UNIVERSIDAD TECNOLOGICA ISRAEL

CARRERAS DE SISTEMAS INFORMATICOS

ESTUDIO DE LA INTEGRACIÓN SOBRE LAS SEGURIDADES EN INTERNET PARA SERVIDORES AS/400.

AUTOR:

Freddy Medardo Vargas Salinas

TUTOR:

Ing. Mario Mejía

Quito - Ecuador

2013

UNIVERSIDAD TECNOLÓGICA ISRAEL

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Graduación certifico:

Que el Trabajo de Graduación "ESTUDIO DE LA INTEGRACIÓN SOBRE LAS SEGURIDADES EN INTERNET PARA SERVIDORES AS/400.", presentado por Freddy Medardo Vargas Salinas, estudiante de la carrera de Sistemas Informáticos, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del Tribunal de Grado, que se designe, para su correspondiente estudio y calificación.

Quito, enero 2013

TUTOR

Ing. Mario Mejía

C.C. 170658885-0

UNIVERSIDAD TECNOLÓGICA ISRAEL

AUTORÍA DE TESIS

El abajo firmante, en calidad de estudiante de la Carrera de Sistemas Informáticos declaro que los contenidos de este Trabajo de Graduación, requisito previo a la obtención del Grado de Ingeniero en Sistemas Informáticos, son absolutamente originales, auténticos y de exclusiva responsabilidad legal y académica del autor.

Quito, enero del 2013

Freddy Medardo Vargas Salinas

CC: 010476367-7

DEDICATORIA

La presente tesis le dedico a mi Dios y Padre quien por su gran amor me da todas las bendiciones que hoy tengo en mi vida, a mis padres el Sr. Ángel Vargas y la Sra. Mercedes Salinas quienes me han apoyado incondicionalmente y me han sabido guiar incansablemente para alcanzar esta meta importante para mi vida; a mis hermanos, amigos

Hay que pensar que en este momento el sacrificio ha dado buenos resultados ya que las cosas nos han resultado bien y agradecer a la institución que nos ha brindado un poco de apoyo al realizar la culminación de nuestra vida universitaria.

AGRADECIMIENTO

Agradezco de manera especial a mi Dios por todas las cosas que me ha enseñado en el camino de mi vida y porque nunca me ha soltado de su mano; agradezco a mis Padres porque nunca me han faltado sus muestras de cariño y apoyo a quienes los guardaré siempre en el corazón,

Un agradecimiento especial para la institución que nos ha enseñado a realizar nuestras tareas y proyectos para poder terminar nuestros estudios, ya que con las bases nos han ayudado a tener la capacidad de desenvolvernos de una manera apropiada para realizar un buen proyecto de tesis.

RESUMEN

El tema propuesto para el desarrollo de nuestrotrabajo de graduación está relacionado sobre las seguridades en internet para servidores AS/400. En el cual se propuso como objetivos específicos la recopilación de información sobre la planificación de seguridades en Internet para equipos (As/400), los niveles de seguridad para la disponibilidad básica de Internet en equipos iSeries o (AS/400) y las opciones de seguridad de la red para equipos iSeries o (AS/400). A más de documentar la configuración de TCP/IP para dichos equipos la cual facilitara el momento de brindar acceso a la red (Internet) a nuestra empresa u organización.

SUMMARY

The theme proposed for the development of our work is related graduation on internet assurances AS/400 server. In which specific objectives proposed collection of information on the Internet assurances planning for equipment (AS/400) security levels for basic Internet availability in teams or iSeries (AS/400) and options network security equipment or iSeries (AS/400). In addition to documenting the TCP / IP for the equipment which provide the time to provide access to the network (Internet) to our company or organization.

TABLA DE CONTENIDO.

TABLA DE CONTENIDO DE FIGURAS.

CONTENIDO DE TABLAS Y MAPA CONCEPTUAL.

CONTENIDO DE ANEXOS

CAPÍTULO 1

1. Introducción

Para realizar el estudio de la integración sobre las seguridades en Internet para servidores As/400, lo primero habrá que puntualizar que el presente trabajo trata de aportar una investigación sobre la planificación de las seguridades en internet para los servidores AS/400, una breve explicación sobre los niveles de seguridad que nos brinda estos equipos, explicar alguna opciones de seguridad y documentar los pasos para la configuración de TCP/IP en servidores AS/400.

Así que, el presente proyecto investigativo, tiene por objeto orientar sobre una buena integración de seguridades en internet para servidores AS/400, que deberían ser tomados en cuenta, por el área o persona responsable de la misma, para así mejorar las seguridad para estos equipos, la cual, realmente prevenga los riesgos de pérdida o alteración de la información.

Un buen documento informativo implica que sea entendible, amigable y fácil de manipular para las personas que estén interesados en el tema, por esto se pretende realizar dicho documento sobre las seguridades en internet para equipos iSeries.

Al desarrollar este trabajo se pretende realizar un documento para usuarios que trabajen con servidores iSeries, capacitando de una manera sencilla y entendible sobre las seguridades en internet para estos equipos, de esta manera se brinda conocimiento para que puedan prevenir la intromisión de terceras personas a la información de la empresa manteniendo una red segura.

1.1. Antecedentes

Hoy en día las empresas han optado por servidores para un mejor manejo de sus actividades y así provee de servicios a otras computadoras denominadas clientes, y la alta disponibilidad de recursos se ha vuelto muy importante en las diferentes organizaciones.

En nuestro medio hoy en día las empresas necesitan un nivel alto de disponibilidad de información y los equipos iSeries es una salida para lograr con esto porque es un servidor de proceso que entrega información y es muy seguro.

El documento que realizaremos tendrá la finalidad de brindar información a los usuarios sobre las consideraciones principales en la planificación de las seguridades que tendrán que tomar al momento de dar acceso a una empresa u organización en el servicio de Internet.

1.2. Formulación del Problema

¿Con la planificación de las seguridades en internet para servidores AS/400 y teniendo en cuenta los niveles y opciones de seguridad investigadas, permitirá a los usuarios tomar decisiones con respecto a las seguridades de estos equipos?

1.3. Sistematización

1.3.1. Análisis FODA

FACTORES INTERNOS	FACTORES EXTERNOS
Fortalezas	**Oportunidades**
- Seguridad de la información en la internet - Profesionalismo del personal	- Disponibilidad de información - Acceso a usuarios con permisos
Debilidades	**Amenazas**
- Falta de profesionales capacitados en la rama. - Falta de una guía adecuada para los usuarios. - Inversión costosa	- Fraude informático - Infección con Virus - Intrusión de Hackers

ANALISIS DEL ENTORNO FODA

El FODA constituye una herramienta muy importante ya que ayuda a establecer los factores positivos y negativos del entorno interno y externo dentro del mercado, adicionalmente permite procesar dicha información obtenida para poder tomar decisiones que serán las estrategias que permitirán determinar que el presente estudio sea viable y sostenible.

FORTALEZAS

- Presentar una guía para usuarios a cerca de las seguridades en internet para servidores iSeries.
- Difundir a los usuarios la importancia de mejorar la seguridad de la información que maneja una determinada empresa.

- Permitir a una empresa conocer sobre las herramientas existentes para salvaguardar la información con una adecuada seguridad.
- Facilitar a los profesionales interesados en el tema un documento para profundizar sus conocimientos sobre la planificación de las seguridades en internet para equipos AS/400.

DEBILIDADES

- La implementación de un servidor AS/400 iSeries implica una inversión un tanto costosa.
- Falta de profesionales a nivel local capacitados y dedicados en la implementación de este tipo de servidores iSeries.
- Falta de información concisa y adecuada a cerca de la planificación de las seguridades en internet.

OPORTUNIDADES

- Concientizar a las empresas sobre la importancia de mantener su red e información aseguradas.
- Dar a conocer sobre la importancia de contar con un servidor de seguridad ya que este permitirá el acceso solo a usuarios que estén registrados en el sistema.
- Generar una oportunidad de negocio profesional asesorando a las empresas sobre la importancia de una adecuada planificación de las seguridades en internet para equipos AS/400.

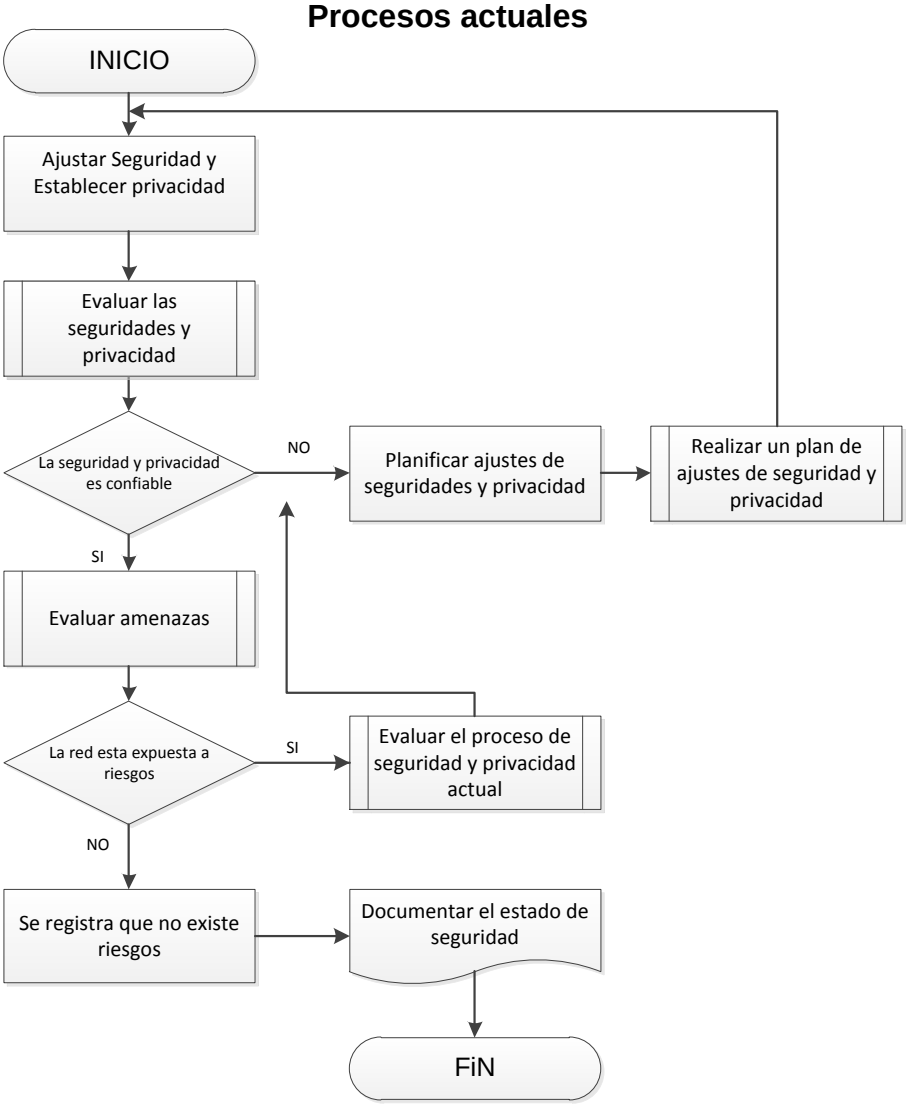
AMENAZAS

- La mayoría de empresas no destinan el suficiente presupuesto para lograr una buena seguridad en internet para este tipo de servidores.
- Sin una adecuada seguridad de la información una empresa está expuesta a un fraude informático.
- Un nivel de seguridad adecuado impedirá que la información que maneja una empresa sea blanca de infecciones con virus.
- Una inadecuada seguridad en la red de una empresa permitirá la intrusión de Hackers poniendo en manos fraudulentas la información de los clientes.

1.3.2. Diagnóstico.

- En la actualidad en la ciudad de Cuenca en la empresa de Etapa no cuentan con personal suficiente que tengan un conocimiento sobre las seguridades en internet con servidores iSeries.
- El no mantener una buena planificación sobre seguridades en internet para equipos iSeries no nos garantiza la integridad de los datos de la empresa.
- Falta de información a cerca de una buena planificación de las seguridades en internet para servidores AS/400.
- No toman en consideración los niveles de seguridad en internet para servidores AS/400.
- Poco interés sobre las opciones de seguridad de la red para equipos iSeries.

Procesos actuales



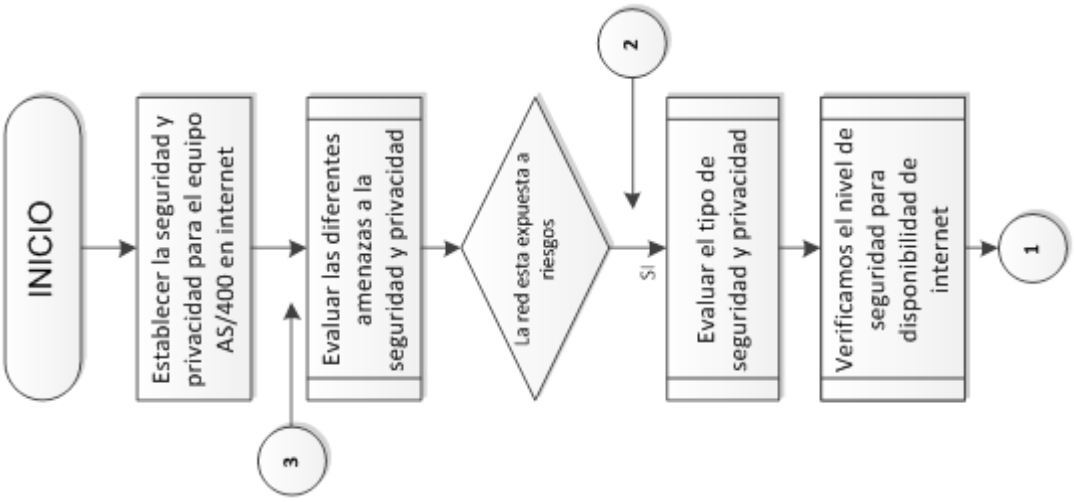
1.3.3. Pronóstico.

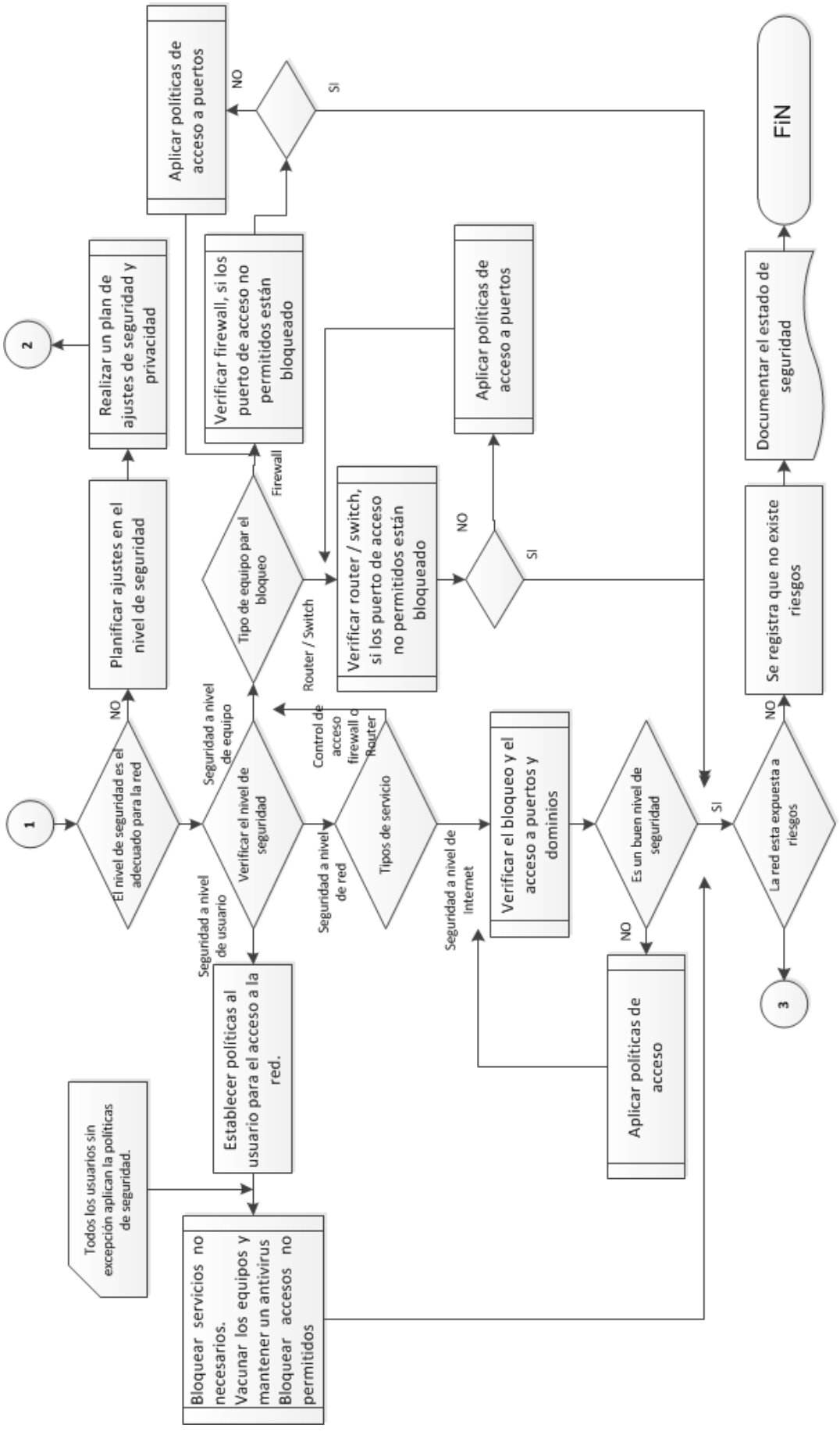
- Al no contar con el conocimiento suficiente las personas que están encargadas de estos servidores no podrán realizar un trabajo óptimo para así eliminar inconvenientes y los problemas que se presenten en la seguridad en internet.
- De no contar con una buena planificación de seguridad en internet para servidores iSeries cualquier persona hackers podría intervenir en nuestra red y manipular información muy importante de nuestra organización o empresa que disponga de estos equipos.
- El no contar con una información buena sobre las seguridades en internet, no se podría mantener segura la red y datos de los servidores AS/400.
- Al no contar con un buen nivel de seguridad la información que este en el servidor se ara vulnerable a ser infectados con virus.

1.3.4. Control del Pronóstico.

Para solucionar este problema se recomienda tener en cuenta el contenido de este proyecto que tiene como fin ser una guía del usuario para brindar información acerca de las seguridades en internet para servidores iSeries.

Teniendo en cuenta la investigación sobre la planificación de las seguridades en internet para equipos AS/400, los diferentes niveles de seguridad para una buena disponibilidad básica de internet en estos servidores y lo investigado sobre las opciones de seguridad de la red para equipos iSeries.




1
El nivel de seguridad es el adecuado para la red
NO
Planificar ajustes en el nivel de seguridad
Realizar un plan de ajustes de seguridad y privacidad
2
Seguridad a nivel de usuario
Verificar el nivel de seguridad
Seguridad a nivel de equipo
Tipo de equipo par el bloqueo
Firewall
Verificar firewall, si los puerto de acceso no permitidos están bloqueado
Aplicar políticas de acceso a puertos
NO
SI
Router / Switch
Verificar router / switch, si los puerto de acceso no permitidos están bloqueado
Aplicar políticas de acceso a puertos
NO
SI
Seguridad a nivel de red
Tipos de servicio
Control de acceso firewall o Router
Seguridad a nivel de Internet
Verificar el bloqueo y el acceso a puertos y dominios
Es un buen nivel de seguridad
NO
SI
La red esta expuesta a riesgos
NO
Se registra que no existe riesgos
Documentar el estado de seguridad
FIN
3
Establecer políticas al usuario para el acceso a la red.
Aplicar políticas de acceso
Todos los usuarios sin excepción aplican la políticas de seguridad.
Bloquear servicios no necesarios.
Vacunar los equipos y mantener un antivirus
Bloquear accesos no permitidos

1.4. Objetivos

1.4.1. Objetivo General

Elaborar un documento sobre la integración de las seguridades en internet para equipos As/400 “iSeries”.

1.4.2. Objetivos Específicos

- Investigar la planificación de las seguridades en internet para equipos iSeries, con el fin de brindar información a las personas interesadas sobre esta temática.
- Explicar los diferentes niveles de seguridad para la disponibilidad básica de internet en equipos iSeries.
- Investigar las opciones de seguridad de la red para equipos iSeries, con el fin de que las personas se informen el cómo salvaguardar la información de la empresa.

1.5. Justificación

Con el desarrollo de este módulo se pretende capacitar y ampliar los conocimientos tanto a las personas que tengan conocimiento como a las que no la tengan sobre la planificación de seguridades en internet para servidores iSeries, de una manera fácil y concisa.

1.5.1. Justificación Teórica

Con este proyecto de investigación de las seguridades en internet para quipos iSeries, se pretende brindar información a personas para un mejor rendimiento y para mantener una mejor disponibilidad de la información en una forma segura.

Cabe destacar que con este proyecto se quiere llegar a personas que estén interesadas para que así puedan informarse el cómo mantener una buena seguridad en internet para servidores iSeries, salvaguardando la información y protegiendo la integridad de la misma.

1.5.2. Justificación Práctica

Con el desarrollo de esta temática podemos percibir notables cambios a nivel de seguridad de los recursos de la empresa en servidores iSeries.

Desde esta perspectiva las organizaciones deben implementar seguridades en el internet para mantener la información de una forma segura y disponible para las diferentes actividades que se realizan en las empresas.

Un contexto global muestra cambios notables en cuanto a seguridades en internet para equipos AS/400, lo cual esto permite tener una mayor competitividad a empresas que trabajan con estos servidores. Es por esto que se realiza el estudio de la integración sobre las seguridades en internet para servidores AS/400.

1.5.3. Justificación Metodológica

El método de investigación para el desarrollo de este proyecto será el deductivo ya que con esta temática se pretende brindar información útil sobre las seguridades en internet para equipos iSeries, para mantener una red segura en las organizaciones salvaguardando la información.

1.6. Alcance y Limitaciones

1.6.1. Alcance

El proyecto a realizar pretende ser una guía amigable y fácil de manipular por parte de los usuarios, la cual permitirá realizar consultas sobre la planificación de las seguridades que se deben tener en el acceso a Internet, los niveles de seguridad para la disponibilidad básica de internet y las opciones de seguridad de la red. Para esto se empleara:

- Un método totalmente investigativo el cual se realizara en español, el mismo se pretenderá publicar en sitios gratuitos de Internet como lo es (blog y redes sociales), para que cualquier usuario pueda tomar como guía este módulo, realizando consultas.

1.6.2. Limitaciones

Con este trabajo de investigación se pretende realizar una guía de la integración de las seguridades para servidores iSeries, lo cual va a ser detallado en los capítulos siguientes.

En el marco de referencias (Capitulo II) se dará a conocer el contenido teórico del presente trabajo tomando en cuenta conceptos relacionados con la temática y en

el desarrollo (Capitulo III) se dará a conocer la planificación de la seguridad en Internet para iSeries, detallando paso a paso los puntos a tomar en cuenta para la planificación de la misma, con lo que se pretende lograr un documento entregable y tendrá un sustento teórico por lo que no se realizara la implementación a la hora de la sustentación.

1.7. Estudios de Factibilidad

1.7.1. Técnica

El proyecto de investigación es variable ya que se utilizaran aspectos tecnológicos, el internet, la PC y humanos para llegar a la culminación del mismo.

1.7.2. Operativa

El presente trabajo de graduación tiene un fin; realizar un documento que provea una alta disponibilidad de información para los usuarios, capacitando así a las personas para mejorar la planificación de seguridad en internet para servidores iSeries.

1.7.3. Económica

En este punto se detallara de forma breve los factores económicos necesarios para el desarrollo de este proyecto que es un aproximado de 259,90 $ dólares lo cual se detallara brevemente a continuación:

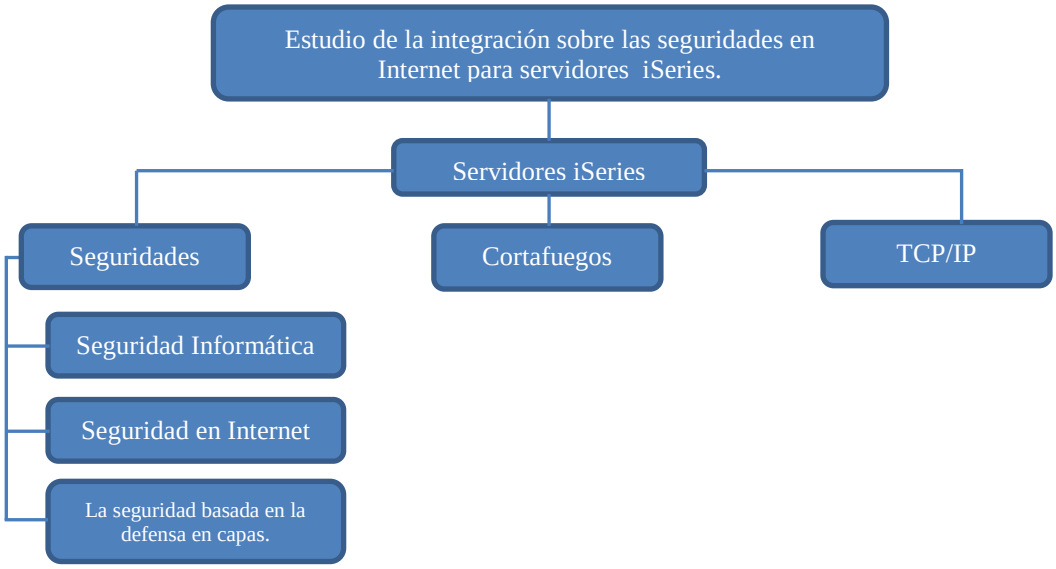
	Septiembre				Octubre				Noviembre				Diciembre				Total
	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	
Internet		5	5	6	5	4,5	6	7	6	5	5						54,5
Impresiones		2	2,5	3	3	2	1	4,4	1	5	5						28,9
Copias		1	1	1,5	1	0	2	0	1	2	2						11,5
Transporte		7	7	7	6	6,5	7	6	7	6	7						66,5
Extras		12	12	8,5	10	10	9	9	9	10	9						98,5
																	259,9

Tabla #1.
Autor: Freddy Vargas.
Gastos Económicos

CAPÍTULO 2

2. Marco de referencia

2.1. Marco Teórico



Mapa Conceptual #1.
Autor: Freddy Vargas
Teorías.

2.1.1. Introducción

En el marco teórico detallado en el Capítulo II se dará a conocer el contenido teórico del presente trabajo tomando en cuenta conceptos relacionados con el tema, para así entender de mejor manera la planificación de las seguridades en internet que se debe tomar en cuenta utilizando equipos iSeries o (AS/400).

Los servidores AS/400 actualmente también conocidos como iSeries, es un servidor de gama media y alta diseñado para empresas pequeñas y departamentos de grandes empresas y ahora rediseñado para que funcione bien en redes distribuidas con aplicaciones Web. Es un sistema integrado de software, hardware, base de datos y seguridades. Estos equipos son muy seguros ya que poseen un sistema operativo propio llamado OS/400 el cual está basado en objeto y bibliotecas, probablemente es el más robusto y bien integrado de todos los actuales y pasados OS, soporta otros sistemas operativos tales como GNU/Linux,

AIX o incluso Windows en una placa Intel integrada, soportando también de forma nativa múltiples aplicaciones antes reservadas a Windows.

Los servidores AS/400 utilizan un microprocesador PowerPC, con múltiples terabytes de almacenamiento en disco y una memoria virtual de Java estrechamente ligado al sistema operativo de IBM OS/400, estos servidores son muy versátiles que puede sustituir a los servidores de PC y servidores web en los negocios del mundo, compitiendo tanto con Wintel y servidores UNIX, al tiempo que su base de cliente presente un enorme salto inmediato en la Internet.

2.2. Marco Conceptual

Servidores iSeries:

"El sistema AS/400 es un equipo de IBM de gama media y alta, para todo tipo de empresas y grandes departamentos.

Se trata de un sistema multiusuario, con una interfaz controlada mediante menús y comandos CL (Control Language) intuitivos que utiliza terminales y un sistema operativo basado en objetos y bibliotecas, denominado OS/400. Un punto fuerte del OS/400 es su integración con la base de datos DB2/400, siendo los objetos del sistema miembros de la citada base de datos. Ésta también da soporte para los datos de las aplicaciones, dando como resultado un sistema integrado potente y estable. Actualmente, con la denominación IBM i, anteriormente conocida como System i e iSeries, soporta otros sistemas operativos tales como GNU/Linux, AIX o incluso Windows en una placa Intel integrada, soportando también de forma nativa múltiples aplicaciones antes reservadas a Windows."[1]

- **Seguridad Informática:**

"Son todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

[1] **http://es.wikipedia.org/wiki/as400_inform%C3%A1tica**

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos"[2]

- **Seguridad en Internet**

Al hablar de seguridades en internet nos estamos refiriendo a un tema cuya importancia va en aumento de acuerdo al valor y la accesibilidad que va tomando las transacciones en la red. Frente a esto, la necesidad a que las seguridades en el internet sean forzadas se incrementa.

La impresión de las Seguridades en Internet en la actualidad va tomando ajustes mucho más complejos y especializados. En la actualidad, se incluye servicios y estrategias para proteger de una mejor manera la integridad de los datos. Y para salvaguardar el intercambio de datos cada vez va surgiendo mejor instrumentos y más precisos que facilitan seguridad en toda la red salvaguardando los servidores con acceso a Internet y a redes privadas.

Además se puede decir que, el tema de las seguridades en Internet se ha convertido en un asunto importante para las empresas que realizan actividades de transmitir información confidencial en la "nube". Y de estas organizaciones depende la confianza de las visitas a su sitio web ya que los consumidores se resisten a facilitar fácilmente datos personales, como son los; números de tarjetas de crédito, contraseñas o cualquier información confidencial por la duda a que manipulen y que sea interceptada con malas intenciones y los exponga a peligros como estafas o robo de identidad.

- **Cortafuegos**

Los cortafuegos son sistemas creados para prevenir el uso y acceso no autorizado desde o hasta una red privada con el fin de inmiscuirse a un ordenador para hacer uso inapropiado de la información.

Los cortafuegos o también conocidos como firewall en ingles pueden ser creados en software o hardware como también en una combinación de ambos. Estos tipos

[2] **http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica**

de sistemas se los utilizan con el fin de no permitir el acceso de usuarios no autorizados a redes privadas.

Los cortafuegos funcionan de la siguiente manera son los encargados de descifrar y examinar todos los mensajes que salen y entran desde y hasta la red privada, de esta manera si se encuentra con mensajes que no cumplen con los permisos de seguridad específicos los bloquea.

- **Planificación de las Seguridades en Internet Para Equipos iSeries.**

  Para la planificación se debe documentar los Siguientes Aspectos:

  1. La configuración de la red.
  2. Información de configuración del servidor de correo electrónico y DNS.
  3. La conexión con el proveedor de servicios de Internet (ISP).
  4. Qué servicios de Internet desea utilizar.
  5. Qué servicios desea proporcionar a los usuarios de Internet.

Con la documentación de esta información nos permitirá determinar de una mejor manera cuáles son los peligros a los que está expuesta la seguridad y cuáles serían las medidas necesarias a tomar para disminuirlas.

Seguridad Basada en la Defensa por Capas:

La estrategia por la cual se habla de seguridad es para detalla qué es lo que se espera resguardar y lo qué se espera de los usuarios del sistema. Nos presta una plataforma para crear una planificación excelente de la seguridad a la hora de crear nuevas aplicaciones o cuando se requiera ampliar la red actual. Detalla las distintas responsabilidades de la persona que esté a cargo de la red, como las de prevenir que la información sea confidencial en su totalidad y cuando creen contraseñas no sean fáciles de descifrar por intrusos.

Al realizar actividades empresariales que tengan acceso a internet lleva asociado grandes riesgos. Por esta razón al crear una política de seguridad, debe estar obligado a examinar el abastecimiento de servicios con el control del acceso a la red y los datos.

En los sistemas que están relacionados con la red, la seguridad es más ardua a causa de que el propio canal de comunicaciones está expuesto a los ataques. Así que; como los riesgos permitidos de Internet se pueden ocasionar en varios niveles, deberá disponer de medidas de seguridad que brinden múltiples capas de defensa frente a los riesgos las cuales son:

1. **Seguridad a Nivel de Sistema:** Configurar adecuadamente los valores básicos de seguridad del sistema iSeries.
2. **Seguridad a Nivel de Red**: Como ya se había hablado antes de los cortafuegos o firewall se dice que son los sistemas más comunes para garantizar la seguridad de la red. Conjuntamente con las seguridades que provee el ISP (Proveedor de Servicios Internet), así también como las reglas de filtrado de la conexión del direccionador y las previsiones del servicio de nombres de dominio (DNS) público.
3. **Seguridad a Nivel de Aplicaciones:** Debe configurar valores de seguridad para cada una de las aplicaciones que maneje.
4. **Seguridad a Nivel de Transmisión:** Configurar las aplicaciones para que utilicen SSL (capa de sockets segura).

Política y Objetivos de Seguridad: en el momento q se crea y desarrolla una política de seguridad, lo primero que se debe tener cuenta son los objetivos. Los objetivos de seguridad entran dentro de una o varias de estas categorías:

1. **Protección de Recursos:** Detallar con claridad las diferentes clases de usuarios que tengan el acceso al sistema y precisar el tipo de autorización de acceso que se desea permitir a dichos usuarios.
2. **Autenticación:** Establecer a los usuarios los niveles de permisos y contraseña.
3. **Autorización:** En este punto se fijar quienes puede acceder a la información o ejecutar determinadas actividades en los recursos del sistema.
4. **Integridad de los dato:** Para lograr una buena integridad de datos se podría utilizar un cortafuegos para limitar la entrada y

salida de la información y para mantener las seguridades de la tecnología IPV4 e IPV6 para prevenir que los datos no sean alterados.

5. **No Repudio:** Para soporte al no repudio podremos utilizar los certificados digitales y la criptografía de claves públicas para firmar transacciones, mensajes y documentos.
6. **Confidencialidad:** Al cifrar de los datos con capas de sockets segura (SSL) y certificados digitales le permitirán asegurar la confidencialidad al transmitir datos entre redes que no sean de confianza.
7. **Actividades de Seguridad de Auditoría:** El conocimiento de los objetivos de seguridad le ayudará a crear una política de seguridad que satisfaga todas sus necesidades de seguridad de Internet y de la red.

Niveles de Seguridad Para la Disponibilidad Básica de Internet En Equipos iSeries:

Para lograr una buena disponibilidad de internet para los servidores AS/400 se debe configurar adecuadamente los valores de la seguridad básica del i5/OS:

Se debe establecer el nivel de seguridad QSECURITY más adecuado. Se aconseja utilizar el nivel de seguridad 50 porque proporciona el máximo nivel de protección de la integridad datos, lo cual es recomendable para salvaguardar el sistema en entornos de alto riesgo como Internet.

1. Configurar los valores del sistema que estén relacionados con la seguridad para que estén al menos tan restringido como los valores recomendados.
2. Cerciorarse de que ninguno de los perfiles de usuario, ni siquiera los suministrados por IBM, tenga contraseñas por omisión. El mandato ANZDFTPWD (Analizar contraseñas por omisión).
3. Para proteger los recursos más importantes del sistema es recomendable utilizar la autorización sobre objeto.
4. Configurar la autorización sobre objeto en el sistema.

Opciones de Seguridad de la Red Para Equipos iSeries: Para conocer las medidas de seguridad más populares y las que se deben ajustar a nivel de red, se recomienda utilizar esta información y así podrá lograr proteger los recursos internos:

1. Para lograr una mejor protección de un equipo iSeries se puede optar por manejar un sistema cortafuego de funcionalidad completa o también poner en vigor tecnologías de seguridad de red determinadas como parte de la implementación TCP/IP del i5/OS. Esta implementación está formada por la característica de reglas de paquetes (que incluye el filtrado IP y la NAT) y la característica de servidor proxy HTTP para iSeries.

Análisis.

Para una buena planificación de seguridad en internet en necesario comenzar a vincular la empresa con servidor AS/400 (sistema de cómputo) con internet.

El sistema AS/400 típico existe en un ambiente seguro, con un conjunto de usuarios potenciales bien definido. Proporciona una entrada de seguridad (de inicio de sesión y contraseña) y el acceso relativamente abierto una vez que estás dentro. La mayoría de los archivos están disponibles para ser vistos por cualquier usuario que pueda iniciar sesión en el sistema.

Desde una perspectiva de seguridad, el AS/400 típico lo podríamos asemejar a un edificio. Las puertas y ventanas; están bloqueados. Los usuarios tienen una clave (password) para acceder. Dentro del edificio, la mayoría de las habitaciones tienen puertas que no están bloqueados. Algunas de las habitaciones, o cajones de archivos dentro de las habitaciones, tienen cerraduras que requieren claves para su autorización.

Al proporcionar acceso a su sistema a través de Internet, es posible de dejar muchos extranjeros de todo el mundo entrar en el sistema, o al menos mostrar documentos que están en su sistema.

El punto de vista de su sistema que se muestra como una casa puede hacerle sentir incómodo, y así debería ser. Tienes que mover a una necesidad de conocer

acercamiento al pensamiento de seguridad. Decida lo que el visitante necesita saber (Internet), e impedir el acceso a cualquier otra cosa.

Además de tomar un estricto aspecto más riguroso en una seguridad en su propio sistema, es necesario ampliar su punto de vista. A medida que su red crece, tanto a nivel interno con LAN, por ejemplo, y externamente con el Internet, es necesario tener en cuenta tanto la seguridad del sistema y la seguridad de la red.

Para comenzar a planificar hay que tomar en cuenta lo siguiente.

En este momento, usted necesita tomar el primer paso importante de convertirse en un pensador de seguridad más rigurosos. Cambie de una necesidad de saber y una necesidad de hacer mentalidad. Cada vez que desee hacer una nueva aplicación disponible en Internet, comience por hacer las siguientes preguntas:

¿Qué hace el usuario de Internet, que necesita saber y hacer?

¿Cómo evitar que el usuario de Internet pueda ver o hacer cualquier otra cosa?

¿Qué acceso dará a los usuarios de Internet a su programa o aplicación, ya sea directa o indirectamente?

TCP / IP e Internet están diseñados para la apertura y la interoperabilidad para que los clientes de Internet y servidores de Internet de diferentes proveedores puedan comunicarse e intercambiar información con éxito. Esta apertura hace que sea difícil de construir en las capacidades de seguridad de red. En primer lugar, los distintos proveedores deben ponerse de acuerdo sobre las normas de seguridad. Por ejemplo, al enviar contraseñas cifradas, ambos lados deben utilizar el mismo método para generar claves de cifrado y los mismos algoritmos para cifrar y descifrar.

Los usuarios de Internet son muy pocos los maliciosos. La mayoría están simplemente buscando información y formas más eficientes de hacer negocios. Sin embargo, los hackers están ahí fuera, y hay que estar preparado. El AS/400 provee de capacidades de seguridad más integradas que muchos servidores de Internet. Sin embargo, dado el entorno actual es más amigable que el Internet, es posible que no esté utilizando todas las capacidades de seguridad de AS/400 que están disponibles.

Por esta razón, más adelante se presentara algunos ejemplos para adoptar un enfoque paso a paso para la conexión a Internet. Se comienza con el lado de Internet de su sistema encerrado lo más fuerte posible, al igual que el edificio que se describió anteriormente.

Definición de seguridad

Como ya se había mencionado antes más adelante se realizaran ejemplos de cómo vincular un equipo AS/400 con el internet los cuales estarán detallados en el capítulo cuatro. En los cuales se incluirán consideraciones y consejos para garantizar una buena seguridad.

Pero antes de realizar lo dicho anteriormente, primero se expondrá una definición de lo que se entendemos por seguridad.

Una política de seguridad

La definición de lo que se quiere proteger y lo que espera de los usuarios del sistema.

Una política de seguridad define la importancia de la información de la empresa que está en nuestro sistema. Proporciona una planificación de seguridad cuando sea diseñar nuevas aplicaciones o ampliar su red. En él se describen las responsabilidades del usuario, tales como la protección de la información confidencial y la creación de contraseñas importantes.

La autenticación del usuario

Asegurarse de que sólo las personas autorizadas puede entrar en su sistema. Al vincular el sistema a una red pública como la Internet, la autenticación de usuario toma una nueva dimensión. Una diferencia importante entre la Internet y de la intranet es su capacidad de confiar en la identidad de un usuario que se registre.

Protección de los recursos

Garantizar que sólo los usuarios autorizados pueden acceder a los objetos en el sistema. La capacidad de proteger todos los tipos de recursos de sistemas es una fortaleza de los servidores AS/400. Sin embargo, también se puede dar cuenta

que no se utiliza todas las capacidades de seguridad de AS/400, especialmente si se basan principalmente en el control del menú de acceso. Se puede también encontrar que la conexión a Internet que le obliga a cambiar su definición de "público" de usuario en el sistema.

La integridad del sistema es la capacidad para proporcionar resultados estables y esperados con el rendimiento esperado. Para AS/400, la integridad del sistema es el componente más común pasado por alto de seguridad, ya que la integridad del sistema es una parte fundamental de la arquitectura AS/400, por ejemplo, hace que sea extremadamente difícil para un fabricante de software pirata, el de imitar o modificar un programa de sistema operativo (cuando se utiliza seguridad de nivel 40 o 50).

Cuando se piensa acerca de la conexión a Internet, se necesita pensar acerca de la integridad de su sistema y cómo un hacker puede intentar intervenir en su sistema AS/400. Un hacker puede poner en peligro la integridad de su sistema sin tener éxito en la sesión del sistema.

Un hacker puede, poner en peligro la capacidad del sistema para dar servicio a solicitudes de los usuarios por las inundaciones en el sistema. Su almacenamiento en disco puede ser inundado, por ejemplo, con correo no deseado. Su procesador puede ser abrumado, por las solicitudes de error. Esto comúnmente se llama denegación de servicio. Sus usuarios legítimos no pueden iniciar sesión o reciben malos resultados debido a que su sistema está gastando los recursos que tramiten solicitudes no autorizadas.

Integridad de los datos

Garantizar la fiabilidad de los datos que entra en su sistema. Cuando los datos que entra en el sistema provienen de una red pública, es posible que tenga varias protecciones de seguridad:

Proteger los datos de ser husmeada e interpretado, por lo general mediante el cifrado de la misma. Se debería asegurar de que la transmisión no ha sido alterado (integridad de los datos). Demostrar que la transmisión ocurrió. En el futuro, es posible que tenga el equivalente electrónico del correo registrado o certificado.

Seguridad de auditoría

Seguimiento de eventos relevantes para la seguridad de proporcionar un registro de accesos exitosos y no exitosos (negados). Accesos exitosos decirte quién está haciendo qué. Accesos fallidos decir tampoco que alguien está tratando de romper su seguridad o que alguien está teniendo dificultades para acceder a su sistema.

Seguridad AS/400 mínima

Los temas que se describen a continuación asumen que se está comenzando con un sistema AS/400 que es básicamente seguro. Como mínimo, el sistema debe cumplir con las siguientes normas de seguridad:

- Establecer el nivel de seguridad QSECURITY para ser de al menos 30. Nivel 40 o 50 es muy recomendable debido a que proporcionan protección de la integridad mejorada.
- Establecer los valores relevantes para la seguridad del sistema a ser al menos tan restrictivas como la configuración recomendada. Se puede utilizar los atributos del sistema de impresión de seguridad para comparar sus ajustes.
- Asegurarse de que no hay ningún perfil de usuario, incluidas a las suministradas por IBM, que tengan contraseñas por defecto.
- Utilizar las herramientas de seguridad y consejos de herramientas para la seguridad del AS/400 para ayudar a administrar y supervisar la seguridad en el sistema.

2.3. Marco Legal

El marco legal en este caso no se aplica, porque el mismo no se sustenta en una normativa legal.

2.4. Marco Espacial

La investigación de este proyecto se la realizara en la ciudad de Cuenca en la empresa Etapa, con una duración de 10 semanas, empezando el 10 de septiembre con el diseño del proyecto hasta el 24 de noviembre que es la entrega de los trabajos empastados.

El proyecto va destinado a personas interesadas en la temática de las seguridades en internet para servidores iSerie.

Cronogramas de actividades.

	Septiembre				Octubre				Noviembre				Diciembre			
	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
Diseño de proyectos y aprobación del tema		*														
Diseño del Anteproyecto			*	*												
Revisión del Anteproyecto																
Desarrollo del Proyecto					*	*	*	*	*	*	*					
Entrega del proyecto empastado											*					
Defensa del proyecto													*			

Tabla #2.
Autor: Freddy Vargas.
Cronograma de actividades

CAPÍTULO 3

3. Metodología

3.1. Proceso de Investigación

3.1.1. Unidad de Análisis

Es un tema dirigido a usuarios que deseen capacitarse y profundizar los conocimientos sobre la planificación de las seguridades para servidores iSeries, el cual se realizara mediante una investigación en el internet, de donde se tomara parte de la información para el desarrollo de esta temática.

3.1.2. Tipo de Investigación

El tipo de investigación para este proyecto será de tipo documental y explicativo.

Documental: debido a que se tomara como base información existente que será de referencia para la elaboración de la investigación.

Explicativa porque se dará a conocer en nuestra guía el cómo mantener una buena integración de las seguridades en internet para servidores iSeries.

3.1.3. Método

El método de investigación que se aplicara en nuestro trabajo es el deductivo por ser un proyecto investigativo o de recopilación de información, el cual se utilizara en el desarrollo de la temática generando un módulo teórico para el uso de los usuarios interesados en el tema.

3.1.4. Técnica

Para desarrollar el presente proyecto nos basaremos en la técnica de observación directa para la recopilación de toda la base teórica, que se detallara brevemente en el punto 3.1.5.

3.1.5. Instrumento

Los instrumentos que se utilizaran para el desarrollo del proyecto serán las siguientes:

- Recopilar información y bibliografía mediante una investigación en la web, sobre la temática propuesta.

- Consultas que se la realizara mediante encuestas a personas que estén relacionados con estos servidores iSeries.
- Aplicación de los conocimientos aprendidos en el transcurso de ciclos anteriores.
- Y con la información recopilada realizar el desarrollo del proyecto.

3.2. Encuesta realizada.

Para el presente trabajo de investigación se tuvo la necesidad de elaborar una encuesta para realizar un sondeo sobre la realidad de la Seguridad en internet de los servidores AS/400 en las empresas que cuentan con estos equipos.

Se realizó un escogimiento de empresas cuencanas en las cuales estén realizando sus labores con estos equipos y que tengan conocimiento de las seguridades de estos servidores en la “nube”.

Se pretendió buscar generalidades sobre tendencia que las compañías presentan en cuanto a la necesidad de mantener segura su información en la internet que es el objetivo de la investigación y con esto hemos logrado recopilaron los siguientes resultados.

Las Preguntas de la encuesta se enlistan a continuación:

1. Cree usted importante una buena planificación de seguridades en internet para los equipos AS/400
2. En su empresa existe algún tipo de planificación para mantener seguros sus datos en internet.
3. ¿En su empresa tienen un PLAN DE SEGURIDAD que contemple la disponibilidad de internet en el servidor AS/400?
4. ¿El plan o mecanismo de seguridad que utiliza para la disponibilidad de internet es factible?
5. Para mantener un servidor AS/400 funcionando se requiere del mismo número de personas que para un servidor tradicional no IBM
6. Indique un aproximado del presupuesto que su empresa ahorra al usar los servidores AS/400.

Estas preguntas fueron formuladas en una encuesta, se presenta a continuación.

PREGUNTA	SI	NO
1. Cree usted importante una buena planificación de seguridades en internet para los equipos AS/400		
2. En su empresa existe algún tipo de planificación para mantener seguros sus datos en internet.		
(Si responde afirmativamente la pregunta 2, califique con buena, muy buena, excelente si es tan fiable la planificación en su empresa) _____		
3. ¿En su empresa tienen un PLAN DE SEGURIDAD que contemple la disponibilidad de internet en el servidor AS/400?		
4. ¿El plan o mecanismo de seguridad que utiliza para la disponibilidad de internet es factible?		
5. Para mantener un servidor AS/400 funcionando se requiere del mismo número de personas que para un servidor tradicional no IBM		
6. Indique un aproximado del presupuesto que su empresa ahorra al usar los servidores AS/400.	**$:_____**	

Tabla #3.
Autor: Freddy Vargas.
Encuesta

3.2.1. Importancia de una buena planificación de seguridades en internet para equipos AS/400.

Tener una buena planificación para equipos AS/400 es muy importante en su totalidad según las encuestas realizadas a gerentes y profesionales del departamento de sistemas nos han respondido un 100% que es importante este punto.

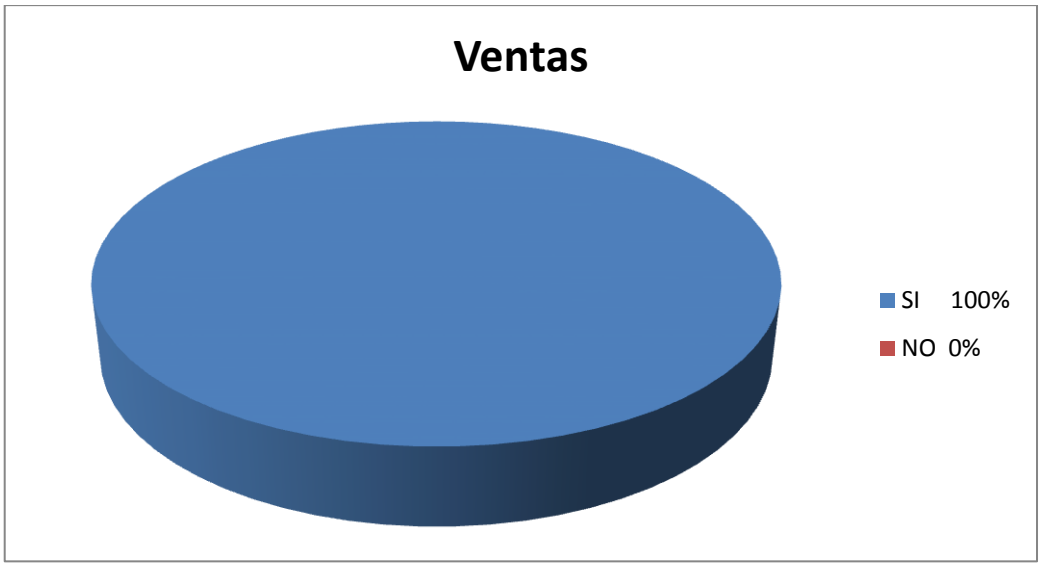


Figura #1.
Autor: Freddy Vargas.
Porcentajes de la importancia de la planificación

3.2.2. Existencia de un tipo de planificación en las empresas para la seguridad de los daos.

De la misma manera como se vio en la importancia de una planificación de seguridad en internet para AS/400 en este punto se pudo apreciar que en un 90% las empresas en cuenca que tiene servidores AS/400 mantienen una planificación de seguridades.

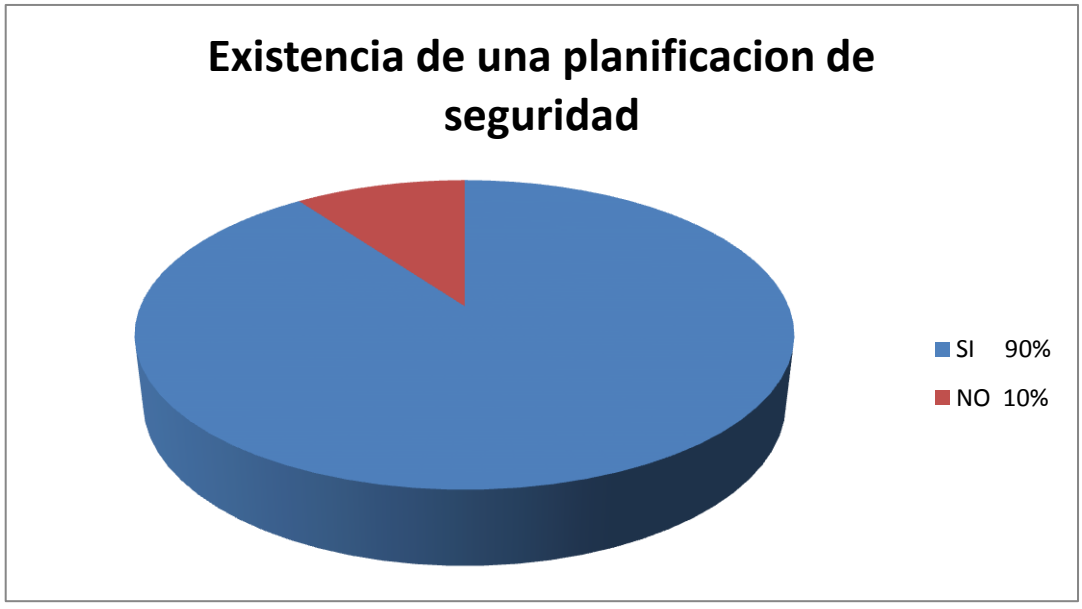


Figura #2.
Autor: Freddy Vargas.
Porcentaje de la existencia de una planificación

Un gran porcentaje de las personas que mantienen una planificación en sus empresas la califican como bueno y muy bueno, con un 42% calificándolo como bueno, un 48% de muy bueno y solo un 10% lo califican como excelente.

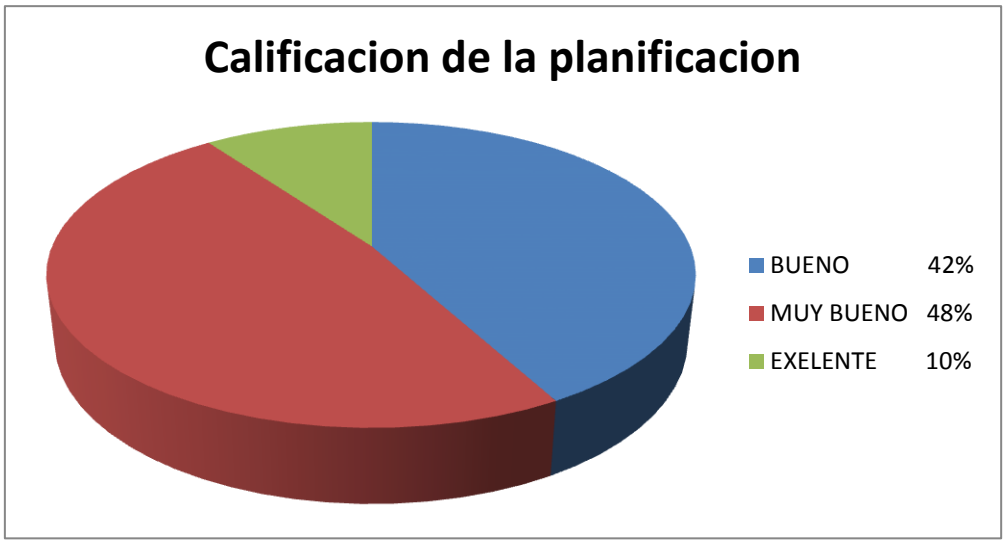


Figura #3.
Autor: Freddy Vargas.
Porcentaje; calificación de la planificación

3.2.3. Factibilidad del plan de seguridad para la disponibilidad de Internet

Este resultado es similar al del punto 3.2.2 ya que muchas de las empresas no le toman en cuenta esto de planificar las seguridades y lo pasan de alto.

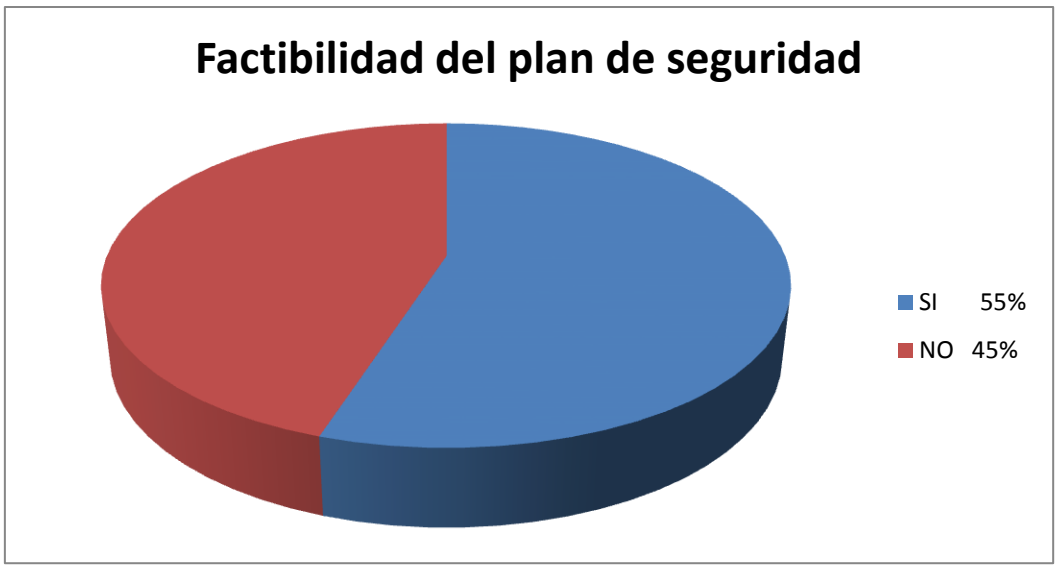


Figura #4.
Autor: Freddy Vargas.
Porcentaje; planificación del plan de seguridad

3.2.4. Recursos humanos para el funcionamiento de los servidores AS/400

En estos resultados podemos ver que para mantener un servidor AS/400 funcionando los 24 horas al día, 7 días a la semana y los 365 días del año no se necesita del mismo número de personas como cualquier otro servidor no IBM. Con un 100% para el no y un 0% al sí.

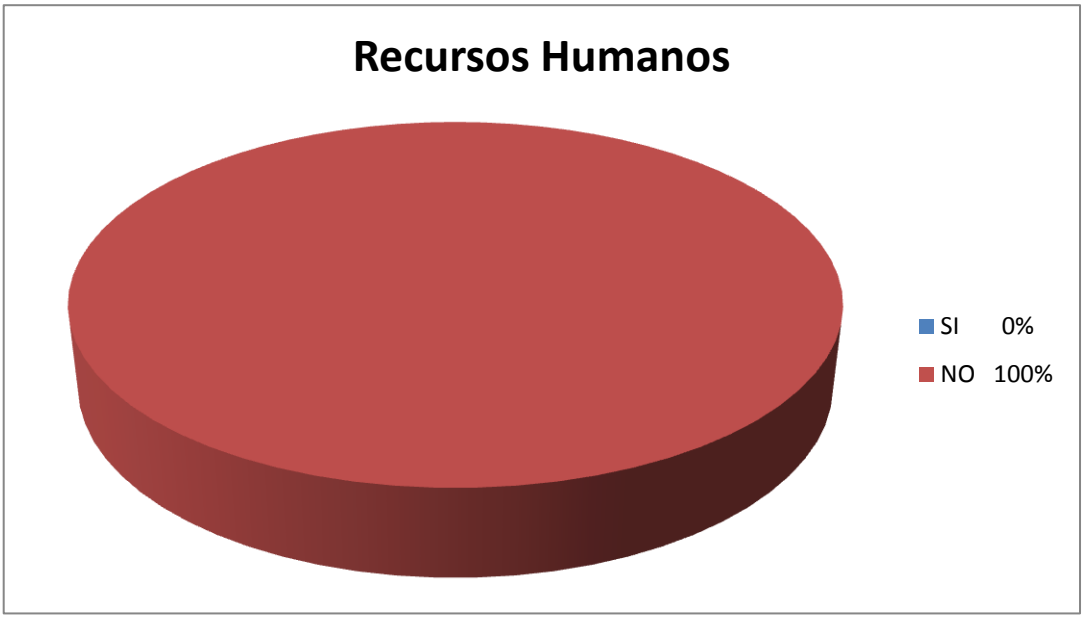


Figura #5.
Autor: Freddy Vargas.
Porcentaje; recursos humanos.

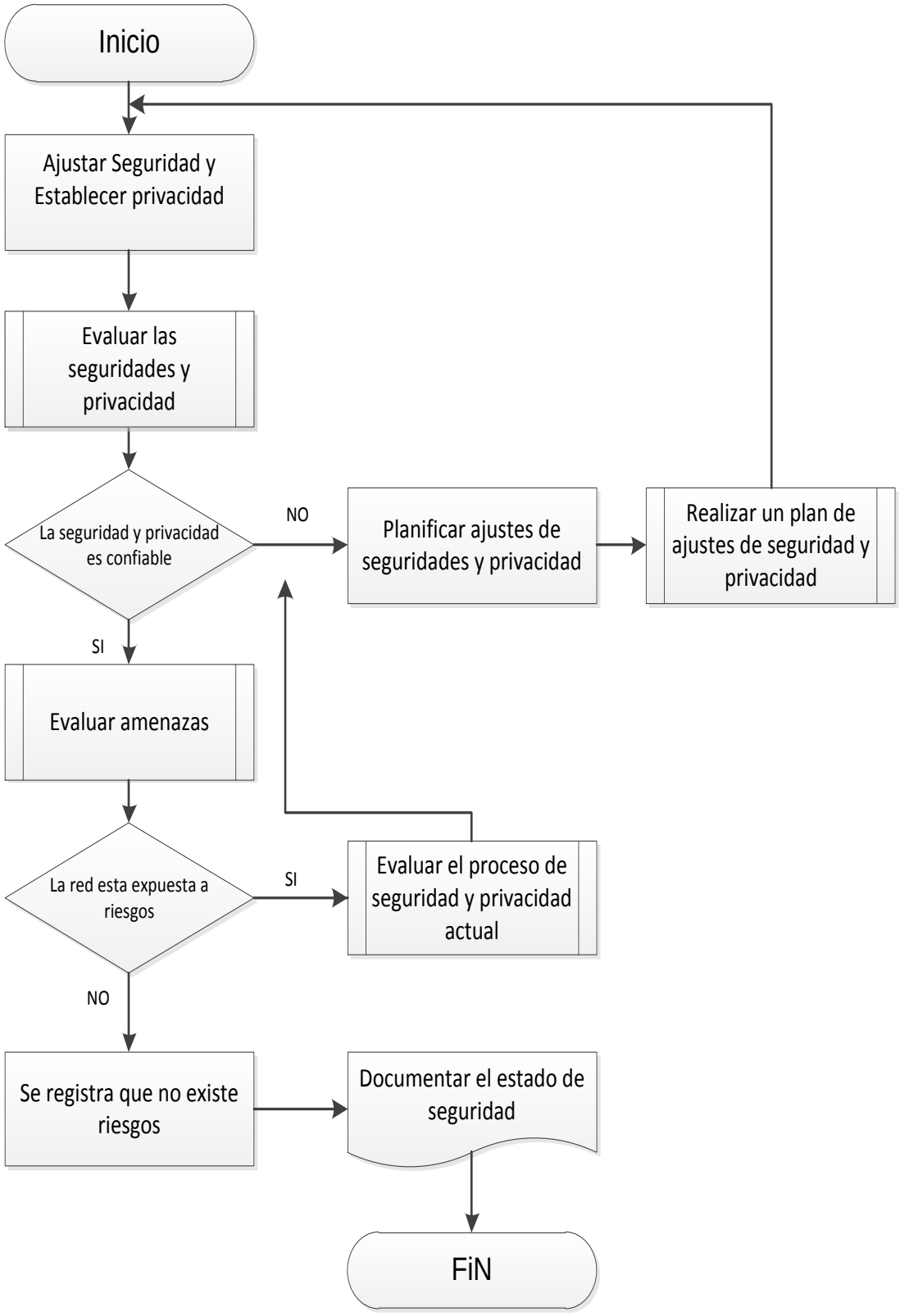
Estos resultados dejan marcada una línea muy bien definida, en la cual no solo vemos la importancia de una buenaplanificación de las seguridades para estos equipos.

También podemos decir que son equipos muy costosos pero con muy buenas ventajas ya sea hablando en lo económico, porque se requiere de los servicios de menos recursos humanos para mantener en ejecución estos equipos, de esta manera las empresas de ahorran los salarios de mínimo tres personas, se podría decir que al adquirir un servidor de estos está haciendo una inversión a corto plazo.

CAPÍTULO 4

4. RESULTADOS

4.1. Levantamiento de procesos actuales



4.2. Documento de visión.

Problema de:	No se cuenta con personal suficiente que conozca sobre el tema.
Afecta a:	La empresa
Impacto del cual es:	No poder realizar un trabajo óptimo para disminuir problemas
Una solución exitosa seria:	Tomar en cuenta el contenido del proyecto

Problema de:	No mantener una buena planificación sobre seguridades en internet.
Afecta a:	Los datos.
Impacto del cual es:	Intervención de hackers a la red y manipulación de información importante de la organización.
Una solución exitosa seria:	Toman en cuenta la investigación realizada sobre la planificación de las seguridades en internet para equipos AS/400.

Problema de:	Falta de información sobre la planificación de las seguridades en internet.
Afecta a:	Empresa, red y datos.
Impacto del cual es:	No se podrá mantener segura la red y los datos de la empresa.
Una solución exitosa seria:	Tener en consideración la investigación realizada sobre la planificación de las seguridades en internet para equipos AS/400.

Problema de:	No tomar en consideración los niveles de seguridad en internet para servidores AS/400.
Afecta a:	Servidor, red y datos.
Impacto del cual es:	La información del servidor se hace vulnerable a ser infectada ya sea por un virus, de diferentes motivos mediante la red o por usuarios.
Una solución exitosa seria:	Considerar los diferentes niveles de seguridad para una buena disponibilidad básica de internet en equipos iSeries.

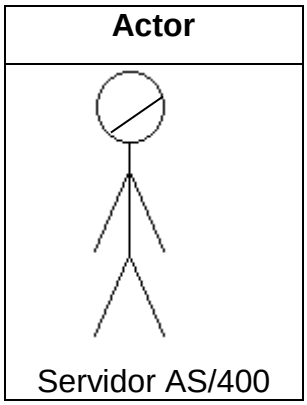
Problema de:	Falta de interés sobre las distintas opciones de seguridad de la red para equipos AS/400.
Afecta a:	Red, servidor, datos y empresa.
Impacto del cual es:	Al mantener el problema la red, servidor y datos de la empresa estarán expuestos a daños por intervención de terceras personas o por programas virus.
Una solución exitosa seria:	Considerar las opciones investigadas sobre de seguridad de la red para servidores AS/400.

Declaración del producto

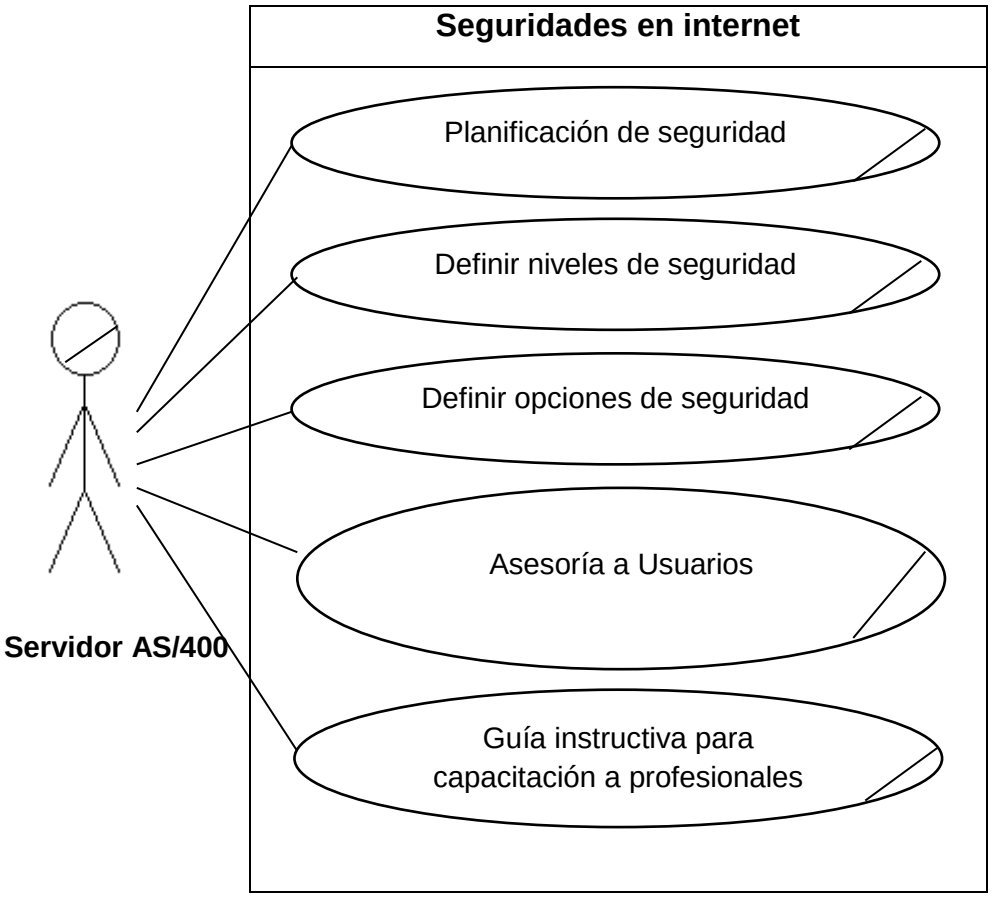
Para:	Elaborar un documento sobre la integración de las seguridades en internet para equipos As/400 “iSeries”.
Quien:	Usuarios que estén a cargo de estos servidores, para este caso profesionales de la empresa Etapa.
Nombre del producto:	Estudio de la integración sobre las seguridades en Internet para servidores As/400 “iSeries”.

Que:	Mantener una buena seguridad en internet para estos equipos, de esta manera salvaguardar la red el servidor y los datos.
Nuestro producto:	Es un plan de seguridades de internet para la necesidad de la emresa y de los usuarios que estén a cargo del servidor AS/400

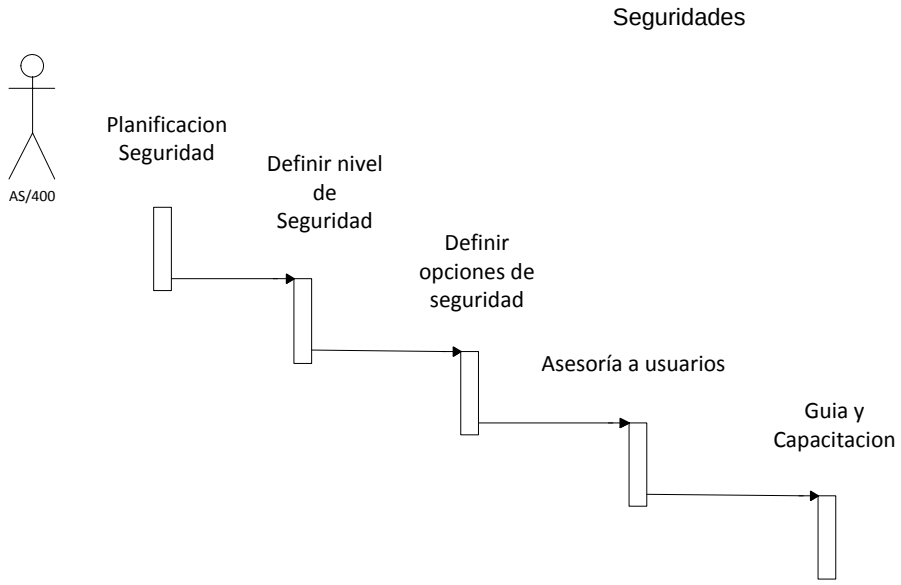
4.3. Definición de Actores



4.4. Definición de caso de uso



4.5. Diagrama de actividades



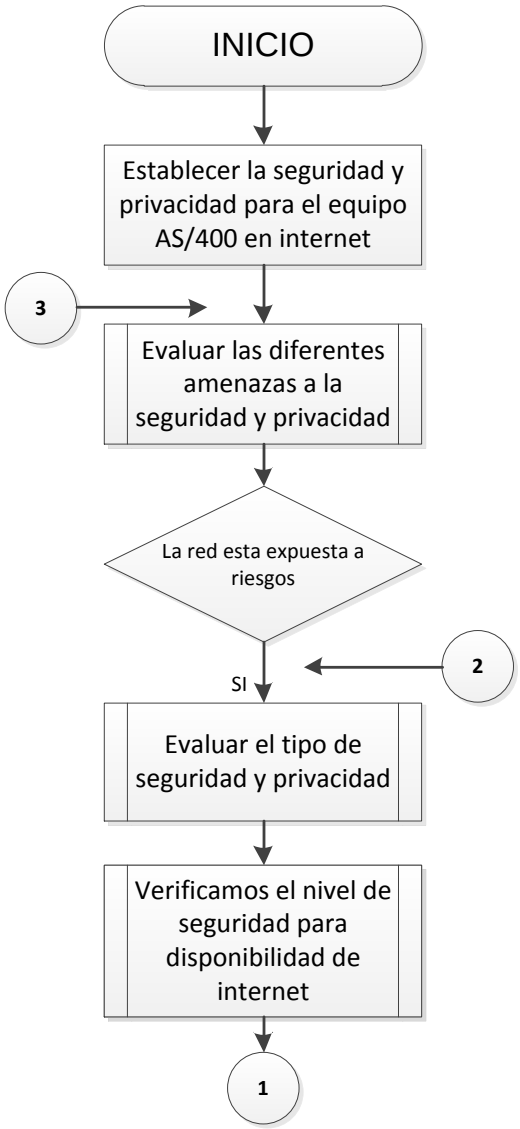
4.6. Lista de riesgos

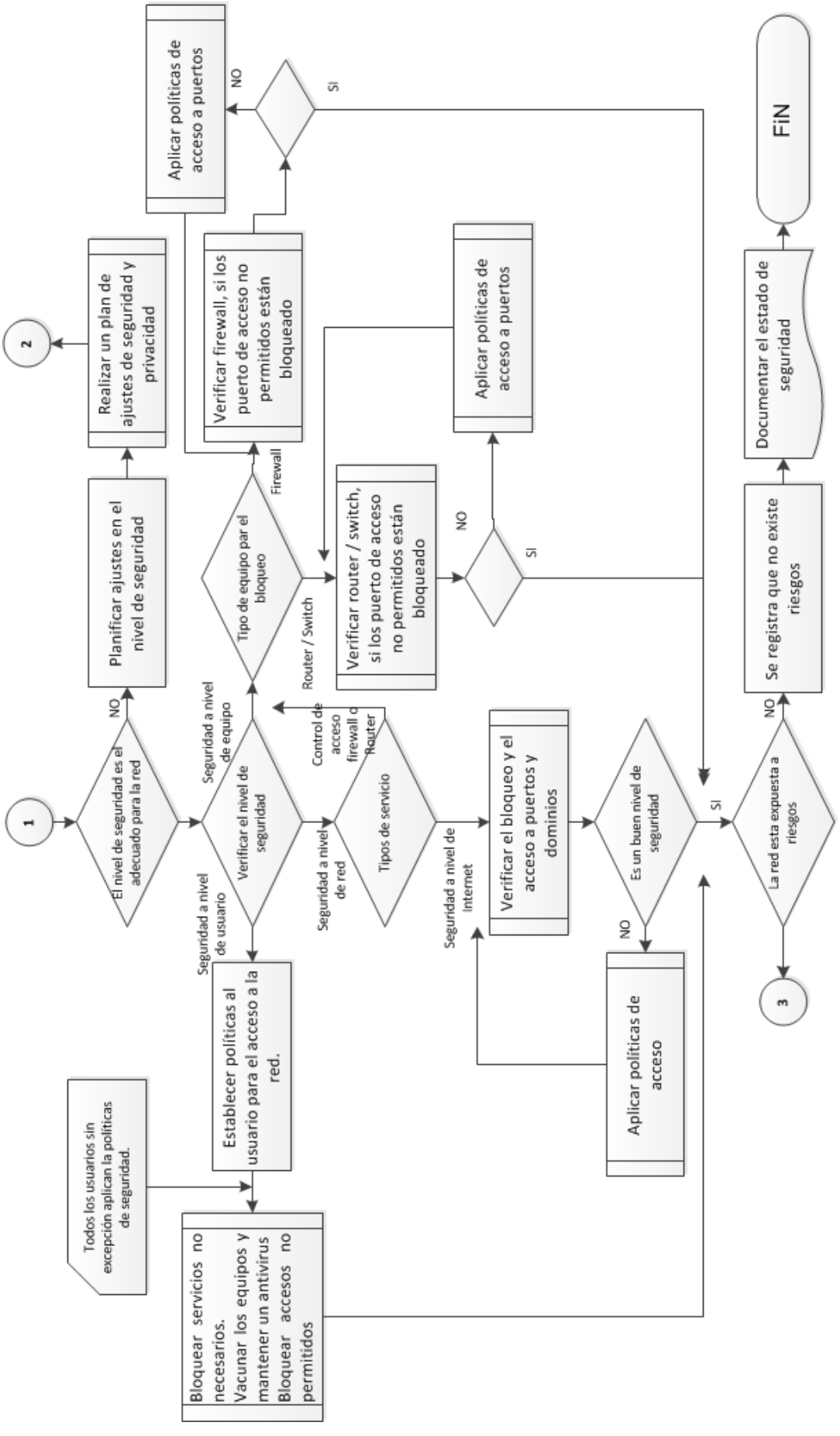
Problema	Descripción	Prioridad
Ataque a la red por hackers	Este problema se puede dar por la mala planificación de las seguridades.	MEDIO
Robo o alteración de datos importantes.	Se puede dar por la mala planificación de la seguridad, por medio de una persona con las habilidades de hacker.	ALTO
Infección de virus los datos de nuestra red.	Esto se puede dar por descargas de programas infectados o por navegación de usuarios.	ALTO
Falta de conocimiento sobre seguridades en internet para servidores AS/400	Para combatir este problema se recomienda el contenido del proyecto.	MEDIO

4.7. Requerimiento funcional del sistema.

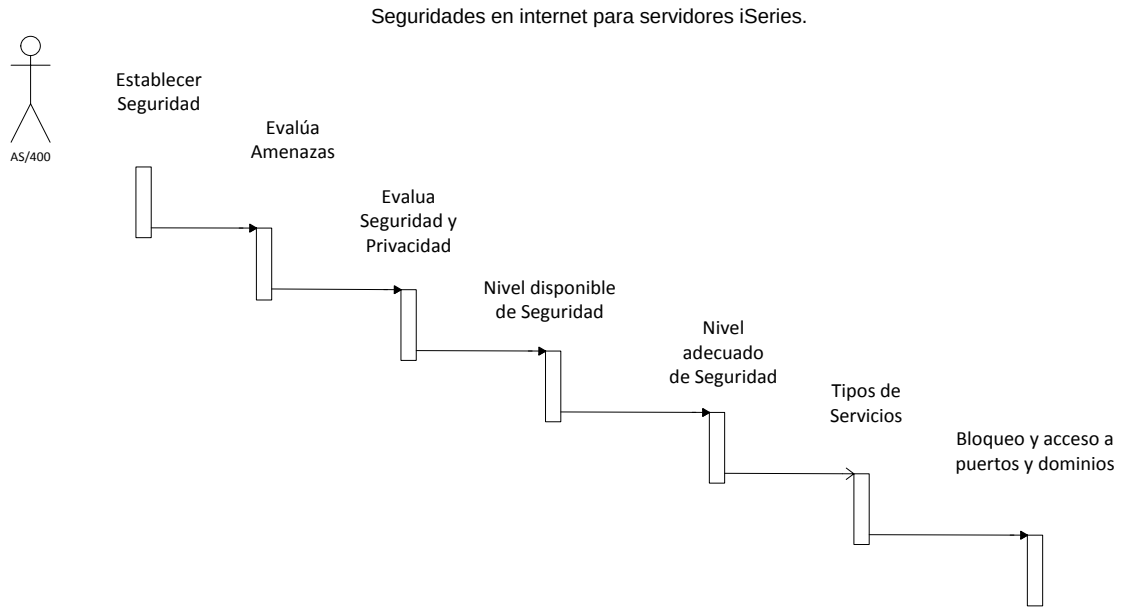
- Mantener un buen nivel de seguridad de la red.
- Prevenir que los datos sean vulnerables a infecciones por virus.
- Capacitar a profesionales que estén a cargo del funcionamiento de estos servidores.
- Mantener un buen nivel se seguridad ara la disponibilidad básica de internet.
- Restablecer la seguridad en internet para equipos AS/400 en el menor tiempo posible en el caso que se presente.

4.8. Arquitectura básica para seguridades en internet para servidores AS/3400




1
El nivel de seguridad es el adecuado para la red
NO
Planificar ajustes en el nivel de seguridad
Realizar un plan de ajustes de seguridad y privacidad
2
Seguridad a nivel de equipo
Verificar el nivel de seguridad
Tipo de equipo par el bloqueo
Firewall
Verificar firewall, si los puerto de acceso no permitidos están bloqueado
NO
Aplicar políticas de acceso a puertos
SI
Router / Switch
Verificar router / switch, si los puerto de acceso no permitidos están bloqueado
NO
Aplicar políticas de acceso a puertos
SI
Control de acceso firewall o Router
Seguridad a nivel de usuario
Establecer políticas al usuario para el acceso a la red.
Seguridad a nivel de red
Tipos de servicio
Seguridad a nivel de Internet
Verificar el bloqueo y el acceso a puertos y dominios
Es un buen nivel de seguridad
NO
Aplicar políticas de acceso
SI
La red esta expuesta a riesgos
NO
Se registra que no existe riesgos
Documentar el estado de seguridad
FIN
3
Todos los usuarios sin excepción aplican la políticas de seguridad.
Bloquear servicios no necesarios.
Vacunar los equipos y mantener un antivirus
Bloquear accesos no permitidos

4.9. Diagrama de actividades



4.10. PLANIFICAR LA SEGURIDAD EN INTERNET PARA EQUIPOS iSeries o (AS/400)

A la hora de elaborar planes para el uso de Internet, lo primordial que se debe tener en consideración es planificar detenidamente las necesidades de seguridad en internet. Para esto deberá recaudar información puntual a cerca de los planes del uso de Internet y documentar de una forma clara la configuración de la red interna. Luego de obtener estos recursos se podrá evaluar de una forma precisa las necesidades de seguridad.

A continuación se les dará algunas pautas de los aspectos que se debe describir y documentar, para una buena planificación:

- Documentar la configuración de la red actual.
- Información de la configuración del servidor de correo electrónico y DNS.
- La conexión con el proveedor de servicios de Internet (ISP).
- Tomar en consideración las diferentes opciones de servicios de Internet que desea utilizar.
- Qué servicios desea proporcionar a los usuarios de Internet.

Al documentar información de este tipo les permitirá fijar cuales son los diferente riesgos de seguridad a los que se expone y también determinar las medidas necesarias para disminuir estos riesgos.

Para alcanzar una buena ayuda en la elaboración de planes de seguridad con el uso de Internet, es recomendable tener en consideración los siguientes temas y consultarlos.

La Seguridad Basada en la Defensa por Capas

El objetivo de las políticas de seguridad es definir qué es lo que se desea proteger en la red, clasificar las amenazas, determinar mecanismos para prevenirlos, verificar los mecanismos de protección y evaluar sus consecuencias. La seguridad basada en defensa por capas proporciona una base para la planificación de las seguridades cuando se pretenda ampliar la red y también cuando se diseñe nuevas aplicaciones. También especifica responsabilidades de los usuarios como las de proteger información privada e importante y crear contraseñas no fáciles de descifrar.

Cuando en las empresas realizan actividades con acceso a internet esto lleva consigo asociado muchos riesgos, siempre y cuando que se cree una política de seguridad, habrá que calcular el suministro de servicios con el control del acceso a las funciones y los datos. La seguridad es más difícil en los sistemas conectados en red, puesto que el propio canal de comunicaciones está abierto a los ataques de intrusos.

Existen servicios de Internet que son más sensibles a ciertos tipos de ataques que otros. Por esto, es elemental que comprenda los riesgos que presume cada servicio que se proponga utilizar o prestar. Además, el conocimiento de los posibles riesgos de seguridad ayuda a determinar un conjunto claro de objetivos de seguridad.

En la web existen determinados individuos que son una amenaza para la seguridad de las comunicaciones por Internet. A continuación se lista diferentes riesgos de seguridad más típicos a los que se podría enfrentar:

- **Ataques Pasivos:** En los ataques pasivos, acure de la siguiente manera, para conocer los secretos o seguridades de la empresa el intruso supervisa el tráfico de la red. Estos ataques se fundan en la red, indagando los enlaces de comunicaciones como también se puede basar en el sistema, sustituyendo un componente del mismo por un programa por ejemplo caballo de Troya que captura los datos clandestinamente. Estos ataques son los más difíciles de detectar, y es importante estar a la defensiva y tener en mente que cualquiera puede estar a la expectativa de lo que se envía por la web y realizar un ataque a la información.
- **Ataques Activos:** En este tipo de ataque el autor intenta abrirse paso por medio de sus defensas para así infiltrarse en los sistemas de la red. Existen varios tipos de ataques activos:
    - **Tomar el control:** En los intentos de acceso al sistema, el atacante intenta hacer valer las brechas de seguridad para intervenir a un cliente o un sistema y controlarlo.
    - **Usurpación:** En los ataques de usurpación, el atacante intenta abrirse paso a través de sus defensas haciéndose pasar por un sistema de confianza o bien un usuario he intenta convencer de que le envíe información secreta.
    - **Denegación de servicio:** En los ataques de denegación de servicio, el atacante intenta acceder en las operaciones para tomar el mando o detenerlas, redirigiendo el tráfico o bombardeando el sistema con correo basura.
    - **Ataques secretos:** El atacante intentará Hackear o robar las contraseñas para esto utilizará herramientas especializadas para intentar descifrar los datos cifrados.

- **Múltiples Capas de Defensa**

Los riesgos potenciales en la Internet se pueden producir en varios niveles, así también es recomendable configurar medidas de seguridad que brinden múltiples capas de defensa contra los riesgos. En general, cuando se enlace a Internet, se debe tener en cuenta y dar por seguro que se producirán problemas de seguridad

y no preguntarse si abra alguna posibilidad de que se produzca intrusiones o ataques a la información de un sistema o a un sistema que está enlazada con la red. De esta forma, la mejor defensa será un ataque proactivo y deliberado. El uso de un enfoque por capas al planificar la estrategia de seguridad de Internet garantiza que el atacante que logre entrar en una de las capas de defensa será detenido en una de las capas posteriores.

El crear la estrategia de seguridad deberá incluir medidas de defensa que brinde protección en las diferentes capas de modelo informático de la red tradicional, así que se deberá planificar las seguridades desde el nivel más básico que es la seguridad del sistema hasta el nivel más complejo que son las seguridades de transacciones.

- **Seguridad a Nivel de Sistema**

El nivel de seguridad del sistema representa la última línea de defensa contra los riesgos de seguridad relacionados con el Internet, pero no la menos importante, Por lo que, lo primero que se debe realizar para crear una estrategia completa de seguridad de internet es la configuración debida de los valores básicos de seguridad del sistema iSeries.

- **Seguridad a Nivel de Red**

El nivel de seguridad de la red son las que están a cargo del control del acceso al sistema iSeries y a otros diferentes sistemas de la red. El momento de conectar la red a Internet, se debe cerciorar que las medias de seguridad a nivel de red están debidamente implantadas para así proteger los recursos internos de la red frente a intrusiones no deseadas y el acceso no autorizado.

Para lograr una buena garantía de seguridad de la red el medio más común es un cortafuego. El proveedor de servicios de Internet (ISP) puede y debe proveer una parte importante del plan de seguridad de la red. El único que debe indicar las medidas de seguridad que le va a proporcionar el ISP a la red, es el esquema de seguridad del proveedor de servicios de Internet.

Las medidas de seguridad que proporciona el ISP son: las precauciones del servicio de nombres de dominio (DNS) público y las reglas de filtrado de la conexión del direccionador del ISP.

- **Seguridad a Nivel de Aplicaciones**

La seguridad a nivel de aplicaciones son los que controlan cómo pueden integrar a los usuarios con las aplicaciones concretas. En general, habrá que configurar los valores de seguridad para todas las aplicaciones que se utilice sin excepción de ninguna. Sin embargo, lo conveniente es tomar precauciones especiales para configurar los servicios que utilizará de Internet o prestará a la misma y la seguridad de las aplicaciones. Estos servicios y aplicaciones son vulnerables al uso inadecuado de los usuarios que no están autorizados al acceso los mismos que buscan una manera de entrar a los sistemas de la red. Deberán incluir los riesgos del lado del servidor y del lado del cliente, a la hora de decidir qué medidas de seguridad se utilizara.

- **Seguridad a Nivel de Transmisión**

La seguridad a nivel de transmisión es la encargada de proteger las comunicaciones de datos dentro de la red local y entre distintas redes. Cuando se enlaza a una red que no es confiable como el Internet, no se le hace tan fácil el controlar cómo fluye el tráfico desde el origen hasta el destino y viceversa. El tráfico y los datos transportados fluyen a través de distintos servidores que están fuera de su control. Esto sería diferente si implanta medidas de seguridad como las de configurar las aplicaciones para que utilicen SSL (capa de sockets segura), así los datos direccionados en la red estarán a disposición de cualquier usuario que desee verlos y utilizarlos. Con estas medidas de seguridad que son las de nivel de transmisión podemos proteger los datos mientras fluyen entre los límites de otros niveles de seguridad.

4.10.1. Política y Objetivos de Seguridad

En este punto nos permitirá definir los datos importantes que se deben proteger y qué es lo que se esperar de los usuarios.

- **La Política de Seguridad**

Debemos suponer que los servicios que prestan internet y los que se van a utilizar no son tan fiables, y tendrá riesgos para nuestra red a la que estará conectado y de igual manera para nuestro sistema iSeries. Una política de seguridad son un conjunto de reglas que se aplican a las actividades del sistema y a los recursos de

comunicaciones que forman parte de una organización. En estas reglas incluyen áreas importantes como la seguridad administrativa, personal, física y de la red.

En la política de seguridad se define qué es lo que se desea proteger y qué se espera de los usuarios del sistema. Nos facilita una base para la planificación de la seguridad al ampliar la red actual o al diseñar nuevas aplicaciones. Detalla responsabilidades del usuario así como las de crear contraseñas que no sean fáciles de descifrar y proteger información confidencial. La política de seguridad también debe describir cómo se va a supervisar la efectividad de las medidas de seguridad. Esta supervisión le ayudará a definir si algún usuario está tratando de esquivar sus defensas.

Para crear una política de seguridad, lo primordial seria el definir de una manera clara y concisa sus objetivos de seguridad. Luego de crear la política de seguridad, el segundo paso es poner en práctica las reglas de la política. En este paso se incluye la suma de piezas de hardware y programas que se requiere para poner en marcha las reglas y también la formación de los usuarios. Asimismo, a la hora de realizar cambios en el entorno informático, deberá actualizar la política de seguridad. Para cubrir los posibles riesgos que puedan incluir a los cambios realizados.

- **Los Objetivos de Seguridad**

Al momento de crear una política de seguridad, se deberá tener en cuenta los objetivos de seguridad, los mismos que entran en las siguientes categorías:

- **Protección de Recursos**

  En este esquema nos garantiza que únicamente los usuarios que tengan la autorización puedan acceder a los objetos del sistema. La capacidad de mantener seguro todos los recursos del sistema es una de las ventajas del iSeries. Para esto primero tiene que definir con precisión las diferentes categorías de usuarios que pueden acceder al sistema. De igual modo, cuando cree la política de seguridad, deberá definir para estos grupos de usuario qué tipo de autorización de acceso desea establecer

- **Autenticación**

La autenticación es muy importante porque mediante esto podemos probar que el recurso (persona o máquina) ubicado en el otro extremo de la sesión es efectivamente el que dice ser. Con una autenticación convincente se protege de mejor manera el sistema contra riesgos de seguridad como las imitaciones, en donde el remitente o el destinatario utilizan identidades falsas para acceder al sistema.

Como una tradición, los sistemas han utilizado contraseñas y nombres de usuario para la autenticación; otra ventaja de seguridad son los certificados digitales que pueden ofrecer un método más seguro de autenticación.

Debemos tomar en cuenta que la autenticación de usuario toma nuevas dimensiones al enlaza su sistema con una red pública como Internet. Por esto, se debería considerar seriamente la posibilidad de usar métodos más potentes de autenticación que los procedimientos tradicionales de conexión mediante nombre de usuario y contraseña. Los usuarios autenticados según su nivel de autorización pueden tener distintos tipos de permisos.

- **Autorización**

Este tipo de seguridad consiste en que la persona o el sistema situado en el otro extremo de la sesión va a tener permiso para concluir con la petición.

La autorización es el proceso de fijar quién o qué tiene el permiso a ejecutar determinadas actividades en un sistema o el acceso a los recursos del sistema. Normalmente, la autorización se realiza en el contexto de la autenticación.

- **Integridad**

Esta seguridad consiste en que la información entrante es la misma que la que se ha enviado. Para comprender sobre la integridad, primero deberá entender de qué se trata la integridad de los datos e integridad del sistema.

  - **Integridad de los Datos:** Consiste en que los datos están protegidos contra riesgos de seguridad como manipulaciones no autorizados,

donde una persona interviene y modifica la información y datos almacenados en la red sin tener la autorización para ello. Para garantizar la integridad de datos que proceden de fuentes no confiables deberá necesitar medidas de seguridad adicionales.

Cuando la información que entra en su sistema es procedente de una red pública, necesitará métodos de seguridad para:

1. Proteger los datos para que no puedan ser interpretados.
2. Asegurar que las transmisiones no han sido alteradas.
3. Demostrar que se ha producido la transmisión.

- **Integridad del Sistema:** El sistema facilita resultados lógicos con el rendimiento esperado. En el caso de los sistemas AS/400, el componente de seguridad más vigilado es la integridad del sistema, por el motivo que es una parte fundamental de la arquitectura del AS/400.

  Por ejemplo, en la arquitectura del sistema AS/400 si se utiliza los niveles de seguridad 40 o 50, dificulta enormemente a los intrusos la simulación o el cambio de un programa del sistema operativo.

  "Niveles de Seguridad: En el sistema AS/400 existen los siguientes niveles de seguridad:

  - **Nivel 10:** Los usuarios no disponen de contraseña ni se controla el acceso a los recursos. Este nivel dejó de estar soportado desde la versión v4R2 del sistema operativo de IBM.
  - **Nivel 20:** proporciona únicamente seguridad por contraseña.
  - **Nivel 30:** proporciona seguridad por contraseña y recursos.
  - **Nivel 40:** proporciona seguridad por contraseña y recursos; seguridad de integridad. Este es el nivel de seguridad que por defecto implementan los sistemas actuales.
  - **Nivel 50:** proporciona seguridad por contraseña y recursos; protección de integridad mejorada. El nivel de seguridad 50 se aplica en sistemas que necesitan un nivel de seguridad certificado."[3]

[3] iSeriesInformation Center, Versión 5 Release 4

Desde el punto de vista de la seguridad es conveniente disponer como mínimo un nivel de 30 o superior en el parámetro QSECURITY el que establece el nivel de seguridad real en el servidor AS/400, por lo tanto, se debe implementar una política de seguridad que consista en que todos los accesos permanezcan controlados por un nombre de usuario único y su respectiva contraseña y privilegios y permisos que permita a los usuarios tener acceso a los recursos del sistema.

- **Confidencialidad**

Consiste en mantener privada la información confidencial y que no sean visibles para intrusos. Este tipo de seguridad es fundamental para la seguridad total de los datos. Para asegurar la confidencialidad de los datos que están siendo transmitidos entre varias redes que no son de confianza, se podría tener en cuenta la capa de socket segura (SSL) y el cifrado de los datos con certificados digitales. La política de seguridad deberá mostrar los métodos que se usaran para facilitar la confidencialidad de los datos dentro de la red y la información que sale de ella.

- **Actividades de Seguridad de Auditoría**

Esto consiste en mantener una supervisión de los eventos que estén relacionados con la seguridad para producir un archivo de apuntes de todos los accesos satisfactorios y de los denegados. Todos los registros de accesos satisfactorios muestran quién está realizando las tareas en los sistemas, y los registros de accesos desfavorable o denegado, nos indica que alguien de una red pública está intentando ingresar a la red a través de las barreras de seguridad del sistema o que algún usuario que tengan permiso de acceso tiene algún tipo de inconveniente para ingresar al sistema.

Al tener conocimiento de estos objetivos de seguridad le ayudara crear una buena política de seguridad que satisfaga todas sus necesidades de seguridad de la red y de internet para los servidores AS/400.

4.10.2. Ejemplos para una buena planificación de las seguridades en internet para equipos AS/400.

Los ejemplos que se detallaran proporcionan opciones típicas para conectar su sistema AS/400 a Internet. Aquí se discuten los riesgos de seguridad y posibles soluciones. Estas no son las únicas opciones disponibles, ni son necesariamente las opciones más seguras. Un cortafuego correctamente configurado y administrado casi siempre es el método más seguro para conectar su sistema al resto del mundo. Mediante el uso de un servidor de seguridad, están limitando sus puntos de exposición y ocultación de la configuración de red a los demás. La necesidad de considerar un cortafuegos cuando se conecta el servidor AS/400 a Internet no es diferente que cuando se conecta a otros servidores de Internet.

Como organizaciones que necesitan ampliar el uso de Internet y cada vez proporcionar acceso a la información mediante la web, los cortafuegos son recomendados para mantener una buena seguridad en su red. En los ejemplos q se detallaran a continuación se verá que varios de ellos no cuentan con servidores de seguridad. La mayor parte de las consideraciones de seguridad son válidas con o sin un firewall.

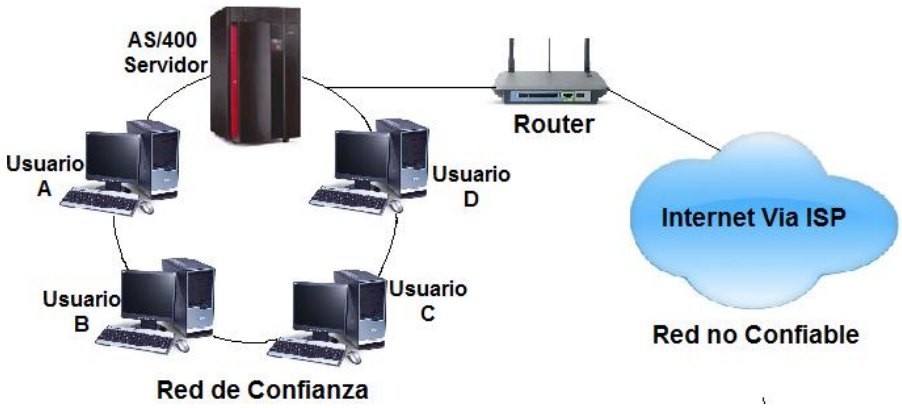


Figura #6.
Autor: Freddy Vargas.
Arquitectura servidor AS/400

4.10.2.1. Ejemplo 1.Conectar a los usuarios al Internet

Su primer peligro que puede correr en la Internet podría ser la de proporcionar a los usuarios el acceso a la Internet. Vamos a suponer que su AS/400 y sus equipos ya están en una LAN (red de área local). En lugar de poner un módem en

cada PC, se desea proporcionar un punto central de acceso a Internet. Cada PC tiene software de navegador de la Web.

En la configuración que se muestra en la figura #6 muestra una forma común para conectar los usuarios de la LAN a Internet. Los usuarios de PC pueden ir directamente a Internet a través del router. También pueden seguir accediendo a su AS/400 a través de la LAN.

Análisis de seguridad para este ejemplo. A continuación se describirá algunos de los riesgos de seguridad para el Ejemplo 1 y alternativas para hacer frente a los riesgos. En este ejemplo lo que se busca es que no se quiere que nadie desde fuera de la red pueda acceder a AS/400. El objetivo particular es proteger el AS/400 y sus datos.

4.10.2.1.1. Riesgo 1 - Direcciones IP pública:

Generalmente con este tipo de conexión de una red LAN a internet mediante un router, cualquier PC que se conecta a Internet debe tener una dirección IP. Contar con una dirección IP es similar a tener un número de teléfono público. Siempre que un usuario de la red envía una solicitud de Internet, el paquete contiene la dirección IP del ordenador del usuario. Cualquier host en Internet que hace contacto con la PC conoce la dirección IP de la misma. Un intruso potencial podría ser capaz de acceder a esa información e intentar acceder a la computadora mediante el uso de la dirección IP.

Soluciones de seguridad

Asegúrese de que el AS/400 no tiene una dirección IP. Esto protege su AS/400 de los ataques directos, incluidos los ataques de denegación de servicio.

Eduque a sus usuarios de PC sobre la necesidad de proteger sus equipos de intentos de intrusión. Asegúrese de que un extraño que con éxito se introduce en una computadora no puede ir más allá de ese PC en la red. Esta protección puede ser difícil, y depende en cierta medida de las prácticas de seguridad de los usuarios de PC. Un intruso se verá en un ordenador para obtener información, como los nombres de sistema o las

comunicaciones de puesta en marcha de programas, lo que podrían ayudar al intruso para la ruptura de otro sistema de la red. El intruso también buscará identificadores de usuario y contraseñas almacenados en el PC.

Su AS/400 es vulnerable tanto para el enlace más débil (PC con las prácticas de seguridad pobres) y la contraseña más vulnerables a los ataques de los hackers.

Asegúrese de que nadie empiece cualquier servidores TCP / IP en el sistema. Los hackers suelen ser más familiarizados con el uso de TCP / IP (por ejemplo, FTP y TELNET) de lo que son con AS/400 Client Access. Si un pirata informático encuentra el nombre del sistema AS/400 cuando se navega por un PC, el hacker probablemente intentará utilizar TELNET o FTP para acceder al AS/400.

Controlar IOSYSCFG autoridad especial para restringir quién puede configurar TCP / IP. Restringir el que tiene la autoridad para utilizar la STRTCP (Start TCP/IP) de comandos.

4.10.2.1.2. Riesgo 2 - Descarga de virus:

Un virus es un programa que puede modificar otros programas para incluir una copia de sí mismo. El programa de virus por lo general realiza operaciones que pueden ocupar los recursos del sistema o destruir datos.

Cuando los usuarios se conectan a Internet, de forma no intencionada puede descargar un programa con un virus. Se pueden almacenar el programa infectado en una carpeta compartida o en el sistema de archivos integrado en el AS/400. Este virus puede entonces ser copiado accidentalmente a otros ordenadores en su red.

Soluciones de seguridad

En el equipo AS/400, realizar un control de autoridad para que los usuarios puedan y no crear nuevos objetos. Si los usuarios de PC utilizan las carpetas compartidas, utilice la autoridad de DLO (objetos de biblioteca de documentos) para limitar la creación de nuevos documentos en carpetas específicas.

Si los usuarios de PC utilizan el sistema de archivos integrado, es recomendable utilizar la autoridad para controlar a los directorios donde pueden colocar nuevos objetos.

Regularmente ejecutar programas de detección de virus contra los directorios o carpetas en donde los usuarios de PC colocar nuevos objetos. Instalar el software de exploración de virus en todos los PC que requieren que los usuarios para que funcione con regularidad. Considerar la inclusión del programa antivirus en cada rutina de arranque del PC.

Considere organizar el movimiento de objetos nuevos a partir de unidades de PC privadas a un entorno compartido. Mover a una unidad temporal (carpeta compartida o directorio) en primer lugar. Luego haga que un administrador del sistema mueva a un medio ambiente compartido después de ejecutar un programa de antivirus.

4.10.2.2. Ejemplo 2.Proporcionar E-Mail

Ahora que sus usuarios están conectados, quieren intercambiar e-mail (notas y mensajes electrónicos) con el mundo exterior.

La configuración de la red será igual a la figura 6. Ya sea que usted necesite agregar software de correo electrónico, o puede utilizar el software que usted ya tiene. A continuación se presentan dos opciones de software posibles.

- Si ya se utiliza OfficeVision o JustMail para OS/400, puede realizar cambios en la configuración para poder enviar y recibir mensajes de correo electrónico a través de Internet. Usted necesita iniciar a ambos TCP / IP y el SMTP (Protocolo de transferencia de correo simple.) del servidor. Es necesario realizar cambios en el directorio de distribución del sistema para que funcione correctamente con SMTP.
- Puede instalar software de correo electrónico, como UltiMail Lite en sus PC proporciona la capacidad de cargar y descargar el correo. Conecta tu computadora a un servidor de almacenamiento y reenvío de correo. AS/400 proporciona esta capacidad con el Protocolo de correo de oficina. (POP) del servidor. O bien, los PC se pueden utilizar un servicio de correo fuera de la tienda y reenvío de un proveedor de servicio.

Consideraciones de seguridad para este ejemplo

Al agregar el correo electrónico, la planificación de su seguridad debe ser más específica. Ya no se puede simplemente configurar un router para excluir a todas las sesiones, cuyo origen se encuentra fuera de su red. Ahora podemos asumir que el AS/400 no participará. Los usuarios de AS/400 que no tienen capacidad de navegador pueden enviar y recibir correo electrónico si usted se los permite.

A continuación se presentan tanto los riesgos de seguridad al agregar e-mail y las alternativas para hacer frente a los riesgos. En este ejemplo se da por supuesto que no quiero que nadie de fuera de la red pueda exceder a cualquier sistema dentro de la red, con la excepción del envío de correo electrónico a los usuarios de la red. El objetivo particular es proteger el AS/400 y sus datos.

4.10.2.2.1. Riesgo 1 - Publicar al público el Directorio del AS/400:

Si desea que su AS/400 proporcione servicios de correo electrónico a sus usuarios, es necesario registrar el AS/400 en Internet con una dirección IP. Su AS/400 ahora se hace visible al mundo exterior y sin perjuicio de intento de intrusión.

Soluciones de Seguridad

- Utilice las capacidades de seguridad del AS/400 para proteger su sistema de inicio de sesión no autorizado. Esto incluye tanto la configuración de inicio de sesión y los valores de contraseña del sistema y nos debemos asegurar que no hay ningún perfil de usuario que tiene contraseñas por defecto.
- Hasta que esté listo para las aplicaciones internas TCP/IP, siguiendo las precauciones descritas en el ejemplo posterior, configurar TCP / IP para que sólo el servidor SMTP y, posiblemente, el servidor POP iniciará automáticamente, se debe cambiar los atributos de mandatos para impedir que otros servidores se inicien automáticamente. Por ejemplo, para evitar que TELNET se inicie automáticamente, escriba lo siguiente: CHGTELNA AUTOSTART (* NO).

- El comando para iniciar los servidores TCP / IP es (STRTCPSVE). Asegúrese de que la autoridad no ha sido cambiada y revisar la lista de los usuarios que están autorizados a utilizar el comando.
- Considere cambiar el valor predeterminado para el parámetro Server en el comando STRTCPSVR.
- Si ejecuta la aplicación TCP / IP (como FTP) en su red interna, debe configurar su router para rechazar todos los paquetes externos que van a cualquier puerto excepto el SMTP (correo) del puerto. Todas las aplicaciones TCP/IP están asociadas con un puerto especial de TCP/IP. Un puerto es como una puerta en la configuración TCP / IP.

4.10.2.2.2. Riesgo 2. Inundaciones del sistema:

Uno de los juegos utilizados por los hackers consiste en inundar el sistema con el correo no deseado. Esto puede afectar negativamente el rendimiento del sistema. El correo también puede tomar tanto espacio en el almacenamiento en disco que el sistema deje de funcionar.

Soluciones de seguridad:

Las siguientes son sugerencias para limitar el impacto de los intentos de inundar su sistema.

- Si es posible, evite el uso de un *ANY *ANY entrada en el directorio de distribución del sistema. Esto hace que sea más difícil para alguien que quiera inundar el sistema con el correo no deseado que se direcciona a través de su sistema a otro sistema. Sin un *ANY *ANY entrada, el sistema rechazará el correo que no se dirige a un usuario válido en la red.
- Establecer un límite de almacenamiento auxiliar. Esto evita que los objetos no deseados de la inundación nuca funcionen.

4.10.2.2.3. Riesgo 3. Recepción de los virus a través de E-Mail

El correo entrante es una fuente potencial de virus para las PC. Alguien puede adjuntar un programa a una nota. O alguien puede enviar un programa a un

usuario en el sistema. Tal vez ni el emisor ni el receptor se dio cuenta de que el programa aparentemente inofensivo se está propagando un virus.

Soluciones de seguridad

- Debido a la arquitectura AS/400, el correo entrante es poco probable que infectan AS/400. Un programa no puede llegar disfrazado de otra cosa a nuestro AS/400. Sin embargo, los virus de PC pueden llegar en el correo. Y se deberá seguir las mismas soluciones los que se describieron en el riesgo 2 “descarga de virus” del ejemplo 1.
- Educar a los usuarios sobre la posibilidad de recibir programas de virus a través de e-mail, posiblemente, de sus amigos y colegas.

4.10.2.2.4. **Riesgo 4. E-mail dirigido.**

Cuando el correo electrónico interno del sistema está conectado a la Internet, usted tiene la posibilidad de que un usuario envíe información confidencial con el mundo exterior. Esto puede ocurrir por accidente, y tal vez incluso sin el conocimiento del usuario, si su conexión de correo electrónico no está configurado correctamente.

Soluciones de seguridad

- Al configurar su dirección de e-mail, pruebe lo que ocurre con el correo dirigido incorrectamente. Va a tener un ID de usuario incorrecta o un nombre de sistema incorrecto (que no está en tu red) que el correo que se envía a través de su enlace de correo de Internet.
- Si es posible, configure su sistema de correo electrónico para requerir confirmación del usuario antes que el e-mail se envíe fuera de su red.
- Educar a los usuarios acerca de sus políticas para el envío de información confidencial a través del correo electrónico.

4.10.2.2.5. Riesgo 5. La exposición de información confidencial

Al ampliar el uso de Internet y de las redes en general, los usuarios pueden explorar diferentes formas de trabajar. Tal vez se puede marcar en su sistema desde su casa o mientras viajan. Pueden utilizar el correo electrónico como una

herramienta para colaborar con sus colegas en un proyecto. Con la tecnología actual, la información en Internet no suele ser encriptado. Se transmite en una manera clara, lo que significa que es vulnerable a hackers.

Soluciones de seguridad:

La solución principal para la posibilidad de inhalación de datos confidenciales es la educación. Es necesario que actualice su política de seguridad y educar a los usuarios. Se debe tratar a una red pública tal y como tratar las líneas telefónicas no protegidos y los lugares públicos.

- Si la información es lo suficientemente sensible que no lo leería en un autobús o en avión, entonces probablemente no se debería enviar a través de Internet.
- Si la información es confidencial suficiente como para que no lo replique en un teléfono celular, entonces probablemente no se debería enviar a través de Internet.
- Si no desea enviarlo a través del correo normal, excepto tal vez con un doble sobre, entonces probablemente no se debería enviar a través de Internet.
- Considere proporcionar perfiles de usuario independientes para uso de Internet y de correo electrónico, al menos para los usuarios con perfiles de gran alcance. De esa manera, si alguien ve un correo electrónico que un empleado envía, el intruso no tendrá el nombre de un perfil de gran alcance en su sistema.

4.11. NIVELES DE SEGURIDAD PARA LA DISPONIBILIDAD BÁSICA DE INTERNET EN EQUIPOS iSeries

Introducción

Este tema proporciona una breve revisión de los niveles básicos de seguridad que trabajan juntos para proporcionar seguridad para equipos iSeries. En este tema se tomara en cuenta los diferentes niveles de seguridad y ofrecer consejos para un buen uso de los mismos y así llegar a satisfacer las necesidades de la organización.

Los niveles de seguridad

Se puede elegir el nivel de seguridad que desee para su sistema, para mantener de mejor manera la integridad de datos y de la red, mediante el establecimiento de nivel de seguridad QSECURITY valor del sistema. El sistema ofrece cinco niveles de seguridad los cuales se detallaran a continuación:

Nivel 10:

El sistema no aplica ningún tipo de seguridad. No es necesaria ninguna contraseña. Y proporciona a los usuarios acceso para todos los recursos.

Es importante tomar en cuenta que si el sistema se encuentra actualmente en el nivel de seguridad 10, y si cambia el nivel de seguridad a algún otro nivel superior, no podrá cambiar nuevamente al nivel 10. Debido a que el nivel 10 no proporciona ninguna protección de seguridad, la seguridad nivel 10 no es recomendado por IBM.

IBM no proporcionará el apoyo a los problemas que se producen a nivel de seguridad 10 a menos que el problema también se pueda crear en un nivel de seguridad mayor.

Nivel 20:

El sistema requiere un ID de usuario y la contraseña para iniciar la sesión. El nivel de seguridad 20 se refiere a menudo como el inicio de sesión predeterminado security.By, y si todos los usuarios tuvieran autorización *ALLOBJ. Estos usuarios tendrían acceso a los objetos que deseen.

Nivel 30:

El sistema requiere un ID de usuario y la contraseña para iniciar la sesión. Este nivel también es conocido como la seguridad de los recursos. Porque los usuarios deben tener autoridad para utilizar objetos ya que los usuarios no tienen ninguna autoridad por predeterminado.

Nivel 40:

El sistema requiere un ID de usuario y la contraseña para iniciar la sesión. Además seguridad de recurso, el sistema proporciona función de protección de integridad.

Funciones de protección de integridad, tales como la validación de los parámetros de interfaces con el sistema operativo, están destinados a proteger tanto al sistema y los objetos del sistema de manipulación por parte de usuarios del sistema experimentados. Para la mayoría de las instalaciones, y se recomienda el nivel de seguridad 40. Cuando se recibe un nuevo sistema iSeries con V4R5 o con versiones posteriores, el nivel de seguridad se establecido en 40.

Nivel 50:

El sistema requiere un ID de usuario y la contraseña para iniciar la sesión. En este nivel de seguridad el sistema impone tanto la seguridad de los recursos y la protección de la integridad de nivel 40, pero añade protección de integridad mejorada, como la restricción de manejo de mensajes entre los programas del estado del sistema y los programas del estado del usuario. Este nivel de seguridad 50 está diseñado para sistemas iSeries con altos requisitos de seguridad.

Las medidas de seguridad del sistema representan la última línea de defensa contra un problema de seguridad relacionado con Internet. Debe realizar las siguientes acciones para garantizar que la seguridad del sistema cumple los requisitos mínimos:

- “Establezca el nivel de seguridad (valor QSECURITY del sistema) en 50. El nivel de seguridad 50 proporciona el máximo nivel de protección de la integridad, que es lo recomendable para proteger el sistema en entornos de alto riesgo como Internet.
  Nota: Si se está ejecutando un nivel de seguridad menor que 50, es posible que tenga que actualizar los procedimientos de funcionamiento o las aplicaciones. Debe consultar la información de la publicación, iSeries Security Reference antes de pasar a un nivel de seguridad mayor.

- Configure los valores del sistema relacionados con la seguridad para que sean al menos tan restrictivos como los valores recomendados. Puede utilizar el Asistente de seguridad de iSeries Navigator para configurar los valores de seguridad recomendados.
- Asegúrese de que ninguno de los perfiles de usuario, ni siquiera los suministrados por IBM, tenga contraseñas por omisión. El mandato ANZDFTPWD (Analizar contraseñas por omisión) le permitirá comprobar si tiene contraseñas por omisión.
- Utilice la autorización sobre objeto para proteger los recursos importantes del sistema. Aplique un enfoque restrictivo en el sistema. Esto es, restrinja por omisión a todos los usuarios el uso (PUBLIC *EXCLUDE) de recursos del sistema como las bibliotecas y los directorios. Autorice solamente a algunos usuarios a acceder a los recursos restringidos. La restricción del acceso mediante menús no es suficiente en un entorno de Internet.
- Debe configurar la autorización sobre objeto en el sistema."[4]

4.11.1. Nivel de seguridad según el sistema de valores.

Este valor del sistema le permite establecer el nivel de seguridad para el sistema. Este ofrece cinco diferentes niveles de seguridad. Cada uno de estos niveles de seguridad de proporcionar controles de seguridad específicos para el sistema. En función de las decisiones que tomó en la política de seguridad, puede seleccionar un nivel de seguridad que usted necesita.

IBM envía todos los nuevos sistemas con el nivel de seguridad 40, que proporciona un alto nivel de seguridad que es necesario para la mayoría de las instalaciones. No se recomienda que cambie el nivel de seguridad en un nuevo sistema más bajo que este valor. A pesar de que IBM recomienda mantener los sistemas en el nivel 40, los valores más bajos se describen para proporcionar una comparación función por función entre cada nivel de seguridad.

[4] iSeriesInformation Center, Versión 5 Release 4

Nivel de seguridad	Descripción de series de navegadores
10 (sin seguridad)	No se necesitan contraseñas y los usuarios tienen la autoridad para todos los recursos
20 (baja seguridad o relajado)	Las contraseñas son necesarios y los usuarios tienen la autoridad de todos los recursos
30 (seguridad media o promedio)	Las contraseñas son necesarios y acceso de los usuarios se basa en su autoridad
40 (alta seguridad o estricto)	Proteger de las interfaces del sistema indocumentados
50 (alta seguridad o estricto)	Mejorar la protección de las interfaces del sistema

Tabla #4.
Autor: Freddy Vargas.
Comparación entre los diferentes niveles de seguridad,
Sobre la Descripción de series de navegadores

Nivel de seguridad	Funciones permitidas
10 (sin seguridad)	Proporcionar a los usuarios acceso *ALLOBJ para todos los objetos.
20 (baja seguridad o relajado)	Proporciona a los usuarios acceso * ALLOBJ para todos los objetos. El nombre de usuario debe iniciar la sesión. Se requiere una contraseña para iniciar la sesión. Contraseña de seguridad activo. Menú inicial y programa de seguridad activo. Capacidades de auditoría de seguridad disponibles. Los programas que contienen instrucciones restringidas no se pueden crear o compilar. * USRSPC, USRIDX *, y * USRQ objetos sólo se pueden crear en las bibliotecas especificadas en el valor del sistema QALWUSRDMN.

30 (seguridad media o promedio)	Permite realizar las mismas funciones del nivel de seguridad 20.
40 (alta seguridad o estricto)	Permite realizar las mismas funciones que los niveles 20 y 30 además de las siguientes. Los punteros se utilizan en los parámetros son validados por dominio de usuario. Espacio asociado un programa no puede modificarse directamente. Bloques de control interno están protegidos.
50 (alta seguridad o estricto)	Nos permite realizar las mismas funciones del nivel 40

Tabla #5.
Autor: Freddy Vargas.
Comparación entre los diferentes niveles de seguridad,
Funciones permitidas

Nivel de seguridad	Las funciones no permitidas
10 (sin seguridad)	NA
20 (baja seguridad o relajado)	Recursos de seguridad activa. Perfil de usuario creado automáticamente. Los programas que utilizan las interfaces no compatibles darán un error en tiempo de ejecución. Mayor protección de hardware de almacenamiento compatible. Los punteros se utilizan en los parámetros, se validan para los programas de usuario de dominio que se ejecutan en el estado del sistema. Normas de tratamiento de mensajes se aplican entre el sistema y los programas del estado del usuario. Espacio asociado un programa no puede modificarse directamente. Bloques de control interno están protegidos.

30 (seguridad media o promedio)	Permitir el acceso a todos los objetos. Las mismas funciones que del nivel 20.
40 (alta seguridad o estricto)	Permitir el acceso a todos los objetos Perfil de usuario creado automáticamente. Normas de tratamiento de mensajes se aplican entre el sistema y los programas del estado del usuario.
50 (alta seguridad o estricto)	Permitir el acceso a todos los objetos. Perfil de usuario creado automáticamente.

Tabla #6.
Autor: Freddy Vargas.
Comparación entre los diferentes niveles de seguridad,
Las funciones no permitidas.

1. El nivel de seguridad 10 ya no es compatible. Si pasar del nivel de 10 al 20, 30, 40 o 50 no sería recomendable que usted volviera al nivel 10.

2. IBM envía todos los sistemas nuevos con un nivel de seguridad de 40. IBM le recomienda que deje el nivel de seguridad establecido en 40.

3. En el nivel de seguridad 50, no hay bloques del sistema de control interno se puede modificar. En comparación algunos bloques del sistema de control interno se pueden modificar el nivel de seguridad 40. Con relación a su política de seguridad.

4.11.2. Los niveles con relación a la política de seguridad

En su política de seguridad, si bien usted intenta mantener un equilibrio entre la protección de sus bienes, el acceso del usuario y el rendimiento del sistema. Y si el sistema contiene material altamente confidencial o información que comprometería seriamente su negocio si se pierde o es robado, ese sistema requeriría un nivel de seguridad más alto que un sistema que contiene información menos sensible. Además, es posible tener un sistema que está conectado a una red insegura, tal como Internet, y podría ser potencialmente objeto de un ataque. Estos sistemas también necesitan un mayor nivel de seguridad para protegerlos.

Cabe recalcar; que los niveles de seguridad por sí sola no protegen los sistemas conectados a redes inseguras de los ataques. Si usted está planeando para conectarse a Internet o a cualquier otra red insegura, es necesario analizar los riesgos no sólo a su sistema, sino también toda la red.

4.12. OPCIONES DE SEGURIDAD DE LA RED PARA EQUIPOS iSeries o (AS/400).

Cuando se conecta a una red insegura, su política de seguridad debe describir un plan integral de seguridad, incluidas las medidas de seguridad que se implementan a nivel de red. Instalación de un servidor de seguridad es uno de los mejores medios para desplegar un conjunto integral de medidas de seguridad de red.

También, su proveedor de servicios de Internet (ISP) puede y debe proporcionar un elemento importante en su plan de seguridad de la red. Su esquema de seguridad debe describir las medidas de seguridad de su proveedor de servicios de Internet (ISP) que le proporcionará, como las reglas de filtrado para la conexión del router ISP y el servicio público de nombres de dominio (DNS).

Aunque un firewall sin duda representa una de sus principales líneas de defensa en el plan de seguridad total, no debería ser la única, debido a los posibles riesgos para mantener bien seguro el Internet, pueden ocurrir en una variedad de niveles, es necesario establecer medidas de seguridad que proporcionan múltiples capas de defensa contra estos riesgos.

Mientras que un firewall proporciona una enorme cantidad de protección contra ciertos tipos de ataque, Por ejemplo, un servidor de seguridad no necesariamente puede proteger los datos que se envían a través de Internet a con aplicaciones como el correo SMTP, FTP y TELNET, a menos que usted elija para cifrar estos datos, cualquier usuario de Internet puede acceder a él a medida que viaja a su destino.

Debería considerar seriamente utilizar un producto cortafuegos como línea principal de defensa siempre que se conecte el sistema iSeries o su red interna a Internet. Aunque ya no se puede comprar el IBM Firewall para AS/400 y el apoyo

al producto ya no está disponible, hay una serie de otros productos que se pueden utilizar.

Las reglas de filtrado de paquetes también permiten proteger sus sistemas informáticos mediante el rechazo o la aceptación de paquetes IP de acuerdo con los criterios que usted defina. Reglas NAT permiten ocultar la información de su sistema interno de los usuarios externos mediante la sustitución de una dirección IP por otra dirección IP, pública.

Aunque las reglas de filtrado de paquetes IP y NAT son fundamentales las tecnologías de seguridad de red, que no proporcionan el mismo nivel de seguridad que un cortafuegos totalmente funcional hace. Usted debe analizar cuidadosamente sus necesidades y objetivos de seguridad al momento de decidir entre un producto de servidor de seguridad completa y la función de paquete de iSeries reglas.

Cortafuegos

Los firewall protegen la red interna de muchos posibles riesgos relacionados con Internet. Cualquier dispositivo que controla el tráfico de red entre dos redes para la seguridad puede ser llamado un servidor de seguridad. El termino cortafuego se utiliza de una manera genérica.

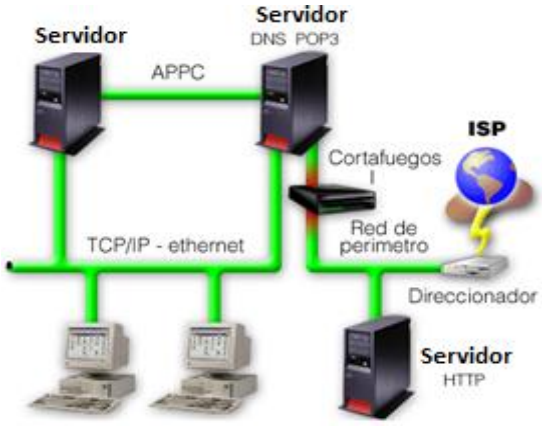


Figura #7.
Copiado de: iSeriesInformation Center, Versión 5 Release 4
Función de un Cortafuegos en una red

Sin embargo, existen tres principalmente tipos de cortafuegos que utilizan diferentes técnicas para la protección de los recursos de red.

Los diferentes tipos de cortafuegos

La mayoría de los dispositivos de firewall se construyen en los routers y su trabajo es en las capas inferiores de la red. Ellos proporcionan filtrado de paquetes y se llaman a menudo firewalls o routers de red de detección.

Puertas de enlace del servidor proxy en el trabajo capas superiores de la pila de protocolo, hasta la capa de aplicación. Ellos proporcionan servicios proxy en redes externas para clientes internos y realizar una vigilancia avanzada y control del tráfico.

El tercer tipo de firewall stateful utiliza técnicas de inspección.

1. **Cortafuegos de Red o filtrado de paquetes de primera generación.**

Firewalls o routers de red de detección pueden ver la información relacionada con la capa de red y los tipos de conexiones (capa de transporte) y luego proporcionar filtrado basado en esa información. Un servidor de seguridad de red puede ser un dispositivo independiente de enrutamiento o un ordenador con dos tarjetas de interfaz de red (base dual de puerta de enlace). El router conecta dos o más redes y realiza el filtrado de paquetes para controlar el tráfico entre las redes.

Usted puede construir un conjunto de reglas de filtrado de paquetes IP. Los puertos también se pueden bloquear, por ejemplo, puede bloquear todas las aplicaciones excepto los servicios HTTP. Sin embargo, las reglas que se pueden definir para los routers pueden no ser lo suficientemente seguro para proteger los recursos de red.

2. **Cortafuego de Estado de segunda generación.**

Uno de los problemas de la representación es el rendimiento. Se debe evaluar una gran cantidad de información de una gran cantidad de paquetes, y debe instalar un proxy independiente para cada aplicación. Otro tipo de producto cortafuegos utiliza la inspección de estado. En lugar de examinar el contenido de cada paquete, el patrón de bits de los paquetes se compara a los paquetes ya conocidos para ser de confianza.

Eso significa que si accede a algún servidor exterior, el firewall recuerda cosas sobre su solicitud original, como fuente y número de puerto de destino, de origen y dirección de destino.

Cuando el servidor de fuera responde a su solicitud, el cortafuego compara los paquetes recibidos con el estado guardado a determinar si se les permite que se transmitan a la red interna. Un ejemplo, el cortafuegos almacena información sobre una solicitud de conexión saliente (puertos de origen y de destino y las direcciones IP) y comprueba todas las llamadas entrantes respuestas de la Internet si la solicitud correspondiente se inició de un cliente interno.

Si hay una falta de coincidencia en uno de los puertos o direcciones, el paquete se descarta. Si bien la inspección de estado proporciona velocidad y transparencia, una de las mayores desventajas es que los paquetes dentro de su camino a la red exterior exponen a sus direcciones IP internas a la Internet.

Algunos vendedores de firewall utilizan la inspección de estado de proxies o NAT, juntos adicionan seguridad. La combinación de estas funciones también le da la capacidad de ocultar su información de la red interna de Internet.

3. Cortafuego de aplicación de tercera generación.

Un nivel de aplicación de servidor proxy funciona a un nivel superior en la pila de protocolos para vigilar y controlar el acceso entre redes. Un servidor proxy transmite mensajes de los clientes internos a los servicios externos y los cambios de la propiedad intelectual dirección de los paquetes del cliente para ocultar la dirección de cliente IP interna a la Internet y actúa como un agente proxy para el cliente en el Internet.

Hay dos tipos de servidores proxy, pasarelas de nivel de circuito y la aplicación gateways de nivel.

Para el nivel de circuito, un circuito virtual existe entre el cliente interno y el servidor proxy. Las solicitudes de Internet pasan por el servidor proxy, y el servidor proxy proporciona estas peticiones a la Internet después de cambiar la dirección IP.

Los usuarios externos sólo ven la dirección IP del servidor proxy. Las respuestas son recibidos por el servidor proxy y enviado de vuelta al cliente. Los sistemas externos nunca ven el sistema interno y la dirección IP del sistema. Cuando los paquetes de Internet llegar a la puerta de entrada, se comprueban y evalúan para determinar si la política de seguridad permite que el paquete entran en el red interna. El servidor no sólo evalúa la dirección IP, sino que también mira los datos de los paquetes para detener los piratas informáticos de ocultar información en los paquetes.

Una puerta de enlace de nivel de aplicación típica puede proporcionar servicios de proxy para aplicaciones y protocolos como Telnet, FTP, HTTP y SMTP.

Tenga en cuenta que para cada aplicación de un servidor proxy independiente debe estar disponible con proxy, las políticas de seguridad pueden ser mucho más potentes y flexibles, ya que toda la información en paquetes pueden ser utilizados para escribir las reglas que determinan cómo se manejan los paquetes.

Funciones y tareas de un corta fuego

Un firewall proporciona una barrera que controla el flujo entre redes, normalmente utilizado entre la empresa (segura) y la red de Internet (red no segura). El servidor de seguridad es también un punto de control donde se puede controlar todo el tráfico entre las redes.

Permite que el tráfico interno fluya de forma segura desde la red interna a la red externa, mientras que la protección de los hosts internos de ataques externos, permite selectivamente el tráfico externo para llegar a servidores específicos internos. Estas dos funciones a menudo están en conflicto entre sí. En esta sección se describen las funciones utilizadas para realizar esta tarea.

Los servidores proxy

Un servidor proxy es una aplicación de TCP. Su propósito es recibir las solicitudes de un cliente y volver a enviarlos a un servidor. También vuelve a enviar la respuesta desde el servidor al cliente. Con el fin de mantener el estado de la información de modo que pueda enviar las respuestas de vuelta al cliente apropiado. Los servidores proxy son únicos para el protocolo particular.

Por lo tanto es necesario utilizar diferentes servidores proxy para diversas aplicaciones, por ejemplo, Telnet proxy, proxy HTTP, y así sucesivamente. En el servidor proxy también se puede romper la conexión TCP/IP y podría esconderse informaciones internas de la red.

Los servidores proxy normalmente también proporcionan funciones de caché. Por ejemplo, en el caso de un proxy HTTP del servidor proxy almacena en caché las páginas HTTP. Si otro cliente hace la peticiones a la red interna de una página web que ya está en la memoria caché, la página se libra de la caché en lugar de volver a cargar desde Internet.

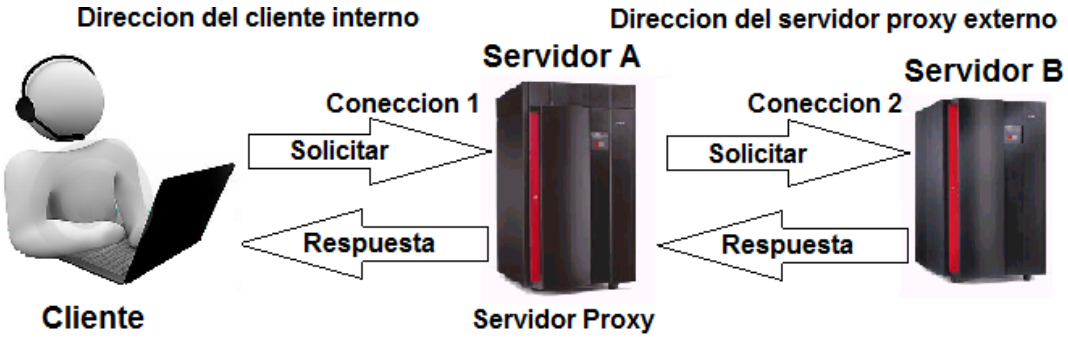


Figura #8.
Autor: Freddy Vargas
Funcionamiento de un servidor Proxy

Sistema de nombre de dominio (DNS).

El sistema de nombres de dominio (DNS) del servidor, este impide que los usuarios fuera de la red puedan ver las direcciones de los hosts de la red privada, mientras que ayudan a los anfitriones en la solución de seguridad las direcciones de los servidores de la red no segura (Internet). Desde el punto de vista exterior, el servidor de nombres en el servidor de seguridad sólo se conoce y nunca se da información sobre los nombres dentro de la red privada. Desde el punto de vista interior, este servidor de nombres conoce la red Internet y es útil para acceder a cualquier host en Internet por su nombre.

Un servidor DNS interno es el que envía peticiones DNS para nombres de terceros en el firewall DNS, que a su vez remite la solicitud a una raíz del dominio de servidor de Internet o el nombre del servidor ISP, también se llama un DNS dividido.

Traducción de dirección de red (NAT)

Traducción de Dirección de Red (NAT), es una alternativa al proxy o SOCKS.

NAT traduce direcciones IP de cliente, direcciones IP dinámicamente a público registrado. La NAT permite que el servidor de seguridad pueda ocultar las direcciones IP de los hosts en la red segura. También puede utilizar NAT para acceder a un host en una red segura desde una red no segura (Internet) mediante la asignación de una dirección IP pública frente a la dirección IP privada de ese host específico.

Hay básicamente dos tipos de traducción de direcciones:

- Ocultación (enmascaramiento).- Este método de NAT traduce una o muchas direcciones internas IP de host a una dirección IP registrada única en la red no segura. La función de NAT asigna para cada solicitud de salida de un puerto de origen diferente y asigna las nuevas respuestas a los clientes originales, las Dirección IP y el puerto.
  La ocultación de NAT no se puede utilizar para conexiones de entrada para acceder a un servidor de correo o web servidor detrás del firewall.

- El enfoque estático Static NAT.- Se utiliza sobre todo para conexiones que requieren una dirección IP fija, asignan la dirección IP registrada para la dirección interna y viceversa.
  Esto es típicamente necesario para acceder a los recursos detrás del firewall desde Internet. Hay diferencia en la implementación en los productos de proveedores diferentes. Básicamente, usted puede realizar un NAT estático para todos los puertos de una dirección o para un único puerto.

  Por ejemplo, si usted proporciona el acceso de los usuarios de Internet a un servidor Web detrás del servidor de seguridad, debe utilizar una asignación de puerto estático para el puerto 80 (HTTP) y 443 (HTTPS) en lugar de mapear todos puertos de la interfaz no segura a la correspondiente una en la red segura.

Red privada virtual (VPN)

Una red privada virtual (VPN) se puede utilizar para extender de forma segura a redes corporativas a través de Internet a las oficinas remotas y usuarios. VPN proporciona al usuario autentificación, encriptación de datos y la integridad de datos para garantizar la seguridad de los mismos, mientras están en tránsito a través de redes privadas y de Internet.

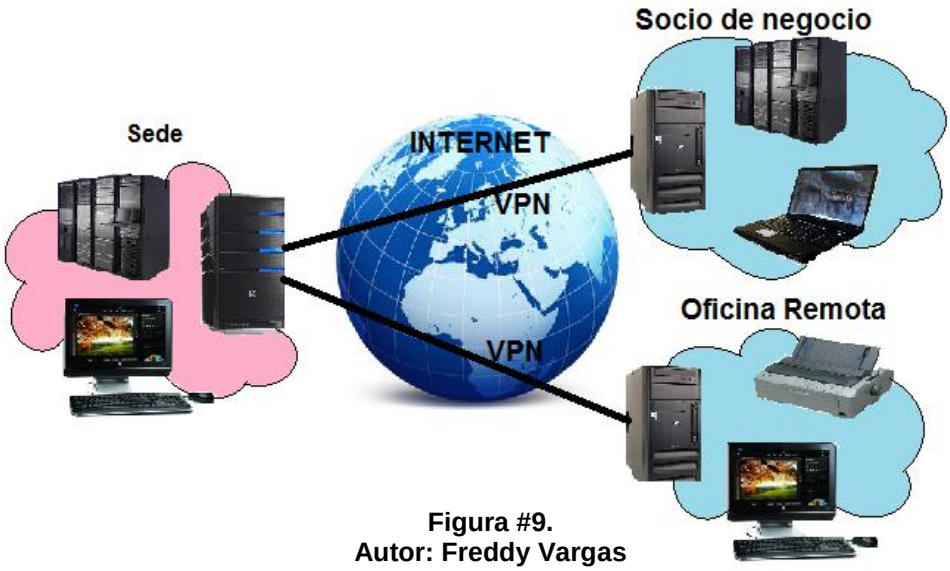


Figura #9.
Autor: Freddy Vargas
Funcionamiento de una VPN

Supervisión y registro

Supervisión y registro es importante para mantener un registro del tráfico entre la red segura y no segura. Mayormente el registro no atrapa una intrusión como usualmente debe suceder, pero los registros son una herramienta útil para descubrir los daños que fueron hechos y lo que otros sistemas pudieron haber sido comprometidos. También puede utilizar la información para evitar una intrusión de la próxima vez.

El registro también puede proporcionar información valiosa sobre su e-business clientes. Por ejemplo, si usted registra todas las peticiones HTTP que son realizadas desde Internet a su servidor Web, se obtiene información sobre qué páginas se solicitan con más frecuencia, lo que el navegador utiliza en los clientes para acceder a su servidor, y así sucesivamente. Por supuesto, el registro puede tener un gran impacto en el

rendimiento del firewall. Por lo tanto se recomienda encender sólo las capacidades de registro que son absolutamente necesario.

Proxy server

El sistema AS/400 tiene una función de proxy nativo incluido en su Web de servidores HTTP. Este proxy soporta HTTP, HTTPS, FTP, Gopher y las conexiones, por lo que cubre casi las mismas funciones de proxy como el Firewall IBM para AS/400. Cuando el producto hace un nuevo servidor de seguridad no tiene un proxy integrado que es una buena idea de utilizar el servidor proxy de AS/400 nativo, ya que está disponible en su Sistema AS/400 sin ningún coste adicional.

Algunas de las ventajas del uso de un servidor proxy nativo e AS/400:

- Puede actuar como un portero seguro, la gestión de las sesiones HTTP entre la red interna y servidores de Internet, sin comprometer la seguridad.
- Cuando se configura como un proxy caché, el caché del servidor proxy devuelve Páginas Web de las peticiones que se hacen por todos los usuarios del servidor proxy. En consecuencia, cuando los usuarios solicitan una página, el servidor proxy comprueba si la página está en la caché. Si lo está, el servidor proxy devuelve la página en caché. El servidor proxy es capaz de brindar páginas web más rápido, que a eliminar potencialmente peticiones de servidor web de internet. Las ventajas de rendimiento de una memoria caché son más significativas si los usuarios tienden a solicitar las mismas páginas Web de Internet, y si el vínculo a la ISP es relativamente lento.
- El servidor proxy proporciona excelentes servicios de registro. Se puede registrar toda la URL las solicitudes de seguimiento de uso.
- Las solicitudes de registros del servidor proxy que se cumplieron desde el caché. Este registro ayuda a entender cómo efectivamente la memoria caché se está utilizando.
- Puede registrar los hosts internos, tienen acceso a varios sitios web a través de su servidor proxy o AS/400.

- Puede ser configurado para requerir autenticación de usuario antes de permitir el acceso a la Internet.
- Se puede configurar para delimitar los sitios que pueden acceder a los usuarios a través del servidor proxy.
- Desvío de IP que no tiene por qué estar habilitadas en su seguridad AS/400, puerta de enlace.

Desventajas utilizando el servidor proxy en el sistema AS/400

En realidad, no hay muchas desventajas. Las desventajas más relevantes son:

- La utilización de tamaño del sistema AS/400 puede tener un efecto negativo impacto en el rendimiento del servidor proxy. El servidor proxy depende de la aplicación. Por lo tanto, siempre hay que comprobar si el servidor proxy de su elección apoya la aplicación deseada. El servidor HTTP Proxy para AS/400 soporta HTTP, HTTPS, FTP y Gopher.

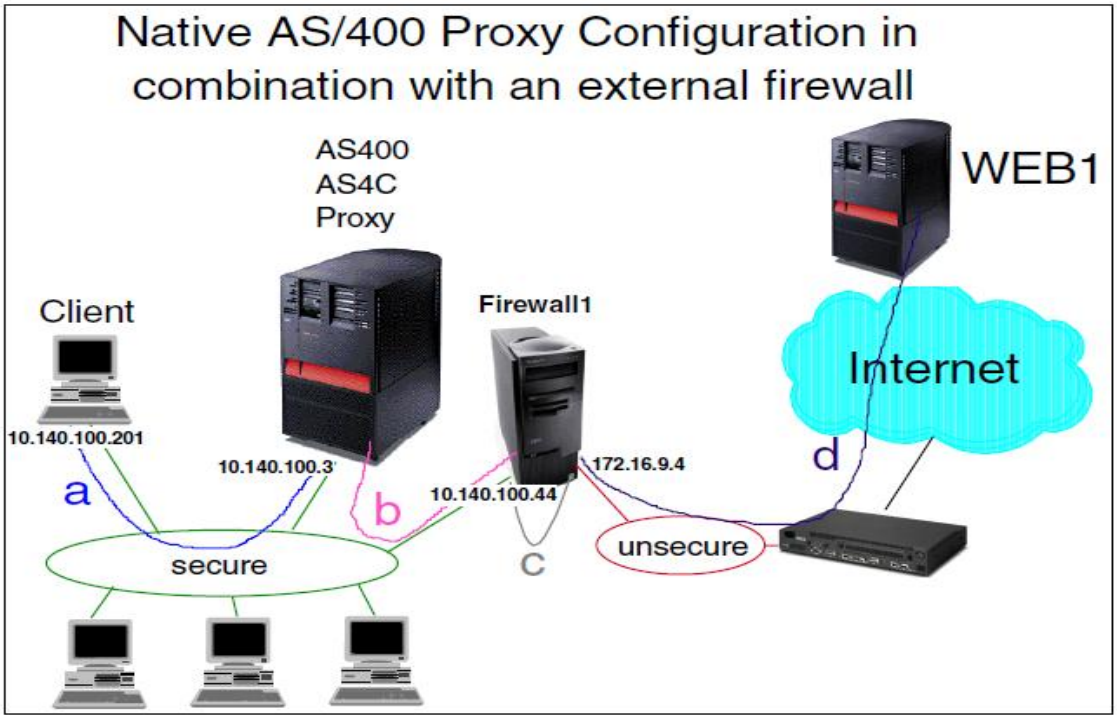


Figura #10.
Copiado de: iSeriesInformation Center, Versión 5 Release 4
Este grafico muestra nuestro escenario con un AS/400 nativo proxy HTTP y NAT en el cortafuegos.

Para obtener una mejor comprensión de cómo el servidor proxy trabaja en el sistema AS/400, se describe el flujo de una solicitud de cliente interno a un servidor Web.

a. Web1 en Internet: El cliente interno con la dirección IP 10.140.100.201 envía una solicitud para el proxy en AS4C (10.140.100.3) en la que el cliente solicita una página Web de la web1 servidor de Internet.

b. El proxy HTTP interrumpe la conexión de TCP y envía una nueva petición para Firewall1 (10.140.100.44). Firewall1 recibe la solicitud de la dirección IP 10.140.100.3. Esto significa que el firewall no sabe nada acerca del cliente que originó la petición.

c. Firewall1, que recibió la petición por traducir recibió una interfaz segura de la dirección IP 10.140.100.3 AS4C, utilizando NAT a una IP virtual frente a la interfaz no segura 172.16.9.4.

d. Web1 recibe la solicitud de la dirección IP 172.16.9.4. Web1 nunca ve una dirección IP de origen de 10.140.100.3. La respuesta del servidor Web1 va a través de las mismas traducciones en el camino de vuelta al cliente solicitante.

Traducción de direcciones de red (NAT) o Filtrado de paquetes IP

Debido a que el filtrado de NAT e IP son partes integrantes de su OS/400, proporcionan una forma económica para que usted pueda proteger sus datos personales. En algunos casos, estas tecnologías de seguridad pueden proporcionar todo lo necesario sin compras adicionales. Estas tecnologías, sin embargo, no crean un servidor de seguridad verdadero, funcional. Puede utilizar la seguridad de paquete IP por sí sola o en combinación con un servidor de seguridad, en función de sus necesidades y objetivos de seguridad. Nota: No se debe tratar de tomar ventaja de los ahorros de costes si usted está planeando para asegurar un sistema de producción de iSeries. En situaciones como ésta, la seguridad de su sistema debe tener prioridad sobre el costo. Para asegurarse de que proporcionen la máxima protección para su sistema de producción, debe considerar el uso de un firewall.

¿Qué es NAT y filtrado de paquetes IP y cómo trabajan juntos?

Traducción de direcciones de red (NAT) cambia la fuente o las direcciones IP de destino de los paquetes que fluyen a través del sistema. NAT ofrece una alternativa más transparente para el proxy y servidores SOCKS de un firewall.

NAT también puede simplificar la configuración de la red por la habilitación de redes incompatibles con las estructuras de direccionamiento para conectar el uno al otro. Por lo tanto, puede utilizar las reglas de NAT para que el sistema iSeries pueda funcionar como una pasarela entre dos redes que tienen esquemas de direccionamiento conflictivos o incompatibles.

También puede utilizar NAT para ocultar las direcciones IP reales de una red de forma dinámica la sustitución de uno o más direcciones de los reales. Debido a que el filtrado de paquetes IP y NAT se complementan entre sí, a menudo los utilizan en conjunto para mejorar la seguridad de la red.

Uso de NAT

También puede hacer que sea más fácil de operar un servidor web público detrás de los cortafuegos. Las direcciones IP públicas para el servidor web para traducir direcciones IP privadas internas. Esto reduce el número de direcciones IP registradas que son requeridos y minimiza a la red existente. También proporciona un mecanismo para que los usuarios internos accedan a Internet al mismo tiempo ocultar las direcciones IP internas privadas.

Filtrado de paquetes IP

Proporciona la capacidad de bloquear de forma selectiva o proteger el tráfico IP basado en la información en las cabeceras de los paquetes. Puede utilizar el Asistente para la instalación de Internet en Operations Navigator para configurar rápida y fácilmente reglas básicas de filtrado para bloquear el tráfico de red no deseado.

Puede utilizar filtrado de paquetes IP para hacer lo siguiente:

Crear un conjunto de reglas de filtrado para especificar qué paquetes IP puede permitir el acceso a la red y a quienes se le niega el acceso a la red.

Al crear reglas de filtrado, se las aplica a una interfaz física (por ejemplo, un anillo Token o una línea Ethernet). Puede aplicar las reglas a múltiples interfaces físicas, o puede aplicar reglas diferentes para cada interfaz.

Reglas para permitir o denegar paquetes específicos que se basan en la información de cabecera:

- Dirección IP de destino
- IP de origen, Dirección de protocolo (por ejemplo, TCP, UDP)
- Puerto de destino (por ejemplo, es el puerto 80 para HTTP)
- Puerto de origen
- Dirección IP datagrama (entrante o saliente)

Impedir el tráfico innecesario o indeseable de alcanzar las aplicaciones en el sistema. Además, puede evitar que el tráfico de reenvío a otros sistemas. Esto incluye el nivel bajo de los paquetes ICMP (por ejemplo, paquetes PING).

Se debe especificar si una regla de filtro crea una entrada de registro con información sobre los paquetes que coincidan con la regla en un diario del sistema. Una vez que la información se escribe en un diario del sistema, no se puede cambiar la entrada de registro. En consecuencia, el registro es una herramienta ideal para la actividad de auditoría de red.

Seguridad de red de iSeries

Son redes de soluciones de seguridad que protegen el acceso no autorizado generalmente se basan en tecnologías de firewall para proporcionar la protección. Para proteger su sistema iSeries 400, puede optar por utilizar una capacidad completa de productos de firewall o usted puede elegir para poner en práctica las tecnologías específicas de la red de seguridad como parte de la aplicación OS/400 TCP/IP. Esta aplicación consiste en la función de las reglas de paquetes (que incluye el filtrado de IP y NAT) y HTTP para iSeries función del servidor proxy.

La elección de utilizar la característica de reglas de paquetes o un firewall depende del entorno de red, los requisitos de acceso y las necesidades de seguridad. Debería considerar seriamente utilizar un producto cortafuegos como línea principal de defensa siempre que se conecte el sistema iSeries, o su red interna a Internet o a otra red insegura.

En este caso un servidor de seguridad es preferible debido a que un servidor de seguridad es típicamente un hardware dedicado y de software del dispositivo con un número limitado de interfaz para el acceso externo. Al utilizar las tecnologías OS/400 TCP/IP para la protección del acceso a Internet está utilizando una plataforma informática de uso general. La diferencia es importante por una serie de razones. Por ejemplo, un producto de servidor de seguridad no proporciona otras funciones o aplicaciones más allá de aquellos que comprenden los propios cortafuegos.

En consecuencia, si un atacante elude el firewall y accede al mismo, el atacante no puede hacer mucho. Considerando que, si un atacante evita las funciones de seguridad de TCP/IP en el iSeries, el atacante podría tener acceso a una variedad de aplicaciones útiles, servicios y datos. El atacante puede utilizar esto para causar estragos en el sistema o para obtener acceso a otros sistemas de la red interna.

Por lo tanto, cada vez es aceptable utilizar el TCP iSeries. Al igual que con todas las opciones de seguridad que usted hace, usted debe basar su decisión en el costo versus beneficio concesiones que está dispuesto a hacer. Debe analizar sus objetivos de negocio y decidir qué riesgos está dispuesto a aceptar en comparación con el costo de cómo garantizar la seguridad para minimizar estos riesgos.

En la siguiente tabla se proporciona información acerca de cuándo es apropiado usar TCP/IP de seguridad frente a un dispositivo de cortafuegos totalmente funcional. Se puede utilizar esta tabla para determinar si debe utilizar un servidor de seguridad, TCP/IP de seguridad, o una combinación de ambos para proporcionar a su red y la protección del sistema.

La tecnología de seguridad	Mejor uso de OS/400 TCP/IP tecnología	Mejor uso de un cortafuegos totalmente funcional
Filtrado de paquetes IP	Para proporcionar protección adicional para un solo sistema iSeries, como por ejemplo un servidor web público o un sistema de intranet con datos sensibles. Para proteger una subred de una intranet corporativa cuando el sistema iSeries está actuando como una puerta de enlace (router casual) para el resto de la red. Para controlar la comunicación con una pareja algo de confianza en una red privada o extranet donde el sistema iSeries está actuando como una puerta de enlace.	Para proteger una red corporativa a través de Internet u otra red que no se confía en que la red está conectada. Para proteger una subred grande con tráfico pesado desde el resto de una red corporativa.
Traducción de direcciones de red (NAT	Para activar la conexión de dos redes privadas incompatibles con las estructuras de direccionamiento. Para ocultar las direcciones en una subred de una red menos fiable.	Para ocultar las direcciones de los clientes que acceden a Internet o una red no confiable. Para utilizar como alternativa a los servidores proxy y SOCKS. Para que los servicios de un sistema en una red privada disponible para los clientes a través de Internet.
Servidor proxy	Para proxy en lugares remotos en una red corporativa cuando un servidor de seguridad central proporciona acceso a Internet.	Para apoderado de una red corporativa cuando se accede a Internet.

Tabla #7.
Autor: Freddy Vargas.
Comparación entre los diferentes tipos de seguridad.
Sobre tecnología y cortafuegos.

Conclusiones.

En conclusión se puede decir que existen muy buenas razones para implementar un servidor AS/400 en empresas grandes, desde su aparición en el mercado en el año de 1988 estos equipos fueron diseñados para ofrecer un verdadero valor a los compañías, proporcionando confiabilidad, seguridad y una excepcional potencia; veinticuatro horas al día, siete días a la semana, los 365 días del año con un margen de fallo de 0.99 %, con esto presente se puede decir que el AS/400 proporciona poder y control sin límites para ayudar a las empresas a mantenerse al frente del competitivo mundo de hoy en día.

Hoy en día la competitividad mundial es muy amplia por lo que podemos decir que, ninguna empresa es igual a otra por lo mismo ningún cliente es idéntico al otro y en si cada expectativa va a ser muy diferente a otra. Por eso cabe recalcar que cada empresa necesita un servidor distinto que sea capaz de ayudarlo a llevar un negocio con un único objetivo, los de cada organización. Debe ser un servidor flexible y versátil, fácil de administrar y con menos personal para mantenerlo funcionando con esto nos permite ahorrar los salarios de tres o cuatro personas lo cual no se puede hacer con otros servidores del mercado.

Con otros servidores tradicionales se requiere pagar a más personal o a costosos consultores especializados en cierta rama como seria la instalación y el cómo interactuar con el resto de piezas del software.

Las empresas que están equipadas con servidores con NT y Unix necesitan administradores de base de datos para gestionar como y donde se almacenen los datos, como recuperar y mantener una buena seguridad sin quebrantar su integridad y mantener un buen funcionamiento lo que ocasionar que se de deba pagar salarios elevados. Al contrario con un AS/400 no se necesita de mucho recurso humano, porque el sistema operativo realiza todas estas tareas.Es decir el AS/400 reduce los costes en infraestructura de cualquier organización generando beneficios.

Recomendaciones

Es recomendable la consideración del presente trabajo de investigación previo a la realización de una planificación de las seguridades en internet para servidores AS/400, ya que contempla generalidades de cómo realizar una planificación en las seguridades en Internet para servidores AS/400 y se puede poner en práctica, a más de esto la importancia y consideraciones sobre el ciclo del control y la finalidad de realizar el mismo.

Bibliografía

- iSeriesInformation Center, Versión 5 Release 4
- http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica
- http://www.certsuperior.com/SeguridadInternet.aspx
- http://es.wikipedia.org/wiki/Modelo_TCP/IP
- iSeriesInformation Center, Versión 5 Release 4
- http://www.mastermagazine.info/termino/6907.php
- http://es.wikipedia.org/wiki/Ping

Anexos

Anexo 1: Encuesta realizada.

Universidad Tecnológica Israel

Encuesta sobre la planificación de las seguridades en internes para servidores AS/400

Cargo:_____.

PREGUNTA	SI	NO
2. Cree usted importante una buena planificación de seguridades en internet para los equipos AS/400		
7. En su empresa existe algún tipo de planificación para mantener seguros sus datos en internet.		
(Si responde afirmativamente la pregunta 2, califique con buena, muy buena, excelente si es tan fiable la planificación en su empresa) _____		
8. ¿En su empresa tienen un PLAN DE SEGURIDAD que contemple la disponibilidad de internet en el servidor AS/400?		
9. ¿El plan o mecanismo de seguridad que utiliza para la disponibilidad de internet es factible?		
10. Para mantener un servidor AS/400 funcionando se requiere de del mismo número de personas que para un servidor tradicional no IBM		
11. Indique un aproximado del presupuesto que su empresa ahorra al usar los servidores AS/400.	**$:_____**	

Anexo 2: Definición de tesis de grado.

Tema: Estudio de las seguridades en Internet para servidores iSeries.

1. **¿Cuál es el problema?**

El principal problema es la falta de conocimiento e información que tienen los usuarios al momento de destinar el uso del internet utilizando equipos iSeries, de no controlar las distintas opciones de conexión de los sistemas a Internet esta será vulnerable para cualquier usuario que podría intervenir en nuestra red y robar o dañar información muy importante de nuestra organización o empresa que disponga del iSeries.

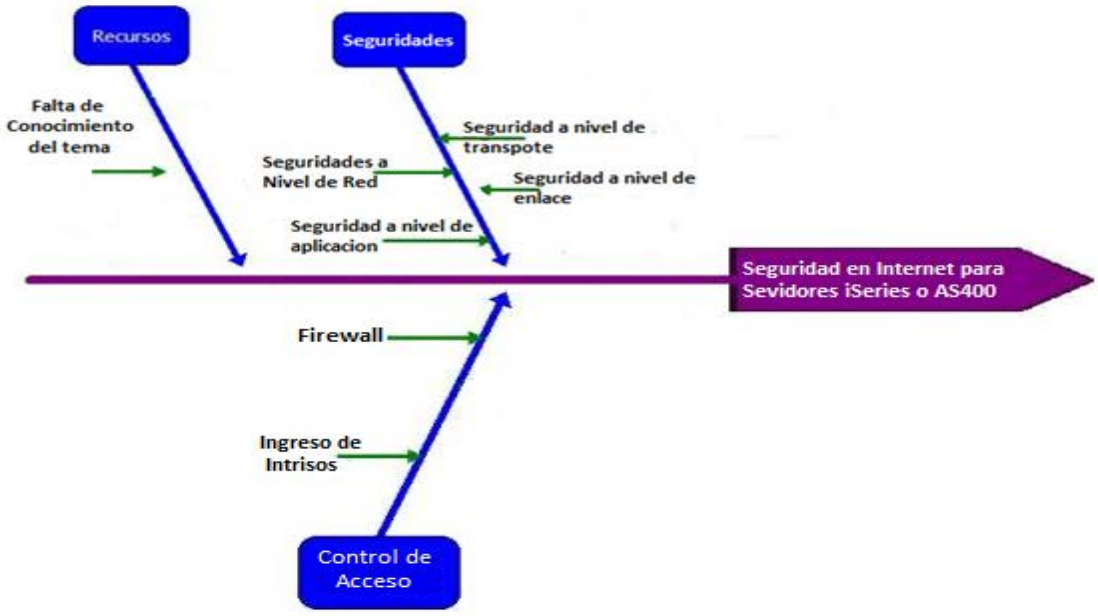
Problemas:

- Recursos
    1. Falta de conocimiento del tema.

- Seguridades
    1. Seguridades a Nivel de Red.
    2. Seguridades a Nivel de Aplicación.
    3. Seguridades a Nivel de Trasporte.
    4. Seguridades a Nivel de Enlace.

- Control de Acceso
    1. Firewall
    2. Ingresos de Intrusos.

Diagrama causa efecto.



2. ¿Por qué es importante investigar sobre el tema?

La aplicación de medidas de seguridad en las redes supone desplegar diversos productos: sistemas de detección de intrusos, y esto que en muchos casos controles de autenticación y autorización, cortafuegos y otros servicios. Habitualmente la información se encuentra vulnerable a la manipulación de terceras persona (intrusos) y esto que en muchos casos por la falta de conocimiento de las seguridades, según lo antes mencionado se pretende difundir información a los usuarios de estos servidores para que de esta forma tengan mayor responsabilidad en las seguridades de la información de sus empresas.

3. ¿Qué se conoce al respecto dentro y fuera del país (Referencias Comprobables)?

A nivel internacional los servidores iSeries (AS400) son bien utilizado y existen muchos profesionales Ing. En Sistemas especializados en estos servidores, a continuación se presenta un link de un blog creado en Venezuela que nos dice que se puede pedir el acceso un servidor AS400 localizado en Alemania: http://iseriesvenezuela.blogspot.com/2010/07/acesso-gratis-servidor-as400-remoto-en.html

Ing. Sistemas Liliana Suárez. 25 años de Experiencia; Desarrollo de Proyectos a Distancia en plataforma iSeries/AS400; Asesoría, Diagnóstico, Análisis y Optimización de Sistemas; domingo, 18 de julio de 2010.

Y a nivel nacional estos servidores son utilizados únicamente por empresas grandes como en Etapa Cuenca, que lo adquirieron en el año 2008, a continuación un link:

http://www.etapa.net.ec/Empresa/Lists/Contratos%202008/Lectores%20Externos.aspx?Filter=1&FilterField1=Objeto&FilterValue1=Adquisici%C3%B3n%20de%20equipos%20servidor%20iseries&View={7FA4B1DF-B02F-4F6A-B5D8-021831110B84}

4. ¿Por qué lo va hacer?

Al prevenir la intervención de terceras personas a nuestra red se asegura salvaguardar la información con una buena seguridad ya que esta es muy importante para la empresa y es esto la misma radica su éxito. Y con este tema se pretende dar conocimiento a los usuarios y difundir conciencia ya que la importancia de la seguridad en una empresa que le interese presentarse al mundo exterior como confiable, y de esta manera puedan aplicar en el diario vivir en cada una de sus empresas.

5. ¿Cómo lo va a realizar?

Se lo realizara previo a una investigación en donde se reflejara las seguridades en internet para AS/400, esto se pretende realizar mediante cuestionarios y entrevistas a cerca de las seguridades en los servidores iSeries. Se realizara encuestas a profesionales que conozcan del tema.

Análisis de la información recopilada acerca de las seguridades del iSeries y difundirlo a las personas que no sepan sobre el tema.

6. ¿Cuáles son los resultados esperados?

Brindar información sobre las seguridades en internet para servidores iSeries para que de esta forma los usuarios pueda mantener su red e información de sus empresas de una manera segura.

7. ¿Cómo va a transferir y difundir los resultados?

Este trabajo se llevara a cabo mediante una investigación profunda de fácil comprensión y de dominio para los lectores del documento y se plantea transferir y difundir mediante redes sociales y blogs a empresas que tengan servidores iSeries.

8. ¿Qué efectos e impactos podrían tener las nuevas tecnologías o los nuevos conocimientos en el grupo objetivo?

Los efectos e impactos que podría tener es difundir los conocimientos de usuarios a cerca de las seguridades en internet para servidores iSeries y de esta forma dar conciencia para que ejerzan responsabilidades.

Anexo 3: Glosario de palabras

A

AS/400: Son equipos de IBM, es un sistema multiusuario.

ANZDFTPWD: Nos ayuda a analizar las contraseñas por omisión.

AIX: Ejecutivo interactivo avanzado, es un sistema operativo de UNIX, propiedad de IBM y corre en servidores IBM.

APPS: Plataforma de desarrollo para información empresarial.

Anillo Token: Es una arquitectura de red desarrollada por IBM, es una topología típica en anillo.

ADDTCPRTE: Línea de comando para abrir la pantalla para la configuración de una ruta por omisión.

AUTOSTART * YES:Se arrancan los servidores y las interfaces TCP/IP

ALLOBJ: Proporcionar a los usuarios acceso para todos los objetos.

B

Business Partner: Es una entidad comercial,

C

CL: Lenguaje de control.

CFGTCP: Comando para acceder al menú de Configurar TCP/IP

CRTLINETH:Línea de comando para acceder al panel de control de solicitud crear desc línea (Ethernet)

CHGTCPA:Línea de comando para acceder a la pantalla cambiar atributos TCP/IP

CHGTELNA AUTOSTART (* NO): Comando para evitar que TELNET se inicie automáticamente

D

DB2/400: Es una marca comercial propio de IBM la cual comercializa sistemas de gestión de base de datos.

DNS: Sistema de nombre de dominio.

DFTROUTE: Proyectar tener la tabla de direccionamientos definida de forma que siempre exista una entrada, como mínimo una ruta por omisión

DLO:objetos de biblioteca de documentos.

E

Ethernet: Es un estándar de redes de área local para computadores, es una técnica usada en redes Ethernet para mejorar sus prestaciones.

EZ-Setup: Asistente de configuración para TCP/IP.

F

Filtrado IP: Es un mecanismo que decide qué tipos de datagramas de IP serán procesados normalmente y cuáles serán descartados. Por descartados se entiende que el datagrama se elimina y se ignora completamente, como si nunca se hubiera recibido.

Filtrado NAT: Es un filtrado de paquetes

FTP: Protocolo de transferencia de Archivos.

G

GNU/Linux: Es uno de los términos empleados para referirse a la combinación del núcleo o kernel libre similar a Unix denominado Linux con el sistema operativo GNU

H

HTTP: Protocolo de transferencia de hipertexto.

Hackers: Es una persona que entra de forma no autorizada a computadoras y redes de computadoras, para causar daños a las mismas.

Head quarter: Es una sede, la entidad en la parte superior de una sociedad que asume plena responsabilidad por el éxito general de la empresa.

I

IOSYSCFG: Autoridad especial para restringir quién puede configurar TCP / IP.

IBM i: Este término se refiere a los sistemas operativos I5/OS antes conocido también como OS/400 es un sistema propio de la familia de los servidores AS/400 o iSeries

ISP: Proveedor de Servicios de Internet.

IPV4: Protocolo de internet versión 4.

IPV6: Protocolo de internet versión 6.

I5/OS: Es un sistema operativo robusto usado en los servidores iSeries de IBM.

ICMP: Protocolo de mensaje de control de internet.

iSeriesNavigator: Es la interfaz gráfica de usuario que permite gestionar y administrar el servidor desde el escritorio Windows

J

JustMail: software de correo electrónico

L

LAN: red de área local

M

Microprocesador Power PC: Es el nombre original de la arquitectura de computadoras de tipo RISC (Computador con Conjunto de Instrucciones Reducidas), fue desarrollada porIBM, Motorola y Apple.

Multiusuarios: Se refiere a un concepto de Sistemas Operativos que puede ser utilizado por varios usuarios al mismo tiempo, e incluso se puede referir a otro tipo de programa de computadora de otro tipo como aplicaciones de base de datos.

N

NAT: Traducción de dirección de red.

O

OS/400: Es un sistema operativo utilizado por la línea de microrordenadores AS/400 i también llamado servidores iSeries

OfficeVision: software de correo electrónico.

P

Programa caballo de Troya: Es un virus informático, programa creado y que opera bajo un aspecto inofensivo pero finalmente causa estragos y daños en un equipo.

PUBLIC * EXCLUIDE: Comando para restringir por omisión a los usuarios.

Perfiles PPP: Es un sistema perfilador de competencias personales.

Paquetes PING: Es un buscador o rastreador de paquetes en redes

POP: Protocolo de correo de oficina.

Q

QSECURITY: Hace referencia al nivel de seguridad de los servidores AS/400

QALWUSRDMN: Comando que permite a las bibliotecas del sistema que pueden contener objetos de usuario del dominio.

R

Request: Solicitud de información.

S

Sistem i: Es el sistema de servidores AS/400 anterior al IBM i.

SSL: Capa de sockets segura.

SOCKET: Es un punto final de un enlace de comunicación bidireccional entre dos programas que se ejecutan en la red.

Servidor Proxy: En una red informática, es un programa o dispositivo que realiza una acción en representación de otro, esto es, si una máquina A solicita un recurso a una C, lo hará mediante una petición a B; C

SMTP: Protocolo de transferencia de correo simple.

STRTCP: Inicializa y activa el proceso de TCP/IP

STRTCPSVE: Es el comando para iniciar los servidores TCP / IP.

SLIP: Protocolo de interfaz de línea de serie.

T

TCP/IP: (Protocolo de control de transmisión / Protocolo de Internet); es una denominación que permite identificar al grupo de protocolos de red querespaldan a Internet y que hacen posible la transferencia de datos entre redes de ordenadores.

TELNET: Red de telecomunicaciones,

TCPADM: Comando que Visualiza el menú de administración TCP/IP.

U

UDP:(Protocolo de datagrama de usuario) es un protocolo no orientado a conexión de la capa de transporte del modelo TCP/IP.

UltiMail Lite: Software de correo electrónico.

URL: Localizador de recursos uniformes.

V

VPN: Red privada virtual.

V4R2: Versión del sistema operativo de IBM.

***IOSYSCFG:** Comando para par la configuración de entrada y salida

***USRSPC:** Objeto de usuario de dominio “Espacio de usuario”

***USRIDX:**Objeto de usuario de dominio “Índice de usuario”

***USRQ:** Objeto de usuario de dominio “Cola de usuario”

***ANY *ANY:** comando para entrada en el directorio de distribución del sistema