UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

INFORME DEL EJERCICIO PROFESIONAL 1997 – 2007 EN INFORMÁTICA PARA CORPORATIVOS

TESIS
QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

PRESENTA:

SAGRERO GUERRERO CARLOS

DIRECTOR DE TESIS: **VEGA MUYTOY SILVIA**.

2009

Agradecimientos.

Gracias a Dios, por permitirme vivir esta vida y gozar de ella.

Gracias a mis padres, María Elena y Carlos, y a mi hermana Adriana, por su cariño, apoyo y guía.

Gracias a mi esposa, Laura Olivia, por aceptarme en su vida y hacerme feliz a su lado; por su comprensión y apoyo desde el primer día, y por ser ella quien me animó a postularme para un puesto de trabajo en InfoCorp.

Gracias a Grupo Sphaera (Soportec e InfoCorp) por aceptarme como empleado a pesar de no haber tenido ninguna experiencia; por la confianza, el apoyo, el crecimiento y por todo el aprendizaje.

Gracias a mis compañeros de escuela y de trabajo, por todos los buenos momentos, y por su apoyo en los malos momentos.

Gracias a la Profesora Ing. Silvia Vega Muytoy, por su invaluable apoyo y guía para la realización y culminación de este proyecto.

Índice.

Introducción.

En 1997 se inició formalmente la vida profesional de quien esto escribe, y fue en una empresa privada llamada INFORMÁTICA PARA CORPORATIVOS (InfoCorp), que es parte de GRUPO SPHAERA (junto con Soportec).

Escribir parte de las experiencias, clientes y proyectos vividos por un servidor durante 10 años de labor profesional en esa empresa pudiera ser considerado como aburrido o poco novedoso. Pero en realidad puede resultar una historia interesante. Una historia de crecimiento personal y profesional. Una historia de retos y conflictos. Una historia que muestra que sí es posible ir mejorando y creciendo.

Tal y como menciona la frase popular: “hay que empezar desde abajo”, esta historia comienza con un puesto de perfil relativamente modesto: Ingeniero de Soporte Técnico; sin experiencia alguna respecto al mundo “real” de los negocios y de la Tecnología de Información. Gracias al apoyo de muchas personas en la Empresa y con mucho esfuerzo personal, se fue ganando experiencia y confianza en uno mismo. El esfuerzo rindió frutos y poco a poco se logró ser considerado para obtener nuevos puestos, que implicaban mayores responsabilidades, siendo la primera promoción la de Líder de Mesa de Ayuda de Symantec.

Una vez que se había adquirido un muy buen nivel de experiencia y conocimiento técnico de los productos de Symantec, se tuvo oportunidad de pasar a otro nivel y que fue el inicio de un crecimiento mayor y dio acceso a una gran cantidad de experiencias y conocimientos nuevos. Como Ingeniero de Soporte Especializado se tuvo contacto con clientes de todos tamaños, incluyendo grandes corporativos. En muchos casos se conoció a mucha gente valiosa, que enriqueció enormemente el actuar profesional de quien esto escribe. Y nuevamente, gracias al empeño y buenos resultados mostrados a la Empresa, se pudo llegar a ser Supervisor de Soporte Técnico Especializado. Las responsabilidades también crecieron y se empezó a observar también el tema económico del negocio, es decir, hacer que las actividades fueran rentables para la Empresa.

Llegar a ocupar una Gerencia fue algo esperado y deseado, aunque en muchos aspectos no se logró tener la formación real que un Gerente debiera tener. La importancia de los proyectos fue en aumento y se tuvo la capacidad de sacar adelante los retos presentados. Un motivador especial fue ver cómo la gente

respondía positivamente a los cambios y las propuestas; crear un verdadero equipo de trabajo, automotivado, es una verdadera satisfacción.

La intención de este escrito es mostrar cómo se puede ir creciendo en una Empresa y cómo el esfuerzo puede ser recompensado. De nada sirve esforzarse por sobresalir o crecer en un ambiente no propicio; y de igual forma, de nada sirve estar en el mejor ambiente, adecuado para crecer, y no desear participar del crecimiento. Se incluyen extractos de documentación creada en su momento por quien esto escribe para cumplir un doble objetivo: primeramente, mostrar el tipo de redacción que se tenía y notar conforme se avanza en la lectura la evolución que se tuvo; y por otro lado, para que sirva a quien pudiera estar requiriendo orientación acerca de qué medidas implementar para mejorar un proceso o servir de base para crear documentación. No es un manual de procesos, ni tampoco contiene la fórmula para lograr ascensos en una Empresa.

Es tan sólo una pequeña muestra de lo que se puede lograr si se juntan voluntad, empeño, medios apropiados y apoyo. El proceso no fue necesariamente fácil (llegando en ocasiones a ser hasta un poco doloroso), pero al final del período y en retrospectiva, se puede decir con honestidad que ha valido la pena.

Capítulo 1.
Ingeniero de Soporte Técnico.

Período: Agosto, 1997 a Noviembre, 1998.
Jefe Directo: Ing. Antonio Damián.

Cómo comenzó todo.

A tan sólo 2 meses de haber finalizado los estudios en la entonces ENEP Aragón, y después de haber dejado algunos Curriculums Vitae y asistido a algunas entrevistas en varias empresas, se respondió a un anuncio en el periódico de una "Empresa Líder en su ramo", y aunque solicitaban personal con 2 años de experiencia, aceptaron el CV y se tuvo entrevista con el Ing. Antonio Patiño Coz. Cuatro días después de la entrevista, se recibió la oferta formal de trabajo y se comenzaron labores el 20 de agosto de 1997.

Originalmente, la contratación fue para participar en un proyecto de Lotus Notes junto con otras 2 personas, y que iniciaba con un entrenamiento por parte de un mayorista en la solución. Al presentarse al primer día de entrenamiento, se indicó que sólo había lugar para 2 personas.

Ante esa situación, la Empresa tomó la decisión de cambiar de proyecto y enfocarse al proyecto de "Mesa de Ayuda de Symantec". Con tan sólo una semana y algunos manuales de referencia, se iniciaron actividades en este proyecto el 2 de septiembre de 1997.

Inicio en la Mesa de Ayuda de Symantec.

La Mesa de Ayuda de Symantec (en esquema de *Call Center*) tenía la responsabilidad de atender a usuarios de esta marca y brindar soporte telefónico en horario hábil a toda su familia de productos para todo el país. Este proyecto sólo contaba con 2 personas, el Ing. Antonio Damián García como responsable y un servidor, y se tenía un promedio de 150 reportes al mes, de los cuales, un 70% eran atendidos por quien esto escribe.

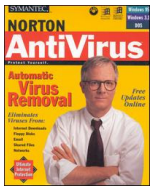
Aunque el responsable recibió capacitación de Symantec antes de iniciar operaciones y durante una semana en Cupertino (California), la cantidad de productos y el desconocimiento de los mismos complicaron la operación al inicio.

Sólo se tuvo una semana para "repasar" los manuales de referencia antes de iniciar a dar soporte, y lamentablemente, no se tenían todos los programas (ni el equipo) para realizar laboratorios y aprender realmente los productos. Los manuales

de referencia, abordaban temas avanzados de resolución de problemas y, en la mayoría de los casos, ni siquiera enseñaban a usar el producto.

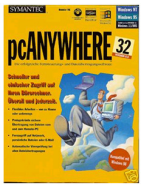
Con todo y esto, se comenzó a dar soporte a usuarios y durante algunos días, se aprendió a usar algunos productos en base a lo que los usuarios comentaban. Sin embargo, era evidente que no se contaban con las bases necesarias para brindar el soporte de forma adecuada, y se solicitó al responsable la oportunidad de instalar y estudiar algunos de los productos.

Aprendiendo los productos.



El producto estrella en ese entonces, era Norton Antivirus (NAV) y un 70% de las llamadas de soporte eran relativas a dicho producto. Su interfase de usuario era sencilla y fácil de usar; su nivel de detección era suficientemente bueno y tenía buena fama por el señor Peter Norton, cuya foto en mangas de camisa y con cara de experto siempre estaba en las cajas de los productos.

El producto en sí no daba muchos problemas, y la mayoría de las consultas eran relativas a problemas con virus y algunas veces a problemas de instalación. Aprender el producto fue sencillo y sólo bastaba con ir siguiendo la evolución de los virus y sus nuevas características.



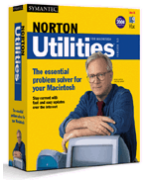
Durante los primeros días de dar soporte, el producto pcAnywhere (PCA) fue complicado, pues los usuarios hablaban de “signos raros” en pantalla o botones no habilitados y no se tenía ni idea de qué debería ver el usuario. Por eso se decidió iniciar laboratorios con este producto, que permite tomar control remoto de un equipo (a través de un módem y línea telefónica, un cable paralelo o una conexión de red).

La primera vez que se observó una sesión de control remoto con este producto fue sorprendente la forma de ver el escritorio del equipo controlado y cómo respondía éste, tal y como si se estuviera frente al equipo. Una vez que se entendió qué era y qué hacía el producto se pudieron brindar mejores soluciones.

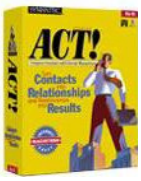
Pocos usuarios llamaban para pedir soporte del producto WinFax, pues era en realidad fácil de usar y hacía lo que tenía que hacer: enviar faxes a través del módem de la computadora y sin necesidad de imprimir las hojas a ser enviadas. Los problemas principales eran la corrupción de su base de datos o incompatibilidad con ciertos modelos de módems.

Algo en lo que se quedaba corto este producto era en su capacidad de trabajo en red.

Un clásico de todos los tiempos es Norton Utilities, que realmente era el "kit de emergencia" para problemas de disco o con Windows. Pocos usuarios llamaban para pedir soporte, pues aunque era un producto sumamente popular, eran pocos los usuarios que lo habían adquirido de forma legal.



En muchos casos, la herramienta era capaz de resolver problemas de corrupción lógica, y sólo en los casos de daño físico no podía ayudar. Este producto ayudó a conservar varios empleos, pues ante lo que parecía irreparable, llegaba Norton Utilities y lo arreglaba.



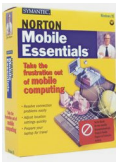
Otro producto que causó varios dolores de cabeza, hasta que se decidió dedicarle tiempo para aprenderlo, fue ACT!. Este manejador de contactos (que podría considerarse como el antecesor de los modernos manejadores de recursos o de contactos empresariales) era un buen producto y casi no generaba problemas. Las consultas en realidad eran acerca de cómo hacer ciertas cosas, y era ahí en donde radicaba el problema, pues algunas acciones no se podían aprender tan intuitivamente.

Cosa extraña: en cuanto se llegó a conocer este producto a un buen nivel, el número de llamadas para pedir soporte disminuyó notablemente.

Symantec siempre está adquiriendo empresas y productos, y uno de ellos fue Ghost. Este producto, fue pionero en clonación de equipos y pocos saben que su nombre en realidad significa "*General Hardware Oriented System Transfer*" (o Sistema de Transferencia General Orientado a Hardware).

El producto era realmente efectivo y fácil de usar, pero enfrentó muchos problemas porque se usaba de forma ilegal para clonar equipos sin considerar pagos por uso de licencia (del software de Symantec y de los programas contenidos en la imagen a clonar).

Algunos otros productos a los que se daba soporte, sin que llegasen a trascender realmente fueron:



- Norton Mobile Essentials, para administración de conexiones de red y perfiles de usuarios móviles.
- Visual C@fé, para desarrollo en Java

Características del servicio.

- El horario de atención era de lunes a viernes de 9:00 AM a 7:00 PM en días hábiles, sin interrupción para comer (había turnos para comer).

- El servicio estaba abierto, de forma gratuita e ilimitada, a todo usuario que hubiera adquirido un producto de Symantec en la República Mexicana.
- Se atendía principalmente vía telefónica y algunos pocos casos por correo electrónico.
- Se atendía en idioma español, aunque en algunas ocasiones se tuvo que dar soporte en inglés a extranjeros que radicaban en México (sin hablar bien español).
- Aunque no existían métricas formales de *Call Center*, se esperaba que se resolviera el 80% de los casos en la primera llamada.
- Se utilizaba un sistema de Distribución Automática de Llamadas (ACD, por sus siglas en inglés) con capacidad de manejar hasta 14 agentes.
- Sólo se tenían 2 agentes contestando llamadas telefónicas.
- El tiempo promedio de llamada era de 15 minutos y el tiempo promedio de espera era de 7 minutos.
- Se atendía un promedio de 150 reportes cada mes.
- Se generaba un reporte mensual, con información estadística del número de llamadas recibidas y el número de reportes (*tickets*) atendidos durante el mes.

Actividades como Ingeniero de Soporte Técnico.

- Al iniciar el día, firmarse en el equipo de cómputo, iniciar el sistema de *Call Tracking* (sistema de base de datos para registro de casos) e iniciar sesión en el sistema ACD.
- Al recibir una llamada, iniciar con el saludo estándar, definido para el servicio.
- Posterior al saludo, validar con el usuario si llama por un caso nuevo o para dar seguimiento a un caso previo.
- Si es un caso nuevo, abrir un reporte en el *Call Tracking* y recabar información personal del usuario, validar la legitimidad del software y documentar el problema reportado. Indicar al usuario el número de reporte con el que se dará seguimiento al problema.
- En base a la información proporcionada por el usuario, brindar una solución al problema, ya sea usando conocimiento del agente (experiencia), bases de conocimientos de Symantec o recreando el problema en un laboratorio.
- Guiar al usuario en la aplicación de la solución, y si es necesario, indicarle paso a paso lo que debe hacer.
- La solución propuesta y su resultado, debía ser documentada en el reporte.
- Si es para seguimiento, solicitar al usuario el número de reporte y acceder a él en el sistema de *Call Tracking.*
- Validar las acciones realizadas hasta el momento y verificar resultados.
- Si el problema aún no se resuelve, repetir el proceso de investigación/laboratorio hasta hallar una solución.
- En algunos casos, era necesario escalar el problema al soporte de Symantec en Estados Unidos, para obtener una solución aún no documentada.
- Creación del reporte estadístico mensual y presentación a Symantec.

Interacción con Symantec de México.

En aquel entonces, la oficina de Symantec de México trabajaba con 8 personas y se encontraba en Insurgentes Sur (frente al edificio de Radio Mil). Había un número cada vez más creciente de distribuidores y muchos de ellos llamaban para pedir soporte a la Mesa de Ayuda.

El área de Ingeniería en Symantec era responsabilidad del Ing. Víctor Ibáñez Lechuga y también era el encargado de monitorear el servicio proporcionado en la Mesa de Ayuda. Mensualmente, se preparaba para Symantec un reporte en PowerPoint, con estadísticas que indicaban:

- Número de reportes atendidos,
- Información de los usuarios que solicitaron servicio,
- Distribución de los reportes (por producto y por tipo de servicio).

En los primeros meses, el responsable del proyecto debía crear el reporte mensual y presentarlo a Symantec. Posteriormente, se absorbió la función de crear el reporte y el responsable lo presentaba a Symantec. Finalmente, también se absorbió la responsabilidad de presentar el reporte.

Capacitaciones.

En octubre de 1998, la Empresa inscribió a varios empleados en el curso "*Supporting Windows 95*", en las instalaciones de DuPont, uno de los clientes de ese entonces. El curso fue impartido por un instructor de la empresa Executrain y asistieron unas 15 personas.

En realidad, el curso fue pesado pues todas las tardes se tenía que ir de la oficina ubicada en el sur a la oficina de DuPont en Polanco para tomar 2 horas de capacitación. Entre el cansancio del día, y lo tedioso del curso, realmente no hubo un aprendizaje efectivo. Terminado el curso, se tenía que presentar un examen, pero el poco aprovechamiento del curso y destinar el tiempo en aprender los productos de Symantec, resultaron en un examen de certificación reprobado.

Tiempo después, conforme se iba ganando experiencia en los productos de Symantec, se recibió invitación para tomar diversas capacitaciones de productos de Symantec, impartidos por el Ing. Ibáñez. Siempre fue reconocida la labor como miembro de la Mesa de Ayuda y en varias ocasiones se terminó impartiendo dichas capacitaciones.

Otras actividades.

Como parte de un grupo de trabajo, y estando en una Empresa que atiende diversos clientes, en varias ocasiones se participó en proyectos ajenos a la Mesa de Ayuda de Symantec, siendo los más significativos:

- McDonald's

  Este proyecto atendía en modo de Mesa de Ayuda a las tiendas originales propiedad de McDonald's de México, y después se fueron incrementando franquiciatarios. Se brindaba soporte telefónico a los Gerentes de restaurante y cada mes se establecía una conexión vía pcAnywhere a cada restaurante, para descargar la base de datos con precios actualizados y promociones. Adicionalmente, se auxiliaba a los Gerentes a bajar respaldos, realizar cierre del día, enviar información de ventas al Corporativo o canalizar problemas con el reloj checador o las cajas a sus respectivos proveedores. Se inició con 15 restaurantes y creció hasta llegar a cerca de 30.

- Colgate Palmolive

  Este cliente sólo había comprado algunos servicios de mantenimiento preventivo y correctivo (atendido por otra área en la Empresa), pero debido al potencial de crecimiento que tenía esta cuenta, se decidió apoyarles en sitio en diversas contingencias de virus. En esas ocasiones, se les brindaba apoyo en sitio y se revisaban los equipos que tenían problemas de este tipo. En muchos casos se dejaban libres de virus y en algunos otros se indicaba al personal de TI cómo erradicar los virus en el resto de los equipos.

Evento de Canales de Symantec.

En Octubre de 1998, se tuvo una invitación de Symantec –junto con 2 directivos de la Empresa- al Evento Anual de Canales para Latinoamérica. El evento se llevó a cabo durante una semana en el condado de Coronado, en San Diego (California).

Durante el evento, se asistió a presentaciones de productos nuevos y algunas sesiones de entrenamiento técnico. Se convivió con otros canales de Symantec, provenientes de México, Brasil, Argentina, Uruguay y Chile.

En la cena de gala, que sirvió de clausura al evento, se entregó a InfoCorp el reconocimiento como "*VAR* del Año" (Distribuidor de Valor Agregado), no tanto por las ventas de productos de Symantec, sino por el servicio de la Mesa de Ayuda.

Asistir al evento, permitió reforzar el trato que se tenía con personal técnico y administrativo de Symantec en Estados Unidos, y así obtener, más recursos para la Mesa de Ayuda.

Principales logros.

- Ser considerado como experto en diversos productos de Symantec.
- Participar en el desarrollo y mejoramiento del servicio de la Mesa de Ayuda de Symantec.
- Atender y resolver más del 80% de los reportes.
- Mejorar la relación técnica/comercial con Symantec (México y Estados Unidos).
- Ser considerado para ser Líder de Proyecto.

Capítulo 2.
Líder de la Mesa de Ayuda de Symantec.

Período: Noviembre, 1998 a Marzo, 2000.
Jefe Directo: Lic. Araceli Arceo.

La "nueva" Mesa de Ayuda de Symantec.

Conocer el proyecto desde el principio, y ser parte operativa de él, permitió identificar áreas de oportunidad y definir procesos de mejora. La presencia de Symantec en México se iba fortaleciendo y había más demanda en el servicio.

El equipo de la Mesa de Ayuda estaba conformado ya por 3 ingenieros de soporte (incluyendo a quien esto escribe), y las características del servicio continuaban siendo las mismas. Sin embargo, la complejidad de los problemas reportados iba en aumento, así como el número de reportes mensuales, que llegó a duplicar el contrato original, quedando en 300 reportes mensuales.

Dado que se era la imagen de Symantec ante el cliente, se puso especial atención en estandarizar el esquema de atención y evitar que el usuario final recibiera un servicio diferente de cada ingeniero. Para esto, se creó un Manual de Políticas y de Procedimientos de Operación de la Mesa de Ayuda y se hizo del conocimiento del equipo, para luego aplicarlo y monitorear su ejecución.

La incorporación de los otros 2 ingenieros, permitió disminuir el tiempo promedio de espera, pero requirió de entrenamiento y experimentar sus curvas de aprendizaje. No contaban con experiencia en los productos de Symantec y no se quiso repetir el mismo proceso por el que se atravesó al inicio del proyecto, por lo que se destinaron horarios y recursos para que cada uno de los ingenieros pudiera entrenarse en los diferentes productos. De igual forma, en horarios sin excesiva carga de llamadas, se destinó tiempo para que se pudieran transmitir conocimientos de los productos y evaluar lo aprendido. Este esquema de entrenamiento permitió que, en un período relativamente corto, el nivel de servicio de la Mesa de Ayuda aumentara, y los usuarios pudieran resolver sus problemas en menos tiempo.

Como Líder del Proyecto, se tuvo facultad para establecer nuevas métricas y esquemas de evaluación a los Ingenieros e iniciar un proceso de mejora continua.

Algunas mejoras.

Desde el inicio de operaciones, el sistema de *Call Tracking* fue desarrollado internamente utilizando Lotus Notes. Aunque no se participó en el entrenamiento de Lotus Notes, se logró aprender algunas acciones de administración básica y posteriormente, desarrollar algunas mejoras al sistema.

Se incrementó el número de campos de información que debían llenarse en cada reporte, y al mismo tiempo se automatizó el llenado de ciertos campos. Esto permitió disminuir el tiempo de captura del reporte y evitó diversidad de errores tipográficos. Asimismo, se generaron nuevas vistas, que al ser exportadas, permitían obtener el reporte mensual más rápidamente.

La elaboración del reporte mensual siguió recayendo en quien esto escribe, pero se había propuesto un nuevo formato y se incrementó la información que contenía, indicando:

- Número de reportes atendidos,
- Información de los usuarios que solicitaron servicio,
- Distribución de los reportes (por producto, por tipo de problema, por tipo de solución, por distribución geográfica, por tiempo de solución)
- Tiempo promedio de llamada, tiempo promedio de espera, total de llamadas, llamadas abandonadas y llamadas perdidas.
- Problemas pendientes.
- Retroalimentación de los usuarios.

Aunque en otros proyectos en la Empresa se tenía cierta rotación de personal, en el proyecto de Mesa de Ayuda de Symantec fue casi nula. Se logró formar un equipo sólido en donde todos se sentían a gusto haciendo su trabajo.

No se dejó de atender reportes de usuarios, y aunque se atendía poco menos del 25% de los reportes, se estableció un esquema de soporte a segundo nivel, en donde se asignaban los reportes de problemas más difíciles y se liberaba a los ingenieros de estos problemas que les tomaban demasiado tiempo. En caso de que no se pudiera resolver el problema, se escalaba con el soporte de Symantec en Estados Unidos (lo que se consideraba un soporte de tercer nivel) y se daba seguimiento hasta su cierre.

El sistema de Distribución Automática de Llamadas (ACD), estaba siendo sub-utilizado hasta entonces. Se aprendió a usarlo y sacarle más provecho y así obtener más información estadística para el reporte mensual. Esto también redundó en una menor dependencia del proveedor de ACD.

Al finalizar este periodo, el proyecto de Mesa de Ayuda de Symantec, ya contaba con 5 ingenieros y se atendían un promedio de 600 reportes al mes.

Y llegó el año 2000.

Ante el cambio en los relojes de las computadoras, de 19xx a 2000, se creó cierto temor (y en algunos casos paranoia) respecto a cómo y qué tanto se verían afectadas. Hubo muchas especulaciones, y aunque sí era necesario realizar algunas verificaciones, se consideró que el problema fue mal ponderado y exagerado en su mayor parte.

Symantec no fue ajeno a todo este movimiento y desarrolló Norton 2000, un producto que prometía analizar la computadora y determinar si era "*2KY-Compliant*" (Compatible con el año 2000) o si tendría algún problema al llegar el cambio de año, en cuyo caso ofrecía remediar el problema o, por lo menos, indicar en qué consistía para que el usuario final lo corrigiera.

La Empresa vendió algunas cajas de este producto y algunos contratos de análisis y corrección para que las empresas fueran "*2KY-Compliant*", pero no se participó directamente en este proyecto.

Aunque la Mesa de Ayuda atendía sólo en horario hábil, para tan especial ocasión, el nuevo Gerente de Ingeniería de Symantec, el Ing. Rafael García Ladrón de Guevara, solicitó que se brindara el servicio de forma ininterrumpida de las 9:00 AM del 31 de diciembre de 1999 a las 7:00 PM del 1 de enero de 2000.

Se estableció el esquema de atención, considerando 3 horarios:

- de 9:00 AM a 7:00 PM del 31 de diciembre, en la Empresa;
- de 7:00 PM del 31 de diciembre a las 9:00 AM del 1 de enero, fuera de la Empresa; y
- de 9:00 AM a 7:00 PM del 1 de enero, en la Empresa.

Se asignó el primer horario a uno de los ingenieros (sólo él trabajaría el 31), el tercer horario al otro ingeniero (sólo él trabajaría el 1), y el segundo horario lo tomó quien esto escribe. Todos se reintegrarían al trabajo el día 2 de enero.

La guardia fue cubierta desde casa. Se dejaron instrucciones para que el primer ingeniero redireccionara las llamadas entrantes a la Mesa de Ayuda hacia el teléfono particular (en ese entonces no había tantos celulares) al terminar su horario el día 31. El segundo ingeniero, tenía instrucciones para deshabilitar el redireccionamiento, al iniciar su horario el día 1. El redireccionamiento fue posible gracias al sistema ACD.

La fiesta de fin de año en la familia de un servidor se iba a realizar en casa de un familiar, cerca de casa. Como no se tenía intención de pasar el año nuevo solo en casa, se conectó un largo cable telefónico y se sacó la base del teléfono inalámbrico, hasta colocarla sobre la marquesina de un vecino. El alcance del teléfono inalámbrico, permitió estar en la fiesta.

Y ahí se estaba, cargando para todos lados el teléfono inalámbrico y teniendo a mano la computadora portátil para capturar todos los reportes que llegaran. Sólo hubo 3 llamadas. La primera poco después de las 9:00 PM, y era el Ing. García, que quería verificar que el servicio estuviera activo. La segunda, un número equivocado antes de las 12:00 AM. Y la tercera, después de las 12:00 AM y aunque sí era un usuario de Symantec, sólo quería preguntar si ya había reportes de algún problema.

El 1 de enero no hubo ninguna llamada, y el ingeniero asignado para cubrir este horario pudo retirarse a su casa a las 12:00 PM (previa autorización del Ing. García).

Como se mencionó anteriormente: no había que qué preocuparse.

Actividades como Líder de Mesa de Ayuda de Symantec.

- Atención de reportes vía telefónica y por correo electrónico.
- Solución de problemas de nivel 2 y escalamiento a Symantec (nivel 3).
- Creación de procedimientos de atención a usuarios y de resolución de problemas.
- Supervisión y monitoreo de los Ingenieros de Soporte Técnico.
- Creación de planes de capacitación e impartición de los mismos al personal de la Mesa de Ayuda.
- Administración del sistema ACD Star 14, controlando el sistema para los diferentes proyectos de mesa de ayuda de la Empresa.
- Creación de reporte mensual estadístico y presentación del mismo.

Interacción con Symantec de México.

Poco a poco, se fueron mejorando las relaciones con Symantec de México (que si bien no eran malas, eran escasas) y se aumentó el contacto con Symantec Estados Unidos. La oficina de Symantec en México continuaba creciendo y el servicio de soporte técnico gratuito e ilimitado y de calidad para todos los usuarios, se convirtió en un diferencial ante los otros fabricantes de software y fue aprovechado por su departamento de Mercadotecnia, encabezado por el Ing. Roberto Massa para aumentar la penetración de la marca.

Symantec llamaba a la Mesa de Ayuda para canalizar a usuarios especiales o importantes, y para que se les diera una atención preferencial, y utilizaba las experiencias positivas para publicitar más la marca.

A lo largo de los meses, se logró establecer tal relación con Leticia Oseguera (Gerente de Producto – División Productividad para Latinoamérica) y con Francisco José Odón (Gerente de Producto – División Seguridad para Latinoamérica) que todo producto nuevo o lanzamiento de versión nueva era enviado por mensajería a InfoCorp, en lugar de ser enviado a la oficina de Symantec en México. En este sentido, se tuvo acceso al producto con nombre código “Typhoon”, y se participó como evaluador del producto antes de su lanzamiento oficial como “pcAnywhere 9.0”.

Sin crear conflicto con la oficina de Symantec en México, se empezó a enviar información a los Gerentes de Producto, acerca de cómo se comportaba cada producto o cada nueva versión, ya que ellos podían acceder más fácilmente al equipo de desarrolladores e implementar nuevas características o retroalimentar en cuanto a problemas encontrados en los programas.

Como distribuidores VAR de Symantec, se participó en el primer proyecto de renta de software de Symantec en México, que comprendía la renta del programa pcAnywhere para Colgate Palmolive y se trabajó como interfaz entre Symantec y el cliente, pues se trató de un nuevo concepto y se tuvo la responsabilidad de implementarlo en diversos equipos del cliente.

En aquel entonces, Symantec tenía subcontratadas a varias empresas para brindar el soporte a usuarios de forma local en los diferentes países de Latinoamérica. Cuando se inició la Mesa de Ayuda en México, se sabía de la existencia de la empresa Software de Plata, en Buenos Aires (Argentina) y se sabía que era el mejor proveedor de soporte de la región. Con el trabajo desarrollado en México, se logró que el servicio de InfoCorp igualara en efectividad, calidad y tiempos de respuesta al servicio proporcionado por Software de Plata. Viéndose lo anterior reflejado en el aumento de reportes que provenían de regiones fuera de México, aún a sabiendas de la existencia de otros centros regionales. El reconocimiento de parte de Symantec en cuanto a la calidad del servicio que proporcionábamos resultó aún más evidente cuando se recibió invitación para participar en un anteproyecto para brindar soporte a la región norte de Sudamérica (Colombia, Venezuela, etc.).

Casi al final de este período, Symantec reconoció la necesidad de controlar y agrupar los esfuerzos individuales de cada país de la región y todos tenían que reportar a la recién creada Gerencia de Soporte para Latinoamérica, basada en Miami (Florida). La responsable de la Gerencia era K. A. Lalsing y puso principal atención a los centros de soporte de Argentina (Software de Plata), Brasil (Symantec) y México (Grupo Sphaera).

Apoyo a Symantec.

Por la confianza que Symantec tenía en nuestra Empresa, solicitó apoyo en diversas ocasiones para representarlos en diversos eventos, siendo los más representativos:

- Entrevista en ABC Radio.

  En el programa “Así lo dice Lamont” conducido por Federico Lamont y trasmitido de lunes a viernes de 6:00 AM a 9:00 AM en ABC Radio (XE ABC 760 AM), se requería responder a una entrevista acerca del creciente problema de los virus. Para la fecha solicitada, no había personal de Symantec disponible para atender al programa, por lo que se asignó a quien esto escribe para representar la marca, sin decir que era trabajador de otra empresa.

  La entrevista se desarrolló vía telefónica. Estando en las oficinas de InfoCorp, personal de ABC Radio llamó 15 minutos antes de salir “al aire” y solicitaron permanecer en línea hasta el momento de la entrevista.

  Fue una entrevista corta (no más de 10 minutos) y se tuvo oportunidad de explicar en qué consiste un virus y cómo tomar algunas medidas de precaución para evitar infecciones o pérdidas de información. Se preguntó si se consideraba que los teléfonos celulares, que empezaban a popularizarse, podrían ser sujetos de ataques de virus. Se comentó que en el ambiente que reinaba en ese momento, los teléfonos celulares no contaban con los elementos necesarios para ser susceptibles de infección, pero que no habría que sorprenderse si

conforme fueran evolucionando los teléfonos y brindaran más funcionalidades, se empezara a ver este tipo de ataques.

No se recuerda un estado de nerviosismo ni antes ni durante la entrevista, pero la pregunta anterior no era esperada y aunque se pudo responder de forma adecuada, sí generó nerviosismo. Solicitaron un comentario final y al querer dar un mensaje de confianza a los usuarios y que no dejaran que ciertas informaciones alarmistas los preocuparan innecesariamente, se escapó la palabra "*empanicar*" (en lugar de decir "apanicar"). Hasta la fecha, es una anécdota en la familia: debut radiofónico y creación de una nueva palabra.

- Evaluación de Antivirus para la revista PC Semanal.

Esta revista especializada en Tecnologías de Información invitó a todos los fabricantes de antivirus del momento (y con presencia en México) para participar en una evaluación imparcial y poder publicar un estudio que indicara cuál era el mejor antivirus.

Nuevamente, Symantec no tenía personal disponible para esa fecha y solicitaron que se asistiera para representar la marca (una vez más, sin decir que no se trabajaba en Symantec).

Asistieron McAfee, Panda, PC Cillin, Computer Associates y Symantec. La evaluación consistía en:

- Tomar un equipo con virus y uno sin virus.
- En ambos equipos, instalar el producto antivirus.
- Ejecutar análisis contra virus en ambos equipos.
- En el equipo infectado, cada antivirus debía detectar y eliminar los virus.
- En el equipo libre de virus, una vez instalado el antivirus, se copiaría un CD con un número específico de archivos infectados, y se tomaría nota de cuántos se detectaban.

La evaluación fue considerada eficiente, pero tenía un punto de falla: no se permitía actualizar las firmas (o definiciones) que permiten a todos los productos detectar virus recientes. Todos los productos cuentan con un juego de firmas (o definiciones) de virus incluido en los archivos de instalación, pero se entiende que los CDs de instalación son creados de forma masiva por los fabricantes y que pueden tener varios lotes de producto fabricados desde meses atrás. Lo anterior fue informado a los editores antes de iniciar el proceso y comentaron que no cambiarían el esquema de evaluación. Ante la insistencia acerca de lo incompleta y parcial que podría resultar la evaluación, los editores aceptaron que todos los participantes firmasen una carta de inconformidad ante este hecho, y que se publicaría junto con la evaluación en la revista, pero que no cambiarían en nada la evaluación, pues consideraban que "un producto antivirus debe servir al 100% justo al momento de sacarlo de su caja e instalarlo… aún sin actualizarlo vía Internet".

La evaluación se realizó y los resultados fueron los que se habían previsto: ningún antivirus detectó el 100% de las muestras y el desempeño global de todas las marcas no fue superior al 70%, pues se tenían muchos virus recientes. Algunos productos tenían firmas (o definiciones) de virus de hasta 6 meses de atraso y el antivirus que menos atraso tenía era de 2 meses.

Al ver los resultados de la evaluación, parecía que ninguno de los productos antivirus servía realmente, y los editores querían publicarla indicando que el nivel de efectividad global era realmente malo. Dado que esto no era del todo correcto y retomando la carta de inconformidad, se creó una controversia entre fabricantes y editores, que derivó en la no publicación de la evaluación en la revista.

Los editores prometieron redefinir la metodología de evaluación y reprogramar la fecha de la nueva evaluación, pero este compromiso nunca fue cumplido por los editores.

Capacitaciones.

Durante algunas semanas del mes de mayo del 2000, se asistió a los cursos:

- Networking Essentials,
- Administering Windows NT 4.0,
- Windows NT 4.0 Core Technologies, y
- Windows NT 4.0 Enterprise Technologies

Impartido en instalaciones de Executrain en la Ciudad de México y pagado por la Empresa.

Para no repetir la experiencia del curso y el examen de Windows 95, se destinaron horarios para poder aprovechar al máximo las capacitaciones y tiempo para poder estudiar más los manuales del curso antes de presentar los exámenes de certificación.

Se presentaron los 4 exámenes de certificación en un centro Prometric y se aprobó cada examen al primer intento. Al finalizar el proceso de exámenes, se obtuvo la certificación “Microsoft Certified Professional” (MCP ID #2013482) que fue vigente hasta diciembre de 2001.

Principales logros.

- Mejorar el servicio de la Mesa de Ayuda, a través de la estandarización y creación de procesos.
- Duplicar el contrato mensual con Symantec.

- Equiparar el servicio proporcionado con el del mejor proveedor de la región.
- Estrechar relaciones técnicas y comerciales con Symantec.
- La certificación “Microsoft Certified Professional” para Windows NT 4.0.
- Tener el reconocimiento de Symantec para poder representarlos en los medios de comunicación.
- Ser considerado para un nuevo puesto en la Empresa.

Capítulo 3.
Ingeniero de Soporte Técnico Especializado.

Período: Marzo, 2000 a Abril, 2002.
Jefe Directo: Ing. Efraín Medina.

De soporte a usuario final a soporte para corporativos.

Después de 3 años de atender a usuarios finales (desde estudiantes hasta profesionistas, novatos y expertos) y de conocer a fondo el producto principal de Symantec (Norton Antivirus), la Empresa decidió fortalecer su presencia como Distribuidor de Valor de Agregado (VAR) de Symantec.

Hasta entonces, la actividad principal de la Empresa como VAR era vender cajas de productos o licenciamiento de los mismos, pero se definió como estrategia corporativa aumentar el portafolio de productos e incluir servicios que brindaran más valor para los clientes. Se trataba de romper el paradigma y dejar de vender productos, para empezar a vender soluciones.

En ese momento, la Empresa ya tenía destinado a otro ingeniero que se encargaba de dar estas soluciones y servicios a clientes corporativos, pero él se enfocaba sólo en productos de respaldo de información, ya que en ese entonces, InfoCorp era distribuidor de Seagate Software (con su producto estrella Backup Exec). Al ser incluido en esta nueva actividad, la Empresa buscaba robustecerse y poder ofrecer soluciones de disponibilidad (respaldo) y de seguridad (antivirus) de la información.

Meses atrás, Symantec ya había lanzado al mercado una versión de antivirus específica para corporativos y había mucha demanda del mismo. Los otros VARs de Symantec también habían robustecido sus esquemas de atención y también buscaban atacar nuevos horizontes.

El área de ventas de la Empresa ya tenía ubicados varios proyectos que requerían no sólo de un producto, sino de apoyo para poder sacarle el mayor provecho. Ahora, con 2 ingenieros que podían ayudar técnicamente, se tenía más posibilidad de atraer más negocio.

Se dejó la responsabilidad del proyecto de Mesa de Ayuda de Symantec a uno de los mejores ingenieros con los que se trabajó y que conocía a fondo la operación de la Mesa de Ayuda (pues era parte de ella). A él se le ofreció el puesto de Líder de la Mesa de Ayuda de Symantec, y sirvió como un motivador para él, y para el resto del equipo, pues demostraba que la Empresa reconocía el trabajo y el empeño de sus integrantes.

Durante algunas semanas, antes y después de la separación de la Mesa de Ayuda, se dio entrenamiento al nuevo Líder en lo relativo al uso del sistema ACD y se le proporcionó toda la documentación de control y monitoreo que se había creado hasta entonces. Aún después de la separación, se siguieron asignando algunos

casos de dificultad elevada, pero conforme el personal iba ganando experiencia, esto fue cada vez menos común.

Servicios proporcionados por Soporte Especializado.

Dado que se buscaba ofrecer soluciones, en lugar de tan sólo vender productos, se inició con la oferta de los siguientes servicios:

- Demostración de producto

La mayoría de los clientes ya conocían Norton Antivirus, pero muchos desconocían la existencia de una versión corporativa. Asimismo, muchos clientes tenían predilección por alguna otra marca de antivirus. Es por esta razón, que se ofrecía a los clientes realizar una evaluación de Norton Antivirus Edición Corporativa, en un ambiente controlado y limitado, dentro de sus instalaciones. La idea, era que conocieran el producto y pudieran verlo trabajando en sus equipos. Así podían medir qué tanto afectaba el desempeño de los equipos, y sobre todo, qué tanto los protegía.

En muchos casos, los usuarios demostraban renuencia o desinterés en la evaluación, pero al trabajar en conjunto (vendedor-técnico) se lograba ganar el interés del cliente y en muchas ocasiones, se logró cerrar la venta.

- Instalación

Una vez que el cliente adquiría la solución, se podía hacer la instalación del producto en los servidores y estaciones de trabajo de su red. Lo que garantizaba a los clientes la rápida y eficaz implementación del producto en su red.

La instalación podía hacerse de forma local (visitando equipo por equipo) o de forma remota (usando *login scripts*, distribución remota o software de control remoto).

Para la instalación, se enviaba primero al cliente los requerimientos de instalación y una vez que confirmaba tenerlos, se agendaba la visita de instalación.

Parte de los problemas que se encontraban durante la instalación, eran ocasionados por falta de espacio en disco duro, daños en el sistema operativo Windows, infecciones de virus o problemas con otros antivirus instalados previamente.

- Capacitación

Aunque los productos siempre cuentan con un manual de usuario, es una realidad que la mayoría de los clientes no tienen el tiempo necesario para poder leerlos en su totalidad o se tiene presión de tiempo para implementar alguna solución o cambio.

Por esta razón, se ofrecía a los clientes un programa de capacitación que les permitiera conocer el producto en poco tiempo y obtener beneficios de él en el corto plazo.

La capacitación podía darse en las oficinas de InfoCorp o en las instalaciones del cliente.

- Soporte Técnico

Independientemente de si el cliente había instalado por su cuenta el producto, o si InfoCorp lo había instalado, e incluso, sin ser obligatorio haber comprado el producto a InfoCorp, se podía ofrecer soporte telefónico, vía correo o en sitio, para resolver problemas derivados de la instalación, configuración, uso y migración del producto.

Para casi todos los clientes que compraban el producto, se ofrecía soporte telefónico como valor agregado (sin costo para el cliente).

El caso Funlove.

En esa época, se inició trato con diversas empresas, con muchas de las cuales, aún al final del período de trabajo en InfoCorp se mantenía relación de trabajo. A continuación dos ejemplos de ellas, en las cuales, gracias al virus W32.Funlove.4099, se cerró negocio; y un ejemplo de un negocio que no se logró, pero que generó aprendizaje.

- Qué hace el virus Funlove.

Este virus, ataca archivos EXE, SCR y OCX en sistemas Windows 95, Windows 98, Windows Me, Windows NT, Windows 2000, Windows XP y Windows Server 2003.

El código del virus, mide 4099 bytes (de ahí su nombre) y fue uno de los primeros virus en atacar vulnerabilidades de seguridad de Windows, así como en instalarse como servicio en Windows NT.

El proceso viral principal, llamado FLCSS.EXE era responsable de infectar todos los archivos EXE, SCR y OCX del equipo, y además, se encargaba de hacer un barrido a la red corporativa para encontrar equipos con carpetas compartidas sin protección y una vez localizados,

se inyectaba a los archivos del equipo remoto. Aún en carpetas compartidas con contraseña, Funlove es capaz de inyectarse explotando una vulnerabilidad en el sistema de seguridad de Windows.

Las versiones de Norton Antivirus anteriores a la 7.3, se veían afectadas por la forma de ataque de este virus, pues éste es capaz de hacer creer al sistema operativo, que los archivos infectados por él no han sido modificados. NAV revisaba sólo aquellos archivos que el sistema operativo reportaba como modificados (para no afectar el desempeño del equipo). Este tipo de protección no era útil ante esa nueva forma de ataque, lo que originó que Symantec rediseñara el producto y en la versión 7.3, NAV revisaba ya todo archivo que hubiera sido leído o escrito en disco duro (aún si el sistema operativo indicaba que no había sido modificado).

Este virus no es destructivo, pero puede causar lentitud en el equipo de cómputo (todos los archivos EXE son más grandes, y en consecuencia, se usa más memoria) y puede saturar de tráfico una red, hasta hacerla casi inservible (por la infección vía red). Hasta la fecha, hay muchas empresas que aún tienen problemas con este virus.

- Demostración en Grupo Nacional Provincial

Se inició negociación con el personal de TI de esta empresa de seguros, y aunque el área es responsabilidad de la empresa EDS, aceptaron hacer una evaluación de Norton Antivirus en la red (en ese entonces, se tenía como estándar corporativo el antivirus de McAfee).

Se instaló NAV en algunos servidores, una consola y algunas estaciones de trabajo en un ambiente productivo de sus oficinas al sur de la ciudad (Taxqueña). Durante varios meses, se estuvo evaluando el producto, y hubo varios problemas de comunicación y desinterés por parte de EDS.

Después de diversas actividades y de ir avanzando poco en la evaluación formal de NAV, se recibió un llamado urgente de EDS, pues la red de GNP estaba colapsando por un virus que McAfee no detectaba. Se atendió en sitio, y después de investigar, se encontró que los equipos instalados con NAV no se habían infectado, pues detectaban y eliminaban el virus sin problemas.

Ante este escenario, y después de varias reuniones con EDS se acordó instalar más equipos en modo demostración (incluyendo servidores de producción) y si se observaba que la infección se controlaba, se haría la adquisición del producto.

Se coordinaron esfuerzos con el personal de EDS y después de algunos días de realizar instalaciones de NAV, se observó estabilidad en las áreas más críticas de la red y que los equipos con NAV no se infectaban. Obviamente, McAfee quiso hacer su labor para no ser removidos de la cuenta, y aunque hicieron esfuerzos para que su producto detectara el virus, en muchos casos se volvían a infectar después de un tiempo.

EDS recomendó el cambio de antivirus hacia NAV e InfoCorp pudo vender licenciamiento para 5000 nodos (ver sección “El caso Grupo Nacional Provincial” más adelante en este capítulo).

- Soporte a Sabritas

Con este cliente no se había iniciado ninguna negociación, ni se tenían referencias de él. Sin embargo, Symantec recibió una llamada de su parte, solicitando apoyo para atender una contingencia de virus; Symantec canalizó a InfoCorp con este cliente y se asistió a sus oficinas para ver cuál era el problema.

En una de sus oficinas (Zona Rosa), tenían una infección masiva de Funlove y servidores críticos para la operación diaria estaban siendo afectados por él. No contaban con un antivirus en los equipos y había muchas carpetas compartidas sin protección en la red.

Se instaló un servidor NAV y una consola, y se inició con la desinfección de algunos equipos y servidores. En estaciones de trabajo, no hubo mayor problema, pero en algunos servidores, era necesario reiniciar para completar la instalación de NAV y no se podía asignar una ventana de tiempo en el corto plazo. Los servidores tenían arreglos RAID 5 y no se podían desmontar los discos duros para realizar el análisis contra virus y desinfección de los mismos.

Ante este escenario, se definió un método alternativo de eliminación (en parte automatizado y en parte manual), el cual resultó efectivo, pero demoraba unas 3 horas por servidor (pues había que hacer un análisis a fondo). Al comentar esta alternativa con el responsable de TI, decidió que no podían darse el lujo de gastar 3 horas por servidor. El personal de TI, sugirió entonces formatear los servidores y restaurarlos usando respaldos anteriores (lo que les llevaría menos de 2 horas por servidor) y una vez restaurados, les instalarían NAV para evitar que se contaminaran con el virus.

Se verificó el proceso con ellos en unos 3 servidores, y al ver que era funcional, decidieron replicarlo en los demás servidores. Después de 2 días, la red estaba estable, sin virus y con NAV instalado en los equipos. Ese mismo día, enviaron a InfoCorp su orden de compra para 100 nodos de NAV.

- Demostración a Seguros Comercial América.

Dado que ya se estaba teniendo contacto con GNP, Symantec asignó a InfoCorp para dar una demostración en esta otra empresa de seguros. Se asistió a las oficinas del cliente (Insurgentes Sur) y comentaron que tenían ya 2 días sin poder trabajar, y que la red estaba apagada definitivamente, pues se reinfectaban cada vez que conectaban un equipo a la red.

No se recuerda cuál antivirus tenían instalado, pero el Gerente de Soporte odiaba la marca Symantec. Sólo aceptó la demostración, porque la Directora de TI se lo indicó. Se asignaron equipos de laboratorio (aislados de la red principal) y se nos dejó trabajar hasta que terminásemos la instalación. En ese momento, el Gerente infectó intencionalmente uno de los equipos de prueba y NAV lo pudo reparar sin problemas. Al ver esto, se decidió hacer pausa para comer. Al regresar, todos los equipos del laboratorio estaban ya infectados con Funlove aún teniendo NAV activo.

Se repitió el proceso de desinfección y mientras se estuvo ahí, no se reinfectaron. Se cerró el aula de pruebas y al otro día que se regresó para finalizar la demostración se encontró que todos los equipos estaban infectados otra vez.

Ante esto, se empezó a sospechar del Gerente de Soporte, y se llegó a pensar que durante la ausencia, él había detenido los servicios de NAV e infectado los equipos. Se decidió recopilar evidencia de lo sucedido y fue extraño no encontrar nada anómalo. Mientras se hacía esta investigación, los equipos se volvieron a infectar sin que nadie hubiera hecho nada.

Después de mucho analizar, y de hacer conferencias telefónicas con Symantec (en México y en Estados Unidos), se llegó a la conclusión de que NAV no revisaba los archivos que ya habían sido infectados (pues el virus reportaba al sistema operativo que no había modificado el archivo) y por eso se reinfectaban los equipos.

Symantec liberó muy rápidamente la versión 7.3 de NAV y se pudo instalar en la red de prueba del cliente. El resultado, ahora sí, fue contundente: no había reinfecciones (y se dejó de sospechar del Gerente).

Al Gerente y a la Directora, les encantó la solución y comentaron respecto a hacer pruebas en producción mientras se comenzaba a tratar el tema comercial. Sin embargo, al validar la estructura de su red, informaron que el 80% de sus servidores ejecutaban servicios de Terminal. La versión de NAV no soportaba esta característica y no permitía su instalación.

Symantec no pudo ofrecer un tiempo válido de solución a este inconveniente y el cliente tomó la decisión de no comprar NAV, pues no podría usarlo en la parte más importante de su red.

No se ganó este cliente, pero se aprendió mucho acerca del mecanismo de infección del virus y se generó una corrección en la forma de trabajar de NAV.

Los productos soportados.

En ese entonces, Symantec tenía agrupados los productos de seguridad antivirus en un paquete para licenciamiento corporativo que terminó siendo denominado Symantec Antivirus Enterprise Edition (SAV EE) versión 8.5, que incluía los siguientes productos:

- Symantec Antivirus Corporate Edition 8.0 for Workstations and Net Servers (incluye Symantec System Center)

Este producto debía instalarse en los servidores y en las estaciones de trabajo de la red, para protegerlos contra un eventual ataque de virus (por correo, por red, por discos flexibles, etc.) y estaba orientado a los sistemas operativos más recientes en ese momento.

La instalación del producto en estaciones de trabajo, requería Windows 98 / 98 SE / Millenium / NT 4.0 (Workstation-Server-Terminal Server) con Service Pack 6a / 2000 (Professional-Server-Advanced Server) / XP (Home- Professional). Este producto protegía únicamente al equipo en donde se encontraba instalado.

Adicionalmente, se requería instalar un servidor SAV, que es el encargado de administrar a los clientes SAV y enviarles definiciones de virus, y recibir alertas e historiales. Este producto requería Windows NT 4.0 (Workstation-Server-Terminal Server) con Service Pack 6a / 2000 (Professional-Server-Advanced Server) / XP Professional. En este mismo equipo (o uno de características similares) podía instalarse la consola de administración de SAV, llamada Symantec System Center, que funcionaba como un visor que permite controlar y conocer el estado de la red antivirus instalada.

La ventaja de la solución, es que un servidor SAV no necesariamente tiene que ser un equipo con HW o SW de servidor (podía usarse una PC) y los servidores verdaderos, podían instalarse como clientes SAV. Esto era una ventaja, pues no se requería que el cliente adquiriera más servidores para la administración de SAV y no se saturaban a los servidores existentes con funciones adicionales de SAV.

La versión 8 de SAV no era compatible con Windows 95, por lo que se tenía la alternativa de usar la versión 7.6 que sí podía ser instalada en este sistema operativo. A pesar de ser versiones diferentes, todo podía ser administrado usando la versión más reciente en servidores y consola.

También podían protegerse servidores Novell que ejecutaran Netware. En este caso, la instalación de SAV siempre era como servidor SAV (aunque no fuera a administrar clientes).

La gran mayoría de los clientes sólo adquirían esta solución, dejando de lado las otras opciones de protección; en parte por desconocimiento de la existencia de dichos productos y en parte porque no contaban con presupuesto adicional.

- Symantec Antivirus/Filtering 3.0 for Microsoft Exchange 2000

Este producto, brinda protección antivirus y filtrado de contenido para correo electrónico basado en Microsoft Exchange versión 2000 exclusivamente. Se instala en el mismo servidor de correo electrónico y funciona como un servicio anexo a Exchange.

La función antivirus permite que el correo entrante o saliente se encuentre libre de virus, lo que se traduce en una mayor seguridad, menor uso del ancho de banda, de espacio en disco y de tiempo de procesador en el servidor de correo.

La función de filtrado de contenido, permite al administrador definir qué tipo de información se desea permitir o bloquear en el correo electrónico. El filtrado se puede realizar en base al nombre o extensión del archivo adjunto, por remitente, por destinatario o por alguna palabra en el cuerpo o asunto del mensaje. Principalmente, se utilizaba la opción de filtrar por tipo de archivo, para bloquear la recepción de archivos susceptibles a ser atacados por un virus (EXE, COM, SCR, VBS, BAT, PIF) y así proveer protección desde el primer momento, aún para virus nuevos o desconocidos (y no tener que esperar hasta que sean liberadas las definiciones de virus que evitarán que el virus entre a la red). Adicionalmente, se puede restringir el envío o recepción de ciertos mensajes que no se desean manejar, ya sea porque pueden resultar en distracción para el personal (chistes, cadenas, oraciones) o porque pueden consumir demasiado ancho de banda (música, video, presentaciones multimedia).

- Norton Antivirus 2.1 for Microsoft Exchange 5.5

Funciona bajo el mismo esquema que el producto anterior, pero orientado a la versión previa de Exchange. Las funcionalidades de filtrado de contenido, son muy limitadas en esta versión (no se puede filtrar por tipo de archivo).

- Symantec Antivirus/Filtering 3.0 for Domino (Windows NT/2000)

Con las mismas funciones que el producto para Exchange 2000, pero para instalarse sobre el servidor de Lotus Domino. Puede proteger y revisar contra virus las bases NSF (tanto de correo como de otros tipos).

- Symantec Antivirus 3.0 for SMTP Gateways

Para los casos en los que el cliente no cuente con servidor Exchange o de Lotus Domino (por ejemplo algún sistema basado en Linux), la protección antivirus y de filtrado de contenido se instala en un equipo Windows que no tendrá otra función más que la de recibir el correo de Internet (ya sea por DNS o directo del Firewall), analizarlo, aplicar las reglas definidas y entregar el correo – filtrado y libre de virus- al servidor de correo.

Esta protección tiene la ventaja de que se libera de carga administrativa al servidor de correo (incluso si es Exchange o Lotus Domino) y se garantiza que el servidor de correo siempre recibirá correo limpio, lo que se traduce en un menor uso de procesador, de ancho de banda y de espacio en disco duro.

A este producto, se le considera protección perimetral y es el primer punto de revisión contra virus y para filtrado de correo electrónico en la red.

- Symantec Web Security 2.5

Para complementar la protección perimetral, se cuenta con este producto que permite analizar contra virus el tráfico HTTP y FTP entrante de Internet. Asimismo, permite definir y controlar qué sitios Web visitan los usuarios, ya sea a través del uso de categorías predefinidas por Symantec (Alcohol, Drogas, Sexo, Violencia, Entretenimiento, Vehículos, Chat, Armas, Noticias) o basándose en el contenido de las páginas Web.

El uso de categorías, simplifica enormemente la administración del control de sitios a los que se dará o negará acceso a los usuarios, ya que no hay necesidad de estar capturando manualmente cada sitio Web que se desea controlar. Symantec alimenta cada categoría con las direcciones de los sitios Web que sus investigadores van encontrando en Internet, por lo que el producto se actualiza en listas de sitios Web tal y como se actualiza en las definiciones de virus que permiten detectar y eliminar los nuevos virus. Una desventaja que tiene el uso de las listas, es que en su mayoría están orientadas al mercado de Estados Unidos, y algunos sitios regionales no se encuentran en las categorías (aunque pueden ingresarse manualmente por el administrador).

Otro mecanismo de filtrado de contenido es el llamado "Reconocimiento Dinámico de Documentos" (DDR, por sus siglas en inglés). Algunos otros productos de filtrado Web, permiten definir palabras que se consideran como "prohibidas", de tal forma que cuando algún usuario está por ver alguna página Web que contiene por lo menos una ocurrencia de las palabras "prohibidas", el sistema la bloquea completamente. En el caso de Symantec Web Security, se definen las palabras prohibidas y se tienen diccionarios predefinidos por Symantec (que se actualizan periódicamente al igual que las categorías de URL) y el administrador puede definir sus propios diccionarios. A diferencia de los otros productos, Symantec Web Security asigna un valor a cada palabra "prohibida" y va sumando puntos por cada ocurrencia. El administrador, define un valor máximo para DDR y si la suma de puntos de las palabras encontradas es inferior a él, entonces la página Web es desplegada; si por el contrario, la suma es mayor al valor definido por el administrador, la página Web no es mostrada.

DDR permite mejorar el control acerca del contenido de una página Web, pues al analizar todo el contexto de la página Web (y no sólo la ocurrencia única de una palabra restringida) se disminuye el número de falsos positivos. Como ejemplo se puede tomar a un usuario que desea llenar un formulario de inscripción a un curso, y la página Web contiene

las palabras “Nombre”, “Edad”, “Sexo”, “Nacionalidad”. En un sistema de filtrado Web tradicional, al encontrarse la palabra “Sexo”, se determinaría que la página es de contenido no deseable y no se mostraría al usuario. En el caso de Symantec Web Security, se encuentra la palabra “Sexo” y se suma el valor asignado a esa palabra, se continúa analizando el resto de la página Web, y al no encontrar más palabras restringidas, se compara el resultado de la suma contra el valor asignado por el administrador. Dado que sólo hubo una ocurrencia de una palabra restringida, el resultado de la suma es inferior al valor definido y la página Web se muestra al usuario.

Para el caso de que un usuario realizase una búsqueda en algún sitio Web especializado en búsquedas o si encontrara una página de contenido no deseable, pero que no está listada aún en las categorías de Symantec Web Security, DDR irá sumando los valores de las ocurrencias de las palabras restringidas y el resultado de la suma será mayor que el valor definido por el administrador, y en consecuencia, la página Web no se mostrará al usuario.

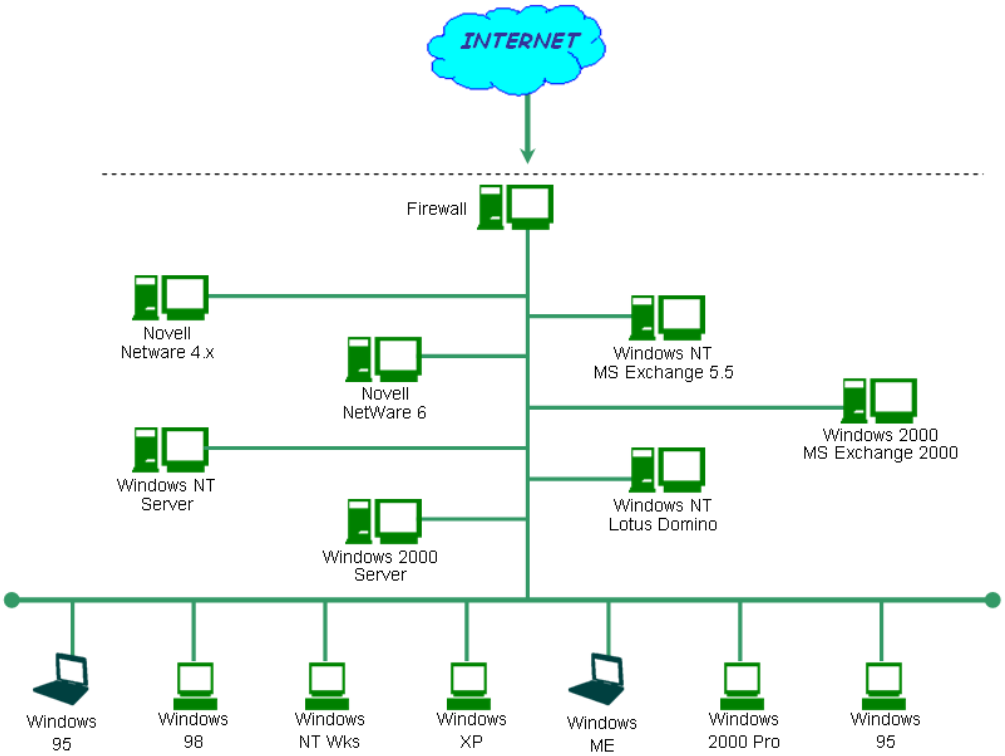


Figura 1. La red ANTES de implementar Symantec Antivirus EE.

La Figura 1, muestra una red típica, en donde se tienen diferentes sistemas operativos y se cuenta con diversos sistemas de correo electrónico. Se tiene un *firewall* para proteger la red del mundo Internet.

En todos los niveles de esta estructura, se puede instalar algún componente de Symantec Antivirus Enterprise Edition, sin que sea obligatorio instalar toda la suite de productos.

La instalación de SAV CE en los equipos clientes, puede realizarse vía *login script* (Windows 98/ME) o desde una consola central (Windows NT/2000/XP). Para mantener protegidos a los equipos con sistemas operativos "descontinuados", se complementa la solución antivirus con NAV CE 7.6.

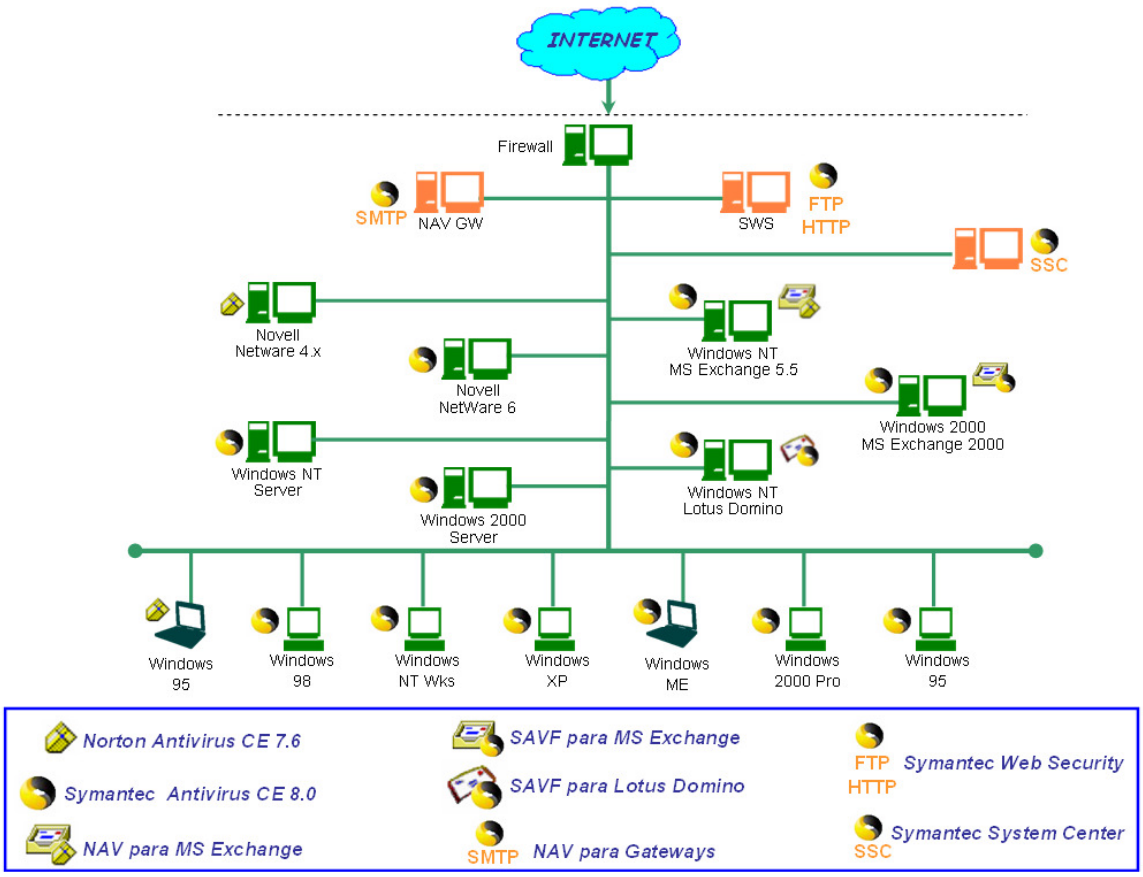


Figura 2. La red DESPUÉS de haber implementado Symantec Antivirus EE.

En la Figura 2, se observa en dónde se han instalado los productos de SAV EE. Tanto las estaciones de trabajo, como los servidores, tienen instalado SAV CE o NAV CE. Los servidores pueden instalarse como "Servidores SAV CE" o como "Clientes SAV CE", según se requiera. Los servidores de correo electrónico, tienen instalado SAV CE para proteger su sistema operativo y además tienen instalado el antivirus correspondiente al sistema de correo electrónico. Para proteger el tráfico proveniente desde Internet, se necesita agregar a la red 2 equipos que se encargarán de revisar el tráfico SMTP, FTP y HTTP.

Toda la estructura se controla a través de un equipo, en donde se instala la consola de administración, llamada Symantec System Center y desde donde pueden accederse las consolas de los demás productos, usando un navegador de Internet.

El caso Grupo Nacional Provincial.

En este proyecto se tuvo una gran participación en conjunto con personal de Symantec. Las actividades desarrolladas iniciaron incluso antes de la separación de la Mesa de Ayuda. El proyecto se dividió en dos etapas.

La primera parte correspondió a la preparación, planeación de la instalación y pruebas de funcionamiento. Cuando se iniciaron actividades, se usó la versión 7.0 de NAV y conforme se fue avanzando, se fueron usando las versiones más recientes.

Dentro de esta primera fase, se hicieron pruebas instalación remota vía *login script*, pero tenía que probarse también la desinstalación remota del antivirus anterior (McAfee). Se realizó el diseño de la estructura de solución NAV (definición de servidores y clientes) y uso de la Cuarentena Central. Se hicieron pruebas de funcionamiento en diversas plataformas (servidores Novell, Windows NT, Lotus Notes, Clientes Windows 95) tanto en ambiente de prueba como en ambiente productivo, a fin de determinar si no había problemas de convivencia con las aplicaciones usadas por GNP.

El plan de instalación debía contemplar la instalación de NAV en 100 servidores Windows NT. InfoCorp realizaría un porcentaje de las instalaciones y enseñaría a EDS el proceso, a fin de que ellos lo replicaran y abarcaran todos los servidores.

También se realizaron pruebas de funcionamiento y desempeño en los servidores de correo basados en Lotus Notes sobre Windows NT. En este caso, GNP utilizaba el antivirus de Trend, pero no tenía la efectividad requerida.

Al mismo tiempo, se seguían con pruebas en los clientes y se encontraron algunas incidencias, tales como problemas de desempeño en equipos muy viejos o dañados en su sistema operativo, o incompatibilidad con un programa de manejo de audio. En todos los casos, se pudo comprobar que los problemas no eran imputables al antivirus y hubo alternativas de solución. Hubo un error relativo al antivirus en conjunción con el cliente de Lotus Notes y Symantec confirmó que era un problema en la versión de NAV, el cual fue corregido y probado exitosamente. También fue necesario realizar ajustes al sistema de Cuarentena Central a fin de optimizar su funcionamiento.

Al iniciar trato con personal de EDS, se mostraban reacios a aceptar la solución propuesta y tenían cierto recelo del personal de InfoCorp. Poco a poco, y con trabajo constante, profesional y bien documentado, se logró ganar la confianza de los involucrados en las diferentes áreas de TI administradas por EDS.

La segunda fase de este proyecto ya no pudo ser desarrollada por InfoCorp, pues EDS logró una renegociación del contrato anterior con GNP, y se incluyó la migración a NAV en la totalidad de equipos de la red de GNP. InfoCorp solamente brindó asesoría técnica para el proceso de migración y se capacitó al personal de EDS para poder administrar la solución de forma adecuada.

Algunos clientes.

Para finales del 2001, la cartera que InfoCorp manejaba contaba con la presencia de clientes de todos tamaños y de diversos ramos:

- Aceros Cuatro Caminos (20 nodos)
- Adidas De México (90 nodos)
- Asesores Libres Para Empresas (10 nodos)
- Celanese Mexicana (940 nodos)
- Colegio Suizo (58 nodos)
- Colgate Palmolive (800 nodos)
- Cosbel L´Oreal (421 nodos)
- Ekco (10 nodos)
- Fundación Mexicana Para El Desarrollo Rural (50 nodos)
- Gedas North America (4000 nodos)
- Grupo Idesa (100 nodos)
- Grupo Interdom (45 nodos)
- Grupo Nacional Provincial (5000 nodos)
- Ici Mexicana (70 nodos)
- Instituto Mexicano Del Petróleo (4500 nodos)
- Instituto Nacional De Psiquiatría (50 nodos)
- Kmpg Cárdenas Dosal (2500 nodos)
- McDonald´s (36 nodos)
- Naviplastic (11 nodos)
- Nextel (450 nodos)
- Nissan Mexicana (916 nodos)
- No Sabe Fallar (Bic) (200 nodos)
- Pepsi Gemex (236 nodos)
- Posadas (1550 nodos)
- Sabritas (1200 nodos)

Principales logros.

- Conocer y dominar la suite de productos de Seguridad de Symantec.
- Aumentar el nivel de ventas de la Empresa al promocionar nuevos servicios.
- Mejorar los niveles de descuento y de apoyo por parte de Symantec hacia la Empresa.
- Iniciar relaciones con clientes corporativos y establecer contratos de corto y mediano plazo.
- Ser considerado para ocupar un puesto de supervisión en la Empresa.

Capítulo 4.
Supervisor de Soporte Técnico Especializado.

Período: Abril, 2002 a Junio, 2003.
Jefe Directo: Ing. Efraín Medina.

Nuevas definiciones.

Con la familia de productos de Symantec ya aprendida y teniendo conocimiento de las necesidades y requerimientos de los clientes corporativos (tomando muchas experiencias del caso GNP), se tuvo oportunidad de plantear un nuevo esquema en los servicios proporcionados por InfoCorp, el cual fue aceptado por el área de Ventas y la Dirección de la misma.

Ahora, ya se contemplaba como "Proyecto de Seguridad Antivirus", que constaba de varias etapas:

1. Análisis Inicial

Tiene por objeto conocer la infraestructura tecnológica del cliente y así proponer una solución confiable de protección contra virus. En esta etapa se requiere de un diagrama de red del cliente, en donde se indiquen claramente cuántas localidades tienen, la velocidad y tipo de enlace que existe entre ellas; por localidad se requiere saber cuántos servidores hay, sobre qué sistema operativo, con qué configuraciones, qué aplicaciones tienen instaladas y cuántas estaciones de trabajo y qué sistemas operativos tienen. De igual forma, se requiere saber el tipo de correo electrónico que se tiene y la infraestructura existente para la salida a Internet.

Se hará llegar al cliente los requerimientos de instalación (configuraciones, *Service Packs*, cuentas de usuario, etc.) para que éste confirme si cuenta con ellos o no. En caso de no cubrirlos, es responsabilidad del cliente realizar las actividades necesarias para que dichos requerimientos se cumplan. El cliente deberá informar si actualmente cuenta con alguna versión de software antivirus en los equipos contemplados para la instalación.

Se le pedirá al cliente que indique cuál es la disponibilidad que puede tener para la implementación y qué ventanas de tiempo pueden ofrecer (de forma general).

Se deberán establecer puntos de contacto, tanto de InfoCorp como del cliente, y conocer quiénes estarán involucrados en el proyecto (realizar un pequeño directorio).

2. Planeación

En base a la información recopilada en la etapa de Análisis Inicial, se creará una propuesta del plan de trabajo que se seguirá. Dicha propuesta se presentará al cliente y se ajustará de acuerdo a sus observaciones, de aquí, se obtendrá un plan de trabajo definitivo, que será aceptado por escrito por el cliente y por todos los involucrados en el proyecto, y en el que se definirán también los responsables de llevar a cabo las actividades mencionadas en el plan de trabajo definitivo.

Se presentarán al cliente los documentos que se utilizarán durante el proyecto y cómo se irá capturando la información relativa al proyecto (control de cambios por servidor, bitácoras, avances en la instalación, etc.).

De igual forma, se presentarán los elementos de control que se usarán y cómo se manejarán las situaciones en las que alguna actividad se retrase.

3. Instalación

Esta etapa del proyecto se refiere a la inserción del software antivirus en los equipos definidos durante la etapa 1 siguiendo el plan de trabajo de la etapa 2.

Symantec Antivirus será instalado de acuerdo al diseño de la solución generado en la etapa 1. El cliente puede elegir la opción de que se instale el 100% de equipos de su red o sólo que se instale en un grupo piloto y que de ahí se derive una capacitación a su personal para que ellos se encarguen de realizar toda la instalación. Si el cliente decide que se instale el 100% de equipos, el cliente deberá proporcionar un inventario detallado de los equipos por localidad, a fin de tomarlo como referencia e ir marcando los avances en la instalación. En cualquiera de los dos casos, se proporcionará capacitación respecto a la instalación al personal operativo y/o de soporte del cliente, a fin de que ellos mantengan la integridad de la base instalada.

En esta etapa, deberán considerarse tiempos y procesos definidos en la etapa 2. La instalación para los equipos clientes puede realizarse de forma remota (desde la consola, sólo para Windows NT y 2000), automática (vía *login script*) o manual (físicamente equipo por equipo). En el caso de servidores, se puede realizar la instalación remota o manualmente (en algunos casos será necesario reiniciar el servidor).

Dentro de esta etapa, se parte del supuesto que la red del cliente no presenta una infección masiva de virus, ya que eso puede interferir en los tiempos contemplados en la planeación. En caso de que sí se tenga una incidencia masiva de virus, se deberán contemplar tiempos y recursos diferentes a los que se tendrían sólo con la instalación de SAV (durante la etapa de planeación, el cliente debe indicar si tiene una infección masiva).

Para el caso de módulos adicionales (protección antivirus para correo electrónico y/o tráfico Internet) se definirá también si se realizarán todas las instalaciones o sólo una parte proporcional de equipos.

Durante esta etapa, se creará la estructura lógica de Protección Antivirus y se verificará que los equipos clientes "hereden" la configuración y definiciones de virus de su servidor Padre. De igual forma, se implementará la solución de Cuarentena Central y envío automático de muestras de virus (si el cliente lo desea).

En el caso de que se realice la instalación del 100% de equipos, conforme se vaya avanzando en el proceso de instalación, se hará del conocimiento del cliente dicho avance y éste irá firmando de conformidad las fases que se vayan cubriendo. Si por alguna razón, alguno de los equipos (que ya se hayan instalado y que el cliente haya verificado y firmado de conformidad) presenta algún problema (falla de hardware, reinstalación de sistema operativo, etc.) que amerite la reinstalación de NAV, el cliente será responsable de realizar dicha re-instalación (apoyándose en la capacitación que se proporcionó a su personal operativo y de soporte).

Al finalizar esta etapa, se entregará al cliente una memoria técnica, en la que se incluirá toda la documentación relativa al proyecto, que podrá incluir algunas recomendaciones. El cliente será responsable de implementar todas sus políticas de protección antivirus a través de la consola de administración, a menos que haya contratado el servicio de Implementación.

4. Implementación

Esta etapa comprende la implantación de las políticas de protección antivirus en los elementos de la red para que la solución funcione de acuerdo a las necesidades del cliente. Puede utilizar la información y requerimientos del cliente (etapa 1) o puede ser el fruto del proceso de Consultoría (si el cliente lo contrató).

Durante esta etapa, se configurarán los servidores de antivirus, clientes, antivirus de correo electrónico y de tráfico de Internet de acuerdo a las políticas de protección antivirus sugeridas por InfoCorp o definidas por el cliente. De igual forma, se personalizarán los mensajes de alertas, correos electrónicos o errores, que el cliente requiera (en los casos que aplique). Por último, se configurará el sistema de alertas de acuerdo a los requerimientos y necesidades del cliente.

Al finalizar esta etapa, se entregará al cliente una memoria técnica en la que se incluirá toda la configuración de la solución Antivirus (políticas), que podrá incluir algunas recomendaciones.

Asimismo, la gama de servicios ofrecidos, fue mejorada y se aumentaron algunos más, tales como:

- Consultoría

En este servicio, el cliente dará a conocer sus necesidades específicas de protección antivirus y se generarán políticas de protección antivirus (o se mejorarán las existentes), se harán recomendaciones y en los casos en los

que sea factible, se podría buscar la optimización de procesos. Este servicio puede realizarse durante la etapa de Análisis inicial.

Al finalizar el análisis de la información, se entregará por escrito al cliente las políticas, recomendaciones o mejoras encontradas durante el proceso.

Es responsabilidad del cliente implementar las políticas, mejoras o recomendaciones sugeridas; a menos que el cliente haya contratado la Implementación, en cuyo caso, personal de InfoCorp se encargará de dejar plasmadas en los servidores de antivirus, clientes, antivirus de correo electrónico y de tráfico de Internet dichas políticas, recomendaciones o mejoras y asegurarse de su correcto desempeño.

Este servicio no es un servicio que el cliente deba tener contratado de forma permanente, sino que lo contratará según sus necesidades (por evento).

- Soporte Técnico

Tiene por objeto auxiliar al cliente cuando se presente algún problema con el software antivirus. Si el cliente contrata este servicio, se definirán métodos de atención y tiempos de respuesta.

En ningún caso se resolverán problemas relativos al hardware. Si se detecta que el problema es relativo al hardware, se indicará al cliente cuál es el problema para que éste último pueda canalizarlo al proveedor correspondiente. Una vez resuelto el problema de hardware, se puede brindar apoyo al cliente para verificar que el problema ha sido resuelto.

El soporte técnico puede tener diferentes modalidades:

- Telefónico
- En sitio
- Por evento
- Por período de tiempo (con base a un número de eventos o con eventos ilimitados)
- 5 X 9
- 7 X 24

Se realizará un directorio que incluirá todos los puntos y formas de contacto entre las partes involucradas en el proyecto, a fin de optimizar la comunicación.

Si el cliente contrata el servicio de Soporte Técnico, se considerará como fecha de inicio del contrato la fecha en la que se inicie labores (Instalación y/o Implementación) en las instalaciones del cliente y se indicará cuál es la fecha de término de este servicio, todo eso será debidamente documentado para que sea del conocimiento de todas las partes involucradas.

El servicio de Soporte Técnico considera apoyo al cliente en el caso de contingencias de virus, más no implica que InfoCorp será responsable de la

erradicación del virus en la red del cliente. El apoyo que se proporciona en estos casos, es información relativa al virus y cómo evitar que se siga propagando, procedimientos de eliminación, envío de herramientas de eliminación del virus (en los casos en los que Symantec las genere) y capacitación al personal operativo y/o de soporte técnico en la erradicación del mismo.

Los eventos de virus que se presenten durante el período de instalación, no serán considerados como puntos en contra para dar por terminada la etapa de Instalación y serán atendidos de forma independiente a dicha etapa. Es decir, si el cliente encuentra problemas en el uso diario del software, sobre equipos en los que ya se finalizó la etapa de instalación, podrá estar tranquilo ya que se verificará cuál es el problema y se corregirá, sin importar que todavía falten equipos por instalar.

Se recomienda que el cliente contrate este servicio en alguna de sus modalidades por algún período de tiempo (de acuerdo a sus necesidades).

- Capacitación

Se podrá capacitar a un número determinado de personas en el uso de Symantec Antivirus en sus diferentes versiones, contemplando temas como:

  - Instalación
  - Administración
  - Resolución de problemas a nivel básico
  - Uso de la herramienta

Se proporcionará material de consulta (manuales o procedimientos, generados por InfoCorp o Symantec) a los asistentes. Al terminar la(s) sesión(es) de capacitación, se realizará una pequeña evaluación al personal que asistió y los resultados obtenidos serán entregados al líder de proyecto. Esto tiene por objetivo darle al cliente elementos para que él conozca si el personal operativo que será responsable del software antivirus tiene los conocimientos suficientes para dar confiabilidad a la solución. Este paso puede ser omitido, si el cliente así lo desea.

Una variante del proceso de capacitación puede darse si el cliente desea que se capacite al personal conforme se van realizando las etapas de Instalación y/o de Implementación. Esto pudiera retrasar un poco dichos procesos, pero tiene la ventaja de que el personal es capacitado sobre los equipos que van a operar diariamente.

En cualquier caso, se propondrá al cliente un calendario de capacitación. Incluso se puede tener una extensión de este servicio, si el cliente desea capacitación tiempo después de las fases de Instalación y/o de Implementación (por ejemplo, por rotación de personal).

En este servicio se define el número de sesiones, el número de participantes y el tipo de capacitación. No es un servicio que el cliente deba tener contratado de forma permanente, sino que lo contratará según sus necesidades (por evento).

- Instalación de Actualizaciones

Si el cliente adquirió el seguro de actualización del software de Symantec (que le garantiza recibir las nuevas versiones liberadas durante la vigencia del seguro), se puede brindar el servicio de instalación de nuevas versiones mediante la contratación de este servicio.

Siempre es importante contar con versiones recientes de software y si el cliente las estará recibiendo por su seguro de actualización, es conveniente instalar el nuevo software y así disfrutar de sus mejoras.

El proceso de instalación de actualizaciones requerirá de un análisis de la infraestructura, planeación, instalación e implementación, por lo que se podría considerar como un nuevo proyecto de instalación y/o implementación por sí mismo, cuyo costo variará dependiendo de la complejidad encontrada.

Este proceso no está considerado como parte del servicio de Soporte Técnico en sí, ya que dicho servicio sólo incluye asesoría al cliente para que él realice el proceso, pero no hay compromiso de visita en sitio o responsabilidad de realizar la instalación de la actualización.

Este servicio no es un servicio que el cliente deba tener contratado de forma permanente, sino que lo contratará según sus necesidades (por evento).

- Auditoría

InfoCorp podrá realizar auditorías a la solución antivirus y generar un informe en donde se reflejen los resultados de dicho proceso. Esta información es de utilidad al cliente, ya que le permitirá saber si la solución antivirus sigue trabajando de forma óptima o si requiere algún ajuste.

En el caso de que la auditoría indique que se deben realizar ajustes menores, se podrá auxiliar al cliente en su implementación como parte del servicio de Soporte Técnico (si tiene contratado este servicio).

Durante la auditoría no se realizarán instalaciones ni se resolverán eventos de soporte técnico, sólo se observará cómo trabaja la solución, se investigarán registros de información y se entregarán resultados al cliente. No se interferirá con la operación de la solución antivirus y en ningún caso se realizarán correcciones sin el conocimiento y autorización escrita del cliente.

Las auditorías pueden realizarse de forma mensual, trimestral, semestral o anual, y el cliente podrá contratar el número de eventos que desee, según sus necesidades.

- Administración de la solución antivirus

Con el objeto de que el cliente obtenga los mejores resultados de uso de la suite Symantec Antivirus Enterprise Edition, InfoCorp ofrece el servicio de Administración de SAV, ya que aunque con la versión corporativa de SAV se

reducen drásticamente los tiempos de administración, no se debe dejar a "la deriva" la solución una vez que ha sido instalada. Si el cliente lo desea, personal de InfoCorp visitará sus instalaciones de forma periódica a fin de monitorear el comportamiento de la solución. Este servicio ofrece al cliente la ventaja de que no tiene que "sobre-utilizar" al personal operativo y/o de soporte técnico para procesos de administración de SAV, y al mismo tiempo asegura que el potencial de la solución se utilice al máximo. Es por esto, que el enfoque que se da al servicio de administración es preventivo, más que correctivo. El Administrador de Antivirus asignado al proyecto realizará las siguientes actividades:

- Visitas periódicas en las instalaciones del cliente (no se recomienda tener más de 2 visitas por semana ya que la solución es lo suficientemente estable como para no requerir a una persona de tiempo completo; ni menos de 2 al mes ya que el enfoque preventivo se podría perder).
- Verificación del estado de las definiciones de virus en los equipos.
- Mantenimiento a la Cuarentena Central.
- Creación de manuales y procedimientos personalizados.
- Vinculación con el personal operativo y/o de soporte técnico a fin de mejorar la comunicación y el proceso de soporte (si el cliente contrató el servicio de Soporte Técnico).
- Creación de reportes de incidencias de virus de forma mensual. Estos reportes permiten al personal de TI tomar decisiones respecto al antivirus y políticas de seguridad, para así realizar acciones preventivas.
- Verificación periódica de la integridad de las políticas de seguridad antivirus.
- Ejecución de análisis contra virus de forma periódica en la solución antivirus.
- Monitoreo remoto de la solución a través de software de control remoto (opcional).
- Notificaciones sobre nuevos virus, amenazas o mitos.
- Envío oportuno de "posibles virus" o archivos "sospechosos" a Symantec, para su análisis y creación de vacuna (cuando aplique).
- Apoyo al personal de TI en Auditorías.

Este servicio ayuda al cliente a aumentar la confiabilidad de la solución antivirus, con el objeto de reducir al máximo los riesgos de infección; sin embargo, no puede asegurar que no habrá ningún evento de virus o de pérdida de información ya que los programadores de virus siempre van "un paso adelante" que cualquier fabricante de antivirus.

- Notificaciones vía correo electrónico

Como un valor agregado de parte de InfoCorp, a todos sus clientes les son enviadas notificaciones vía correo electrónico respecto a:

- Publicación de nuevas definiciones de virus.
- Surgimiento de nuevos virus de mediana o alta peligrosidad.

- Información sobre “mitos” (hoaxes) acerca de virus que no existen.
- Procedimientos de eliminación de virus.
- Reportajes acerca de SAV.
- Información de utilidad para practicar “Computación Segura”

Dichos correos electrónicos son enviados a través de una lista de distribución de información, por lo que no se divulgan las direcciones de correo de los recipientes. Se le solicita al cliente una lista de todos los contactos que recibirán los correos: Directores y Gerentes de TI o Personal de Soporte Técnico; no se recomienda que esta información sea enviada a los usuarios finales, ya que podría ocasionar confusión o temor injustificado.

Servicio de Capacitación de NAV.

Con base en la experiencia obtenida en diversos corporativos, y habiendo participado en varias implementaciones de NAV, se creó un plan de capacitación para clientes, el cual trataba de abarcar los temas más importantes de la operación del producto, considerando un curso estándar y uno de administración. A continuación, se anexan los temarios de las capacitaciones desarrolladas.

CAPACITACIÓN NORTON ANTIVIRUS CE 7.x.

Objetivo del curso:
Proporcionar una capacitación básica al personal responsable de la operación de Norton Antivirus Edición Corporativa, en servidores y/o en estaciones de trabajo, que les permita utilizarlo correctamente. Dicha capacitación abarcará el proceso de instalación, características y configuración de NAV CE, y herramientas para la solución de problemas.

Prerrequisitos:
Los Asistentes deberán contar con conocimientos sobre terminología de computadoras, incluyendo conocimientos acerca de trabajo en red (protocolos de comunicación) y correo electrónico. Se requiere además que cuenten con conocimientos sólidos respecto a los sistemas operativos Microsoft Windows 9x / NT / 2000.

Temario del curso:

1. Introducción 60 minutos
    - Qué es un virus
    - Tipos de virus
    - Tecnología de virus
    - Nomenclatura de virus
    - Síntomas de infección
    - Ciclo de vida de un virus
    - Cómo practicar “Computación Segura”
    - Esquema de Protección NAV CE (Grupo NAV)

- Protección Total NAV
- Conceptos Usados en NAV CE

2. Instalación del Servidor NAV CE 60 minutos
    - Instalación NAV CE en Servidores
    - Requerimientos
    - Windows NT Server / Windows 2000 Advanced Server
    - Novell Netware
    - Proceso de Instalación Paso-a-Paso
    - Servicios NAV CE

3. Instalación del Cliente NAV CE 60 minutos
    - Instalación NAV CE en Estaciones de Trabajo
    - Requerimientos
    - Windows 9x / NT Wks / 2000 Professional / XP / ME
    - Proceso de Instalación Paso-a-Paso
    - Otros métodos de instalación

4. Norton Antivirus CE 60 minutos
    - Breve descripción de los componentes de NAV CE
    - Opciones de Configuración
        - Protección en Tiempo Real
        - Opciones Avanzadas de Protección a Archivos
        - Análisis Heurístico (*BloodHound*)
        - Análisis Automático de Discos Flexibles
        - Actividad similar a la de un Virus (*Virus-like Activity*)
        - Protección al correo electrónico (Lotus Notes / Exchange / Outlook)
    - Estructura en Disco de los componentes de NAV CE
    - Programa
    - Configuración
    - Definiciones de Virus
    - Análisis contra virus
        - Manual
        - Programado
    - Protección de Correo Electrónico
    - Consulta de Historiales
        - De Virus
        - De Análisis contra virus
        - De Eventos (NAV)
    - LiveUpdate
    - Cuarentena Local

5. Resolución de Problemas 30 minutos
    - Consejos para la Instalación
    - Desinstalación de NAV CE
        - Automática

    - Manual
- Proceso de Actualización de definiciones de virus
    - Automático (VDTM)
    - Manual (Intelligent Updater)
    - LiveUpdate
- Discos de Rescate
- Información necesaria para resolver problemas

Total: 270 minutos (4.5 horas)

CAPACITACIÓN NORTON ANTIVIRUS CE 7.x
Administración SSC y Módulos Adicionales

Objetivo del curso:
Proporcionar una capacitación básica al personal responsable de la operación de Norton Antivirus Edición Corporativa para que puedan realizar el proceso de Administración del Antivirus y utilizar correctamente la consola SSC. Dicha capacitación abarcará también los módulos Antivirus para correo electrónico y tráfico HTTP, FTP y SMTP. La duración del curso dependerá de los módulos de NAV que el cliente tenga instalados (si el cliente no tiene instalado cierto módulo de NAV no se deberá tomar capacitación sobre dicho módulo).

Prerrequisitos:
Los asistentes deberán haber asistido al curso de Capacitación Básica de NAV CE 7.x (4.5 horas). Se requiere además que cuenten con conocimientos sólidos respecto a los sistemas operativos Microsoft Windows 9x / NT / 2000 y Novell Netware (en caso de contar con este Sistema Operativo). Para los módulos adicionales de NAV se requiere además de conocimientos a nivel administración de sistemas de correo electrónico (Exchange o Lotus Notes) así como conocimientos acerca de Internet (tráfico SMTP, HTTP, FTP, DNS, etc.).

Temario del curso:

1. Instalación de Symantec System Center 60 minutos
    - Introducción a Symantec System Center y Cuarentena Central
    - Requerimientos de Instalación
    - Instalación SSC
    - Instalación de la Consola de Cuarentena
    - Instalación y Configuración de la Cuarentena Central
    - Instalación de Módulo de Administración (Snap-In)
    - Instalación de Módulo de Instalación (Add-On)
    - Servicios SSC, AMS y Cuarentena Central.

2. Administración de NAV CE 60 minutos
    - Planeación del tráfico de red y Grupos NAV
    - Administración de Grupos NAV
    - Asignación de Servidor Primario NAV CE por grupo
    - Contraseña de Grupo NAV CE

- Administración de Clientes desde SSC
- Implementación de Política Antivirus en Clientes y Servidores
- El Archivo GRC.DAT
- Análisis contra virus de Clientes y Servidores desde SSC
  - Manual
  - Programado
- "Barrido de Virus" (Virus Sweep)
- Consulta de Historiales de Clientes y Servidores desde SSC
- Reportes de Virus
- Mantenimiento de la Cuarentena Central
- La utilería "DISCOVERY"

3. Instalación de Clientes NAV CE 60 minutos
   - Instalación de clientes vía *Logon Script*
   - Windows NT Server / Windows 2000 Advanced Server
   - El archivo VPLOGON.BAT
   - Ubicación de *Logon Scripts* en NT /2000
   - Asignación del script de instalación a los usuarios
   - Recursos compartidos creados por NAV CE
   - Novell Netware
   - Verificación de la asignación del Script a las Organizaciones, Unidades Organizacionales, Grupos y/o Usuarios
   - El Grupo NortonAntivirusUsers
   - Recursos compartidos creados por NAV CE
   - El archivo SETUP.WIS
   - Migración de versiones anteriores de NAV
   - Uso de la herramienta "PACKAGE.EXE"

4. Alertas y Notificaciones 30 minutos
   - Introducción al Sistema de Alertas (Alert Management System - AMS)
   - Tipos de Alertas
   - Configuración del Sistema de Alertas
   - Historial de AMS

5. Actualización de Definiciones de Virus 30 minutos
   - Uso del Transporte de Definiciones de Virus (VDTM)
   - Uso de LiveUpdate Administrator Utility

6. NAV/SAVF para Lotus Notes 20 minutos
   - Introducción a NAV/SAVF para Lotus Notes
   - Requerimientos de instalación
   - Instalación
   - Configuración
   - Cómo comprobar que NAV/SAVF para Notes está funcionando
   - Registro de actividades
   - Cuarentena
   - Análisis contra virus

7. NAV/SAVF para MS Exchange 20 minutos
    - Introducción a NAV/SAVF para MS Exchange 5.5 y 2000
    - Requerimientos de Instalación
    - Instalación
    - Configuración
    - Cómo comprobar que NAV/SAVF para Exchange está funcionando
    - Registro de Actividades
    - Cuarentena
    - Análisis contra virus

8. NAV para Gateways (SMTP) 20 minutos
    - Introducción a NAV para Gateways
    - Requerimientos de Instalación
    - Instalación
    - Configuración
    - Cómo comprobar que NAV para Gateways está funcionando
    - Registro de Actividades
    - Cuarentena

9. Symantec Web Security (HTTP y FTP) 20 minutos
    - Introducción a Symantec Web Security (sólo para Filtrado Antivirus)
    - Requerimientos de Instalación
    - Instalación
    - Configuración
    - Cómo comprobar que Symantec Web Security está funcionando

Total: Mínimo 240 minutos (4 horas) - Máximo 320 minutos (5.3 horas)

REQUERIMIENTOS.

Cantidad	Descripción
1	Equipo Windows NT 4.0 / Win 2000 que cubra los requisitos de instalación de Norton Antivirus CE y SSC para uso del Instructor. Idealmente un equipo que no se encuentre en Producción y que no necesariamente debe ser un servidor.

Los siguientes elementos pueden auxiliar en un mejor desempeño del curso, por lo que se recomienda que en la medida de lo posible se cuente con ellos.

Cantidad	Descripción
1	Video proyector para proyectar el monitor del equipo del Instructor y diapositivas de apoyo
1	Pizarrón para marcador fugaz, marcadores y borrador

1	Equipo Windows 9x / NT 4.0 / Win 2000 que cubra los requisitos de instalación de NAV CE y SSC para cada uno de los participantes (deseable que se encuentren en red con el equipo del Instructor)

En ese entonces, el conocimiento que se tenía de las soluciones de Symantec para el correo electrónico, no era tan vasto como para poder dar una capacitación formal y real a los clientes. El enfoque que se dio era más del tipo introducción a los productos y no se consideraba una sección de preguntas y respuestas.

El proyecto Coca Cola FEMSA.

En abril del 2002 se inició formalmente el proyecto de instalación y administración de NAV en Coca Cola FEMSA, que es embotelladora y comercializadora de refrescos de la marca Coca Cola, y en ese entonces la más grande e importante fuera de Estados Unidos. Aunque el grupo FEMSA cuenta con 4 divisiones, que son Cervecería Cuauhtémoc, Cadena de tiendas OXXO, FEMSA Empaque y Coca Cola FEMSA, el proyecto de administración de SAV sólo contempló a la última división.

Los objetivos que se plantearon al inicio del proyecto fueron:

- Brindar una solución de antivirus integral para toda la información de Coca Cola FEMSA, en base a su infraestructura de red.
- Estandarizar el software de antivirus en toda la compañía y así lograr un mejor control de los problemas ocasionados por contingencias de virus.
- Tener una administración efectiva del antivirus que permita informar oportunamente, prevenir y corregir cualquier contingencia de virus.

No había un estándar en cuanto a la configuración de NAV ni en cuanto a las versiones utilizadas (incluso muchos servidores contaban con McAfee NetShield), por lo que el proyecto inició realizando una prueba piloto la cual arrojó resultados preliminares positivos respecto a la configuración propuesta de NAV y del impacto en desempeño en los equipos.

Como Líder de Proyecto, se coordinó la obtención de información del cliente acerca de su estado actual (incluyendo inventario de equipos por localidad) y se definió el Universo que se usaría para la prueba piloto. En conjunto con un ingeniero asignado al proyecto se realizó la implementación de la prueba piloto y se presentó el resultado a la Dirección de TI.

Una vez realizados los ajustes necesarios, y considerando como positivas las pruebas del piloto, se creó un plan de ataque para la instalación de NAV en todos los equipos de la red de FEMSA. El acuerdo original contemplaba como responsabilidad

de InfoCorp el instalar todos los equipos del Valle de México, y entrenar a los responsables de la regiones del Interior.

Se viajó a Oaxaca a impartir una capacitación de 2 días a los Coordinadores Regionales de TI, a fin de darles los elementos necesarios para la implementación de NAV y su posterior administración local (aunque la administración total sería realizada por InfoCorp desde el DF).

Cada coordinador definió su plan de trabajo para su región y semanalmente se revisaban avances. Mientras tanto, dos ingenieros a cargo de quien esto escribe realizaban la instalación en las oficinas del Valle de México.

Para dar una mejor idea de la magnitud del proyecto, se enlistan a continuación las ubicaciones de FEMSA administradas en ese entonces:

Corporativos
- Almacén Ceylán
- Corporativo Cedro
- Planta Cedro
- Corporativo La Mansión
- Corporativo Lerma
- Corporativo Santa Fe
- Planta Mega Toluca

Zona Centro
- Distribuidora Centro Histórico
- Mini Bodega Costa Rica
- Mini Bodega Garibaldi
- Mini Bodega Marsella
- Distribuidora La Viga
- Distribuidora Mega Iztapalapa
- Bodega Central de Abastos
- Planta Tlalpan II
- Distribuidora Mega Vallejo
- Distribuidora Mixcoac
- Distribuidora Sacramento
- Distribuidora Xocongo

Zona Oriente
- Distribuidora Chalco
- Distribuidora Los Ángeles
- Distribuidora Mega Los Reyes
- Planta Los Reyes
- Distribuidora Texcoco
- Distribuidora Xochimilco
- Distribuidora Zaragoza

Zona Poniente
- Distribuidora Atizapán
- Distribuidora Coacalco
- Bodega Teotihuacán
- Distribuidora Cuautitlán
- Bodega Hueypoxtla
- Planta Cuautitlán
- Distribuidora Huixquilucan
- Distribuidora Santa Clara
- Distribuidora Tlalnepantla

Ixtacomitán
- Bodega Cárdenas
- Bodega Comalcalco
- Distribuidora Ecológica Ixta
- Bodega Emiliano Zapata
- Planta Ixtacomitán
- Bodega Macuspana
- Bodega Palenque
- Bodega Tenosique

Juchitán
- Bodega Arriaga
- Bodega Huatulco
- Planta Juchitán
- Bodega Matías Romero
- Bodega Pochutla
- Bodega Puerto Escondido
- Distribuidora Tehuantepec

Minatitlán
- Bodega Acayucan
- Bodega Agua Dulce
- Distribuidora Coatzacoalcos
- Bodega Las Choapas
- Planta Minatitlán
- Bodega San Andrés

Tapachula
- Distribuidora Ecol. Tapachula
- Bodega Escuintla
- Bodega Huixtla
- Bodega Mapastepec
- Bodega Pijijiapan
- Planta Tapachula

Tuxtla
- Bodega Bochil

- Bodega Comalapa
- Bodega Comitán
- Distribuidora Ecológica SCLC
- Distribuidora Ecológica Tuxtla
- Bodega Independencia
- Bodega Ocosingo
- Bodega Ocozocuautla
- Bodega Pujiltic
- Planta San Cristóbal
- Distribuidora Tuxtla Gutiérrez
- Bodega Villaflores
- Bodega Yabteclum
- Bodega Yajalon

Oaxaca

- Bodega Ayutla Mixe
- Distribuidora Ecológica Oaxaca
- Bodega Huajuapan
- Distribuidora Mega Oaxaca
- Bodega Miahuatlan
- Bodega Nochixtlán
- Planta Oaxaca
- Bodega Ocotlán
- Bodega Sola de Vega
- Bodega Tlacolula
- Bodega Tlaxiaco

En total, se administraron 2130 equipos, de los cuales 1534 se encontraban en el Valle de México y 596 en Sureste.

El proceso de instalación de NAV en la totalidad de equipos requirió de cerca de 4 meses de trabajo conjunto. Conforme se instalaban equipos con NAV el tráfico entre localidades disminuía (por el diseño de la solución que se planteó al inicio del proyecto) y los ataques de virus comenzaron a disminuir.

Para la atención de problemas se logró trabajar de manera conjunta con el soporte en campo –proporcionado por Unisys en esquema de Outsourcing- y se les apoyaba vía telefónica o en sitio (sólo para el Área Metropolitana). Para el Sureste, cada Coordinador de TI se encargó de atender los problemas locales, contando con apoyo remoto de personal de InfoCorp. Se logró crear un buen equipo de trabajo con ellos.

Adicionalmente, se utilizó NAV para Lotus Notes, que era el sistema de correo electrónico usado por FEMSA. El proteger el correo electrónico desde el servidor, ayudó a mitigar las infecciones en las estaciones de trabajo y a ahorrar ancho de banda.

Se logró disminuir en un 70% el número de incidentes de virus, tras un año de trabajo. El éxito en el proyecto fue tal que se empezó a considerar extender el alcance y considerar la división de Cervecería Cuauhtémoc, basada en Monterrey.

Sin embargo, y a pesar de todos los esfuerzos realizados, al llegar el final del contrato anual y al estar negociando la renovación del licenciamiento de NAV y del servicio de administración, FEMSA tomó la decisión corporativa de tercerizar toda el área de TI, por lo que decidieron que todo el personal de esa área sería contratado por EDS para atender a FEMSA. EDS contaba con un acuerdo de trabajo con Computer Associates, por lo que como parte de su propuesta de servicios, se incluía la licencia y administración del producto antivirus Innoculate sin costo para FEMSA. Ante este escenario, FEMSA decidió no renovar los servicios de InfoCorp ni el licenciamiento con Symantec.

Certificación SAV 8.

Con base en la experiencia obtenida con el proyecto FEMSA, y dedicando algunas horas al autoestudio, en junio de 2003 se presentó y se aprobó el examen de certificación de SAV 8.

Anteriormente, Symantec no tenía un esquema de capacitación real y no había exámenes de certificación formal. El aprobar este primer examen significaba validar la experiencia obtenida en años anteriores y aumentar la confianza de Symantec en InfoCorp, como uno de sus mejores socios de negocios.

Capítulo 5.
Gerente de Soporte Técnico y Operaciones.

Período: Junio, 2003 a Enero, 2005
Jefe Directo: Ing. Efraín Medina.

De regreso al Call Center.

Por problemas económicos, Grupo Sphaera tuvo que realizar un recorte de personal. Varios puestos fueron absorbidos por la operación, y las plazas no se recuperaron, a fin de dar un respiro económico.

Por esta razón, se asignó nuevamente la responsabilidad de operar el Call Center a quien esto escribe, pero ahora contemplado los 3 proyectos que se tenían en él: Ingram Micro, Línea Gurú y Symantec (el cuál se mantenía desde 1997 y que en realidad no había sufrido modificaciones).

Las actividades en el Call Center debían realizarse al mismo tiempo que las actividades de Soporte Técnico Especializado, por lo que se coordinó el trabajo de un promedio de 14 ingenieros de soporte telefónico y 3 ingenieros de soporte en sitio.

El proyecto Ingram Micro.

Ingram Micro era el mayorista más importante para lo relacionado a Tecnologías de la Información y Comunicaciones en ese entonces. Uno de los problemas principales que tenían no era la falta de ventas, sino los errores originados por el comprador (y que derivaban en reclamaciones, garantías, devoluciones o cancelaciones). A fin de minimizar estos impactos negativos, Ingram implementó un servicio de asesoría telefónica gratuita para todos sus compradores.

La idea de este servicio, era orientar al comprador acerca de lo que realmente necesitaba adquirir o informarle acerca de las características de lo que deseaba adquirir. Toda la información necesaria para hacer una buena compra, era comentada o enviada al comprador. Una vez que éste se encontraba seguro de lo que quería adquirir, se le transfería al área de pedidos y realizaba su compra.

Para acceder a este servicio, sólo bastaba con llamar y dar el número de distribuidor que se tuviera en Ingram. La idea al principio fue un éxito, pero poco a poco fue desvirtuándose a causa del mal uso que los compradores le daban. Había casos de compradores que exigían orientación y cotizaban varios productos, pero no levantaban un pedido. Había casos en los que sólo se pedía información para comparar contra otros mayoristas y había compradores que llamaban para consultar cualquier detalle.

Mensualmente se elaboraba un reporte estadístico y se enviaba a Ingram para su valoración. En conjunto, se detectaron problemas y se plantearon alternativas de solución.

Aunque el soporte brindado sólo era de preventa (no resolución de problemas), la gran cantidad de marcas y productos que Ingram manejaba complicaba el esquema de atención. Después de trabajar un tiempo en el proyecto, se asignó a un Líder de Proyecto y con su apoyo se establecieron métricas para la atención telefónica, y se definieron esquemas de entrenamiento interno y mejoramiento de la calidad. Se definieron "expertos" por áreas y se promovió el autoestudio y el fácil acceso a la información.

Se trabajó en hacer un grupo de trabajo unido, que compartiera información y se responsabilizara del éxito del proyecto. Se repartieron responsabilidades entre los miembros más destacados y se logró reducir el índice de rotación entre los agentes telefónicos.

El trabajo realizado se consideró el inicio de un proceso de expansión del servicio que, a la larga, redundó no sólo en la conservación del proyecto, sino su expansión y traslado a las oficinas de Ingram Micro.

El proyecto Línea Gurú.

Concebido como idea original de Grupo Sphaera, Línea Gurú pretendió ser la nueva alternativa de soporte para el usuario casero o de la PyME, que no cuenta con grandes conocimientos en TI y que no tiene a quién recurrir si se le presenta un problema al usar su equipo de cómputo.

Este servicio no obliga al usuario a adquirir una póliza o contrato de soporte, con los grandes costos que esto podría significar. Trabaja en esquema de prepago (como la telefonía celular), pero en lugar de comprar "minutos de soporte" o "eventos de soporte", el usuario adquiere un periodo de tiempo, durante el cual, puede pedir soporte telefónico, sin límite de eventos, sin límite de tiempo por llamada y en esquema de servicio 7x24.

Esta "membresía" de soporte técnico, puede ser adquirida con vigencia mensual, bimestral, semestral o anual y tiene como público objetivo a los estudiantes, profesores, amas de casa, profesionistas independientes y pequeñas empresas. Si el problema no podía ser resuelto vía telefónica, el usuario tenía la opción de pagar un monto adicional a la membresía, y un ingeniero de soporte le atendía en sitio.

Grupo Sphaera realizó un estudio de mercado previo al lanzamiento del proyecto y se mostraba como viable. Sin embargo, no tuvo la penetración esperada y la venta de membresías no fue muy grande, lo que ocasionó a su vez que la demanda de llamadas de usuarios fuera realmente baja.

Se hicieron algunos esfuerzos adicionales para aumentar las ventas del servicio, incluyendo trabajo en conjunto con CompuDabo y Bancomer (como parte

de los premios de “El Libretón”), pero los usuarios que recibían las membresías nunca las activaron.

Se logró una asociación con Todito (ISP de prepago del Grupo Salinas) y cuando un usuario llamaba al Call Center de Todito, si se detectaba que los problemas en la conexión eran derivados de una falla de HW o SW ajena al servicio de Todito, se proporcionaba al usuario información acerca de Línea Gurú, pero en un esquema especial de atención en sitio sin necesidad de comprar la membresía (aunque obviamente se trataba de venderla también).

Tratando de diversificar el concepto y de captar más clientes potenciales, se creó Línea Gurú Empresarial, la cual conservaba el esquema de membresía de soporte telefónico y algunas visitas de soporte en sitio, esto a un costo un poco más elevado que la membresía estándar, pero a un precio sumamente atractivo para las PyMES.

Casi al final de este período, se logró además una asociación con Únete, mediante la cual se brindaba apoyo a los profesores de escuelas rurales que habían sido acondicionadas con equipo de cómputo gracias a las campañas de “Redondeo” en tiendas departamentales. En este esquema, Únete adquirió un número determinado de membresías, que serían manejadas independientemente de la escuela que lo requiriera. El servicio de Línea Gurú se mantenía en lo relativo a brindar soporte técnico telefónico, pero funcionaba además para que los profesores pudieran reportar problemas de HW, eléctricos o de enlace satelital a Internet, en cuyo caso, Línea Gurú tomaba nota del reporte y lo canalizaba a Únete para su atención.

Mensualmente, se tenían cerca de 40 reportes y una venta promedio de 20 membresías. Muchas membresías se vendían, pero pocos registraban sus datos (y en consecuencia, nunca usaban el servicio).

Hasta el final de la relación laboral con InfoCorp, Línea Gurú seguía funcionando, pero continuaba sin tener la penetración deseada y teniendo pocos reportes al mes.

El proyecto Symantec.

El soporte técnico para usuarios de Symantec seguía siendo parte de las actividades más importantes, pero poco había sido mejorado desde 1997. Muchos procedimientos y descripciones de puesto seguían siendo los que fueron creados por un servidor mientras se estuvo en la posición de Líder de Proyecto.

La mayoría del personal que atendía este proyecto era nuevo en él y había pocos agentes experimentados. Se había perdido la estandarización en el servicio y había muchas cosas por corregir.

Por primera vez, después de 6 años de estar dando este servicio a Symantec, se logró definir con exactitud el tipo de usuarios que deberían recibir el soporte gratuito. Se determinó que sólo se atendería a usuarios finales y sólo para productos “caseros” (no corporativos). Se contó con la autorización de Symantec para indicar a

los clientes corporativos que debían comunicarse a otros teléfonos para obtener soporte de dichos productos.

Previamente, Symantec había cambiado su estrategia para manejar el soporte para Latinoamérica, y ahora, todo se controlaba desde Brasil. Por esta razón, los reportes mensuales y semanales se debían enviar a Brasil y la oficina de Symantec en México ya no tenía control sobre el servicio. En diversas ocasiones, la Gerente Regional de Soporte para *Retail* de Symantec, Cristiane Mendonça, visitó México y en conjunto se verificaron las estadísticas y los nuevos requerimientos que se tenían, para mantener el servicio al nivel requerido y esperado.

El número de reportes que no se resolvían al primer contacto iba en aumento (a causa de la falta de experiencia de algunos agentes) y no había un control en la captura de los reportes, lo que ocasionaba que la elaboración de los reportes semanales y mensuales tomara demasiado tiempo. Se logró reestablecer mecanismos de control en el sistema de Call Tracking, a fin de evitar errores de captura y conseguir que se capturara toda la información pertinente.

Se brindó capacitación a los agentes más nuevos, acerca del antivirus y los procedimientos de eliminación. Aunque ya no se conocían los productos de *retail*, la teoría y los mecanismos de eliminación seguían siendo los mismos. Había grandes lagunas en el uso de productos como pcAnywhere, que se pudieron eliminar gracias a pláticas de producto y establecimiento de programas y tiempos de autoentrenamiento para los agentes.

Symantec ofreció por primera vez dar una capacitación formal y del mismo nivel que el de los agentes propios de Symantec en las otras regiones. Se destinó al mejor elemento del proyecto para asistir durante semana y media al entrenamiento en Sao Paulo (Brasil) por cuenta de los especialistas de Symantec. Se definió un esquema de transmisión del conocimiento luego del regreso del agente que tomó la capacitación.

Asimismo, fue la primera vez que Symantec invitó formalmente a Grupo Sphaera a participar como postulante para proveer soporte técnico telefónico para otras regiones de Latinoamérica, por lo que se participó en la elaboración de la respuesta al RFP (Request for Proposal, Petición de Propuesta) enviado por Symantec. Desafortunadamente, el proceso de evaluación de proveedores por parte de Symantec, se vio afectado por cambios en sus planes de crecimiento y manejo de los recursos y el proyecto se detuvo.

El proyecto Epson.

Durante tres meses, se trabajó en un proyecto especial para Epson llamado “De regreso a clases con Epson” que consistía en recibir las llamadas de los usuarios que hubieran comprado ciertos modelos de impresora durante cierto período de tiempo. Los equipos participantes contenían un cupón que, previo registro telefónico, servía para recibir gratuitamente y a domicilio una mochila escolar.

Se coordinó la logística de implementación del proyecto, así como la creación del sistema de captura de reportes y la contratación y capacitación de dos capturistas de datos para atender el proyecto.

Semanalmente se generaba una estadística para Epson, que indicaba el número de registros recibidos, la distribución geográfica y los modelos de los mismos y se canalizaban para que se entregaran las mochilas a los usuarios finales.

El proyecto fue considerado como un éxito, pues la campaña creada por Epson atrajo a muchos clientes y cerca de un 95% de las mochilas fueron entregadas. Según estimaciones, hubo un 5% de mochilas que no fueron entregadas por problemas de la empresa de distribución o porque no se vendieron todas las existencias de la promoción.

Los cambios en el Call Center.

Para poder implementar los cambios que eran necesarios en el área, se inició con el proyecto Symantec, pues era algo que ya se conocía y resultaba más fácil reajustar los procesos. Mientras se hacían estos cambios, se iba conociendo más a detalle los proyectos Gurú e Ingram.

Se dedicó tiempo para platicar con cada ingeniero de soporte y ver qué pensaban del servicio que daban, de sus compañeros y de la Empresa. Se identificó a los mejores elementos y se designaron Líderes de Proyecto para Symantec e Ingram (Línea Gurú no justificaba tener un líder). Se tuvieron sesiones de motivación y se proporcionaron pequeños cursos de asertividad y atención a clientes.

Se definieron nuevos esquemas de evaluación y esquemas de recompensas para los agentes más destacados y dedicados. Hubo algunos agentes que se resistían a aceptar los cambios y hubo alguno que incluso renunció. Se logró crear un ambiente más relajado y se empezó a crear un grupo de trabajo que ya no sentía estar dividido por proyecto. Se propuso un esquema de “agentes combinados” para poder destinar más agentes a Symantec o Ingram si alguno de ellos experimentaba una carga inusual de llamadas. De igual forma, se definió un esquema de reconocimiento al esfuerzo con una especie de “plan de carrera” en la Empresa, ofreciendo oportunidades de desarrollo en proyectos de mayor complejidad (y mayor remuneración económica) dentro y fuera del Call Center.

Se redujo el número de faltas y retardos y la rotación de personal se vio altamente disminuida, pasando de tres a cuatro renuncias por mes a una renuncia bimestral. Esto redundó en un aumento de experiencia en los agentes y en la consecuente mejora de los servicios y atención a clientes.

Los reportes mensuales se generaban más rápidamente al evitar desde el sistema de captura de reportes los errores de los agentes y creando vistas y filtros para exportar. Se crearon y modificaron algunas vistas y formatos de captura del sistema (basados en Lotus Notes). Se incorporaron más elementos estadísticos y se trabajó en reducir los tiempos de espera y de atención de todos los proyectos. Cada líder de proyecto era responsable de elaborar y presentar los reportes mensuales a los contactos de cada proyecto.

En promedio, el Call Center contó con 15 agentes asignados a los 3 proyectos y el número de reportes atendidos por proyecto aumentó en 30% para Symantec (cuando se tomó el proyecto se tenían 600 reportes mensuales y se llegó a los 800); en 25% para Ingram Micro (pasando de 2000 a 2500 reportes mensuales) y casi sin variación para Línea Gurú (manteniéndose en promedio 50 reportes por mes).

Seguimiento con Soporte Técnico Especializado.

A la par de la administración del Call Center, se continuó brindando soporte a usuarios corporativos y coordinando las actividades de 3 ingenieros de soporte. El grueso de las soluciones vendidas seguía siendo la suite de antivirus de Symantec, por lo que 3 personas atendían los requerimientos de preventa y postventa. Para la parte de servicios para soluciones de respaldo, se continuó trabajando con Backup Exec de Veritas y un ingeniero se encargaba de atender preventa y postventa.

Las certificaciones de Symantec tienen una duración de 2 años, por lo que era necesario renovar la certificación de SAV 8 obtenida en 2003. Nuevamente, usando la experiencia acumulada en el uso de la suite y dedicando tiempo para autoestudio, el 13 de diciembre de 2004 se logró la certificación como Symantec Certified Technology Architect - Virus Protection & Integrated Client Security Solutions.

Se apoyó con pláticas de producto y elaboración de programas de autoestudio a que dos de los ingenieros de soporte también obtuvieran esa certificación.

El proyecto KPMG.

KPMG es una firma internacional de consultores que ofrece sus servicios a grandes empresas. Aunque no se les vendieron las licencias de Symantec Antivirus por que las adquirieron a través de un acuerdo global (del corporativo en Holanda), se les ofreció el servicio de Administración de SAV, por lo que se iniciaron operaciones en Junio de 2003.

La responsabilidad adquirida incluía visitar cada semana (todos los miércoles) las instalaciones de KPMG de la Cd. de México (ubicadas en ese entonces en Bosques de las Lomas) y revisar la consola de SAV y realizar las acciones necesarias a fin de mantener la solución antivirus estable y actualizada, de acuerdo a los requerimientos del cliente.

Antes de que se iniciara este servicio, KPMG tenía graves problemas de virus, no había conocimiento del estado real de los equipos de la red y muy

frecuentemente eran “desconectados” de la red internacional de KPMG por saturar el enlace con virus.

Lo primero que se realizó fue verificar el inventario de localidades y de equipos, a fin de crear una correlación entre dicho inventario y los equipos visibles en consola. El proceso se complicó, porque muchos equipos de usuarios móviles no se encuentran la mayor parte del tiempo conectados a la red de KMPG, sino basados en las oficinas de los clientes a los cuales brindan sus servicios de consultoría.

Una vez identificados los equipos faltantes, se procedió a implantar el estándar corporativo de configuración para SAV desde la consola y a nivel global, ya que anteriormente, cada equipo tenía posibilidad de cambiar dicha configuración e incluso muchos usuarios desactivaban el antivirus, lo que ocasionaba la mayoría de las infecciones en equipos.

Adicionalmente, se inició el seguimiento puntual al estado de las actualizaciones de las definiciones de virus en servidores y clientes. En muchos casos, los servidores no se actualizaban y en consecuencia, sus clientes eran vulnerables a ataques de virus recientes. Al monitorear el estado de los servidores, y corregir las ocasiones en que no se actualizaban, se logró disminuir aún más el número de incidencias de virus en los equipos.

Se creó un vínculo con el Centro de Atención a Usuarios (CAU) de KPMG, a fin de ayudarles a resolver problemas relativos a SAV o con virus, al ser ellos los responsables de recibir las llamadas de soporte de los usuarios finales. Se dieron varias sesiones de capacitación a los ingenieros de campo del CAU y se creó un repositorio central de información, con herramientas de software, procedimientos personalizados e información relativa a SAV en KPMG. El soporte al CAU se brindaba en sitio si era necesario (si coincidía con la visita de los miércoles) y vía telefónica o por correo si no coincidía con la visita semanal. Esto ayudó a disminuir el tiempo de atención de reportes en el CAU y ayudó a disminuir la carga de trabajo de los ingenieros.

Poco a poco se fue fortaleciendo la estructura antivirus y los eventos masivos de virus disminuyeron de uno por mes a menos de uno por semestre. Durante la administración que se realizó en KPMG sólo se tuvo una “desconexión” de la red mundial por eventos de virus, y desde entonces no se volvió a presentar una nueva desconexión.

Como parte del servicio, se respondió exitosamente a 2 auditorías internas de TI (realizadas por personal de KPMG del corporativo en Holanda), lo que aumentó aún más la confianza de KPMG en el servicio y atención proporcionados por InfoCorp.

Semanalmente se creaba un reporte de visita, en donde se indicaba el estado general de la consola, servidores y clientes SAV, así como la protección al correo electrónico. Se indicaban además las actividades desarrolladas en conjunto con el CAU o las correcciones realizadas a la solución antivirus. Mensualmente, se generaba un reporte estadístico que mostraba el número de clientes y servidores administrados, información del estado de SAV en cada uno de ellos y estadísticas del historial de virus de los equipos, resaltando el número de ataques virales, equipos y usuarios con mayor incidencia de virus, entre otros datos.

Después de año y medio de realizar la administración semanal, se asignó a otro ingeniero (suficientemente capacitado) para realizar esta función semanal y

poder dedicarse a atender a otros clientes. Se siguió apoyando al ingeniero como soporte de segundo nivel o a cubrirlo si tenía alguna dificultad personal.

En promedio, se administraban cerca de 1200 equipos, 30 servidores y 14 servidores de correo, distribuidos en las siguientes ubicaciones:

- Bosques de Ciruelos (anexo al Corporativo)
- Bosques de Duraznos (Corporativo)
- Chihuahua
- Ciudad Juárez
- Ciudad Obregón
- Culiacán
- Guadalajara
- Hermosillo
- Mérida
- Mexicali
- Monterrey
- Monterrey Ábaco
- Nuevo Laredo
- Puebla
- Reynosa
- Tijuana
- Toluca

El proyecto Pepsi Gemex.

Pepsi Gemex era un embotellador de Pepsi en México e inicialmente se les vendió sólo el licenciamiento antivirus y soporte telefónico para resolución de problemas básicos.

Sin embargo, la rotación de personal, la falta de estándares corporativos y el poco control del antivirus, redundaron más de una vez en diversos problemas de virus, para los cuales, se apoyó en sitio.

Problemas con el virus Funlove (explicado en el capítulo 3) hicieron que la red de Pepsi Gemex se viera sumamente afectada y que el enlace a Plano, Texas fuera apagado en diversas ocasiones.

Aunque el cliente no contaba con una póliza de soporte en sitio, se decidió apoyarles sin costo durante las contingencias que tuvieran. Por lo que en múltiples ocasiones se les asistió a fin de verificar la configuración de la consola, asegurar la correcta propagación de las definiciones de virus a los clientes y a definir procedimientos de eliminación de virus, incluyendo entrenamiento a los ingenieros de soporte para que ellos erradicaran el virus en los equipos de la red.

Lamentablemente, al no existir un responsable formal de la administración del antivirus, los problemas de virus eran muy recurrentes e incluso se pensó en que el problema era el antivirus y que no era suficientemente efectivo. A través de diversas visitas y sesiones con diversos encargados de TI, se logró demostrar que el problema no era el antivirus, sino la falta de administración y seguimiento a problemas. En conjunto, se definió un breve plan de capacitación a los responsables de la administración y se definieron políticas y configuraciones para ser aplicadas en todos los equipos.

Aunque Pepsi Gemex no contaba con presupuesto para contratar los servicios de administración de SAV, se logró la renovación del licenciamiento por 2 años consecutivos.

El proyecto Hipotecaria Su Casita.

En 2004 se inició trato con esta empresa, vendiéndoles en principio sólo el licenciamiento de Symantec Antivirus para casi 650 nodos. Como valor agregado a la venta de las licencias, se ofrecieron auditorías trimestrales a SAV.

Las auditorías contemplaban la toma de datos de la consola de administración de SAV y su posterior procesamiento en Excel para presentar reportes gráficos y recomendaciones para mejorar el uso del producto.

En principio, se coordinó el calendario de auditorías para el cliente, y se participó en el diseño de la solución antivirus. Se definió instalar servidores SAV en cada localidad y manejar todo desde el corporativo del DF. Se realizaron las primeras 2 auditorías y posteriormente se supervisó al ingeniero que fue asignado a dicho proyecto.

En ese entonces, las localidades con que contaba Hipotecaria Su Casita eran:

- Aguascalientes
- Cancún
- Canoa
- Cd. Del Carmen
- Cd. Obregón
- Celaya
- Chihuahua
- Coacalco
- Cuauhtémoc
- Culiacán
- Del Valle
- Durango
- Ecatepec
- Guadalajara
- Hermosillo
- Ixtapaluca
- León
- Mérida
- Mexicali
- Monterrey
- Morelia
- Pachuca
- Puebla
- Puerto Vallarta
- Querétaro
- Reynosa
- Saltillo
- San Jerónimo
- San Luis Potosí
- Tampico
- Tapachula
- Tijuana
- Toluca
- Torreón
- Tuxtla
- Veracruz

Meses después, se logró vender el servicio de auditoría mensual a este cliente.

Capítulo 6.
Gerente de Soporte Técnico Especializado.

Período: Enero, 2005 a Diciembre, 2007.
Jefe Directo: Ing. Efraín Medina / Ing. Alejandro Medina.

De regreso a soporte especializado.

Después de los ajustes en la plantilla de personal, y gracias a que algunos proyectos se consolidaron adecuadamente, la Empresa tomó la decisión de volver a crear la plaza de Gerente de Call Center y se promovió a uno de los ingenieros, líder de proyectos de Help Desk remotos, para que él ocupara esta posición.

Dado que era una persona que ya conocía los proyectos del Call Center y considerando que los proyectos ya estaban "realineados", con nuevas métricas y con un líder por cada proyecto, la transferencia de conocimientos y la entrega del puesto resultaron muy fáciles de realizar.

Una vez concluida la entrega del Call Center, se regresó de forma exclusiva a las actividades de soporte especializado, desarrollando diversos proyectos y fortaleciendo los existentes. Aunque era responsabilidad de quien esto escribe vigilar todos los proyectos, se pudo delegar la operación de KPMG y de Pepsi Gemex en uno de los ingenieros con mejor nivel, y se pudieron establecer nuevos procedimientos y documentación para los demás proyectos.

El proyecto Grupo Nacional Provincial.

Luego de varios años de relación con este cliente, se logró establecer un mecanismo de cooperación y soporte con EDS (responsable del área de TI de GNP) que no representara pérdida para InfoCorp, ya que hasta entonces exigían servicio en sitio y atención inmediata, pero sin haber pagado por dicho servicio.

El personal de EDS mantenía confianza en InfoCorp, pero por temas de carácter económico no se logró posicionar el servicio de administración de SAV (como en el caso KPMG) y se ofreció como valor agregado a la compra de licencias nuevas el servicio de auditorías bimestrales a la solución antivirus.

A pesar del buen trabajo de administración del área de TI por parte de EDS, era una realidad que la administración del antivirus se vio seriamente afectada por la rotación de personal que tenía EDS y por no dedicarle recursos suficientes a esta tarea. Luego de varios cambios de responsables de SAV en GNP, se destinó a un ingeniero de seguridad para ser responsable de la administración de SAV y, en conjunto con él, se logró estandarizar los procesos administrativos, definir configuraciones de acuerdo a perfiles de usuario y control y monitoreo de la consola

de SAV. Se presentaron algunos eventos de virus, pero a raíz del trabajo desarrollado por EDS –en conjunto con el servicio proporcionado por InfoCorp-, se logró minimizar el impacto de los ataques de virus y esto redundó en menores interrupciones en el trabajo de los empleados de GNP. Gracias a esto, el cliente renovó su licenciamiento de SAV año con año.

De acuerdo a la distribución física y lógica definida por EDS, en el 2007 GNP contaba con los siguientes grupos de clientes SAV:

- Acapulco
- Aguascalientes
- Basalto
- Cancún
- Cd. Juárez
- Cd. Obregón
- Centro Cómputo
- Chihuahua
- Comedor, Cera
- Coatzacoalcos
- CR Guadalajara
- CR Mérida
- CR Mexicali
- CR Norte Ref
- CR Sur
- Cuernavaca
- Culiacán
- Dep. Telexp Aut
- Desactualizados
- Ed Cen Aut No
- Edificio Sur
- EDS
- Hermosillo
- Hospitales
- INCAP
- Jalapa
- LAPTOP
- León
- Lomas Verdes
- Matamoros
- Médica Integral
- Mochis
- Monterrey
- Montes Rocall
- Morelia
- Nvo. Laredo
- Oaxaca
- Pachuca
- Patriotismo
- Puebla
- Querétaro
- Reforma
- Reynosa
- Saltillo
- SLP
- STA Culiacán
- STA Guadalajara
- STA Mérida
- STA Mty
- Tampico
- Tijuana
- Toluca
- Torre Diamante
- Torreón
- Tuxtla Gutiérrez
- Veracruz
- Villahermosa
- VPN

El número total de clientes SAV era de 4000 equipos administrados por EDS y soportados por InfoCorp.

Adicionalmente, se instaló el producto Symantec Web Security para el filtrado y control de la navegación Web, y el Symantec Mail Security para SMTP. Lamentablemente, ambos productos fueron desplazados por soluciones de Computer Associates (socio de negocio de EDS) por fallos en funcionalidad de los mismos. El Symantec Mail Security para Lotus Notes (tanto en Windows como en AIX), continuó instalado en 12 servidores a nivel nacional.

El proyecto Pepsi Bottling Group.

Pepsi Gemex fue adquirido por The Pepsi Bottling Group (PBG) y se creó PBG México, el mayor embotellador de Pepsi para América Latina. Gracias al trabajo desarrollado por InfoCorp en Pepsi Gemex, se nos recomendó para continuar siendo el proveedor de seguridad antivirus del nuevo grupo, por lo que se tuvo la oportunidad de duplicar el licenciamiento que se había vendido originalmente.

Después de diversas negociaciones, y en vista del tipo de soporte que InfoCorp provee, en el 2006 se logró vender el servicio de Administración de SAV para PBG, por lo que se coordinó, junto con uno de los ingenieros de soporte, el calendario de visitas semanales, actividades mensuales y reportes a ser entregados.

La administración se realizaba en una visita semanal a las oficinas corporativas del cliente (ahora ubicadas en Torre Altiva), durante la cual se tenía acceso a la consola principal de SAV y se generaban estadísticas semanales y mensuales. Hubo también vinculación con personal de soporte técnico, de administración de servidores y de auditorías (incluso internacionales).

PBG México, constaba de varias ubicaciones geográficas y diversas razones sociales. Además de la marca Pepsi, son fabricantes de Electropura y maquila de Squirt y Señorial. Por esta razón, y basándose en la infraestructura de telecomunicaciones de PBG, se tenían los siguientes grupos de clientes SAV:

- Acoxpa (Planta y Corporativo)
- Altiva (Corporativo)
- Centro
- Electro
- Golfo
- Kio
- Metro
- Noreste
- Norte
- Proplasa
- SIO
- Sur
- Sureste

A finales de 2006, PBG adquirió BEPUSA, embotellador líder del Noroeste del país, con lo que aumentó su presencia nacional, su producción conjunta y el licenciamiento de SAV. En total, se administraron cerca de 3400 clientes de forma semanal.

Por problemas derivados de una vulnerabilidad de Symantec Antivirus (reportada al cliente desde mayo del 2006), en enero de 2007 se tuvo un ataque masivo de virus en la red, lo que provocó lentitud en la operación de PBG (afectando producción y ventas). Aunque la solución era aplicar una nueva versión de SAV (lanzada por Symantec desde que se descubrió la vulnerabilidad), el cliente no quiso aceptar la falta de seguimiento al reporte que InfoCorp hizo en mayo de 2006 y consideró que no era su responsabilidad hacer la migración en la totalidad de los clientes. Sin embargo, el servicio de migración/instalación de SAV no estaba incluido en el servicio original de administración de SAV. Después de múltiples negociaciones, se logró acordar que InfoCorp haría remotamente la migración de versión en los 26 servidores de SAV a nivel nacional y apoyaría en la migración de los corporativos de Altiva y Acoxpa. Luego de 4 días de problemas en la red y de migración de versión de SAV, la infección fue controlada y la operación fue restablecida.

El cliente expresó en diversas ocasiones su malestar con respecto al producto antivirus de Symantec y en parte, a lo que ellos llamaban “falta de seguimiento de

InfoCorp". Se convocó a una reunión con Symantec y PBG para que se platicara respecto a esas inconformidades, pues PBG estaba a punto de cambiar de antivirus.

Se logró que PBG no cambiara de antivirus, pero no se logró que renovaran el servicio de administración de SAV (a pesar de que se les había seguido brindando 3 meses después de haber concluido el primer contrato).

Sinceramente, se considera que InfoCorp brindó un buen servicio, llegando en muchas ocasiones a dar mucho más de lo contratado por PBG, incluso representando pérdida económica para InfoCorp, pero que no fue valorado por los responsables de TI de PBG. Se apoyó al ingeniero asignado a la administración de SAV en PBG, y se participó en reuniones de revisiones mensuales y en la resolución de los problemas de la contingencia de enero. Se brindó soporte fuera de horario (a pesar de no tener contratado ese servicio) y se laboró en fin de semana para recuperar la operación normal. Adicionalmente, en InfoCorp hubo cambios en el equipo de ventas, y el ejecutivo asignado a PBG dejó la empresa en octubre de 2006; el personal de PBG no aceptó de buen grado al nuevo ejecutivo y pidió 2 cambios posteriores. A título personal, se considera que la no renovación de licenciamiento ni del contrato de administración, fue originada por la contingencia de enero y la falta de aceptación con el nuevo ejecutivo de ventas, pero con marcados tintes personales o fallos de percepción del cliente.

El proyecto Vitalmex.

Vitalmex es una empresa 100% mexicana que se encarga de producir y comercializar muchos de los elementos utilizados en operaciones quirúrgicas para grandes hospitales públicos y privados.

En 2003 se inició relación con esta empresa, asesorando muy superficialmente a la responsable de TI, pues no existía un contrato de soporte ni póliza de servicios vendidos. La relación inició por amistad del dueño de Grupo Sphaera con el hijo del dueño de Vitalmex.

Un año después, se logró formalizar un acuerdo de servicios de mantenimientos preventivos y correctivos para los equipos de cómputo y la venta de licenciamiento de Symantec Antivirus. Adicionalmente, solicitaron apoyo para recomendar una solución ERP (Enterprise Resource Planning) y migración de servidores. Por problemas éticos y morales con el entonces encargado de TI, Vitalmex solicitó se tomará la administración de TI en esquema de *outsourcing* pues el encargado fue despedido.

Se participó en parte de la recepción de información a la salida del encargado de TI y en la creación y publicación del perfil para la contratación del nuevo encargado de TI (pero ahora contratado por InfoCorp). Se entrevistó a diversos candidatos y se emitieron recomendaciones acerca de los mejores prospectos. Se elaboraron y calificaron los exámenes de conocimientos técnicos de los candidatos.

Mientras tanto, Vitalmex comunicó su plan de desarrollo y solicitó se les apoyara para cubrir 7 aspectos que servirían de base tecnológica para llevar a cabo dicho plan. Se tuvo la función de coordinar globalmente el proyecto e involucrarse en todas

las fases. En algunos casos, sólo se participó en la planeación y seguimiento del desarrollo; en otros, se asumió la responsabilidad total.

- Reemplazo de servidores

Migrar los sistemas actuales a servidores nuevos, que contemplen y cubran las necesidades actuales y futuras. Estandarización de versiones y migración a las versiones más recientes. Regularización del licenciamiento. Implementación de nuevos servicios.

Para cumplir con este requerimiento, se planteó la necesidad de adquirir 6 servidores nuevos, un rack, un multiplexor para monitor y teclado, y una pantalla LCD. Adicionalmente, y para cubrir algunas funciones administrativas, se solicitó una estación de trabajo.

Se auxilió en la implementación del Active Directory y del servicio de DNS. Se instaló además el servidor de MS Exchange y se crearon las nuevas cuentas de usuarios y de equipos. Se definió un nuevo estándar para la nomenclatura de los equipos y para la asignación de IPs.

- Reemplazo del conmutador.

El conmutador existente, amén de ser obsoleto y sin opción de actualización, ya no podía soportar la operación diaria de Vitalmex. Se considera su reemplazo, buscando crear un nuevo sistema de comunicación –basado en telefonía IP- que permita operar eficientemente a los empleados de Vitalmex y que redunde en el fortalecimiento de las relaciones con clientes y proveedores.

Dado que InfoCorp no era especialista en conmutadores, se hizo asociación con la empresa Altigen, quienes apoyaron en el análisis de necesidades, diseño de la solución, recomendación de componentes, cotización, venta de componentes, instalación y puesta a punto, y soporte postventa. Se instalaron 2 conmutadores-servidores Altigen y casi 100 teléfonos IP.

Al utilizar telefonía basada en IP, se logró también eliminar los costos de larga distancia asociados a la comunicación entre el corporativo y las dos oficinas foráneas.

Para este punto, se participó en las reuniones de diseño, así como de presentación de las alternativas de solución ante VItalmex. En trabajo conjunto con el fabricante y el nuevo Coordinador de TI en Vitalmex se desarrolló el plan de trabajo y se dio seguimiento a cada fase hasta su conclusión.

- VPN entre el Corporativo y las 2 localidades, y conexión a Internet.

Inicialmente, las dos localidades estaban conectadas con el Corporativo a través de enlaces dedicados, caros y limitados en ancho de banda. Se requería una solución que incrementara el ancho de banda, sin aumentar demasiado el costo de la renta mensual y que además ofreciera mayor flexibilidad y seguridad. Se contactó a RedUno de Telmex y ofrecieron la alternativa de VPN (red privada virtual, por sus siglas en inglés). Este servicio, a diferencia de una VPN

tradicional basada en IPsec, satisfacía las necesidades del cliente a un costo razonable. Telmex brindaría la infraestructura de VPN como una "segunda Internet" por la que los datos viajan encriptados y sólo los equipos autorizados tienen acceso a ella.

Al no depender de la infraestructura tradicional de Internet, se podía garantizar la Calidad del Servicio (QoS) para los diferentes tipos de datos que viajarían por el cable. Telmex garantizaría una alta disponibilidad del enlace y facilidad de incorporar nuevos puntos de acceso a la VPN (tanto para sitios remotos como para equipos portátiles).

Se ayudó en el diseño de la solución, y se supervisó la implementación por parte de Telmex. Se hicieron pruebas de enlace y se corrigieron en conjunto los problemas que se encontraron. La nueva solución fue pensada también para aprovechar la telefonía IP y se consideró también una holgura para el posible uso futuro de videoconferencia.

Adicionalmente, se negoció con Telmex un nuevo contrato para el enlace a Internet, y se creció de 256 Mbps y 16 IPs públicas a 1 Mbps y sólo 4 IPs públicas. Aunque se incrementó el ancho de banda, al reducir las IPs públicas (que en realidad no se usaban) se compensó en parte el costo, y el incremento en la renta mensual del enlace no fue demasiado elevado. Lo anterior, sumado al hecho de integrar los enlaces de VPN y de restar los gastos en larga distancia, logró un buen balance del costo total de telecomunicaciones con Telmex.

- Cambio de cableado y concentradores de red.

Aunque la infraestructura existente de conexión en red era de Categoría 5, había problemas de comunicación por la mala implementación original y la falta de mantenimiento. Adicionalmente, se usaban concentradores (hubs) de 10Mbps, lo que saturaba el ancho de banda disponible y desperdiciaba las tarjetas de 100 Mbps de los equipos más nuevos.

Nuevamente, al no ser InfoCorp especialista en cableado, se buscó el apoyo del proveedor SintCom, quienes se encargaron de revisar y valorar el cableado existente. Ellos recomendaron cambiar todo el cableado a Categoría 6, y usar cable nuevo. Aunque esto elevaba el costo, garantizaría la óptima operación de la red y se certificaría su operación por parte de Hubbel. También recomendaron los modelos de switches 100 Mbps que formarían la red.

Se coordinó con ellos el plan de trabajo para el recableado y la instalación de los nuevos switches. Vitalmex, al ver el buen trabajo desarrollado por SintCom, decidió "aprovechar" para cablear un área de trabajo nueva recién implementada.

En total, se recablearon 183 nodos de voz y datos, y se cablearon 15 nodos más. Se instalaron 4 switches de 48 puertos 10/100 Mbps, 4 paneles de parcheo y un "backbone" de datos de fibra óptica. Se entregó a Vitalmex la certificación del cableado y garantía por 25 años.

- Energía eléctrica ininterrumpida.

Vitalmex se encuentra en una zona al sur de la ciudad en donde la energía eléctrica falla constantemente. Aunque se contaba con algunos UPS (Sistema de

Alimentación Ininterrumpida, por sus siglas en inglés) para el site y para algunos equipos, los cortes de electricidad podían durar horas, lo que se traducía en la consecuente descarga de los UPS y la total inactividad de los empleados de Vitalmex.

Vitalmex deseaba contar con su propia planta generadora de energía eléctrica. Se sugirió además una solución de UPS de alta capacidad para el site y se eliminaron los UPS de las estaciones de trabajo.

En esta fase del proyecto, sólo se validó que los tiempos de implementación se cumplieran.

La planta instalada originalmente, presentó problemas de arranque automático “en frío” (es decir, entrar en operación después de estar inactiva por un largo período) por lo que tuvo que ser reemplazada. Luego de varias negociaciones con el proveedor original, se llegó a la devolución de la planta y la consecuente compra con otro fabricante.

Se instaló una planta de 100 KW basada en motor diesel, un tablero de transferencia y un UPS de 20 KW para el site. Ya no se tuvieron problemas de funcionamiento de la planta.

- Rediseño del Site.

Aunque se contaba con un espacio físico para los servidores, éste se encontraba sin las adecuaciones que garantizaran la integridad y el buen funcionamiento de los servidores y conmutador originales. Al cambiar e incrementar los servidores, el espacio resultaba inadecuado y poco funcional. Amén del desorden de cables, cajas algunos otros elementos que no debían estar en el site.

Aprovechando una remodelación y adecuación de una nueva área, se definió la nueva configuración del site, que ahora incluiría piso falso, un mejor y más grande sistema de aire acondicionado, dos racks para servidores, espacio para el UPS, un rack de telecomunicaciones, control de acceso con lectura biométrica (huella digital) y aislamiento térmico.

Toda esta labor, fue realizada por el arquitecto “de confianza” de Vitalmex, de acuerdo a las especificaciones y requerimientos que se le plantearon. La labor del arquitecto incluyó el diseño, la contratación del personal, adquisición de materiales, instalación y acabado.

- Instalación de *Firewall*.

Al contar con un enlace a Internet, Vitalmex tenía un *firewall* basado en Linux, que ni siquiera conocía el ex-coordinador de TI y que no estaba cumpliendo con todas las funciones de seguridad o de control del uso de Internet. Como distribuidores de Symantec, InfoCorp propuso un equipo Symantec Gateway Security 5420 con funciones de firewall, filtrado antivirus, detección y prevención de intrusos y control de navegación Web basado en categorías.

Esta parte del proceso de migración tecnológica de Vitalmex fue en su totalidad responsabilidad de quien esto escribe, pues era el especialista del

producto en InfoCorp. Se realizó el análisis de la situación actual y de los requerimientos de operación y de seguridad del cliente; se propuso el modelo de *firewall* que cubría esos requerimientos, considerando cierta holgura para el crecimiento futuro sin perder la mejor relación costo-beneficio.

Se configuró el equipo de acuerdo al plan definido al inicio y se hicieron pruebas piloto de funcionamiento en horario no hábil. Una vez validada la operación adecuada del nuevo *firewall*, se procedió a desconectar permanentemente el anterior. Al siguiente día hábil, los usuarios experimentaron una navegación en Internet más rápida, pero a la vez, vieron bloqueados los accesos a ciertas aplicaciones no autorizadas por la Dirección y que antes no se controlaban. Las posibles molestias de los usuarios, fueron previstas y manejadas a través del área de Recursos Humanos, que informó de las nuevas disposiciones y su fecha de puesta en marcha.

La instalación resultó exitosa y casi no hubo necesidad de hacer correcciones posteriores. A pesar de todo, y como parte del servicio hacia Vitalmex, se continuó siendo responsable del soporte día-a-día del *firewall* y encargado de mantenerlo operando en óptimas condiciones.

La conclusión de las actividades asociadas al cambio tecnológico en Vitalmex se llevó a cabo a la par de los procesos de administración de TI por parte del Coordinador de TI. Se incluyó además, la estandarización de Symantec Antivirus en toda la red y se redujeron grandemente los eventos de virus que comúnmente afectaban a sus equipos.

Mensualmente se tenían reuniones de revisión del proceso de mejora tecnológica y de administración de TI. Se apoyó al Coordinador de TI en la elaboración de reportes y en la solución de algunos problemas varios. El entonces Director de Procesos de Vitalmex (a quien se reportaba directamente), se convirtió en el mejor “publicista” de InfoCorp al interior de Vitalmex, pues estaba muy satisfecho con el desempeño mostrado. Al iniciar el proceso, él era el que más fuertemente cuestionaba y a quien había que demostrar la valía del trabajo desarrollado. Poco a poco, y gracias al trabajo del equipo, se logró ganar su confianza y apoyo incondicional para lograr nuevas mejoras e incluso mejorar el contrato.

Desafortunadamente, ese Director abandonó Vitalmex luego de 2 años y medio de trabajo conjunto. En su lugar llegó un nuevo elemento que estaba acostumbrado a trabajar de forma distinta y que se apoyaba en otras empresas para realizar sus labores. Se trabajó durante 6 meses más en el proyecto, pero el nuevo Director ponía cada vez más trabas y generaba problemas donde no los había.

Durante este período, se instalaron otros dos Symantec Gateway Security, pero ahora modelo1620, para las localidades de Tula y Puebla. Adicionalmente, se migró de la versión 2.5 a la 3.1 en el SGS 5400 instalado en el corporativo.

Al llegarse la fecha de renovación del contrato, el Director presionó tanto en cuanto al precio de los servicios que incapacitó a InfoCorp a seguir con la gama de servicios ofrecidos hasta entonces, pues él deseaba el paquete completo por un 50% del costo. Entonces, él contrató a otra empresa que -supuestamente- haría lo mismo que InfoCorp por el 40% del costo. Así, se inició la fase de “entrega” a los nuevos responsables de TI, y que concluyó con la entrega de

reportes y memorias técnicas de las soluciones administradas y/o implementadas por InfoCorp.

El proyecto Castillo Miranda.

Horwath, Castillo, Miranda y Compañía es una firma de consultores similar a KPMG, pero de menor tamaño y con menor presencia e impacto en el mercado, aunque habían experimentado un gran crecimiento en los últimos meses.

Con este cliente, se vendieron e instalaron 250 licencias de:

- Symantec Antivirus
- Symantec Mail Security para SMTP
- Symantec Gateway Security 5620

Para el caso del antivirus, se desplazó a McAfee por problemas de detección de virus. Se instaló un servidor SAV y una consola de administración; se coordinó la instalación de 120 licencias de SAV. Se realizó la instalación y configuración del SMS para SMTP en versión 4.0 (y un año después la migración a versión 5.0).

La instalación del *firewall* SGS, fue muy sencilla y rápida de realizar (sobre todo, usando la experiencia en Vitalmex). Sin embargo, hubo una funcionalidad que no se habilitaba de forma adecuada: VPNs del tipo L2TP. Aunque se tenía conocimiento de esta utilidad, y aunque se realizó la configuración necesaria, al poner en marcha el SGS, las VPNs no se construían. Después de mucho revisar la configuración, y de ver que no se corregía el problema, se tomó la decisión de no instalar el *firewall* y solicitar soporte a Symantec. Dos días después del primer intento de instalación, y en compañía de un ingeniero de Symantec, se reintentó la conexión del SGS y, con apoyo telefónico de otro ingeniero de Symantec, se logró habilitar la conexión vía VPN.

El cliente experimentó un gran rotación de personal de TI en el último año, lo que redundó en “abandono” de las soluciones antivirus. En InfoCorp se trató de apoyar al cliente con sesiones de capacitación a los nuevos responsables, pero la gran carga de trabajo y los cambios de personal, complicaron el poder operar correctamente. Para poder ayudarles más, se propusieron pólizas de soporte y administración de los productos instalados, con lo cual, los responsables de TI podrían atender otros pendientes mientras InfoCorp se encargaba del antivirus. Sin embargo, el cliente estaba renuente a adquirir estas pólizas, pues consideraba que su personal debería hacerse cargo de todo y sin necesidad de “gastar” en dichas pólizas.

Se inició el proceso de renovación de licenciamiento de Symantec por tercer año consecutivo y se incluyó licenciamiento de Backup Exec.

La fusión Symantec-Veritas.

La relación de InfoCorp con Veritas Software, se inició en el 2003. En ese entonces el trato era con la empresa Seagate Software, quienes fabricaban el software de respaldo líder en ambientes Windows: Backup Exec. Seagate no tenía representación en México e InfoCorp logró ser su distribuidor exclusivo. Toda licencia de Backup Exec vendida en México tenía que ser facturada por InfoCorp, con un porcentaje de ganancia por el procesamiento de las órdenes de compra y la entrega del producto.

La presencia de Backup Exec ganó importancia en México y Seagate decidió establecer una pequeña oficina local, con sólo un representante de ventas y un ingeniero de preventa. El producto continuó posicionándose como líder y pronto fue tal la demanda que Seagate abrió la distribución a otro mayorista: Ingram Micro. Poco después, se incorporaron a otros mayoristas, y la participación de InfoCorp fue disminuyendo cada vez más hasta que se convirtió en "otro" distribuidor más de la marca.

Entonces, Seagate Software consideró que era momento de ampliar sus horizontes y atacar el mercado Unix, por lo que inició una búsqueda mundial de alguna empresa a la cual comprar. Encontraron a Veritas Software, líderes en respaldo de equipos Unix, y al iniciar la negociaciones el comprador resultó comprado: Veritas ofertó por la compra de Seagate y ésta fue absorbida.

Veritas sí contaba con representación local en México y al adquirir a Seagate amplió su abanico de soluciones de respaldo y fortaleció su imagen. En InfoCorp se trabajó entonces con Veritas y bajo su esquema de venta y soporte. No representó un problema el cambio de razón social ni de estrategia comercial.

Dado que el área de respaldos era ya de importancia en InfoCorp, se destinó a uno de los ingenieros de soporte especializado para ser el encargado de las soluciones de Veritas. Así, se asignó a quien esto escribe a dicho ingeniero y –aún sin ser el especialista en Veritas- se coordinaban sus actividades. Se logró su certificación en Backup Exec versiones 8 y 9, consecutivamente y su trabajo impulsó el desarrollo económico de la Empresa.

En el 2005 se informó la decisión de Symantec de adquirir a Veritas Software. Dada la magnitud de la operación se tuvo un proceso largo y complejo a nivel mundial, y sin ser la excepción, en México la fusión tardó demasiado en iniciarse. Durante varios meses, ambas empresas continuaron trabajando por separado e InfoCorp seguía siendo distribuidor de las dos empresas. Una vez iniciado el proceso de fusión en México, se desapareció la razón social de Veritas y ahora todo se facturaba a Symantec. El proceso de fusión requirió de casi dos años para finalizarse y para InfoCorp representó una ventaja el conocer ambas empresas y tener ingenieros para cada solución. Algunas empresas, sólo vendían respaldos y tuvieron que iniciar su aprendizaje de antivirus, y viceversa.

Algo que llamó la atención de propios y extraños, distribuidores y clientes, fue el hecho de que algunos de los puestos de trabajo más importantes en Symantec (incluyendo el de Director General), fueron ocupados por personal de Veritas. Incluso hubo clientes que preguntaban: "¿no que Symantec compró a Veritas? Pareciera ser al revés…"

El proyecto Instituto Mexicano del Petróleo.

En el año 2000 se iniciaron relaciones con el Instituto Mexicano del Petróleo (IMP) al recibir de parte de Symantec la instrucción de visitarles para verificar ciertos problemas que tenían con NAV 7.0. En ese entonces, se visitó a los responsables de TI y personal de soporte en diversas ocasiones para solucionar problemas de instalación y funcionamiento con SAV. El IMP ya no estaba a gusto con su proveedor de Symantec y estaban a punto de cambiar de marca. Symantec asignó a InfoCorp para evitar que se cambiara de marca y ver si se podía crecer el proyecto.

Afortunadamente, esas visitas de soporte "sin compromiso" ayudaron a resolver la mayoría de los problemas y se logró ganar la confianza del personal de TI. Lo anterior, sumado a la intervención del ejecutivo de ventas, logró que para la fecha de vencimiento del licenciamiento de NAV no sólo se renovara por un año más, sino que fue adquirido ahora a través de InfoCorp.

Así inició una relación técnica y comercial que por diversas circunstancias, siendo las más importantes la rotación de personal y la falta de políticas de seguridad, atravesó por múltiples incidencias de virus y que daban la impresión de que NAV no era una solución eficaz.

En todos los casos, se pudo demostrar que NAV sí era efectivo y que los problemas eran ocasionados por otros factores, tales como falta de parches de Windows, falta de administración de NAV, fallas en la seguridad de carpetas compartidas, etc.

Aunque a veces resultaba desgastante, las oportunidades que el IMP dio de demostrar una y otra vez el buen nivel de protección que NAV ofrecía, hicieron que se ganase experiencia en el uso de la herramienta y del manejo de situaciones con mandos medios no técnicos.

Así, al pasar del tiempo, se lograron renovaciones consecutivas del licenciamiento de SAV y ya se incorporaban servicios de valor agregado. Se inició incluyendo 2 ó 3 visitas de soporte gratuito y en sitio –adicional al soporte telefónico ilimitado-, luego se agregaron auditorías a SAV de forma cuatrimestral y posteriormente trimestral y bimestral.

El número de equipos administrados se mantuvo más o menos igual desde el inicio de la relación, contemplando alrededor de 3500 nodos en promedio.

Desde el 2006 se tuvo una relación estable con el Instituto y en 2007 se logró vender la renovación del licenciamiento de Symantec para 3 años (finalizando en 2010).

Las principales actividades en sitio que se desarrollaron en el IMP fueron:

- Auditorías mensuales.

  Se hace un levantamiento de información a través de la consola de Symantec (clientes y servidores visibles en consola, e historial de virus). Se realiza una revisión a las configuraciones de grupo desde la consola y se comenta con el administrador acerca de posibles problemas o dudas que hayan surgido en la operación de SAV. Adicionalmente, se revisa la consola de Symantec Mail

Security para MS Exchange y se toman historiales y se revisa la configuración. Posteriormente, se genera un informe escrito complementado con un reporte estadístico, que incluye observaciones y recomendaciones. Se comprometieron con el IMP un total de 36 visitas de auditoría mensual.

- Migración de SMS MSE.

Se apoyó al responsable del correo para los usuarios de mayor nivel en el Instituto para la instalación de Symantec Antivirus/Filtering 2.5 para MS Exchange y se explicó el proceso de configuración de las políticas de filtrado de contenido y de virus. Cuando se liberó la versión 3, se le proporcionó una copia de la media de instalación y él pudo hacer la instalación. Sin embargo, cuando Symantec generó la versión 4, pidió apoyo para la instalación, que requirió pasos adicionales, pues cambió de SAVF a SMS. Tiempo después, se liberó la versión 5 de SMS y el responsable del correo tuvo problemas para la migración. Se asistió en sitio para verificar el problema y fue necesario desinstalar la versión anterior e iniciar prácticamente desde cero.

- Implementación de SMS 8300.

El *appliance* SMS 8300 adquirido por el IMP en el 2007 fue puesto primero en modo de prueba para validar su funcionamiento y eficacia. Una vez que se comprobó que operaba correctamente, se realizó la configuración requerida para implementarse definitivamente en producción. El equipo estuvo funcionando por unas semanas, pero empezó a generar algunos problemas de caída del sistema, lo cual fue corregido por Symantec con diversos parches. Después de varias correcciones y pruebas, se volvió a poner en funcionamiento, pero días después se detectó que se estaban generando correos no deseados. Se validó con Symantec y se realizo la configuración recomendada, lo que eliminó este problema. El SMS quedó en producción y detectaba un promedio de 90% de correo entrante como *spam*.

- Inicio de planeación para migración a SEP 11

Al igual que con muchos otros clientes, con el IMP se inició el proceso de evaluación de la nueva solución antivirus de Symantec, llamada Symantec EndPoint Protection. Dado que la migración no es tan transparente como en casos anteriores, se brindó apoyo en la planeación de las pruebas piloto y en la elaboración del plan de migración.

Se observó una gran mejoría en la seguridad de la red del IMP, originada –primeramente- por el trabajo de administración de SAV realizado por el personal del Instituto, y por el grado de integración técnica que se logró con ellos. Se avanzó enormemente en los procesos de comunicación, lo que coadyuvó a reducir tiempos de respuesta y a mejorar la percepción del servicio de InfoCorp y de la calidad de los productos de Symantec.

El proyecto Comercial Mexicana.

Al igual que en el caso del IMP, Symantec indicó que se debía visitar este corporativo porque el distribuidor que estaba asignado no estaba cumpliendo las expectativas del cliente. A finales del 2005 se inició con una auditoría de la estructura SAV instalada y se encontró que no había ningún control real del antivirus. Operativamente, esta empresa se encuentra dividida en corporativos y tiendas. El 65% de los equipos de la red corresponden a las tiendas mientras que el 35% restante se encuentra dividido en los corporativos. Cada área era responsable de una porción de equipos, por lo que no se contemplaba como un todo: no había estándares de configuración, había múltiples versiones instaladas, nadie monitoreaba las actualizaciones de definiciones de virus y en consecuencia, había gran cantidad de problemas de virus. En esa primera auditoría, sólo se veían en consola 1636 clientes y 9 servidores SAV.

Al principio, todos los servicios fueron ofrecidos sin costo y sin haber vendido ninguna licencia al cliente, pues se "apostó" a lograr que la renovación del licenciamiento se lograra ahora a través de InfoCorp. Y así fue.

Una vez lograda la renovación con InfoCorp, se incluyeron servicios de valor agregado, consistentes básicamente en auditorías mensuales y soporte telefónico. Durante la mayor parte del 2006, los resultados de las auditorías mostraban muy pocas mejoras en lo relativo a la administración.

La tabla 1 muestra las fluctuaciones presentadas en 2006:

Mes	Total de cliente visibles en consola	Porcentaje de clientes con definiciones de virus al día
Julio 2005	1636	92%
Marzo 2006	1238	79%
Abril 2006	1271	77%
Mayo 2006	1575	85%
Julio 2006	2736	81%
Agosto 2006	2965	19%
Septiembre 2006	4917	44%
Octubre 2006	3536	62%
Noviembre 2006	4750	72%

Tabla 1. Resultado de las auditorías realizadas en CM durante el 2006.

De lo más relevante por mencionar, respecto a la Tabla 1, es que aunque el número de clientes visibles en consola se iba incrementando por la incorporación de más servidores de tiendas (que antes no se veían en consola), el porcentaje de equipos actualizados en definiciones de virus mostraba grandes fluctuaciones, pero con una tendencia a la baja. Adicionalmente, el problema de tener más de 7 diferentes versiones de SAV en toda la red derivaba en poco control de nuevas amenazas. Aunque aún había un 35% de equipos Windows 9x (que no soportarían la versión 10 de SAV), había un gran porcentaje de equipos XP y 2000 que tenían versiones viejas de NAV y que deberían tener la 10.

Nuevamente estaba por vencer el período de mantenimiento del licenciamiento de Symantec y Comercial Mexicana no estaba muy segura de renovar el licenciamiento, pues a su parecer el antivirus no estaba siendo 100% útil. Se hizo labor de venta y se mencionaron los casos de KPMG, IMP y Pepsi, e incluso se presentaron ejemplos de reportes –previa autorización de los clientes y sin revelar información confidencial-. Después de una gran labor, se logró vender el contrato de administración semanal de SAV para Comercial Mexicana, y se tomó responsabilidad del mismo, por el tamaño del cliente y el número de problemas que había que enfrentar.

Así, el martes 2 de enero de 2007 se realizó la primera visita de administración semanal de SAV. El servicio consistía en revisar, cada martes del año, la consola de SAV y generar reportes semanales, mensuales y semestrales de lo visible en consola, reportar los problemas encontrados y dar soporte al personal de TI de Comercial Mexicana. El alcance estaba limitado por costos, pero contemplaba un posible crecimiento de equipos a administrar, considerando hasta 6500.

Durante todo el 2007, se realizaron las visitas semanales y se cumplió con los reportes comprometidos. Aunque se empezó a notar mejoría en el uso de SAV y el número de eventos de virus comenzó a disminuir gracias al seguimiento preventivo realizado cada semana, fue una realidad que pasaron muchos meses antes de poder considerar la plataforma como estable. Las excesivas ocupaciones del personal de TI les impedían atender los problemas reportados cada semana, y podían pasar semanas sin que se resolvieran.

Por esa razón, en julio del 2007, en la presentación semestral de resultados ante la subdirección de TI, se informó del estado general de la estructura SAV y se mencionaron los problemas encontrados y la forma en que se estaban atacando, pero que lograr una mayor estabilidad estaba tomando más tiempo del previsto. El personal de TI se comprometió a resolver los problemas en menos tiempo y en vincular a más personas, pero los resultados aún tardaron en mostrarse.

Las tablas 2 y 3 muestran la evolución mostrada durante la administración de SAV en el 2007:

	Enero 07	Febrero 07	Marzo 07	Abril 07	Mayo 07	Junio 07
Total de clientes	5121	5210	5181	5176	5198	5333
Porcentaje de clientes con definiciones al día (total)	65%	32%	89%	92%	90%	89%
Porcentaje de clientes que nunca han ejecutado un análisis contra virus	19%	41%	41%	41%	39%	39%
Servidores visibles en consola	172	175	177	179	185	182
Eventos de virus reportados en el mes	13639	65459	65487	53359	57344	42177
Diferentes virus reportados en el mes	54	82	96	92	106	110
Clientes con eventos de virus	77	300	268	356	381	438
Porcentaje de equipos con virus	2%	6%	5%	7%	7%	8%

Tabla 2. Información estadística de SAV en CM durante el primer semestre del 2007.

	Julio 07	Agosto 07	Septiembre 07	Octubre 07	Noviembre 07	Diciembre 07
Total de clientes	5139	5001	4656	4802	4929	5519
Porcentaje de clientes con definiciones al día (total)	85%	75%	87%	88%	83%	79%
Porcentaje de clientes que nunca han ejecutado un análisis contra virus	37%	35%	29%	19%	16%	13%
Servidores visibles en consola	179	175	181	182	184	188
Eventos de virus reportados en el mes	15069	15516	19117	39737	31050	21221
Diferentes virus reportados en el mes	111	102	103	114	127	115
Clientes con eventos de virus	466	485	440	476	480	560
Porcentaje de equipos con virus	9%	10%	9%	10%	10%	10%

Tabla 3. Información estadística de SAV en CM durante el segundo semestre del 2007.

Para comprender mejor las tablas 2 y 3, es necesario tener en cuenta las siguientes consideraciones:

- El número de clientes comenzó a crecer conforme se incorporaban servidores de tiendas a la consola.

- A partir de septiembre, se inició el cambio de versión SAV a la 10, pero aunque se migraban los servidores, los clientes no eran actualizados y por tanto no aparecían en consola.

- El número de eventos de virus, de diferentes virus y de clientes con eventos de virus no disminuía (y en algunos meses mostró una tendencia a la alza). Esto era ocasionado porque no existían políticas de uso aceptable del equipo de cómputo y los usuarios no tenían conciencia del riesgo que corren sus equipos al introducir memorias USB de la escuela, casa o de amigos.

Se trabajó con el personal de Comercial Mexicana para iniciar una campaña de concientización para los usuarios, a fin de reducir el impacto, pero no se logró avanzar de forma masiva.

A lo largo del año 2007 se impartieron 4 sesiones de capacitación de SAV y su administración al personal de TI de Comercial Mexicana, a fin de darles elementos para poder resolver problemas del día a día por sus medios y para aprovechar la consola de SAV y sus funciones.

Se crearon más de 14 procedimientos personalizados para la instalación, corrección de problemas, limpieza de virus, migración y configuración de SAV, de acuerdo a las necesidades expresadas por Comercial Mexicana.

Gracias a la labor realizada, se logró a finales de 2007 renovar el licenciamiento de Symantec por 2 años más, así como la renovación del contrato de administración semanal de SAV.

A pesar de que Comercial Mexicana pertenece a un grupo de empresas, para la operación de tiendas se considera solamente los formatos de tiendas Al Precio,

Bodega Comercial Mexicana, Tienda Comercial Mexicana, Mega Comercial Mexicana, City Market y Sumesa (formato por desaparecer y ser reemplazado por Al Precio).

Para diciembre del 2007, se manejaban servidores antivirus para cada una de las siguientes localidades y tiendas:

- Al Precio Chalco
- Al Precio Costitlán
- Al Precio Lerma
- Al Precio Marte
- Al Precio Ojo de Agua
- Al Precio Plan de Ayala
- Al Precio Temixco
- Al Precio Yautepec
- Bodega Acapulco Renacimiento
- Bodega Acozac
- Bodega Actopan
- Bodega Aguascalientes I
- Bodega Aguascalientes III Casa Blanca
- Bodega Azcapotzalco
- Bodega Center Plaza
- Bodega Centro
- Bodega Chalco Centro
- Bodega Chalco Galerías
- Bodega Coacalco I
- Bodega Cuautepec
- Bodega Ecatepec Centro
- Bodega Ecatepec Vía Morelos
- Bodega Insurgentes
- Bodega Irapuato
- Bodega Iztapalapa
- Bodega Iztapalapa Las Torres
- Bodega Jojutla
- Bodega La Merced
- Bodega Las Armas
- Bodega López Portillo
- Bodega Naucalpan
- Bodega San Juan de Aragón
- Bodega San Luis Potosí Río Verde
- Bodega Sta. Ma. la Rivera
- Bodega Tacuba
- Bodega Tenayuca
- Bodega Teoloyucan
- Bodega Tepeji del Río
- Bodega Texcoco Centro
- Bodega Tlalnepantla
- Bodega Tlalpan
- Bodega Toluca II
- Bodega Tultitlán
- Bodega Veracruz II
- Bodega Xochimilco
- Bodega Zaragoza
- Bodega Zumpango
- City Market
- CorporativoMixcoac
- CorporativoSan Mateo
- CorporativoSatélite
- CorporativoTultitlán
- CorporativoVallejo
- Mega Alamedas
- Mega Angelópolis
- Mega Arboledas II
- Mega Atizapán
- Mega Av. Central
- Mega Boca del Río Veracruz
- Mega Campeche
- Mega Cancún III
- Mega Cancún IV Niños Héroes
- Mega Casino de la Selva
- Mega Coacalco
- Mega Coapa
- Mega Coatzacoalcos
- Mega Coyoacán
- Mega Cuautitlán Izcalli
- Mega Cuautla
- Mega Cuernavaca
- Mega Diamante
- Mega El Olivar
- Mega Ensenada
- Mega Estadio
- Mega Flamingos
- Mega Gran Sur
- Mega Guadalajara
- Mega Izcalli
- Mega Jalapa
- Mega Jiupetec
- Mega La Cascada Los Cabos
- Mega Las Flores
- Mega Las Palmas
- Mega León
- Mega Los Reyes
- Mega Mazatlán
- Mega Mérida Balcones
- Mega Metepec
- Mega Mexicali Anáhuac
- Mega Mexicali Carranza
- Mega Mexicali Triángulo

- Mega Morelia Chapultepec
- Mega Morelia Independencia
- Mega Naciones
- Mega Nuevo Vallarta
- Mega Pachuca
- Mega Pilares
- Mega Playa del Carmen
- Mega Pozuelos
- Mega Puebla
- Mega Puebla II
- Mega Pueblo Nuevo
- Mega Rojo Gómez
- Mega Rosarito Villa Turística
- Mega San Luis Potosí Tangamanga
- Mega San Jerónimo
- Mega San Mateo
- Mega San Miguel de Allende
- Mega San Miguel Huehuetoca
- Mega Satélite
- Mega Tampico Alijadores
- Mega Tijuana Oasis
- Mega Tlatelolco
- Mega Tres Ríos
- Mega Tulancingo
- Mega Vía Morelos
- Sumesa Arboledas
- Sumesa Bajío
- Sumesa Centenario
- Sumesa Colima
- Sumesa Lomas
- Sumesa Londres
- Sumesa Mier y Pesado
- Sumesa Oaxaca
- Sumesa Pilares
- Sumesa Polanco
- Sumesa San Ángel
- Sumesa San Diego
- Sumesa Valle
- Sumesa Yucatán
- Tienda Acapulco Costa Azul
- Tienda Acapulco I
- Tienda Acapulco II
- Tienda Acapulco III
- Tienda Aguascalientes II
- Tienda Aragón
- Tienda Asturias
- Tienda Cancún II
- Tienda Celaya III
- Tienda Chilpancingo
- Tienda Coapa
- Tienda Cuernavaca I
- Tienda Cuernavaca III
- Tienda Culiacán
- Tienda El Dorado
- Tienda Ermita Iztapalapa
- Tienda Guadalajara las fuentes
- Tienda Guanajuato
- Tienda Irapuato
- Tienda Ixtapa Zihuatanejo
- Tienda La Herradura
- Tienda La Viga
- Tienda La Villa
- Tienda León Campestre
- Tienda León Insurgentes
- Tienda Lomas Anáhuac
- Tienda Manzanillo
- Tienda Mérida
- Tienda Mixcoac
- Tienda Morelia II
- Tienda Morelia III
- Tienda Nezahualcóyotl
- Tienda Pabellón Bosques
- Tienda Plaza Coacalco
- Tienda Puebla I
- Tienda Puebla III
- Tienda Querétaro I
- Tienda Querétaro Plaza del Parque
- Tienda Salamanca II
- Tienda San Juan del Rio
- Tienda San Luis Potosí I
- Tienda Satélite
- Tienda Texcoco
- Tienda Tijuana Carrusel
- Tienda Tijuana Los Pinos
- Tienda Tijuana Otay
- Tienda Tijuana Playas
- Tienda Tijuana Plaza Dorada
- Tienda Tijuana Río
- Tienda Tijuana Rosarito
- Tienda Tijuana Santa Fe
- Tienda Toluca I
- Tienda Tulyehualco
- Tienda Uruapan
- Tienda Vallarta Marina
- Tienda Vallarta Satélite
- Tienda Villacoapa
- Tienda Villas de la Hacienda
- Tienda Zamora

Dando un total de.

Al Precio:	8 Tiendas
Bodega:	39 Tiendas
City Market:	1 Tienda
Mega:	63 Tiendas
Sumesa:	14 Tiendas
Tienda:	59 Tiendas
Corporativo:	5 Corporativos
Total:	189 Localidades

Adicionalmente, se tuvo la responsabilidad de instalar Symantec Mail Security para MS Exchange 5 en los 2 servidores de correo de Comercial Mexicana así como de su administración semanal. También se instaló, usó y administró durante 1 año un *appliance* Symantec Mail Security 8300 para protección perimetral al correo electrónico (sobre todo para el manejo de *spam*); sin embargo, y derivado de un mal manejo del licenciamiento por parte de Symantec (en donde se utilizaban sólo licencias temporales de 30 días cada una), Comercial Mexicana tomó la decisión de reemplazar dicha solución por un equipo de IronPort.

La administración en Comercial Mexicana fue el proyecto más grande y de mayor duración en el que se participó. Gracias al esfuerzo conjunto, se logró estabilizar la red corporativa y reducir las afectaciones por ataques virales. Además, se logró que el personal de TI pudiera "vender" internamente el uso de SAV y el contrato de administración como una excelente inversión que maximizaba los beneficios de la solución adquirida.

Inicio de relación con Juniper Networks.

Durante muchos años, el foco de negocios de InfoCorp se centró exclusivamente en soluciones de Symantec. Hubo algunos intentos de generar alianzas con otros fabricantes (que no representaran competencia para Symantec), pero por distintas razones (casi siempre comerciales) no prosperaban.

Para el caso de protección perimetral de la red a través de un *firewall* con UTM (Unified Threat Management, Manejo unificado de amenazas), Symantec ofrecía tres familias de *firewall* bajo el nombre "Symantec Gateway Security":

- La serie 400: para pequeñas redes, oficinas remotas o sucursales
- La serie 1600:para redes medianas, y
- La serie 5600: para grandes corporativos

En InfoCorp, se instalaron varios SGS y ya se tenía cierto dominio sobre los productos. Pero a finales del 2006, Symantec anunció el fin del ciclo de ventas de todas las familias de *firewall* Symantec Gateway Security y se "invitaba" a todos los distribuidores y socios a acercarse a Juniper Networks, pues se había hecho una asociación entre ambas empresas: Juniper proveería los *appliances* y la tecnología de *firewall*, y Symantec proveería las firmas y mecanismos de filtrado contra virus, *spam* y filtrado Web.

El plan de Symantec era dejar de vender SGS a partir de enero del 2007, seguir soportando el producto hasta finales del 2009 y desaparecer el producto para el 2010. La asociación con Juniper mostraría sus primeros frutos en 2008.

Así las cosas, y con un requerimiento de venta de un *firewall* en puerta, se contactó a Juniper y se nos hizo una presentación formal de esa empresa y sus soluciones.

Juniper se mostró sumamente interesado en recibir a los distribuidores de Symantec, pues al tener poco tiempo de estar en México, su red de distribuidores no era tan madura como deseaban. En cambio, los distribuidores de Symantec ya tenían más experiencia y sólo faltaría familiarizarse con sus productos. A fin de cuentas, un *firewall* es un concepto genérico y sólo era necesario mencionar cómo se trabaja en Juniper.

Como parte de la bienvenida de Juniper, se nos otorgó una breve capacitación del sistema ScreenOS y la familia pequeña de los firewall que manejaban. Esta familia, se basa en la tecnología creada por Netscreen y que fue adquirida y mejorada por Juniper.

El ingeniero de Juniper que dio la capacitación quedó tan impresionado por aprendizaje del personal de InfoCorp que comentó con el ejecutivo de ventas asignado que debían proveer más incentivos. A los 2 días de haber recibido la capacitación, Juniper hizo llegar a InfoCorp un *firewall* 5GT completamente gratis, a fin de usarlo como laboratorio y poder lograr la certificación a la brevedad.

Lamentablemente, el foco de negocios de InfoCorp no contempló desarrollar más esta rama y se indicó que sólo se debía hacer lo mínimo necesario para cerrar la venta que se tenía en puerta. A pesar de ello, se logró crear una buena relación con el personal técnico de preventa de Juniper e incluso se tuvo su apoyo en la implementación de 2 *firewalls*.

No se avanzó en la certificación porque no había entrenamiento en México y porque, en ese momento, sólo se deseaba cerrar una venta.

En opinión de quien esto escribe, los equipos de Juniper son muy superiores a los de Symantec: son más fáciles de usar, son más pequeños y más poderosos. Pareciera ser que Symantec se dio cuenta de que no era líder en ese segmento y por tanto decidió salir.

El proyecto PrestaComer.

A finales del 2006 se inició relación con esta empresa -que es el banco de Comercial Mexicana- a través de la venta del licenciamiento de SAV y originada por la excelente relación que se logró con esta última.

Para la implementación de SAV, se designó a uno de los ingenieros a cargo de un servidor para realizar las tareas necesarias y no perder el prestigio que abrió las puertas a esta cuenta. Los resultados fueron satisfactorios y PrestaComer solicitó

apoyo para implementar un *firewall* perimetral. PrestaComer prácticamente acababa de nacer y apenas se estaba terminando de definir la infraestructura sobre la que basaría su operación.

Se inició entonces el levantamiento de información para poder dimensionar el modelo de *firewall* que se les ofrecería. Dado que el número de usuarios no era muy grande (cerca de 100 usuarios), se ofertó un modelo intermedio de la familia de *firewalls* de Symantec. Se tuvieron reuniones de planeación e incluso se llevó el equipo a las instalaciones del cliente en Polanco. Sin embargo, en esas fechas se dio el fin del ciclo de ventas y se tuvo que desechar la idea de usar un SGS de Symantec y cambiar a un equivalente de Juniper.

Se utilizó la información que ya se tenía, y personal de Juniper validó la propuesta de arquitectura que se había planteado para la demostración del equipo. Se definió usar un *firewall* pequeño compatible con ADSL y se contó con el apoyo de personal de Juniper para su instalación.

En esencia, el equipo no dio problemas graves durante la demostración y aunque se tuvieron que atender varias llamadas de soporte telefónico, no fue en realidad por mal funcionamiento, sino por dudas del personal de PrestaComer.

Aunque se delimitó con certeza qué configuración se implementaría en el *firewall*, y el cliente lo aceptó, conforme veían que el equipo ofrecía más funciones, se solicitaba que se configuraran más cosas. Muchas de ellas se realizaron de forma remota usando la consola Web y otras se resolvieron a través de llamadas telefónicas. El ejecutivo de ventas de InfoCorp para PrestaComer no deseaba que se pusiera ninguna traba a los requerimientos del cliente, pero era una realidad que la demostración se estaba alargando y el cliente estaba sobre-utilizando el equipo y el servicio de InfoCorp sin mostrar deseos de finalizar la demostración y realizar la compra del equipo.

Se coordinó la nueva delimitación de la demostración y el cierre exitoso de la misma. El cliente decidió comprar 2 *firewalls* más grandes que el demostrado y con todos los módulos disponibles.

Se liberó la orden de compra pero los equipos tardarían en llegar, y el cliente tenía necesidad de proteger la red de su nueva oficina en Reforma y Constituyentes sin quitar el *firewall* instalado en Polanco. Se negoció con Juniper el préstamo de un segundo equipo y se tuvo la responsabilidad de configurarlo y de conectarlo a la nueva red. Se contó nuevamente con el apoyo del personal de Juniper, pero ya sólo fue a nivel de revisión de configuración y no de implementación.

Se logró configurar correctamente el equipo y se tuvo la responsabilidad de brindar soporte telefónico y remoto al administrador del *firewall* en PrestaComer en los días siguientes.

Posteriormente, llegaron los equipos comprados y se solicitó apoyo a InfoCorp para cambiar el equipo instalado en Reforma. Aunque el cambio hubiera sido de lo más sencillo, el cliente había hecho algunos cambios en la planeación de su red y se incorporó un balanceador de carga para manejar dos enlaces a Internet. Por tanto, se tuvieron reuniones con PrestaComer y con un distribuidor de Foundry Networks, para planear la implementación de la nueva estructura.

Una vez que se definió el nuevo esquema de red y que hubo coordinación en cuanto a las interacciones de los sistemas, se agendó la instalación. Se realizó toda

la configuración del *firewall* fuera de línea, y cuando se informó que el dispositivo de Foundry estaba listo, se realizó la conexión, en esta ocasión sin solicitar el apoyo de Juniper. Inicialmente no funcionó el tráfico entrante a la red, pero se debió a fallas en el equipo Foundry. Una vez corregido el problema, todo funcionó transparentemente para el usuario.

Días después de la implementación se reportó que había problemas de lentitud extrema en la navegación cuando usaban los dos enlaces a Internet; si se usaba uno sólo –cualquiera- la navegación era normal. Se aplicaron los conocimientos que se tenían hasta el momento para tratar de resolver el problema, pero no eran elementos suficientes para resolverlo. Entonces, se comentó con el cliente la necesidad de levantar un reporte al soporte de Juniper. Se les ayudó a dar de alta la póliza de soporte y se levantó el caso vía Web. El soporte de Juniper en E.U. se comunicó con el cliente y empezaron a verificar el problema; sin embargo, el cliente estaba teniendo problemas para entender al soporte en inglés, por lo que hubo necesidad de actuar como intermediario (e intérprete) entre el cliente y Juniper. Se enviaron múltiples registros e historiales, y el problema llevaba ya dos semanas sin resolverse.

En un último intento, se sugirió cambiar los DNS del *firewall* y el técnico de Juniper en E.U. dijo que no era necesario. Sin embargo, le dio la idea de usar otro DNS en un equipo de la red (en lugar de usar el definido en el Active Directory). El resultado fue sorpresivo: la navegación fue rápida. Entonces se determinó que el problema era el DNS, que al usar los dos enlaces, causaba una gran lentitud. Juniper dio por cerrado el caso y el cliente tuvo que validar por su cuenta el DNS. Lo hicieron y ya no hubo problemas de navegación al usar los dos enlaces.

Se siguió apoyándoles con consultas y soporte de antivirus y se proporcionó soporte esporádico al *firewall*, pues hubo nuevos requerimientos de operación. La naturaleza del proyecto ayudó a comprender más el funcionamiento de los equipos Juniper y confirmó la idea de que son equipos más flexibles y poderosos que los que Symantec fabricaba.

El proyecto Televisa San Ángel.

En octubre del 2006 se tuvo un requerimiento de soporte para el área de Postproducción de Audio y Video de Televisa San Ángel. El problema que tenían era saturación del ancho de banda de la red y alto uso de memoria y procesador en muchos equipos. Ya habían intentado instalar otros antivirus pero las ventanas se cerraban inexplicablemente. Cuando se informó del problema, se supo que tenían el virus de "moda" en ese momento: W32.BlackMal.E@mm (como lo llamó Symantec) o Kamasutra como lo llamaban otros antivirus.

En esta parte de la red, ninguno de los equipos contaba con antivirus, pues hasta poco antes de la infección, era una red aislada que funcionaba de la siguiente manera:

- Los contenidos son grabados en los foros.
- Estas grabaciones se almacenan en discos de red compartidos (NAS).

- Hay varios servidores que administran cada uno entre 3 y 5 programas (en su mayoría telenovelas) y que brindan acceso a los videos.
- Los editores, productores y actores, pueden revisar posteriormente el contenido grabado, y decidir qué se queda y se transmitirá y qué se almacena sin ser televisado, utilizando para ello cabinas de edición con equipos para el manejo de video.
- Adicionalmente, se elige qué contenido se pasará a Alta Definición.
- Todo se maneja utilizando tecnología para manejo de videos de la marca Avid.

Mientras la red se mantuvo de esa forma, no tuvieron nunca problemas de virus, pues no había ningún método de infección: no había Internet ni correo, no se usaban medios de almacenamiento extraíbles y la red estaba aislada físicamente del resto de la red de Televisa.

El problema se presentó cuando por requerimientos de otras áreas, tuvieron que conectar físicamente esta red a una red que estaba conectada a su vez al resto del corporativo. Aunque el estándar de antivirus en todo Televisa era el antivirus de Trend Micro, era un hecho que la red tenía problemas de virus.

Una vez entendido el problema y la estructura, se usó la herramienta de eliminación creada por Symantec en uno de los servidores más afectados e inmediatamente desaparecieron los síntomas. Sin embargo, al estar en red con equipos infectados, se volvió a infectar al poco tiempo. Entonces se explicó la necesidad de instalar SAV en todos los equipos de la red. Ese día, se ayudó a eliminar el virus e instalar SAV en 7 servidores críticos. El personal de Audio y Video –que no eran especialistas en TI- aprendió el proceso y se comprometió a replicarlo en el resto de los equipos. Parte del problema era que algunos servidores no podían ser tocados mientras se estuviera grabando, por lo que tendrían que esperar ventanas de tiempo en la madrugada.

Al otro día, se dio seguimiento telefónico y el problema estaba controlado. Inmediatamente, y usando la facultad de poder destinar su presupuesto de forma independiente, el área de PostProducción hizo una orden de compra a InfoCorp por licencias de SAV, soporte en sitio, auditorías mensuales e implementación y capacitación del producto.

Una vez que los trámites administrativos se arreglaron, se asistió en sitio para instalar –ya con más calma- la consola de administración de SAV y dar una breve explicación de su uso. Días después, se impartió capacitación formal a 15 técnicos de audio y video y se resolvieron dudas que tenían.

Se coordinó el calendario de auditorías y se asignó a otro ingeniero de InfoCorp para que él se encargara de realizarlas. Se monitoreó esa actividad mensual y se revisaba con él los reportes antes de enviarlos al cliente.

Todo estuvo trabajando de maravilla durante 11 de los 12 meses del contrato inicial.

En diciembre del 2007, se reportó un problema de lentitud en los servidores Avid. Esta lentitud ocasionaba grandes retrasos en la postproducción y solicitaron una visita en sitio.

Cuando se llegó a las oficinas del cliente, el especialista de Avid ya estaba ahí y se conversó acerca de cuál era el problema: él decía que hacía pocos días se

había migrado la versión de SAV a una más reciente y que eso estaba ocasionando el problema. Dicha migración fue realizada por el ingeniero de InfoCorp a cargo del proyecto y él no había reportado problema alguno. Se comentó con el especialista de Avid que no era imposible que hubiera alguna incompatibilidad, pero que sí era sumamente improbable. Se preguntó si habían hecho algún cambio en la configuración de Avid y la respuesta fue un rotundo "no". Se realizaron algunas pruebas de configuración en SAV y el desempeño se veía normal. Se solicitó al especialista de Avid la configuración recomendada para trabajar con cualquier antivirus, pero aunque llamó a E.U. nunca facilitó esa información. El personal de PostProducción en su intento por resolver el problema, ya había desactivado el antivirus en todos los equipos, pero el problema continuaba. Se comentó que el desactivar el antivirus era la mejor forma de probar que SAV no era responsable del problema, pero eso no convenció a Avid.

Como ya habían detectado que había dos períodos del día en que se presentaba con más notoriedad la lentitud, a las 11:00 AM y a las 7:00 PM, se propuso esperar al período de las 7:00 PM y ver si los ajustes que se habían hecho al antivirus evitaban la lentitud. Se pidió que en caso de que el problema se presentara, se desinstalara SAV para descartar completamente la interferencia de SAV y todos los presentes, incluyendo al especialista de Avid, estuvieron de acuerdo.

Ese mismo día, pero a las 8:00 PM, se recibió llamada del ejecutivo de cuenta de InfoCorp para Televisa, indicando que había muchos problemas con el cliente y que se requería presencia en sitio con urgencia. Se asistió nuevamente en sitio y el problema fue que el personal administrativo de Avid asignado a Televisa hizo un escándalo porque se había recomendado quitar SAV (recomendación hecha casi 10 horas antes y que su especialista había aceptado) y ellos no lo aceptaban como válido, pues ponía en riesgo toda la red (siendo que SAV llevaba desactivado 3 días). Como Avid seguía insistiendo que el problema era ocasionado por el cambio de versión y lo hablaron con el Vicepresidente de Telenovelas, se dio la orden de regresar SAV a la versión anterior. El problema tomó tal magnitud que no sólo se veía amenazada la renovación del licenciamiento de SAV, sino el empleo de los jefes de PostProducción.

En la madrugada, se desinstaló la versión reciente de SAV y se instaló en todos los servidores y clientes la versión anterior que supuestamente no ocasionaba el problema. Se acordó esperar a las 11:00 AM para ver si el problema se volvía a presentar, y se indicó que no era necesario que se estuviera presente. Mientras tanto se comentó que se iba a verificar la fecha exacta de la migración de versión de SAV.

A las 11:00 AM, el resultado fue el que se esperaba: la lentitud seguía. Se validó la fecha de migración, y había sido realizada tres meses antes del inicio de la lentitud. Se comentó esta información con el cliente, y confirmaron, con las bitácoras que InfoCorp les había entregado, que era correcto. También investigaron con Avid, y descubrieron que unos días antes habían hecho una migración de versión e incorporación de más discos al arreglo, y que fue a partir de eso que empezaron los problemas.

El personal de PostProducción coincidió con InfoCorp en que la actitud del personal de Avid no fue correcta, y que lejos de buscar soluciones, quisieron culpar a InfoCorp, atacaron y ocultaron información. El jefe de PostProducción comentó incluso comentaron que tenía un documento de Avid en donde les recomendaban no tener ningún antivirus instalado (y luego se ofendieron ante la propuesta de quitar SAV para probar).

Obviamente, ya no hubo necesidad de asistir en sitio una vez más. Avid realizó una reconstrucción de la base de datos y el problema desapareció.

A los pocos días, se recibió la nueva orden de compra para un año más de servicios y licenciamiento.

Certificaciones.

Antes de la fusión de Symantec con Veritas, el esquema de entrenamiento y certificación para Symantec, estaba subcontratado con tercero. Los cursos los daba la empresa Aster y los exámenes se realizaban en centros Prometric (al igual que las certificaciones de Microsoft). Bajo ese esquema, se lograron algunas de las certificaciones mencionadas en los capítulos anteriores.

A finales del 2004, Symantec cambió su política de certificación e incluyó un requerimiento adicional: para ser reconocido por Symantec, se debía presentar el comprobante de certificación en seguridad de un tercero. Las certificaciones aceptadas (por orden de complejidad) eran:

- CompTIA – Security+
- CISSP
- GIAC SANS

Por cuestiones de costo, en InfoCorp se decidió que los ingenieros presentaran el examen más económico: el de CompTIA.

Dado que no existía un curso de preparación para el examen, se recomendó tomar el curso "MOC 2810A Fundamentals of Network Security" de Microsoft. El curso tuvo una duración de una semana y se realizó en Aster en noviembre del 2004. En los dos primeros intentos para pasar el examen no se logró aprobarlos; al tercer intento, realizado el 17 de marzo de 2005, se logró aprobar el examen.

Aunque semanas antes ya se había presentado y aprobado -al primer intento- el examen de certificación para Symantec Antivirus, no se adjudicó la certificación hasta que no se presentó la certificación de CompTIA.

Bajo este esquema, se lograron las siguientes certificaciones:

SYMANTEC CERTIFIED TECHNOLOGY ARCHITECT
Firewall & Integrated Security Appliances Solutions.
Vigente desde: 09 de agosto de 2005.

CompTIA
Security+ Certified Professional
Vigente desde: 17 de marzo de 2005.

Luego de la fusión con Veritas, y dado que esta empresa sí contaba con un área propia de entrenamiento, se intentó centralizar el entrenamiento y dejar de usar proveedores. Los cursos fueron impartidos entonces por personal de Symantec (a un costo muy elevado) y ya no se hacían exámenes Prometric, sino basados en Web y usando el portal de socios de Symantec. Ya no se requería la certificación del tercero en seguridad.

Considerando este nuevo esquema, en junio del 2007 se lograron las siguientes certificaciones:

SYMANTEC TECHNICAL SPECIALIST
Symantec AntiVirus 10 / Symantec Client Security 3

SYMANTEC TECHNICAL SPECIALIST
Symantec Backup Exec System Recovery 6.5

SYMANTEC SALES EXPERT
Symantec AntiVirus 10 / Symantec Client Security 3

SYMANTEC SALES EXPERT
Symantec Mail Security for SMTP Gateway 5

Relación con Symantec.

Gracias al buen trabajo desarrollado en equipo (tanto por la parte técnica como por la comercial) se logró mantener una excelente relación con Symantec. En múltiples ocasiones, InfoCorp fue de los 3 distribuidores que más vendían y se tuvo el reconocimiento de ser considerado uno de los 5 mejores socios de Symantec.

Se pasó de ser socio de tipo "*Gold*" a ser "*Platinum*", que es el nivel más alto que un distribuidor puede aspirar. Algunos de los contratos de servicios y licenciamiento más largos y duraderos que tenía Symantec, fueron logrados y administrados por InfoCorp.

Gracias a ese desempeño, InfoCorp fue invitado por Symantec para ser parte del grupo de "Symantec Technical Support Partner Program" (TSPP) para el área de disponibilidad de datos. Este esquema, ofrecía la oportunidad de brindar servicios de soporte e implementación en nombre de Symantec. Sin embargo, el foco de negocio

de InfoCorp era la seguridad, y no la disponibilidad, por lo que no se contaba con los recursos necesarios para entrar al programa y se decidió no invertir en él. Cabe mencionar que la invitación no vino de parte de Symantec México, sino del corporativo en E.U.

Por otra parte, quien esto escribe fue uno de los únicos cinco ingenieros (no empleados de Symantec) que fueron invitados a ser parte activa de los foros de discusión de la recién creada “Symantec Technology Network”. Esta iniciativa de Symantec a nivel mundial, buscaba dar más elementos de soporte a la comunidad de usuarios. El nivel de acceso que se otorgó fue más allá del simple usuario, y aunque no llegó a ser el de un Ingeniero de Symantec, en sí ya era un reconocimiento a la experiencia y conocimiento.

Conclusiones.

Hacer un recuento de estos diez años de vida profesional ha servido para reforzar la conciencia de que aún hay mucho por aprender.

En Tecnologías de la Información, el mundo cambia y evoluciona constantemente. Lo que hoy es novedad, en semanas será obsoleto. Es una realidad que no se puede ser especialista de todo; y a pesar de enfocar los esfuerzos en un camino, el tratar de mantenerse al día requiere de mucho esfuerzo y dedicación.

Al tener desarrollo como especialista en soluciones de seguridad de Symantec, se tuvo oportunidad de conocer muchas empresas y gente muy valiosa. Resulta interesante la diversidad de ambientes y problemas con los que se tuvo contacto y es motivo de orgullo poder decir que se ha contribuido –aunque sea con un granito de arena- a que las empresas sean más productivas y más exitosas. Exagerando un poco, se podría decir que se siente como que se cumple con la parte de “ayudar a hacer un México mejor”.

No todo fue alegría o miel sobre hojuelas. Salir al mercado laboral sin experiencia y sólo con la formación que la UNAM brindó, no fue necesariamente un proceso fácil. El estigma que tiene la Universidad con respecto a ser una escuela de vagos, a los ojos de muchos reclutadores en las empresas, tampoco ayudó al principio. Se tuvo la oportunidad y se aprovechó.

Se trabajó con muchas personas, a las que se reportó o a las que se tuvo que coordinar. También es motivo de orgullo pensar que se logró enseñarles algo (no exclusivamente técnico) o por lo menos ayudarles, y en algunos casos, se pudo cultivar una amistad. Hubo mucho aprendizaje de la gente “buena”, técnica o comercial, pero de igual forma se aprendió de los “no tan buenos”. Ese aprendizaje, del tipo “no se debe ser así”, también ha ayudado a crecer como persona y como profesional.

Respecto a lo que aún falta por aprender o mejorar, es sabido que hay que trabajar aún en el manejo del recurso humano. Se debió de aprovechar más el conocimiento proporcionado por la Universidad en las áreas administrativas, y eso hubiera ahorrado algunos dolores de cabeza, pero tampoco hay que olvidar que algunos contenidos se encontraban ya un poco obsoletos.

También se desea iniciar el proceso que permita dejar de ser 100% técnico y operativo, pues no es un objetivo pasarse la vida atendiendo contingencias a deshoras de la noche. Se desea seguir siendo un especialista y ser el mejor del área. Se desea iniciar el desarrollo de actividades realmente gerenciales y pasar de lo operativo a lo estratégico.

Hubo varias oportunidades de cambiar de empleo. Algunas a punto de realizarse, pero que por las contraofertas que se recibieron de InfoCorp, no fueron contempladas. El recibir contraofertas para que no se cambiara de empleo, ayudó a sentirse apreciado y valorado. Hubo otras ofertas que no fueron suficientemente buenas como para tomarlas, y otras que simplemente no se lograron.

Diez años sin arrepentimiento por no haber cambiado de empresa. Diez años en los que se pudo iniciar la formación de un pequeño patrimonio, y de sentar las bases para crear una nueva familia. Considerándolos como un período muy bueno de la vida, con un buen marcador global y resaltando lo positivo. Valorando la relación ganar-ganar que se logró establecer con la Empresa. Crecer con ella y sentirse parte integral de la misma. Hablar de ella y los proyectos como propios, y no sólo como un empleado, sino como parte integral de la misma. Sin sentirse así sólo en los éxitos, sino también en los fracasos.

A más de diez años del inicio de la vida profesional y de la relación laboral con InfoCorp, aún se tienen muchas ganas de seguir adelante. Este período tan importante fundó las bases que sustentan una valiosa carrera profesional. Brindó los elementos primigenios para poder representar dignamente a la Universidad Nacional Autónoma de México y decir con orgullo: SOY EGRESADO DE LA UNAM. ¡GOYA!

Numeralia.

Diez años en números:

1	Entrevista de radio
1	Ingeniero despedido
1	Viaje a Estados Unidos
4	Jefes directos
6	Puestos diferentes
10	Años de trabajo en InfoCorp
10	Certificaciones
15	*Firewalls* instalados
25	Ingenieros coordinados a lo largo del tiempo
+60	Demostraciones de productos
+70	Capacitaciones impartidas
+100	Reportes de auditoría mensual
+120	Empresas con alguna relación directa o indirecta
+1,000	Nodos instalados de SAV
+7,000	Tickets de soporte atendidos
+20,000	Nodos administrados de SAV

Empresas con alguna relación directa o indirecta (no todos fueron clientes de InfoCorp, pero sí se tuvo contacto):

1. Abamex Chevrolet
2. Aceros Cuatro Caminos
3. Adidas
4. Akra
5. Alsea (Domino's Pizza)
6. Áncora
7. Arrocera Covadonga
8. Asesores Libres para Empresas
9. Audio Mundo de México
10. Auto Centro de Celaya
11. Avangard México
12. Avon*
13. Banamex
14. Banco Autofin
15. Bancomext*
16. BIC No sabe fallar
17. Biometría Aplicada
18. bNexus
19. CABI
20. Cables Automotrices de Hidalgo
21. Caja de Ahorro de los Telefonistas
22. Calefacción y Ventilación (CYVSA)
23. Canon
24. Casa Veerkhamp
25. Casas GEO*
26. Celanese Mexicana
27. CENEVAL*
28. Coca Cola FEMSA
29. Colegio Suizo
30. Colgate Palmolive
31. Comisión Nacional de Áreas Naturales Protegidas (CONANP)*
32. Cosbel Frabel (L'oreal)
33. DuPont
34. Ecko
35. EDS
36. El Palacio de Hierro*
37. Elektra*
38. Epson
39. Estafeta Mexicana
40. Fondo para el Desarrollo Social de la Ciudad de México
41. Ford Zapata
42. Fotorama de México
43. Fundación Mexicana para el Desarrollo Rural
44. GA Comunicación
45. Gedas North America
46. Gillette

47. Grupo Autofin
48. Grupo Bursátil Mexicano (GBM)
49. Grupo DINA
50. Grupo Idesa
51. Grupo Interdom
52. Grupo Nacional Provincial (GNP)
53. Grupo Posadas
54. Grupo San Luis Rassini
55. Hewlett Packard*
56. Hipotecaria Su Casita
57. Horwath, Castillo, Miranda y Cía.
58. Ici Mexicana
59. In House
60. Industria Nacional de Autopartes
61. Ingenio Casasano
62. Ingram Micro
63. Inmobiliaria EMBA
64. Instituto de Investigaciones Filosóficas - UNAM
65. Instituto de Investigaciones Sociológicas - UNAM
66. Instituto Mexicano de Telemarketing
67. Instituto Mexicano del Petróleo (IMP)
68. Instituto Nacional de Migración (INAMI)
69. Instituto Nacional de Psiquiatría
70. Instituto Tecnológico Autónomo de México (ITAM)
71. Interacciones
72. ITrans Technology
73. Jafra
74. Johnson Controls
75. Juniper Networks
76. KPMG, Cárdenas, Dosal
77. Librería Porrúa*
78. Mancera, Ernst & Young
79. Martí*
80. McDonald's de México
81. Merck
82. Metronet*
83. Nacional Financiera (NAFIN)
84. Naviplastic
85. Neocenter
86. Nextel
87. Nissan Mexicana
88. Novag Infancia
89. Novartis
90. Omnibus Cristóbal Colón*
91. Pauta Creativa
92. Peñoles*
93. Pepsi Gemex / Pepsi Bottling Group (PBG)
94. PrestaComer
95. Revista Proceso*
96. RG López Abogados
97. Sabre
98. Sabritas (Fritolay)
99. Sanofi Aventis
100. SARE*
101. Seguros Atlas*
102. Seguros Banamex*
103. Seguros Comercial América*
104. Servicio Continental de Mensajería
105. Sida Yoga Dham de México
106. Siderúrgica de Yucatán
107. Solloa Tello*
108. Storage Tek
109. Symantec
110. Tania Internacional
111. Telcel*
112. Televisa (Corporativo)*
113. Televisa San Ángel (Postproducción de audio y video)
114. Tiendas Comercial Mexicana
115. Tracomex
116. Transportes Marva
117. Unisys
118. Valle Redondo
119. Valores Mexicanos (Valmex)
120. Vitalmex Internacional

* Con estos clientes, hubo contacto para llenado de cuestionarios, presentaciones de productos, visita de detección de necesidades o intento de inicio de relación comercial, pero no se logró formalizar ningún proyecto.