene ningún costo para quien lo recibe.

3.11 Soluciones de respaldo de información

Tener backups y respaldos de nuestros datos es importante, pero también es importante saber qué tipo de backup es el mejor para nosotros. En forma general y a grandes rasgos, existen 4 tipos distintos de backups, y son los siguientes:

-Backup completo: este tipo de backup hace un respaldo completo de todas las carpetas y archivos seleccionados. El respaldo abarca el 100% de los datos, por lo que suele ser el que lleva más tiempo en realizarse.

-Backup diferencial: contiene los archivos que han cambiado desde la última vez que se hizo el backup. Solo se incluyen los archivos nuevos y/o modificados desde el último backup.

-Backup incremental: se realiza un respaldo de todos los archivos que han sido modificados desde que fue ejecutado el último backup completo, diferencial o incremental. Es el método más rápido para realizar respaldos.

–Backup espejo: similar al backup completo, pero la diferencia es que los archivos no son comprimidos y no pueden ser protegidos usando un password.

3.11.1 Tipos de respaldos y medios de almacenamiento

Conforme aumenta la capacidad de almacenamiento de los dispositivos de información, también los usuarios tienden a necesitar guardar mayores cantidades de datos (videos, música, archivos de Office, imágenes, etc.). En el caso de las empresas que manejan grandes volúmenes de información, siempre ha sido necesidad el respaldo (bases de datos de sus empleados, reportes de ventas, clientes de correo electrónico, etc.), lo que para ellos es crucial. Un problema del respaldo, es que si no se tiene cuidado con la copia de seguridad, este puede ser utilizado por otras personas para crear nuevas copias y así hacer mal uso de la información.

Entre los dispositivos y servicios para respaldo de información están los siguientes:

- Cintas de almacenamiento.
- Servidores Web.
- Discos duros.
- Discos espejo de servidores

3.12 Conceptos y terminología para redes informática

En telecomunicaciones, un enlace de datos (en inglés: data link) es el medio de conexión entre dos lugares con el propósito de transmitir y recibir información. Puede hacer referencia a un conjunto de componentes electrónicos, que consisten en un transmisor y un receptor (dos piezas de un equipo terminal de datos) y el circuito de telecomunicación de datos de interconexión. Esto se rige por un protocolo de enlace que permite que los datos digitales puedan ser transferidos desde una fuente de datos a un receptor de datos.

Existen al menos tres configuraciones básicas para un enlace de datos:

- Símplex, todas las comunicaciones se realizan en una única dirección.
- Semidúplex, las comunicaciones se realizan en ambas direcciones, pero no al mismo tiempo.
- Dúplex, las comunicaciones se realizan en ambas direcciones simultáneamente.

3.12.1 Enlace dedicado y jerarquía PDH

La jerarquía digital plesiócrona, abreviada como PDH, del inglés Plesiochronous Digital Hierarchy, es una tecnología usada en telecomunicación tradicionalmente para telefonía que permite enviar varios canales telefónicos sobre un mismo medio (ya sea cable coaxial, radio o microondas) usando técnicas de multiplexación por división de tiempo y equipos digitales de transmisión. También puede enviarse sobre fibra óptica, aunque no está diseñado para ello y a veces se suele usar en este caso SDH (Synchronous Digital Hierarchy).

La jerarquía usada en Latinoamérica es la misma de Europa que agrupa 30+2 canales de 64Kb/s para obtener 2048 kbit/s (E1). Luego multiplicando por 4 sucesivamente se obtiene jerarquías de nivel superior con las velocidades de 8 Mbit/s (E2), 34 Mbit/s (E3) y 139 Mbit/s (E4).

En el sistema europeo, se tiene hasta cinco jerarquías, como se puede observar en la **Tabla 3.1.**

Tabla 3.1. Jerarquías PDH

Jerarquía	Velocidad	Canales	Trama
E1	2048 Kbit/s	30	256 bits = 125 us
E2	8448 Kbit/s	120	848 bits = 100.38 us
E3	34368 Kbit/s	480	1536 bits = 44,7 us
E4	139264 Kbit/s	1920	2904 bits = 20.85 us
E5	564992 Kbit/s	7680	2688 bits = 4.7 us

Un equipo multiplicador digital recibe un número N de señales numéricas, llamadas tributarios, que se presentan a su entrada en paralelo y produciendo una señal digital de mayor velocidad de información como mínimo N veces superior a la de los tributarios, v**er ecuación 3.1**.

- $fm >= N \times ft$ …(3.1)

donde:

fm = frecuencia múltiplo.

ft = frecuencia de tributario.

Los tributarios de entrada deberán estar en fase y en igualdad de frecuencia entre sí, pero en realidad no es así sino que tienen distinta fase entre sí y variación de las frecuencias, **ver ecuaciones 3.2 y 3.3**.

- $ft< = ft \pm \Delta ft$ …(3.2)
- $fm = fm \pm \Delta fm$ …(3.3)

A cada señal tributaria se le añaden unos bits que se llaman de relleno o de justificación, y unos bits que se llaman de control de justificación, para que el extremo receptor pueda distinguir los bits que son de información y los que son de relleno. Este proceso es conocido como justificación, y tiene por objeto absorber las ligeras diferencias de frecuencia que pueden presentar los distintos tributarios, ya que pueden haberse constituido con fuentes de reloj diferentes. De esta forma, a los tributarios más lentos es necesario añadirles más bits de relleno que a los tributarios más rápidos. En el extremo receptor, los bits de relleno

son oportunamente reconocidos y cancelados gracias a la información que transportan consigo los bits de control de la justificación. En consecuencia, la velocidad de la señal agregada es mayor que la suma de las velocidades de las señales tributarias, **ver ecuación 3.4**.

- $fm > N \times ft \dashrightarrow fm = (N \times ft) + fr$ …(3.4)

  donde:

  fr = frecuencia de los bits de redundancia.

PDH se basa en canales de 64 kbps. En cada nivel de multiplexación se van aumentando el número de canales sobre el medio físico. Es por eso que las tramas de distintos niveles tienen estructuras y duraciones diferentes. Además de los canales de voz en cada trama viaja información de control que se añade en cada nivel de multiplexación, por lo que el número de canales transportados en niveles superiores es múltiplo del transportado en niveles inferiores, pero no ocurre lo mismo con el régimen binario.

Existen tres jerarquías PDH: la europea, la norteamericana y la japonesa. La europea usa la trama descrita en la norma G.732 de la UIT-T mientras que la norteamericana y la japonesa se basan en la trama descrita en G.733. Al ser tramas diferentes habrá casos en los que para poder unir dos enlaces que usan diferente norma haya que adaptar uno al otro, en este caso siempre se convertirá la trama al usado por la jerarquía europea.

En la **Tabla 3.2** se muestran los distintos niveles de multiplexación PDH utilizados en Norteamérica (Estados Unidos y Canadá), Europa y Japón.

Tabla 3.2. Jerarquías internacionales para PDH

Nivel	Norteamérica			Europa			Japón		
	Circuitos	kbit/s	Denominación	Circuitos	kbit/s	Denominación	Circuitos	kbit/s	Denominación
1	24	1544	(T1)	30	2048	(E1)	24	1544	(J1)
2	96	6312	(T2)	120	8448	(E2)	96	6312	(J2)
3	672	44 736	(T3)	480	34 368	(E3)	480	32 064	(J3)
4	4032	274 176	(T4)	1920	139 264	(E4)	1440	97 728	(J4)

3.12.2 Lan to Lan o L2L, MPLS, Frame Relay y ATM

LAN to LAN

LAN to LAN es un servicio pensado para acortar distancias, diseñado para clientes con necesidad de interconexión de sus redes de datos mediante circuitos digitales punto a punto.

Permite unificar las redes de datos de diferentes sitios como si estuvieran ubicados físicamente en el mismo lugar y sin necesidad de equipamiento adicional. Esta solución utiliza enlaces dedicados que transportan la información manteniendo el protocolo nativo de la red.

Características:

- Tecnología broadcast (difusión) con el medio de transmisión compartido.
- Capacidad de transmisión comprendida entre 1 Mbps y 1 Gbps.
- Uso de un medio de comunicación privado.
- Posibilidad de conexión con otras redes.

MPLS

MPLS (Multiprotocol Label Switching) es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP **[16]** .

Multi Protocol Label Switching está reemplazando rápidamente frame relay y ATM como la tecnología preferida para llevar datos de alta velocidad y voz digital en una sola conexión. MPLS no sólo proporciona una mayor fiabilidad y un mayor rendimiento, sino que a menudo puede reducir los costos generales mediante una mayor eficiencia de la red. Su capacidad para dar prioridad a los paquetes que transportan tráfico de voz hace que sea la solución perfecta para llevar las llamadas VoIP, **ver Figura 3.46**.

Los objetivos establecidos para MPLS son:

- MPLS debía funcionar sobre cualquier tecnología de transporte, no sólo ATM
- MPLS debía soportar el envío de paquetes tanto unicast como multicast
- MPLS debía ser compatible con el Modelo de Servicios Integrados del IETF, incluyendo el protocolo RSVP
- MPLS debía permitir el crecimiento constante de la Internet
- MPLS debía ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP

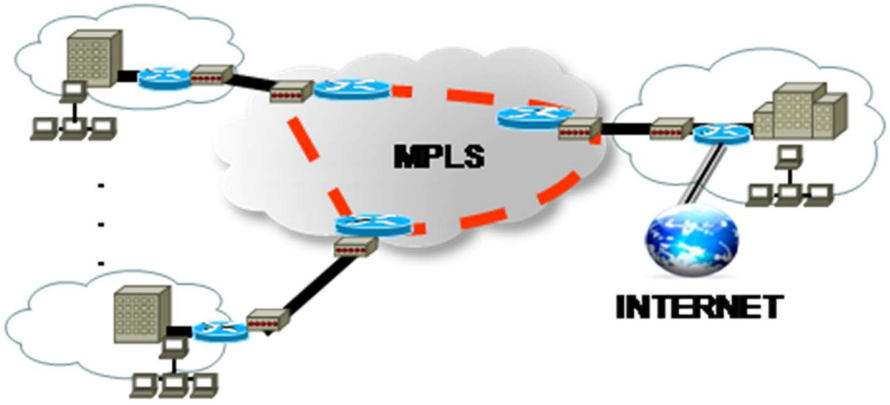


Figura 3.46. Diagrama de topología MPLS

Frame Relay

Frame Relay o (Frame-mode Bearer Service) consiste en una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de tramas o marcos ("frames") para datos, perfecto para la transmisión de grandes cantidades de datos.

La técnica Frame Relay se utiliza para un servicio de transmisión de voz y datos a alta velocidad que permite la interconexión de redes de área local separadas geográficamente a un coste menor.

Frame Relay proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada punto a punto, esto quiere decir que es orientado a la conexión.

ATM

El modo de transferencia asíncrona (Asynchronous Transfer Mode, ATM) es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

ATM es una tecnología de red reciente que, a diferencia de Ethernet, red en anillo y FDDI, permite la transferencia simultánea de datos y voz a través de la misma línea.

El ancho de banda se comparte (multiplexado) entre los usuarios según una desagregación temporaria, una red ATM transfiere datos de manera asíncrona, lo que significa que transmitirá los datos cuando pueda.

Además, las redes ATM sólo transmiten paquetes en forma de celdas con una longitud de 53 bytes (5 bytes de encabezado y 48 bytes de datos) e incluyen identificadores que permiten dar a conocer la calidad del servicio (QoS), entre otras cosas. La calidad de servicio representa un indicador de prioridad para paquetes que dependen de la velocidad de red actual.

Por lo tanto, ATM posibilita la transferencia de datos a velocidades que van desde 25 Mbps a más de 622 Mbps (incluso se espera que las velocidades alcancen más de 2 Gbps a través de la fibra óptica). Debido a que el hardware necesario para redes ATM es costoso, los operadores de telecomunicaciones las utilizan básicamente para líneas de larga distancia.

CAPÍTULO 4 Diseño e implementación de la infraestructura y recursos tecnológicos para una sede alterna de Contact Center.

En "Soluciones Multicanal S.A. de C.V." se trabajan operaciones multicanal para segmentos bancario y aerolíneas, el cual ofrece sus servicios desde noviembre de 2010, iniciando operaciones con 1250 estaciones operativas para servicios de cobranza telefónica bancaria, debido al éxito en su gestión de negocio y tecnológico fue creciendo en posiciones hasta el momento tener 1500, incluyendo ahora servicios a una aerolínea. El crecimiento fue exponencialmente dentro de la sede principal, el cliente ha solicitado tener un crecimiento de sus servicios de multicanalidad, por lo cual es los siguientes apartados documenta el trabajo realizado para la implementación de esta solicitud, así como la implementación de un plan de continuidad de negocio para una contingencia.

La implementación de una sede alterna, solo tiene un significado, el rumbo del Contact Center es el correcto, a los clientes de la línea de negocio les interesa mantener sus operaciones dentro de la empresa, por lo cual es necesario establecer y mejorar los procesos de la sede principal así como desde la implementación de una sede alterna ya se tengan establecidos estos procesos.

Las respectivas áreas de negocio reciben las peticiones de los clientes y planifican las peticiones de operaciones que requieren, que a su vez estas peticiones son revisadas con el personal de tecnología, las cuales son recibidas concretamente y se realiza la segunda planificación de los componentes tecnológicos y los tiempos en los cuales se realizará dicha implementación.

Se recibe por parte de las áreas de negocio de la siguiente forma:

Tabla 4.1 Requerimiento de crecimiento en la nueva sede

Sede principal Contact Center		Implementación en Contact Center (Sede Alterna)		
Cliente	Números de Posiciones Operativas(PA´s)	Números de Posiciones Operativas(PA´s)	Porcentaje de posiciones operativas para el PCN o BCP	Posiciones para Plan de Continuidad de Negocio (PCN o BCP)
Segmento Bancario Cobranza	1250	300 (150 Cobranza, 150 redes sociales)	5%	60
Segmento Aerolínea Reservaciones	250	0	10%	25

La **Tabla 4.1** muestra las características en las cuales actualmente se tienen establecidas las operaciones en la sede principal y así mismo se puede apreciar la petición de los clientes para la sede alterna. El crecimiento se interpreta de la siguiente forma, en la sede alterna se construye 300 estaciones de operador para el segmento bancario, en la cuales los servicios del segmento bancario de la sede principal y el nuevo servicio de redes sociales da servicio , y dentro de esas mismas estaciones de trabajo se prepara, configura y diseña la infraestructura para el plan de contingencia en caso de presentarse se pueda operar el 10 % de las operaciones de cobranza y de segmento de reservaciones de una aerolínea.

La implementación necesita tener el reconocimiento de los actuales componentes tecnológicos de la sede principal, documentando, comparando y estableciendo los requerimientos tecnológicos para el diseño de la arquitectura de la sede alterna. En el apartador 6 retoma el plan de continuidad en caso de contingencia para definir las figuras y procedimientos para realizarse.

Nota: Por temas de seguridad y confidencialidad de la empresa, se realiza bajo otro nombre de una razón social diferente.

Se debe considerar lo siguiente dentro del trabajo:

- **La petición del cliente es recibida por las figuras de mayor jerarquía de las áreas de trabajo dentro del Contact Center (Negocio, Servicios de Infraestructura, Planeación, Recursos Humanos y Tecnología), la duración de la sede alterna se establece contractualmente y mediante un proyecto de inversión en el cual los directivos establecen con el cliente la duración y el reflejo de la recuperación de la proyección superior a 1 año, después del periodo de 6 meses se espera tener ganancias costo-beneficio.**
- **El trabajo sólo plantea lo referente al área de tecnología, por lo cual no se muestra información de ubicación de la sedes del Contact Center.**
- **La sede alterna de acuerdo a las características analizadas por las áreas especializadas dentro del Contact Center (Servicios de Infraestructura y Electromecánica), realizan la implementación correspondiente a su especialidad, permitiendo el trabajo de ejecución para el área de tecnología, tanto simultáneamente como posterior a su trabajo, lo cual incluye todos los servicios correspondientes al edificio: sanitarios, electricidad, planta de emergencia, UPS, etc.**
- **Se contempló en el caso del segmento Aerolinea principalmente y para todos los servicios de negocio, horarios 24x24, derivado a tener una disponibilidad los 365 días del año, por lo cual representa lo siguiente**
    1. **Tecnologia. Tener disponbilidad de los recursos de infraestructura 24x365.**
    2. **Recursos Humanos. Operadores telefónicos en 3 turnos de 8 horas C/U. Tener disponbile 2 ingenieros de tiempo completo para la implementación del Contact Center.**
- **La sede principal se tienen 4 ingenieros de soporte en los servicios requeridos hacia el soporte en sitio, sin mencionar a los de áreas de segundo nivel TI (redes, servidores, telecomunicaciones) por lo cual para la sede alterna se contrató un ingeniero para**

realizar la implementación y de planta una vez finalizado, los soportes de segundo nivel, es atendido para ambas sedes.

El planteamiento del proceso para la implementación se refleja en la **Figura 4.1.**

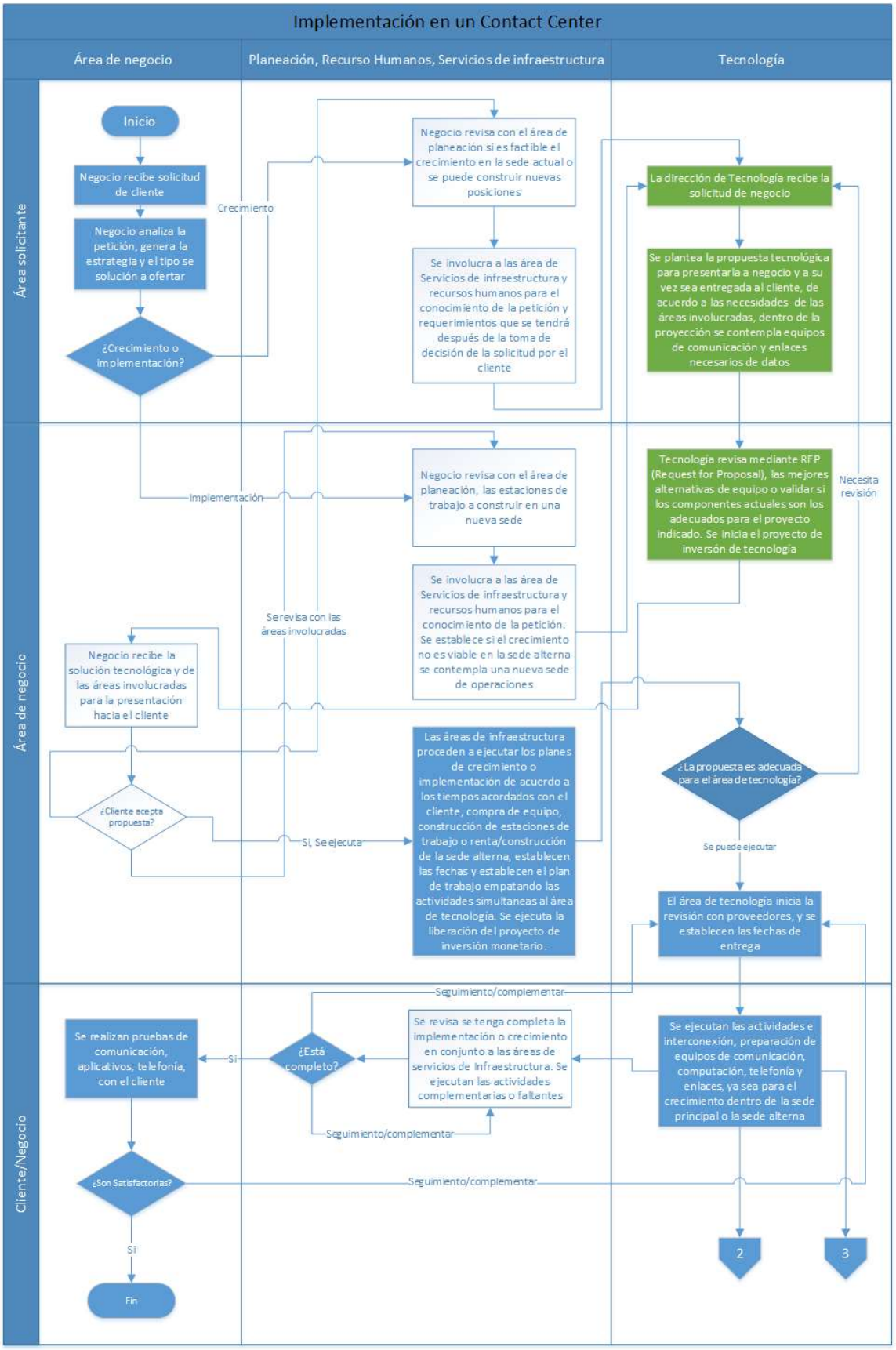

Implementación en un Contact Center
Área de negocio
Planeación, Recurso Humanos, Servicios de infraestructura
Tecnología
Área solicitante
Área de negocio
Cliente/Negocio
Inicio
Negocio recibe solicitud de cliente
Negocio analiza la petición, genera la estrategia y el tipo se solución a ofertar
¿Crecimiento o implementación?
Crecimiento
Negocio revisa con el área de planeación si es factible el crecimiento en la sede actual o se puede construir nuevas posiciones
Se involucra a las área de Servicios de infraestructura y recursos humanos para el conocimiento de la petición y requerimientos que se tendrá después de la toma de decisión de la solicitud por el cliente
La dirección de Tecnología recibe la solicitud de negocio
Se plantea la propuesta tecnológica para presentarla a negocio y a su vez sea entregada al cliente, de acuerdo a las necesidades de las áreas involucradas, dentro de la proyección se contempla equipos de comunicación y enlaces necesarios de datos
Implementación
Negocio revisa con el área de planeación, las estaciones de trabajo a construir en una nueva sede
Se involucra a las área de Servicios de infraestructura y recursos humanos para el conocimiento de la petición. Se establece si el crecimiento no es viable en la sede alterna se contempla una nueva sede de operaciones
Tecnología revisa mediante RFP (Request for Proposal), las mejores alternativas de equipo o validar si los componentes actuales son los adecuados para el proyecto indicado. Se inicia el proyecto de inversón de tecnología
Necesita revisión
Se revisa con las áreas involucradas
Negocio recibe la solución tecnológica y de las áreas involucradas para la presentación hacia el cliente
¿Cliente acepta propuesta?
Si, Se ejecuta
Las áreas de infraestructura proceden a ejecutar los planes de crecimiento o implementación de acuerdo a los tiempos acordados con el cliente, compra de equipo, construcción de estaciones de trabajo o renta/construcción de la sede alterna, establecen las fechas y establecen el plan de trabajo empatando las actividades simultaneas al área de tecnología. Se ejecuta la liberación del proyecto de inversión monetario.
¿La propuesta es adecuada para el área de tecnología?
Se puede ejecutar
El área de tecnología inicia la revisión con proveedores, y se establecen las fechas de entrega
Seguimiento/complementar
Se ejecutan las actividades e interconexión, preparación de equipos de comunicación, computación, telefonía y enlaces, ya sea para el crecimiento dentro de la sede principal o la sede alterna
Se revisa se tenga completa la implementación o crecimiento en conjunto a las áreas de servicios de Infraestructura. Se ejecutan las actividades complementarias o faltantes
¿Está completo?
Si
Seguimiento/complementar
Se realizan pruebas de comunicación, aplicativos, telefonía, con el cliente
¿Son Satisfactorias?
Seguimiento/complementar
Si
Fin
2
3

Figura 4.1 Diagramade flujo de la implementación del Contact Center

El diagrama mostrado en la **Figura 4.1**, muestra el desarrollo de la implementación de un Contact Center, inciando en la recepción de la solicitud del cliente para un crecimiento o implementación, en el cual las áreas directivas de la empresa, ofrecen una solución y es presentada al cliente, en caso de ser aceptada se procede a la ejecución del propuesta, y establecer un control en las pruebas y tiempos de entrega. Este trabajo se puede presentar para el área de tecnología mediante el siguierte organigrama de personal, **ver Figura 4.2**, cabe mencionar que solo se enfocará al área de soporte tecnologicó, sin inculuir las áreas de segundo nivel.

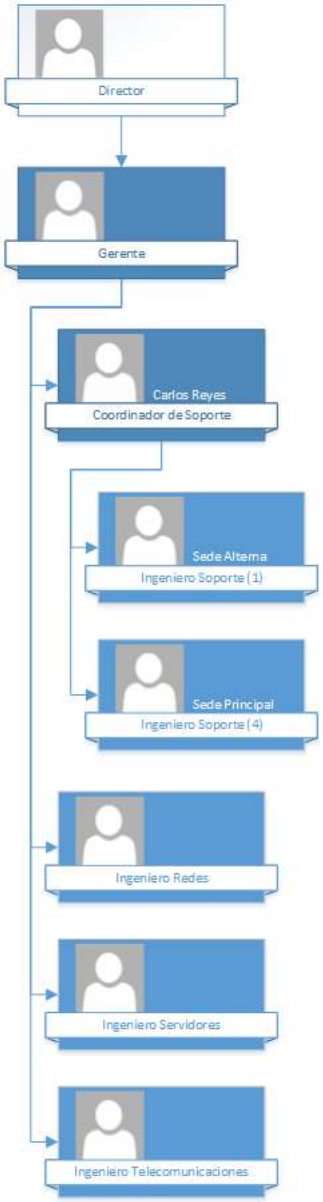


Figura 4.2. Organigrama de ingenieros de Soporte

Considere en la **Figura 4.1** referente al Diagrama de Bloques de la implementación la interconexión entre los diagramas para 2 y 3, respectivamente revisarlos en el apartado 5 para el diseño de los procesos de seguridad de la información y apartado 6 para la creación del plan de continuidad de negocio.

4.1 Reconocimiento de infraestructura tecnológica e implementación de un proceso continuo para la administración

En primer lugar, lo más importante para las áreas de Tecnología dentro del Contact Center es tener dentro del conocimiento y memoria técnica los componentes de su infraestructura tecnológica, abarcando desde cada uno de los equipos de comunicación y configuraciones especiales de la forma en la que viaja la información.

Las áreas de conocimiento que se deben de tener son las siguientes:

- Inventario de equipos de cómputo, equipos VoIP de telefonía e impresoras
- Inventario de servidores, switches, routers y firewall
- Inventario de aplicaciones desarrolladas por el Contact Center y del cliente
- Diagramas de red

4.1.1 Inventario de equipos de cómputo, equipos VoIP de telefonía e impresoras

Implementar de herramienta libre para el monitoreo de equipos de cómputo mantendrá en constante alerta el funcionamiento óptimo de las estaciones de trabajo, así como mantener en tiempo real el funcionamiento de los equipos, si se presenta una falla física de Disco Duro, memoria RAM, tiempo activo en la red, la herramienta tiene la capacidad de alertar estas situaciones, adicional agregando a que permite mantener reportes de las características físicas de los equipos, lo cual permite evaluar el rendimiento sea el correcto para las funciones de los operadores y estar alertados para mantener la disponibilidad del servicio.

Las principales características de la que se deben de mantener en consideración de los equipos de cómputo, son las siguientes:

- Espacio en disco Duro
- Memoria RAM, tecnología y capacidad
- Modelo y frecuencia del microprocesador
- Conexión de red
- Segmentos de red en monitoreo en tiempo real

4.1.1.1 Instalación de la herramienta de software libre para el monitoreo en tiempo real

Para poder realizar este monitoreo de los componentes del Contact Center se implementa de software libre Spiceworks, la cual permite agregar y tener el auto-reconocimiento de los componentes de red, monitoreo en tiempo real, reportería y alertas al correo electrónico de lo que está sucediendo dentro de la red, mismas que son configuradas mediante umbrales de interés del administrador de tecnología, **ver Figura 4.3**.

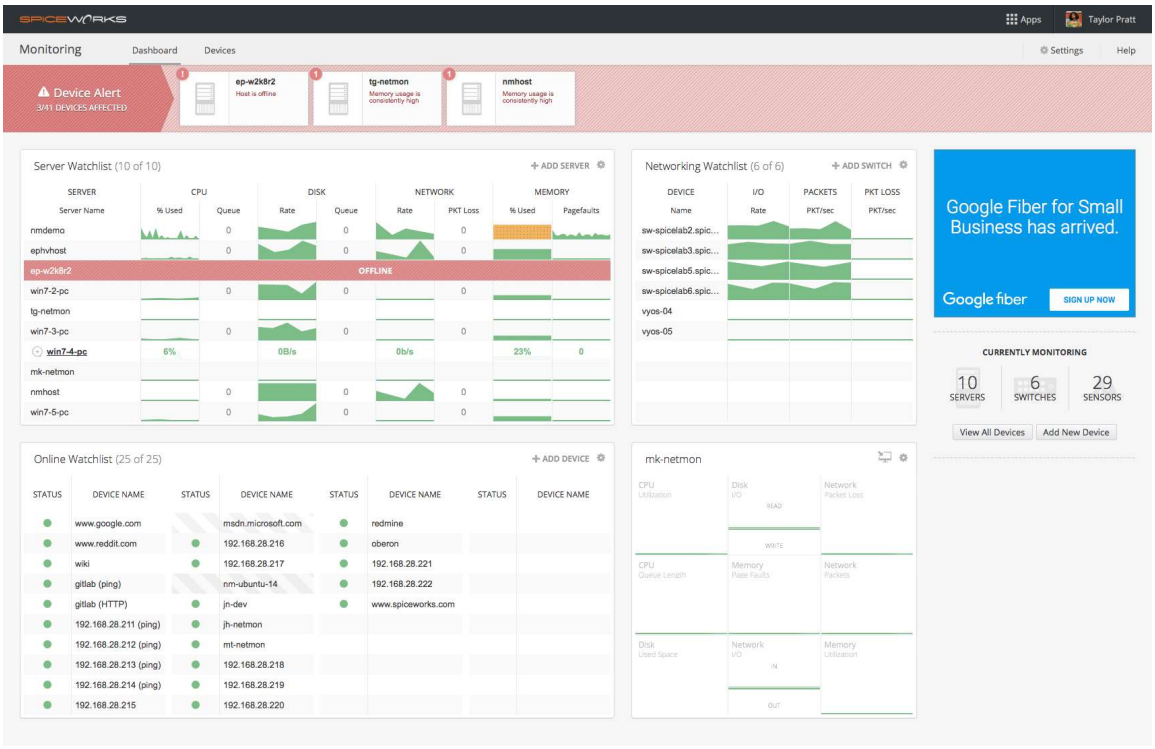


Figura 4.3 Monitoreo en tiempo real en la herramienta Spiceworks

Dentro de la herramienta Spiceworks, se puede obtener diferentes reportes, incluyendo las características mencionadas o añadiendo otras diferentes como la que se muestra a continuación en la **Figura 4.4**

Soluciones Multicanal: Inventory Summary
1423 Items.
Sep 28, 2016

Name	Manufacturer	Device Type	Model	IP Address	Serial Number	Operating System
sm-45-2	Hewlett-Packard	Desktop	6000 Pro SFF PC	172.27.45.2	MXL0380P0F	Windows 7 Pro
sm-45-20	Hewlett-Packard	Desktop	6000 Pro SFF PC	172.27.45.20	MXL0341BLN	Windows 7 Ent

Figura 4.4 Reporte presentado por la herramienta Spiceworks

Así mismo la herramienta tiene la funcionalidad de notificarnos por correo electrónico cualquier eventualidad en los componentes conectados a la red, estas configuraciones permiten configurar umbrales en los cuales envia un correo de alerta, el siguiente correo es una notificación de los

equipos que tuvieron actualizaciones del software instalado y actualizaciones automáticas del sistema operativo, **ver Figura 4.5**.

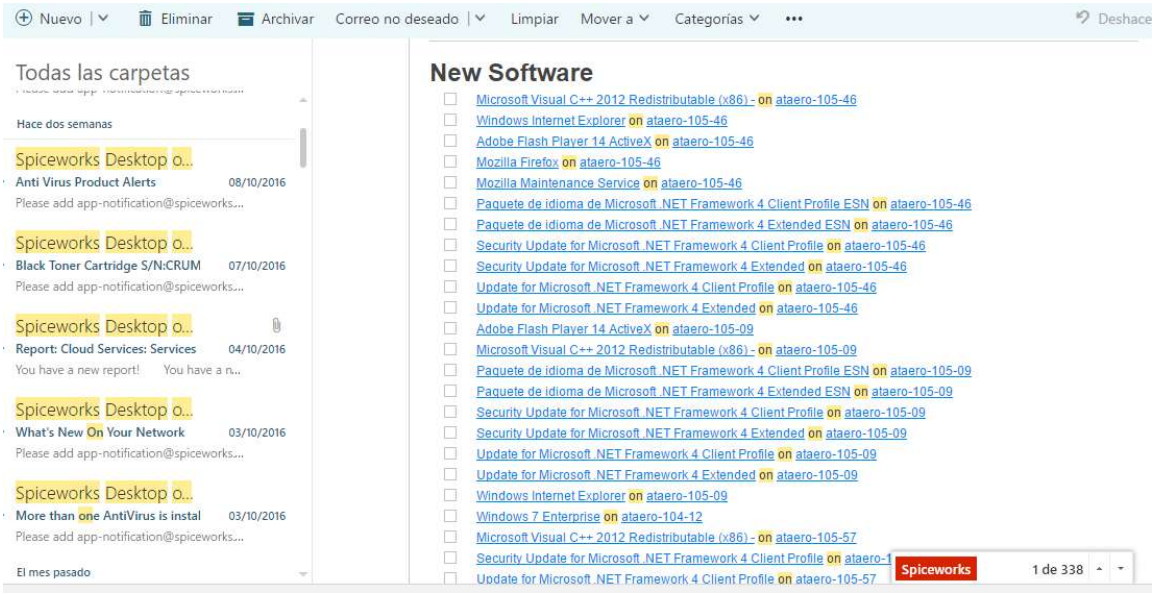


Figura 4.5 Aletas por correo electrónico de la herramienta Spiceworks

Así mismo la herramienta nos permite ver las VLAN de Voz e inventariarlas de la misma que las VLAN de datos, al igual que las impresoras.

Spicework nos permite ver un "pizarrón" o "dashboard con la IP's que se encuentran activas en la red, **ver Figura 4.6.**

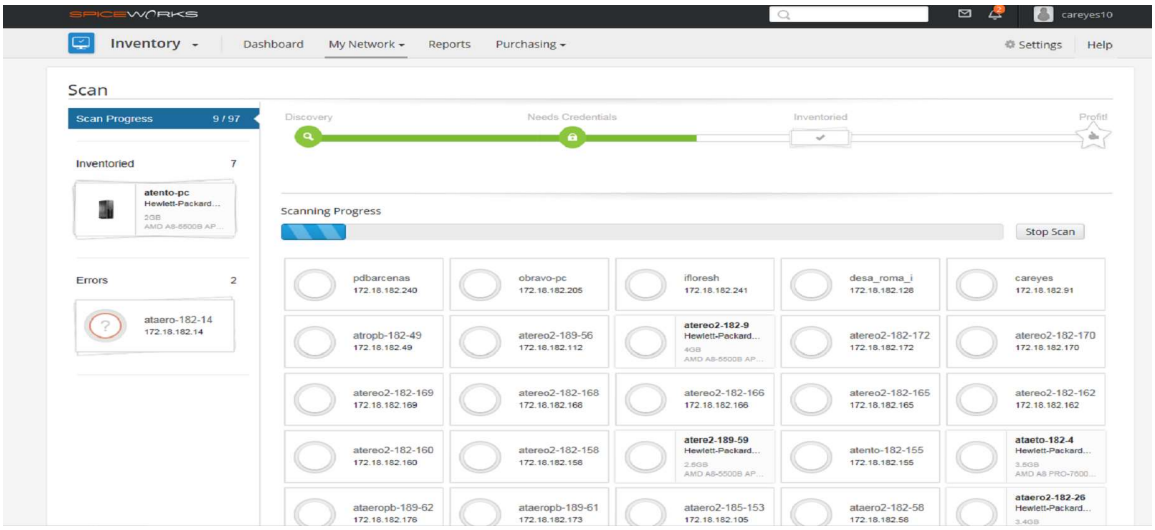


Figura 4.6. Dashboard o "pizarrón" de Spiceworks

Con esta herramienta resulta más eficiente el proceso de poder mapear e identificar las características de los equipos que se tienen en la sede principal y poder proyectar la implementación para la sede alterna. Todo administrador de tecnología en un Contact Center debe de contar con un mapa de las estaciones de trabajo asociadas con algún identificador y algún dato tecnológico que permita identificarlo, ya sea IP o extensión telefónica, **ver Figura 4.7**.

Figura 4.7. Mapa de administración de estaciones de trabajo del Contact Center

Es importante que el administrador de tecnología al tener el mapa ubicado de sus posiciones a cada una de ellas le asocie la siguiente información, **ver Tabla 4.2**:

Tabla 4.2. Información de posiciones asociadas a un ID

ID	Dato
IP	
Extensión	
IP Avaya	
IP Call Server Avaya (PBX)	
Hostname	
Política del Firewall	
IP Antivirus	
Dominio	
Switch/Pila/Puerto	
Piso	

Se empata los resultados se tiene lo siguiente para las estaciones de trabajo, considerándolos por cada una de las líneas de trabajo dentro de la sede principal, **véase en la Tabla 4.3**.

Tabla 4.3. Proyección para la implementación de la sede alterna

Soluciones Multicanal S.A. de C.V.	Segmento Bancario Cobranza		Segmento Aerolínea Reservaciones		
Componente	Operativo	Área Staff (supervisor, formador, agente de calidad, coordinador, clientes implant)	Operativo	Área Staff (supervisor, formador, agente de calidad, coordinador, clientes implant)	Total
Equipos de cómputo(CPU, monitor, teclado, mouse)	1200	50	230	20	1500
Teléfono (hardphone)	1200	50	230	20	1500
Diadema	1200	0	230		1430
Auricular		50		20	70
Impresoras		1		1	2

Así mismo se realiza la cuantificación de cada uno de los componentes principales dentro de la sede principal, **véase en la Tabla 4.4**.

Tabla 4.4. Cuantificación de los componentes de la sede principal

Soluciones Multicanal S.A. de C.V.					
Componente	Marca	Modelo	Memoria RAM	Microprocesador	Cantidad
Equipos de computo	Hewlett-Packard	Pro 6305 SFF	4 GB	AMD A8-6500B 3.50GHz	345
	Hewlett-Packard	EliteDesk 705 G1 SFF	4 GB	AMD A series A6 PRO-7400B / 3.5 GHz	279
	Hewlett-Packard	Pro 6300 SFF	4 GB	intel Core i5 3.2 GH	876
Teléfono VoIP	Avaya	9600	N/A	N/A	30
	Avaya	9650	N/A	N/A	800
	Avaya	4620	N/A	N/A	670
Diadema	Plantronics	Hw121n	N/A	N/A	1430
Adaptador HIC para Hardphone Avaya	Plantronics	A10-16	N/A	N/A	1420

4.1.2 Inventario de servidores, switches, routers y firewall

La segunda parte del reconocimiento de la infraestructura tecnológica son los componentes que se encuentran dentro de los SITE e IDF, estos son los principales equipos que permiten que sea

posible que los operadores puedan realizar sus funciones y atender a los clientes de los segmentos que se trabajan dentro de la empresa.

4.1.2.1 Servidores

Los servidores se encuentran dentro del SITE, y los cuales es importante tener de igual forma identificados al igual que los equipos de cómputo, pero agregando características de acuerdo al rol en los cuales se tienen utilizando.

La **Tabla 4.5** permite tener las principales características de cada uno de los servidores.

Tabla 4.5. Formato de inventario de Servidores

Inventario de Infraestructura Tecnológica- Servidores	Servidor 1	Servidor 2	Servidor 3
Centro	CC Soluciones Multicanal Sede Principal		
Numero de Fuentes de Poder	2		
Numero de Procesadores / Tipo / Velocidad	2-Intel(R) Xeon(R) CPU X5660 @ 2.80GHz		
Memoria	12 GB		
Nombre de Red	DNS_CC1		
Direccion (es) IP (s)	172.34.156.2		
Sistema Operativo	Microsoft Windows Server 2012 Standard		
Aplicaciones	DNS, AD, GPO		
Dominio	Solmulticanal.mexico.com		
Roll	DNS		
Marca	HP		
Modelo	ProLiant DL380 G7		
Número de Serie	PWE3455KJ3		
Número de Inventario	345-453222		
Número y Tipo de Discos Duros	5 SAS 10 K		
Número de Puertos de Red	2 ETERNETH		
Responsable de Administración	Tecnología		
Físico/Virtual	Físico		
Si es Virtual (IP del servidor Físico)	N/A		

El administrador de tecnología, dentro de su funciones y la más obligada, es tener estos componentes inventariados, etiquetados físicamente y tener el conocimiento de cada uno, adicional para complementar su administración deben ser agregados al sistema de monitoreo y poder siempre analizar y observar su comportamiento, y en caso de tener una falla critica, poder resolverla inmediatamente.

Otra buena práctica importante del administrador de tecnología es tenerlo en un segmento de red (VLAN) diferente a los equipos de cómputo, y equipos de comunicación (routers, SW, Firewall), cada categoría debe de estar en segmentos independientes.

Haciendo el empate con la herramienta SpiceWorks se tiene la siguiente información de los servidores actuales para la sede principal, **véase en la Tabla 4.6**.

Tabla 4.6. Cantidad de servidores de la sede principal

Soluciones Multicanal S.A. de C.V.											
Modelo de Servidores	Rol										
	Antivirus	BBDD	DCHP	DNS	FileServer	FileServer	Hyper-V	IIS	Backup	Grabación	Total general
HP ProDesk 600 G1 SFF	1										1
ProLiant DL380 G5						1		1	1		3
ProLiant DL380 G6		2			1					2	5
ProLiant DL380 G7						1	1	1			3
ProLiant DL380p Gen8							2	1			3
ProLiant DL580 G5				1							1
System x3650 M2 -[7947AC1]-										1	1
Z1506										1	1
Virtual		2	1	1		3		12			19
Total general	1	4	1	2	1	5	3	15	1	4	37

4.1.2.2 Switches, router, firewall y enlaces de comunicación

Al igual que los servidores, se debe tener el inventario de los equipos de comunicación, y deben de ser monitoreados dentro de la herramienta implementando, el área de tecnología debe tener dentro de su inventario de la siguiente forma los componentes de infraestructura (**ver Tabla 4.7, 4.8, 4.9**):

Switch:

Tabla 4.7. Formato de inventario de Switches

Inventario de Infraestructura Tecnológica- Switches	Switch/Stack 1	Switch/Stack 2	Switch/Stack 3
Centro	CC Soluciones Multicanal Sede Principal		
Ubicación	Piso 1		
Marca	AVAYA		
Modelo	4850GTS-PWR+		
Direccion IP de Administración	10.236.220.10		
Protocolo de Auntenticación	TELNET		
VLANs a las que da Servicio	Datos (50,51,52,53) Voz (60,61)		
Número de Serie	12U4893LKLK		
Número de Inventario	354—23453		
Número y Tipo de Puertos	48 Ethernet, 2 FO		

Velocidad 10/100/1000	100		
Responsable de Administración	Tecnología		
Fecha de actualización			

Routers:

Tabla 4.8. Formato de inventario de Routers

Inventario de Infraestructura Tecnológica- Routers	Router 1	Router 2	Router 3
Centro	CC Soluciones Multicanal Sede Principal		
Ubicación	Piso 1		
Marca	CISCO		
Modelo	Serie 3800		
Direccion IP de Administración	10.236.221.11		
Protocolo de Auntenticación	TELNET		
Número de Serie	234FG789		
Número de Inventario	124HDF48		
Número y Tipo de Puertos	2 Eterneth		
Responsable de Administración	Tecnología		
Fecha de actualización			

Firewall:

Tabla 4.9. Formato de inventarios de Firewall

Inventario de Infraestructura Tecnológica- Firewall	Equipo 1	Equipo 2	Equipo 3
Centro	CC Soluciones Multicanal Sede Principal		
Ubicación	Piso 1		
Marca	Palo Alto		
Modelo	PA-500		
No.Serie	00189PAN-500		
Direccion IP de Administración	10.236.221.20		
Protocolo de Auntenticación	SSL		
Número y Tipo de Puertos	4		
Responsable de Administración	Tecnología		
Fecha de actualización			

En la **Tabla 4.10** se tiene contabilizado los siguientes componentes:

Tabla 4.10. Equipos contabilizados en la sede principal

Equipo	Marca	Modelo	Tipo	Cantidad
Switch	AVAYA	4850GTS-PWR+	Acceso	38
Switch	Avaya	7000 series	Perimetral	2
Router	HP	HPE MSM Controller Series	WiFi	1
Access Point	HP	M330 802.11ac	WiFi	5
Router	Cisco	3800		2

Es importante tener dos consideraciones, en este punto:

- Los enlaces de comunicación en el caso del Contact Center son contratados hacia un proveedor tercero, tanto para los enlaces de internet y enlaces dedicados, por lo cual ellos son los encargados de instalar la infraestructura necesaria para poder realizar la comunicación entre los diferentes puntos de conexión
- En necesario contar con routers de configuración para poder realizar ruteos o direccionamientos y NAT a destinos específicos, para ligas web y aplicaciones cliente-servidor del cliente.

4.1.3 Diagramas de red

El siguiente paso, después de tener identificado los componentes tecnológicos se debe plasmar en un diagrama de red en el que se pueda apreciar el cómo se tiene configurado, para poder realizar la conexión hacia la nueva sede.

En la **Figura 4.8** se puede observar la interconexión de los equipos de cómputo al switch de acceso más cercano, posteriormente estos switches conectados por puerto de fibra óptica hacia el switch perimetral.

El switch perimetral, recibe a su vez los routers de conexión y permite la interacción entre todos los routers de internet, dedicados y enlace del tipo MPLS hacia las estaciones de trabajo de los asesores.

Así mismo se realizan las interacciones entre la telefonía del PBX, correos, servidores y las estaciones de trabajo.

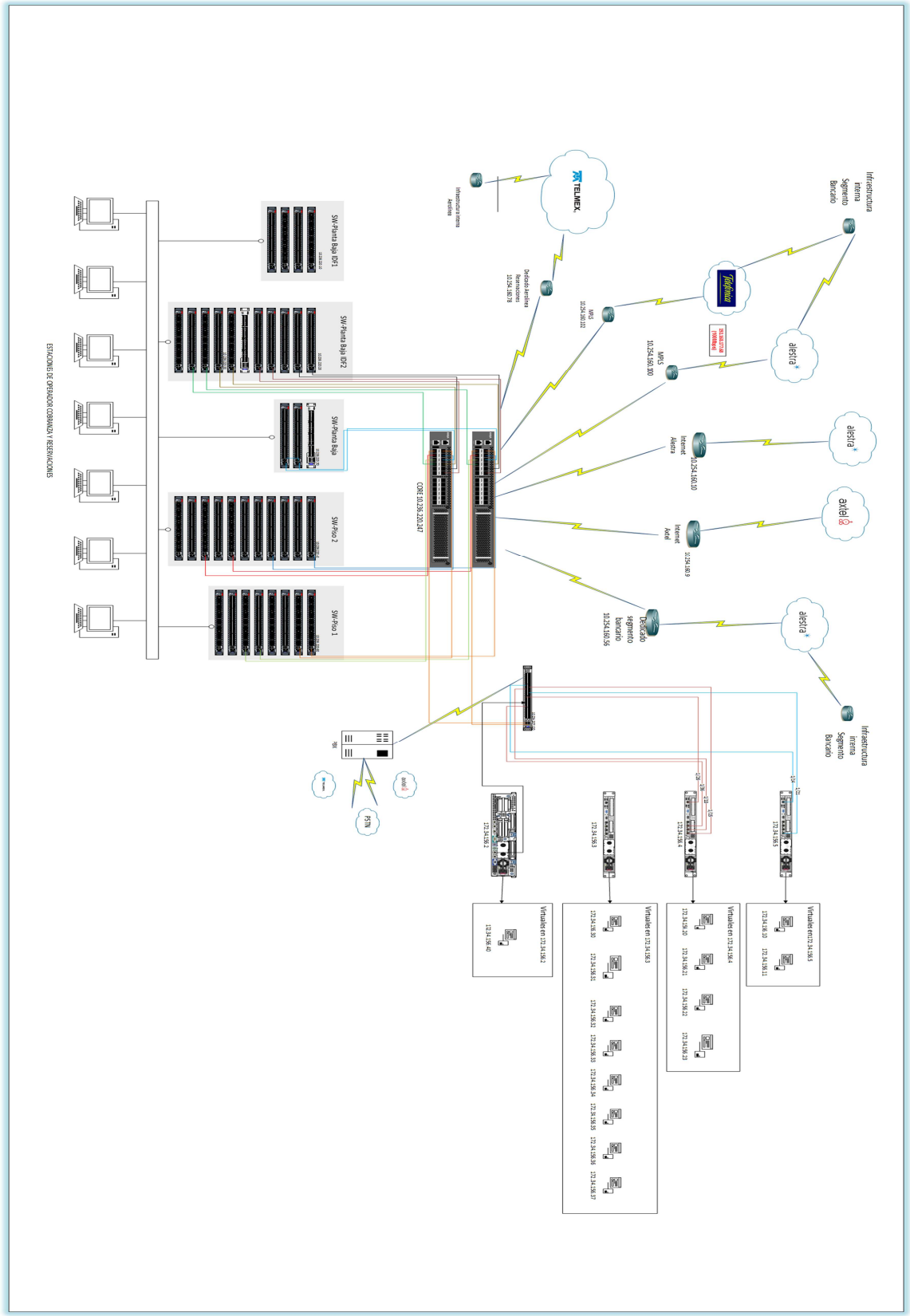

TELMEX
Infraestructura interna Segmento Bancario
Telefónica
alestra
axtel
MPLS 10.254.160.100
Internet Alestra 10.254.160.10
Internet Axtel 10.254.160.9
Dedicado segmento bancario 10.254.160.55
Dedicado Servicios Remotos 10.254.160.78
MPLS 10.254.160.101
CORE 10.226.220.247
SW-Planta Baja IDF1
SW-Planta Baja IDF2
SW-Planta Baja
SW-Piso 2
SW-Piso 1
ESTACIONES DE OPERADOR COBRANZA Y RESERVACIONES
PBX
PSTN
Virtuales en 172.24.136.2
Virtuales en 172.24.136.3
Virtuales en 172.24.136.4
Virtuales en 172.24.136.5

Figura 4.8. Diagrama de red de la sede principal

4.2 Diseño de la nueva sede y su implementación

Teniendo identificado todos los componentes actuales de la sede principal del Contact Center se realiza la proyección para poder abastecer los requerimientos solicitados por el cliente, dando por resultado el siguiente listado de componentes a comprar, la sede alterna toma algunos componentes de la sede primaria tales como son el PBX, y recursos de algunos servidores de aplicaciones.

EL nuevo Contact Center cuenta con su propio servidor DNS, Almacenamiento, bases de datos y aplicaciones en sistema de redundancia en caso de caer en la sede principal, se pueda utilizar en la sede alterna aminorando la afectación por la caída de la sede principal. El nuevo edificio debe de contar con su propio esquema de cortafuegos, **ver Tabla 4.11**.

El proyecto deberá contemplar lo siguiente para su implementación:

Tabla 4.11 Proyección de la inversión para la implementación de la sede alterna

CANTIDAD	DESCRIPCION	COSTO UNITARIO	TOTAL USD	TOTAL MXN + IVA
320	PC´S	USD 560.00	USD 179,200.00	MXN 4,157,440.00
7	SWITCH	USD 5,000.00	USD 35,000.00	MXN 812,000.00
2	SWITCH PERIMETRAL	USD 5,000.00	USD 10,000.00	MXN 232,000.00
2	Switch para Core	USD 80,000.00	USD 160,000.00	MXN 3,712,000.00
8	Servidores HP DL380 Gen9 6SFF CTO SERVER #2	USD 110,000.00	USD 880,000.00	MXN 20,416,000.00
2	GRABACION	USD 800.00	USD 1,600.00	MXN 37,120.00
280	GRABACION	USD 800.00	USD 224,000.00	MXN 5,196,800.00
320	LICENCIAS MSFT	USD 43.02	USD 13,766.40	MXN 319,380.48
280	DIADEMAS + POLARIS	USD 35.00	USD 9,800.00	MXN 227,360.00
320	HARDPHONE AVAYA	USD 155.00	USD 49,600.00	MXN 1,150,720.00
10	CINTA DE RESPALDO LTO5	USD 98.00	USD 196.00	MXN 4,547.20
44	LICENCIAS DE OFFICE	USD 300.00	USD 13,200.00	MXN 306,240.00
640	PATCH CORD + CAT5 - RJ45 DE 3 METROS	USD 7.00	USD 4,480.00	MXN 103,936.00
2	ALMACENAMIENTO	USD 40,000.00	USD 80,000.00	MXN 1,856,000.00
3	LICENCIAMIENTO SERVER	USD 3,000.00	USD 9,000.00	MXN 208,800.00
2	LICENCIAMIENTO SQL	USD 2,700.00	USD 5,400.00	MXN 125,280.00
2	LICENCIAMIENTO VIRTUAL	USD 1,000.00	USD 2,000.00	MXN 46,400.00
1	SERVIDOR BBDD	USD 15,000.00	USD 15,000.00	MXN 348,000.00
1	FIREWALL	USD 68,000.00	USD 68,000.00	MXN 1,577,600.00

1	LICENCIAS BLANCCO	USD 500.00	USD 500.00	MXN 11,600.00
		Total:	USD 1,760,742.40	MXN 40,849,223.68

Adicional de estos componentes para poder realizar la implementación se requiere la contratación de los proveedores para los enlaces dedicados y de internet.

Manteniendo el mismo esquema de la sede principal, se necesitan dos enlaces dedicados con configuración MPLS que en primera instancia permitan la comunicación punto a punto entre los Contact Center, así como la conexión y el destino privado del segmento bancario de cobranza, mismo que se le solicita al área de tecnología del banco otorgue los permisos en sus cortafuegos, de igual forma como sistema de contingencia hacia el segmento bancario se puede configurar un NAT en el router de la sede principal, para que la información viaje del enlace MPLS y dar el salto por el enlace dedicado que se tiene en la sede principal.

Sobre estos mismos enlaces teniendo la conexión a la sede principal se podrá realizar el enrutamiento y los NAT necesarios para permitir la comunicación para el plan de continuidad de negocio del segmento de la aerolínea.

Adicional se contrata dos servicios de internet a proveedores distintos para cumplir con un enlace de redundancia. La solicitud a los proveedores serían los siguientes enlaces Eterneth, **ver Tabla 4.12**.

Tabla 4.12. Proyección de los enlaces de comunicación para la sede alterna

Proveedor	Tipo de enlace	Capacidad
Telmex	Dedicado MPLS	50 MB Simétrico
Telefónica	Dedicado MPLS	50 MB Simétrico
Alestra	Internet	25 MB Simétrico
Telmex	Internet	25 MB Simétrico

La adquisición del ancho de banda a contratar se puede definir de la siguiente manera:

Por cada estación de operador se ocupan 1.5 canales de E1, en los cuales ya están incluidos los servicios VoIP y de datos por función local de consumo de datos y utilización para sus servicios.

Lo cual lleva a la siguiente información para la adquisión de los enlaces dedicados para 300 Estaciones de operador:

Canales E1= 1.5*300= 450

Canales disponibles por E1=30

E1's necesarios= 450/30 = 15

Utilización en MB's por E1= 2MB

Ancho de banda requerido = 2 MB*15 (E1's)= 30 MB

La adquisición de un enlace dediado de 50 MB da una garantía de tener una disponibilidad para una no saturación de 30-40 %.

Las **Tablas 4.13 y 4.14** se pueden apreciar el costo de contratación para los enlaces dedicados por el proveedor Telmex, así como los costos por renta mensual, de acuerdo a las capacidades que se requieren.

Tabla 4.13 Costos de instalación de enlaces de comunicación

Cargos iniciales:

Las tarifas que aplicarán por concepto de gastos de instalación, por cada Sitio, dependerá del tipo de interfase entregada al cliente, las cuales serán: Fast Ethernet ó Giga bit Ethernet y uno o varios tramos de Larga Distancia si existe la necesidad de conectar poblaciones con distintas redes interurbanas.

Ancho de Banda	Local		Larga Distancia	
	GI Fast Ethernet	GI GB Ethernet	GI Fast Ethernet	GI GB Ethernet
4 Mbps	$125,000	No Aplica	$ 62,500	No Aplica
6 Mbps	$ 125,000	No Aplica	$ 62,500	No Aplica
8 Mbps	$ 125,000	No Aplica	$ 62,500	No Aplica
10 Mbps	$ 250,000	No Aplica	$ 125,000	No Aplica
20 Mbps	$ 250,000	No Aplica	$ 125,000	No Aplica
30 Mbps	$ 250,000	No Aplica	$ 125,000	No Aplica
40 Mbps	$ 250,000	No Aplica	$ 125,000	No Aplica
50 Mbps	$ 250,000	No Aplica	$ 125,000	No Aplica
60 Mbps	$ 250,000	No Aplica	$ 125,000	No Aplica
70 Mbps	$ 250,000	No Aplica	$ 125,000	No Aplica
80 Mbps	$ 250,000	No Aplica	$ 125,000	No Aplica
90 Mbps	$ 250,000	No Aplica	$ 125,000	No Aplica
100 Mbps	$ 250,000	$ 500,000	$ 125,000	$ 250,000
150 Mbps	No Aplica	$ 500,000	No Aplica	$ 250,000
200 Mbps	No Aplica	$ 500,000	No Aplica	$ 250,000
250 Mbps	No Aplica	$ 500,000	No Aplica	$ 250,000
300 Mbps	No Aplica	$ 500,000	No Aplica	$ 250,000
350 Mbps	No Aplica	$ 500,000	No Aplica	$ 250,000
400 Mbps	No Aplica	$ 500,000	No Aplica	$ 250,000
450 Mbps	No Aplica	$ 500,000	No Aplica	$ 250,000
500 Mbps	No Aplica	$ 500,000	No Aplica	$ 250,000
550 Mbps	No Aplica	$ 500,000	No Aplica	$ 250,000
600 Mbps	No Aplica	$ 500,000	No Aplica	$ 250,000
750 Mbps	No Aplica	$ 500,000	No Aplica	$250,000
1000 Mbps	No Aplica	$ 500,000	No Aplica	$ 250,000

Estos Precios No Incluyen IVA

Tabla 4.14 Costos de renta mensual de los enlaces

Cargos Recurrentes:

Las tarifas que aplicarán por concepto de renta mensual por cada sitio, son las siguientes:

Ancho de Banda	Fast y Gigabit Ethernet	
	Local	LD X KM
4 Mbps	$ 9,500	$ 75.00
6 Mbps	$ 13,000	$ 87.00
8 Mbps	$ 16,500	$ 102.00
10 Mbps	$ 18,500	$ 114.00
20 Mbps	$ 25,500	$ 120.00
30 Mbps	$ 29,800	$ 140.00
40 Mbps	$ 39,400	$ 156.00
50 Mbps	$ 46,200	$ 180.00
60 Mbps	$ 50,300	$ 198.00
70 Mbps	$ 54,600	$ 210.00
80 Mbps	$ 58,900	$ 216.00
90 Mbps	$ 63,200	$ 220.00
100 Mbps	$ 65,000	$ 225.00
150 Mbps	$ 95,800	$ 315.00
200 Mbps	$ 122,600	$ 420.00
250 Mbps	$ 144,000	$ 488.00
300 Mbps	$ 165,500	$ 585.00
350 Mbps	$ 187,100	$ 683.00
400 Mbps	$ 208,500	$ 780.00
450 Mbps	$ 230,000	$ 878.00
500 Mbps	$ 251,500	$ 894.00
550 Mbps	$ 272,900	$ 983.00
600 Mbps	$ 294,500	$ 1,073.00
750 Mbps	$ 399,700	$ 1,341.00
1000 Mbps	$ 507,100	$ 1,625.00

Estos Precios No Incluyen IVA

En las **Figuras 4.9 y 4.10** se puede observar que la capacidad contratada es proporcional a la cantidad de estaciones de operador y no se logra superar las capacidades dentro de los horarios picos en la sede central.

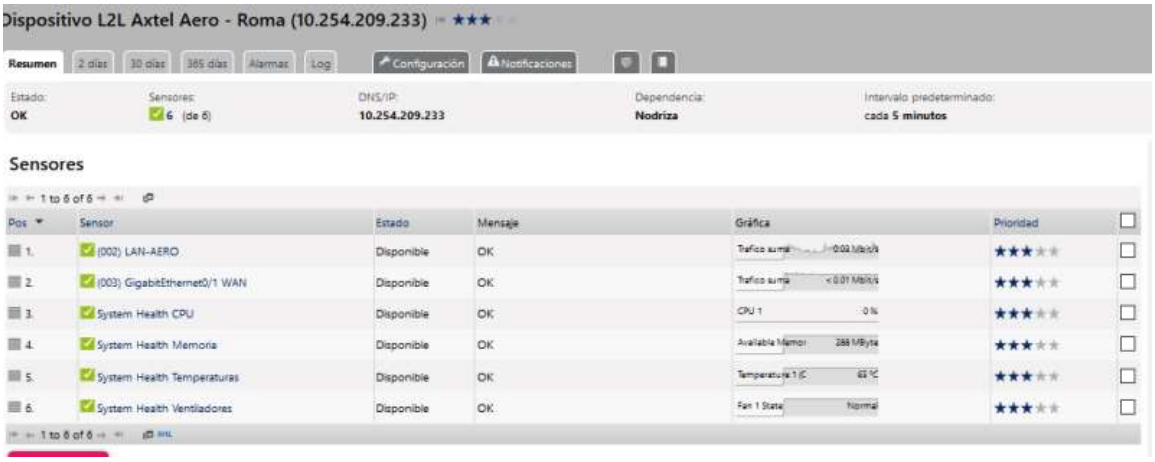


Figura 4.9. Imagen del sistema de monitoreo de tráfico en tiempo real enlace dedicado

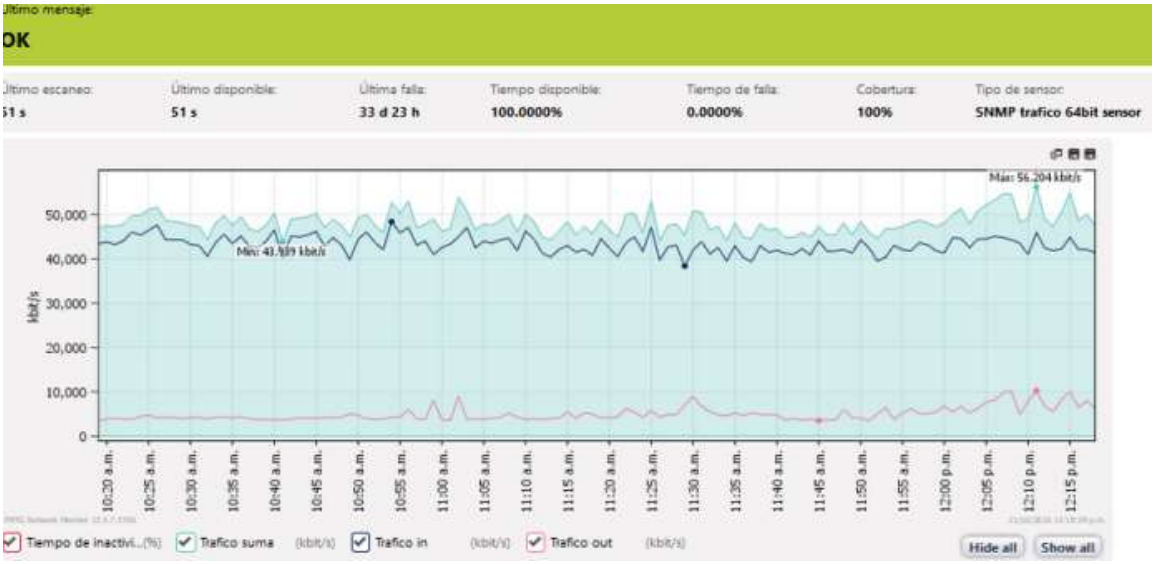


Figura 4.10. Grafica del sistema de monitoreo de tráfico en tiempo real del enlace de internet

La implementación de la sede alterna se puede completar en este momento una vez teniendo la sede alterna, y solicitando a los proveedores la instalación de los enlaces de comunicación.

Al tener la dependencia de la sede principal, llega a facilitar y centralizar los servicios, por lo cual la implementación se completa de la siguiente forma, mostrada en la **Figura 4.11** que muestra el diagrama de red.

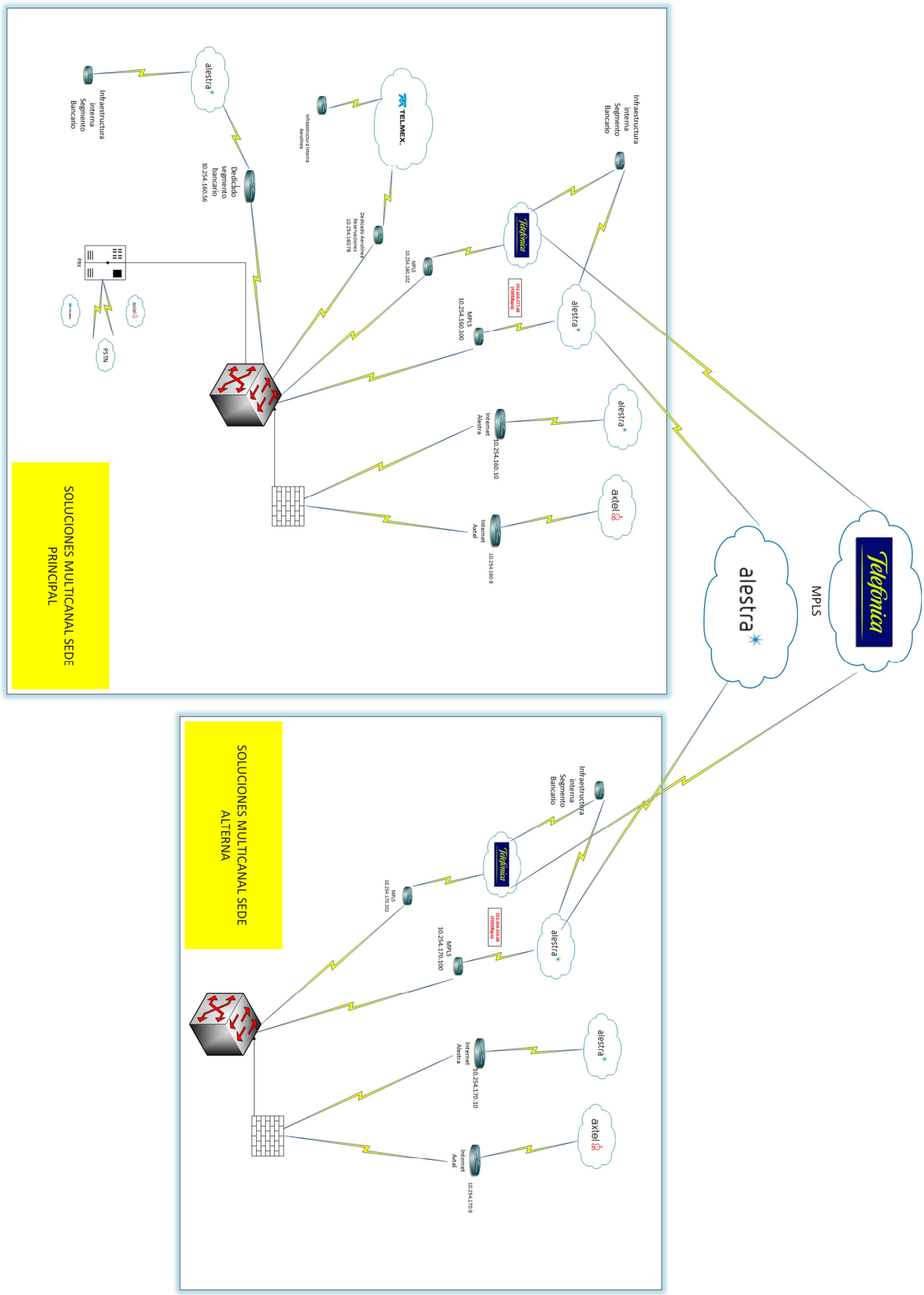

SOLUCIONES MULTICANAL SEDE PRINCIPAL
Infraestructura interna Segmento Bancario
alestra
Dedicado segmento bancario 10.254.160.56
TELMEX
Infraestructura interna Asesores
Dedicado Asesores Reservaciones 10.254.160.78
PBX
PSTN
MPLS 10.254.160.102
Telefónica
MPLS 10.254.160.100
alestra
Internet Alestra 10.254.160.10
axtel
Internet Axtel 10.254.160.9
MPLS
alestra
Telefónica
SOLUCIONES MULTICANAL SEDE ALTERNA
Infraestructura interna Segmento Bancario
MPLS 10.254.170.102
MPLS 10.254.170.100
alestra
Internet Alestra 10.254.170.10
axtel
Internet Axtel 10.254.170.9

Figura 4.11. Diagrama de red e interconexión entre la sede principal y alterna

La **Figura 4.11.** Muestra la interconexión entre las sedes del Contact Center, en la cual se aprecia la conexión entre las sedes por los enlaces dedicados, respectivamente por el enlace principal y por el sistema de redundancia. La nueva sede cuenta con la infraestructura para abastecer las necesidades de internet para los segmentos bancarios y la aerolínea, conectados a un Firewall que previene la intrusión de alguna amenaza externa y control absoluto de los accesos de las estaciones de trabajo, solo permitiendo los accesos justificados contractualmente. La sede principal abastece de los servicios de telefonía y algunos servicios de servidores como correo.

Lo restante para esta implementación es la configuración de los equipos con los mismos aplciativos de la sede principal, configuración de los switches internos y creación de las VLAN y propagarlas en los equipos perimetrales y routers para el reconocimiento entre las redes de ambas sedes, actividad que realiza el áera dedicada de redes.

CAPÍTULO 5 Estructura administrativa de los procesos de seguridad informática.

Desarrollar las directrices para el tratamiento, transmisión y almacenamiento de información buscando la disponibilidad, integridad y confidencialidad de la misma, con el fin de garantizar como proveedor la confidencialidad de los clientes y mantener los lineamientos de seguridad informática para cada una línea de negocio, es el tema a tratar en este apartado, ya que por temas de seguridad informática, es una petición de los clientes tener homologados los procesos a mencionar.

Es de aplicación en todas las fases del ciclo de vida de la información utilizada por Soluciones Multicanal (generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción) y en las infraestructuras (sistemas y redes) que la procesan (análisis, diseño, desarrollo, implantación, explotación y mantenimiento).

La **Figura 5.1,** indica las funciones a desempeñar en el área de tecnología, aprecie que posterior a la solicitud de implementación realizada en el apartado 4, se deben diseñar controles de seguridad de la información, estos procesos de la misma forma se reciben y analizan con las áreas de negocio a solicitud del cliente, el área de seguridad informática establece los controles para ser enviados a tecnología para su revisión y ejecución. Finalizando y confirmando estas actividades el cliente revisa sean los correctos para evitar fugas de información y poder garantizar la confidencialidad de sus clientes finales, estableciendo una revisión por gestión propia o mediante algun auditor externo.

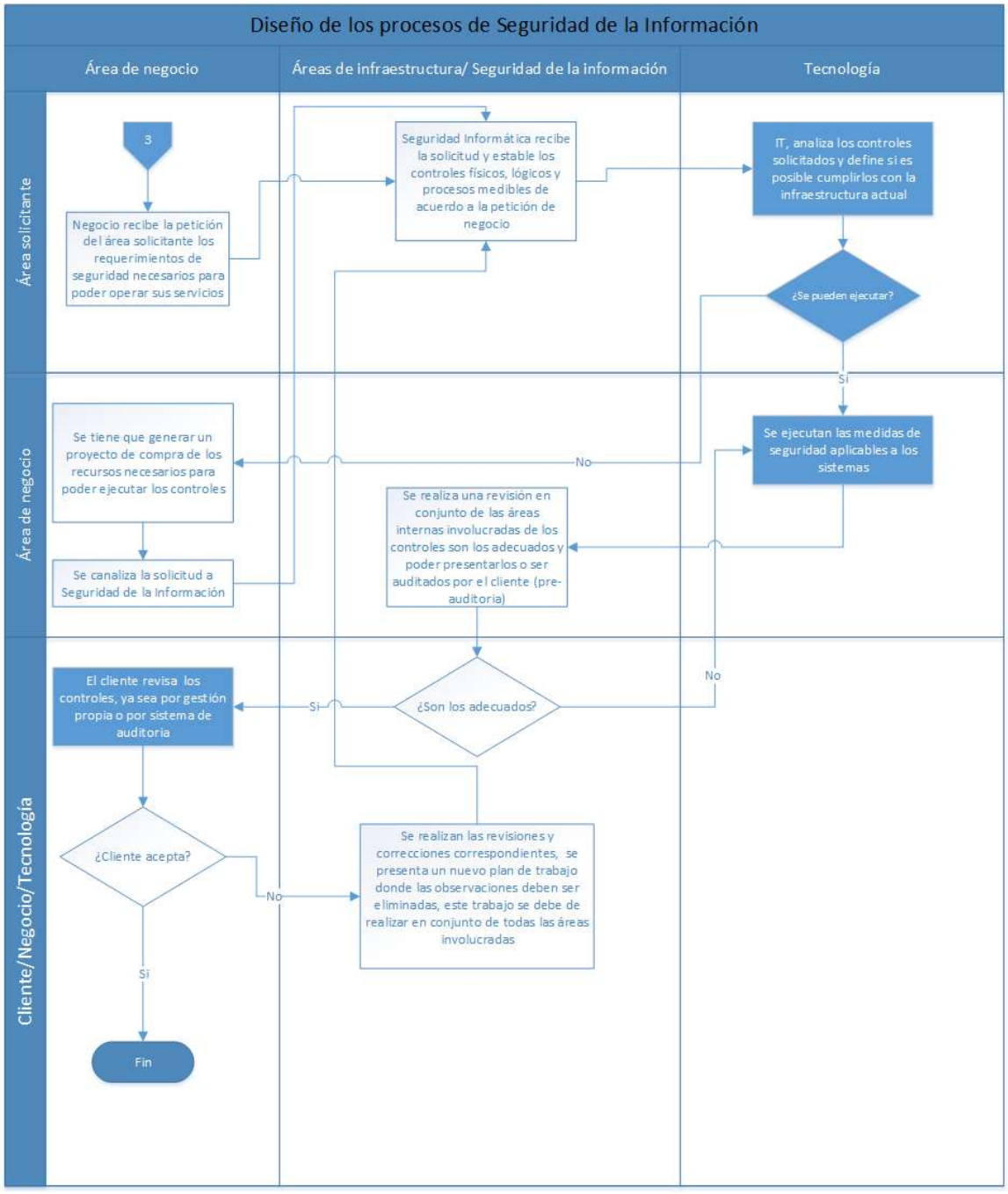


Figura 5.1. Diagrama de flujo del diseño de los procesos de Seguridad de la información

5.1 Desarrollo de la política de calidad y seguridad

La Política de **Calidad y Seguridad** establece el compromiso con la calidad en la gestión en un marco de seguridad de los activos involucrados en el modelo de negocio, sirviendo de referencia de actuación en estos ámbitos para todas las operaciones de Soluciones Multicanal.

Se ha integrado un comité de seguridad autónomo (conformado por Tecnologia, Seguridad Informatica, Servicios de Infraestructura, Recursos Humanos) que debe informar y responder todo requerimiento, evento o situación contraría a las políticas establecidas, este comité debe de estar incluido todos los representantes de tecnología y las principales figuras de las áreas administrativas (recursos humanos, relaciones laborales, servicios generales).

Dentro de la empresa se deben de realizar los siguientes lineamientos:

- Todo integrante de la empresa debe de conocer las políticas de seguridad física y tecnológica de la empresa
- Los gerentes de cada área deben de asegurar que las funciones y responsabilidades establecidas para cada uno de los empleados.
- Dentro de la carpeta de control se integran los contactos con la policía local, protección civil, servicio de ambulancia y bomberos de cada Contact Center, la cual ha de estar de forma visible y/o accesible.
- El gerente de cada área es responsable de mantener actualizados los contactos con los proveedores críticos correspondientes a los activos de información.
- La información no puede ser guardada en los equipos portátiles, solo en los servidores de Soluciones Multicanal y la conexión fuera de las instalaciones se realiza mediante una VPN que es configurada de acuerdo a la autorización del comité y firmando una carta responsiva y autorizando solo los accesos necesarios para sus funciones.
- Todos los activos están asignados a un propietario que forme parte de la organización.
- Los recursos proporcionados por Soluciones Multicanal son utilizados únicamente para propósitos relacionados a la organización.
- En caso de incurrir en alguna violación a las políticas de Soluciones Multicanal se realizaran las acciones, que son una carta administrativa que se presentará ante el Comité de Seguridad y en caso de acumular dos cartas, procederá a desvinculación de la empresa, o en su efecto, desvinculación inmediata de la empresa.

5.1.1 Clasificación de la información

Toda información referente a la operación y negocios está clasificada en virtud de su importancia para la organización como lo indica el documento.

Tabla 5.1. Clasificación de la información

Información Reservada	Información de alta sensibilidad para la compañía, que debe ser protegida, ya sea por su relevancia sobre decisiones estratégicas, por imperativo legal o contractual, o por el impacto económico o de otra naturaleza, que puede producirse en caso de difundirse fuera de los límites especificados.

Información Restringida	Información sensible, interna de un área o propia de un proyecto, a la que sólo debe tener acceso controlado un grupo reducido de personas debido a que su difusión puede poner en peligro el buen fin de una operación, o afectar negativamente a los intereses de la compañía, sus clientes, asociados o empleados.
Información de Uso Interno	Información que, sin ser reservada ni restringida, debe mantenerse dentro el ámbito interno de la compañía, para salvaguardar sus intereses frente a sus competidores y por ser útil y necesaria únicamente sólo a efectos internos, salvo a terceras partes que estén involucradas con un previo compromiso de confidencialidad y consentimiento por parte del propietario del documento.
Información Pública	Información de dominio público cuya divulgación no afecta negativamente a la empresa en términos de pérdida de imagen y/o económica. Así mismo, esta información puede ser consultada por cualquier persona internamente o fuera de la empresa.
Personas Iniciados	Relación de personas de Soluciones Multicanal que tienen acceso a la información dependiendo de su clasificación definida; estas personas, deben firmar el correspondiente acuerdo de confidencialidad, quedando obligadas en los términos allí recogidos, durante el plazo previsto en esta norma o el que determine el propietario de la Información.

Siguiendo el siguiente flujo de información, se define por el comité y en conjunto con el cliente de la respectiva línea de negocio el tratamiento a seguir de acuerdo a la información que es entrega a Soluciones Multicanal, **ver Figura 5.2**.

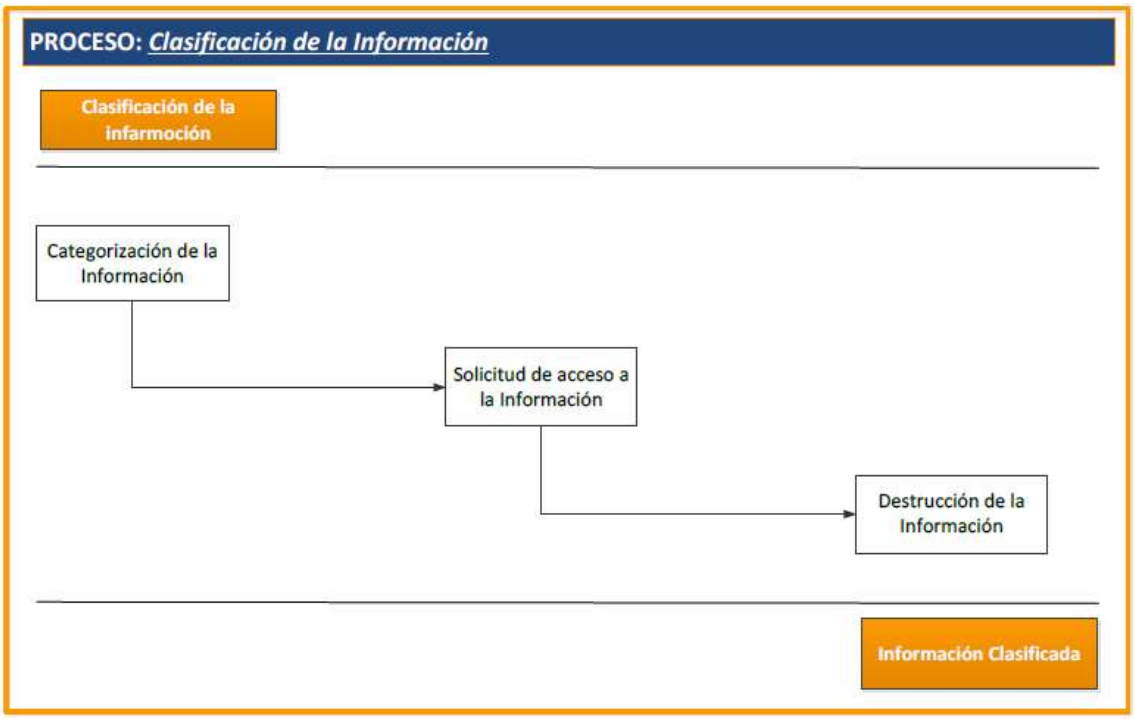


Figura 5.2. Proceso para la clasificación de la información

5.1.2 Manipulación de los soportes

Se prohíbe la extracción de información y se debe de tener una herramienta de borrado seguro

- Los accesos a internet, puertos activos para discos flexibles, USB, CD, DVD o cualquier dispositivo magnético o electrónico que permita poner en riesgo la seguridad de la información se encuentran deshabilitados.
- La destrucción de los dispositivos de almacenamiento que contengan información sensible se efectúa de la siguiente forma:

El Usuario solicita al Gerente, el borrado seguro de la información, para que esté proceda con el levantamiento dentro de alguna herramienta para reporte de incidencias y requerimientos, la solicitud de la depuración de la información requerida. Cuando la solicitud es liberada, se direcciona al área de Soporte Tecnológico, la cual analiza la requisición e identifica el proceso, si se va a realizar en dispositivos de almacenamiento se procede a contratar los servicios de borrado seguro a especialistas, los cuales ejecutan directamente en el centro que requiere el servicio, el proceso de borrado, obteniendo y entregando al responsable de Soporte Tecnológico un acta de hechos, donde marca la realización del proceso satisfactorio. En caso de que no sean dispositivos de almacenamiento, Soporte Tecnológico realiza el proceso de borrado seguro con el aplicativo que adquirió Soluciones Multicanal, para el cumplimiento de este proceso, **ver Figura 5.3**.

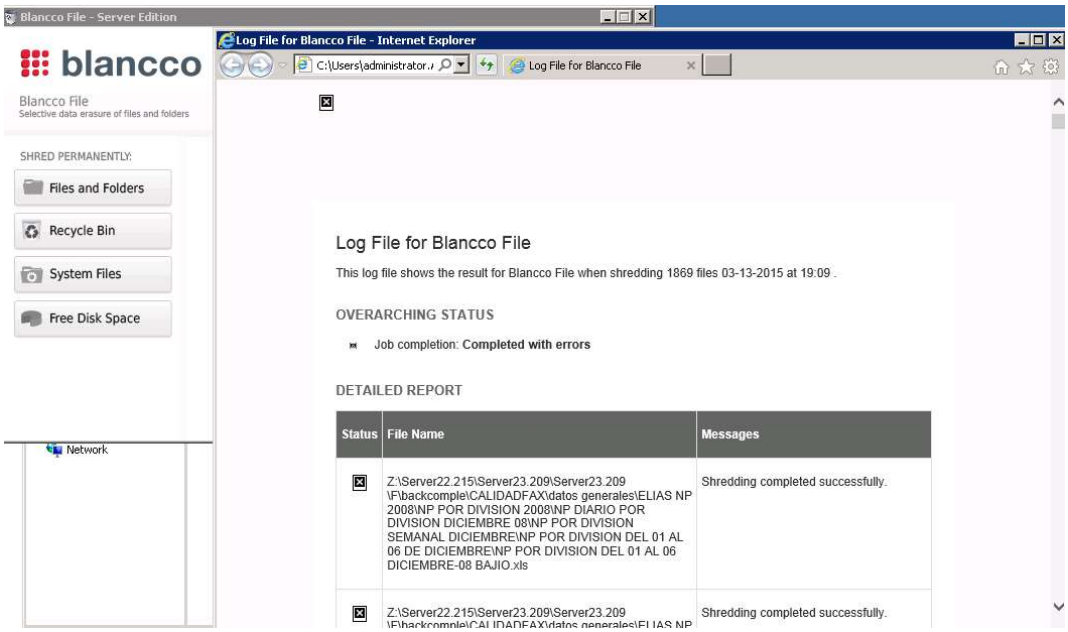


Figura 5.3. Evidencia de borrado seguro mediante la herramienta Blancoo

5.1.3 Control de acceso a sistemas y aplicaciones

Se debe de tener el control absoluto en los sistemas tecnológicos que impliquen un riesgo a la información e integridad de Soluciones Multicanal.

1. Todos los sistemas sensibles en Soluciones Multicanal se encuentran en ordenadores dedicados (aislados) y el acceso y/o privilegios de los sistemas se realiza bajo las siguientes normativas:
    - Usuario de perfil único y personalizado.
    - Contar con claves secretas o contraseñas de encendido únicas con las siguientes especificaciones:
    - Expirar en rangos de 30 días o menos y mantener un histórico de 12 contraseñas para el personal administrativo y operativo.
    - Tres intentos fallidos consecutivos en el registro del password, bloquean el usuario.
    - Todo password del empleado utilizado por primera vez, debe ser modificado inmediatamente.
    - Las contraseñas se otorgan de forma presencial y/o vía telefónica.
    - Las contraseñas de administrador de los equipos de red y comunicaciones (Routers, Switch´s, servidores, etc.) están bajo resguardo del coordinador de soporte tecnológico del sitio donde se encuentren en operación los equipos, quedando prohibido el compartir y divulgar estas contraseñas a personal no autorizado.
    - Los equipos de red y comunicaciones tienen un usuario administrador total que es el responsable de gestionar los equipos. Si por motivos operativos debe existir más de un administrador de los equipos se han de crear cuentas de administrador, con un nivel jerárquico menor al del administrador total.
    - Suspender la sesión del usuario después de mostrar inactividad por más de 2 minutos para equipos operativos y 15 minutos para personal administrativo.
    - Contar con el papel tapiz y el protector de pantalla institucional.
2. Todos los usuarios tienen un identificador único (ID de usuario) y contraseña para su uso personal y exclusivo después de 3 intentos fallidos de ingreso el acceso se bloqueara.
3. Las normativas de seguridad en contraseñas han de seguir estos lineamientos:
    - Las contraseñas de acceso a los sistemas de información son de uso confidencial y no deben ser proporcionadas a otros usuarios.
    - Los usuarios deben mantener la confidencialidad de sus contraseñas, por lo cual queda prohibido anotarlas en un lugar de fácil descubrimiento, como son: libretas, notas, hojas, etc.
    - Los usuarios que tengan acceso a los sistemas críticos deben tener una cuenta personalizada ya que está prohibido generar cuentas de usuario genéricas o de grupo.
    - Los privilegios de estas cuentas deben estar restringidos, evitando que puedan tener acceso a información y sistemas confidenciales.
    - La configuración de las contraseñas deben ser suficientemente robustas para evitar un fácil descubrimiento por parte del personal no autorizado, incluyendo los equipos de comunicaciones.
    - No utilizar como password el identificador del usuario.
    - No utilizar el nombre del cliente, ni ninguno relacionado.
    - Utilizar caracteres alfanuméricos, mayúsculas, minúsculas, números y caracteres especiales, si el sistema lo soporta.
    - Longitud mínima de 8 (ocho) caracteres.

5.1.4 Controles Criptográficos

Toda la información sensible y crítica debe de ser encriptada para garantizar la seguridad de la misma

- La información clasificada como reservada, restringida y/o contenga datos personales (información sensible) así como la que este regulada por contratos con el cliente, debe ser enviada o trasmitida de forma cifrada, **ver Figura 5.4**. Los sistemas de cifrado utilizados cumplen con los requerimientos de seguridad así como con las normas o recomendaciones internacionales sobre algoritmos de cifrado, las bases de datos se manejan de manera cifrada y bajo los parámetros de seguridad que determine el área de seguridad informática, los cuales son:
- Seguridad en los archivos de sistemas
- Seguridad en los procesos de desarrollo y soporte
- Gestión de la vulnerabilidad técnica
- Las contraseñas para el cifrado de la información cumplen con los estándares deben cumplir con los estándares de establecidos en el apartado 5.1.3.

Figura 5.4. Aplicativo de encriptación

5.1.5 Seguridad de los equipos

Se debe de tener seguridad en los SITE e IDF y acceso controlado, asi como ir estableciendo procesos para tecnología.

- En cada uno de los diagramas del site y/o IDF´s de los diferentes Contact Center están localizados los sensores, equipos contra incendio, alarmas, accesos y salidas de emergencia, el ingreso a los mismos ha de ser controlados mediante accesos digitales y cartas responsivas de control de acceso.
- En caso de falla del suministro energético se solventa con la planta de energía.

- Las verticales eléctricas están bajo llave y los IDF´s por acceso de biométrico, solo se podrá ingresar con autorización del área responsable de igual forma el cableado de telecomunicaciones debe estar identificado y debidamente protegido.
- Los mantenimientos preventivos y correctivos para las instalaciones de Soluciones Multicanal se realizan de acuerdo a lo acordado con el cliente y estipulado por el comité y el responsable de tecnología, **ver Figura 5.5**

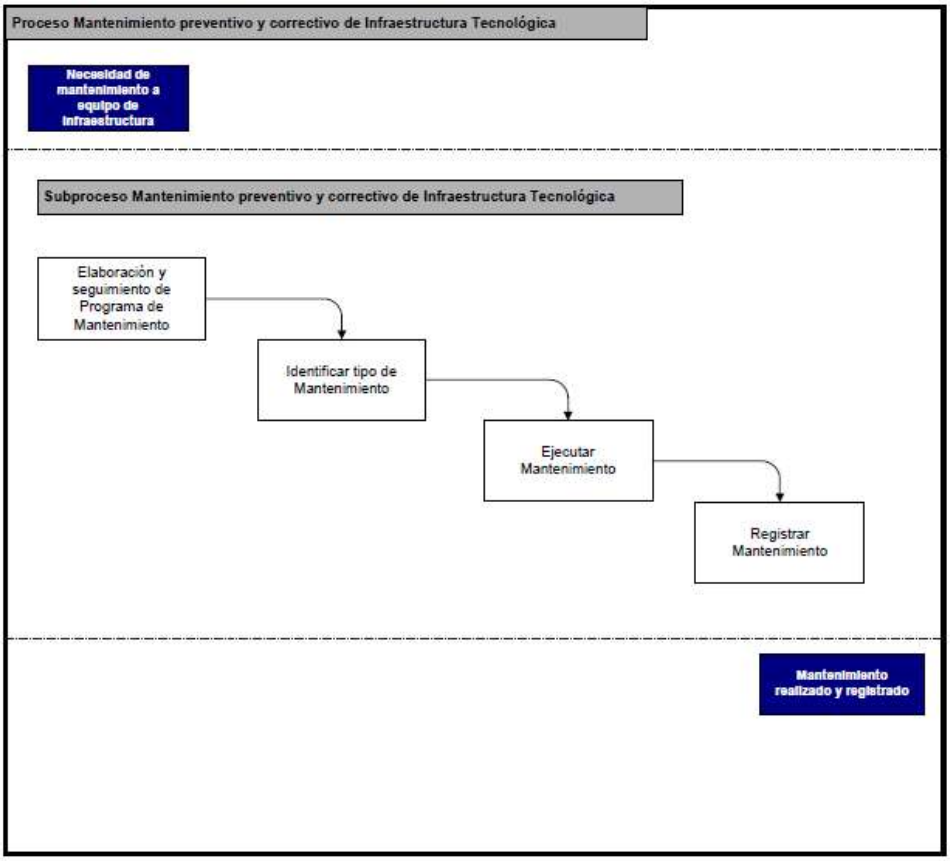


Figura 5.5. Procesos de Mantenimientos preventivos y correctivos

- Todas las PC's y laptops utilizadas por los empleados en el desarrollo de sus funciones han de ser bloqueados por el mismo antes de abandonar su puesto de trabajo.
- No está permitido utilizar hojas o libretas en las estaciones de trabajo, así como medios de almacenamiento desmontables.
- Soluciones multicanal tiene una solución antivirus corporativo que permite una administración de forma centralizada para tener un control de las actualizaciones y solución de incidencias de virus. Antes de ingresar a la red corporativa los equipos de cómputo (PC´s y servidores) han de tener instalado y actualizado el sistema antivirus. En caso de proveedores o clientes que requieran ingresar a la red corporativa del Contact Center se debe verificar que tengan instalado y actualizado un sistema antivirus; ante cualquier indicador de una posible infección masiva de

virus se debe de proceder a desconectar los equipos infectados y realizar los procedimientos de limpieza que estén establecidos para estas incidencias.

5.1.6 Copias de seguridad

Se deben de tener copias de seguridad (Bakcup) de la información almacenada en los servidores corporativos.

- Los respaldos se deben llevar a cabo de acuerdo a los lineamientos del procedimiento, **ver Figura 5.6.**

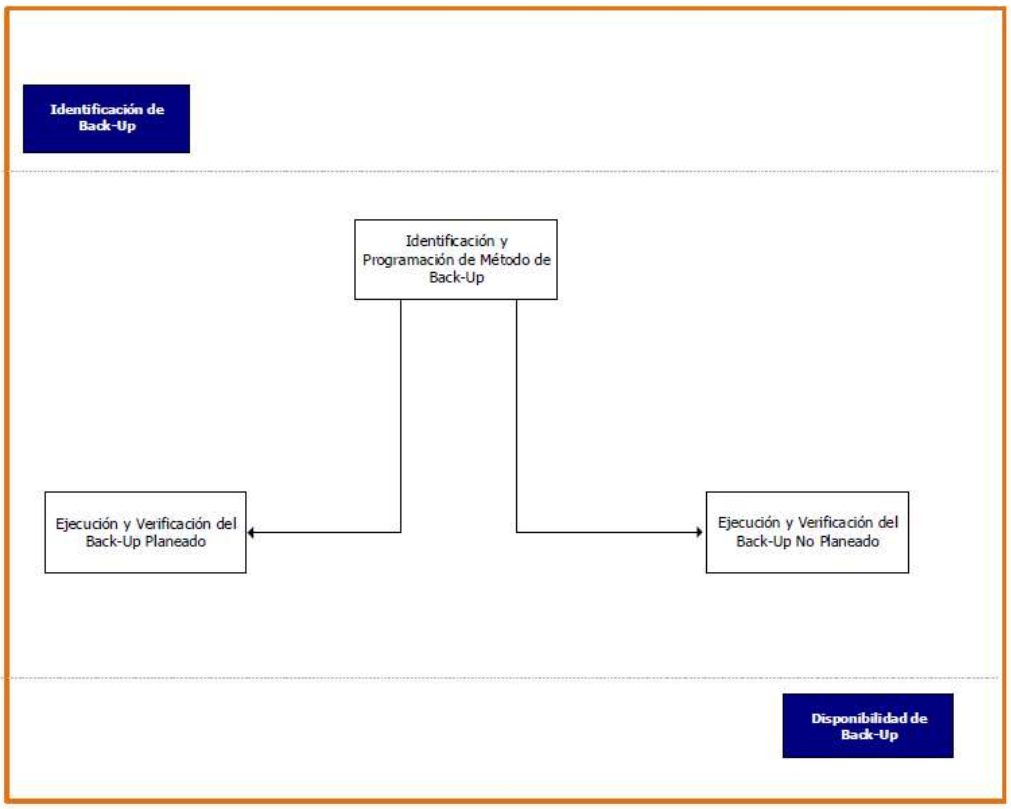
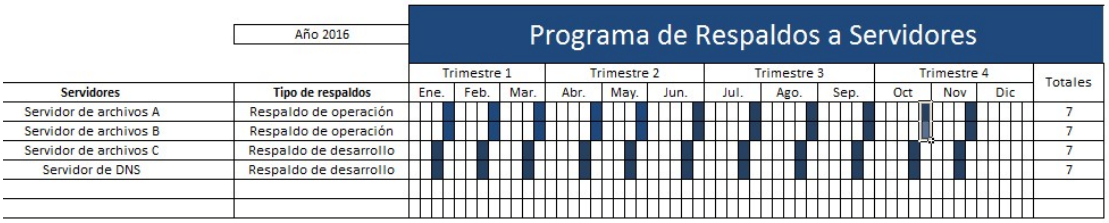


Figura 5.6. Proceso para los respaldos planeados y no planeados

Proceso para realizar los respaldos programados:

- Validar los servidores dedicados que contienen información de las operaciones, información de cliente, bases de datos, grabaciones de audio, ya que son los que se anexan al calendario de respaldos programados
- De acuerdo a la cantidad de información por cada servidor y lo establecido contractualmente se debe generar el calendario de respaldos, **ver Figura 5.7**.



Año 2016

Programa de Respaldos a Servidores

Servidores	Tipo de respaldos	Trimestre 1			Trimestre 2			Trimestre 3			Trimestre 4			Totales
		Ene.	Feb.	Mar.	Abr.	May.	Jun.	Jul.	Ago.	Sep.	Oct	Nov	Dic	
Servidor de archivos A	Respaldo de operación													7
Servidor de archivos B	Respaldo de operación													7
Servidor de archivos C	Respaldo de desarrollo													7
Servidor de DNS	Respaldo de desarrollo													7

Figura 5.7. Calendario de Respaldos Programados

- Establecer la nomenclatura para los respaldos

Ej. Día/mes/Año Hostname_servidor últimos_dos_octetos_IP

- Llenado de formato de respaldos, donde se tendrá registrado la actividad realizada, **ver Figura 5.8.**

MÉTODO DE BACKUP

NOMBRE DEL BACKUP: 09_16 156_34_E_H_SS

Área Usuaria SOPORTE TECNOLOGICO/OPERACIONES

Contenido del Backup:

Información correspondiente al servidor dentro de las unidades de almacenamiento.

Ubicación de Datos	Frecuencia
Servidor de archivos de sistemas y administrativos	Mensual
Nombre del equipo: FILE SERVER (172.34.156.34)	

Medio de Almacenamiento: Cinta LTO ULTRIUM 4

Reescritura sobre el medio de almacenamiento: SI NO

Se elimina el medio: SI NO **Período de Conservación de Medio:** 1 año

Automático

Nivel de Importancia de datos: Básico Intermedio Mayor **Modo de Ejecución:** Manual

Método del Backup:

Desde el servidor de respaldos y empleando el software de backup de Windows del mismo servidor se realiza el respaldo de las siguientes unidades mapeadas: \\172.34.156.34\E$,

Figura 5.8. Formato de respaldo

- Almacenamiento de logs al completar el respaldos, **ver Figura 5.9**.

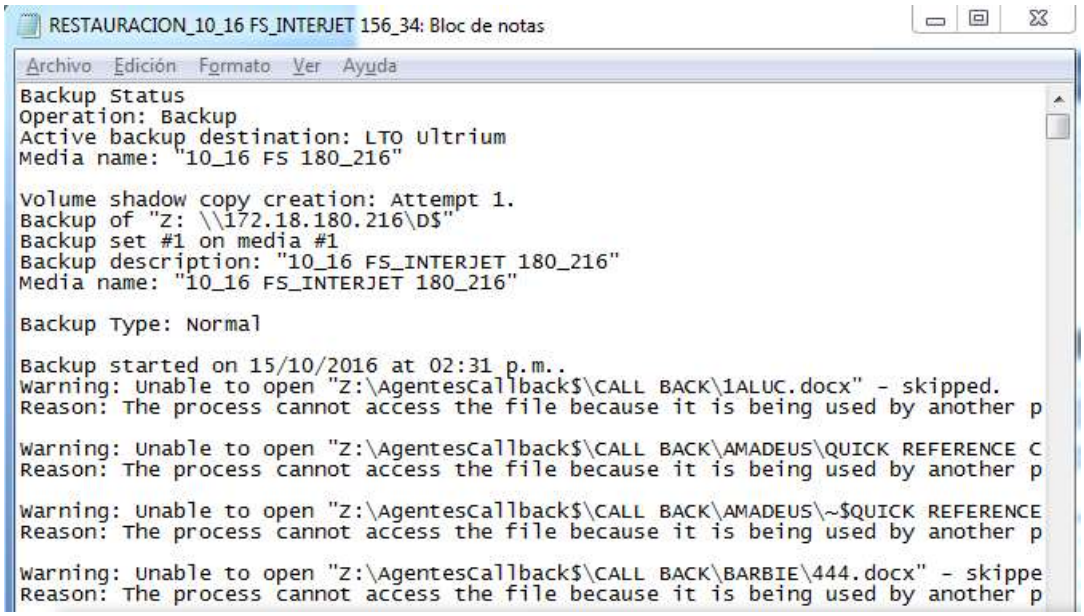


Figura 5.9. Log de finalización de respaldo en la herramienta Backup de Windows

- Restauración de un archivo de la cinta a través de la herramienta de respaldos, para garantizar la sanidad del respaldo, así como el llenado del formato de bitácoras de restauraciones, **ver Figura 5.10 y 5.11**.

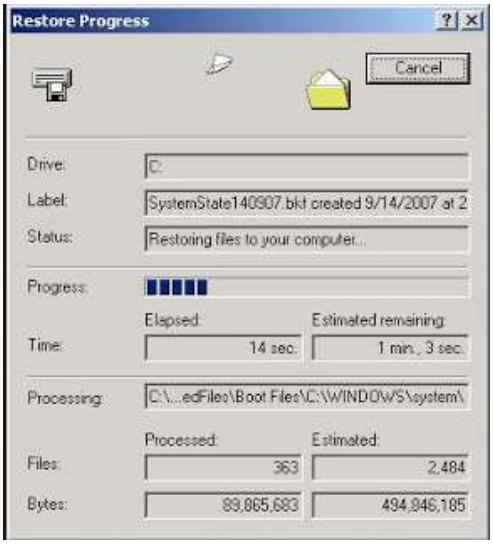


Figura 5.10. Restauración en la herramienta ntbackup

Bitácora de Restauración/ Recuperación de Archivos

Fecha de Restauración / Recuperación	Información a Restaurar / Recuperar		Número y tipo de Cinta		Observaciones	Responsable	Firma
	Archivo a Restaurar/Recuperar						
	Nombre del Archivo/Carpeta	Ruta	Tipo de	Identificador de Cinta			
12/09/2016	QR MARTITHA.pdf	\\172.34.156.134$\aerolinea$	Ultrium 4	09_16 180_225_E_H_SS	Correcto	Carlos Reyes	

Figura 5.11. Formato de bitácoras de restauraciones

- Almacenamiento de logs al completar el respaldos, **ver Figura 5.12**.

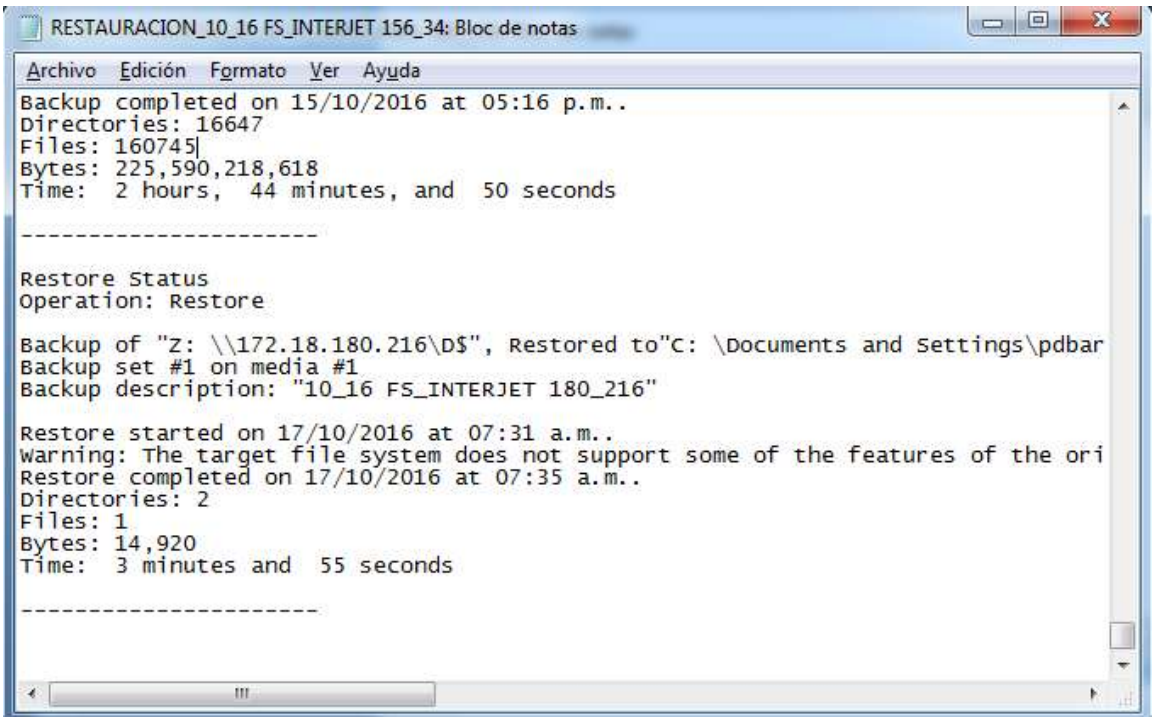


Figura 5.12. Almacenamiento de log de restauración

- El tiempo de resguardo de la información sensible debe estar en función a las necesidades del cliente, dicho acuerdo requiere estar asentado bajo contrato.
- Para la configuración de los equipos informáticos, dentro de Soluciones Multicanal se configura en todos los servidores con un Network Time Protocol (NTP), este es un protocolo de internet en la plataforma cliente-servidor, utilizado para sincronizar todos los dispositivos en una misma fecha y hora a través de una IP, esto se consigue haciendo referencia a una zona horaria pública.

5.1.7 Gestión de la seguridad en redes

Revisión y aseguramiento de no vulnerabilidades en la red de la siguiente forma:

- Las redes están adecuadamente controladas y gestionadas con las características de seguridad

- El personal autorizado por Soluciones Multicanal supervisa el equipo, sistemas y tráfico de la red en todo momento, así como monitorear el tráfico de los sistemas de forma periódica.
- La red corporativa esta segmentada en VLAN´s que permiten separar y delimitar el acceso lógico a los sistemas del área operativa y del área administrativa.
- La interconexión de redes de distintos centros y hacia el exterior cuentan con un firewall (en donde los medios lo permitan) de listas de acceso en cada extremo para tener un control del tráfico permitido entre los diferentes centros.
- Él envió electrónico de información clasificada como Reservada o Restringida (información sensible) se efectúa con el documento cifrado, y la contraseña de este solo se puede comunicar de manera personal o vía telefónica al destinatario.
- Los aplicativos están configurados con las mejores prácticas para la gestión de los correos, el personal de Seguridad Informática diariamente realiza revisiones a las herramientas.
- Las PC´s tanto del personal administrativo como de operaciones se configura de acuerdo a los niveles de accesos y software´s necesarios para que desempeñen sus labores.

5.1.8 Control de Acceso a los Site's y Sistemas de Seguridad

Tener establecido un sistema de control de acceso físico a los SITE´s, de modo que se impida el acceso al personal no autorizado.

- El personal que esté autorizado para entrar a los SITE´s tiene un código de acceso único e intransferible, así como una carta responsiva, autorizada por el área de seguridad informática.
- Toda persona que acceda a los SITE´s se registra anotando su nombre, hora de acceso, hora de salida, empresa de procedencia y actividades realizadas.
- Colocar un mensaje en la puerta de acceso a los SITE´s el cual indique claramente que se trata de una zona de acceso restringido al personal técnico.
- Los SITE´s cuentan con un sistema de video vigilancia para monitorear las actividades de los usuarios que ingresan al SITE.
- Los SITE´s poseen aires de precisión adecuados para conservar la temperatura y humedad necesarias para la correcta operación de la infraestructura tecnológica.
- Exigir a todo el personal ajeno a los SITE´s que porte alguna identificación visible.
- No se permite tomar fotografías, videos o audios de la Infraestructura que se tiene dentro de los SITE´s a menos de que esté autorizado por el área de Infraestructura.
- No se podrán introducir alimentos o bebidas a los SITE´s.
- No se permite fumar dentro de los SITE´s.
- El SITE es solo para equipos de cómputo, de ninguna manera se podrá utilizar para guardar cajas o material inflamable.
- Queda prohibido mover de su posición original, desconectar, cambiar, maltratar, ensuciar o modificar el equipo de cómputo o cualquier tipo de periférico que se encuentre dentro de los SITE´s.

5.2 Mejoras en la administración del Directorio Activo (Active Directory) y Servidor de Archivos (File Servers)

La administración y la reingeniería de los perfiles de usuario en el directorio activo permiten una mejor administración de los recursos, permisos y trazabilidad de un usuario en el manejo de la información del cliente y corporativa.

Normalmente los Directorios Activos dentro del ramo del Contact Center no cuentan con un proceso para su manejo, debido a los acelerados cambios dentro de ellos, al ser una rama de la ingeniería y recursos tecnológicos de gran demanda.

Se deben realizar estandarizaciones en los siguientes puntos:

- Organización y mejoras en la nomenclatura de las Unidades Organizacionales dentro del Directorio Activo

La nomenclatura se debe de realizar mediante la siguiente tabla de jerarquía, separando dentro de la jerarquía las líneas de negocio que se tienen en el corporativo, así como los usuarios permitidos para impresión segura mediante la integración de Servidor de impresión.

Este árbol de jerarquía será utilizado para las Directivas de Grupo (GPO), **ver Tabla 5.2**.

Tabla 5.2 Tabla de jerarquía de OU's en el Directorio Activo

Jerarquía	Unidad Organizacional (OU)
1	CC_Soluciones_Multicanal
2	CC_Soluciones_Multicanal_ Cobranza
3	Cobranza_Operador
4	Cobranza_Operador_A
4	Cobranza_Operador_B
4	Cobranza_Operador_C
3	Cobranza_Supervisor
4	Cobranza_Supervisor_A
4	Cobranza_Supervisor_B
4	Cobranza_Supervisor_C
3	Cobranza_MejoraContinua
4	Cobranza_Formacion

Unidades Organizacionales configuradas bajo la tabla de jerarquía, se muestran de la siguiente forma en el Directorio Activo, **ver Figura 5.13 y 5.14**.

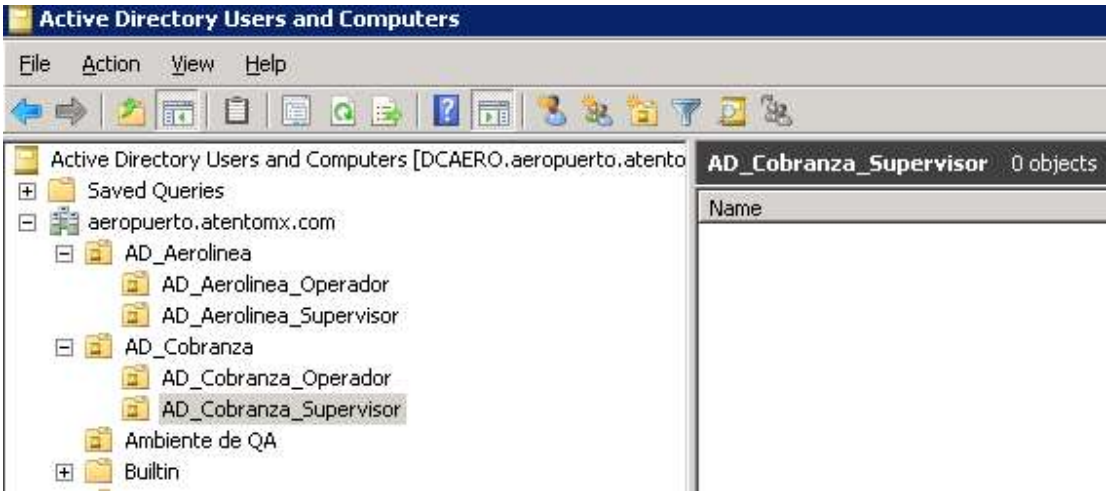


Figura 5.13. Unidades Organizacionales Creadas en el Directorio Activo

Figura 5.14. Directivas de Grupo configuradas en el Directorio Activo

Teniendo configuradas las unidades organizacionales, se deben de crear grupos de dominio, baja la misma nomenclatura de la jerarquía, anteponiendo "Gpo.". Ejemplo: "Gpo.Cobranza_operdor_A"

- Modificación en las políticas de seguridad

Se deben de configurar las Directivas de Grupo de acuerdo a lo establecido en la política de seguridad presentada en el **apartado 5.1.3**. Así como lo solicitado contractualmente para cada una de las líneas de negocio.

Las directivas consisten en lo siguiente: se aplican voluntariamente por las aplicaciones específicas. En muchos casos, esto sólo consiste en deshabilitar la interfaz de usuario para una función determinada, sin desactivar el nivel más bajo de los medios para acceder a él, **ver Figura 5.15 y 5.16**.

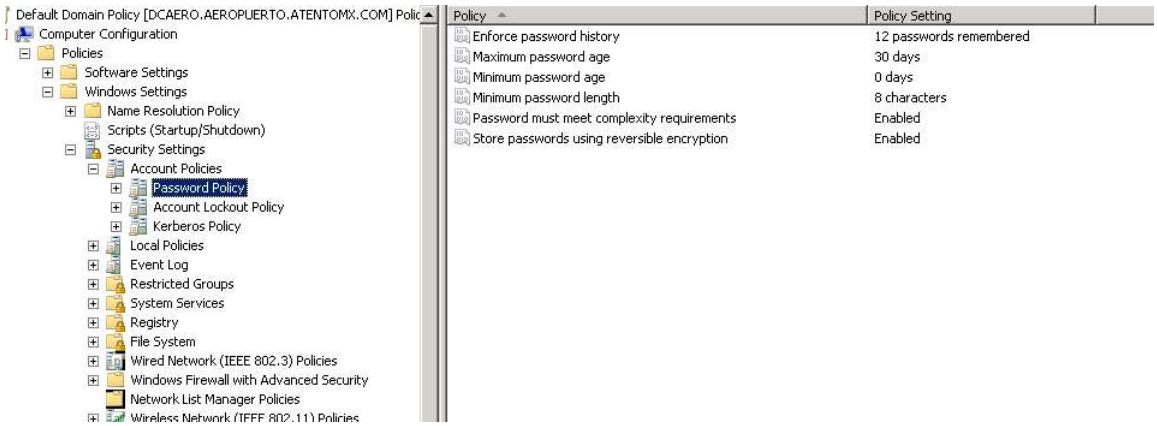


Figura 5.15. Configuración de políticas de seguridad del punto 5.1.3

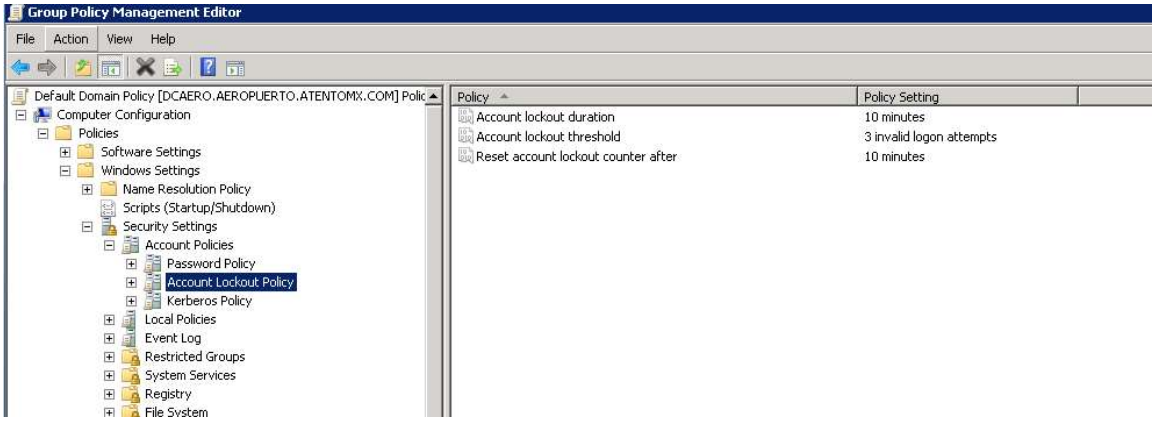


Figura 5.16. Configuración de las políticas para cada usuario

- Creación de menús de inicio independientes con nomenclatura de acuerdo a las Unidades Organizacionales (OU) y los Objetos de Directivos de Grupo (GPO), **ver Figura 5.17**.

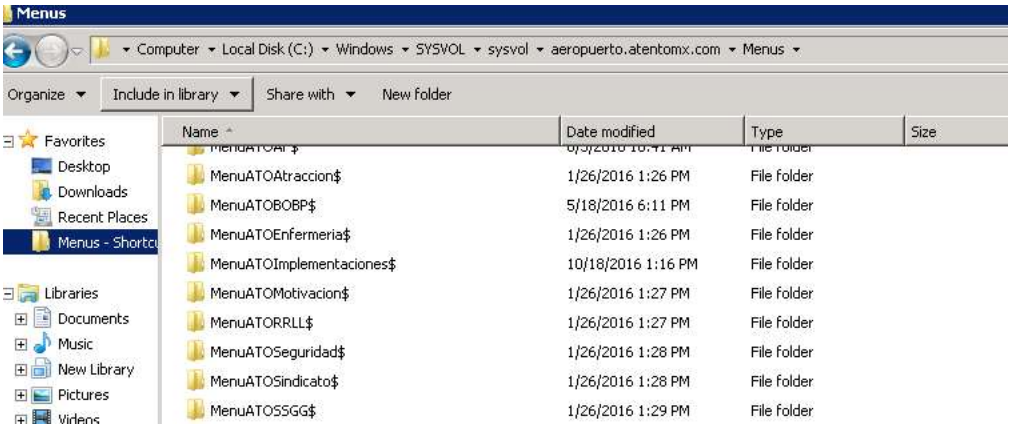


Figura 5.17. Imagen de la configuración del menú de inicio

- Creación de usuarios en identificador único, este debe de ir asociado a su número de empleado dentro de la empresa-
  Tener un usuario identificado y que sea homologado a todos los sistemas que tiene acceso, permite la trazabilidad de todo su trabajo. En caso de cometar algún fraude o alguna actividad que impacte a la empresa se facilita su localización y trazabilidad, **ver Figura 5.18**.

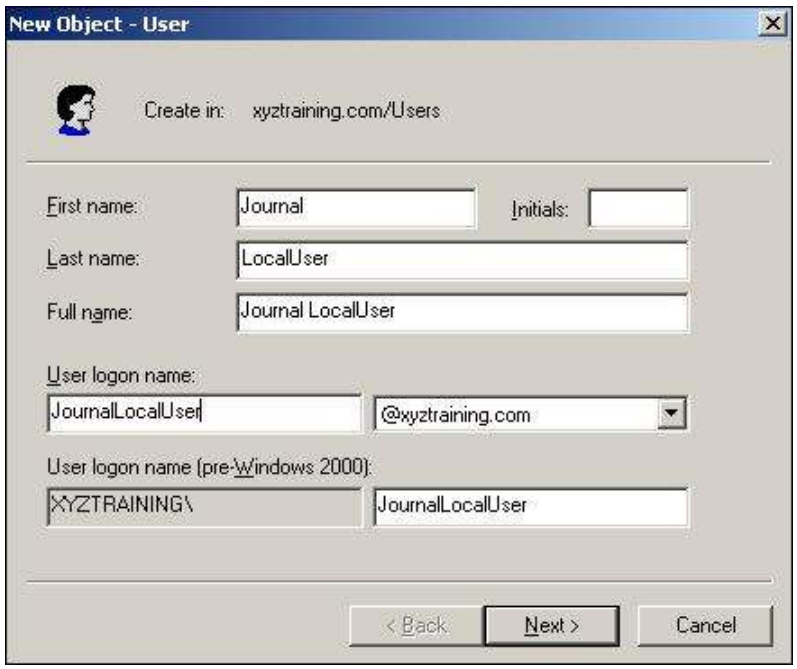


Figura 5.18. Creación de usuario con número de empleado

- Creación de sesión única, para que ningún usuario pueda realizar préstamo de sus credenciales de sesión de Windows.

Se realiza la integración de bats de interacción con el servidor de dominio, el cual son agregados a la función "logon" para que cada vez que se inicie sesión, permita crear una bandera de conexión en el servidor y no permite autenticarse dos veces en diferentes estaciones de trabajo.

Al archivo "logoff" cuando el usuario en su sesión realice la acción, "cerrar sesión", "reiniciar" y "apagar", permitirá eliminar la bandera de conexión y así se pueda autenticar en otra estación de trabajo, **ver Figura 5.19, 5.20 y 5.21.**

```
' Logon7.vbs
' VBScript Logon script para forza le sesión única por usuario.
'
' ----------------------------------------------------------------------
' Copyright (c) 2010 Richard L. Mueller
' Hilltop Lab web site - http://www.rlmueller.net
' Version 1.0 - May 29, 2010
' Version 1.1 - June 3, 2010
'         Usted tiene los derechos de uso o modificación, reproducción
' y distribución de este script ,

Option Explicit

Dim objFSO, objNewFile, objNetwork
Dim intCount, objShell, intTimeout
Dim strComputerEncoded, strShare, strFlagFile, strComputer
Dim objOldFile, strLine, strValue, objChars, strErrorLog
Dim objWMIService, colOperatingSystems, objOperatingSystem
Dim strTitle, strText, intConstants, intAns
Dim strHexValue, strUserEncoded, objSysinfo, strUserDN, objUser
Dim strShare2, objErrorLog

Const B64 = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"
Const ForReading = 1
Const ForWriting = 2
Const ForAppending = 8
Const OpenAsASCII = 0
Const CreateIfNotExist = True
Const LOGOFF = 0

' Specify shared folder.
strShare = "\\172.18.180.200\LimitLogin$\Logs"

' Specify alternate shared folder to log errors if the first is unavailable.
strShare2 = "\\\MyServer2\MyShare\Logs"
intTimeout = 4

Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objNetwork = CreateObject("Wscript.Network")
Set objShell = CreateObject("Wscript.Shell")

' Retrieve user and computer information.
Set objSysInfo = CreateObject("ADSystemInfo")
strUserDN = objSysInfo.UserName
Set objUser = GetObject("LDAP://" & strUserDN)
strComputer = objNetwork.ComputerName
```

```
' Base64 encode computer name and user GUID.
strHexValue = TextToHex(strComputer)
strComputerEncoded = HexToBase64(strHexValue)

strHexValue = TextToHex(objUser.GUID)
strUserEncoded = HexToBase64(strHexValue)
' Remove trailing "=".
strUserEncoded = Replace(strUserEncoded, "=", "")

' Create flag file based on encoded user GUID.
strFlagFile = strShare & "\" & strUserEncoded & ".log"

' Check if flag file exists for this user.
If (objFSO.FileExists(strFlagFile) = True) Then
' Read encoded computer name from the flag file.
Set objOldFile = objFSO.OpenTextFile(strFlagFile, ForReading)
strLine = objOldFile.ReadLine
objOldFile.Close
' Check encoded computer name.
If (strLine <> strComputerEncoded) Then
' Does not match encode local computer name. Decode computer name.
' Setup dictionary object.
Set objChars = CreateObject("Scripting.Dictionary")
objChars.CompareMode = vbBinaryCompare
' Load dictionary object.
Call LoadChars
' Alert user.
strValue = Base64ToHex(strLine)
strValue = HexToText(strValue)
strTitle = "Too many logon Sessions"
strText = "You must logoff (or restart) computer: " & strValue
intConstants = vbOKOnly + vbCritical
intAns = objShell.Popup(strText, intTimeout, strTitle, _
intConstants)

' Logoff.
Set objWMIService = GetObject("winmgmts:" _
& "{impersonationLevel=impersonate,authenticationLevel=Pkt,(Shutdown)}!\\" _
& strComputer & "\root\cimv2")

Set colOperatingSystems = objWMIService.ExecQuery _
("Select * from Win32_OperatingSystem")

For Each objOperatingSystem in colOperatingSystems
objOperatingSystem.Win32Shutdown(LOGOFF)
Next
Wscript.Quit
End If
End If

' Write computer name to flag file.
On Error Resume Next
Set objNewFile = objFSO.OpenTextFile(strFlagFile, _
```

```
ForWriting, CreateIfNotExist, OpenAsASCII)
If (Err.Number = 0) Then
On Error GoTo 0
' Write to flag file.
objNewFile.WriteLine strComputerEncoded
objNewFile.Close
Else
On Error GoTo 0
' Unable to open text file. Log error to alternate location.
strErrorLog = strShare2 & "\Error.log"
On Error Resume Next
Set objErrorLog = objFSO.OpenTextFile(strErrorLog, _
ForAppending, CreateIfNotExist, OpenAsASCII)
If (Err.Number = 0) Then
On Error GoTo 0
' Make three attempts to write, in case many users are affected.
intCount = 1
Do Until intCount = 3
On Error Resume Next
objErrorLog.WriteLine "## Logon Error" _
& vbCrLf & "Time: " & CStr(Now()) _
& vbCrLf & "Share unavailable: " & strShare _
& vbCrLf & "User: " & strUserDN _
& vbCrLf & "Computer: " & strComputer _
& vbCrLf & "Flag file not created"
If (Err.Number = 0) Then
On Error GoTo 0
Exit Do
Else
Err.Clear
intCount = intCount + 1
Wscript.Sleep 200
End If
On Error GoTo 0
Loop
objErrorLog.Close
End If
End If
On Error GoTo 0

Function TextToHex(ByVal strText)
' Function to convert a text string into a string of hexadecimal bytes.
Dim strChar, k

TextToHex = ""
For k = 1 To Len(strText)
strChar = Mid(strText, k, 1)
TextToHex = TextToHex & Hex(Asc(strChar))
Next
End Function

Function HexToBase64(ByVal strHex)
' Function to convert a hex string into a base64 encoded string.
' Constant B64 has global scope.
```

```
Dim lngValue, lngTemp, lngChar, intLen, k, j, strWord, str64, intTerm

intLen = Len(strHex)

' Pad with zeros to multiple of 3 bytes.
intTerm = intLen Mod 6
If (intTerm = 4) Then
strHex = strHex & "00"
intLen = intLen + 2
End If
If (intTerm = 2) Then
strHex = strHex & "0000"
intLen = intLen + 4
End If

' Parse into groups of 3 hex bytes.
j = 0
strWord = ""
HexToBase64 = ""
For k = 1 To intLen Step 2
j = j + 1
strWord = strWord & Mid(strHex, k, 2)
If (j = 3) Then
' Convert 3 8-bit bytes into 4 6-bit characters.
lngValue = CCur("&H" & strWord)

lngTemp = Fix(lngValue / 64)
lngChar = lngValue - (64 * lngTemp)
str64 = Mid(B64, lngChar + 1, 1)
lngValue = lngTemp

lngTemp = Fix(lngValue / 64)
lngChar = lngValue - (64 * lngTemp)
str64 = Mid(B64, lngChar + 1, 1) & str64
lngValue = lngTemp

lngTemp = Fix(lngValue / 64)
lngChar = lngValue - (64 * lngTemp)
str64 = Mid(B64, lngChar + 1, 1) & str64

str64 = Mid(B64, lngTemp + 1, 1) & str64

HexToBase64 = HexToBase64 & str64
j = 0
strWord = ""
End If
Next
' Account for padding.
If (intTerm = 4) Then
HexToBase64 = Left(HexToBase64, Len(HexToBase64) - 1) & "="
End If
If (intTerm = 2) Then
HexToBase64 = Left(HexToBase64, Len(HexToBase64) - 2) & "=="
End If
```

```
End Function

Function HexToText(ByVal strHex)
' Function to convert a string of hexadecimal bytes into a text string.
Dim strChar, k

HexToText = ""
For k = 1 To Len(strHex) Step 2
strChar = Mid(strHex, k, 2)
HexToText = HexToText & Chr("&H" & strChar)
Next
End Function

Function Base64ToHex(ByVal strValue)
' Function to convert a base64 encoded string into a hex string.
Dim lngValue, lngTemp, lngChar, intLen, k, j, intTerm, strHex

intLen = Len(strValue)

' Check padding.
intTerm = 0
If (Right(strValue, 1) = "=") Then
intTerm = 1
End If
If (Right(strValue, 2) = "==") Then
intTerm = 2
End If

' Parse into groups of 4 6-bit characters.
j = 0
lngValue = 0
Base64ToHex = ""
For k = 1 To intLen
j = j + 1
' Calculate 24-bit integer.
lngValue = (lngValue * 64) + objChars(Mid(strValue, k, 1))
If (j = 4) Then
' Convert 24-bit integer into 3 8-bit bytes.
lngTemp = Fix(lngValue / 256)
lngChar = lngValue - (256 * lngTemp)
strHex = Right("00" & Hex(lngChar), 2)
lngValue = lngTemp

lngTemp = Fix(lngValue / 256)
lngChar = lngValue - (256 * lngTemp)
strHex = Right("00" & Hex(lngChar), 2) & strHex
lngValue = lngTemp

lngTemp = Fix(lngValue / 256)
lngChar = lngValue - (256 * lngTemp)
strHex = Right("00" & Hex(lngChar), 2) & strHex

Base64ToHex = Base64ToHex & strHex
```

```
j = 0
lngValue = 0
End If
Next
' Account for padding.
Base64ToHex = Left(Base64ToHex, Len(Base64ToHex) - (intTerm * 2))

End Function

Sub LoadChars
' Subroutine to load dictionary object with information to convert
' Base64 characters into base 64 index integers.
' Object reference objChars has global scope.

objChars.Add "A", 0
objChars.Add "B", 1
objChars.Add "C", 2
objChars.Add "D", 3
objChars.Add "E", 4
objChars.Add "F", 5
objChars.Add "G", 6
objChars.Add "H", 7
objChars.Add "I", 8
objChars.Add "J", 9
objChars.Add "K", 10
objChars.Add "L", 11
objChars.Add "M", 12
objChars.Add "N", 13
objChars.Add "O", 14
objChars.Add "P", 15
objChars.Add "Q", 16
objChars.Add "R", 17
objChars.Add "S", 18
objChars.Add "T", 19
objChars.Add "U", 20
objChars.Add "V", 21
objChars.Add "W", 22
objChars.Add "X", 23
objChars.Add "Y", 24
objChars.Add "Z", 25
objChars.Add "a", 26
objChars.Add "b", 27
objChars.Add "c", 28
objChars.Add "d", 29
objChars.Add "e", 30
objChars.Add "f", 31
objChars.Add "g", 32
objChars.Add "h", 33
objChars.Add "i", 34
objChars.Add "j", 35
objChars.Add "k", 36
objChars.Add "l", 37
objChars.Add "m", 38
objChars.Add "n", 39
```

```
objChars.Add "o", 40
objChars.Add "p", 41
objChars.Add "q", 42
objChars.Add "r", 43
objChars.Add "s", 44
objChars.Add "t", 45
objChars.Add "u", 46
objChars.Add "v", 47
objChars.Add "w", 48
objChars.Add "x", 49
objChars.Add "y", 50
objChars.Add "z", 51
objChars.Add "0", 52
objChars.Add "1", 53
objChars.Add "2", 54
objChars.Add "3", 55
objChars.Add "4", 56
objChars.Add "5", 57
objChars.Add "6", 58
objChars.Add "7", 59
objChars.Add "8", 60
objChars.Add "9", 61
objChars.Add "+", 62
objChars.Add "/", 63

End Sub
```

Figura 5.19. Logon de Sesión de única

```
' Logoff7.vbs
' VBScript Logon script para forza le sesión única por usuario.
'
' ----------------------------------------------------------------------
' Copyright (c) 2010 Richard L. Mueller
' Hilltop Lab web site - http://www.rlmueller.net
' Version 1.0 - May 29, 2010
' Version 1.1 - June 3, 2010
'         Usted tiene los derechos de uso o modificación, reproducción
' y distribución de este script ,

Option Explicit

Dim objFSO, objNetwork, strComputer, strComputerEncoded
Dim strShare, strFlagFile, objFile, strLine, objFolder
Dim strHexValue, strUserEncoded, objSysinfo, strUserDN, objUser
Dim strShare2, objErrorLog, strErrorLog, intCount

Const B64 = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"
Const ForReading = 1
Const ForAppending = 8
Const OpenAsASCII = 0
Const CreateIfNotExist = True

' Specify shared folder.
strShare = "\\172.18.180.200\LimitLogin$\Logs"
```

```
' Specify alternate folder if the first is unavailable.
strShare2 = "\\MyServer2\MyShare\Logs"

Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objNetwork = CreateObject("Wscript.Network")

' Retrieve user and computer information.
Set objSysInfo = CreateObject("ADSystemInfo")
strUserDN = objSysInfo.UserName
Set objUser = GetObject("LDAP://" & strUserDN)
strComputer = objNetwork.ComputerName

' Base64 encode computer name and user GUID.
strHexValue = TextToHex(strComputer)
strComputerEncoded = HexToBase64(strHexValue)

strHexValue = TextToHex(objUser.GUID)
strUserEncoded = HexToBase64(strHexValue)
strUserEncoded = Replace(strUserEncoded, "=", "")

' Create flag file based on encoded user GUID.
strFlagFile = strShare & "\" & strUserEncoded & ".log"

' Check if flag file exists for this user.
If (objFSO.FileExists(strFlagFile) = True) Then
   ' Read encoded computer name from the flag file.
   Set objFile = objFSO.OpenTextFile(strFlagFile, ForReading)
   strLine = objFile.ReadLine
   objFile.Close
   ' Check encoded computer name.
   If (strLine = strComputerEncoded) Then
      ' Delete the file.
      objFSO.DeleteFile strFlagFile
   End If
   Wscript.Quit
End If

' No flag file found for this user. Make sure share is available.
On Error Resume Next
Set objFolder = objFSO.GetFolder(strShare)
If (Err.Number <> 0) Then
   On Error GoTo 0
   ' Log error to alternate location.
   strErrorLog = strShare2 & "\Error.log"
   On Error Resume Next
   Set objErrorLog = objFSO.OpenTextFile(strErrorLog, _
      ForAppending, CreateIfNotExist, OpenAsASCII)
   If (Err.Number = 0) Then
      On Error GoTo 0
      ' Make trhee attempts to write, in case many users are affected.
      intCount = 1
      Do Until intCount = 3
         On Error Resume Next
         objErrorLog.WriteLine "## Logoff Error" _
            & vbCrLf & "Time: " & CStr(Now()) _
            & vbCrLf & "Share unavailable: " & strShare _
            & vbCrLf & "User: " & strUserDN _
            & vbCrLf & "Computer: " & strComputer _
```

```
            & vbCrLf & "Flag file: " & strFlagFile
        If (Err.Number = 0) Then
          On Error GoTo 0
          Exit Do
        Else
          Err.Clear
          intCount = intCount + 1
          Wscript.Sleep 200
        End If
        On Error Goto 0
      Loop
      objErrorLog.Close
    End If
End If
On Error GoTo 0

Function TextToHex(ByVal strText)
    ' Function to convert a text string into a string of hexadecimal bytes.
    Dim strChar, k

    TextToHex = ""
    For k = 1 To Len(strText)
      strChar = Mid(strText, k, 1)
      TextToHex = TextToHex & Hex(Asc(strChar))
    Next
End Function

Function HexToBase64(ByVal strHex)
    ' Function to convert a hex string into a base64 encoded string.
    ' Constant B64 has global scope.
    Dim lngValue, lngTemp, lngChar, intLen, k, j, strWord, str64, intTerm

    intLen = Len(strHex)

    ' Pad with zeros to multiple of 3 bytes.
    intTerm = intLen Mod 6
    If (intTerm = 4) Then
      strHex = strHex & "00"
      intLen = intLen + 2
    End If
    If (intTerm = 2) Then
      strHex = strHex & "0000"
      intLen = intLen + 4
    End If

    ' Parse into groups of 3 hex bytes.
    j = 0
    strWord = ""
    HexToBase64 = ""
    For k = 1 To intLen Step 2
      j = j + 1
      strWord = strWord & Mid(strHex, k, 2)
      If (j = 3) Then
        ' Convert 3 8-bit bytes into 4 6-bit characters.
        lngValue = CCur("&H" & strWord)

        lngTemp = Fix(lngValue / 64)
        lngChar = lngValue - (64 * lngTemp)
        str64 = Mid(B64, lngChar + 1, 1)
```

```
        lngValue = lngTemp

        lngTemp = Fix(lngValue / 64)
        lngChar = lngValue - (64 * lngTemp)
        str64 = Mid(B64, lngChar + 1, 1) & str64
        lngValue = lngTemp

        lngTemp = Fix(lngValue / 64)
        lngChar = lngValue - (64 * lngTemp)
        str64 = Mid(B64, lngChar + 1, 1) & str64

        str64 = Mid(B64, lngTemp + 1, 1) & str64

        HexToBase64 = HexToBase64 & str64
        j = 0
        strWord = ""
    End If
Next
' Account for padding.
If (intTerm = 4) Then
    HexToBase64 = Left(HexToBase64, Len(HexToBase64) - 1) & "="
End If
If (intTerm = 2) Then
    HexToBase64 = Left(HexToBase64, Len(HexToBase64) - 2) & "=="
End If

End Function
```

Figura 5.20 Logoff de Sesión única

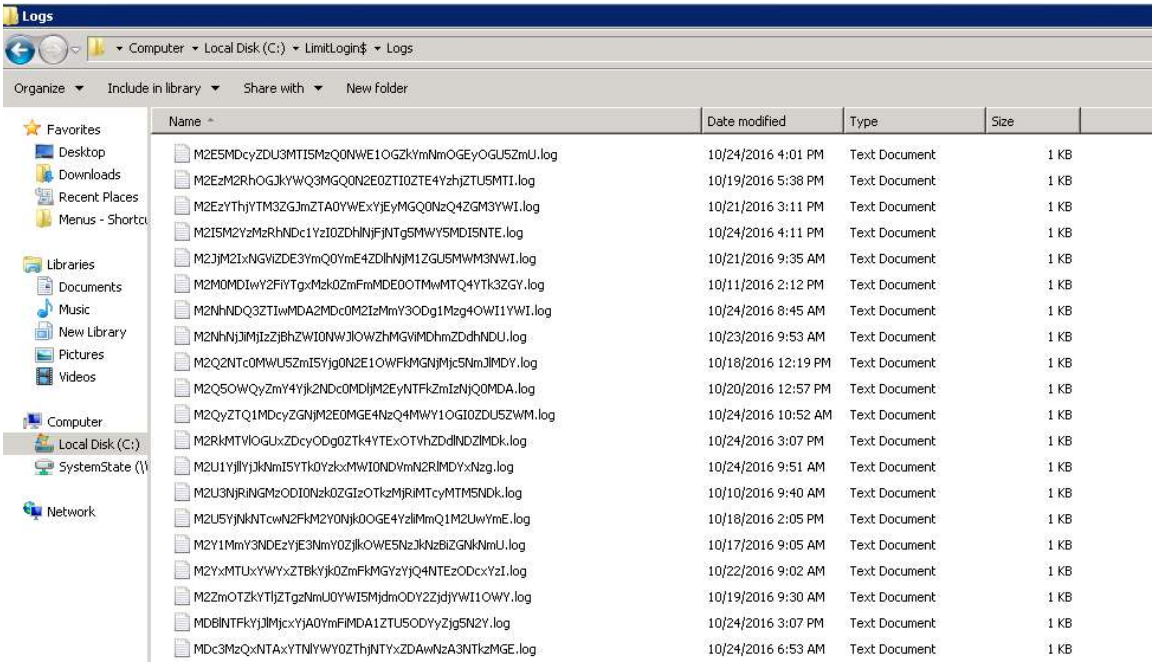


Figura 5.21. Banderas creadas por la función sesión única

- Permisos en servidores de archivos de acuerdo al perfil del empleado

Se realiza la creación de las carpetas de red bajo la misma estructura de jerarquía y otorgando permisos a los grupos de dominio identificados, por campaña o subcampaña. Esta estructura primero debe de ser validada por el área de negocio, y posteriormente se ejecuta por el área de tecnología, **ver Figura 5.22 y 5.23**.

Campaña	Subcarpeta
Cobranza	Operador_Análisis
	Operador_Mesas
	Operador_Recepción
	Operador_Sanción
	Operador_NF
	Operador Multiskill Hipotecario
	Supervisor
	Coordinador
Aerolinea	Operador_Análisis y Domi
	Operador_Bastanteos y Verificaciones
	Operador _Reversaciones
	Supervisor
	Coordinador

Figura 5.22. Estructura de las carpetas de red, revisada con operaciones

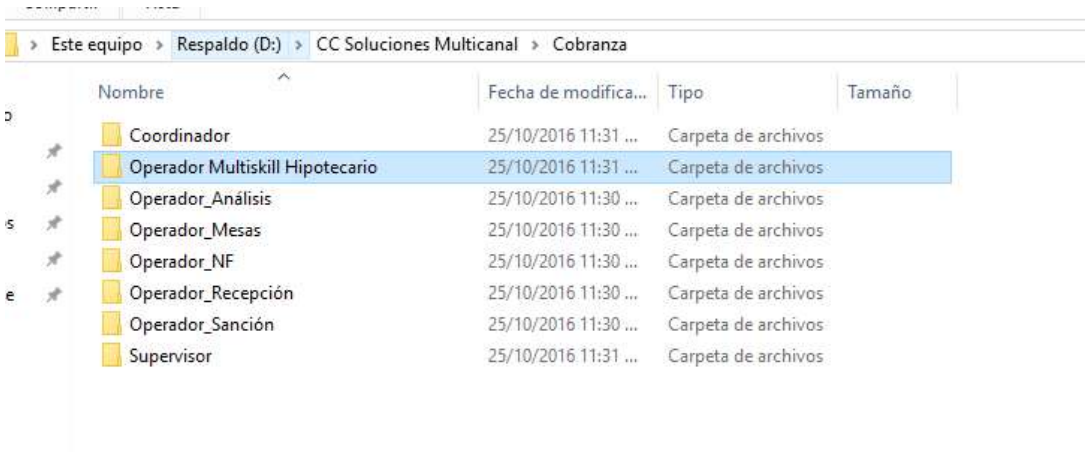


Figura 5.23. Carpetas de red dentro del Servidor de Archivos (File Server)

- Integración y acceso controlado a impresoras con Servidor de impresión

Dentro de la organización del Directorio Activo, se definieron por separado los usuarios permitidos con permisos de impresión, el Servidor de Impresión permite tener la integración de las impresoras conectadas en red y darle el acceso a las colas de impresión mediante el Directorio Activo y las Directivas de Grupo, a los usuarios permitidos, **ver Figura 5.24 y 5.25**.

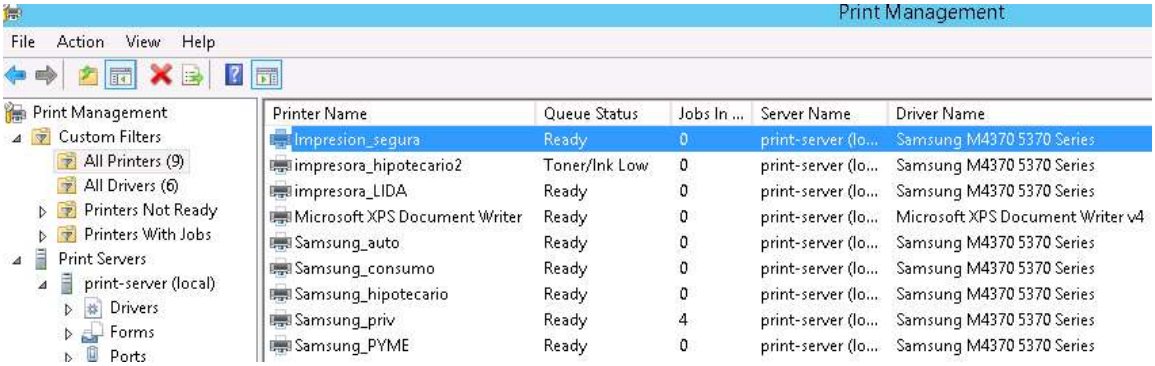


Figura 5.24. Impresoras Compartidas

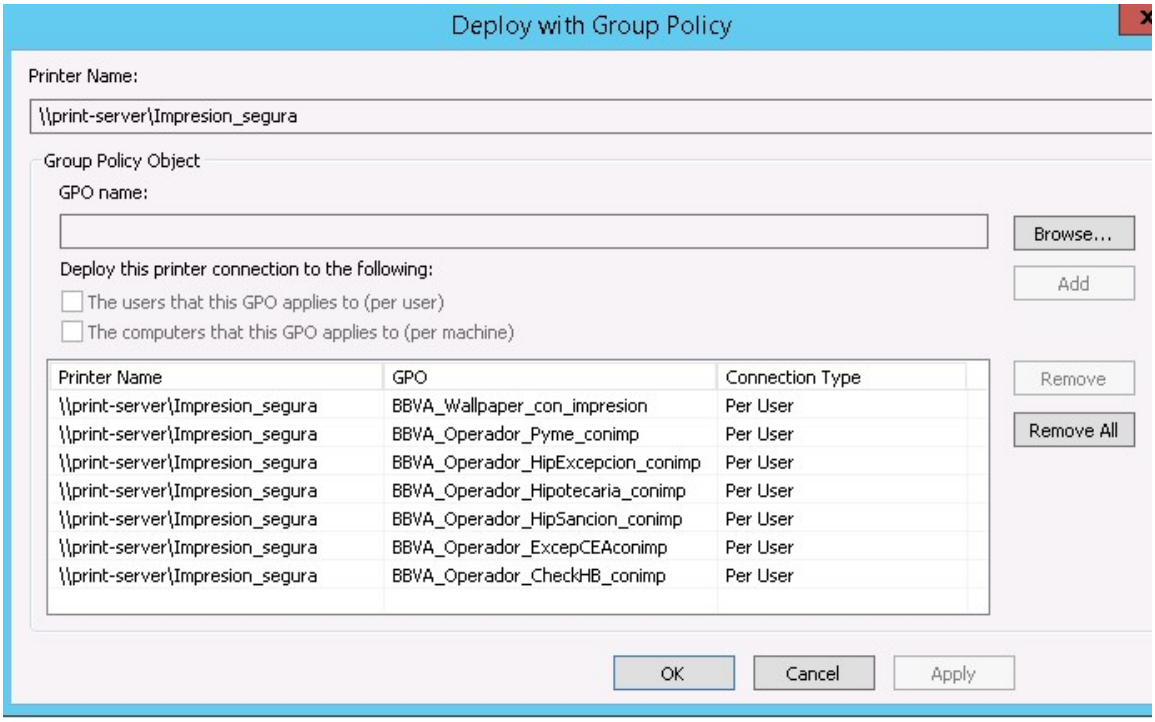


Figura 5.25. Configuración de las impresoras mediante el rol de impresión

5.3 Implementación de políticas de seguridad en Firewall

Las configuraciones importantes a realizar dentro de la red para el control de la salida de internet de los empleados del corporativo son las siguientes:

- Eliminar el acceso a páginas de correo electrónico, juegos, pornografía, videos y música por internet, comunicación por internet (Whatsapp, telegram, Skype), almacenamiento en la nube y redes sociales.
- Permitir el acceso exclusivamente a las ligas permitidas y mencionadas contractualmente.
- Si algún servicio de las líneas de negocio requiere acceso a correos electrónicos o redes sociales, el cliente de la línea de negocio debe de hacer responsable del uso de internet y las implicaciones que pueda llevar el acceso en caso de algún fraude.

El Cortafuegos "Palo Alto" dentro de sus principales funciones permite el control de las salidas de internet por categorías, permitiendo facilitar la actividad y control de la salida de internet de la red interna al exterior.

1. Inicialmente se debe de crear las categorías o filtrados personalizados dentro del URL Category, hacia las ligas de acceso permitidas contractualmente, **ver Figura 5.26.**

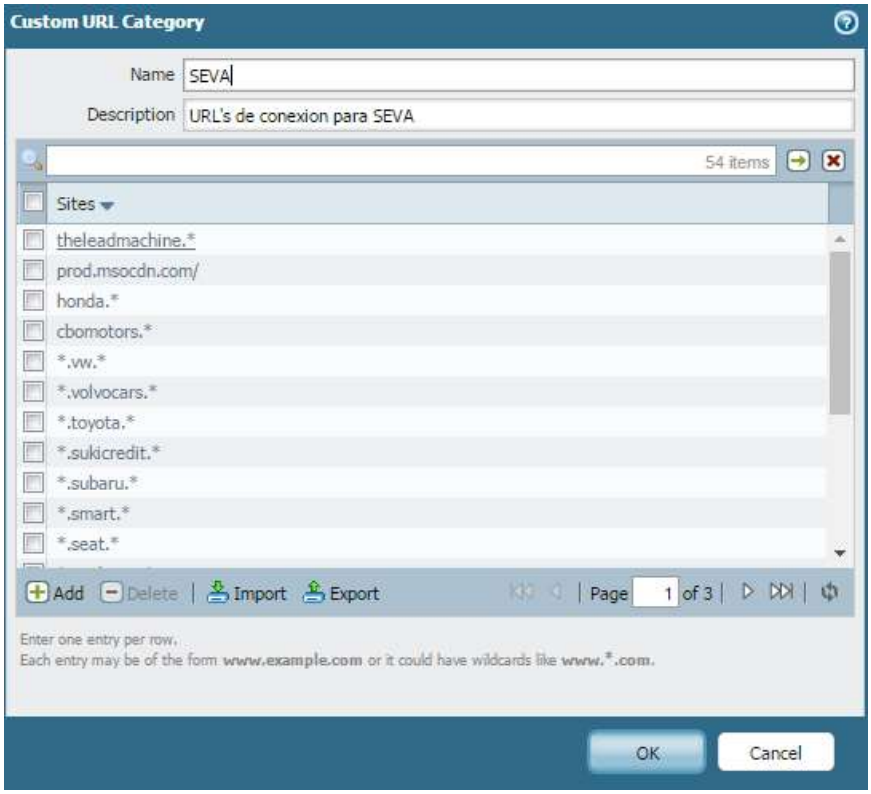


Figura 5.26. Configuración de filtrado personalizado "URL Category"

2. Creación de los URL Filtering permitiendo acceso a categorías especificas o bloqueo total de internet dando solo salida a las categorías personalizada, **ver Figura 5.27**.

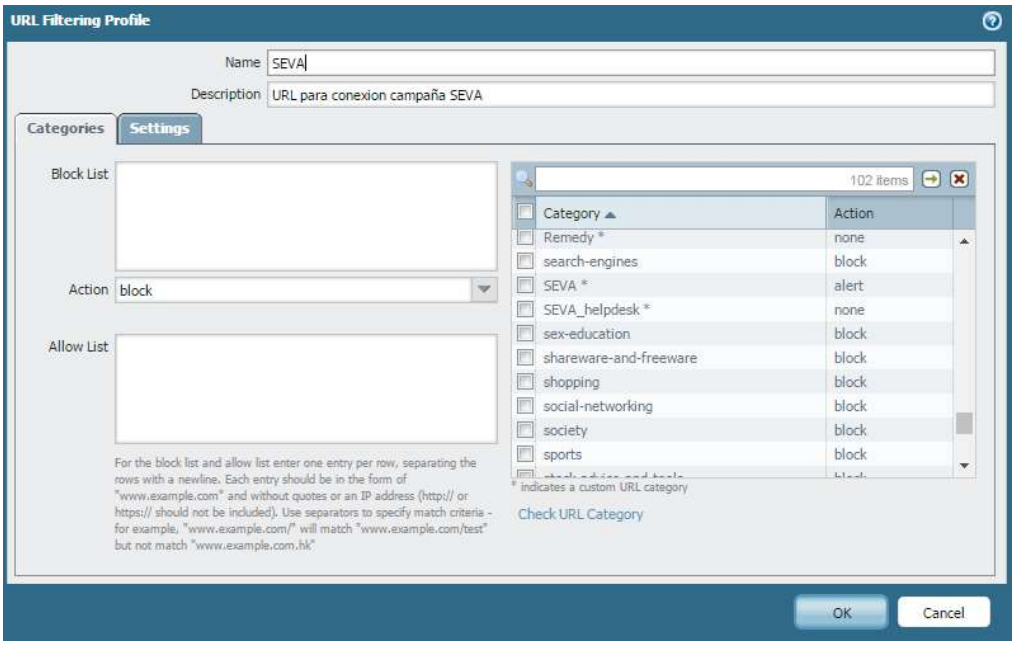


Figura 5.27. Creación de "URL Filtering"

3. Creación de las políticas de bloqueo, de arriba hacia abajo toma las politícas, por lo cual la política que creemos debe de ir sobre una de bloqueo total, **ver Figura 5.28**.

Figura 5.28. Políticas de bloqueo

4. Monitoreo del tráfico que está pasando por lo equipos, **ver Figura 5.29 y 5.30**.

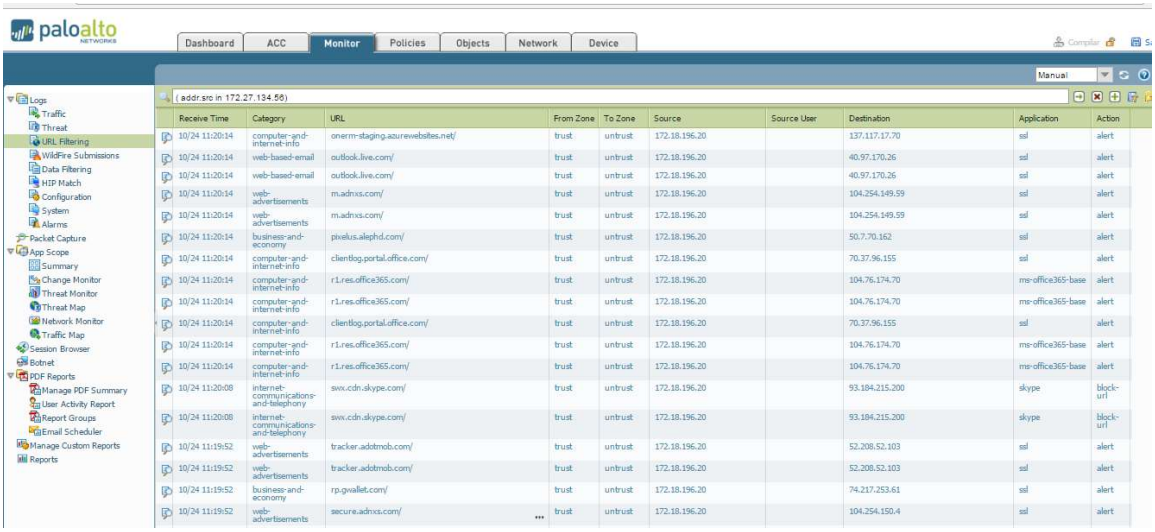


Figura 5.29. Monitoreo de funcionamiento de la política

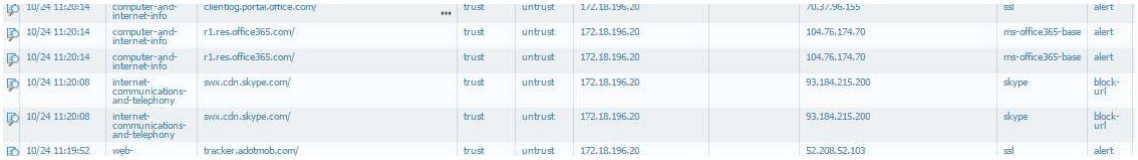


Figura 5.30. Evidencia de política activa

5.4 Configuración del Antivirus

Soluciones Multicanal cuenta con una solución corporativa, la cual previene esta vulnerabilidad, es importante después de que la herramienta fue entregada por el proveedor, seguir las siguientes consideraciones para disminuir los riesgos:

- Revisar la consola de antivirus mensualmente y cuente con la última versión así como este realizando la descarga de la base de datos continuamente, actualmente se está utilizando la soluciones Trend Micro Office Scan, **ver Figura 5.31**.

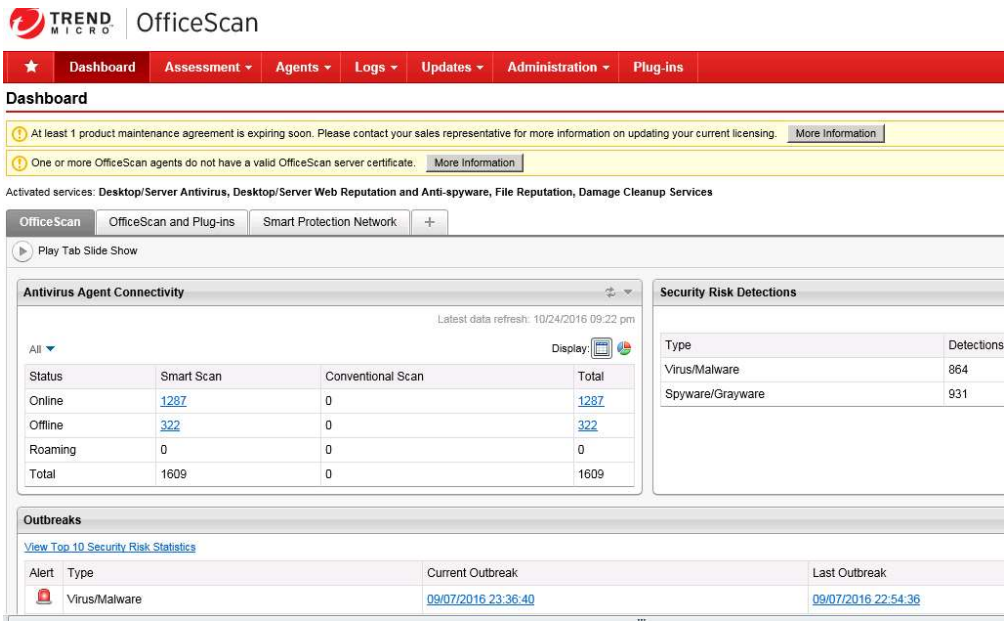


Figura 5.31. Consola de Antivirus

- Activar las políticas de seguridad para prevención de Ramsomware (virus encriptador), **ver Figura 5.32.**

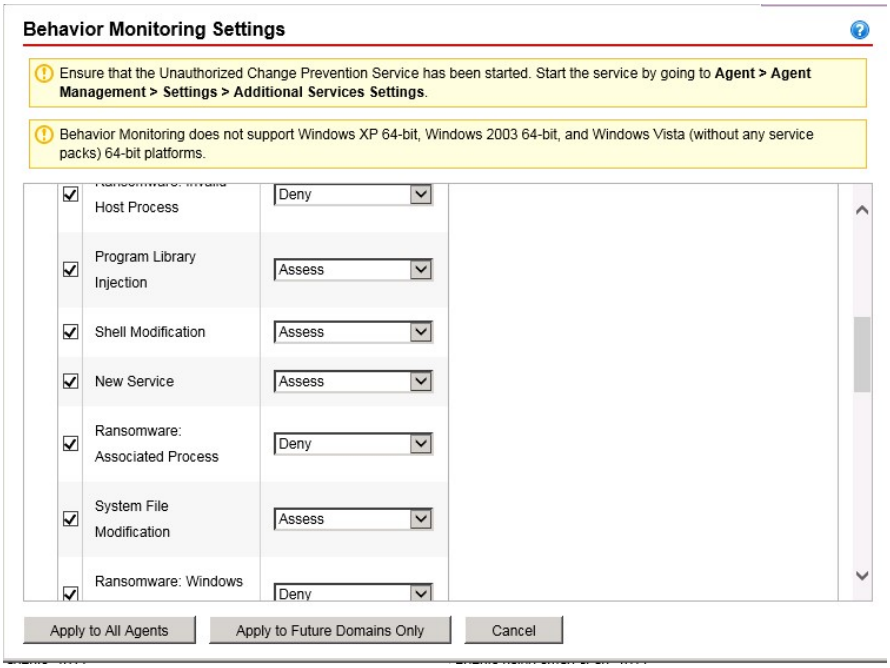


Figura 5.32. Configuración y prevención del Ramsomware

- Activar las políticas de bloqueo de dispositivos de almacenamiento masivo. Con la finalidad de evitar fugas de información por medio USB, CDs, **ver Figura 5.33**.

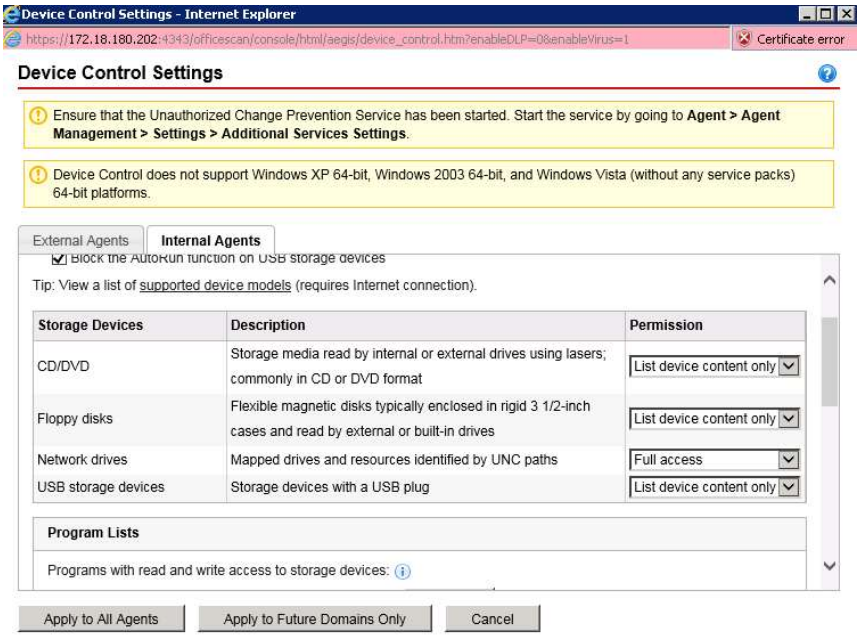


Figura 5.33. Bloqueo de almacenamiento masivo.

- Configuración de DLP en estaciones de trabajo que manejen correo y reciban bases para su tratamiento o información sensible y critica, **ver Figura 5.34.**

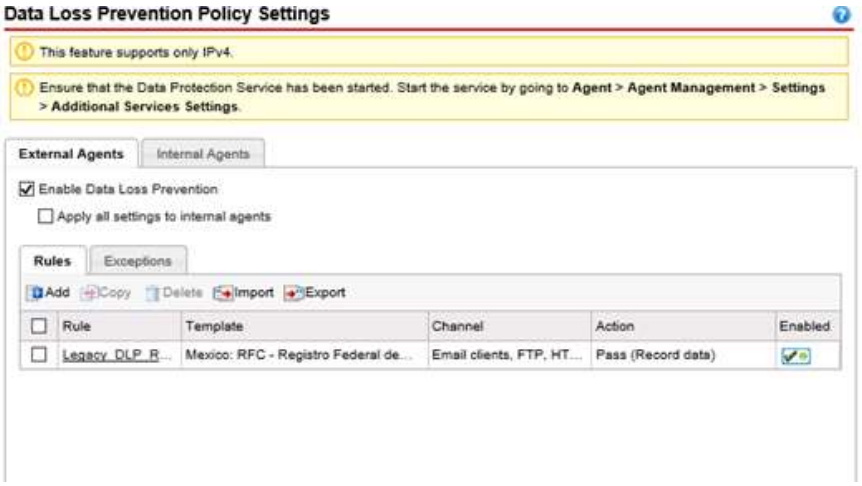


Figura 5.34. Imagen de políticas DLP

CAPÍTULO 6 Creación de un plan de continuidad de infraestructura tecnológica para el negocio

Realizar un plan logístico para ofrecer al cliente la capacidad estratégica y táctica de planificar la recuperación gradual de sus actividades críticas derivado de alguna contingencia imprevista de un ámbito social, tecnológico, entre otras, que impida la correcta operación, **ver Figura 6.1.**

La **Figura 6.1** tiene una conexión con la **Figura 4.1** del apartado 4, donde la solicitud del clientes es tener un plan de continuidad de negocio en la sede alterna, y poder operar sus servicios en la sede alterna en caso de contigencia en numero proporcinalmente menor, el diagrama especifica las actividades de todas las áreas involucradas, a su vez puntualizando las actividades de TI a ejecutar.

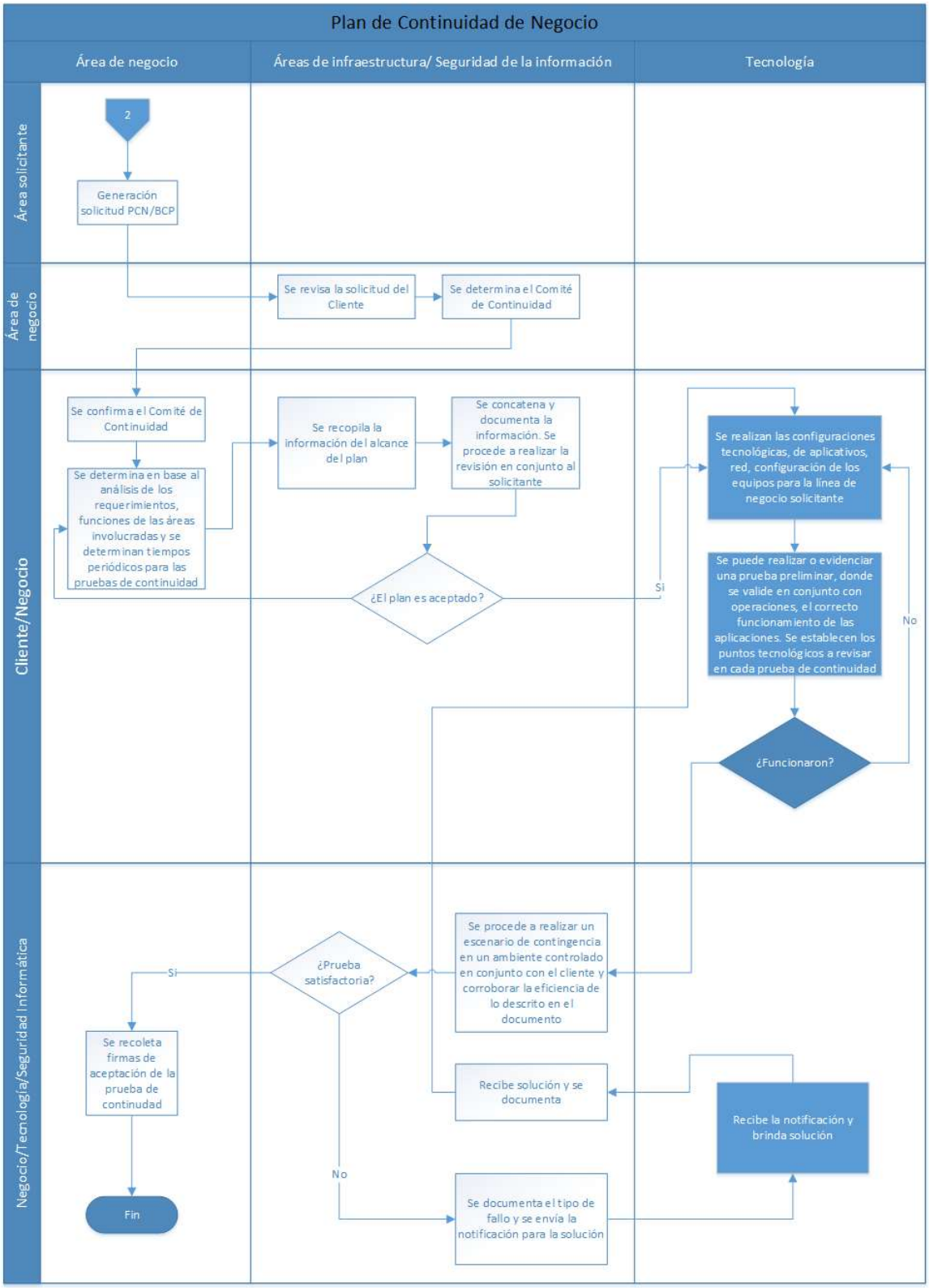


Figura 6.1. Diagama de flujo del plan de continuidad

6.1 Terminología de plan de continuidad

La terminología es la parte principal del plan, para su conocimiento y poder abarcar los requisitos necesarios para cumplirlo, principalmente en el ámbito tecnológico.

Tabla 6.1. Términos del PCN

TÉRMINO	EXPLICACIÓN
Plan de Continuidad del Negocio PCN (BCP-Business Continuity Plan)	Estrategia documentada y probada con el fin de responder ante una contingencia de manera adecuada, logrando así el mínimo impacto a la operación del negocio de los clientes.
Contingencia	Puede ser un problema de corrupción de datos, suministro eléctrico, problema de software o hardware, errores humanos, intrusión, desastres naturales, interrupción en la cadena de suministro con los proveedores, etc.
Plan de Contingencia	Es un plan almacenado dentro del **PCN** donde se contempla la estrategia de reacción ante una contingencia presente que afecte la disponibilidad o los servicios ofrecidos por los sistemas de información.
Plan de Recuperación de Desastres (DRP: Disaster Recovery Plan)	Es aquella parte del **Plan de Contingencia** y del **Plan de Continuidad de Negocio (PCN)**, que aborda aquellas contingencias que, por su gravedad, no permiten continuar prestando el servicio desde el centro local y debe ser reubicado en un centro alterno, mientras el centro origen está indispuesto.
Unidad de Control de Apoyo (UCA)	Es el personal involucrado directamente en las diferentes actividades requeridas para complementar la ejecución correcta de la estrategia de recuperación del **PCN.**
Comité de Continuidad	Son todas aquellas personas responsables de dirigir la correcta gestión de las operaciones de los clientes (RRHH, IT, etc.)
Centro Origen	Es el **Contact Center** donde se lleva la correcta gestión y operación de las actividades de los clientes.
Centro Alterno	Es el **Contact Center** donde se llevará a cabo la réplica de las operaciones de los servicios del cliente, el cual debe contar con la infraestructura tecnológica necesaria de recuperación, en un rango mínimo de **5 kilómetros** de distancia del **Centro Origen**.

6.2 Desarrollo del plan de negocio

En general el proceso del plan de continuidad se puede estructurar en tres principales bloques

1. Crear o modificar el plan de continuidad.

En esta parte del plan se define con cada cliente o línea de negocio los puntos en los cuales el plan de negocio es aplicable, los principales puntos de criticidad de la contingencia y el tiempo de reacción que se debe de tener en caso de presentarse.

2. Análisis y modificación del plan.

Posterior a la definición es necesario establecer puntos de control que se deben de revisar, establecer el centro alterno y porcentaje de operaciones que deberá operar en caso de la contingencia, revisión de la infraestructura tecnológica y pruebas a realizar. La definición algunos estos puntos debe de ser establecido con el cliente de acuerdo a las necesidad de cada línea de negocio, y esto converge con el análisis de infraestructura tecnológica y los puntos que se deben de realizar.

3. Plan de continuidad

Una vez completado el plan de negocio, se debe de establecer la frecuencia con la que se debe de realizar, números de posiciones, y en presencia del comité del Plan de Continuidad, **ver Figura 6.2**.

El comité del plan de continuidad esta establecido por las principales áreas que conforman la empresa: áreas de negocio, servicios Generales, Recursos Humanos y Tecnología.

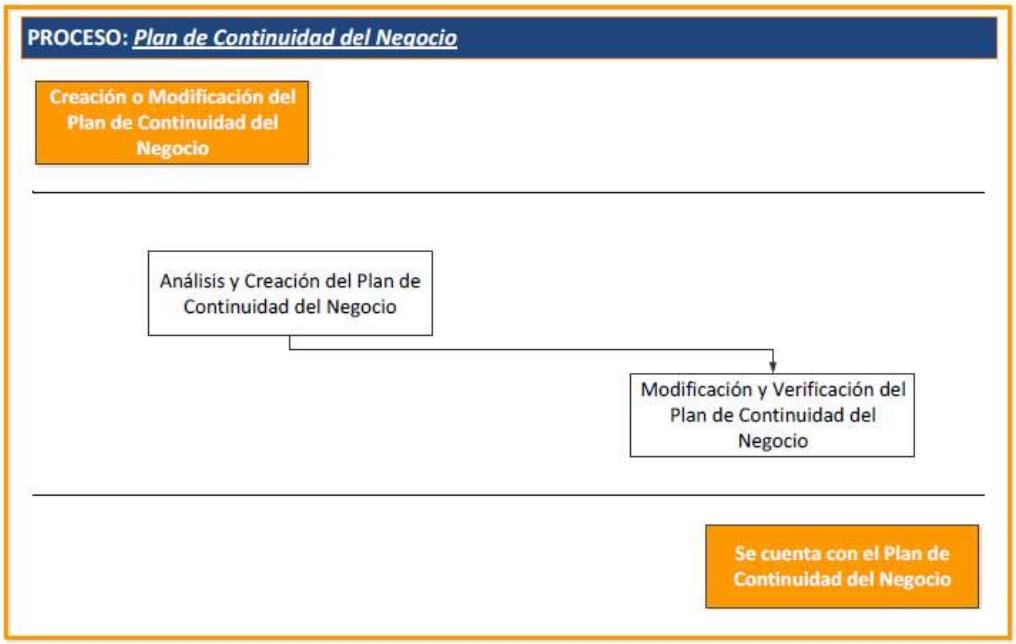


Figura 6.2. Bloques del PCN

6.3 Prueba tecnológica del plan de continuidad

La prueba de continuidad de negocio se implementa de acuerdo a la **Tabla 4.1** observada en el capítulo 4, considerada dentro de los crecimientos de la sede principal a la alterna y a lo acordado con el cliente.

Tabla 6.2 Proyección para el PCN

PCN Soluciones Multicanal	
Línea de negocio	Posiciones para Plan de Continuidad de Negocio (PCN o BCP)
Segmento Bancario Cobranza	125
Segmento Aerolínea Reservaciones	25

El objetivo del PCN es presentar el siguiente escenario de una contingencia real, para fines prácticos se realiza un prueba hipotética en la cual se presenta un escenario en el cual se determina realizar las pruebas durante 1 hora en la sede alterna. El caso hipotético se presenta de la siguiente forma:

Se presenta una contingencia por una manifestación en la sede principal por lo cual los empleados no pueden ingresar al edificio, al verse afectados por 2 horas, sin poder laborar e ingresar a las instalaciones, los niveles de servicio caen, al no poder atender el tráfico de llamadas correspondientes a su flujo diario de llamadas para el área de cobranza del segmento bancario, así como las llamadas de reservaciones de la aerolínea; se procede a realizar una conferencia telefónica entre las figuras del comité de PCN, en la cual se determina mover las operaciones en la sede alterna y poder atender el flujo llamadas.

Para poder proceder con las pruebas tecnológicas dentro del PCN, se deben realizar una réplica de los aplicativos y configuraciones correspondientes, para poder realizar operaciones en un periodo de tiempo determinado para las pruebas, pero considérese que no debe de haber un límite de tiempo en un escenario real.

Al estar inaugurando las operaciones en la sede alterna por el momento se tiene configurado los ruteos y NAT necesarios para poder operar desde la telefonía, así como las aplicaciones internas y aplicaciones cliente-servidor de cada respectiva línea de negocio, a través de los enlaces dedicados MPLS, que permite la interconexión entre los centros.

El número de posiciones a realizar pruebas se realizan de acuerdo al plan de la **Tabla 6.3**:

Tabla 6.3 Estaciones de trabajo a operar dentro del plan de continuidad

Línea de negocio	PA's Sede Principal	PA's Sede Alterna	PA's comprometidas para PCN	PA's Operando en la prueba PCN
Segmento Bancario Redes Sociales	0	150	0	65
Segmento Bancario Cobranza	1250	150	60	210
Segmento Aerolínea Reservaciones	250	0	25	25

Las pruebas a realizarse y acordadas con el cliente deben realizarse las pruebas de acuerdo a la **Tabla 6.4**:

Tabla 6.4. Pruebas a realizar durante el PCN

Plan de pruebas tecnológicas a aplicarse en simulación de caída del centro principal		
0	Simulación para realizar la prueba de continuidad de negocio	Definir la estrategia con el cliente, en el cual se puede simular una caída completa de los medios de comunicación del centro principal, para realizar todo el proceso de operaciones en el centro alterno, o elegir la alternativa de realizar operaciones en ambos centros, recibiendo el tráfico de llamadas inbound en ambos.
1	Pruebas de enlace de datos	Validar la disponibilidad del enlace de datos para conexión de los asesores desde el centro alterno hacia los aplicativos del cliente.
		Revisar que los asesores puedan entrar a todos los aplicativos desde las posiciones designadas en el centro alterno, desde la configuración de los perfiles de directorio activo, carpetas de red, aplicativos cliente-servidor y entornos web.
		Validar que los aplicativos entreguen tiempos de respuesta idóneos o lo más cercano posible con los que operan en el centro principal.
2	Pruebas de telefonía	Validar la disponibilidad del enlace de voz en el centro alterno.
		Verificar que la telefonía tanto de PBX y marcadores predictivos, se puedan autenticar y los operadores puedan recibir llamadas y realizar la atención durante un periodo de 1 hora, en el centro alterno.
		Revisar que los tiempos de autenticación se esten reflejando en las herramientas de monitoreo de los sistemas de telefonía.

3	Tiempos de respuesta de áreas de soporte y mesas de ayuda (áreas internas del Contact Center)	Medición de los niveles de servicio para solventar una incidencia mientras se realiza la prueba de continuidad en el centro alterno.
4	Tiempos de respuesta de áreas de soporte y mesas de ayuda (áreas tecnológicas del respectivo cliente y/o proveedores de enlaces)	Medición de los niveles de servicio para solventar una incidencia mientras se realiza la prueba de continuidad en el centro alterno.
5	Revisión de niveles de servicio del plan de continuidad	Validar del porcentaje de atención de llamadas por los agentes de servicio desde el centro alterno, dando el estatus de efectividad de la prueba de continuidad
6	Retorno de operaciones al centro origen	Finalizada la prueba, se regresará el tráfico de llamadas al centro origen (dependiendo de la elección tomada en el punto 0).
7	Calificación de la prueba de continuidad	Establecer con el cliente y las áreas involucradas, qué tan exitosa fue la prueba y documentarla, así como las observaciones realizadas
8	Acciones correctivas.	En caso de contar con una observación negativa, es necesario realizar un plan de acción para realizar la corrección y entregar la documentación de la misma, y entregársela al cliente final, para poder dar como finalizada la prueba, el periodo de corrección no debe superar las 72 horas, una vez finalizada la prueba de continuidad

Posterior a definir las pruebas a realizarse durante la contingencia se debe de establecer PA's en la sede alterna que se ocuparan, y se deben de mantener siempre fijas y ubicadas para todas las áreas de corporativo.

El siguiente mapa presenta las estaciones de trabajo actuales en la nueva sede y como están operando los asesores, del lado izquierdo son las operaciones del segmento bancario cobranza, y del lado derecho se pueden apreciar las operaciones de redes sociales del segmento bancario, **Figura 6.3.**

Figura 6.3. Posiciones del CC Alterno de operaciones

Retomando los datos de la **Tabla 6.3** y estableciendo cuáles son las PA's definitivas del plan de continuidad, las PA's quedan distribuidas de la siguiente forma, **ver Figura 6.4**:

Rojo- PA's Segmento Bancario Cobranza

Azul-PA's Segmento Bancario Redes Sociales

Amarillo-PA's Segmento Aerolínea Reservaciones

Figura 6.4. Posiciones en el PCN

6.4. Resultados de la Prueba de Continuidad de Negocio

Finalizando la prueba de negocio es necesario capturar evidencias de que la prueba fue satisfactoria y en caso de ser lo inverso, tomar el plan de acción correspondiente con tendencia de mejora inmediata y darle de ser posible una solución al momento o generar el plan de acción para corregirse.

De acuerdo a la tabla 6.4 se especificaron las pruebas que deben de realizarse, por lo mismo se toma las mismas evidencias de la prueba:

0. **Simulación para realizar la prueba de continuidad de negocio.** El escenario se definió hipotético para las pruebas en el **capítulo 6.3**
1. **Prueba de enlace de datos.** Se capturan pruebas de comunicación de aplicativos internos como de cliente-servidor, en las cuales se evidencia el cambio de ruteos

Utilizando la herramienta CMD de Windows, se realizan trazados hacia los destinos de interés, véase en la **Figura 6.5 y 6.6**, antes y despúes de la prueba realizada. El primer salto en ambas figuras especifica el puerta de enlace configurada en el equipo Switch perimetral, el segundo y tecer salto dentro del trazado son los routers de comunicación; se puede apreciar en el segundo salto, una diferencia en la IP, la cual es la que se modificó el ruteo del destino de interés para realizar las validaciones de los enlaces alternos y poder validar que la comunicación se puede realizar sin contratiempos en la sede alterna, ambos trazados se completan, por lo cual la comunicación fue exitosa al realizar el enrutamiento.

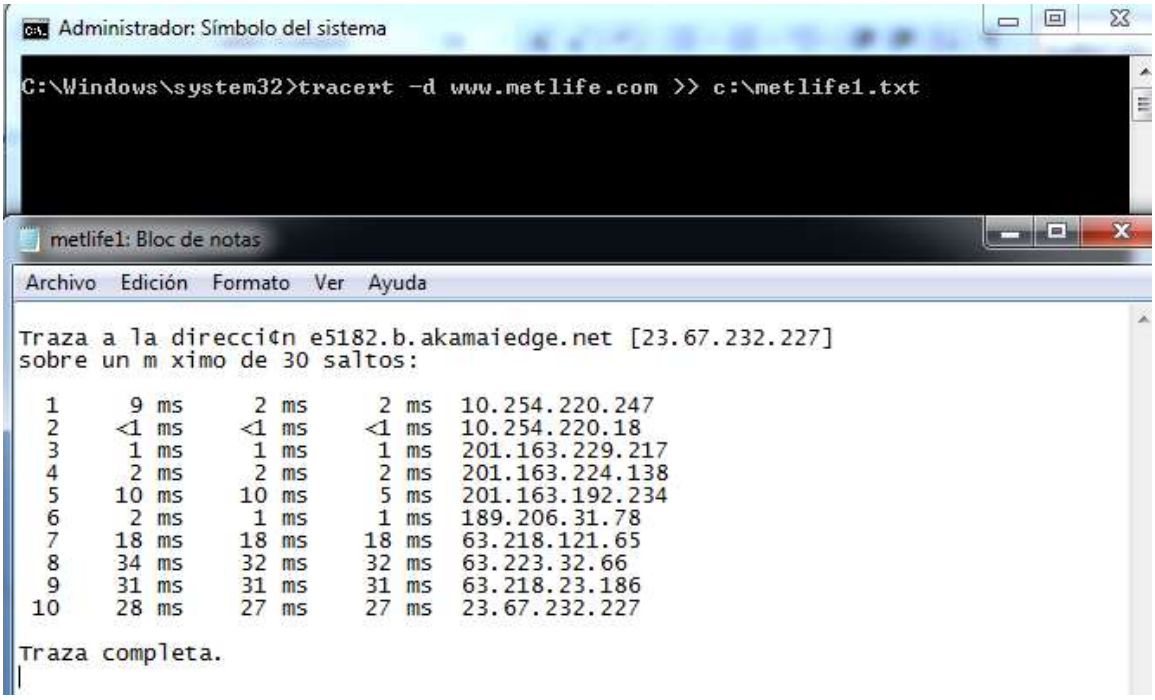


Figura 6.5. Trazados de comunicación en aplicación cliente-servidor antes de iniciar la prueba de contingencia

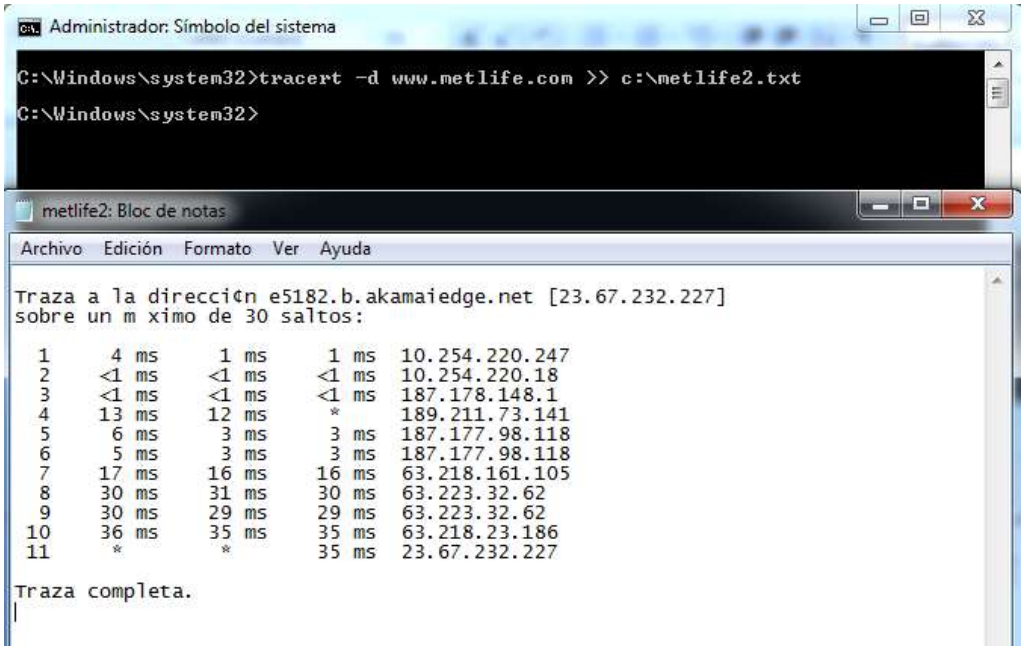


Figura 6.6. Trazados de comunicación en aplicación cliente-servidor después de la prueba de contingencia

2. **Pruebas de telefonía.** Se toman evidencias de pruebas de llamadas recibidas dentro del sistema de monitoreo y gestión de telefonía, así como evidencias de trazados donde se aprecie la variación en los ruteos, **ver Figura 6.7, 6.8 y 6.9**.

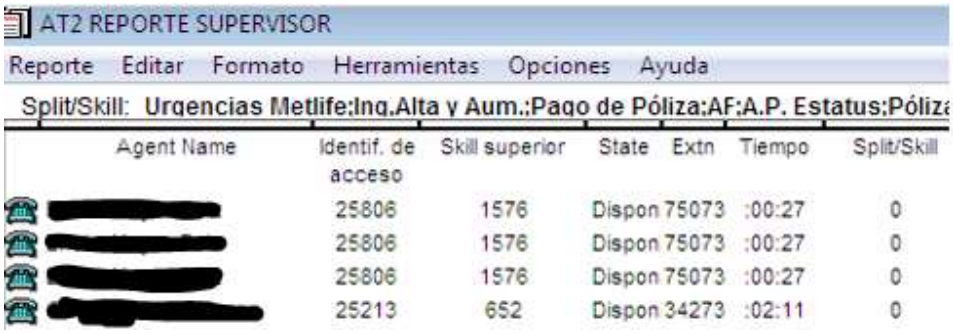


Figura 6.7. Evidencia de CMS de pruebas de telefonía

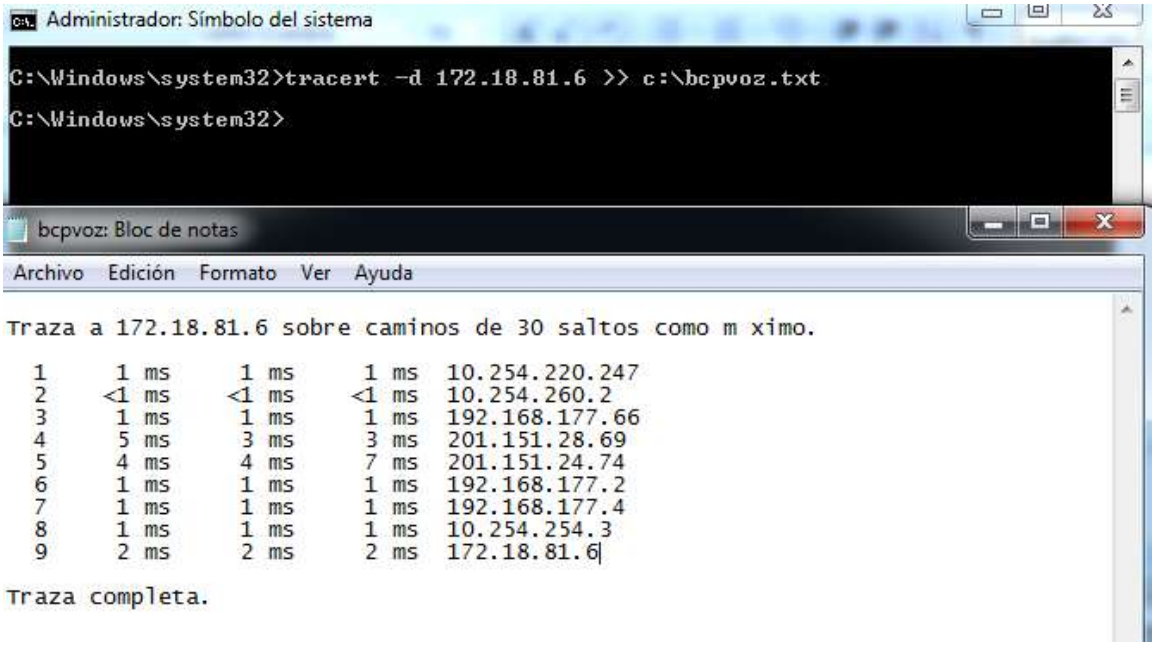


Figura 6.8. Trazado de comunicación antes de iniciar la prueba de contingencia

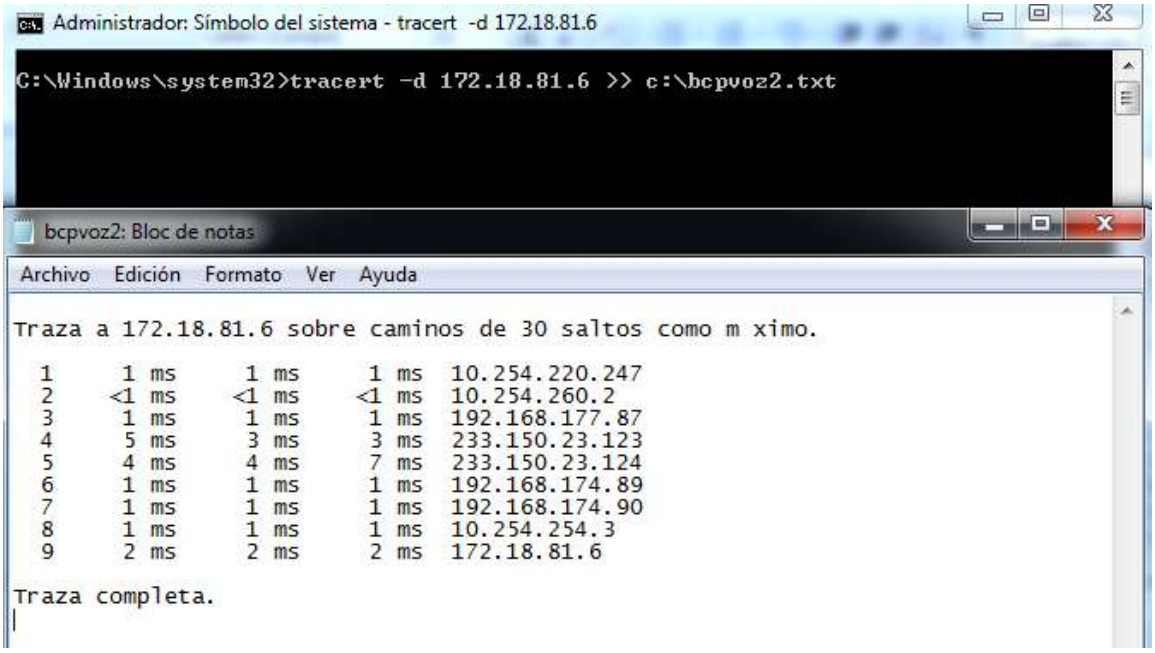
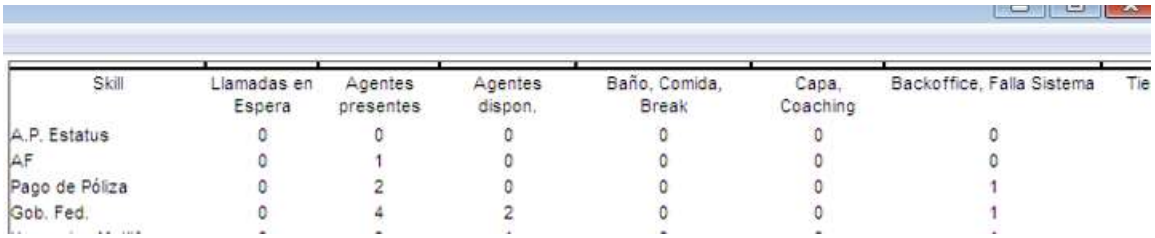


Figura 6.9. Trazado de comunicación después de la prueba de contingencia

3. **Tiempos de respuesta de áreas de soporte y mesas de ayuda (áreas internas del Contact Center).** No se presentó ningún contratiempo
4. **Tiempos de respuesta de áreas de soporte y mesas de ayuda (áreas tecnológicas del respectivo cliente y/o proveedores de enlaces).** No se presentó ningún contratiempo
5. **Revisión de niveles de servicio del plan de continuidad.** Se toma una nueva captura de la herramienta de monitoreo de telefonía, así como pruebas de comunicación ping a los destinos más comunes y validar el tiempo de respuesta, **ver figura 6.10 y 6.11**.



Skill	Llamadas en Espera	Agentes presentes	Agentes dispon.	Baño, Comida, Break	Capa, Coaching	Backoffice, Falla Sistema	Tie
A.P. Estatus	0	0	0	0	0	0	
AF	0	1	0	0	0	0	
Pago de Póliza	0	2	0	0	0	1	
Gob. Fed.	0	4	2	0	0	1	

Figura 6.10. Evidencia de reportería CMS en tiempo real después de 30 min

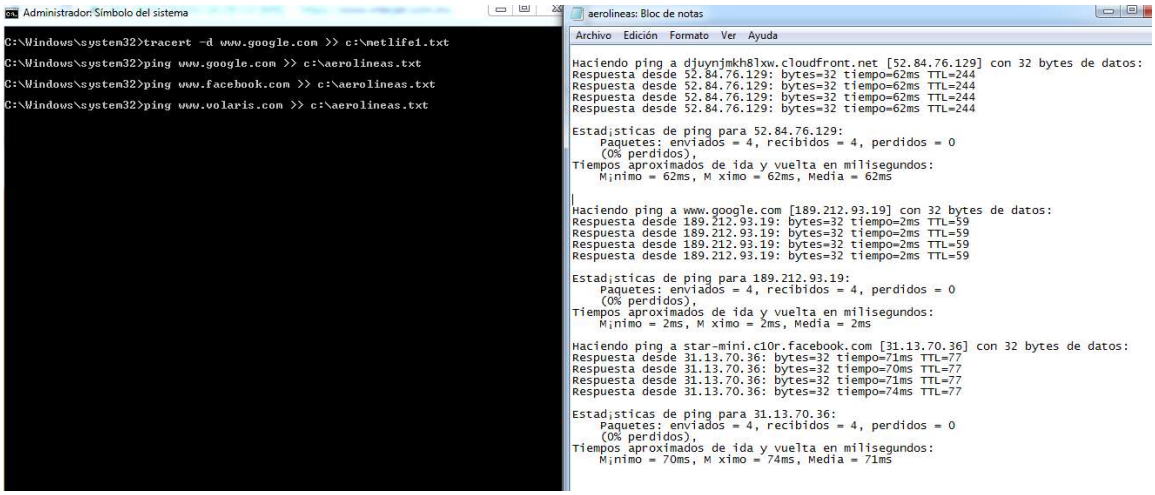


Figura 6.11. Ping a 3 destinos comunes utilizados por los operadores.

6. **Retorno de operaciones al centro origen.** Las operaciones regresan a su normalidad al finalizar la prueba pactada en el intervalo de tiempo definido.
7. **Calificación de la prueba de continuidad.** Satisfactoria
8. **Acciones correctivas.** No se requieren acciones correctivas, se cierra la prueba

Al finalizar las pruebas, estos comentarios se deben de agregar al acta donde debe de ser firmada por el comité del plan de continuidad, por temas de seguridad de la información no se puede presentar el acta oficial, firmada, para garantizar la integridad de la empresa.

Se debe agregar en el formato membretado las siguientes tablas, ver **Tabla 6.5 y 6.6**, donde se especifica y documenta si la prueba de continuidad fue exitosa o se requiere alguna corrección y las firmas correspondientes del comité de continuidad.

Tabla 6.5 Formato para la confirmación de la prueba de continuidad

Nombre del Plan	Plan de Continuidad de Negocio Soluciones Multicanal
Responsable del Plan	Carlos Reyes
Sede Primaria:	CC Soluciones Multicanal Sede Principal
Sede Alterna:	CC Soluciones Multicanal Sede Alterna
Tipo de Prueba:	Prueba con Aviso

Fecha de Prueba	
Hora de Inicio:	08:42 hrs
Hora Fin:	09:40 hrs.
Objetivo:	Comprobar la operatividad del Plan de Continuidad de Negocio del segmento bancario y aerolinea en la sede alterna
Descripción de la prueba	Recuperación de los servicios enContact Center simulando los siguientes escenarios: No acceso al Centro de Trabajo. No acceso a Sistemas. Indisponibilidad de Recursos Humanos Críticos. Indisponibilidad de los Proveedores Críticos. Destrucción Total.

Tabla 6.6 Tabla de firmas de los involucrados en las pruebas de continuidad

Nombre	Puesto	Firma
	Oficina de Continuidad de Negocio Segmento Bancario	
	Oficina de Continuidad de Negocio Segmento Aerolínea	
	Control Interno Segmento Bancario	
	Coordinador de Operaciones	

Carlos Reyes Martínez	Coordinador de Soporte Tecnológico	

CAPÍTULO 7 Reducción de software del licenciamiento Microsoft

Actualmente el Contact Center utiliza software de licenciamiento, el cual les permite trabajar todos los programas a un costo elevado. Para llevar a cabo esto, se hizo un plan de migración en el cual se reemplaza el software con licenciamiento por el software libre. De tal forma que se puedan realizar las mismas tareas que se llevan a cabo actualmente con software con licenciamiento. En algunos casos específicos, se permite el uso de software con licenciamiento, éstos pasan por un proceso de justificación y autorización para definir que su uso sea imprescindible y no reemplazable por algún otro libre, principalmente esto representa a las figuras administrativas como supervisores, coordinadores y áreas de mejora continua, que utilizan correo institucional.

Como parte del proceso para una reducción de licenciamiento de Microsoft (Visio, Project, Office, Servers) se revisan diferentes opciones de implementación de software libre. De tal manera que el cambio signifique tener el menor impacto a los usuarios sin que se vea afectada la operación.

El software libre se utiliza cada vez más, no solo por el ahorro de adquisición del licenciamiento sino también por la disponibilidad del código fuente que permite al usuario especializado adaptar, configurar o modificar dicho software para sus necesidades, así como elaborar nuevas aplicaciones ya sea con fines comerciales o para difusión como nuevo software libre.

7.1 Objetivo

Migrar e Implementar el software de licenciamiento con costo a software libre con el menor impacto en la operación. Llevando el proceso de manera que no se vean afectadas las diferentes campañas y requerimientos del centro.

7.2 Desarrollo

El análisis realizado de esta migración es fundamentado en las siguientes situaciones:

1. La sede principal del Contact Center, cuenta con licenciamiento Microsoft en todas las estaciones de trabajo operativas, desde su implementación, por lo cual se ha notificado a los respectivos clientes que se realiza la migración exponencial de la solución por una libre.
2. La sede alterna también fue implementada con licenciamiento Microsoft para no generar un cambio en cuanto a la forma de trabajo en el crecimiento del segmento bancario, ya que este proyecto se está prestando en dos etapas, iniciando por la sede principal

3. El costo del licenciamiento Microsoft, es de costo anual (MXN 1,447,192.80) , por lo cual la reducción del licenciamiento puede ser reutilizado en costos de mantenimiento, refacciones o renovación de componentes de las estaciones de trabajo.
4. Los únicos con licenciamiento Microsoft serán las figuras administrativas de ambos Contact Center.
5. Las soluciones propuestas y validadas sin generarles ninguna afectación a la forma de trabajo de ambas líneas de negocios son: Open Office, Libre Office, **ver Figura 7.1.**

Para utilizar el software la única limitante encontrada fue en la compatibilidad de las macros de Microsoft Office y las dos versiones diferentes de software libres.

En los foros localizados para realizar compatibilidad entre softwares en las macros, es necesario utilizar programación en línea de comandos para las macros, por lo cual no todo el personal está preparado y capacitado para realizarlo. Microsoft Office presenta una interfaz más amigable, para el diseño de la macros, y solo son utilizadas por figuras administrativas de la empresa y de operaciones, los operadores de los segmentos cobranza y reservaciones no requieren este tipo de macros, y el uso de las hojas de cálculo y de datos son de "uso cotidiano", revisión de ortografía, copiar y pegar para facilitar el escribir las mismas frases para las tipificaciones de sus aplicativos.

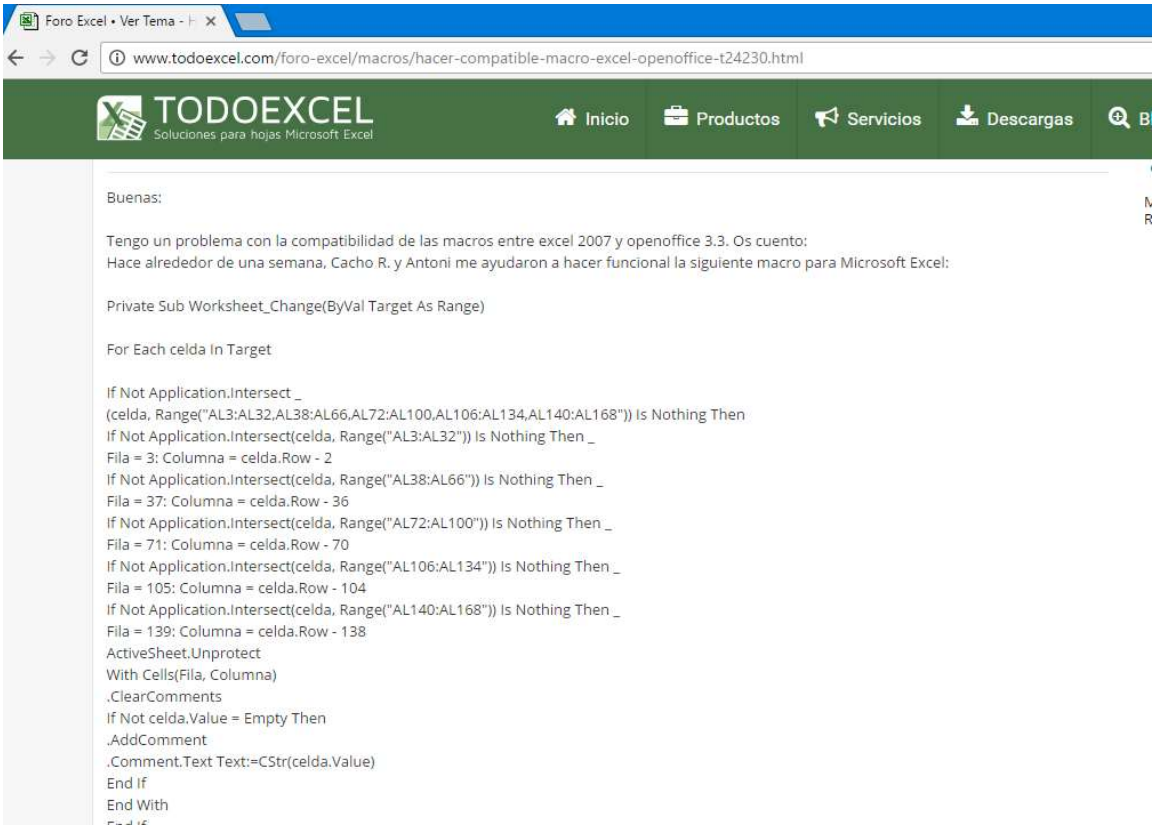


Figura 7.1. Propuesta de solución web de macros para Open Office

En Soluciones Multicanal se tiene registrado el siguiente licenciamiento, se puede apreciar una diferencia en el número de PA's reportadas en la **Taba 7.1.** Debido a que la proyección presentada representa la petición operativa del cliente hacia Soluciones Multicanal, en la siguiente tabla se está contemplando las estaciones de personal administrativo (IT, Relaciones Laborales, Recursos Humanos, etc.).

Tabla 7.1. Licenciamiento Microsoft del corporativo

Soluciones Multicanal S.A. de C.V.		
Sede Principal	Bancario	1250
	Aerolínea	250
	Administrativos	50
Sede Alterna	Bancario	300
	Administrativos	20
	Total PA's	1870

Es importante la consideración dentro de las estaciones operativas el total incluye el dato de supervisores, coordinadores y áreas de mejor continua, por la cual la proyección de desinstalación como se aprecia en la **Tabla 7.2**:

Tabla 7.2 Licenciamiento Microsoft a reducir

Numero de licencias de Soluciones Multicanal S.A. de C.V. a reducir	
Sede Principal	1450
Sede Alterna	280
Total PA's	1730

La **tabla 7.3** representa la reducción del número de licencias contemplado solo dejar las necesarias para administrativos de corporativo y de operaciones, se visualiza el ahorro en la factura por el licenciamiento, la reducción es de 1830 licencias a 1730, representando el 93 % en el costo de licenciamiento.

Tabla 7.3. Beneficio monetario a reducir con el licenciamiento

Soluciones Multicanal S.A. de C.V.		Costo por licencia:	USD 43.02
Sede Principal	1450	USD 62,379.00	MXN 1,447,192.80
Sede Alterna	280	USD 12,045.60	MXN 279,457.92
	Total	USD 74,424.60	MXN 1,726,650.72

La migración del software contempla tecnológicamente contemplar los siguientes pasos:

1. Desinstalación del software Microsoft Office, desde Programas->Panel de control, **ver Figura 7.2**.

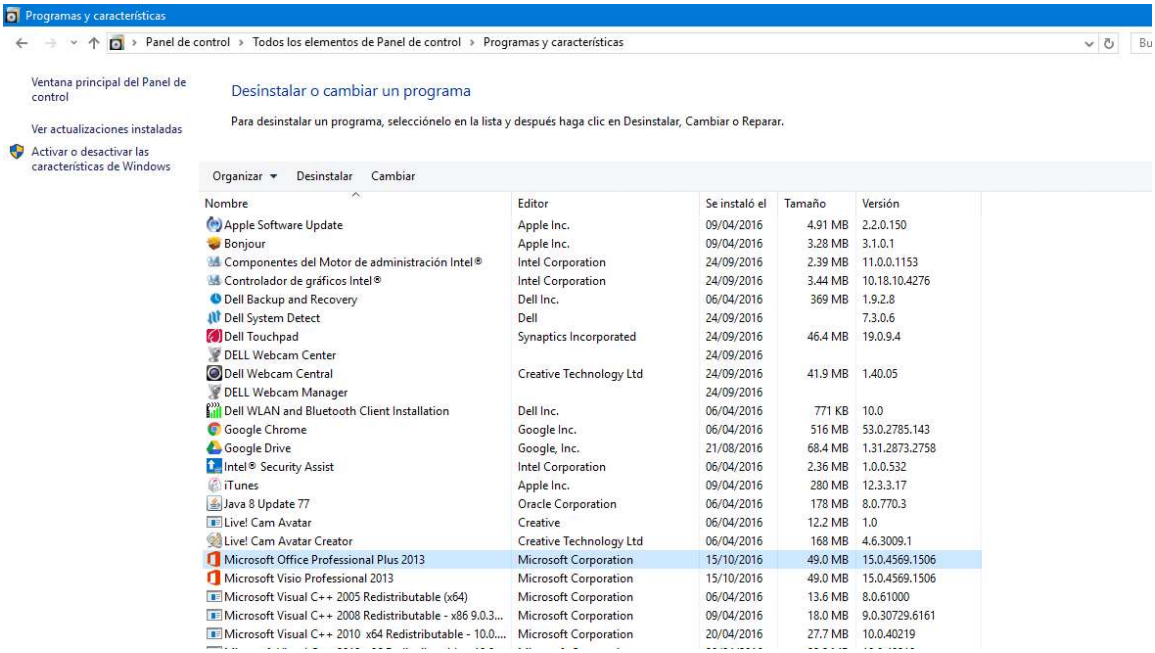


Figura 7.2. Panel de Control de Windows

2. Descarga y ejecución de la herramienta "Fixit" de Microsoft para eliminar las llaves de registro del licenciamiento de Office en todas sus versiones, **ver Figura 7.3.**

Office 2003,2007,2010:

https://blogs.technet.microsoft.com/office_sp/2011/06/13/tiene-problemas-para-desinstalar-office-2010-2007-2003-desde-el-panel-de-control-use-la-herramienta-fix-it/

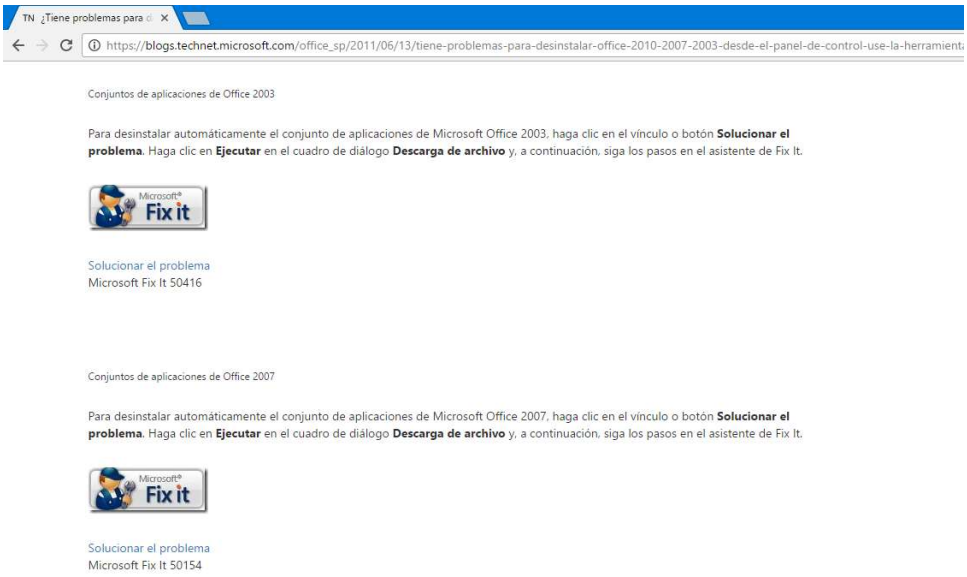


Figura 7.3. Herramientas Fix it, para desinstalación completa del licenciamiento

3. Descarga e instalación de Libre Office para el reemplazo del licenciamiento Microsoft, **ver Figura 7.4**.

https://es.libreoffice.org/descarga/libreoffice-estable/

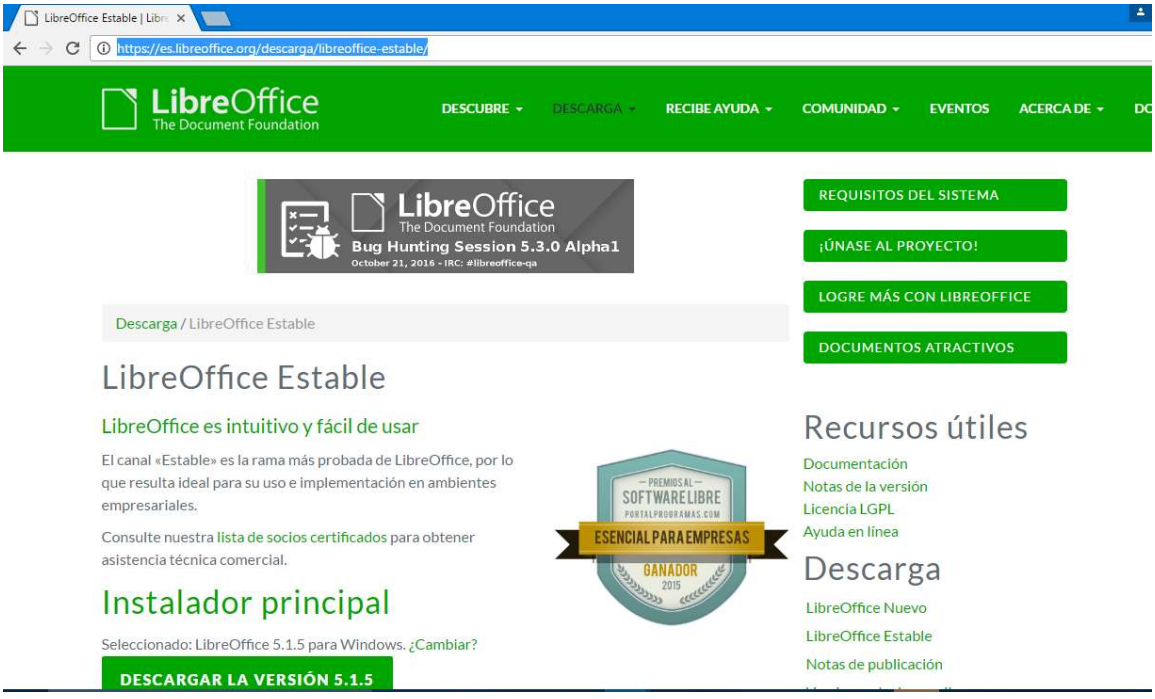


Figura 7.4. Software libre "Libre Office"

4. Agregar al menú de inicio de los operadores de los servicios del segmento bancario y aerolínea los accesos directos para su uso, **ver Figura 7.5 y 7.6**.

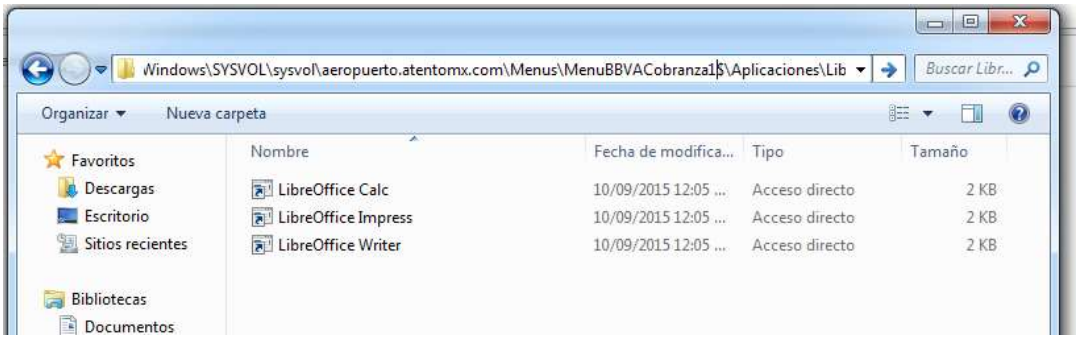


Figura 7.5. Accesos directos de la nueva paquetería agregados al menú de inicio por Active Directory

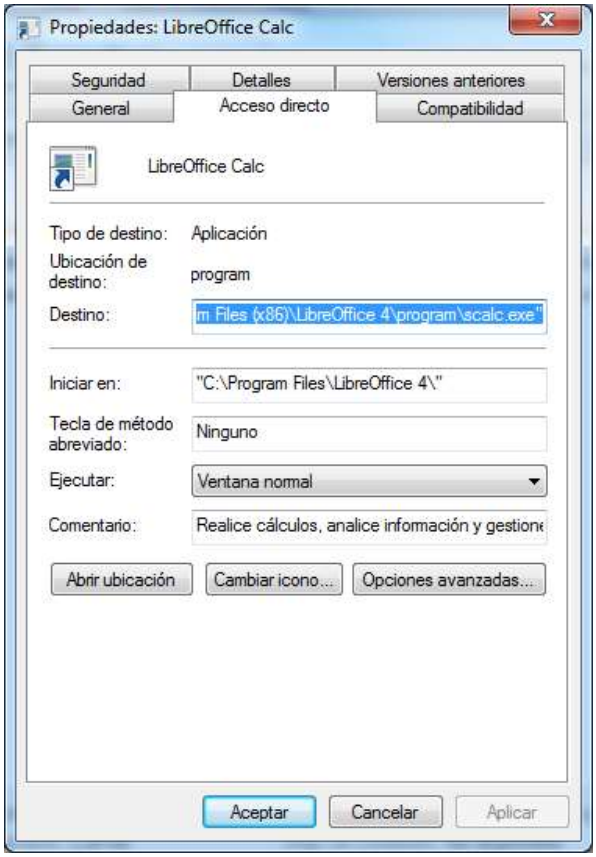


Figura 7.6. Validación de los acceso directos apuntando a la ruta de instalación localmente.

7.3 Plan de trabajo para la migración y evidencias de realización

El tiempo de muestra para la actividad completa por estación de trabajo es de aproximadamente 45 min, se presenta el siguiente plan de trabajo en el cual las actividades se realizan fuera de horario productivo de operaciones, para no generar afectación ni un impacto en los niveles de servicio de operación. Se realiza la desinstalación de 100 Posiciones de operador por noche.

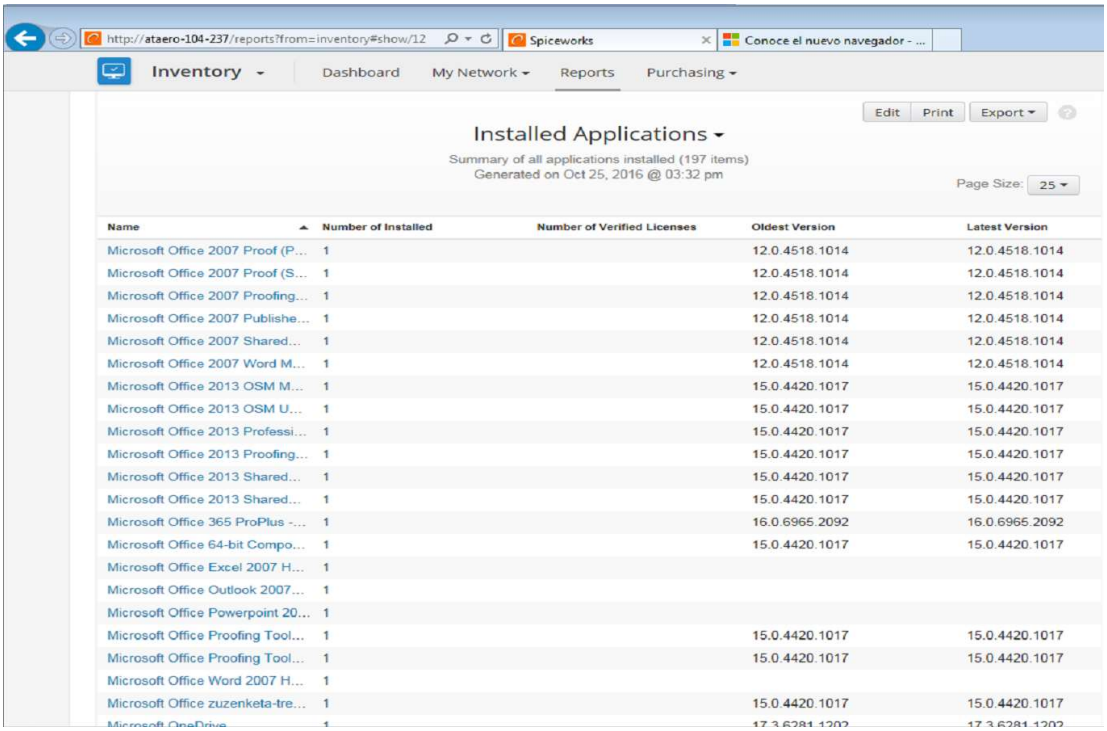
Las evidencias son entregadas mediante la herramienta de monitoreo implementada Spiceworks, que en su sección de reportería permite el análisis del software instalado.

Tabla 7.4 Plan de trabajo para la desinstalación de Office

Plan de desintalación de Licenciamiento Office																		
Fecha	26/09/2016	27/09/2016	28/09/2016	29/09/2016	30/09/2016	03/10/2016	04/10/2016	05/10/2016	06/10/2016	07/10/2016	10/10/2016	11/10/2016	12/10/2016	13/10/2016	14/10/2016	17/10/2016	18/10/2016	19/10/2016
PA's	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	30
															Total:		1730	

Evidencias de la actividad:

La **Figura 7.7** muestra mediante la herramienta Spiceworks el trabajo realizado para la desintalacion de Office, se puede apreciar un número reducido de licenciamiento registrado por lo cual el objetivo se ha cumplido, de acuerdo a la **Tabla 7.2**.



Name	Number of Installed	Number of Verified Licenses	Oldest Version	Latest Version
Microsoft Office 2007 Proof (P...	1		12.0.4518.1014	12.0.4518.1014
Microsoft Office 2007 Proof (S...	1		12.0.4518.1014	12.0.4518.1014
Microsoft Office 2007 Proofing...	1		12.0.4518.1014	12.0.4518.1014
Microsoft Office 2007 Publishe...	1		12.0.4518.1014	12.0.4518.1014
Microsoft Office 2007 Shared...	1		12.0.4518.1014	12.0.4518.1014
Microsoft Office 2007 Word M...	1		12.0.4518.1014	12.0.4518.1014
Microsoft Office 2013 OSM M...	1		15.0.4420.1017	15.0.4420.1017
Microsoft Office 2013 OSM U...	1		15.0.4420.1017	15.0.4420.1017
Microsoft Office 2013 Professi...	1		15.0.4420.1017	15.0.4420.1017
Microsoft Office 2013 Proofing...	1		15.0.4420.1017	15.0.4420.1017
Microsoft Office 2013 Shared...	1		15.0.4420.1017	15.0.4420.1017
Microsoft Office 2013 Shared...	1		15.0.4420.1017	15.0.4420.1017
Microsoft Office 365 ProPlus -...	1		16.0.6965.2092	16.0.6965.2092
Microsoft Office 64-bit Compo...	1		15.0.4420.1017	15.0.4420.1017
Microsoft Office Excel 2007 H...	1			
Microsoft Office Outlook 2007...	1			
Microsoft Office Powerpoint 20...	1			
Microsoft Office Proofing Tool...	1		15.0.4420.1017	15.0.4420.1017
Microsoft Office Proofing Tool...	1		15.0.4420.1017	15.0.4420.1017
Microsoft Office Word 2007 H...	1			
Microsoft Office zuzenketa-tre...	1		15.0.4420.1017	15.0.4420.1017
Microsoft OneDrive	1		17.3.6281.1202	17.3.6281.1202

Figura 7.7 Licenciamiento de office en Spiceworks

CONCLUSIONES

Para el diseño de una sede es importante en primer lugar tener el conocimiento de todos los componentes tecnológicos que son ocupados para abastecer los servicios dentro del Contact Center, incluyendo desde los componentes físicos tenerlos identificados así como el funcionamiento y características de la configuración general y particulares (ruteos y NAT en el caso de los equipos de comunicación), y la ubicación física dentro de las instalaciones.

Seguir la misma directriz para los servidores y equipos de cómputo, proporciona tener identificado las posibles fallas y sus prontas soluciones, pero principalmente en caso de que el cliente requiera un crecimiento de sus operaciones, facilitar y mejorar los tiempos de implementación.

La implementación de la sede alterna se logró debido a estas prácticas en el diseño, y el reconocimiento de las características tecnológicas, lo cual provee una satisfacción al cliente (encuesta de uso interno realizada anualmente) al tener un control y una eficiente implementación. La proyección de la implementación en el caso de los planes de crecimiento siempre se realizan contratualmente a un año para su licitación, con otros proveedores, para este tipo de proyectos se puede llegar a "fracasar", sólo en dirección a las fechas establecidas y compretidas de su implementación, por algun tema de retraso de proveedores o de las áreas contiguas del Contact Center, o hasta del misma área de TI. Por eso se debe de realizar la correcta proyección, gestión de tiempo y en caso de ser necesario, solicitar una ampliación de días para la entrega de los servicios correspondientes. Así mismo es necesario garantizar que el cliente final pueda realizar sus operaciones de la sede principal hacia la sede alterna, de acuerdo a las características del Plan de Continuidad de Negocio para Tecnología, el cual permite en caso de un desastre imprevisto, tener la menor afectación en las operaciones realizadas en las líneas de negocio.

Como valor agregado y como requisito principal es mantener los procesos de seguridad informática, los cuales se desarrollan y generan las políticas de seguridad física y lógica, para el control de la información y acceso de quien deba tenerla, generando controles de seguridad, los cuales se reflejan en garantizar la confidencialidad en primer lugar de Soluciones Multicanal hacia sus proveedores y de los proveedores a los usuarios finales, evitando perdidas y fugas de información y prevención de fraudes. Estas características y procesos que permiten ir obteniendo mayor continuidad y crecimiento en el negocio, fidelizando en primer lugar a los clientes que se tienen, así como permitir la inclusión de nuevos clientes. Es importante agregar que el cumplimiento de estos procesos de seguridad permite al Contact Center obtener certificaciones y mejorar su estrategia de negocio y reducir posibles problemas hacia el usuario final.

Otra parte importante en la gestión de los Contact Center es realizar una reducción en los gastos, lo mismo que se ha logrado inicialmente en los costos de licenciamiento de software Microsoft para los operadores. Estas ganancias económicas permiten ofrecerle al cliente soluciones innovadoras y funcionales en software libre, así como la reutilización de estos gastos para tener un plan de prevención y de almacenamiento de componentes que puedan a tener una falla física por defecto de fábrica o mal funcionamiento por antigüedad, ej. Adquisición de un servidor, fuentes de alimentación, discos duros de servidores o periféricos para los equipos de operaciones.

Glosario

Back Office

Conjunto de actividades de apoyo al negocio, es la parte de las empresas que realizan las tareas destinadas a gestionar la propia empresa y que no tienen contacto directo con el cliente, como las labores informáticas y de comunicaciones, de gestión de recursos humanos, contabilidad o finanzas.

Discar

Marcar un número de teléfono

HTML

HTML, sigla en inglés de HyperText Markup Language (lenguaje de marcas de hipertexto), hace referencia al lenguaje de marcado para la elaboración de páginas web. Es un estándar que sirve de referencia del software que conecta con la elaboración de páginas web en sus diferentes versiones, define una estructura básica y un código (denominado código HTML) para la definición de contenido de una página web, como texto, imágenes, videos, juegos, entre otros. Es un estándar a cargo del World Wide Web Consortium (W3C) o Consorcio WWW, organización dedicada a la estandarización de casi todas las tecnologías ligadas a la web, sobre todo en lo referente a su escritura e interpretación. Se considera el lenguaje web más importante siendo su invención crucial en la aparición, desarrollo y expansión de la World Wide Web (WWW). Es el estándar que se ha impuesto en la visualización de páginas web y es el que todos los navegadores actuales han adoptado.

HTTP/HTTPS

HTTP: Hypertext Transfer Protocol o HTTP (en español protocolo de transferencia de hipertexto) es el protocolo de comunicación que permite las transferencias de información en la World Wide Web. HTTP fue desarrollado por el World Wide Web Consortium y la Internet Engineering Task Force, colaboración que culminó en 1999 con la publicación de una serie de RFC, el más importante de ellos es el RFC 2616 que especifica la versión 1.1. HTTP define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, proxies) para comunicarse. HTTP es un protocolo sin estado, es decir, no guarda ninguna información sobre conexiones anteriores. El desarrollo de aplicaciones web necesita frecuentemente mantener estado. Para esto se usan las cookies, que es información que un servidor puede almacenar en el sistema cliente. Esto le permite a las aplicaciones web instituir la noción de "sesión", y también permite rastrear usuarios ya que las cookies pueden guardarse en el cliente por tiempo indeterminado.

HTTPS: Hypertext Transfer Protocol Secure (en español: Protocolo seguro de transferencia de hipertexto), más conocido por sus siglas HTTPS, es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP.

Es utilizado principalmente por entidades bancarias, tiendas en línea, y cualquier tipo de servicio que requiera el envío de datos personales y/o contraseñas.

LAN

Una red de área local o LAN (por las siglas en inglés de Local Area Network) es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.

La topología de red define la estructura de una red. Una parte de la definición topológica es la topología física, que es la disposición real de los cables o medios. La otra parte es la topología lógica, que define la forma en que los hosts acceden a los medios para enviar datos.

Inbound

En la operación de un call center se define como la actividad de atención de llamadas recibidas.

Inhouse

Se denomina el inhouse, cuando el call center vive dentro de la empresa, o bien pertenece a la firma, y presta servicios únicamente a los clientes de esa compañía, probablemente bajo la figura de una filial.

Inshore

Empresas de call center que realizan servicios de outsourcing en el mercado local.

Insourcing

Es delegar todo el trabajo a los empleados directos de la organización, básicamente es lo contrario de la internalización. El propósito del insourcing es mantener el control en las operaciones y procesos de la compañía que deriva en reducir costos y tiempo de capacitación si estas tareas se asignan a terceros, también se evita lidiar con las diferencias culturales de los empleados cuando estos deben tener un trato directo con los clientes y por ejemplo el idioma representa una gran barrera de comunicación, les permite a los empleados sentirse más integrados , ser leales y eficaces por lo que reduce los niveles de rotación.

MAC

En las redes de computadoras, la dirección MAC (siglas en inglés de media access control; en español "control de acceso al medio") es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo. Está determinada y configurada por el IEEE (los primeros 24 bits) y el fabricante (los últimos 24 bits) utilizando el organizationally unique identifier. La mayoría de los protocolos que trabajan en la capa 2 del modelo OSI usan una de las tres numeraciones manejadas por el IEEE: MAC-48, EUI-48, y EUI-64, las cuales han sido diseñadas para ser identificadores globalmente únicos. No todos los protocolos de comunicación usan direcciones MAC, y no todos los protocolos requieren identificadores globalmente únicos.

MAN

Una red de área metropolitana (MAN, siglas del inglés Metropolitan Area Network) es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica extensa, proporcionando capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado (MAN BUCLE), la tecnología de pares de cobre se posiciona como la red más grande del mundo una excelente alternativa para la creación de redes metropolitanas, por su baja latencia (entre 1 y 50 ms), gran estabilidad y la carencia de interferencias radioeléctricas, las redes MAN BUCLE, ofrecen velocidades de 10 Mbit/s ó 20 Mbit/s, sobre pares de cobre y 100 Mbit/s, 1 Gbit/s y 10 Gbit/s mediante fibra óptica.

Otra definición podría ser: Una MAN es una colección de LANs o CANs dispersas en una ciudad (decenas de kilómetros). Una MAN utiliza tecnologías tales como ATM, Frame Relay, xDSL (Digital Subscriber Line), WDM (Wavelenght Division Modulation), ISDN, E1/T1, PPP, etc. para conectividad a través de medios de comunicación tales como cobre, fibra óptica, y microondas.

Nearshore

Nearshore es un tipo de subcontratación o externalización de una actividad con salarios más bajos que en el propio país, que se encuentra relativamente cerca en la distancia o la zona horaria (o ambos). El cliente espera beneficiarse de una o varias de las siguientes construcciones de proximidad: geográficas, temporales, culturales, lingüísticas, económicas, políticas, o de vínculos históricos.

NNTP

Network News Transport Protocol (NNTP) es un protocolo inicialmente creado para la lectura y publicación de artículos de noticias en Usenet(es el acrónimo de Users Network (Red de usuarios). Su traducción literal al español es "protocolo para la transferencia de noticias en red".

Offshore

Empresas que exportan servicios hacia el extranjero, que desarrollan outsourcing de servicios fuera del territorio donde los proveen, deslocalización o servicios empresariales a distancia, comúnmente utilizado en diversos ámbitos para indicar el traslado de un recurso o proceso productivo a otro país.

Outbound

En la operación de un call center se define como la actividad de atención de llamadas realizadas

Outsourcing

Es un término inglés muy utilizado en el idioma español, su vocablo equivalente es subcontratación, el contrato que una empresa realiza a otra para que ésta lleve a cabo determinadas tareas que, originalmente, estaban en manos de la primera.

El outsourcing, en otras palabras, consiste en movilizar recursos hacia una empresa externa a través de un contrato. De esta forma, la compañía subcontratada desarrolla actividades en nombre de la primera. Por ejemplo: una firma que ofrece servicios de acceso a Internet puede subcontratar a otra para que realice las instalaciones. La empresa principal cuenta con la infraestructura de redes necesaria y el plantel para vender el servicio; la segunda, en cambio, se limita a llegar hasta el domicilio del usuario para efectuar la instalación pertinente. Cabe señalar que para el cliente final no existe diferencia alguna entre la empresa contratante y la subcontratada.

PSTN

La red telefónica pública conmutada (PSTN, Public Switched Telephone Network) es una red con conmutación de circuitos tradicional optimizada para comunicaciones de voz en tiempo real. Cuando llama a alguien, cierra un conmutador al marcar y establece así un circuito con el receptor de la llamada. PSTN garantiza la calidad del servicio (QoS) al dedicar el circuito a la llamada hasta que se cuelga el teléfono. Independientemente de si los participantes en la llamada están hablando o en silencio, seguirán utilizando el mismo circuito hasta que la persona que llama cuelgue.

La Interfaz de programación de aplicaciones de telefonía (TAPI, <Telephony Application Programming Interface>) permite a los programas comunicarse fácilmente a través de la red de telefonía tradicional. TAPI permite la conexión directa con una red PSTN y marcado telefónico automático, y proporciona interfaces para llamadas de conferencia, correo de voz e identificador de la persona que llama.

Según la UIT-T podemos definirla como Red Digital de Servicios Integrados (RDSI o ISDN en inglés) como: una red que procede por evolución de la Red Digital Integrada (RDI) y que facilita conexiones digitales extremo a extremo para proporcionar una amplia gama de servicios, tanto de voz como de otros tipos, y a la que los usuarios acceden a través de un conjunto de interfaces normalizados.

Rack

Un rack es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones. Las medidas para la anchura están normalizadas para que sean compatibles con equipamiento de distintos fabricantes. También son llamados bastidores, cabinas, gabinetes o armarios.

Externamente, los racks para montaje de servidores tienen una anchura estándar de 600 milímetros (mm) y un fondo de 600, 800, 900, 1000 y ahora incluso 1200 mm. La anchura de 600 mm para racks de servidores coincide con el tamaño estándar de las losetas en los centros de datos. De esta manera es muy sencillo hacer distribuciones de espacios en centros de datos (CPD). Para el cableado de datos se utilizan también racks de 800 mm de ancho, cuando es necesario disponer de suficiente espacio lateral para el guiado de cables.

SIP

Session Initiation Protocol (SIP o Protocolo de Inicio de Sesiones) es un protocolo desarrollado por el grupo de trabajo MMUSIC del IETF con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos en línea y realidad virtual.

La sintaxis de sus operaciones se asemeja a las de HTTP y SMTP, los protocolos utilizados en los servicios de páginas Web y de distribución de e-mails respectivamente. Esta similitud es natural ya que SIP fue diseñado para que la telefonía se vuelva un servicio más en Internet.

SMTP

Simple Mail Transfer Protocol (SMTP) o "protocolo para transferencia simple de correo", es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA, teléfonos móviles, impresoras, etc).

El funcionamiento de este protocolo se da en línea, de manera que opera en los servicios de correo electrónico. Sin embargo, este protocolo posee algunas limitaciones en cuanto a la recepción de mensajes en el servidor de destino (cola de mensajes recibidos). Como alternativa a esta limitación se asocia normalmente a este protocolo con otros, como el POP o IMAP, otorgando a SMTP la tarea específica de enviar correo, y recibirlos empleando los otros protocolos antes mencionados

Telnet

Telnet (Telecommunication Network1) es el nombre de un protocolo de red que nos permite viajar a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella. También es el nombre del programa informático que implementa el cliente. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

UDP

User Datagram Protocol (UDP) es un protocolo del nivel de transporte basado en el intercambio de datagramas (Encapsulado de capa 4 Modelo OSI). Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción. Su uso principal es para protocolos como DHCP, BOOTP, DNS y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

VLAN

VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.1 Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa 3 y 4).

Una VLAN consiste en dos o más redes de computadoras que se comportan como si estuviesen conectados al mismo PCI, aunque se encuentren físicamente conectados a diferentes segmentos de una red de área local (LAN). Los administradores de red configuran las VLAN mediante software en lugar de hardware, lo que las hace extremadamente fuertes.

WAN

"Wide Area Network" o "Red de Área Amplia") es una red de computadoras que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física. Muchas WAN son construidas por organizaciones o empresas para su uso privado, otras son instaladas por los proveedores de internet (ISP) para proveer conexión a sus clientes.

Hoy en día, internet brinda conexiones de alta velocidad, de manera que un alto porcentaje de las redes WAN se basan en ese medio, reduciendo la necesidad de redes privadas WAN, mientras que las redes privadas virtuales que utilizan cifrado y otras técnicas para generar una red dedicada sobre comunicaciones en internet, aumentan continuamente.

Acrónimos

TI- Information technology, Tecnologías de la Información

KPI- Performance Indicators, Indicadores clave del desempeño

IVR- Interactive Voice Response, La respuesta de voz interactiva

CTI- Computer telephony integration, Integración de Telefonía Informática

SLA- Service Level Agreement, Acuerdo de Nivel de Servicio

VoIP- Voice over IP, Voz por protocolo de internet

Bibliografía

- [1] Micheli, J. Los Call Centers y los nuevos trabajos del siglo XXI. Confines Nº 005, Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM), Monterrey, México, 2007.
- [2] Paz parra-Piedrahita Echaverry, M. Desarrollo Historico del Marketing, Extracto, Universidad Libre-Cali, Chile, 2007
- [3] Hideki Erigh Hashimura, Fundamentos para establecer una estrategia CRM, 2011
- [4] Granados- Villate, Caracterización General del sector BPO, KPO e ITO, Colombia, 2013
- [5] Eddie Morris, Alfredo Ancajima. Servicios de contact center basados en offshore outsourcing,2009
- [6] Hernández, Comunicación de Datos, Tecnológico de la Laguna, España, 2010
- [7] Steve Taylor and Larry Hettick, www.networkworld.com, 2006
- [8] José Joskowicz, Comunicaciones Corporativas Unificadas, 2013
- [9] Sierra Manuel García, ¿Qué es un servidor y cuáles son los principales tipos de servidores?, DV00408A, Divulgación, Herramientas informáticas, Aprender a programar Versículo
- [10] Sierra Manuel Garcia, ¿Qué es un servidor y cuáles son los principales tipos de servidores?, DV00408A, Divulgación, Herramientas informáticas, Aprender a programar Versículo
- [11] Denwa, Citech, Comunicaciones Convergentes, 2010
- [12] Güimi, Redes de comunicaciones, 2004-2009
- [13] Gustavo Morales, Estudio, diseño e implementación de un Firewall, 2002
- [14] Federico Santa Maria ,Redes Privadas Virtuales (VPN), Universidad Técnica de España, 2014
- [15] Luís Arantón Areosa , Sobre virus y antivirus, 2008
- [16] Ernesto Ariganello, Redes CISCO, Guía de estudio CCNA 640-802, 2da Edición, Alfaomega, 2013
- Verónica Uribe-Echeverría, Atendiendo a los clientes de los clientes, la Industria del Call Center y sus condiciones laborales, Andros Impresores, 2010
- Hualde Alfaro, La economía de servicios y el empleo en los call/Contact Center, México, 2014
- Articulo PRO México, Inversión y Comercio, 2014
- Rafael Moreno, Introducción a las redes, Universidad Complutense de Madrid
- VLAN, Comunicación de datos II. Guía 4, Universidad Don Bosco
- Cheswick, W., and Bellovin, S. Firewalls and Internet Security: Repelling the Wily Hacker. Addison-Wesley, 2000
- Seguridad en los sistemas de información Libre Eleccion, FJRP, FMBR 2008 CCIA
- Ricardo D. Pantazis, Firewalls de Internet, UCEMA, 2003
- Redes Privadas Virtuales (VPN), Universidad Técnica Federico Santa Maria, 2014
- Angélica Mosquerra, Los antivirus y sus tendencias futuras, Universidad Tecnológica de Pererira, 2011
- Richard Segal, Jason Crawford. SpamGuru: An Enterprise Anti-Spam Filtering System, IBM Thomas J. Watson Research Center
- G.Corral, J.Abella. ADSL y MPLS. Editorial Ingeniería La Salle. Madrid, España, 1997.

- Barberá, José. MPLS: Una arquitectura de backbone para la Internet del siglo XXI. Revista: Actas del V Congreso de Usuarios de Internet. Mundo Internet 2000. Madrid, febrero 2000. Madrid, 1997.

Anexos

Anexo 1- Certificaciones IT

ITIL

ITIL es un conjunto de conceptos y prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general. ITIL da descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI, **ver Figura A1.1.**.

Figura A1.1. Proceso ITIL

En pocas palabras, ITIL asegura una gestión de servicios de IT eficiente, gracias al control y una posterior la mejora continua del servicio. Sirve para aquellos servicios que se encuentran en la fase operacional. Dicha fase forma parte de la etapa de mayor tiempo y costo para cualquier solución de IT y es, justamente, donde el negocio depende casi inminentemente de los servicios de TI.

Cabe destacar que ITIL no es una metodología de desarrollo de software: mientras el desarrollo de software (o cualquier tipo de soluciones de IT) hace foco en sistemas que aún no existen o están en desarrollo, ITIL ofrece métodos de control y mejoras para los servicios/productos que se encuentra en la etapa productiva.

El Ciclo de Vida del Servicio consta de cinco fases que se corresponden con los nuevos libros de ITIL®:

5. Estrategia del Servicio: propone tratar la gestión de servicios no sólo como una capacidad sino como un activo estratégico.
6. Diseño del Servicio: cubre los principios y métodos necesarios para transformar los objetivos estratégicos en portafolios de servicios y activos.
7. Transición del Servicio: cubre el proceso de transición para la implementación de nuevos servicios o su mejora.

8. Operación del Servicio: cubre las mejores prácticas para la gestión del día a día en la operación del servicio.
9. Mejora Continua del Servicio: proporciona una guía para la creación y mantenimiento del valor ofrecido a los clientes a traces de un diseño, transición y operación del servicio optimizado.

Como se dijo, ITIL es un conjunto de mejores prácticas, que sin embargo, no recomienda normas para su implementación, ni la secuencia de aplicación ni los procedimientos necesarios tales como políticas y procedimientos que se deben desarrollar para conseguir adoptar adecuadamente dicho marco. En resumen, podemos decir que ITIL nos plantea que debemos hacer pero no nos dice cómo debemos hacerlo. Ya que esto es así y que cada organización tiene sus propias necesidades y requisitos, los procesos o la fase del ciclo de vida del servicio por los que se comience a implementar ITIL serán exclusivos de las necesidades y los requisitos de cada empresa. Las organizaciones deberían comenzar por realizar una evaluación o un análisis de lagunas para identificar su estado actual y compararlo con el estado (final) que deseen alcanzar.

Para implementar ITIL es preciso idear y gestionar de forma estratégica una sólida estructura táctica. Los clientes quieren servicios que estén disponibles y funcionen cuando los necesiten. La gestión de incidencias, problemas, configuración, cambio, despliegues y conocimiento son necesarios para mejorar la disponibilidad del servicio, ya que todos son procesos tácticos y operativos con capacidad de proporcionar rápidamente un rendimiento de la inversión mediante la reducción de la frecuencia de las interrupciones y la disminución del tiempo de respuesta y resolución de problemas y de peticiones de servicios.

La gestión de incidencias y problemas son dos de los procesos de operaciones de servicio que pueden mejorar la disponibilidad del servicio mediante la reducción del número de incidencias y la disminución del tiempo de resolución de errores conocidos. El desarrollo de modelos de incidencias y problemas servirá para que los equipos de Service Desk y de segundo nivel de soporte mejoren su rendimiento y reduzcan el tiempo de inactividad de sus clientes.

Entre el 60 y 80% de fallas en la infraestructura de TI se derivan de los cambios introducidos por TI (muchos de los cuales no se han aprobado ni autorizado). Estas incidencias relacionadas con los cambios se deben normalmente a la falta de planificación, de pruebas o de comprensión del efecto que tiene el cambio en el servicio o la organización en su conjunto. La gestión del cambio evalúa los planes de los costos, los riesgos, la resolución, la implantación y la comunicación de cada cambio.

Implementación de ITIL en 10 pasos

Los proyectos de implementación de ITIL se caracterizan por un curso de acción típico, independientemente del tamaño de la compañía y su negocio básico. Esto hizo que fuera viable inventar un esquema de proyecto comprobado que puede servir como guía para una gran variedad de iniciativas de ITIL.

La mayoría de los proyectos ITIL contienen algunas tareas casi idénticas: por ejemplo, todas las partes involucradas deben familiarizarse con ITIL, y se deben definir prácticas (procesos) de trabajo en conformidad con ITIL.

Paso 1: Preparación del proyecto

Como preparación para cualquier proyecto ITIL o ISO 20000, es esencial que los actores clave dentro de la organización de TI conozcan los principios de ITIL, las maneras de aplicarlos, y los beneficios que ofrecen.

A largo plazo no será suficiente depender exclusivamente de los conocimientos de asesores externos. La aceptación de un proyecto ITIL dentro de una organización de TI aumentará drásticamente si sus colegas están en posición de comunicar de forma competente los beneficios de ITIL, y explicar los pasos necesarios para su implementación

Además de alinear la organización de TI con ITIL, el segundo objetivo importante del proyecto es asegurar que los procesos nuevos sean continuamente monitoreados y mejorados. Esto ofrece numerosos beneficios en sí, pero también es un requisito central para obtener una certificación ISO 20000.

En el caso ideal, en el negocio ya existirá una función de Gestión de Procesos o Gestión de Calidad que también puede manejar los procesos ITIL. Su responsabilidad será:

- asegurar que todos los procesos ITIL funcionen conjuntamente con fluidez;
- proveer herramientas adecuadas para manejar procesos;
- asegurar que se documenten adecuadamente los procesos ITIL;
- ayudar al personal de TI a mejorar sus procesos.

Si no existen estas condiciones, habrá que seleccionarse un miembro adecuado del personal de TI para esta función; a menudo, la persona a cargo de la implementación de ITIL se considera una buena opción, **ver Figura A1.2**.

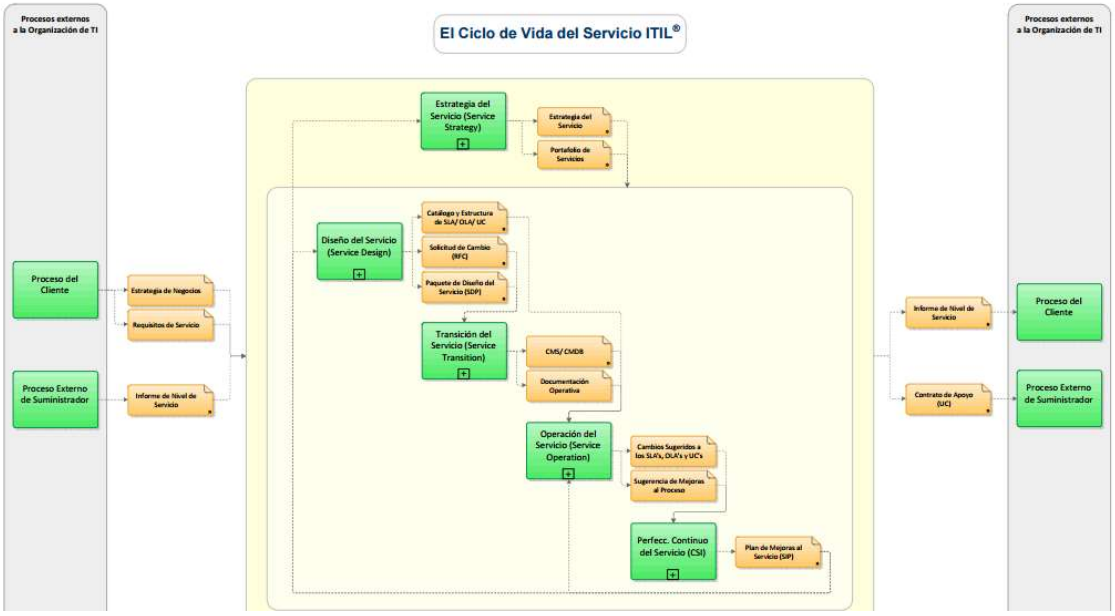


Figura A1.2. Ciclo de vida ITIL

Paso 2: Definición de la estructura de servicios

Cualquier iniciativa ITIL debe comenzar determinando los servicios. Después de todo, la razón principal para introducir ITIL es lograr un mayor enfoque en los servicios.

Servicios de negocios y servicios de soporte

La mejor manera de tener un cuadro claro de los mismos es desarrollar una estructura que incluya los servicios de negocios y los de soporte. Esto refleja uno de los principios más importantes de ITIL: Los servicios de negocios (ofrecidos a clientes) se construyen en una base de servicios de soporte (visible sólo internamente en la organización de TI).

Con frecuencia, hay confusión en las organizaciones de TI en cuanto a qué se considera un servicio de negocios. Los servicios de negocios se caracterizan por representar un valor directo para el cliente, por ejemplo, el hecho de proveer correo electrónico y acceso a Internet.

Los servicios de soporte, por el contrario, no son de valor directo para los clientes sino que sirven de base para sostener los servicios de negocios.

En otras palabras, lo que el cliente quiere es acceso confiable a Internet, no algún tipo específico de infraestructura de redes (de hecho, es irrelevante para el cliente que sea necesaria una infraestructura de redes para proveerle acceso a Internet).

Servicios de negocios y servicios de soporte

La mejor manera de tener un cuadro claro de los mismos es desarrollar una estructura que incluya los servicios de negocios y los de soporte. Esto refleja uno de los principios más importantes de ITIL: Los servicios de negocios (ofrecidos a clientes) se construyen en una base de servicios de soporte (visible sólo internamente en la organización de TI).

Con frecuencia, hay confusión en las organizaciones de TI en cuanto a qué se considera un servicio de negocios. Los servicios de negocios se caracterizan por representar un valor directo para el cliente, por ejemplo, el hecho de proveer correo electrónico y acceso a Internet.

Los servicios de soporte, por el contrario, no son de valor directo para los clientes sino que sirven de base para sostener los servicios de negocios.

En otras palabras, lo que el cliente quiere es acceso confiable a Internet, no algún tipo específico de infraestructura de redes (de hecho, es irrelevante para el cliente que sea necesaria una infraestructura de redes para proveerle acceso a Internet).

Creando una lista de servicios de negocios

Una buena manera de empezar es crear una lista de los servicios de negocios existentes, usando, si fuera posible, acuerdos e información previamente establecidos. Si no está disponible la información relacionada con los servicios, se debe crear una lista básica, que incluya al menos descripciones breves de servicios y clientes que los utilizan.

Determinando los servicios de soporte

Tan pronto esté claro cuáles son los servicios de negocios que se proveen a los clientes, es posible identificar los servicios de soporte necesarios.

Lo principal al definir los servicios de apoyo es asignar responsabilidades para el suministro de tales servicios. Se espera que los Propietarios de Servicios responsables se aseguren de que sus servicios cumplan con las metas de los niveles de servicio, según lo acordado.

Los servicios de soporte, con frecuencia, están relacionados estrechamente con ciertas partes de la infraestructura de TI, por ejemplo, con los sistemas principales de aplicaciones o componentes de la infraestructura: Un ejemplo típico sería "Proveyendo un ambiente de SAP".

Definiendo la estructura de servicios

Al haber identificado los servicios de negocios y soporte, la tarea que falta es crear una estructura de servicios determinando la interrelación entre ambos.

En ella se puede ver que los servicios de soporte están a menudo en escalas; por ejemplo, un servicio que es responsable de manejar cierto sistema de aplicaciones puede que dependa de otro servicio de soporte para proveer un sistema operativo básico.

Esta estructura servirá luego como una aportación valiosa para diseñar el Catálogo de Servicios.

Paso 3: Selección de roles ITIL y propietarios de roles

Antes de comenzar "realmente" el proyecto, es importante designar a los individuos que tendrán a su cargo los nuevos procesos ITIL - se debe determinar qué roles ITIL son necesarios y de quién van a ser.

El manejo de esta cuestión en la etapa inicial es de vital importancia para el éxito del proyecto. La persona que luego será responsable de determinado proceso también debe participar en su diseño. Esto asegurará que la mayor experiencia posible fluya en la definición del proceso, y que los propietarios de roles se identifiquen muy de cerca con cualquier cambio a las prácticas de trabajo existentes.

La identificación de los roles necesarios para ITIL se deriva directamente de las disciplinas ITIL que se introducirán. Por ejemplo, si Gestión de Problemas está por implementarse, se debe nombrar un Gestor de Problemas.

Dentro de las empresas más grandes y donde se considere necesario, la determinación de los roles no es tan sencilla; puede ser necesaria una subdivisión de tareas, resultando en una subdivisión de roles. Si el Gestor de Problemas, por ejemplo, no puede manejar todas la tareas en Gestión de Problemas, se puede considerar el crear roles tales como "Analista de Problemas", "Gestor de Errores", etc.

En esta etapa del proyecto no es absolutamente necesario definir los roles en detalle, por ejemplo, en documentos extensos. Esto se hará implícitamente durante las fases subsiguientes del proyecto. Cuando se definan los procesos en detalle, las actividades individuales aparecerán junto con los

roles responsables de su ejecución. La mayoría de los sistemas de Gestión de Procesos generan los documentos, en los que se resumen las responsabilidades de cada rol en los procesos.

Prerequisitos

Identificar procesos/ disciplinas ITIL por introducir o revisar durante el proyecto (al menos una estimación preliminar, ya que evaluaciones subsiguientes pueden llevar a mayores y/o diferentes perspectivas sobre cómo definir el alcance del proyecto)

Paso 4: Análisis de procesos existentes (Evaluación de ITIL)

Un análisis de la situación actual debe preceder cualquier proceso de reorganización; esto permite decidir qué procesos actuales se pueden dejar sin cambios y dónde hay que actuar urgentemente.

A menudo, el análisis de procesos existentes conlleva documentar laboriosamente estos procesos con mucho detalle.

Según nuestra experiencia, el resultado final, general-mente, no compensa el esfuerzo ya que analizar los procesos existentes se orienta demasiado hacia el pasado. Una fijación en las prácticas laborales existentes, con frecuencias anticuadas, tiende a obstruir la visión cuando se quiere rediseñar procesos más simples y efectivos.

En vez de ello, recomendamos evaluar los procesos existentes usando una serie de criterios objetivos, para identificar los puntos débiles y oportunidades sin un esfuerzo laborioso de documentación de procesos. La Autoevaluación ITIL es ideal para esta tarea.

Esta forma de evaluación también es recomendable si se va a presentar ITIL por primera vez. Como ITIL surge de la experiencia práctica, seguramente habrá áreas donde ya se aplican los principios de ITIL, siendo un indicador de que algunos de los procesos existentes deben continuar en el futuro.

Para las entrevistas de evaluación se debe escoger a miembros de la Gestión de TI y a empleados especializados. El entrevistador orienta a los participantes sobre el cuestionario, ayudando con explicaciones sobre el trasfondo de preguntas específicas cuando sea necesario.

La evaluación subsiguiente destaca:

- Niveles de madurez logrados en las disciplinas individuales de ITIL
- Desviaciones en el juicio de los participantes en entrevistas individuales sobre la calidad de distintos procesos
- Identificación tanto de los puntos débiles en los procesos existentes y sus causas adyacentes, como de las oportunidades

Prerequisitos

- Catálogo de Autoevaluación ITIL v2 (disponible libre de cargos; busca en la web para 'Self Assessment (ITIL V2)')

Resultados / Entregables

- Clasificación de la organización de TI dentro de las disciplinas individuales de ITIL
- Lista de puntos débiles y oportunidades con respecto a las recomendaciones de ITIL

Factores de éxito

- El análisis debe cubrir todas las áreas principales de la organización de TI; por eso es necesario que la mayoría del personal de la Gestión de TI, junto a una selección representativa de empleados especializados, participen en la encuesta.
- El entrevistador ya debe estar familiarizado con los principios de ITIL, para poder contestar preguntas de los participantes en las entrevistas.

Paso 5: Definición de la estructura de procesos

Al concluir el análisis de la situación inicial, se puede decidir con más detalles cuál será el enfoque del proyecto ITIL. En la práctica, es determinar qué procesos ITIL se deben introducir; esto resultará en un desglose estructurado de procesos.

Descripción

Si el proyecto tiene como objetivo mejorar el apoyo al usuario, el proceso de "Gestión de Incidentes" se establece o se mejora. Debido a su enlace con Gestión de Incidentes, los procesos de "Gestión de Problemas" y "Activos de Servicio y Gestión de la Configuración" también deben ser incluidos en el proyecto.

La meta de este paso del proyecto es, primordialmente, escoger los proceso y subprocesos ITIL. La estructura por hacer no contiene descripciones detalladas de los procesos, éstos se desarrollan en una etapa posterior.

El hecho de que el ITIL Process Map contenga una estructura genérica, ayuda en la tarea actual de definir la estructura de procesos. En la mayoría de los casos se puede usar el mapa, solamente, con cambios menores.

Prerequisitos

Resultados de la evaluación de procesos ITIL existentes

Objetivos del proyecto (¿Cuál es la motivación para introducir las mejores prácticas de ITIL?)

Resultados / Entregables

Desglose estructurado de los procesos ITIL por introducir

Factores de éxito

La definición de la estructura de procesos no debe tratar de anticipar los pasos subsiguientes del proyecto; la meta de este paso es identificar los procesos y subprocesos por introducir, sin especificar los procesos con mucho detalle.

Paso 6: Definición de interfaces de procesos ITIL

El próximo paso determina qué entradas (inputs) debe recibir cada proceso de los otros, y qué salidas (outputs) debe producir cada uno para que los subsiguientes puedan funcionar.

Descripción

A menudo, la importancia de las interfaces de procesos para el diseño de un trabajo óptimo se hace patente durante el análisis de los procesos existentes:

Los puntos débiles en los procesos aparecen, con frecuencia, en las interfaces, allí donde termina un proceso y empieza otro. En muchos casos, se producen interrupciones en el flujo de información o en los medios, lo que no permite intercambiar la información deseada.

La definición de las interfaces de procesos es un paso separado en el proyecto, antes de manejar los entresijos de los proceso en detalle. Obviamente, antes de poder definir las actividades detalladas, debe estar claro qué inputs puede esperar un proceso de los anteriores, y qué rendimiento debe producir.

La estructura de procesos previamente desarrollada se utiliza como base para determinar las interfaces de procesos necesarias.

El ITIL Process Map aplica un enfoque riguroso a la definición de interfaces: los objetos de información se pueden seleccionar de un glosario ITIL central, para definir las inputs y los outputs de manera precisa. Cada objeto de información contiene una breve definición para evitar ambigüedades sobre los resultados de los procesos esperados.

Uno de los retos durante la definición de las interfaces es el hecho de que, por lo general, no todos los procesos ITIL se implementan a la vez, lo que a menudo conlleva el que falten algunos de los inputs necesarios para el proceso.

Es posible, por ejemplo, que no haya un proceso de Gestión de la Seguridad de TI, aunque el Service Desk requiera inputs de Gestión de la Seguridad, como Alertas de Seguridad.

Un modelo de procesos como el Mapa de Procesos ITIL ayuda a resolver este problema:

Ofrece un marco estructurado de procesos que permite la definición de enlaces completos, aunque al principio sólo una subserie de procesos ITIL esté definida en detalle.

De esta manera, otros procesos ITIL adicionales se pueden añadir posteriormente al modelo del proceso, según sea necesario.

Prerequisitos

Estructura de los procesos ITIL por introducir

Objetos de información ITIL (términos del glosario ITIL) como inputs y outputs de procesos

Resultados / Entregables

Interfaces de los procesos ITIL por introducir:

- unos con otros
- con otros procesos ITIL
- con clientes y suministradores

Factores de éxito

Los procesos nuevos no deben representar soluciones aisladas y deben considerarse las interfaces a los otros procesos en la organización de TI.

La documentación de las interfaces debe estar claramente estructurada, mostrando todos los detalles cuando sea necesario. Esto requiere diagramas de visiones generales, que presentan el cuadro completo, y diagramas separados, con detalles, de las interfaces para cada proceso.

Paso 7: Estableciendo controles de procesos

Una vez que están claras la estructura de procesos y sus interfaces, se debe definir un enfoque para asegurar que estos procesos fluyan según las expectativas ("Controlling de Procesos").

Descripción

Una estrategia coherente para el controlling de los procesos no solamente ayuda a evaluar si se logran los objetivos que se buscan con la implementación de ITIL; también tiene unos beneficios a largo plazo, ya que presenta los datos necesarios para un proceso de mejoramiento continuo.

¿Cómo decidir si un proceso "fluye bien" o no? Con este propósito se deben determinar unos criterios objetivos (métricas de calidad, también conocidas como Indicadores Claves de Rendimiento o KPI, en inglés).

Cuando estén claros los niveles de calidad que debe lograr un proceso, se pueden diseñar con confianza sus detalles, teniendo en cuenta esas metas.

Determinar los propietarios de procesos

La gestión exitosa de un proceso depende de los propietarios de procesos que se identifiquen de cerca con su tarea, y que tengan suficiente autorización y los medios necesarios.

Por eso, es importante tener a los propietarios de procesos (responsables por el flujo de los procesos luego de su implementación) como participantes activos en el proyecto de implementación.

En la mayoría de los casos, seleccionar los propietarios de procesos es sencillo (por ejemplo, el Gestor de Problemas es el propietario del proceso de Gestión de Problemas).

Definir métricas y procedimientos de medición de TI

Los propietarios de procesos usan criterios objetivos de calidad para evaluar si sus procesos fluyen "bien". Esto los coloca en posición para decidir cuándo es necesario mejorar los procesos.

El primer paso al seleccionar KPIs adecuados siempre debe ser decidir los objetivos generales del proceso (por ejemplo, la tasa de resoluciones de primera instancia en el Service Desk). Con estos objetivos en mente, será posible seleccionar KPI's que sean adecuados para medir la ejecución exitosa de un proceso.

El propietario de proceso también utiliza métricas cuantitativas para enfocar recursos dentro de un proceso (por ejemplo, el número de incidentes recibidos por el Service Desk en el transcurso del tiempo).

Qué KPIs se seleccionarán eventualmente depende de la disponibilidad de posibilidades para medirlos. En el caso ideal, los KPIs pueden ser computados automáticamente, por ejemplo, en un sistema de Service Desk. Los procedimientos de métricas definidos aquí son, por ende, requisitos para los sistemas a implementarse.

El Controlling de Procesos no significa tener un arsenal de KPIs lo más extenso posible. La práctica ha puesto de manifiesto que una estructura de medidas demasiado compleja implica un esfuerzo desproporcionado, tiene poca aceptación, y en breve ya no se aplica.

En vez de ello, se deben definir pocas mediciones significativas, para que la función de medir e informar sobre los KPIs se pueda llevar a cabo en un tiempo y con un esfuerzo que puedan justificarse.

Fijar metas KPI

Los objetivos de valores de los KPI's definen el "éxito" de manera objetiva, y fijan metas para el propietario de proceso. Hay que tener en cuenta, sin embargo, que los objetivos de valores (como tasas de resoluciones por primera vez) no se transfieren fácilmente de negocio a negocio sin ciertas precauciones.

Inicialmente, se recomienda no definir metas fijas KPI's, sino meramente seleccionar KPI's adecuados y comenzar a medir. Cuando haya un número estadísticamente significativo de medidas, y después de un cierto tiempo, habrá una base más sólida para fijar metas.

Definir los procedimientos de informes

Informar sobre la calidad de los procesos es el elemento final dentro del Controlling de Procesos. Los procedimientos para los informes se deben definir especificando qué KPIs se reportarán, de qué manera, y quién recibirá los informes.

Prerequisitos

- La estructura de los procesos ITIL por introducir
- Objetivos de los procesos ITIL

Resultados / Entregables

- Asignación de propietarios de procesos
- Métricas de CSI (KPIs)
- Procedimientos de medición para KPIs
- Especificación de los procedimientos de informes

Factores de éxito

- Solamente se deben usar KPIs que realmente se puedan medir
- La Gestión de TI debe enfatizar que el uso de KPIs tiene como propósito mejorar los procesos, pero no penalizar empleados. De lo contrario, puede darse la situación de que el personal de TI altere las estadísticas a su favor, lo que va en contra de los intereses de toda la organización de TI.
- Las metas para los KPIs (especialmente en la fase inicial, tras presentar los nuevos procesos) se deben revisar regularmente; no siempre es necesario tratar de alcanzar la máxima

puntuación; por ejemplo, en ciertas circunstancias, es aceptable tener una tasa de resolución más baja en el Service Desk si muchas de las consultas requieren conocimientos de un especialista.

Paso 8: Diseñando los procesos en detalle

Determinar las secuencias de actividades individuales dentro de cada proceso es relativamente laborioso. Por eso es muy importante concentrarse en las áreas que realmente cuentan.

Descripción

Las actividades detalladas dentro de cada proceso se deben discutir con todas las partes relevantes, para poder incluir en su diseño toda la experiencia y los conocimientos posibles. El propietario de proceso es responsable por esta tarea.

Como resultado, se llega a un consenso, el cual se documenta en un "flujograma" detallado del proceso.

Se puede añadir información adicional (como documentos relacionados) que describa los procedimientos y outputs en detalle, para facilitar la ejecución del proceso. Por ejemplo, puede haber unas páginas extra que describan qué tipo de información se recopilará durante el registro inicial de un incidente.

Prerequisitos

- Estructura de procesos de Gestión de Servicios de TI por introducir
- Perspectivas generales de los procesos (desglose de procesos)
- Interfaces de los procesos ITIL por introducir
- Métricas de CSI (KPIs) de los procesos por introducir

Resultados / Entregables

- Descripciones detalladas de los procesos (secuencias de actividades)
- Guías/ listas de control
- Definiciones de outputs de procesos

Factores de éxito

- Preparase bien es esencial en este punto, para evitar el riesgo de producir un gran número de documentos, demasiado extensos y que no guarden relación.
- Por eso, nuestro método de "Implementación de ITIL" da una gran importancia al hecho de establecer un marco de estructuras e interfaces de procesos durante los primeros pasos del proyecto. Respetando la definición de las interfaces de proyectos, ya queda establecida la información necesaria para el proceso, y qué resultados debe producir en procesos sucesivos.
- Con esta información claramente especificada, es mucho más fácil definir el flujo de un proceso de manera sencilla y directa.

Paso 9: Selección e implementación de sistemas de aplicaciones

Si se necesitan sistemas de aplicaciones nuevos o cambiados para apoyar los procesos, deben primero procurarse y/o desarrollarse e implementarse.

Definir los requisitos de sistemas

Descripción

Los requisitos funcionales de los sistemas de aplicaciones se derivan mayormente de las descripciones detalladas de los procesos; éstos ilustran qué actividades apoyará el sistema de aplicación.

Se pueden añadir más requisitos (ejemplo: "Crear un Incidente nuevo debe ser posible desde el libro de direcciones de Outlook").

Las definiciones de las outputs de procesos describen qué datos son procesados dentro del sistema. Por ejemplo, el proceso "Registro y Categorización de Incidentes" genera un "Registro de Incidente". El sistema debe poder manejar una estructura de estos datos, y ofrecer interfaces adecuadas para que los usuarios los puedan ver y editar.

Finalmente, se deben identificar todos los requisitos no funcionales para que resulte, como un todo, la siguiente estructura para el documento de requisitos:

- Requisitos funcionales
  - Referencia a modelos detallados de procesos
  - Requisitos adicionales relacionados con la funcionalidad
  - Definiciones de las outputs de procesos (estructura de datos)
  - Requisitos de informes
- Requisitos no funcionales
  - Requisitos relacionados con capacidades y cantidades
  - Ejecución y rendimiento
  - Escalabilidad/ expansión
  - Disponibilidad
- Requisitos desde un punto de vista operacional

- Requisitos desde un punto de vista de Seguridad de TI
- Interfaces con otros sistemas
- Anejo
  - Modelos de procesos
  - Datos que se importarán de sistemas previos

Una vez que estén completos los requisitos, se extrae una lista detallada y con prioridades del documento de requisitos. Esta lista se utiliza como una matriz para evaluar a los proveedores. Los requisitos se deben categorizar como en el siguiente ejemplo:

- Criterios decisivos (Prio 1)
- Requisitos importantes (Prio 2)
- Requisitos deseables (Prio 3)

Objetivo de este paso del proyecto

- Definir los requisitos para sistemas de aplicaciones nuevos o cambiados

Prerequisitos

- Descripciones detalladas de procesos ITIL expresados en forma de secuencias de actividades
- Guías/ listas de control
- Definiciones de outputs de procesos

Resultados / Entregables

- Documento de requisitos para aplicaciones que se cambiarán o se obtendrán
- Lista de prioridades de requisitos

Factores de éxito

Es importante no limitarse a los aspectos funcionales cuando se especifiquen los requisitos del sistema. Los aspectos operacionales son de igual importancia, como lo son las posibilidades de expandir el sistema; especialmente si luego se implementan otros procesos de ITIL.

Perspectivas relevantes del Mapa de Procesos ITIL

Las descripciones detalladas (secuencias de actividades) del ITIL Process Map son una parte importante de los requisitos del sistema.

Además, las listas de control/ plantillas de documentos apoyan la definición de las outputs de procesos. Los atributos usualmente asignados a un Registro de Incidente, por ejemplo, se encuentran en la lista de control de "Registro de Incidente".

Seleccionar sistema(s) de apoyo para los procesos por hacer

Descripción

Una evaluación sistemática de los sistemas adecuados se consigue basándose en la lista de requisitos.

Se ha comprobado que un enfoque de tres partes es lo más eficiente para este propósito:

Primero se puede hacer un acercamiento por escrito a una gran cantidad de proveedores para encontrar los que puedan cumplir los requisitos más importantes.

Se prevé que con este paso se obtenga una lista corta de proveedores, con el fin de solicitarles que presenten una oferta sólida que también incluya información sobre cuotas para licencias y costos de implementación.

La decisión final se toma después de haber visitado a los clientes de referencia, y posiblemente haber realizado una instalación de prueba del proveedor de sistemas considerado.

Objetivo de este paso del proyecto

Seleccionar sistema(s) y proveedor(es) adecuados para el sistema de aplicaciones que vaya a obtenerse

Prerequisitos

Documento de requisitos de las aplicaciones que se cambien u obtengan

Lista de prioridades de requisitos

Resultados / Entregables

Evaluar los sistemas y los proveedores

Paso 10: Implementación de procesos y adiestramiento

Si los participantes se enteran de los nuevos procesos solamente en esta etapa, es inevitable que haya una falta de aceptación. Por eso, es fundamental que la mayor cantidad de empleados posible participe en el diseño de procesos durante las etapas tempranas del proyecto.

Descripción

Ante todo, los participantes se deben familiarizar con los nuevos procesos. Esta guía de implementación asegura en varios puntos que estos participantes estén involucrados en el diseño del proceso desde fases tempranas, de modo que, en la mayoría de los casos, no sea necesario explicar cómo cambiarán los procesos.

Puede haber un adiestramiento adicional en diferentes niveles:

- Un trasfondo de conocimientos de ITIL es decisivo para el éxito de los nuevos procesos, y debe ser provisto a todas las partes involucradas; el adiestramiento básico de ITIL se puede llevar a cabo al comienzo del proyecto para personal clave, para que pueda comunicar los principios de ITIL a los otros participantes del proyecto.
- Miembros específicos del personal de TI necesitarán un adiestramiento más intensivo, dependiendo de sus roles ITIL
- Tras la implementación de un sistema nuevo o cambiado, pueden ser necesarios adiestramientos sobre su operación
- Como suplemento, se pueden considerar adiestramientos que contribuyan a mejorar la imagen pública de la Organización de TI ("¿Cómo actúo con clientes críticos?")
- Al final, se informa a los clientes si, por ejemplo, se estableció un Service Desk nuevo y, como resultado, cambió el procedimiento para las solicitudes de servicio.

Prerequisitos

- Perspectivas generales de los procesos (desglose de los procesos)
- Interfaces de los procesos ITIL por introducir
- detalladas de los procesos ITIL expresadas como secuencias de actividades
- Guías/ listas de control
- Métricas de CSI (KPIs) para los procesos por introducir
- Definiciones de las inputs y outputs de procesos

Resultados / Entregables

- Personal de TI informado
- Clientes informados

Factores de éxito

Como ya se dijo, se debe invitar a todas las partes invo-lucradas para que cooperen y presenten sus experiencias durante el transcurso del proyecto.

ISO 27000

SO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

El ISO-27000 se basa en la segunda parte del estándar británico BS7799 (BS7799:2). Está compuesta a grandes rasgos por:

- ISMS(Information Security Management System).
- Valoración de Riesgo.
- Controles.
- A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares.

La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). la mayoría de estas normas se encuentran en preparación e incluyen:

- ISO/IEC 27000 - es un vocabulario estándar para el SGSI. Introducción y base para el resto. Tercera versión: enero de 2014.
- ISO/IEC 27001 - es la certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estándar internacional en octubre de 2005. Revisada en setiembre de 2013.
- ISO/IEC 27002 - Information technology - Security techniques - Code of practice for information security management. Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. Es código de buenas prácticas para la gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007. Última versión: 27002:2013, de setiembre de 2013.
- ISO/IEC 27003 - son directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001. Publicada el 1 de febrero de 2010. No es certificable.
- ISO/IEC 27004 - son métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Publicada el 7 de diciembre de 2009, no se encuentra traducida al español actualmente.
- ISO/IEC 27005 - trata la gestión de riesgos en seguridad de la información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001. Es la más relacionada a la actual British Standard BS 7799 parte 3. Publicada en junio de 2008. Revisada en junio de 2011.
- ISO/IEC 27006 - Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma especifica requisitos específicos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación. Publicada en 2007 y revisada en diciembre de 2011 y setiembre de 2015.

- ISO/IEC 27007 - es una guía para auditar al SGSI. Publicada en noviembre de 2011.
- ISO/IEC 27016 - es una norma que se concentra en un análisis financiero y económico de equipos y procedimientos de la seguridad de la información. Publicada en febrero de 2014.
- ISO/IEC 27017 - es una guía de seguridad para Cloud Computing. Publicada en diciembre de 2015.
- ISO/IEC 27035:2011 - Seguridad de la información – Técnicas de Seguridad – Gestión de Incidentes de Seguridad. Este standard hace foco en las actividades de: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades. Publicada en agosto de 2011. (1)
- ISO/IEC 27799:2008 - es una guía para implementar ISO/IEC 27002 en la industria de la salud.

ISO 27000 incluye los siguientes aspectos:

Confidencialidad

Servicio de seguridad o condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados. También puede verse como la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él.

La confidencialidad es importante porque la consecuencia del descubrimiento no autorizado puede ser desastrosa. Los servicios de confidencialidad proveen protección de los recursos y de la información en términos del almacenamiento y de la información, para asegurarse que nadie pueda leer, copiar, descubrir o modificar la información sin autorización. Así como interceptar las comunicaciones o los mensajes entre entidades.

Mecanismos para salvaguardar la confidencialidad de los datos:

- El uso de técnicas de control de acceso a los sistemas.
- El cifrado de la información confidencial o de las comunicaciones.

Autenticación

Es el servicio que trata de asegurar que una comunicación sea auténtica, es decir, verificar que el origen de los datos es el correcto, quién los envió y cuándo fueron enviados y recibidos también sean correctos.

Algunos métodos de autenticación son:

- Biomédicas, por huellas dactilares, retina del ojo, etc.
- Tarjetas inteligentes que guardan información de los certificados de un usuario
- Métodos clásicos basados en contraseña:
- Comprobación local o método tradicional en la propia máquina
- Comprobación en red o método distribuido, más utilizado actualmente

Integridad

Servicio de seguridad que garantiza que la información sea modificada, incluyendo su creación y borrado, sólo por el personal autorizado.

El sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga. El problema de la integridad no sólo se refiere a modificaciones intencionadas, sino también a cambios accidentales.

No repudio

El no repudio sirve a los emisores o a los receptores para negar un mensaje transmitido. Por lo que cuando un mensaje es enviado, el receptor puede probar que el mensaje fue enviado por el presunto emisor. De manera similar, cuando un mensaje es recibido, el remitente puede probar que el mensaje fue recibido por el presunto receptor.

Control de Acceso

Un control de acceso se ejecuta con el fin de que un usuario sea identificado y autenticado de manera exitosa para que entonces le sea permitido el acceso.

Los componentes básicos de un mecanismo de control de acceso son las entidades de red, los recursos de la red y los derechos de acceso. Estos últimos describen los privilegios de la entidad o los permisos con base en qué condiciones las entidades pueden tener acceso a un recurso de la red y cómo estas entidades son permitidas para tener acceso a un recurso de la red.

El control de acceso puede ejecutarse de acuerdo con los niveles de seguridad y puede ejecutarse mediante la administración de la red o por una entidad individual de acuerdo con las políticas de control de acceso.

Disponibilidad

En un entorno donde las comunicaciones juegan un papel importante es necesario asegurar que la red esté siempre disponible.

La disponibilidad es un servicio que garantiza que los usuarios autorizados tengan acceso a la información y a otros activos de información asociados en el lugar, momento y forma en que es requerido. Un sistema seguro debe mantener la información disponible para los usuarios. El sistema, tanto hardware como software, debe mantenerse funcionando eficientemente y ser capaz de recuperarse rápidamente en caso de fallo.

Amenazas

Una amenaza se representa a través de una persona, una circunstancia o evento, un fenómeno o una idea maliciosa, las cuales pueden provocar daño en los sistemas de información, produciendo pérdidas materiales, financieras o de otro tipo. Las amenazas son múltiples desde una

inundación, un fallo eléctrico o una organización criminal o terrorista. Así, una amenaza es todo aquello que intenta o pretende destruir.

ISO 9000

ISO 9000 es un conjunto de normas sobre calidad y gestión de calidad, establecidas por la Organización Internacional de Normalización (ISO). Se pueden aplicar en cualquier tipo de organización o actividad orientada a la producción de bienes o servicios. Las normas recogen tanto el contenido mínimo como las guías y herramientas específicas de implantación como los métodos de auditoría.

ISO 9000 especifica la manera en que una organización opera sus estándares de calidad, tiempos de entrega y niveles de servicio. Existen más de 20 elementos en los estándares de esta ISO que se relacionan con la manera en que los sistemas operan.

Ventajas

Su implementación aunque supone un duro trabajo, ofrece numerosas ventajas para las empresas, como pueden ser:

- Estandarizar las actividades del personal que trabaja dentro de la organización por medio de la documentación.
- Incrementar la satisfacción del cliente al asegurar la calidad de productos y servicios de manera consistente, dada la estandarización de los procedimientos y actividades.
- Medir y monitorear el desempeño de los procesos.
- Incrementar la eficacia y/o eficiencia de la organización en el logro de sus objetivos.
- Mejorar continuamente en los procesos, productos, eficacia, entre otros.
- Reducir las incidencias negativas de producción o prestación de servicios.
- Mantener la calidad.

Desventajas

- Los esfuerzos y costos para preparar la documentación e implantación de los sistemas.

Anexo 2- Modelo OSI

Basado en el principio enunciado por Julio Cesar (Dividir y Reinar), el modelo es iniciado por la IBM para redes de computadoras. En IBM se denomina SNA (Systems Network Architectura) y es original de 1974, con versión definitiva en 1985. Este modelo es perfeccionado por la Organización Internacional de Normalizaciones ISO en el estándar ISO 3309. El modelo ISO se inicia en 1977 y se adopta en 1984. Se denomina Modelo de Interconexión de Sistemas Abiertos OSI con 7 capas.

La finalidad del modelo ISO es permitir la cooperación entre sistemas abiertos. Un sistema real abierto es aquel conjunto de ordenadores, material lógico, periféricos, terminales, operadores humanos, etc, que forma un todo autónomo capaz de procesar y/o transferir información. Cada sistema abierto se considera constituido por un conjunto de 7 capas o estratos representados en forma vertical.

El modelo prevé una comunicación vertical entre capas (capa N+1 con N y N con N-1) denominado SERVICIO y una comunicación horizontal (capa N con N) entre distintos sistemas abiertos denominado PROTOCOLO (protocolo entre entidades pares o iguales peer-to-peer). Cada capa N ofrece un servicio a la capa inmediatamente superior N+1 y requiere los servicios de la inferior N-1. Para la comunicación se define los puntos de conexión SAP (Service Access Point) que funcionan como direcciones de la capa superior; una entidad puede tener activas varias direcciones SAP simultáneamente, ver **Figura A2.1**.

Las distintas capas verticales requieren y ofrecen un servicio. **De la Figura A2.1** se puede concluir que:

-Cada capa genérica N recibe una unidad de servicio SDU desde la capa N+1;

-Agrega una información adicional denominado protocolo de control PCI y

-Forma la unidad de datos PDU que corresponde al SDU de la capa N-1.

El término PDU (Protocol Data Unit) es usado por ISO para todas las capas e incluye a SDU y el encabezado PCI. Para cada capa se antepone la inicial a la sigla que la identifica y el nombre más usual:

Capa 1:PhPDU (trama y envoltura).

Capa 2: DPDU (tramas en LAN y FR, celda en ATM y MAN y paquete en X.25).

Capa 3: NPDU (paquete en X.25 y datagrama en IP).

Capa 4: TPDU (segmento en TCP y mensaje en SMTP y SS7).

Capas 7,6, 5: APDU, PPDU, SPDU: para las capas respectivamente.

La dirección que identifica la capa se indica como SAP; de esta forma da lugar a las direcciones NSAP, DSAP y PhSAP. La comunicación entre capas determina 4 servicios primitivos:

-Pedido desde N a N-1 (requerimiento de servicio);

-Indicación desde N-1 a N (notificación de requerimiento);

-Respuesta desde N a N-1 (reconocimiento de indicación);

-Confirmación desde N-1 a N (pedido completado).

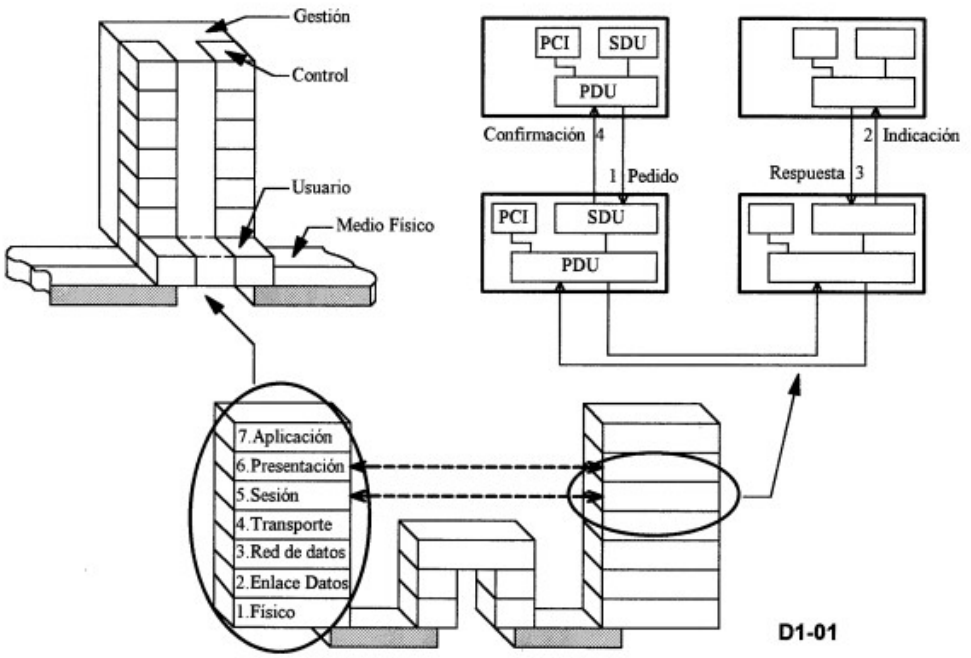


Figura A2.1. Modelo de referencia OSI

Capas del modelo OSI

De acuerdo con la **Figura A2.1** se dispone de un modelo de 7 capas en general. Las capas superiores (5-6-7) corresponden a funciones de elaboración de la información; las intermedias (3-4) corresponden a funciones de comunicación y las inferiores (1-2) a control de la conexión.

Los elementos que determina el protocolo de capa 5-6-7 son: -la sintaxis: formato de datos (relación entre campos de datos), -la semántica: control de información (significado de los datos), -la temporización: adaptación de velocidad y secuencia. Al conjunto de capas superiores pertenecen el sistema de operación del host (MS-DOS, UNIX, Windows NT), el sistema de operación de red LAN (NetWare, IBM OS/2 LAN Server), los programas de aplicación de usuario (Lotus Notes, cc: Mail, MS Mail, Schedule, etc.) y los programas utilitarios de LAN (Transferencia de file, emulación de terminal, etc). Los programas involucrados en las capas 3 y 4 se basan en alguna de las estructuras de facto (Microsoft/IBM Net, Novell SPX/IPX) o de jure (TCP/IP e ISO). En las capas 2 y 1 se identifica la conexión al medio físico. Pueden ser provistas mediante conexiones punto-a-punto o redes de datos (LAN, MAN y WAN). De esta forma se tiene en cuenta el acceso a la red LAN o MAN. También se involucra la operación de internetwork consistente en Switch-Router que permiten la interconexión de redes iguales o distintas.

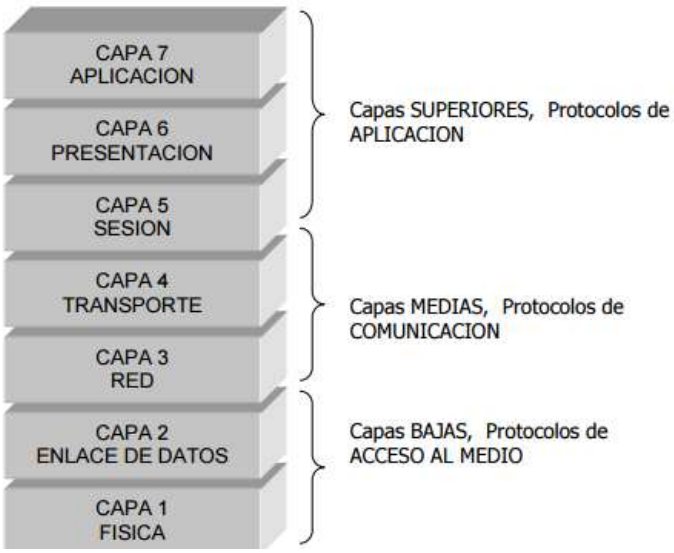


Figura A2.2. Capas del modelo OSI

El diseño se simplifica si separamos los aspectos de comunicación de los de aplicación.

Una red en general consiste de dos componentes:

• La línea de transmisión (circuitos, canales, etc).

• Los elementos de conmutación, (Hub, Switch, Router, etc).

Es importante destacar que OSI es un Modelo de Referencia, y tiene un alto valor académico, sin embargo no existe como una arquitectura de red.

Usando un lenguaje más llano, el Modelo de Referencia define qué es lo que debe hacer cadacapa, pero no siempre especifica los protocolos y servicios exactos que deben llevar a cabo dichas tareas, es decir cómo deben hacerse. La ISO ha elaborado estándares para algunos protocolos, pero los mismos no han tenido gran trascendencia en el mercado.

En el otro extremo se encuentra el Modelo TCP/IP, que a diferencia de OSI es más bien "escaso" en cuanto a las definiciones de las capas, pero cuenta con una gran cantidad de protocolos muy desarrollados, plenamente operacionales y de gran uso en la industria actual, a tal punto que es el modelo que se utiliza en Internet.

Resumiendo, podemos decir que la tendencia actual es la de utilizar el Modelo de Referencia OSI como estructura conceptual y usarlo como una "regla" para comparar otros modelos o simples pilas de protocolos.

A diferencia del sencillo modelo presentado anteriormente a modo de ejemplo, OSI cuenta con 7 capas:

Para facilitar el análisis es preferente considerar a las 7 capas de OSI agrupadas en "Capas Superiores", "Capas Medias" y "Capas Inferiores" como se muestra en la figura 7.

Antes de comentar las funciones encomendadas a cada capa por la gente de la ISO, comparemos el Modelo de referencia OSI con el modelo TCP/IP.

El Modelo TCP/IP consta de menos capas que el OSI, sólo tiene 4. Esto no significa que TCP/IP tenga que realizar menos funciones sino que varias de estas funciones no se encuentran discriminadas en capas distintas. La equivalencia entre ambos modelos se muestra en la siguiente figura **Ilustración A1.3**:

Como se puede observar las diferencias fundamentales se producen en las capas superiores, y de acceso a la red o capa de acceso al medio ya que en el modelo TCP/IP las 3 capas superiores de OSI se encuentran englobadas en una única capa, y sobre las 2 capas inferiores, TCP/IP, no revela detalles, dejando a los protocolos ya estandarizados la función de presentar el acceso al medio. Como mencionaba anteriormente esto no significa que en TCP/IP no sean necesarias las funciones que OSI ha asignado a las capas de Presentación y Sesión, sino que en el caso de TCP/IP éstas deben formar parte de los protocolos implementados en la capa de aplicación, es decir deben "formar parte del mismo paquete".

La otra diferencia fundamental se da en las capas inferiores, ya que TCP/IP no establece características para las capas que se encuentren debajo de la capa de Internet (Red), los diseñadores de TCP/IP confiaron plenamente en las soluciones que la industria había establecido, siempre que sean capaces de comunicarse con la capa Internet, y dado que éstas se apoyan fundamentalmente en OSI, es natural considerar que TCP/IP tiene las mismas capas bajas, **ver Figura A2.3**.

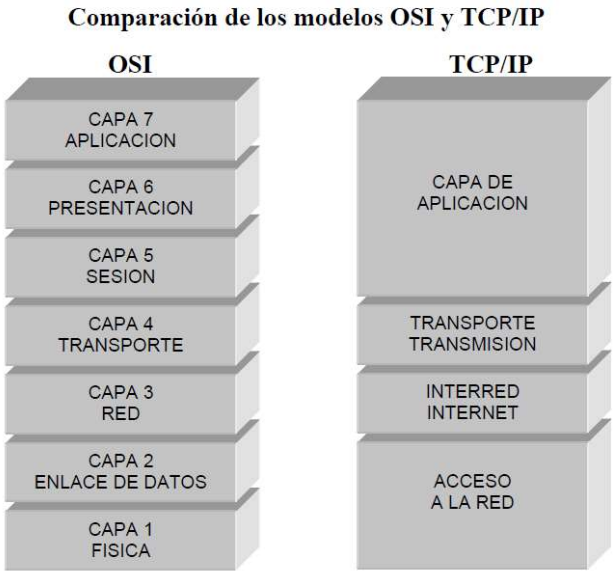


Figura A2.3. Comparación de OSI y TCP/IP

Las capas bajas de ambos modelos se encargan de las topologías de red, las placas de red, los cableados y la forma eléctrica en que se transmitirán los bits a través del medio.

Las capas medias establecen los Protocolos de Comunicación (por ejemplo TCP, IP, UDP, ARP, RARP, ICMP, RIP, IGRP, BGPI y otros, en el caso del modelo TCP/IP), que permitirán que la información llegue a la computadora destino, sin importar dónde se encuentre físicamente.

Son los protocolos que permiten que Ud., por ejemplo, pueda comunicarse desde su casa con una computadora en otro país utilizando Internet.

En las capas altas encontramos los protocolos de aplicación, que en caso de TCP/IP suelen ser: HTTP, FTP, SMTP, Telnet y otros. Los nombres pueden parecer extraños, pero seguramente ya se ha acostumbrado a alguno de ellos: cuando navega por Internet (o por la intranet de su empresa) con el Internet Explorer o el Netscape Navigator está utilizando el protocolo HTTP (Hyper Text Transfer Protocol o Protocolo de transferencia de Hipertexto) que es el que permite que vea las páginas Web. El protocolo HTTP especifica cómo debe hacer su navegador para mostrar en pantalla los Bytes enviados desde el sitio web.

CAPA 7. CAPA DE APLICACIÓN.

Las funciones que realiza la capa de aplicación difieren de los ofrecidos por las otras capas debido al hecho que, como no existe una capa superior, no ofrece servicios. Ejemplos de protocolos de capa 7 son el terminal virtual y transferencia de archivos (file). Se pueden identifican las siguientes funciones:

-Identificación del corresponsal mediante la dirección.

-Determinación de la disponibilidad y establecimiento de la autorización.

-Determinación de la metodología de costos de la comunicación.

-Determinación de la calidad de servicio (errores y costo).

-Selección de disciplina de diálogo y limitaciones de sintaxis.

CAPA 6. CAPA DE PRESENTACIÓN.

Esta capa permite la presentación de la información que las entidades de aplicación comunican o mencionan en su comunicación. Se ocupa de la sintaxis (reglas gramaticales para representación de los datos; secuencia y ortografía de los comandos) y no de la semántica (función que cumple cada parte del mensaje; significado para la capa 7). Ejemplos de protocolos de capa 6 son la compresión de texto, criptografía, reformateo y terminal virtual. Los protocolos UNIX (TCP/IP) no poseen capa 5 y 6. Las funciones de esta capa son:

-Transformación y selección de la sintaxis para la capa 7.

-Transferencia de datos.

-Negociación y renegociación de la sintaxis.

-Establecimiento del formato de datos (compresión de código).

CAPA 5. CAPA DE SESIÓN.

Los servicios que presta esta capa tienen por objeto proporcionar los medios para que la capa 6 organice y sincronice el intercambio de datos. Las funciones son:

-Permite que los usuarios establezcan sesiones de trabajo entre ellos.

-Establecimiento y liberación de la conexión de sesión.

-Intercambio de datos normal o acelerado.

-Sincronización de la conexión. Innecesario en los protocolos TCP/IP de capa 4/3.

La capa de sesión proporciona puntos de verificación en el flujo de datos, con objeto de que, después de una caída del enlace, solo se repitan los mensajes desde el último punto de verificación.

El propósito de la existencia de una sesión en OSI) consiste en proveer a las capas superiores un canal libre de errores, independiente de la tecnología de las capas inferiores.

CAPA 4. CAPA DE TRANSPORTE.

Esta capa optimiza el uso del servicio de la red disponible para ofrecer la calidad de funcionamiento que requiere la capa 5, a un mínimo costo. Son ejemplos TCP, SPX (NetWare). Las funciones son:

-Direccionamiento de la transmisión de datos mediante el concepto de port.

-Multiplexación y división de conexiones (optimiza los costos).

-Detección de errores y comprobación de calidad de servicio. Eventualmente provee la retransmisión.

-Segmentación y concatenación de extremo a extremo.

La capa de transporte es el corazón de la jerarquía de protocolos. Su tarea consiste en asegurar el transporte de datos desde la máquina FUENTE a la máquina DESTINO, independientemente de la red física en uso.

Si trasladamos esto al modelo OSI, podemos ver que las tres capas inferiores se comunican entre adyacentes, o sea del host emisor (origen) al nodo de comunicaciones más cercano, donde están conectadas, desde este nodo al siguiente (puede haber varios en el camino de los mensajes) y de este último al host receptor (destino), mientras que desde la capa de Transporte hacia arriba, todas las demás tienen comunicación extremo a extremo, **ver Figura A2.4.**

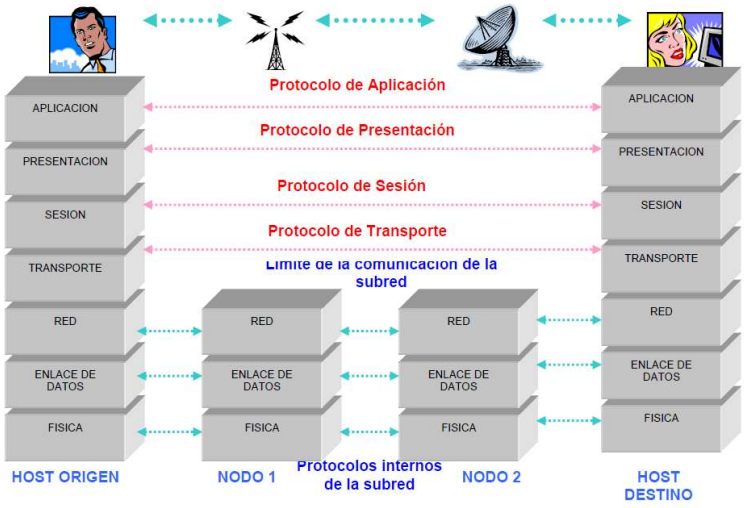


Figura A2.4. Detalles del modelo OSI, mostrando capa de transporte

CAPA 3. CAPA DE RED.

Asegura la independencia de la capa 4 respecto del encaminamiento en la conexión de red. Son ejemplo el protocolo IP (MIL o ISO) y IPX (Netware). Las funciones son:

-Direccionamiento y conexionado en la red de datos.

-Es responsable del ensamble de datos en el servicio sin-conexión.

-Obtención de los parámetros de calidad del servicio y notificación de errores.

-Reiniciación, liberación y acuse de recibo de los datos.

- La capa de red proporciona servicios a la de transporte.

Esta capa se ocupa del control de la operación de la red. Un punto muy importante en su diseño es la determinación de como encaminar los mensajes (o paquetes).

Las rutas podrían basarse en tablas estáticas previamente cableadas en la red, siendo cualquier cambio difícil de realizar. También pueden ser tablas estáticas que se establecen al inicio de cada diálogo.

Por último, pueden ser de tipos dinámicos, determinándose la ruta para cada paquete en el momento en que este es emitido.

- El control de congestión por lo tanto también depende de la capa de red.
- A veces se coloca una función de contabilidad para realizar tareas de facturación.

La responsabilidad para resolver problemas de interconexión de redes heterogéneas recae en la capa de red.

La capa de red opera esencialmente en los Routers, mientras que la de transporte opera en los HOST, los límites entre estas capas, es también el límite entre la red y el Host (usuario). Esto implica que los servicios de la capa de red definen los servicios ofrecidos por la propia red.

Cuando la red es operada por un proveedor de servicios portadores, y los Host son operados por los usuarios, el servicio de capa de red se convierte en la interfase entre el proveedor y los usuarios. Como tal define las obligaciones y responsabilidades del proveedor y del usuario.

Los servicios de la capa de red se han diseñado con los siguientes objetivos:

1. Deben ser independientes de la tecnología de la red.

2. La capa de transporte debe tener oculto el número, tipo y topología de las redes que se encuentren presentes.

3. Las direcciones de red a disposición de la capa de transporte deben utilizar un plan de numeración uniforme, aún a través de redes LAN y WAN.

CAPA 2. CAPA DE ENLACE DE DATOS.

Esta capa proporciona los medios para establecer, mantener y liberar las conexiones entre los niveles 3 de cada extremo. Las funciones que se pueden identificar son:

-Conexión de enlace de datos con sincronismo de trama.

-Identificar los puntos extremos y control del flujo de datos.

-Notificar errores y los parámetros de calidad del servicio.

En esta capa también se define cómo se establecerán las direcciones físicas de cada computadora (direccionamiento físico), y cómo deberán ser las tramas de bits. También se define cómo se establece la secuencia de tramas enviadas (secuenciamiento) y asimismo controla cuándo una computadora puede enviar bits a otra sin saturarla (control de flujo).

Lo más importante de esta capa es que especifica el Método de Acceso al Medio (no nos olvidemos que todas las computadoras de la red usan el mismo medio o cable para comunicarse), como por ejemplo, Token Ring, Frame Relay, MPLS.

Por último también se encarga de detectar posibles errores en la transmisión (control de errores), aplicando por ejemplo algoritmos de suma de verificación (al estilo checksum, CRC,etc.), **ver Figura A2.5.**

La mayoría de las funciones mencionadas se implementan directamente sobre la placa de red, es decir en lo que suele denominarse firmware (software grabado en circuitos integrados).

En cuanto a las normas que cumplen estos requisitos para redes LAN, podemos decir que la norma Ethernet cubre por completo las capas física y de enlace, en tanto que las normas de la

IEEE 802 han subdividido la capa de enlace en dos subcapas:

• LLC (Logic Link Control o Control de enlace Lógico) y

• MAC (Media Access Control o Control de Acceso al Medio)

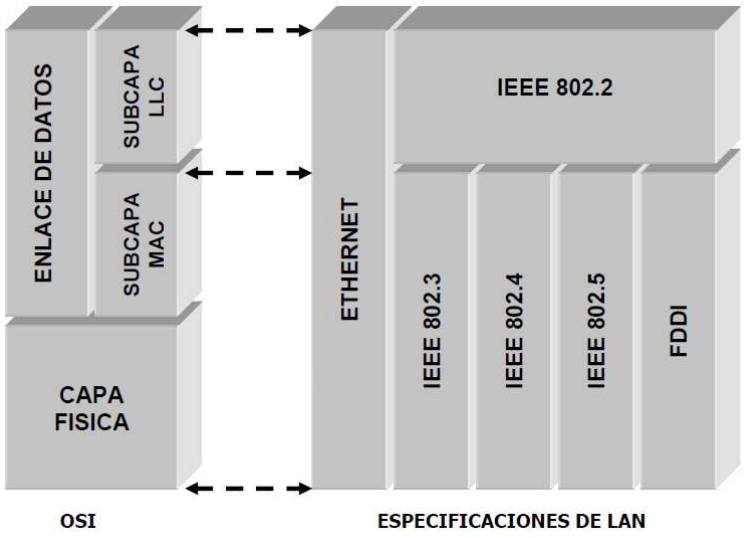


Figura A2.5.Capa de enlace de datos del Modelo OSI

CAPA 1. CAPA FÍSICA.

En esta capa se proporcionan los vínculos necesarios para la conexión al medio de enlace. Las funciones son:

-Conexión física al medio de transmisión.

-Definición de las características mecánicas, eléctricas, funcionales y de procedimiento.

-Identificación del enlace de datos y notificación de condiciones de falla.

-Define cómo deben ser los conectores que vinculan el cable a la placa de red y los conectores que se utilizan para unir distintos segmentos de cable.

La siguiente figura le muestra la relación que existe entre la capa física del modelo OSI (y también del TCP/IP) y algunas normas que lo implementan para redes LAN.

Anexo 3- Eterneth

Ethernet, al que también se conoce como IEEE 802.3, es el estándar más popular para las LAN, usa el método de transmisión de datos llamado Acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD). Antes de que un nodo envíe algún dato a través de una red Ethernet, primero escucha y se da cuenta si algún otro nodo está transfiriendo información; de no ser así, el nodo transferirá la información a través de la red. Todos los otros nodos escucharán y el nodo seleccionado recibirá la información. En caso de que dos nodos traten de enviar datos por la red al mismo tiempo, cada nodo se dará cuenta de la colisión y esperará una cantidad de tiempo aleatoria antes de volver a hacer el envío. Cada paquete enviado contiene la dirección de la estación destino, la dirección de la estación de envío y una secuencia variable de bits que representa el mensaje transmitido. El dato transmitido procede a 10 millones de bits por segundo y el paquete varia en una longitud de 64 a 1518 bytes, así el tiempo de transmisión de un paquete en la Ethernet está en un rango de 50 a 1200 microsegundos dependiendo de su longitud. La dirección de la estación de destino normalmente es referida por una única interfaz de red. Cada estación recibe una copia de cada paquete, pero ignora los paquetes que son dirigidos a otras computadoras y procesa solamente los que son dirigidos a ella.

Versiones de 802.3

Ethernet se tomó como base para la redacción del estándar internacional IEEE 802.3, siendo usualmente tomados como sinónimos. Se diferencian en uno de los campos de la trama de datos. Sin embargo, las tramas originales Ethernet e IEEE 802.3 pueden coexistir en la misma red.

Los estándares de este grupo no reflejan necesariamente lo que se usa en la práctica, aunque a diferencia de otros grupos este suele estar cerca de la realidad.

La primera versión del IEEE 802.3 fue un intento de estandarizar ethernet aunque hubo un campo de la cabecera que se definió de forma diferente, posteriormente ha habido ampliaciones sucesivas al estándar que cubrieron las ampliaciones de velocidad (Fast Ethernet, Gigabit Ethernet y el de 10 Gigabits), redes virtuales, hubs, conmutadores y distintos tipos de medios, tanto de fibra óptica como de cables de cobre (tanto par trenzado como coaxial), **ver Tabla A3.1**.

Tabla A3.1. Versiones de Eterneth

Estándar Ethernet	Fecha	Descripción
Ethernet experimental	1972 (patentado en 1978)	2,85 Mbit/s sobre cable coaxial en topología de bus.
Ethernet II (DIX v2.0)	1982	10 Mbit/s sobre coaxial fino (thinnet) - La trama tiene un campo de tipo de paquete. El protocolo IP usa este formato de trama sobre cualquier medio.
IEEE 802.3	1983	10BASE5 10 Mbit/s sobre coaxial grueso (thicknet). Longitud máxima del segmento 500 metros - Igual que DIX salvo que el campo de Tipo se substituye por la longitud.

802.3ª	1985	10BASE2 10 Mbit/s sobre coaxial fino (thinnet o cheapernet). Longitud máxima del segmento 185 metros
802.3b	1985	10BROAD36
802.3c	1985	Especificación de repetidores de 10 Mbit/s
802.3d	1987	FOIRL (Fiber-Optic Inter-Repeater Link) enlace de fibra óptica entre repetidores.
802.3e	1987	1BASE5 o StarLAN
802.3i	1990	10BASE-T 10 Mbit/s sobre par trenzado no blindado (UTP). Longitud máxima del segmento 150 metros.
802.3j	1993	10BASE-F 10 Mbit/s sobre fibra óptica. Longitud máxima del segmento 1000 metros.
802.3u	1995	100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet a 100 Mbit/s con auto-negociación de velocidad.
802.3x	1997	Full Duplex (Transmisión y recepción simultáneos) y control de flujo.
802.3y	1998	100BASE-T2 100 Mbit/s sobre par trenzado no blindado (UTP). Longitud máxima del segmento 100 metros
802.3z	1998	1000BASE-X Ethernet de 1 Gbit/s sobre fibra óptica.
802.3ab	1999	1000BASE-T Ethernet de 1 Gbit/s sobre par trenzado no blindado
802.3ac	1998	Extensión de la trama máxima a 1522 bytes (para permitir las "Q-tag") Las Q-tag incluyen información para 802.1Q VLAN y manejan prioridades según el estándar 802.1p.
802.3ad	2000	Agregación de enlaces paralelos.
802.3ae	2003	Ethernet a 10 Gbit/s ; 10GBASE-SR, 10GBASE-LR
IEEE 802.3af	2003	Alimentación sobre Ethernet (PoE).
802.3ah	2004	Ethernet en la última milla.
802.3ak	2004	10GBASE-CX4 Ethernet a 10 Gbit/s sobre cable bi-axial.
802.3an	2006	10GBASE-T Ethernet a 10 Gbit/s sobre par trenzado no blindado (UTP)
802.3ap	en proceso (draft)	Ethernet de 1 y 10 Gbit/s sobre circuito impreso.

802.3aq	en proceso (draft)	10GBASE-LRM Ethernet a 10 Gbit/s sobre fibra óptica multimodo.
802.3ar	en proceso (draft)	Gestión de Congestión
802.3as	en proceso (draft)	Extensión de la trama

Formato de la trama Ethernet

La trama es lo que se conoce también por el nombre de "frame".

- El primer campo es el preámbulo que indica el inicio de la trama y tienen el objeto de que el dispositivo que lo recibe detecte una nueva trama y se sincronice.
- El delimitador de inicio de trama indica que el frame empieza a partir de él.
- Los campos de MAC (o dirección) de destino y origen indican las direcciones físicas del dispositivo al que van dirigidos los datos y del dispositivo origen de los datos, respectivamente.
- La etiqueta es un campo opcional que indica la pertenencia a una VLAN o prioridad en IEEE P802.1p
- Ethernetype indica con que protocolo están encapsulados los datos que contiene la Payload, en caso de que se usase un protocolo de capa superior.
- La Payload es donde van todos los datos y, en el caso correspondiente, cabeceras de otros protocolos de capas superiores (Según Modelo OSI, véase Protocolos en informática) que pudieran formatear a los datos que se tramiten (IP, TCP, etc). Tiene un mínimo de 64 Bytes (o 42 si es la versión 802.1Q) hasta un máximo de 1518 Bytes.
- La secuencia de comprobación es un campo de 4 bytes que contiene un valor de verificación CRC (control de redundancia cíclica). El emisor calcula el CRC de toda la trama, desde el campo destino al campo CRC suponiendo que vale 0. El receptor lo recalcula, si el valor calculado es 0 la trama es válida, **ver Figura A3.1**.
- El gap de final de trama son 12 bytes vacíos con el objetivo de espaciado entre tramas.

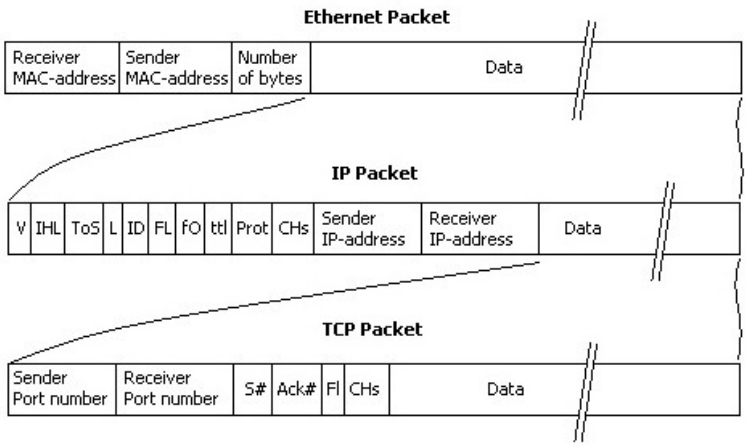


Figura A3.1. Trama Eterneth

Tecnología y velocidad de Ethernet

Hace ya mucho tiempo que Ethernet consiguió situarse como el principal protocolo del nivel de enlace. Ethernet 10Base2 consiguió, ya en la década de los 90s, una gran aceptación en el sector. Hoy por hoy, 10Base2 se considera como una "tecnología de legado" respecto a 100BaseT. Hoy los fabricantes ya han desarrollado adaptadores capaces de trabajar tanto con la tecnología 10baseT como la 100BaseT y esto ayuda a una mejor adaptación y transición.

Las tecnologías Ethernet que existen se diferencian en estos conceptos entre ellos:

- Velocidad de transmisión

Velocidad a la que transmite la tecnología.

- Tipo de cable

Tecnología del nivel físico que usa la tecnología.

- Longitud máxima

Distancia máxima que puede haber entre dos nodos adyacentes (sin estaciones repetidoras).

- Topología

Determina la forma física de la red. Bus si se usan conectores T (hoy solamente usados con las tecnologías más antiguas) y estrella si se usan hubs (estrella de difusión) o switchs (estrella conmutada).

A continuación se especifican los anteriores conceptos en las tecnologías más importantes, **ver Tabla A3.1**:

Tabla A3.1. Velocidades Eterneth

Tecnología	Velocidad de transmisión	Tipo de cable	Distancia máxima	Topología
10Base2	10 Mbit/s	Coaxial	185 m	Bus (Conector T)
10BaseT	10 Mbit/s	Par Trenzado	100 m	Estrella (Hub o Switch)
10BaseF	10 Mbit/s	Fibra óptica	2000 m	Estrella (Hub o Switch)
100BaseT4	100 Mbit/s	Par Trenzado (categoría 3UTP)	100 m	Estrella. Half Duplex (hub) y Full Duplex (switch)
100BaseTX	100 Mbit/s	Par Trenzado (categoría 5UTP)	100 m	Estrella. Half Duplex (hub) y Full Duplex (switch)
100BaseFX	100 Mbit/s	Fibra óptica	2000 m	No permite el uso de hubs

1000BaseT	1000 Mbit/s	(categoría 5e ó 6UTP)	100 m	Estrella. Full Duplex (switch)
1000BaseSX	1000 Mbit/s	Fibra óptica (monomodo)	550 m	Estrella. Full Duplex (switch)
1000BaseLX	1000 Mbit/s	Fibra óptica (multimodo)	5000 m	Estrella. Full Duplex (switch)

Anexo 4- Mascarás de Red y

La máscara de red o redes es una combinación de bits que sirve para delimitar el ámbito de una red de ordenadores.1 Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

Mediante la máscara de red un sistema (ordenador, puerta de enlace, router, etc...) podrá saber si debe enviar un paquete dentro o fuera de la subred en la que está conectado. Por ejemplo, si el router tiene la dirección IP 192.168.1.1 y máscara de red 255.255.255.0, entiende que todo lo que se envía a una dirección IP con formato 192.168.1.X, se envía hacia la red local, mientras que direcciones con distinto formato de direcciones IP serán buscadas hacia afuera (internet, otra red local mayor, etc...), **ver Tabla A4.1**.

Tabla de máscaras de red

Tabla A4.1. Máscaras de red

Binario	Decimal	CIDR	Nº hosts	Clase
11111111.11111111.11111111.11111111	255.255.255.255	/32		
11111111.11111111.11111111.11111110	255.255.255.254	/31		
11111111.11111111.11111111.11111100	255.255.255.252	/30	2	
11111111.11111111.11111111.11111000	255.255.255.248	/29	6	
11111111.11111111.11111111.11110000	255.255.255.240	/28	14	
11111111.11111111.11111111.11100000	255.255.255.224	/27	30	
11111111.11111111.11111111.11000000	255.255.255.192	/26	62	
11111111.11111111.11111111.10000000	255.255.255.128	/25	126	
11111111.11111111.11111111.00000000	255.255.255.0	/24	254	C
11111111.11111111.11111110.00000000	255.255.254.0	/23	510	
11111111.11111111.11111100.00000000	255.255.252.0	/22	1022	
11111111.11111111.11111000.00000000	255.255.248.0	/21	2046	
11111111.11111111.11110000.00000000	255.255.240.0	/20	4094	
11111111.11111111.11100000.00000000	255.255.224.0	/19	8190	
11111111.11111111.11000000.00000000	255.255.192.0	/18	16382	
11111111.11111111.10000000.00000000	255.255.128.0	/17	32766	
11111111.11111111.00000000.00000000	255.255.0.0	/16	65534	B
11111111.11111110.00000000.00000000	255.254.0.0	/15	131070	
11111111.11111100.00000000.00000000	255.252.0.0	/14	262142	
11111111.11111000.00000000.00000000	255.248.0.0	/13	524286	
11111111.11110000.00000000.00000000	255.240.0.0	/12	1048574	
11111111.11100000.00000000.00000000	255.224.0.0	/11	2097150	
11111111.11000000.00000000.00000000	255.192.0.0	/10	4194302	
11111111.10000000.00000000.00000000	255.128.0.0	/9	8388606	
11111111.00000000.00000000.00000000	255.0.0.0	/8	16777214	A

11111110.00000000.00000000.00000000	254.0.0.0	/7	33554430	
11111100.00000000.00000000.00000000	252.0.0.0	/6	67108862	
11111000.00000000.00000000.00000000	248.0.0.0	/5	134217726	
11110000.00000000.00000000.00000000	240.0.0.0	/4	268435454	
11100000.00000000.00000000.00000000	224.0.0.0	/3	536870910	
11000000.00000000.00000000.00000000	192.0.0.0	/2	1073741822	
10000000.00000000.00000000.00000000	128.0.0.0	/1	2147483646	
00000000.00000000.00000000.00000000	0	/0	4294967294	

El número de hosts se determina como el número de IP's posibles menos dos, en cada subred hay una IP con todos los bits a ceros en la parte del host reservada para nombrar la subred y otra con todos los bits a uno reservada para la dirección de Broadcast.

Hay ciertos programas (p.e. Ethereal) que programan la tarjeta en un modo llamado 'promiscuo' en el que se le dice a la tarjeta de red que no filtre los paquetes según la norma explicada, aceptando todos los paquetes para poder hacer un análisis del tráfico que circula por la subred y poder ser escuchado por el PC.

Las máscaras 255.0.0.0 (clase A), 255.255.0.0 (clase B) y 255.255.255.0 (clase C) suelen ser suficientes para la mayoría de las redes privadas. Sin embargo, las redes más pequeñas que podemos formar con estas máscaras son de 254 hosts y para el caso de direcciones públicas, su contratación tiene un coste alto. Por esta razón suele ser habitual dividir las redes públicas de clase C en subredes más pequeñas. A continuación se muestran las posibles divisiones de una red de clase C. La división de una red en subredes se conoce como subnetting.

Clases de máscaras en subredes

Tabla A4.2. Clases de máscaras de red

Clase	Bits	IP Subred	IP Broadcast	Máscara en decimal	CIDR
A	0	0.0.0.0	127.255.255.255	255.0.0.0	/8
B	10	128.0.0.0	191.255.255.255	255.255.0.0	/16
C	110	192.0.0.0	223.255.255.255	255.255.255.0	/24
D	1110	224.0.0.0	239.255.255.255	sin definir	sin definir
E	1111	240.0.0.0	255.255.255.254	sin definir	sin definir

Classless Inter-Domain Routing

"Classless Inter-Domain Routing" o "enrutamiento entre dominios sin clases" se introdujo en 1993 por IETF y representa la última mejora en el modo de interpretar las direcciones IP. Su introducción permitió una mayor flexibilidad al dividir rangos de direcciones IP en redes separadas. De esta manera permitió:

- Un uso más eficiente de las cada vez más escasas direcciones IPv4.
- Un mayor uso de la jerarquía de direcciones (agregación de prefijos de red), disminuyendo la sobrecarga de los enrutadores principales de Internet para realizar el encaminamiento.

CIDR reemplaza la sintaxis previa para nombrar direcciones IP, las clases de redes. En vez de asignar bloques de direcciones en los límites de los octetos, que implicaban prefijos «naturales» de 8, 16 y 24 bits, CIDR usa la técnica VLSM (variable length subnet mask, en español «máscara de subred de longitud variable»), para hacer posible la asignación de prefijos de longitud arbitraria.

CIDR engloba:

La técnica VLSM para especificar prefijos de red de longitud variable. Una dirección CIDR se escribe con un sufijo que indica el número de bits de longitud de prefijo, p.ej. 192.168.0.0/16 que indica que la máscara de red tiene 16 bits (es decir, los primeros 16 bits de la máscara son 1 y el resto 0). Esto permite un uso más eficiente del cada vez más escaso espacio de direcciones IPv4

La agregación de múltiples prefijos contiguos en superredes, reduciendo el número de entradas en las tablas de ruta globales.

Otro beneficio de CIDR es la posibilidad de agregar prefijos de encaminamiento, un proceso conocido como "supernetting". Por ejemplo, dieciséis redes /24 contiguas pueden ser agregadas y publicadas en los enrutadores de Internet como una sola ruta /20 (si los primeros 20 bits de sus respectivas redes coinciden). Dos redes /20 contiguas pueden ser agregadas en una /19, etc.

Esto permite una reducción significativa en el número de rutas que los enrutadores en Internet tienen que conocer (y una reducción de memoria, recursos, etc.) y previene una explosión de tablas de encaminamiento, que podría sobrecargar a los routers e impedir la expansión de Internet en el futuro, **ver Tabla A4.3**.

Tabla A4.3. Tabla de redes por clases

CIDR	No. de redes por clase	Hosts*	Máscara
/32	1/256 C	1	255.255.255.255
/31	1/128 C	2	255.255.255.254
/30	1/64 C	4	255.255.255.252
/29	1/32 C	8	255.255.255.248
/28	1/16 C	16	255.255.255.240
/27	1/8 C	32	255.255.255.224
/26	1/4 C	64	255.255.255.192
/25	1/2 C	128	255.255.255.128
/24	1 C	256	255.255.255.0

/23	2 C	512	255.255.254.0
/22	4 C	1024	255.255.252.0
/21	8 C	2048	255.255.248.0
/20	16 C	4096	255.255.240.0
/19	32 C	8192	255.255.224.0
/18	64 C	16384	255.255.192.0
/17	128 C	32768	255.255.128.0
/16	256 C, 1 B	65536	255.255.0.0
/15	512 C, 2 B	131072	255.254.0.0
/14	1,024 C, 4 B	262144	255.252.0.0
/13	2,048 C, 8 B	524288	255.248.0.0
/12	4,096 C, 16 B	1048576	255.240.0.0
/11	8,192 C, 32 B	2097152	255.224.0.0
/10	16,384 C, 64 B	4194304	255.192.0.0
/9	32,768 C, 128B	8388608	255.128.0.0
/8	65,536 C, 256B, 1 A	16777216	255.0.0.0
/7	131,072 C, 512B, 2 A	33554432	254.0.0.0
/6	262,144 C, 1,024 B, 4 A	67108864	252.0.0.0
/5	524,288 C, 2,048 B, 8 A	134217728	248.0.0.0
/4	1,048,576 C, 4,096 B, 16 A	268435456	240.0.0.0
/3	2,097,152 C, 8,192 B, 32 A	536870912	224.0.0.0
/2	4,194,304 C, 16,384 B, 64 A	1073741824	192.0.0.0
/1	8,388,608 C, 32,768 B, 128 A	2147483648	128.0.0.0
/0	16,777,216 C, 65,536 B, 256 A	4294967296	0.0.0.0

Anexo 5.Componentes internos de Router y Switch

Interface del Cisco IOS en un router.

La interface del IOS es de línea de comandos basada en texto (CLI)

La mayoría de routers y switches Cisco ejecutan un IOS (Internet Operating System).

El IOS fue creado para entregar servicios y habilitar aplicaciones de red. Corre en la mayoría de routers y en algunos switches, **ver Figura A5.1**.

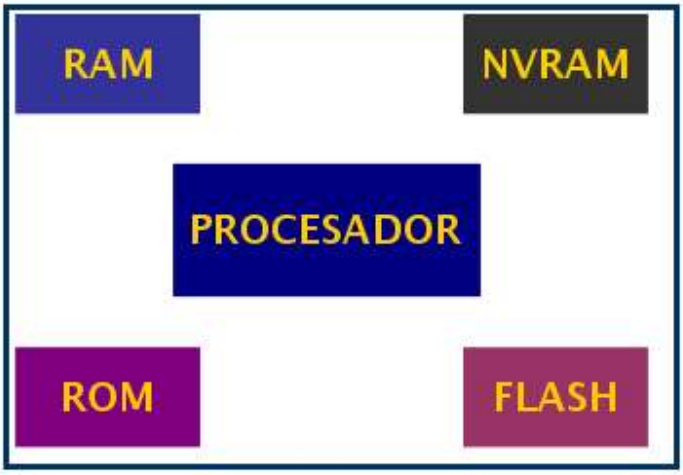


Figura A5.1 Componentes internos del router

Flash. En esta memoria se almacenan una o más imágenes completas del IOS y es el lugar por default desde donde secarga el sistema operativo. La flash puede residir como tarjeta de memoria, o como tarjeta PCMCIA.

RAM. Aquí se carga el IOS, y el archivo de configuración (running-config) con el cual trabaja el router. Las tablas de ARP, de enrutamiento y buffers de entrada y salida tambien residen aquí.

ROM. En la ROM reside el microcódigo del POST, Bootstrap, y de ROMMON. POST realiza pruebas autodiagnóstico del hardware principal del router. El Bootstrap se carga a la RAM y luego, localiza y carga el IOS de acuerdo a la información leída desde el registro de configuración y de la NVRAM. Una vez que el IOS se carga a la RAM, éste toma el control. ROMMON es un IOS reducido que se utiliza para recuperación de un IOS completo, y para recuperación de contraseñas.

NVRAM. Esta es una memoria no volátil, que es utilizada para mantener un respaldo de la configuración del router. El archivo que reside aqui se conoce como startup-config. El registro de configuración se utiliza para controlar como arrancará el router, es parte de la NVRAM, **ver Figura A5.2**.

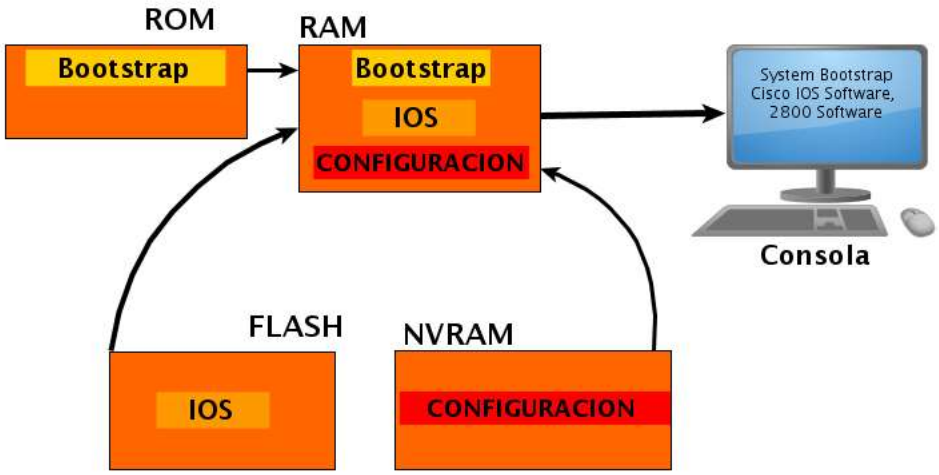


Figura A5.2 Proceso de arranque de un router

Carga del IOS

Al encender un router, éste realiza las siguientes tareas para estar preparado:

Realiza una prueba de autodiagnóstico de hardware (POST-Power On Self Test). Si pasa la prueba ejecuta el paso 2, sino termina.

Carga de la ROM y ejecuta el bootstrap desde la RAM, cuya función es localizar y cargar el IOS a la RAM, a fin de que éste tome el control. Si no encuentra un IOS completo, carga de la ROM un IOS limitado en funciones.

El IOS localiza el archivo de configuración en la NVRAM, o en el lugar que esté especificado, lo carga en la RAM y lo ejecuta. Cuando no localiza un archivo de configuración lanza el diálogo de configuración inicial, **ver Figura A5.3**.

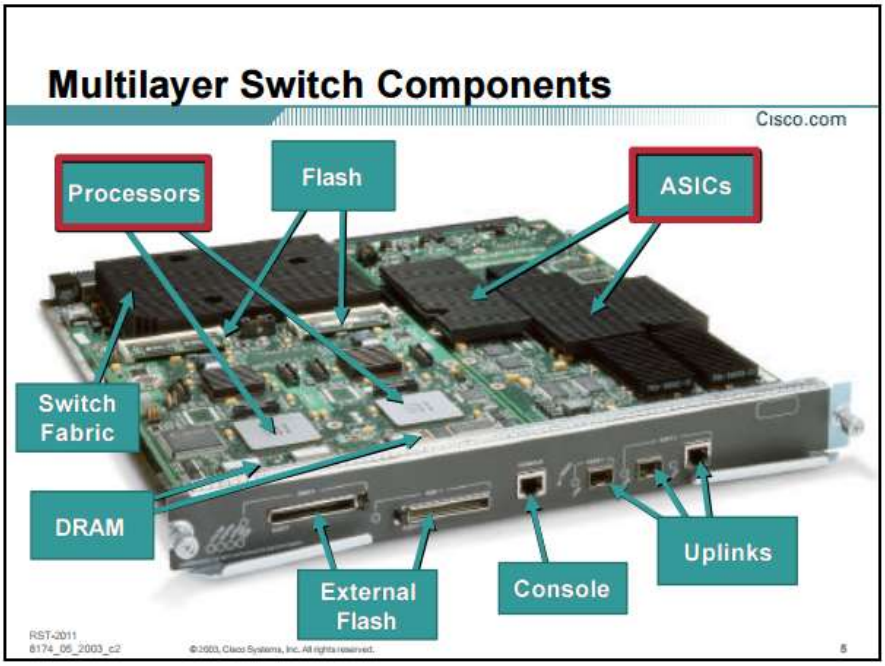


Figura A5.3. Componentes físicos del router.

Tecnologías de un Switch

Conmutador (switch) es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada esta.1

Los conmutadores se utilizan cuando se desea conectar múltiples tramos de una red, fusionándolos en una sola red. Al igual que los puentes, dado que funcionan como un filtro en la red y solo retransmiten la información hacia los tramos en los que hay el destinatario de la trama de red, mejoran el rendimiento y la seguridad de las redes de área local (LAN).

- La transmisión de una trama, de un puerto a otro en un switch se realiza a través del switch fabric
- El switch fabric es el conjunto de canales de comunicación utilizados para transportar tramas a través del switch, **ver Figura A5.4.**

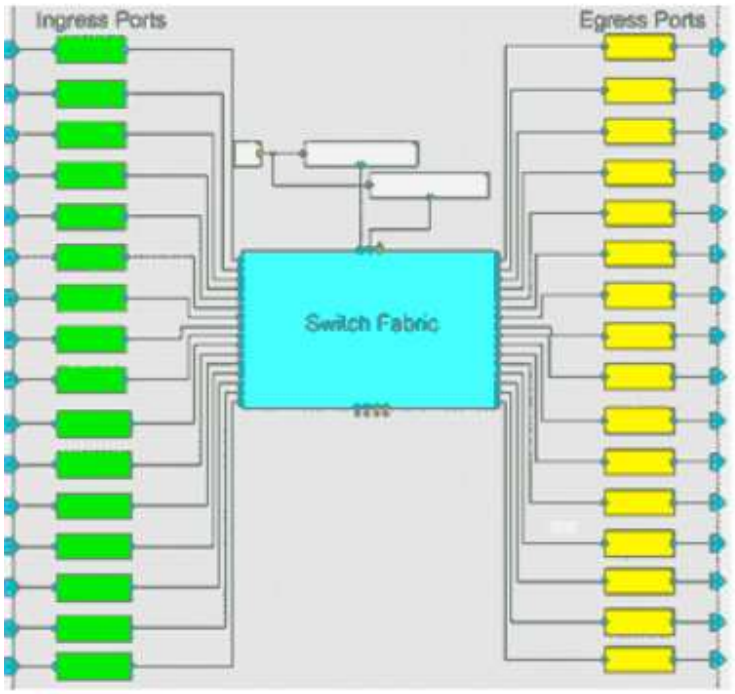


Figura A5.4. Funcionamiento de Switch Fabric, como componente principal de un Switch

Switch Fabric es una topología de red en la que los nodos de red se interconectan a través de uno o más conmutadores de red (particularmente interruptores de barra transversal). Debido a que una red de red conmutada difunde el tráfico de red a través de múltiples enlaces físicos, produce un rendimiento total superior al de las redes de difusión, como la versión 10BASE5 de Ethernet o la mayoría de las redes inalámbricas como Wi-Fi.

Una generación de interconexiones serie de alta velocidad que aparecieron en 2001-2004 y proporcionan conectividad punto a punto entre el procesador y los dispositivos periféricos se denominan a veces telas; Sin embargo, carecen de características tales como un protocolo de paso de mensajes. HyperTransport, por ejemplo, continúa manteniendo un enfoque de bus de procesador incluso después de adoptar una capa física de velocidad más alta. Del mismo modo, PCI Express es sólo una versión serial de PCI; Se adhiere a la arquitectura basada en DMA de host / periféricos de PCI / almacén basada en una capa física y de enlace en serie, **ver Figura A5.5**.

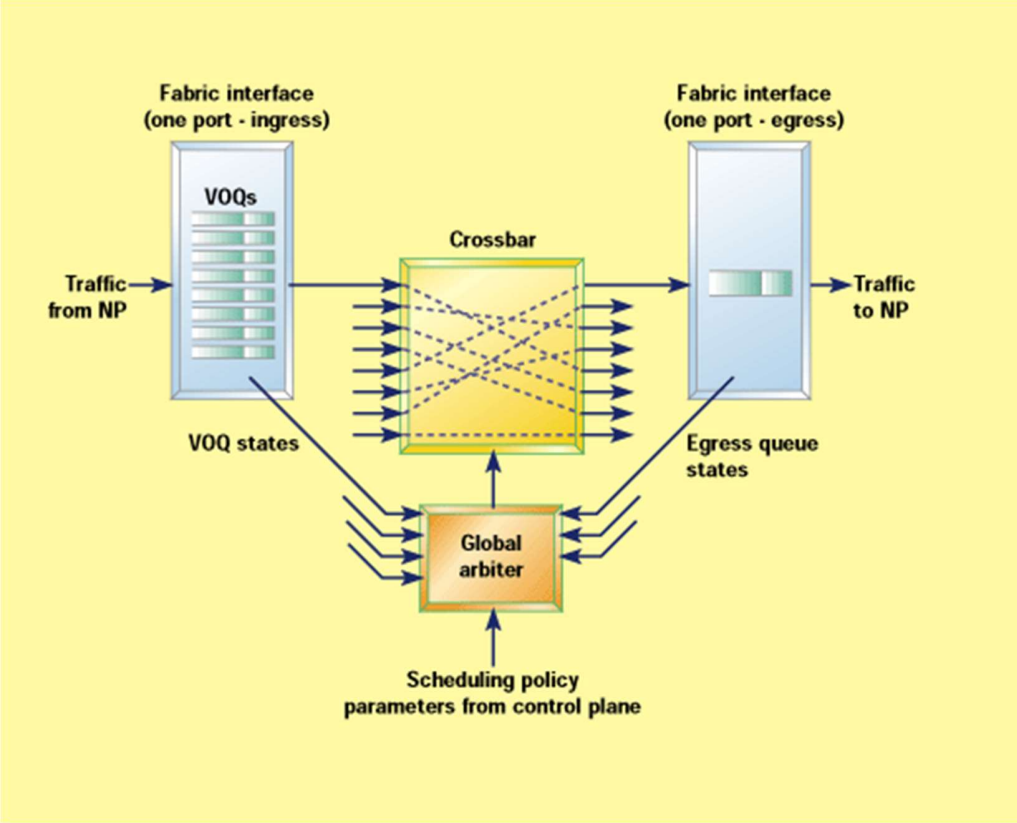


Figura A5.5 Flujo de switch Fabric