UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES

“A R A G Ó N”

“EXPERIENCIA PROFESIONAL EN LA EMPRESA SOLUCIONES DE SEGURIDAD INFORMÁTICA”

INFORME DEL EJERCICIO PROFESIONAL

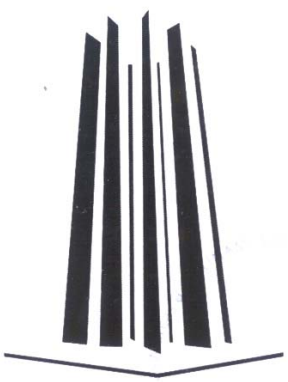
Que para obtener el título de:

INGENIERO EN COMPUTACIÓN

P R E S E N T A :

CARLOS ARMANDO VÁZQUEZ GONZÁLEZ

ASESOR: **ING. ANTONIA NAVARRO GONZÁLEZ.**



San Juan de Aragón, Edo. De México**.** **2009**

AGRADECIMIENTOS

A Dios, porque me ha llevado de su mano y por las bendiciones recibidas.

A mis Padres porque me motivaron a seguir este camino, por sus enseñanzas, desvelos, regaños… Sé que sin ustedes no sería lo que soy…

Papá, has dejado tanto en mi vida, gracias por el apoyo que recibí siempre para alcanzar este objetivo y por dejarme la más grande lección de vida.

Mamá, gracias porque tú eres la que me enseñó de la sensibilidad y amor necesarios para la motivación de seguir siempre adelante.

¡ETERNAMENTE GRACIAS!

Magaly, has estado ahí desde el comienzo de esto, motivándome a ser mejor todos los días.

Gracias por tu amor, paciencia y ternura que siempre me han impulsado a realizar lo que nos hemos propuesto, por ser quién eres...

Esto apenas empieza querida mía… a echarle ganas para lo que sigue. Te amo siempre.

A mis hermanos, como un ejemplo de lo que deben buscar… sigan adelante, esfuércense por crear lo que soñaron. Solo el trabajo, la dedicación y el amor a lo que hacen podrán llenar su vida de satisfacciones. Los quiero mucho.

A todos los demás miembros de mi familia (natural y política) que comparten el gozo de esta experiencia, gracias por el apoyo. Es invaluable para mí su cariño y afecto sincero.

Compañeros de clase, amigos que compartieron las aulas con un servidor, siempre tendrán un lugar especial en mis recuerdos. Gracias por compartir su paso por la escuela conmigo.

A la FES Aragón y mis Profesores, gracias por sus lecciones y dedicación a su trabajo. Sin ustedes no estaría hoy en este lugar.

Ing. Antonia Navarro, por dar la oportunidad a tantos estudiantes que en el espacio que usted dirige han aprendido parte de las cosas que existen fuera de la Escuela. Yo fui uno de ellos, gracias.

INTRODUCCIÓN.

INTRODUCCIÓN

Todos los que hemos pasado por una Universidad pensamos alguna vez que al salir tendríamos todas las herramientas necesarias para desempeñarnos profesionalmente, hoy me puedo dar cuenta que solo la práctica y el conocimiento continuo pueden hacer a un buen profesionista.

En el universo informático existe una gama muy amplia de ramas en las que podemos emplearnos; aunque hay ocasiones que no siempre podemos encontrar el trabajo que deseamos, ya sea por lo económico o por el área específica en la que nos gustaría desempeñarnos, hay que estar siempre optimista de las cosas que podemos aprender en este empleo, ya que solo la constancia y dedicación podrán proporcionarnos la experiencia requerida en el mercado laboral que hará que se abran mejores oportunidades de desarrollo profesional.

Desde hace cinco años yo encontré la oportunidad que necesitaba para adquirir experiencia en el ramo de la Computación, específicamente en una empresa de Seguridad Informática, dedicada a la comercialización de Soluciones destinadas a asegurar la infraestructura tecnológica de sus clientes, mediante la correcta selección de las mismas, así como la calidad en la atención y el servicio proporcionado por las diferentes áreas de la organización.

El presente es un Informe sobre el ejercicio profesional que he tenido en este tiempo, en el que me he desempeñado como Ingeniero de Soporte Técnico en la empresa Soluciones de Seguridad Informática S.A de C.V. ubicada en Melchor Ocampo 193 Torre A Piso 5, Col. Verónica Anzures, Del. Miguel Hidalgo DF, CP: 11300.

Con la finalidad de identificar cuál ha sido mi desarrollo profesional en la empresa anteriormente mencionada este informe está estructurado en cuatro capítulos distribuidos de la siguiente manera:

CAPÍTULO I. Soluciones de Seguridad Informática S.A. de C.V. Dentro de este capítulo doy a conocer de manera más profunda la organización de la empresa para la cual he laborado así como su misión y visión; de igual forma hago un resumen de las diversas actividades que me han sido encomendadas.

CAPÍTULO II. Soporte y Capacitación a Clientes. Muestra de manera más detallada las actividades del área de Soporte Técnico de la empresa, así como la capacitación que hemos brindado a nuestros clientes.

- Soporte en preventa a clientes.
    - Implementación de soluciones en modo de evaluación.
    - Soporte técnico durante el periodo de evaluación.
- Soporte en postventa a clientes.
    - Implementación definitiva de soluciones cuando se ha concretado la venta.
    - Soporte técnico telefónico, en sitio o remoto a la solución.
- Capacitación
    - Hands on training de la solución durante las evaluaciones o implementaciones definitivas.
    - Diseño de temarios para cursos de las distintas soluciones.
    - Diseño de materiales empleados en los cursos (manuales, diapositivas del curso)

CAPÍTULO III. Administración de la infraestructura tecnológica de la empresa. Este capítulo permite apreciar las actividades realizadas como administrador de la infraestructura interna y servicios de red de la empresa, las cuales son:

- Asignación de equipos de cómputo al personal de la empresa.
- Diseño de políticas de acceso a los servicios de red.
- Configuración de servidor de correo electrónico y DNS.
- Instalación y configuración de equipos de cómputo de los usuarios.

- Instalación y configuración de dispositivos de red.
- Implementación de nuevas tecnologías.

CAPÍTULO IV. Proyectos y cursos de actualización. En virtud de los capítulos anteriores este apartado es el reflejo del manejo de los diferentes proyectos en los que he participado en Soporte Técnico que incluyen los tipos de soluciones que utilizamos como son:

- Antivirus.
- Firewalls.
- Seguridad de correo electrónico.

Espero que este documento exprese la experiencia profesional adquirida en este periodo en el cual he tenido grandes satisfacciones, porque me doy cuenta que me ocupé en una de las áreas más vastas de la Informática, misma que me gustaría seguir conociendo por lo interesante de sus contenidos y lo extenso de sus aplicaciones.

CAPÍTULO I:
SOLUCIONES DE SEGURIDAD INFORMÁTICA S.A. DE C.V.

1.1. ACERCA DE SSISA

Soluciones de Seguridad Informática S.A de C.V. es una empresa dedicada a ofrecer productos y servicios enfocados a proveer a los clientes el aseguramiento de su infraestructura tecnológica. Nace en el año 2003 a partir de un grupo de personas provenientes de empresas líderes en el mercado y con amplia experiencia en el ramo de la Seguridad Informática.

Con el capital humano y algunas alianzas comerciales con fabricantes de Soluciones de Seguridad comienza la operación, en un principio como representante de Sophos ® Inc. Fabricante líder en productos antivirus en todos los niveles, posteriormente como proveedor de productos enfocados a enfrentar de manera eficiente amenazas de seguridad desde el punto final o equipo de escritorio hasta el perímetro de la red, ayudando a erradicar problemas de Virus, Gusanos, Spam, Spyware, Phishing, Zombies, Malware, Intrusos o aplicar políticas de Filtrado de contenido, control de acceso y cumplimiento de Regulaciones Gubernamentales o Corporativas.

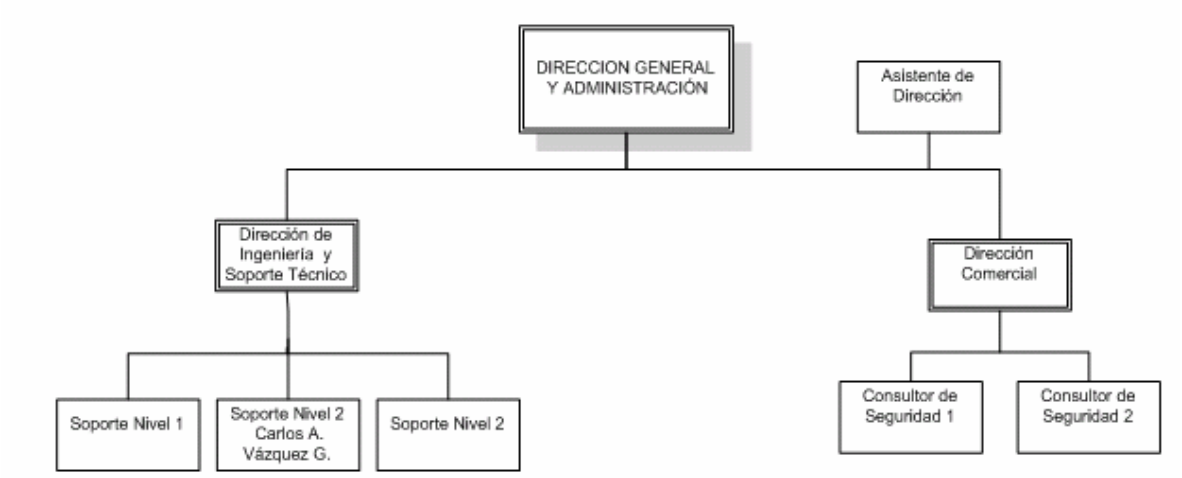
1.2. VISIÓN

“Los compromisos adquiridos con nuestros clientes son un lazo entre socios de negocios. Nuestro éxito en el mercado se debe en gran parte al profesionalismo y a la preparación que poseen nuestros recursos humanos. Gracias a ello podemos resolver las necesidades de los clientes de una manera eficiente y oportuna. Sin embargo, sabemos que siempre hay algo nuevo que aprender, por eso es indispensable mantenernos actualizados. El conocimiento es la base de nuestra fuerza. Si Usted piensa invertir en una solución de seguridad y/o administración es importante cuidar el costo de su inversión, que sea sana además de eficiente.”

1.3. MISIÓN

“Minimizar los riesgos ocasionados por las vulnerabilidades de los bienes informáticos mediante la correcta implementación de las mejores medidas de defensa.”

1.4. ORGANIGRAMA



1.5. PARTICIPACIÓN EN PROYECTOS

Mi participación en la empresa ha sido en la Dirección de Ingeniería y Soporte Técnico, como Ingeniero de Soporte de Nivel 1 (desde Octubre de 2003 hasta Diciembre 2004) y como Ingeniero de Soporte Nivel 2 (desde Enero 2005 a la fecha) siempre interactuando con los clientes ayudando a la detección de sus necesidades y diseñando esquemas integrales que permitan el aseguramiento de su infraestructura tecnológica, así como la protección de su información.

Lo anterior se logra por medio de la oferta de soluciones destinadas a tal efecto, particularmente en tres divisiones:

- Antivirus.
- Firewalls.
- Seguridad de correo electrónico.

En mi caso particular la manera en que he apoyado este objetivo es con conocimientos de redes, sistemas operativos comerciales y conceptos de seguridad que me han ayudado a entender las necesidades del cliente y la oferta de productos y servicios por parte de la empresa. Por otro lado, he tenido que recibir capacitaciones respecto a los productos que maneja la empresa para poder ofrecer amplio conocimiento respecto a los mismos y de esta manera atender al cliente integralmente.

Con el conocimiento de las soluciones que ofertamos, también he podido desenvolverme como instructor en cursos de capacitación dirigidos a clientes que buscan conocer respecto a las herramientas adquiridas, así como ampliar su conocimiento en el manejo de las mismas, desarrollando desde el material de apoyo, hasta los laboratorios que han de aplicar para complementar el aprendizaje.

Así mismo, en mi calidad de Administrador de red (desde Octubre de 2003 a la fecha) he participado en la implementación y administración de la infraestructura de la empresa teniendo a mi cargo los servidores de correo, web, dns, firewalls, routers, switches, filtrado de contenido y políticas corporativas. De igual forma se tiene que brindar soporte a los usuarios de la empresa respecto a sus equipos personales, como a las impresoras, conectividad a la red, antivirus, etc.

Una vez que tenemos una perspectiva general de lo que es la empresa, su misión, visión, organigrama y las responsabilidades que se me han encomendado, podemos continuar definiendo en los siguientes capítulos más detalladamente cada uno de los cargos que he ocupado.

CAPÍTULO II: SOPORTE Y CAPACITACIÓN A CLIENTES.

2.1. INGENIERÍA DE SOPORTE

El soporte técnico dentro de la organización es pieza fundamental ya que en gran medida de este departamento depende que se lleve a cabo con éxito una venta o la permanencia del cliente; es decir, que se mantenga cautivo no solo por la calidad y eficiencia de las soluciones que posee, sino por el servicio que se le ofrece, ya que la confianza en un grupo de personas que se encargan de asegurar sus activos (físicos o lógicos) es fundamental para que nuestra empresa siga siendo parte del equipo de trabajo que el cliente necesita para garantizar su operación lo más posible.

El área de Ingeniería de Soporte se encarga de proporcionar al cliente asistencia técnica referente a los productos de seguridad informática que comercializa la empresa. Este soporte puede ser antes de que el cliente haya adquirido alguna solución (SOPORTE TÉCNICO PREVENTA), o se puede brindar después de la compra (SOPORTE TÉCNICO POSTVENTA).

A continuación se detallan las actividades que se realizan dentro de cada uno de los tipos de soporte ofrecido:

2.1.1. SOPORTE TÉCNICO PREVENTA

El soporte técnico preventa se ofrece a los clientes como un medio para plantear de acuerdo a sus necesidades cual es la solución más adecuada, es decir, el Ingeniero responsable acompañará al consultor que se encarga de las ventas con el cliente para realizar un análisis del entorno y su problemática y de esta manera ofrecer la gama de productos que podrán conformar la solución que el cliente necesita para cubrir sus problemas de seguridad.

Dentro de este tipo de soporte se encuentran las evaluaciones a los productos que incluyen:

- Elaboración de oferta de proyecto.
    - Se tienen que detectar las necesidades del cliente para poder recomendar la solución que cubra con las mismas y de esta manera ofrecer los productos que serán parte de la implementación.
    - El proyecto debe ser presentado al cliente para su aprobación y consentimiento para un periodo de evaluación.

- Licenciamiento temporal (evaluación limitada a un periodo corto de tiempo)
    - Una vez aprobado el proyecto, se tiene que realizar la gestión de la licencia temporal de evaluación de la solución que se instalará con el cliente, la descarga del software requerido y la preparación del hardware (en su caso) que se utilizará durante la prueba.

- Implementación y puesta a punto de la solución en entorno de pruebas.
    - A petición del cliente puede configurarse un entorno de pruebas en el cual se simule la implementación final, con el objetivo de que pueda observarse el desempeño de la solución en un ambiente similar al real y puedan descartarse fallas.
- Implementación y puesta a punto de la solución en entorno operativo.
    - Se debe realizar un análisis previo para poder verificar que se cumplen con los requerimientos de instalación y ver si es viable implementar en el ambiente operativo o se necesitan hacer adecuaciones al mismo que no afecten de manera significativa el esquema original (cambios de direccionamiento ip, rutas estáticas, actualizaciones a los sistemas operativos, entre otros). Así mismo se debe concientizar al cliente de los riesgos que conlleva efectuar dichas modificaciones.
    - Una vez finalizada la implementación se deberán realizar pruebas de funcionamiento con el objetivo de verificar que no existan errores y poder corregirlos en sitio antes de que el cliente libere el servicio de forma permanente.
- Seguimiento y observación de resultados.
    - Durante el periodo de pruebas puede ser que el cliente requiera asistencia técnica o ajustes a las configuraciones que se han establecido en un principio, por lo cual se debe dar un seguimiento puntual a la solución para comprobar que se estén cumpliendo los objetivos establecidos en el planteamiento del proyecto.

- Desinstalación de la solución y adecuación al entorno original.
    - Terminado el periodo de pruebas y si la solución no cumple con las expectativas del cliente o se llegara a posponer la compra del producto, se tiene que dar por terminada la evaluación realizando la desinstalación de los productos, para lo cual se debe adecuar o regresar la configuración del entorno actual al original, para no afectar la operación.

2.1.2. SOPORTE TÉCNICO POSTVENTA

El soporte técnico postventa se ofrece a los clientes una vez que han adquirido alguna solución con la empresa, es decir, ésta es la asistencia técnica que el cliente requiere para poder llevar a cabo una correcta operación del producto que adquirió.

Dentro de este tipo de soporte se encuentra

- Elaboración de proyecto final.
    - Con base en el proyecto de evaluación (si lo hubo) se tiene que elaborar un proyecto definitivo que contemple cambios permanentes en el esquema original del cliente.
- Gestión del licenciamiento definitivo.
    - Trámite ante el departamento comercial del licenciamiento definitivo, previa orden de compra por parte del cliente. Si existe algún error con el licenciamiento se levanta el ticket respectivo ante el fabricante del producto para la corrección.
- Sustitución del licenciamiento temporal por el definitivo.
    - Si la solución ya está implementada debido a una fase de evaluación previa, se le indica al cliente si se puede colocar una licencia definitiva o hay que volver a comenzar con el procedimiento desde el inicio, ya que esto depende del tipo de producto que se haya adquirido, por ejemplo, si la solución en evaluación es de hardware se tiene que hacer la sustitución del equipo actual por el equipo nuevo, realizando los pasos necesarios para que este cambio sea lo más transparente posible para los usuarios (respaldo y restauración

de configuración, cambio de cables en horarios no productivos o reinicios en los sistemas.)

- Pruebas de implementación.
    - A petición del cliente puede configurarse un entorno de pruebas en el cual se simule la implementación final, con el objetivo de que pueda observarse el desempeño de la solución en un ambiente similar al real y puedan descartarse fallas.
- Implementación y puesta a punto de la solución en entorno operativo.
    - Si aún no se ha implementado la solución con el cliente en una fase de evaluación, se debe realizar el análisis previo para poder verificar que se cumplen con los requerimientos de instalación y ver si es viable implementar en el ambiente operativo o se necesitan hacer adecuaciones al mismo que no afecten de manera significativa el esquema original (cambios de direccionamiento ip, rutas estáticas, actualizaciones a los sistemas operativos, entre otros). Así mismo se debe concientizar al cliente de los riesgos que conlleva efectuar dichas modificaciones.
    - Una vez finalizada la implementación se deberán realizar pruebas de funcionamiento con el objetivo de verificar que no existan errores y poder corregirlos en sitio antes de que el cliente libere el servicio de forma permanente.
- Asistencia técnica telefónica.
    - Si el cliente lo requiere se debe ofrecer al cliente el servicio de asistencia técnica del producto adquirido vía telefónica, mismo que consiste en:
        - Sondeo para detectar el problema.
        - Guiar al cliente en el manejo adecuado de la solución.
        - Si existe algún problema técnico con el producto, tratar de resolverlo basado en la experiencia en el manejo del mismo, así como en manuales, bases de conocimiento y asistencia de segundo y tercer nivel.

- Si no se puede resolver el problema, solicitar asistencia técnica telefónica con el fabricante del producto.

- Asistencia técnica remota.
  - Cuando la asistencia telefónica no es suficiente para diagnosticar un problema, el departamento de soporte se puede apoyar de la asistencia remota la cual puede ser:
    - Vía Web. Si el producto lo permite se puede acceder a las consolas de administración de la solución mediante navegadores de Internet para poder revisar configuraciones y detectar probables fallas mediante la revisión de reportes y bitácoras del sistema.
    - Vía CLI. Si el producto lo permite se puede acceder a la administración del producto vía interfaz de línea de comandos (CLI) utilizando para ello cliente de SSH (Secure Shell) o Telnet, con el objetivo de verificar servicios, bitácoras y realizar pruebas de conectividad y/o funcionamiento.
    - Herramienta de Soporte NetSupport. Permite conectarse al entorno Windows del cliente por medio de la red pública (Internet) para poder tomar control y de esta manera revisar configuraciones y diagnosticar probables fallas.
    - Vía correo electrónico. El cliente puede enviar su solicitud de soporte vía correo electrónico, para lo cual se tiene designada una cuenta especifica en donde se recopilan todas las peticiones de asistencia técnica y se canalizan de acuerdo al producto y la severidad del problema.

- Asistencia técnica en sitio.
  - El soporte en sitio se refiere a las actividades que requieren presencia del ingeniero de soporte en las instalaciones del cliente para realizar diagnóstico referente a fallas, reinstalación del producto, entrenamiento “hands on”, modificación a configuraciones, actualizaciones y revisión de la solución como forma de mantener el funcionamiento adecuado de la misma.

2.1.3. NIVELES DE SOPORTE

Dentro de la atención a los clientes existen diferentes niveles de soporte, mismos que deben estar organizados dependiendo el grado de atención que se requiera proporcionar a los usuarios. De aquí se desprenden en nuestro departamento tres niveles de soporte:

NIVEL 1: Atención directa al cliente. La asistencia técnica puede ser proporcionada por un Ingeniero de soporte que no domina un producto específico. Generalmente se ofrece como un primer contacto en el cual se realiza el sondeo respectivo para realizar el levantamiento del caso y su posible solución podrá brindarse mediante consulta de la base de conocimientos o el manual de usuario y/o administración.

NIVEL 2: Ingeniero de soporte con experiencia avanzada en el producto en cuestión. El problema que requiere asistencia es analizado por un especialista en la solución y la respuesta al caso se brindará después de hacer modificaciones o pruebas más puntuales para poder establecer las causas probables de la falla y corregirla.

NIVEL 3: Fabricante del producto. Después de intentar corregir las fallas mediante los conocimientos que se tienen sobre el producto y no se pudiera dar una solución al problema, se tendrá que recurrir al fabricante vía telefónica para levantar un ticket y que con base en la información que ya se recopiló se pueda dar una respuesta a la falla y ejecutar las acciones necesarias para su corrección.

Los pasos para poder canalizar las solicitudes de asistencia en alguno de los tres niveles son:

Levantamiento del caso: El departamento de soporte recibe una llamada por parte del cliente reportando un problema. El ingeniero de soporte levanta el caso preguntando datos generales del cliente para poder determinar si el licenciamiento del producto tiene vigencia.

Sondeo: Se realiza una serie de preguntas al cliente para poder detectar el problema o resolver las dudas que pudiera tener.

Búsqueda de la solución por un problema existente o reportado: Con base en la experiencia que se tenga en cuanto al producto se puede llegar a resolver un problema que haya sido reportado en un caso anterior. Además se pueden consultar bases de conocimiento del fabricante para ubicar mediante códigos de

error o palabras significativas que describan la falla, para que se le indique al cliente que es lo que tiene que hacer para resolver el caso.

Escalamiento a Segundo Nivel: Si el Ingeniero de Nivel 1 no puede resolver el problema, se canaliza a un Ingeniero especializado en la herramienta que presenta la falla.

Pruebas de diagnóstico: Se ejecutan pruebas para diagnosticar el problema y poder dar una solución adecuada. Las pruebas pueden ser desde comandos de diagnóstico (ping, trace routes, test de dns, test de telnet para verificar puertos abiertos, test de envío de correos, entre otros). Así mismo se pueden hacer pruebas monitoreando bitácoras en tiempo real observando los resultados y se deben hacer búsquedas en los registros y reportes para encontrar eventos que pudieran estar relacionados con el problema.

Escalamiento a tercer nivel: Cuando no hay una solución a la falla de acuerdo con la base de conocimientos o que se desprenda de las pruebas realizadas y que se trate de un problema que no está al alcance del Ingeniero de Soporte, se tiene que levantar un ticket con el fabricante, mismo que se hace con base en lo que se pudo diagnosticar durante la asistencia técnica. Dependiendo del producto será el método empleado para el soporte que puede ser vía telefónica, email, chat, remoto o cualquier medio soportado.

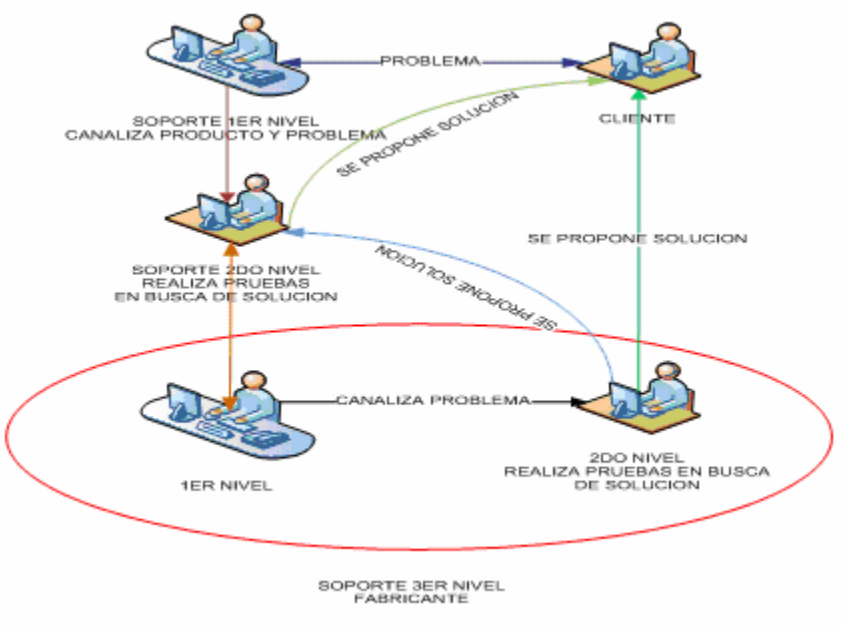


FIGURA 1: FLUJO DE SOPORTE

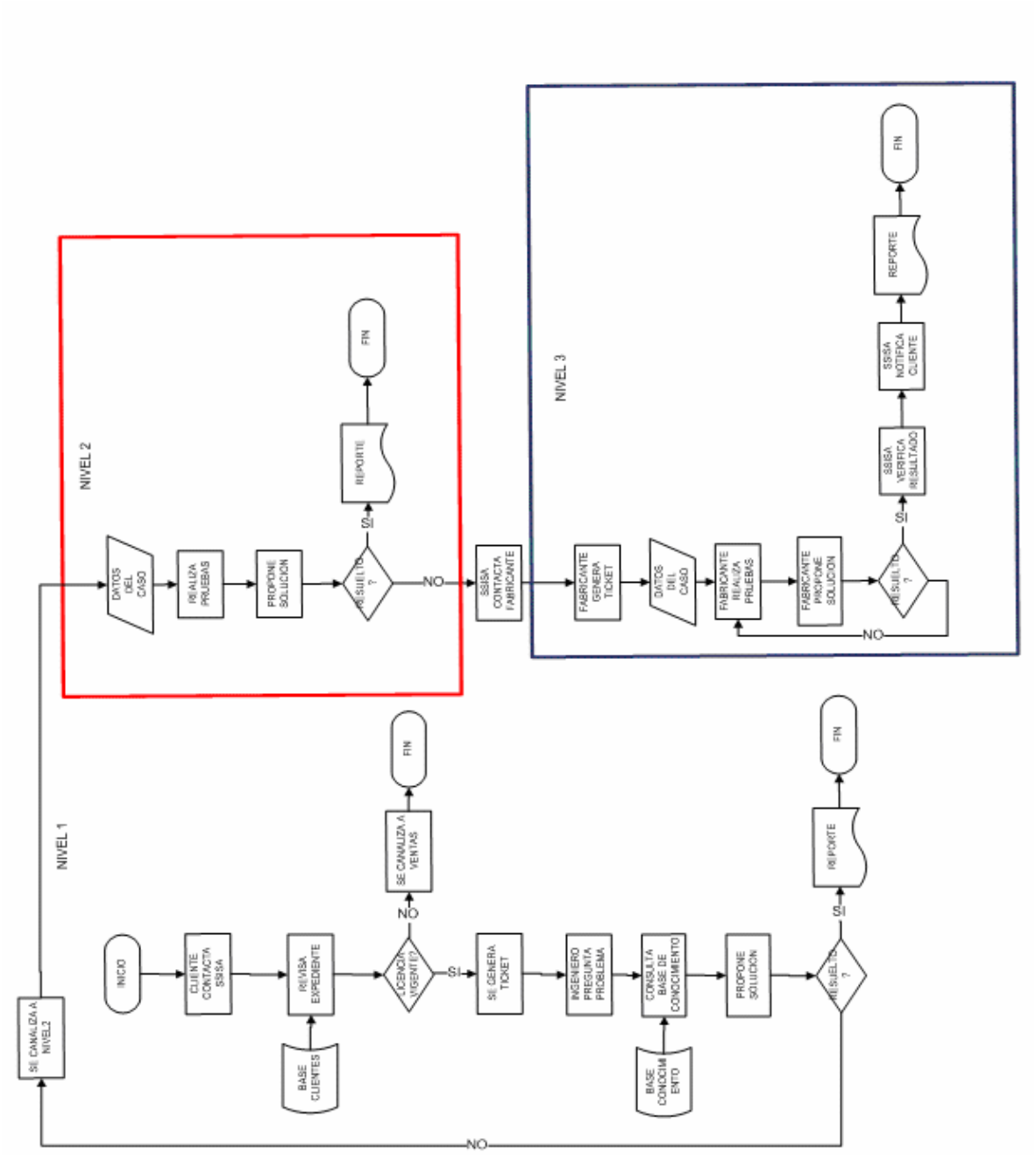


FIGURA2: DIAGRAMA DE FLUJO DEL PROCEDIMIENTO DE SOPORTE

2.2. CURSOS DE CAPACITACIÓN.

El área de soporte también se encarga de impartir cursos de capacitación acerca de los productos que se ofrecen a la venta, los cuales pueden ser de dos tipos:

2.2.1. CAPACITACIÓN "HANDS ON".

La capacitación "Hands on" es llamada así porque se ofrece al cliente como una guía para administrar y configurar su producto enseñándole como debe hacerlo sobre la marcha, es decir, cuando se realiza la implementación de la solución al mismo tiempo que ésta se va configurando se le explica al usuario cuales son las opciones más recomendables y más utilizadas en el producto, así como una descripción a grandes rasgos del producto y sus alcances. Generalmente este tipo de capacitación no requiere material de apoyo (diapositivas, manuales, laboratorios, etc.).

2.2.2. CAPACITACIÓN COMPLETA.

La capacitación es el proceso metodológico encaminado a la mejora, incremento y desarrollo de la calidad de los conocimientos en algún producto que tiene como objetivo que el usuario tenga una dependencia menor de las áreas de soporte técnico, ya que al contar con las habilidades necesarias para el manejo de su solución, será capaz de realizar él mismo el diagnóstico y corrección de fallas, así como los cambios de configuración que requiera.

Este tipo de capacitación requiere materiales de apoyo tales como: diapositivas, proyector, manuales, equipo de pruebas, etc. y es ofrecido por la empresa en salas especializadas.

Dentro de la organización en mi calidad de Ingeniero de Soporte he podido desempeñar actividades referentes a la capacitación de los clientes las cuales han incluido:

- Desarrollo de temarios. Selección de temas que se impartirán en la capacitación.
- Desarrollo de materiales. Elaboración de manuales, ejercicios de laboratorio, diapositivas y documentos de apoyo.
- Diseño de esquema de laboratorio. Dibujar el diagrama del ambiente que se empleará en los ejercicios de laboratorio.

- Preparación de equipos y montaje del laboratorio. Instalación de equipos con los sistemas operativos necesarios para llevar a cabo las prácticas, así como solicitud de licencias temporales para el software o hardware de evaluación y cableado de red.

- Expositor. Impartir los conocimientos derivados del uso de las herramientas de seguridad a usuarios de las mismas, apoyándome en materiales que proporciona el fabricante (manuales, hojas técnicas y bases de conocimiento) y proyectando diapositivas con conceptos clave para el aprendizaje en la utilización de los productos. Asimismo se dan instrucciones de cómo llevar a cabo los ejercicios de laboratorio que contribuirán a reforzar los conocimientos en las soluciones.

A lo largo de este capítulo se expresó la importancia y las actividades realizadas en el puesto de Ingeniero de Soporte Técnico, mismo que ocupo desde Octubre de 2003 fecha en que ingresé a la empresa. Hubo algunos cambios en cuanto al Nivel de soporte en el que me ubiqué, ya que en los inicios estuve como Ingeniero de Nivel 1 (Octubre de 2003 – Diciembre 2004). Posteriormente fui designado Ingeniero de Nivel 2 de las soluciones perimetrales y de algunos antivirus (Enero 2005 a la fecha) y en este tenor he tenido que realizar actividades de preventa, postventa y capacitación.

El puesto de Ingeniero de Soporte Técnico ha contribuido a mi desarrollo profesional en el sentido que he adquirido experiencia en atención a clientes, desarrollo de proyectos, manejo de escenarios múltiples para la oferta de soluciones a clientes y desarrollo de capacitaciones dirigidas a usuarios.

En lo personal creo que este puesto me ha permitido conocer muchas personas a las que he podido ayudar con mi trabajo, no solamente colaborando con mis compañeros de equipo, sino con los diferentes clientes que en ocasiones te llegan a tener la confianza suficiente para considerarte parte de su operación y esto se traduce en altos niveles de renovación de las soluciones, así como también ventas cruzadas, lo cual me deja satisfecho al saber que esto contribuye al crecimiento de la organización.

Además de las tareas de soporte técnico, he tenido que realizar labores administrativas en la empresa, de las cuales platicaré en el siguiente capítulo.

CAPÍTULO III: ADMINISTRACIÓN DE LA INFRAESTRUCTURA INTERNA DE LA EMPRESA.

3.1. LA ADMINISTRACIÓN DE LA INFRAESTRUCTURA.

Esta actividad la he llevado a cabo para la organización y planificación de los recursos tecnológicos disponibles en la empresa. A mi cargo se encuentra desde la organización e implementación de la infraestructura física como son equipos de cómputo, módems ADSL, firewalls, switches, Access points y los Servidores de acceso público y aplicaciones, hasta el diseño de políticas y procedimientos para la utilización de los recursos. Mi puesto para tal efecto ha sido Administrador de red. (Octubre 2003 – a la fecha).

Mis actividades consisten en:

- ***Asignación de equipos de cómputo al personal de la empresa****, así como el inventario y registro de dichas asignaciones.*

- ***Diseño de políticas de acceso a los servicios de red****, configuración de firewall, creación de grupos de acceso y políticas necesarias para brindar seguridad hacia el interior y exterior de la red.*

- ***Configuración de servidor de correo electrónico y DNS,*** *configuración de equipos de seguridad de correo electrónico, listas blancas, negras, adjuntos permitidos, etc. Todo esto con el objeto de que no se reciba correo no deseado que pueda representar problemas de seguridad en la organización, alta de registros MX, A, CNAME, etc en las zonas directa e inversa.*

- ***Instalación y configuración de equipos de cómputo*** *de los usuarios (Computadoras personales y laptops, software, impresoras y periféricos en general).*

- ***Instalación y configuración de dispositivos de red*** *(switches, firewalls, módems y access points).*

- ***Implementación de nuevas tecnologías****; ya sea durante evaluación o adquisición de las mismas.*

A continuación se detallan cada una de las actividades.

3.1.1. ASIGNACIÓN DE EQUIPOS DE CÓMPUTO AL PERSONAL E INVENTARIOS.

Esta función la he llevado a cabo con el objetivo de tener un control de los equipos con los que cuenta la organización, su ubicación, así como tenerlos a disposición en el momento que se requieran y evitar pérdidas de los mismos. Cuando empecé a hacerme cargo de esta actividad no existía una relación de inventarios ni había un control acerca del equipo que se tiene asignado, por lo que había pérdidas constantes de equipo y materiales. Debido a esto se nos planteó la necesidad de generar un registro de todos los equipos y sus ubicaciones, así como formular la metodología para introducir dichos activos de la empresa en una base de datos y tener disponible la información en cualquier momento.
Como no existía anteriormente una política que estableciera la obligatoriedad de llevar el registro de equipo, tuvimos que desarrollar primero la política y el procedimiento necesario para los inventarios.
La política resultante es la siguiente:

"Cualquier equipo nuevo o usado deberá ser registrado en una base de datos e identificado con un ID único por el cual se puedan saber sus características, ubicación, asignación y utilización para llevar un control y orden en cuanto a la administración de los activos de la empresa. Dicho proceso deberá ser efectuado periódicamente, de tal manera que se mantenga actualizado y disponible en cualquier momento."

De esta política se desprenden los procedimientos necesarios para llevar a cabo esta tarea:

- Se debe ubicar cada uno de los equipos electrónicos, de cómputo o de comunicación que existen en la empresa y verificar la localización, características, estado, asignación y uso del mismo y anotar un registro para poder generar una base de datos que se pueda utilizar para el inventario.
- Posteriormente se debe asignar a cada equipo un identificador único marcado físicamente en el equipo para poder ubicarlo fácilmente.

- Se deben introducir los datos recaudados en el sistema informático destinado para tal efecto el cual debe contener lo siguiente:
    - ID
    - Características.
        - Descripción.
        - Número de serie.
        - Fabricante.
        - Estado en que se encuentra.
    - Asignación.
    - Ubicación.
    - Utilización.
- Se deben generar reportes que surjan de datos cruzados como por ejemplo:
    - Equipos del mismo fabricante.
    - Equipos del mismo usuario.
    - Equipos que se utilicen para lo mismo.
    - Equipos que se encuentren en el mismo sitio.
    - Equipos del mismo tipo.
    - Equipos que estén en similares condiciones (nuevo, usado, etc.).
- Se podrán realizar cambios al inventario en el momento que se requiera, previa autorización del Director de Ingeniería y Soporte.
    - Cada que existan equipos nuevos, se deberán de incluir en el inventario.
    - Cada que se desechen equipos, se deben dar de baja del inventario.
    - Cuando el equipo cambia de usuario.
    - Cuando el equipo cambia de ubicación

- El procedimiento de ubicar los equipos en existencia debe realizarse cada 6 meses para verificar el estado actual de los equipos y realizar los cambios pertinentes a la información.

Una vez teniendo esto y debido a que la empresa no posee una gran cantidad de equipos, se construyó una base de datos en Microsoft Access ® debido a que la herramienta cumple con los requerimientos de la empresa en la cual se dieron de alta los campos solicitados y gradualmente se fue recopilando y agregando la información de los activos.

Cuando llega personal nuevo se le asigna equipo de su área y se realizan los cambios en el sistema sobre el nuevo propietario y ubicación. Lo mismo sucede cuando se da de baja personal, se realizan los cambios necesarios en el inventario.

3.1.2. DISEÑO DE POLÍTICAS DE ACCESO A LOS SERVICIOS DE RED.

Esta actividad la realicé debido a la necesidad de llevar a cabo un control sobre los accesos que se tienen desde y hacia la red interna, así como para asignar permisos a los usuarios en cuanto al contenido y tipo de los sitios y servicios que frecuentan utilizar.

Para completar esta tarea primero se tenían que considerar las siguientes interrogantes:

¿Qué es lo que queremos proteger?

La información sensible de la organización así como sistemas operativos de servidor y usuarios, servicios de internet como páginas web, correo, dns y ftp.
A continuación se presenta el esquema de red original de la organización.

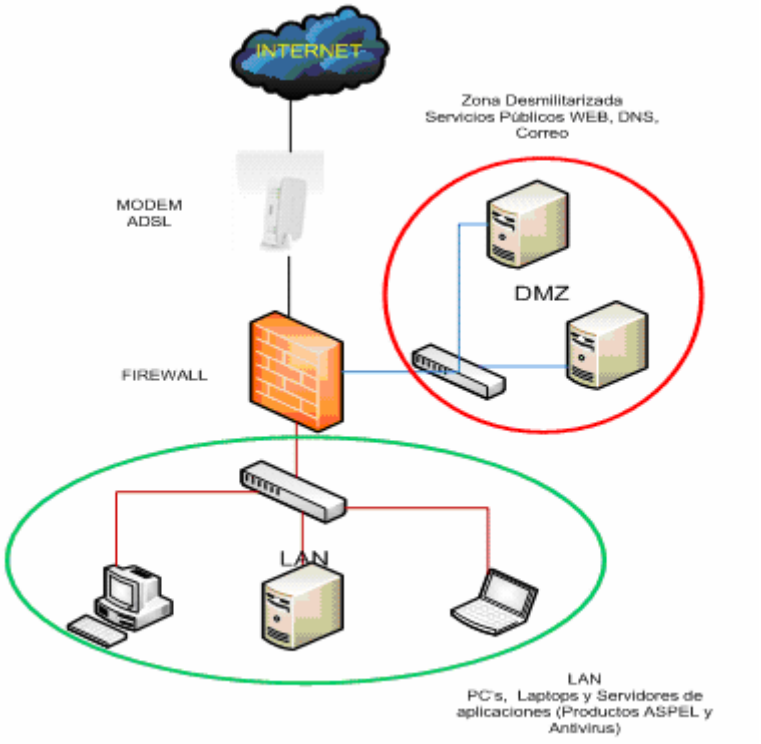


FIGURA 3: ESQUEMA DE RED

En el esquema se muestra la configuración de red de la empresa. Teníamos un firewall sin protección adicional, un 2Wire que nos da la salida a la red pública, nuestra LAN y una DMZ (Zona Desmilitarizada) en donde están los servicios públicos (Servidores DNS, WEB y Correo).

¿De quién lo queremos proteger?

Usuarios de la organización, hackers, virus, gusanos y demás amenazas que pudieran comprometer el sistema.

¿Cómo lo protegeremos?

Primero que nada se tenían que determinar qué es lo que se tenía permitido y qué es lo que se tenía restringido y para quienes, es decir definir el nivel de accesos que los usuarios deben tener y a partir de esto generar grupos a los que se asignarán perfiles de protección.

Los grupos dentro de la empresa son:

Usuarios Restringidos.
Son usuarios que no tendrán conectividad hacía la red pública por lo que su trabajo se limita a utilizar servicios en la red interna.

Usuarios Limitados: Usuarios que poseen acceso a servicios limitados de la red, así como aquellos que tienen restricciones de contenido y calidad en el servicio (ancho de banda limitado).

Usuarios Ilimitados: Usuarios que poseen acceso a todos los servicios de la red y no tienen restricciones de contenido o ancho de banda.

Servidores: Equipos destinados a proveer servicios a otras computadoras de la red.

Con base a la información recopilada acerca de los grupos de usuario de la empresa se fabricó la siguiente matriz para definir el perfil de accesos, restricciones y protección que deberían tener.

GRUPOS / PERFILES	RESTRINGIDOS	LIMITADOS	ILIMITADOS	SERVIDORES
ANTIVIRUS				
HTTP	*	*	*	*
HTTPS	*	*	*	*
FTP	*	*	*	*
INSTANT MESSAGING	*	*	*	*
SMTP	*	*	*	*
POP3	*	*	*	*
FILTRADO DE CONTENIDO				
FILTRADO POR PALABRAS	*	*		*
FILTRADO POR URL	*	*		*
EXCEPCIONES DE URL	*	*	*	*
FILTRADO DE CONTENIDO POR CATEGORÍAS				
FILTRADO EN IMÁGENES				
CATEGORÍAS CONTROVERSIALES (Materiales de Adultos, Relaciones personales y Citas, Drogas, Alcohol, Ocultismo, etc.)	NO	NO	SI	NO
CATEGORÍAS NO PRODUCTIVAS (Web Mail, Web chat, Radio y TV por Internet, etc.)	NO	NO	SI	NO
CATEGORÍAS MALICIOSAS (Hacking, Spyware y Malware)	NO	NO	NO	NO
CATEGORÍAS DE NEGOCIOS Y GUBERNAMENTALES (Gobierno, empresas, IT, etc.)	NO	SI	SI	NO
CATEGORÍAS GENERALES (Noticias y Foros, Bancos, Salud, Deportes, etc.)	NO	SI	SI	NO
DESCARGA DE SOFTWARE	NO	LIMITADO	SI	SI

CONTROL DE ACCESO				
ACCESO A WAN	NO	SI	SI	SI
SERVICIOS	NINGUNO	HTTP, HTTPS, DNS, POP3, SMTP, COMPRANET, INFONAVIT	TODOS	DEPENDE EL SERVIDOR
MESSENGER	NO	NO	SI	NO
P2P	NO	NO	NO	NO

Además de los datos recopilados en la matriz de restricciones y protección, se tuvieron que analizar algunos otros requerimientos de la empresa, como son:

- Sustitución del firewall actual.
- Protección a Servicios Públicos (Servidor DNS, Servidor HTTP, Servidor FTP, Servidor de Correo).
    - Evitar intrusiones.
    - Evitar Ataques.
    - Evitar descarga de código malicioso.
    - Usar los Servidores exclusivamente para el servicio que proporcionan.

- NAT/PAT (Network Address Translation/Port Address Translation). Como sólo se cuenta con una IP proporcionada por el ISP (Telmex/Infinitum) y se tienen diferentes servicios repartidos en distintos servidores, se tiene que realizar un nat de uno a muchos mediante PAT (Port Address Translation) técnica que permite el desvío de conexiones TCP/UDP realizadas a un puerto en la red externa hacía un puerto en la red interna que puede ser igual o diferente.
- VPN (Virtual Private Networks). Aunque no se contaba con este servicio se pensó en la posibilidad de poder conectar usuarios remotos a la oficina para que pudieran compartir servicios colocados dentro de la organización. Como mencioné en el capítulo anterior, la empresa ofrece servicios de soporte técnico remoto por lo cual los clientes para poder dar el acceso a los

ingenieros generan reglas en su firewall para que solo se puedan utilizar los servicios de las herramientas que tienen contratadas mediante la dirección pública de nuestra empresa. Las VPN permiten que el usuario tenga acceso a la oficina central aunque este se encuentre en la Red Pública (Internet) y de esta manera tener disponibles los servicios y políticas de red que le rigen.

Debido a que somos una empresa de pocos empleados (10 usuarios, alrededor de 20 equipos de cómputo), pensamos en una herramienta económica y que fuera única, es decir, no adquirir soluciones para cada uno de los elementos del perfil como son el antivirus perimetral, el filtrado de contenidos, control de accesos y firewall, por lo que la Dirección de Tecnología y Soporte decidió utilizar un equipo UTM (Unified Threat Management ó Administración Unificada de Amenazas) de la marca Fortinet® , modelo Fortigate 100A que posee las siguientes características:

- Firewall.
- VPN PPTP, SSL E IPSEC .
- Antivirus basado en red.
- Intrusion Prevention System (Sistema de Prevención de Intrusos). Basado en firmas y anomalías de tráfico.
- Filtrado de contenido de red. Estático (basado en listas y palabras) y por Categorías.
- Antispam. Estático (basado en listas).
- NAT/PAT. (Direcciones IP Virtuales que permiten PAT)
- 2 Puertos para DMZ, 2 Puertos para WAN y Switch de 4 Puertos para LAN

Con la información recopilada se comenzaron a construir las políticas en el firewall desde el inicio, es decir, se tuvo que realizar la configuración paso por paso hasta introducir todas las configuraciones y se pudo programar el cambio de equipo, mismo que se ajustó con la misma información de red del firewall original para no afectar de manera significativa a los usuarios.

Después que se inició la operación con la nueva herramienta y con base en sus características, fueron surgiendo requerimientos adicionales como:

- Asignación de IP's Dinámicas. Se habilitó el Servicio DHCP, mismo que solo es utilizado por personal directivo en sus laptops, mediante red inalámbrica.

- Restricción en la asignación de las IP's Dinámicas. (IP MAC Binding). Se anotaron las direcciones MAC de las tarjetas de red inalámbrica de aquellos que tendrían derecho a utilizar direcciones dinámicas y mediante la opción IP MAC Binding se configuró una dirección IP para cada dirección MAC por lo que si algún usuario necesita acceder a la red inalámbrica necesita proporcionar su dirección MAC y obtener autorización de la Dirección de Tecnología y Soporte.

Una vez que el UTM quedó implementado y configurado, se desarrollaron las siguientes actividades:

- Mantenimiento a la solución. Actualización de Firmware y revisión periódica de las configuraciones y bitácoras.
- Adición y Eliminación de usuarios a los grupos.
- Adición y Eliminación de servicios.
- Adición y Eliminación de políticas y perfiles de protección.
- Adición y Eliminación de NAT y PAT.

3.1.3. CONFIGURACIÓN DE CORREO ELECTRÓNICO.

Soluciones de Seguridad Informática S.A de C.V. es parte de un grupo de empresas que tienen la necesidad de tener dominios de Internet propios que puedan tener comunicación independiente, ya sea por teléfono o por correo electrónico a pesar de que dos de ellas comparten espacio físico. Es por ello que se contrataron cuatro dominios ante el NIC:

- ssisa.biz
- drsolomon.com.mx
- isw.com.mx
- acuaticanm.com.mx

Una de los primeros problemas a los que me enfrente en la empresa fue el correo electrónico, ya que se tenía la necesidad de preparar un servidor de correo electrónico de emergencia debido a fallas en el servidor actual (Microsoft® Exchange).

Como no teníamos una licencia vigente de Exchange, se optó por introducir Software Libre, ya que no representaba un costo para la empresa en este momento. Se instaló un Servidor Linux Red Hat Versión 9.0 con Sendmail.

Sendmail es un MTA (Mail Transport Agent) que se encarga de enrutar los mensajes de correo electrónico sobre Internet de forma que lleguen a su destino. Se seleccionó este sistema por ser de fácil y rápida implementación y configuración.

La configuración de sendmail fue casi por defecto, solo se ajustó la tabla de acceso (access), la tabla de dominios permitidos (local-host-names), el nombre del dominio default y la configuración de la autenticación para sendmail con el objetivo de permitir la retransmisión de mensajes a usuarios validados en el servidor vía pop3.

Se agregaron todos los usuarios y se configuró el servicio POP3 incluido en Red Hat para que se pudiera tener acceso a los buzones de correo.

Una vez que el sistema de correo funcionó, se necesitaba proteger de ataques que el firewall no pudiera detener como el spam o correo no solicitado, zombies y phishing, por lo que se pensó en una herramienta que cubriera estos aspectos.

Se recurrió de nuevo al portafolio de soluciones de la empresa y se adquirió un Ironmail de la marca Secure Computing ® el cual es un appliance de protección perimetral en correo electrónico que tiene las siguientes características:

- Firewall de correo.
- Antivirus de correo.
- Antispam.
- Filtrado de contenido de correo.
- Mail VPN.
- Cumplimiento de políticas en correo (Listas negras, blancas, revisión de contenido, monitoreo de correo, estampado de correo y análisis de adjuntos).

El esquema de implementación del appliance es como Mail Gateway, es decir, el correo llega primero al sistema para ser revisado, si no cumple con alguna de las

políticas de restricción, el correo será entregado al servidor y posteriormente descargado por el usuario mediante POP3.

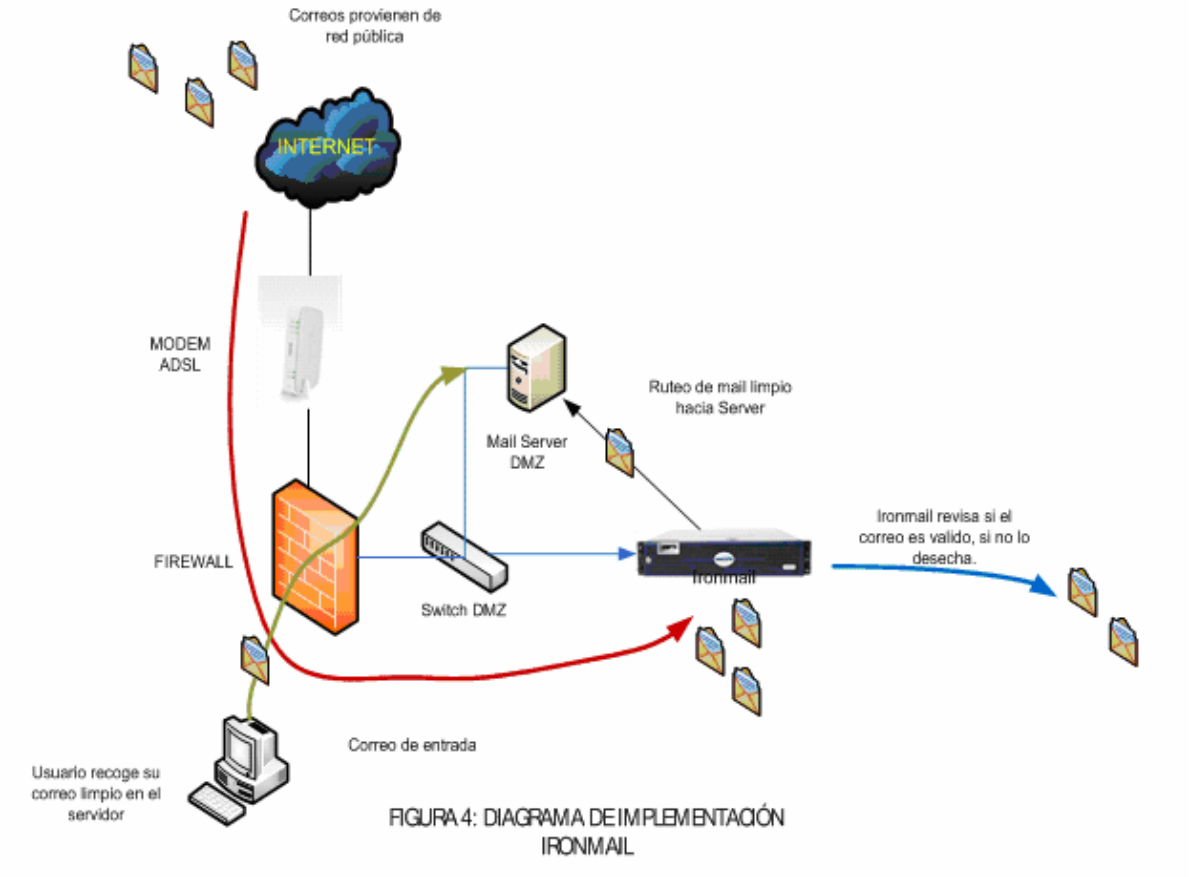


FIGURA 4: DIAGRAMA DE IMPLEMENTACIÓN IRONMAIL

Para la configuración de las políticas y restricciones se diseñó una matriz similar a la utilizada en el firewall, teniendo en cuenta las características del appliance para poder determinar los grupos de usuarios a los cuales aplicarían las reglas.

GRUPOS / CARACTERÍSTICAS	RESTRINGIDOS	LIMITADOS	ILIMITADOS
ANTIVIRUS			
SMTP	SI	SI	SI
CUMPLIMIENTO DE POLÍTICAS			
DICCIONARIOS	SI	SI	SI
LISTAS BLANCAS	NO	SI	SI
MONITOREO DE MAIL	SI	SI	NO

ANÁLISIS DE ADJUNTO	SI	SI	SI
MESSAGE STAMPING	SI	SI	SI
ANTISPAM			
REGLAS DE SPAM BASADAS EN PUNTAJES			
35	Q	Q	PASS
40	Q	Q	Q
50	Q	Q	Q
75	DROP	DROP	DROP
100	DROP	DROP	DROP
CUARENTENA DE USUARIO FINAL	NO	*NO*	*SI*
LISTAS BLANCAS DE USUARIO FINAL	NO	NO	SI
LISTA LOCAL DE NEGACIÓN	SI		
CONTROL DE CONEXIONES	SI		
FIREWALL DE CORREO Y MAILVPN			
MENSAJES POR CONEXIÓN	20		
MÁXIMO TAMAÑO PERMITIDO	10 MB	10 MB	ILIMITADO
MAXIMO DE DESTINATARIOS POR MENSAJE	200		
RELAY PERMITIDO	NO		
AUTENTICACIÓN POR SMTP	SI VIA POP3		
MAIL IDS	SI		
DENIAL OF SERVICE PROTECTION	SI DESPUÉS DE 100 CONEXIONES EN 100 SEGUNDOS		
DNS HIJACK PROTECTION	NO		
PASSWORD CRACKING PROTECTION	SI DESPUÉS DE 3 INTENTOS		
LDAP VALIDATION	SI		
POP3 MAIL VPN	SI		
IMAP 4 MAIL VPN	NO		

Cuando la matriz de datos se completó se configuró el equipo con la información y se planificó el inicio de la operación, mismo que tuvo que analizarse para verificar los cambios necesarios en el esquema actual.

Según el esquema inicial, solo se tenía el servidor de correo recibiendo tráfico mediante registros MX que apuntan a la dirección IP pública de la empresa la cual llega al firewall donde se realiza el NAT correspondiente hacia el servidor. Con el nuevo esquema se tuvo que realizar un cambio en el firewall para redirigir el tráfico de SMTP hacia el equipo de seguridad (Ironmail) y de ahí se generan rutas

estáticas de correo por cada dominio aceptado para encaminar el flujo de mensajes hacia el servidor correspondiente.

Otra de las actividades dentro de este rubro es el mantenimiento, mismo que se da al servidor de correo y al equipo de seguridad el cual consiste en:

Servidor de correo.

- Cambios en configuraciones de correo.
- Alta y baja de usuarios.
- Alta y cambios en passwords.
- Revisión de bitácoras.
- Actualización al software.
- Actualizaciones de seguridad al sistema operativo.

Equipo Ironmail.

- Alta y Baja de direcciones y dominios a Listas Blancas.
- Alta y Baja de direcciones y dominios a Listas Negras.
- Configuración de políticas y diccionarios.
- Cambios en configuraciones de seguridad.
- Revisión y análisis de bitácoras y reportes.
- Actualización de software.
- Actualizaciones de seguridad al sistema operativo.

3.1.4. SERVIDOR DNS.

El servicio de DNS (Domain Name System) es el encargado de traducir los nombres de dominios en direcciones IP. Esto es muy importante para cualquier empresa ya que para un cliente es más fácil recordar los nombres que los números, de manera que éste debe estar perfectamente implementado y configurado.

En Soluciones de Seguridad Informática, como ya mencioné anteriormente, se tienen cuatro dominios, mismos que tienen su NS (Name Server) apuntando a la dirección pública de la empresa, por lo que en nuestras instalaciones también tenemos el servidor de nombres que se encarga de resolver estos dominios.

Este servicio está alojado en un equipo con sistema operativo Windows 2003 al cual se instaló el servidor DNS de Microsoft ® en donde se crearon los registros pertinentes:

Dominio Principal:

Drsolomon.com.mx

NS: dns2.drsolomon.com.mx → 201.155.67.77

A: mailserver.drsolomon.com.mx → 201.155.67.77

A: smtp.drsolomon.com.mx → 201.155.67.77

A: www.drsolomon.com.mx → 201.155.67.77

MX: mailserver.drsolomon.com.mx Preference: 15

Ssisa.biz

NS: dns2.drsolomon.com.mx → 201.155.67.77

A: www.ssisa.biz → 216.69.181.152

MX: mailserver.drsolomon.com.mx Preference: 15

Isw.com.mx

NS: dns2.drsolomon.com.mx → 201.155.67.77

A: www.isw.com.mx → 216.69.181.152

MX: mailserver.drsolomon.com.mx Preference: 15

Acuaticanm.com.mx

NS: dns2.drsolomon.com.mx → 201.155.67.77

A: www.acuaticanm.com.mx → 216.69.181.152

MX: mailserver.drsolomon.com.mx Preference: 15

De igual forma se configuraron los registros de zona inversa para el DNS.

3.1.5. INSTALACIÓN Y CONFIGURACIÓN DE EQUIPOS DE CÓMPUTO

Como parte de la operación de la empresa, se requiere la preparación de equipos de cómputo para personal nuevo, así como el soporte técnico a los usuarios existentes. En este ámbito mis actividades consisten en:

Para asignar equipos:

- Verificar en el inventario equipo disponible.
- Verificar estado del equipo a entregar.
- Instalación y configuración de Software de fábrica para el equipo.
- Instalación y configuración de Software de aplicación requerido por el usuario.

Para brindar soporte interno:

- Recibir llamadas de usuarios y brindar orientación al problema reportado.
- Verificar localmente el problema reportado.
- Efectuar acciones correctivas.
- Llevar bitácora de atención.

3.1.6. INSTALACIÓN Y CONFIGURACIÓN DE DISPOSITIVOS DE RED.

La conectividad entre los equipos de cómputo de la empresa es de suma importancia ya que esto nos permite compartir los servicios y aplicaciones necesarias para la operación. Es por ello que se requieren elementos que permitan la intercomunicación misma que es llevada a cabo siguiendo los dos estándares más comunes:

- LAN Ethernet (IEEE 802.3).
- Wireless LAN IEEE (802.11).

Las actividades para este apartado son:

- Cableado estructurado e implementación de nuevos nodos de red.
- Implementación y configuración de switches.
- Implementación y configuración de access points para la red Wireless.

3.1.7. IMPLEMENTACIÓN DE NUEVAS TECNOLOGÍAS.

En el mercado de tecnologías de información, seguridad informática y comunicaciones, día con día surgen nuevas tecnologías que pueden cubrir necesidades actuales de las organizaciones y que por lo tanto deben ser evaluadas para verificar sus capacidades y poder determinar si la herramienta cumple con los requerimientos de la empresa; además de revisar si ésta puede ser una oportunidad de negocio.

Es por ello que en mi calidad de Administrador de red me he encargado de realizar estas evaluaciones, en las que se efectúan las siguientes actividades:

- Búsqueda de nuevas tecnologías.
- Revisión de características y requerimientos.
- Solicitud de producto para evaluación.
- Preparación del producto para la evaluación.
- Lectura y análisis de los manuales de instalación y usuario.
- Configuración del producto conforme a las necesidades.
- Elaboración de informe detallado de los resultados de la evaluación.

En este capítulo he comentado las actividades realizadas como Administrador de red que han incluido también labores de administración y control sobre los activos informáticos de la empresa.

El puesto de Administrador de red me ha permitido desarrollar habilidades tales como el desarrollo de políticas institucionales, diseño de esquemas que permitan optimizar el uso de los recursos disponibles, asignación de permisos y reglamentos a los usuarios desprendidos de las políticas, así como la implementación de servicios de red necesarios para la operación de la mayoría de las empresas.

En lo personal creo que la administración es una de las actividades que cualquier Ingeniero debe desarrollar ya que esta le permite planificar, organizar, programar y controlar los recursos materiales y humanos que tiene a su cargo para lograr su utilización de forma óptima y eficiente. En este caso solo administré recursos materiales, los cuales en ocasiones no eran los ideales para poder trabajar, sin embargo, los utilicé de manera que la operación se pudo llevar a cabo sin complicaciones.

En el capítulo siguiente retomando mis actividades como Ingeniero de Soporte Técnico, platicaré respecto a los proyectos que se desarrollan en el área de Soporte, los cuales se catalogan por gama de productos que se ofrecen por parte de Soluciones de Seguridad Informática.

CAPÍTULO IV: PROYECTOS Y CURSOS DE ACTUALIZACIÓN.

4.1. PROYECTOS.

Como parte de mis tareas en el puesto de Ingeniero de Soporte Técnico, se han tenido que desarrollar proyectos con clientes ya sea para proponer una solución o para implementarla.

Para entender este tipo de proyectos en Soluciones de Seguridad se debe primero tener en cuenta qué es lo que queremos proteger, de qué queremos protegerlo y cómo lo haremos. Para lograr este objetivo existen medidas preventivas y correctivas que deben llevarse a cabo mediante la concientización por parte de los usuarios en primer lugar y en segundo empleando las herramientas necesarias que funcionen proactiva y reactivamente.

La concientización de los usuarios se lleva a cabo mediante el conocimiento de sus vulnerabilidades, las amenazas a las que está expuesto y el riesgo que corre al estar conectado en red o ejecutar aplicaciones vulnerables. También como ya se mencionó se debe saber qué es lo que se protegerá; principalmente son tres cosas:

- Los datos.
    - Tienen tres características que deben protegerse:
        - Confidencialidad. Solo deben conocerlos las personas adecuadas.
        - Integridad. Que no sean modificados por quién no está autorizado.
        - Disponibilidad. Utilizarlos en el momento necesario.

- Los recursos. Los recursos tecnológicos de la empresa deben estar disponibles para ser utilizados en beneficio de la misma (ancho de banda, discos duros, memoria, etc.), no para ser utilizados por terceros como medio para realizar actividades ilícitas o a favor de quién decide usarlos sin autorización.
- La reputación de la empresa. Al utilizar los recursos, el intruso puede apoderarse también de la identidad de la empresa, lo que repercute directamente en su reputación. Los impostores pueden falsificar correo electrónico, suplantar la identidad en alguna página Web para realizar ataques de phishing, o enviar archivos infectados con virus, lo que seguramente hará que la empresa quede en entre dicho y con esto gane mala reputación que se traducirá en falta de confianza por parte de los clientes.

Otro punto importante es contra qué nos protegemos, en este sentido existen:

- Malware (Virus, Troyanos, Gusanos, Spyware, etc.)
- Intrusos.
- Vulnerabilidades de Sistemas operativos.
- Espionaje.
- Errores humanos.

Y por último, ¿cómo se puede proteger en contra de las amenazas que existen? Por medio de herramientas de seguridad destinadas a detectar, detener y erradicar de forma reactiva y proactiva los ataques para los que están concebidas.

En nuestra empresa nos dedicamos particularmente a tres tipos de herramientas:

- Antivirus.
- Firewalls.
- Seguridad de correo electrónico.

Estas herramientas están catalogadas como proyectos internos, mismos que son desarrollados como se describe a continuación:

4.1.1. ANTIVIRUS.

Mi trabajo concretamente en el rubro de antivirus consistió en la recomendación e implementación de herramientas antivirus en entornos de red para empresas pequeñas, medianas y grandes.

Existen 2 tipos de antivirus que podemos emplear:

- End Point. Se refiere a los antivirus instalados localmente en el equipo que se desea proteger.
- Perimetral. Se refiere a las herramientas integradas en otros sistemas (seguridad de correo, firewalls utm, ips, entre otros) que evitan desde el perímetro de la organización que ingrese código malicioso.

Los proyectos que se manejaron en este apartado siempre fueron enfocados al end point, debido a que el antivirus perimetral generalmente se configura como parte de otras herramientas.

Para poder llevar a cabo la recomendación de una herramienta antivirus (misma que debía ser entregada por el departamento de ventas al cliente), se debe considerar el tamaño de la empresa en cuanto a nodos disponibles, si requieren

administración centralizada, rapidez de los equipos y sistemas operativos que se tienen.

Con esta información se puede recomendar un producto que cubra dichos requerimientos.

4.1.1.1. ETAPAS DEL PROYECTO EN EL ÁREA DE SOPORTE.

Las etapas de los proyectos antivirus son:

- Marco conceptual.
- Definición de objetivos.
- Definición de requerimientos y plataformas.
- Evaluación.
- Seguimiento a la evaluación.
- Obtención de resultados.
- Proceso de venta (Entrega de resultados al cliente y cierre).
- Definición de administración y operación.
- Implementación.
- Capacitación y concientización.
- Seguimiento.

Estas etapas serán descritas en los puntos siguientes.

4.1.1.1.1. Marco conceptual.

Para que el cliente entienda cual es el riesgo que tiene como consecuencia de las vulnerabilidades que presenta, así como las amenazas a las que se enfrenta, es necesario presentarle un marco conceptual referente a estos temas mismos que se presentan a continuación.

¿Qué es un virus?

Un virus informático es un programa con la capacidad de transmitirse entre equipos de cómputo y redes, generalmente sin que el usuario se percate de ello[1]. Los virus pueden tener indeseables efectos secundarios, desde sólo imprimir en pantalla absurdos mensajes, hasta la destrucción de lo más valioso de un sistema informático: los datos.

[1] Sophos Plc. *"Virus informáticos al descubierto"*. Reino Unido, Ed. por Paul Oldfield, Tr. Javier Acebes, 2002. p. 8.

Para que un virus infecte una computadora, necesita ser ejecutado. Con este propósito, los virus pueden adherirse a documentos y programas con tal que cuando un usuario intente abrir el archivo infectado, éste ejecute inmediatamente el código malicioso. En ese momento el virus intentará infectar otros archivos, así como realizar cambios en la computadora.

Adicionalmente a los virus existen otros tipos de código malicioso como son los troyanos, gusanos y spyware.

Troyanos

Un caballo de Troya es un programa que en su ejecución realiza tareas no previstas de antemano[2], es decir, el usuario que lo ejecuta de manera normal, no se percata de que se están realizando tareas ocultas y a menudo malignas. Los troyanos se utilizan regularmente para extender la infección de algún virus o abrir puertas traseras para permitir a un atacante tomar el control de la computadora.

Gusanos

Los gusanos son similares a los virus pero no requieren portador para su ejecución, es decir, es un programa que totalmente contiene código malicioso y para replicarse crean copias exactas de ellos mismos y utilizan las redes para extenderse. Estos gusanos pueden propagarse por correo electrónico o explotar vulnerabilidades de los sistemas operativos para poder ingresar al sistema y provocar daño.

Spyware/Adware

Los programas espía son similares a los troyanos ya que el usuario ejecuta un programa que supuestamente tiene una función, pero de forma oculta se están llevando a cabo procesos que tienen como objetivo que un atacante obtenga el control del sistema para posteriormente llevar a cabo robo de identidad (spoofing), robo de información y espionaje. Los fabricantes de spyware se aprovechan de la ingenuidad de usuarios al proporcionar para sus programas temas relacionados con tarjetas de felicitación, programas para descargas gratuitas, relaciones personales y pornografía, entre otros.

El spyware puede propagarse mediante páginas de Internet en donde de manera involuntaria y oculta se descarga e instala en el sistema para reportar al atacante

[2] Sophos Plc. *"Virus informáticos al descubierto"*. Reino Unido, Ed. por Paul Oldfield, Tr. Javier Acebes, 2002. p.9.

hábitos de navegación, gustos y preferencias del usuario y así poder insertar anuncios que se despliegan de forma automática[3].

Otra de las técnicas es enviar por correo electrónico supuestas tarjetas de felicitación o imágenes pornográficas que provocan el interés de los usuarios. Al abrir la supuesta imagen, en realidad se están instalando programas en la computadora que pueden abrir puertos para que un atacante tome el control del sistema y utilizar los recursos en su favor, por ejemplo, para enviar campañas de spam utilizando el equipo como zombie o revisar archivos y capturar pulsaciones de teclas.

Puntos vulnerables de infección.

Los virus como cualquier otra amenaza de seguridad producen riesgo cuando existe algún punto vulnerable que pueda ser descubierto y explotado por un atacante. Los puntos más sensibles en los cuales se pueden encontrar son:

Internet: Ya que se pueden descargar programas o documentos que puedan contener virus o troyanos, además de que se podría ejecutar código malicioso durante la lectura de ciertos sitios.
Programas: Un programa con virus puede infectar el equipo en cuento se ejecute.
Documentos y hojas de cálculo: Pueden contener virus de macro que podrían infectar y realizar cambios en otros documentos.
Unidades de almacenamiento extraíble: Como diskettes, CD-ROM y Unidades Flash, podrían contener virus en los sectores de arranque, además de que pueden contener documentos o programas infectados.
Email: El email podría venir con archivos adjuntos infectados e incluso ejecutar código malicioso mientras se está leyendo.

[3] http://www.segu-info.com.ar/malware/spyware.htm

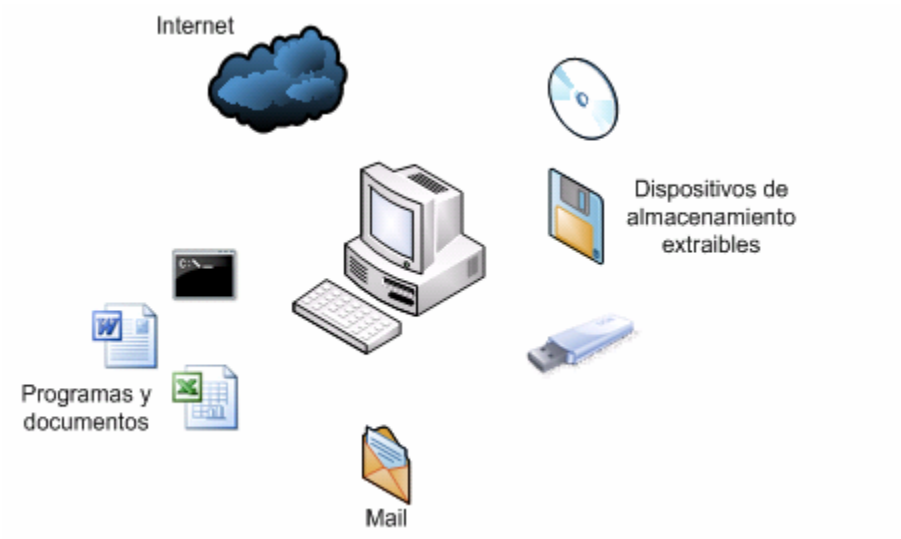


FIGURA 5: Puntos Vulnerables de Infección.

Programas antivirus[4].

Los programas antivirus pueden detectar virus informáticos, prevenir el acceso a archivos infectados y a menudo terminar con el problema de infección.
Los virus como se ha mencionado pueden borrar documentos o modificar datos, aunque este no es el principal inconveniente, sino la consecuencia de que estás situaciones ocurran, ya que los virus pueden bloquear computadoras o forzar a la desconexión de los servicios de red lo cual repercutiría en la perdida de costosas horas de trabajo. De igual modo la confidencialidad puede estar amenazada cuando se trata de código malicioso que envíe información confidencial, así como también se puede poner en entre dicho la reputación de una organización ya que si por ejemplo esto le ocurriera a un banco, las personas no querrían tener sus cuentas ahí.
Existen diferentes tipos de antivirus:

- Escáner: Programas que pueden detectar y a menudo desinfectar los virus conocidos hasta la fecha del programa. Este tipo de antivirus es el más popular aunque hay que actualizarlo a menudo para que reconozca nuevo virus. Por lo regular tiene escaneo en acceso, en demanda o ambos.
- Heurísticos: Los programas heurísticos no basan la detección en un archivo de definición, sino que se basa en la apariencia y comportamiento de lo que escanea, por lo que a menudo puede producir falsas alarmas.
- Verificador: Programas que detectan si un archivo ha sido modificado. Lo mejor de este sistema es que no requiere actualizaciones, sin embargo puede resultar problemático por ejemplo con los documentos, ya que

[4] Sophos Plc. *"Virus informáticos al descubierto"*. Reino Unido, Ed. por Paul Oldfield, Tr. Javier Acebes, 2002. pp. 16-17.

cambian cada que trabajamos con ellos. Otra desventaja es que solo puede detectar el virus una vez que se ha provocado la infección.

Las herramientas antivirus pueden ser de cualquiera de los tres tipos anteriores, aunque a veces podemos encontrar software que combine estas tecnologías.

Las herramientas antivirus también pueden ser:

- Con Administración centralizada. Usualmente la más usada en la empresa ya que está destinada a funcionar en corporativos que requieren la administración sencilla, rápida y desde un punto central, que permita el despliegue y administración de políticas, actualizaciones automáticas y visualización de reportes, así como la ejecución y programación de escaneos.
- Stand alone. Usada para estaciones de trabajo únicas que generalmente no comparten recursos de red aunque pueden estar conectadas a Internet. Este antivirus se configura localmente y las actualizaciones pueden ser manuales o automáticas.

4.1.1.1.2. Definición de objetivos.

Se tienen que definir los objetivos para plantear los alcances del proyecto que permitan tener una idea clara de porqué, para qué, con quién y con qué se llevará a cabo.

El objetivo de una solución antivirus es detectar y prevenir virus informáticos, así como evitar su propagación. Para tal efecto, esta solución debe ser implementada en cada uno de los equipos de la organización a fin de cumplir con la sentencia anterior, además de poderse desplegar desde un punto centralizado cuando se trata de muchos usuarios, para que de esa manera la configuración pueda estandarizarse y las tareas de administración y reporteo sean más sencillas.

4.1.1.1.3. Definición de requerimientos y plataformas.

Se tiene que platicar con el cliente cuales son los requerimientos para poder implementar una solución de este tipo, es decir, si necesita administración centralizada, reportes, escaneos programados, en demanda, etc. Asimismo se le cuestionará respecto a la plataforma en la que será implementada la solución, así como las características mínimas y máximas de sus equipos y de esta manera poder ofrecerle la herramienta adecuada.

4.1.1.1.4. Evaluación.

Una vez que se le ofrece la solución antivirus se establecen fechas para realizar evaluaciones con el software propuesto en entornos destinados a la evaluación o en entornos operativos. Asimismo se determina si la evaluación será en todos sus equipos o estará limitada a un número mínimo de equipos. Para llevar a cabo esta tarea se requiere apoyo del fabricante de la solución para proporcionar los elementos necesarios para la misma como son: paquetes de instalación, licenciamientos temporales y manuales.

4.1.1.1.5. Seguimiento a la evaluación.

Cuando se ha implementado la solución se tiene que tener estrecha comunicación con el cliente para detectar errores y corregirlos, así como ir conociendo sus necesidades más detalladamente y poder aplicar cambios si es necesario y de esta manera sacar el máximo provecho de esta etapa, ya que es aquí donde el cliente basará en gran medida su decisión.

4.1.1.1.6. Obtención de resultados.

Una vez concluido el proceso de evaluación, se deben obtener reportes para poder justificar la compra y que sea más sencilla para el cliente la adquisición. Es necesario realizar un informe detallado de los pormenores y resultados de dicha evaluación para que pueda ser entregado a las personas responsables de autorizar la operación.

4.1.1.1.7. Proceso de venta (Entrega de resultados al cliente y cierre).

Esta tarea se llevará a cabo por el departamento de ventas. De esto depende seguir hacia la implementación o terminar el proyecto.

4.1.1.1.8. Definición de Administración y operación.

Se tendrá que definir quién Administrará el sistema antivirus, así como quien se encargará de instalar, configurar, actualizar y escanear los equipos a implementar.

4.1.1.1.9. Implementación.

Para poder realizar la implementación debemos tener en cuenta las fechas tentativas, así como los equipos y personal requerido.
Se deben realizar pruebas antes de liberar el proyecto, aunque generalmente esta fase se lleva a cabo durante la evaluación y no es necesario volverla a realizar.

4.1.1.1.10. Capacitación y concientización.

Cuando se llega a la conclusión de la implementación se debe hacer una campaña de concientización hacia los usuarios para indicarles qué es lo que se les instaló, para qué sirve y cómo lo pueden utilizar. Asimismo proporcionar información referente a los virus y sus prevención. Además tenemos que ofrecer capacitación al personal encargado de la administración para que aprenda a utilizar la consola central y el software antivirus.

4.1.1.1.11. Seguimiento.

El seguimiento se refiere a estar monitoreando la solución periódicamente para descartar configuraciones erróneas y corregir lo que sea necesario, así como verificar si el cliente tiene requerimientos adicionales o actualizar el software cuando se precise.

4.1.2. FIREWALLS

En el rubro de firewalls los proyectos fueron encaminados a Pequeñas y Medianas empresas y la mayoría se enfocaron a una sola marca de producto, por lo que comentaré mi experiencia con este tipo de dispositivos.

Como en el caso de las herramientas antivirus, existen firewalls de para usuario final y perimetrales. También los hay de software y de hardware.

Los productos que yo manejé fueron de hardware, es decir, es un aparato específicamente diseñado para esta función, con software propietario y endurecido y no se le puede modificar nada, excepto sus configuraciones.

4.1.2.1. ETAPAS DEL PROYECTO EN EL ÁREA DE SOPORTE.

Las etapas de los proyectos de firewalls son:

- Marco conceptual.
- Definición de objetivos.
- Definición de requerimientos y plataformas.
- Evaluación.
- Seguimiento a la evaluación.
- Obtención de resultados.
- Proceso de venta (Entrega de resultados al cliente y cierre).
- Definición de administración y operación.
- Implementación.
- Capacitación y concientización.
- Seguimiento.

Estas etapas serán descritas en los puntos siguientes.

4.1.2.1.1. Marco conceptual.

Para que el cliente entienda cual es el riesgo que tiene como consecuencia de las vulnerabilidades que presenta, así como las amenazas a las que se enfrenta, es necesario presentarle un marco conceptual referente a estos temas mismos que se presentan a continuación.

¿Qué es un firewall?

Un firewall es un elemento de hardware o software que se utiliza en una red de computadoras para controlar los accesos de una red insegura (Internet) a la red segura (LAN). Esto se lleva a cabo mediante políticas de seguridad definidas por el administrador de la red.

Los firewalls son dispositivos que se deben ubicar en el punto de conexión de la red interna con la red exterior aunque también existen firewalls que poseen diferentes segmentos de red en los cuales se puede separar el tráfico entre ellos, lo cual es muy común utilizar para las llamadas DMZ (Zonas desmilitarizadas) que se utilizan para colocar en estos segmentos los servidores públicos de la organización.

Tipos de firewalls.

Firewalls de filtrado de paquetes.

Este tipo de firewalls funcionan a nivel de red (capa 3 del modelo OSI) como filtro de paquetes IP, ya que es aquí donde se restringen o permiten las direcciones IP. También funcionan a nivel de transporte (capa 4 del modelo OSI) para poder restringir servicios y puertos de TCP o a nivel de enlace de datos (capa 2 del modelo OSI) en donde se restringen las direcciones MAC.

El filtrado de paquetes mediante puertos y protocolos, permite establecer qué servicios estarán disponibles para el usuario y por cuales puertos.

Stateful Firewalls.

Son Firewalls que mantienen rastro de las conexiones de red que pasan por él. Usando este método el firewall recopila información del encabezado TCP del paquete como dirección IP origen –destino, puerto origen –destino y número de la secuencia del paquete y lo guarda en su tabla de inspección. Cuando se recibe un paquete de respuesta el firewall compara la información reportada en el encabezado del paquete con la tabla. Si concuerda esta información el paquete es aceptado y si no es desechado. Además registra sesiones para los protocolos no orientados a conexión como UDP para poder realizar su trabajo[5].

Firewalls de aplicación.

El firewall de aplicación es aquel que funciona en capa 7 del modelo OSI, de manera que el filtrado se puede adaptar a características del protocolo en este nivel.
El firewall de capa 7 suele denominarse proxy y es el encargado de filtrar conexiones entre la red interna y la externa fungiendo como intermediario. Cuando el usuario desea un servicio lo hace a través del Proxy a fin de que este realice la petición al servidor destino y devuelva los resultados al cliente. Su función es analizar el tráfico de red en busca de contenido que viole las políticas definidas por el administrador.

[5] http://www.juniper.net/products/integrated/stateful_inspection_firewall.pdf

Deep packet inspection.

Este tipo de tecnología permite examinar no solo el encabezado de TCP sino también los datos contenidos en el paquete a fin de determinar anomalías del protocolo, virus, spam, contenido inapropiado para decidir si el tráfico es aceptado o desechado. La inspección profunda al paquete se lleva a cabo normalmente con firmas definidas o heurística a fin de determinar si lo que va dentro del paquete es permitido o denegado[6].

NAT/PAT.[7]

Network Address Translation es el proceso mediante el cual se modifica la información de la red contenida en el encabezado del datagrama de IP mientras pasa el tráfico por el ruteador con el propósito de volver a trazar la ruta de un rango de direcciones a otro.

Esta técnica es usada en conjunto con el enmascaramiento de dirección, que sirve para esconder un segmento de direcciones atrás de una sola dirección IP. Esto se logra escribiendo una tabla de traducción en la cual se guarda la comunicación de la red interna hacia el exterior, el router cambia la información en el encabezado de IP para que el servidor destino detecte la conexión proveniente del router. Los paquetes de regreso llegan al router y este verifica en su tabla de traducción a que IP de la red interna debe entregar los paquetes. La tabla es reescrita una vez que se termina la comunicación con nuevas conexiones a las que se aplicará el mismo procedimiento.

[6] http://www.securityfocus.com/infocus/1716

[7] http://cbl.abuseat.org/nat.html

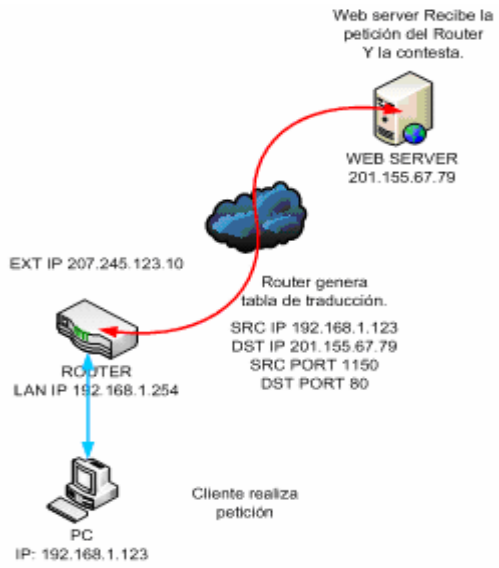


FIGURA 6: Network Address Translation/
Enmascaramiento de red.

Port Address Translation es una característica de un dispositivo de red que tiene como objetivo traducir comunicaciones TCP/UDP hechas entre equipos que se encuentren en redes privadas y equipos de redes públicas. Permite que una sola dirección pública pueda usarse con muchos equipos en la red interna para compartir servicios de TCP/UDP. Esto se logra modificando los paquetes de TCP/UDP de manera que si la comunicación es efectuada en un puerto específico, esta pueda ser reenviada al mismo puerto o a otro distinto en la red interna.

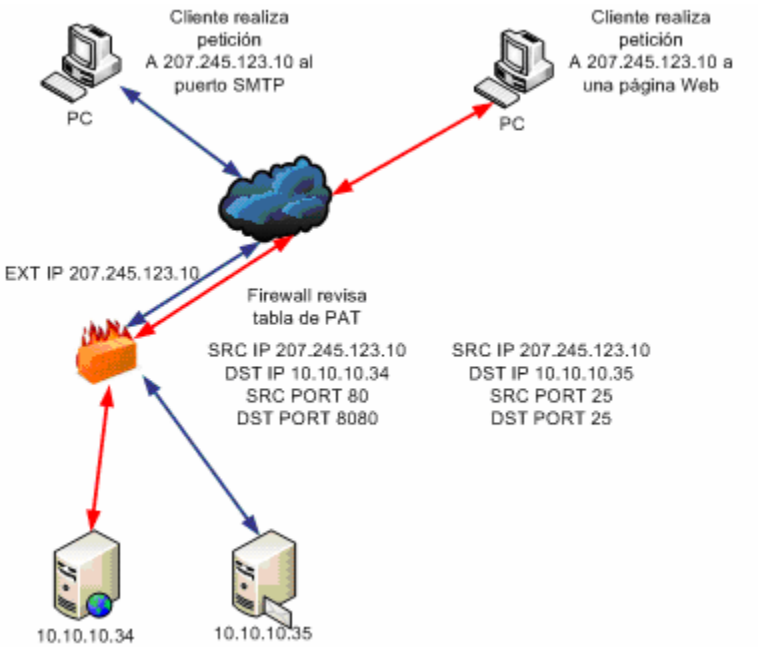


FIGURA 7: Port Address Translation.

4.1.2.1.2. Definición de objetivos.

Teniendo en cuenta las definiciones anteriores, podemos determinar que el firewall dentro de una organización es indispensable, ya que su objetivo es controlar los accesos que existen entre un segmento de red y otro, generalmente entre la red interna y la externa y viceversa ó de la red externa a una DMZ para publicar servicios. Además dependiendo del tipo de firewall podemos inclusive prevenir el acceso no autorizado a los sistemas mediante detección de intrusos, tener un antivirus en el firewall para algunos protocolos, filtrado de contenido en correo y en web, bloqueo de aplicaciones no productivas y funciones de reporteo.

Aunque un firewall puede ayudarnos a mejorar la seguridad de la empresa, no nos protegerá contra ataques de ingeniería social, espionaje e inclusive ataques internos de virus, spyware o en contra de lo que los mismos usuarios realicen en la red local.

4.1.2.1.3. Definición de requerimientos y plataformas.

El cliente debe informarnos cuales son los requerimientos específicos que el tiene para adquirir una solución de este tipo, como son:

- VPN.
- Firewall.
- Filtrado de Contenido.
- Bloqueo de aplicaciones improductivas.
- Antivirus.
- Anti-spam.
- Detección de intrusos.
- Reporteo.

Igualmente debe mencionar:

- Entorno actual (Herramientas de este tipo con las que cuenta, esquema de red, si cuenta con servicios públicos, etc)
- Proveedor de Servicios de Internet.

Todo lo anterior es con el fin de ofrecerle al cliente la solución adecuada y planificar el esquema idóneo en el cual se ajustará la solución.

Ya que se le ha propuesto al cliente el esquema que se considera será el más adecuado, se le tienen que indicar las repercusiones que al implementar se puedan presentar como:

- Desconexión de los servicios por un lapso de tiempo.
- Cambios de direccionamientos IP.
- Necesidad de adición de rutas estáticas en el dispositivo.

Asimismo se debe contar con un plan de rollback con el objetivo de poder retornar al punto inicial.

4.1.2.1.4. Evaluación.

Cuando el cliente acepta la propuesta efectuada por la Dirección de Ingeniería y Soporte, además de estar consciente de las consecuencias, se fija la fecha en que se podrá comenzar con la evaluación, misma que consiste en implementar el esquema propuesto en un entorno de preferencia operativo, aunque a petición del cliente se podrá llevar a cabo en un entorno de pruebas para no afectar la producción. Durante el periodo de evaluación se requiere apoyo del fabricante para habilitar los servicios del equipo de forma temporal, así como por parte nuestra verificar la disponibilidad de un equipo para demostración que pueda ser prestado al cliente.

4.1.2.1.5. Seguimiento a la evaluación.

Se debe mantener comunicación con el cliente una vez iniciada la evaluación para conocer requerimientos adicionales, así como ayudarlo a complementar la configuración de manera que vaya robusteciéndose, ya que entre mejor estén declaradas las políticas, mejor será la seguridad ofrecida por el dispositivo.

4.1.2.1.6. Obtención de resultados.

En el momento que la evaluación concluye se debe generar un reporte que contenga información obtenida directamente del equipo, así como el progreso que se tuvo durante la evaluación, si se alcanzaron los objetivos y cuales aspectos quedaron pendientes, todo esto con el objeto de justificar ante el cliente la manera en que esta solución ayudará a su negocio y se pueda tener como argumento para negociar una adquisición.

4.1.2.1.7. Proceso de venta (Entrega de resultados al cliente y cierre).

El departamento de ventas se encargará de entregar los resultados obtenidos durante la evaluación y negociar con el cliente los costos que representará contar

con la herramienta. Una vez que el cliente acepta la propuesta económica se puede continuar con el proceso.

4.1.2.1.8. Definición de la Administración y operación.

Se debe definir quién administrará el producto, a fin de determinar las personas involucradas en el proyecto durante las fases siguientes.

4.1.2.1.9. Implementación.

Se planifica la implementación estableciendo fechas, personas, equipo y repercusiones en el entorno. Esta planificación contemplará tiempos máximos, ventanas de tiempo, cambios adicionales y sus consecuencias. Generalmente para este tipo de equipos se hace un respaldo de la configuración realizada durante el periodo de evaluación, de manera que cuando ya se tenga el equipo definitivo, el proceso sea mucho menor en tiempo y el cambio sea lo más transparente posible.

4.1.2.1.10. Capacitación y concientización.

Se proporcionará un entrenamiento "hands on" al usuario con el objetivo de que entienda más detalladamente los alcances de esta herramienta y tenga el conocimiento necesario para comenzar con la administración y operación. Asimismo por parte del cliente se deben definir las nuevas políticas que serán aplicadas y comunicadas al usuario final, de manera que entienda sus restricciones y los mecanismos que deberá seguir para pedir permisos especiales (si son viables) o reportar problemas que puedan presentarse.

4.1.2.1.11. Seguimiento.

Monitorear la solución periódicamente es completamente necesario para el seguimiento que se requiere en este tipo de soluciones, ya que nos permitirá descartar fallas o realizar cambios necesarios no contemplados en la configuración inicial, así como atender requerimientos adicionales por parte del cliente.

4.1.3. SEGURIDAD EN CORREO ELECTRÓNICO.

En este apartado el tipo de empresas atendidas fueron Medianas y Grandes. De igual manera que para los firewalls este rubro fue atendido con una sola marca de producto que funciona como un equipo integral de seguridad de correo electrónico al cubrir aspectos como: spam, virus, phishing, fraude y robo de identidad, firewall de correo, detección de intrusos, protección de pop3, imap4 y Webmail.

El producto que utilicé es una solución de hardware, con sistema operativo endurecido y una aplicación propietaria que se administra vía Línea de comandos y Web.

4.1.3.1. ETAPAS DEL PROYECTO EN EL ÁREA DE SOPORTE.

Las etapas de los proyectos de seguridad en correo electrónico son:

- Marco conceptual.
- Definición de objetivos.
- Definición de requerimientos y plataformas.
- Evaluación.
- Seguimiento a la evaluación.
- Obtención de resultados.
- Proceso de venta (Entrega de resultados al cliente y cierre).
- Definición de administración y operación.
- Implementación.
- Capacitación y concientización.
- Seguimiento.

Estas etapas serán descritas en los puntos siguientes.

4.1.3.1.1. Marco conceptual.

Para que el cliente entienda cual es el riesgo que tiene como consecuencia de las vulnerabilidades que presenta, así como las amenazas a las que se enfrenta, es necesario presentarle un marco conceptual referente a estos temas mismos que se presentan a continuación.

Correo Electrónico.

El correo electrónico es un servicio de red que permite el envío y recepción de mensajes mediante sistemas electrónicos usando para ello el protocolo SMTP. Por este medio se puede enviar no solo texto, sino también documentos, imágenes y otros tipos de archivo por lo cual se ha convertido en un medio de comunicación muy eficiente, además de estar desplazando al correo ordinario en muchas aplicaciones.

Las ventajas del correo electrónico son muchas entre las cuales se encuentran:

- Barato. Los costos son bajos en comparación de otros medios de comunicación.
- Rápido. La información o mensaje llega en minutos.

- Confiable. Si la configuración de red de nuestra empresa es correcta, el mensaje siempre llegará a su destino.
- Flexible. Se puede utilizar a todas horas y desde cualquier sitio.
- Se puede utilizar como medio de comunicación interno y externo.
- Posibilidad de adjuntar documentos, imágenes, entre otros tipos de archivos.

Protocolo SMTP (Simple Mail Transfer Protocol[8]).

El protocolo SMTP es el encargado de transferir el correo de un punto a otro utilizando como medio de Transporte el protocolo TCP (Mail Relaying). Este servicio utiliza como puerto estándar el 25/TCP y su funcionamiento se basa en una comunicación cliente – servidor sobre redes perfectamente accesibles una de la otra, asimismo puede ser en la misma red o en cualquier otra vía relay o Gateway del servidor de correo que haga accesible ambas redes. Los mecanismos de Intercambio de correo definidos en el Sistema de Nombres de Dominio (DNS) son usados para identificar el siguiente brinco a donde será transportado el mensaje.

Protocolo POP3 (Post Office Protocol).

Es un protocolo que sirve para obtener los mensajes de correo electrónico de un servidor remoto. Está diseñado para que el usuario pueda tener acceso a sus mensajes sin estar conectado al servidor de correo, de manera que POP3 se encargará de descargar la información en el cliente para que pueda ser consultada después. Además los clientes de correo poseen opciones para dejar los mensajes en el servidor hasta que se decida eliminarlos o para tener un respaldo de los mismos.

Protocolo IMAP4 (internet Message Access Protocol).

Sirve al igual que POP3 para obtener los mensajes de correo electrónico de un servidor remoto.
Es un protocolo más complejo que POP, ya que el cliente permanece conectado al buzón mientras se trabaje con los mensajes y las tareas de creación de carpetas y eliminación de mensajes se efectúan directamente en el servidor.

[8] http://www.ietf.org/rfc/rfc2821.txt
http://www.ietf.org/rfc/rfc2822.txt

Partes del mensaje de correo electrónico.

Un mensaje de correo electrónico consta principalmente de dos partes:

- Encabezado: Contiene la información del correo electrónico, remitente, destinatario, Asunto, fecha de envío, servidores por los que pasó, etc.
- Cuerpo: Contiene el mensaje como tal.

Además de estas dos partes, el mensaje también puede contener archivos adjuntos que pueden ser de cualquier tipo, aunque por seguridad no se recomienda enviar archivos de tipo ejecutable.

Problemas de seguridad en correo electrónico.

Spam.

El spam es el correo comercial no solicitado que llega a nuestros buzones de correo electrónico generalmente ofreciendo productos y servicios tales como:

- Farmacéuticos, drogas o remedios para perder peso o alargar o mejorar partes del cuerpo.
- Esquemas de cómo hacerse rico rápidamente.
- Servicios financieros.
- Escuelas y capacitación.
- Apuestas y juegos en línea.
- Software pirata o a bajos precios.
- Pornografía y materiales de entretenimiento para adultos.

Esto directamente afecta la productividad del personal de la empresa que debe pasar minutos u horas enteras revisando y eliminando los mensajes que saturan su buzón.

Cadenas.

Las cadenas son mensajes que envían personas comunes de forma masiva debido a que se trata de información errónea que pretende alertar y asustar a los usuarios con información falsa sobre ataques terroristas, milagros si se envía el mensaje a un número determinado de destinatarios o maldiciones si ocurre lo contrario. En otros casos pretende que se envíe el mensaje para efectuar peticiones en contra de leyes propuestas o indicando que si se manda tantas veces ganarás un premio o un servicio gratis, así como también los chistes de la existencia de un nuevo virus altamente destructivo ó la cancelación de algún servicio muy popular en Internet.

Las cadenas son un problema porque generan tráfico innecesario en la red, además de que el usuario pierde mucho tiempo enviando estos mensajes que lo único que logran es desinformar y provocar que la cadena se extienda. Al enviar este tipo de mensajes el usuario también podría provocar que se catalogue a la IP de origen como generadora de tráfico "malo" por lo que los mensajes "buenos" podrían tener problemas de entrega.

Phishing.

El phishing es el engaño que se pretende realizar al usuario mediante el uso de elementos aparentemente verídicos para intentar robar datos que el atacante pueda utilizar en perjuicio del usuario.
Esto lo pueden hacer suplantando la identidad de una institución respetable como puede ser por ejemplo un banco. El atacante envía un correo al usuario a nombre del banco indicándole que requieren actualizar sus cuentas y que por lo tanto requiere su número de cuenta, su contraseña de acceso, su PIN y le ofrecen en ocasiones una liga a un sitio Web en la cual se muestra una página del banco suplantada pero que a la vista es idéntica a la original. Si el usuario ingresa sus datos seguramente será víctima de un robo por parte de sus atacantes.

Virus.

Los virus siguen siendo un problema de seguridad, ya que aunque actualmente casi no se reportan ataques de virus de correo, estos pueden infectar alguna máquina localmente y provocar que desde adentro se generen ataques de spam o si es instalado algún troyano de puerta trasera permitir a algún atacante tomar control del equipo para utilizarlo en el envío de correo comercial.

Robo de identidad y spoofing.

Esta técnica se da como resultado del robo de direcciones y dominios que se puede realizar mediante sensores que los atacantes colocan en internet para determinar y almacenar las direcciones de correo electrónico de páginas respetables para después suplantar la identidad y enviar mensajes a nombre de estas personas, lo que se conoce como spoofing. Esta técnica a menudo es usada para atacar el mismo sitio de la cuenta robada para intentar burlar la seguridad instalada.
A consecuencia de esto el dominio de la cuenta robada pudiera recibir miles de notificaciones de entrega fallida debido a que tal vez el atacante esté realizando ataques de robo de directorio, en el cual se intenta obtener direcciones validas mediante fuerza bruta o adivinando las cuentas.

Zombies.

Los zombies son producto de ataques de troyanos de puerta trasera que permiten a algún atacante tomar el control del equipo con el objeto de enviar correo comercial o masivo. Esto se lleva a cabo por la necesidad del atacante de estar

vigente, ya que si éste enviara correo desde su propio sitio, sería rápidamente identificado como spammer y no podría realizar de manera efectiva su ataque. Es por ello que utiliza equipos de usuarios que no se percatan que esto ocurre y casi siempre la ocupación del zombie no durará más de 4 horas.

Técnicas para prevenir y erradicar amenazas de correo electrónico.

Real Time Blackhole List.

Son listas negras en donde se introducen direcciones que generan correo masivo, malicioso o comercial de manera consciente o inconsciente que son consultadas por las herramientas de seguridad para poder determinar si la IP origen es presuntamente maliciosa o no. Las listas negras son tecnología obsoleta y no son muy confiables debido a que aún en la actualidad son alimentadas manualmente mediante reportes de usuarios, además de que en algunos sitios de RBL's listan segmentos de direcciones enteros basándose en la reputación del proveedor de servicios de internet en cuestión.

Reverse DNS Lookup.

Es una técnica que consiste en verificar el Sistema de Nombres de Dominio (DNS) para determinar el dominio al que pertenece una IP específica. Para las herramientas de seguridad de correo, es útil para determinar que la IP corresponda con el dominio de correo que recibimos y comprobar la identidad del remitente.

Sender Policy Framework/Sender ID[9].

Son protocolos que permiten verificar que los mensajes provenientes de una IP específica tengan autorizado utilizar el dominio en los comandos de SMTP HELO ó MAIL FROM basándose en la información proporcionada por la política de envío del propietario. Estas políticas serán publicadas en el sistema de nombres de dominio para poder ser consultadas por herramientas de seguridad y garantizar que el remitente no está suplantando la identidad de un dominio confiable.
Se debe configurar cualquiera de los dos protocolos para comprobar la identidad. Si se tiene implementado este sistema, el destinatario solo recibirá aquellos correos en los que se compruebe que tienen permiso de utilizar el dominio, los demás serán rechazados.

[9] http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx
http://www.openspf.org/

DKIM(Domain Keys Identified Mail[10]).

Es un método de autenticación de correo, permitiendo a la persona que recibe verificar que el correo proviene de quien debe venir y que no ha sido alterado en el camino. Esto se logra aplicando técnicas criptográficas, por lo que una llave pública es incluida en cada mensaje a manera de firma misma que se calcula con el encabezado y cuerpo del mensaje. Cuando llega del lado receptor se vuelve a calcular la firma con el encabezado y el cuerpo y es comparada con la llave que incluye el mensaje. Si ambos valores coinciden se habrá comprobado que el mensaje no fue alterado en tránsito.

Sistemas de reputación.

Son sistemas automatizados de análisis de comportamiento de las direcciones que envían correo electrónico. Estos utilizan sensores colocados en diferentes partes del mundo a fin de ver el tráfico de correo de internet. Cuando una IP es vista se lleva un registro de su actividad (tráfico de correo, contenido de mensajes, segmento de red al que pertenece, variaciones en la cantidad de mensajes que se envían) esto con el objetivo de determinar si su conducta se muestra como confiable o no. Por lo regular los sistemas de reputación asignan una calificación misma que será utilizada por las herramientas de seguridad para aceptar o rechazar el mensaje.

Diccionarios y filtrado de contenido.

Son listas en las que se agregan palabras, frases, expresiones regulares o URL's con el objetivo de determinar el contenido permitido para la organización, evitando que se reciban o envíen mensajes inapropiados para el trabajo o aquellos que provoquen robo de información, espionaje, correo comercial, pornografía, entre otros.

Análisis de encabezado.

Es el análisis que se realiza a los encabezados del mensaje para determinar si cumplen con las recomendaciones establecidas por los estándares RFC 821 y 822 que son los que establecen el funcionamiento de SMTP. Este tipo de análisis también puede ubicar encabezados adheridos por aplicaciones externas, así como el contenido de las diferentes etiquetas del encabezado como el mail from, rcpt to, Delivered, Subject, entre otras.

Sistemas automáticos de detección basada en el comportamiento.

También se pueden aplicar sistemas automáticos que detecten en base a reglas de comportamiento las direcciones IP y el tipo de mensajes que pudieran ser de atacantes o remitentes de correo no solicitado e incluirlas en listas de negación temporal de manera que se apliquen políticas cuando se cumplan estas reglas. Por

[10] http://www.dkim.org/

ejemplo, se podría tener una regla que si se recibe un correo con el mismo subject un número determinado de veces en un periodo de tiempo, el correo sea desechado ó que si se reciben correos detectados como spam desde una misma dirección IP un número determinado de veces en un periodo la IP sea colocada en una lista de negación.

Listas negras.

Las listas negras son repositorios en los que se almacenan direcciones de correo electrónico, direcciones IP y dominios que no queremos recibir en nuestro servidor de correo. Cuando se detecte un correo proveniente de una dirección de la lista, éste será desechado.

4.1.3.1.2. Definición de objetivos.

El objetivo de una herramienta de seguridad correo es proteger al servicio ataques externos e internos, así como que el procesamiento de mensajes se reduzca para quitar carga de trabajo al servidor y que el usuario incremente su productividad al evitar recibir contenido inapropiado o inservible a su trabajo, además de asegurar la integridad de la información que se recibe, la disponibilidad del servicio y la confidencialidad de los datos manejados por la empresa al poder aplicar políticas corporativas que eviten el espionaje empresarial o robo de información.

4.1.3.1.3. Definición de requerimientos y plataformas.

Se deben presentar los esquemas de red actuales en los que funciona el servidor de correo electrónico, así como el sistema operativo donde está el servicio, fabricante o tipo de servidor de correo, si cuenta con LDAP (Directorio Activo), número de usuarios, cantidad de correos enviados y recibidos por hora, hora y número de mensajes pico, listas negras y blancas(si las tienen), así como también definir si tienen alguna necesidad adicional para verificar que sea viable realizarse con el producto propuesto.

4.1.3.1.4. Evaluación.

Se definen fechas para efectuar la evaluación del producto con el cliente y se propone esquema de evaluación. Si el cliente acepta la demostración, se asigna equipo y se tramitan licencias con el fabricante. La solución puede ser implementada en entorno operativo o en entorno de pruebas, lo recomendable es colocarla en producción para poder medir la efectividad.

4.1.3.1.5. Seguimiento a la evaluación.

Se mantiene comunicación constante con el cliente durante el periodo de pruebas a fin de determinar errores, realizar cambios en configuración y detectar necesidades adicionales del cliente a fin de sacar mayor provecho posible a la herramienta.

4.1.3.1.6. Obtención de resultados.

Durante y al término del periodo de pruebas, se generan reportes para poder justificar la adquisición del producto. Estos reportes también permiten al área de ventas dimensionar el tamaño de la solución que se le ofrecerá como parte de la propuesta económica.

4.1.3.1.7. Proceso de venta (Entrega de resultados al cliente y cierre).

Se entregan reportes al cliente y se genera propuesta económica, si el cliente acepta se adquiere el equipo nuevo y mientras nos es entregado, puede seguir con el de evaluación. Si no es adquirido el proceso finaliza y se recoge la solución.

4.1.3.1.8. Definición de la administración y operación.

Si se adquirió el equipo, se definirán el personal que estará a cargo de administrarlo y configurarlo, así como de mantener la comunicación con soporte durante la fase inicial de puesta a punto.

4.1.3.1.9. Implementación.

Se determinan fechas y metodología de implementación. Generalmente el equipo nuevo es configurado antes de colocarse en el sitio del cliente y esto se realiza por medio del respaldo proveniente de la evaluación. Así que al final solo se tiene que interrumpir el servicio unos segundos en lo que se hace el cambio hacia el nuevo dispositivo.

4.1.3.1.10.Capacitación y concientización.

Se ofrece una capacitación “hands on” para que el cliente se familiarice con las configuraciones de la herramienta, sin embargo se imparten cursos más extensos para poder llevar a cabo una administración completa de la solución.
Se debe por parte del cliente, indicar a sus usuarios los métodos que tendrán a su disposición para saber las acciones que se tomaron para los correos maliciosos y si podrán recuperar los mismos (si es viable).

4.1.3.1.11.Seguimiento.

Monitorear la solución periódicamente es completamente necesario para el seguimiento que se requiere en este tipo de soluciones, ya que nos permitirá descartar fallas o realizar cambios necesarios no contemplados en la configuración inicial, así como atender requerimientos adicionales por parte del cliente.

4.2. CURSOS DE ACTUALIZACIÓN.

Para poder realizar una recomendación referente a cualquier solución de las que se comercializan por medio de la empresa, se requiere conocerla detalladamente. Para tal efecto, debí tomar cursos de capacitación de estas herramientas.

Fortinet®/Fortigate.
Duración: 20 hrs.
Objetivo: Administrar, configurar e implementar el firewall Fortigate v.2.8

SecureComputing®/Ironmail.
Duración: 40 hrs.
Objetivo: Administrar, configurar e implementar solución de seguridad de correo electrónico Ironmail v. 4.5

TrendMicro®/OfficeScan v.8.0
Duración: 8 hrs.
Objetivo: Instalar y configurar solución antivirus TrendMicro OfficeScan v.8.0

Facetime ® /RealTimeGuardian
Duración: 20 hrs.
Objetivo: Administrar, configurar e implementar solución de monitoreo de aplicaciones no deseadas FaceTime RealTimeGuardian.

Tipping Point ®/X505/IPS
Duración: 40 hrs.
Objetivo: Administrar, configurar e implementar solución TippingPoint que incluye Firewall X505 e IPS

En mi experiencia profesional desarrollando este tipo de proyectos he podido aprender conceptos muy específicos de la seguridad informática que me han permitido entender cualquier solución referente a las que mencioné. Ahora me es muy fácil manejar herramientas con características similares debido a que la base para el desarrollo de las mismas es aquella que ya se presentó en este capítulo. Es por ello que a los clientes se les debe concientizar respecto a sus vulnerabilidades y amenazas para poder ofrecerle la solución que pueda proveerle la seguridad necesaria para dar continuidad a la operación.

CONCLUSIONES.

CONCLUSIONES

Desde mi ingreso a la empresa, he trabajado con soluciones que me han demandado conocimientos teóricos de redes, seguridad informática, sistemas operativos, administración de equipos y redes, entre otros, mismos que me han servido para poder implementar los mejores esquemas que nos demanden poco esfuerzo, sin perder de vista lo fundamental: la satisfacción de los clientes.

El soporte técnico es básico para cualquier organización, ya que en gran medida depende de este departamento el éxito o el fracaso de cualquier herramienta informática; al ser el responsable de orientar al cliente de manera que pueda lograr los objetivos propuestos por el proyecto. Se presentó en este trabajo una visión general del Departamento de Soporte Técnico de la empresa y sus actividades.

También se comentó respecto a la administración de la infraestructura tecnológica que me ha permitido implementar esquemas de seguridad dentro de la organización como el firewall y el servidor de seguridad para el e-mail, así como conocer la forma de administrar todos los servicios que se ofrecen como son el DNS y el Correo Electrónico.

Expliqué acerca de los proyectos en los que me he involucrado y la metodología de trabajo para poder llevar a cabo de manera satisfactoria la recomendación de una solución, así como posteriormente el éxito logrado durante la implementación, de forma que estas herramientas ayuden a los clientes en el objetivo principal que ya hemos comentado que es: el aseguramiento de sus recursos tecnológicos y por lo tanto de su información.

Como conclusión considero que el trabajo desempeñado durante estos últimos cinco años se ha desarrollado en un esquema de atención a clientes, mismo que he tenido que llevar a cabo investigando su necesidad para poder ofrecerle una solución que se adapte a su esquema operativo y que obtenga con ello, el mejor costo-beneficio.

En cualquier empleo en el que nos encontremos siempre estaremos enfocados a atender clientes, mismos que pueden ser de distintos tipos, pero al final, en cualquier entorno en el que desarrollemos nuestro trabajo tendremos que

garantizar que el cliente esté satisfecho con lo que le ofrecemos; ya sea productos, servicios ó capacitación.

Es por lo anterior que siempre he intentado entender al cliente en sus requerimientos de manera que podamos ofrecer el mejor servicio y que por consiguiente esté contento en la forma que recibe la atención y solución a sus problemas.

La responsabilidad es otro aspecto importante que he aprendido en materia profesional, ya que es por medio de este valor que las personas que tienen a cargo el timón de la organización aprenden a respetar tu trabajo, debido a que te comprometes a hacerlo de la mejor forma posible y eso se puede observar en la preferencia que tienen los clientes hacia la empresa más que nada por la atención.

La actualización constante debe ser menester, porque en materia de tecnología siempre estaremos un paso atrás por el avance tan rápido que se ha observado en los últimos años, por lo que debemos conocer lo nuevo para poder ofrecerlo como solución y estar preparado para la aplicación de estos conocimientos.

Tengo claro que la escuela no te enseña a trabajar, pero te da las herramientas para encontrar el camino: trabajo en equipo, metodología de investigación, aprendizaje de conceptos y métodos. Todo esto en su conjunto aplicado al mercado laboral, es lo que se necesita para poder emprender una carrera exitosa, en donde necesitas estar preparado para poder competir.

El camino recorrido ha sido muy gratificante para mí, ya que he podido aplicar lo aprendido en mi paso por la escuela, pero también he ampliado mi instrucción lo que me ha permitido aplicar la solución a los problemas con los que me he enfrentado, ya sea con los clientes o como administrador de la infraestructura propia.

GLOSARIO DE TÉRMINOS.

DHCP: Dynamic Host Configuration Protocol, es un protocolo de red que permite que los nodos de una red IP obtengan los parámetros de configuración automáticamente.

END POINT: Punto Final, termino utilizado para especificar a las aplicaciones que se ejecutan en las estaciones de trabajo de los usuarios.

HANDS ON: "Manos en", termino utilizado para indicar que se desarrolla una enseñanza práctica. Ejemplo: Mientras se configura un producto se visualizan las opciones principales para posteriormente conocer donde se pueden modificar.

IPS: Intrusion Prevention System, Sistema de Prevención de Intrusos, termino empleado para designar a las herramientas que mediante firmas o detección de anomalías de tráfico pueden detectar y detener ataques e intrusiones.

IPSEC: Conjunto de protocolos que tienen como objetivo asegurar las comunicaciones sobre el protocolo de internet mediante técnicas de autenticación y cifrado.

LDAP: Lightweight Directory Access Protocol, Protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. Es considerado una base de datos a la que pueden realizarse consultas y almacena generalmente datos de los usuarios como login y password.

MAC Address: Direcciones MAC. Media Access Control Address: Dirección Física y única de las tarjetas e interfaces de red que consta de 48 bits y está configurada por el IEEE (últimos 24 bits) y por el fabricante del dispositivo (primeros 24 bits). Esta dirección viene grabada de forma binaria en cada dispositivo en el momento de su fabricación y se representa por un conjunto de 6 octetos en hexadecimal.

NIC: Network Information Center organización encargada de la administración del nombre de dominio territorial, es decir, para cada región existe un NIC que administra los nombres de los dominios en Internet (.mx, .br, .uk, etc.).

PHISHING: Termino relativo a la palabra "Fishing" que significa "pescando" y que es utilizado para referirse a las personas que se dedican a "pescar" usuarios mediante métodos de suplantación de identidad, indicándoles que tienen que realizar alguna actividad que pudiera representar algún beneficio para el atacante, por ejemplo, que el usuario proporcione su número de cuenta y claves de acceso del banco o usuario y password de su correo electrónico. Con la información

recopilada, el atacante puede robar dinero del usuario o robo de información personal que seguramente será utilizada en perjuicio del mismo.

PIN: Personal Identification Number, Número de Identificación Personal utilizado en cajeros automáticos o para realizar transacciones bancarias por teléfono o Internet.

PPTP: Point to Point Tunneling Protocol, Protocolo utilizado para implementar Redes Privadas Virtuales o VPN, actualmente no es de los más utilizados debido a que su seguridad ha sido completamente rota y existen herramientas capaces de descifrar el tráfico de la VPN.

RELAY: Acción disponible en cualquier servidor de correo electrónico y que consiste en permitir a los usuarios transmitir correos electrónicos a otros servidores de correo en Internet.

REGISTRO MX, A Y CNAME: En un DNS (Sistema de Nombres de Dominio), son los que definen el tipo de dirección que se está resolviendo. MX es el que se encarga de definir el Intercambio de Correo (Mail Exchanger), es decir, a donde serán entregados los correos para el dominio en cuestión. A es el registro de dirección, es decir un nombre asociado a una IP y CNAME es el nombre canónico o alias de un nombre existente.

RFC: Request For Comments. Serie de notas sobre internet en el que se detallan las especificaciones sobre los protocolos de internet para ser interpretado sin ambigüedades.

SMTP HELO: Comando del protocolo de SMTP que es la abreviatura de “hello” con el cual el cliente se identifica ante el servidor, con esto se conoce si se logró la conexión.

SUBJECT: Asunto del mensaje, parte del encabezado del mensaje de correo que indica el tópico del correo electrónico.

URL: Uniform Resource Locator, Localizador Uniforme de Recursos, Secuencia de caracteres de acuerdo a un formato estándar utilizado para nombrar recursos como documentos e imágenes por su localización en internet. Esta secuencia contiene protocolo a usar para visualizar el documento, máquina donde se encuentra, directorio y nombre del archivo.

UTM: Unified Threat Management, Administración Unificada de Amenazas; Término empleado para definir a los Sistemas que poseen varias aplicaciones dedicadas a detectar diferentes tipos de amenazas como son Ataques, Intrusos, Virus, Spam y Filtrado de contenido en un solo producto.

WEBMAIL: Cliente de correo electrónico accesible por medio de una página Web. Por ejemplo: Hotmail, Yahoo, etc.

BIBLIOGRAFÍA.

Sophos Plc. *"Viruses and spam: What you need to know"*. Reino Unido, Ed. por Paul Oldfield, 2004.

Sophos Plc. *"Virus informáticos al descubierto"*. Reino Unido, Ed. por Paul Oldfield, Tr. Javier Acebes, 2002.

Chapman, Brent. Zwicky, Elizabeth. *"Construya Firewalls para Internet".* México, McGraw Hill, 1997

OTRAS REFERENCIAS.

www.ssisa.biz

www.isw.com.mx

www.securecomputing.com

www.fortinet.com

www.juniper.com

www.sophos.com

http://www.segu-info.com.ar/ataques/ataques.htm

http://www.segu-info.com.ar/firewall/firewall.htm

http://www.practicallynetworked.com/sharing/firewall.htm

http://www.juniper.net/products/integrated/stateful_inspection_firewall.pdf

http://www.securityfocus.com/infocus/1716

http://cbl.abuseat.org/nat.html

http://www.dkim.org/

http://www.openspf.org/

http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx

http://www.ietf.org/rfc/rfc2821.txt

http://www.ietf.org/rfc/rfc2822.txt