ULACIT

UNIVERSIDAD LATINOAMERICANA DE CIENCIA Y TECNOLOGÍA

Licenciatura en Ingeniería en Sistemas con

Énfasis en Redes y Sistemas Telemáticos

"Análisis para implementar una DMZ en la red de la Asociación Solidarista de un Ente Público"

Sustentante: Christopher Rojas Morera

Proyecto de graduación para optar por el grado de Licenciatura en Informática

San José – Costa Rica

Mayo 2005

DECLARACION JURADA

Yo Christopher Rojas Morera alumno de la Universidad Latinoamericana de Ciencia y Tecnología (ULACIT). declaro bajo la fe de juramento y consciente de la responsabilidad penal de este acto, que soy el autor intelectual de la Tesis de Grado titulada: "Análisis para implementar una DMZ en la red de la Asociación Solidarista de un Ente Público", por lo que libero a la ULACIT, de cualquier responsabilidad en caso de que mi declaración sea falsa.

Brindada en San José - Costa Rica en el día ____ del mes de _____ del año dos mil _____.

Firma del estudiante: _____

Cédula de Identidad: _____

ULACIT
UNIVERSIDAD LATINOAMERICANA DE CIENCIA Y TECNOLOGÍA

TRIBUNAL EXAMINADOR

Reunido para los efectos respectivos, el Tribunal Examinador compuesto por:

_____
Mauricio Vega Díaz, M.Sc
Director del CIDE

_____
Wilbert Molina, M.Sc
Director de la Escuela de Informática

_____
Claudia Voysest, M.Sc
Tutor

RESUMEN EJECUTIVO

El presente proyecto de graduación tiene, como fin solventar el paradigma, de cómo la implementación de una DMZ podría ayudar a mejorar la seguridad de la red de la Asociación Solidarista de Empleados de un Ente Público.

La Asociación Solidarista, cuenta con diversas dependencias, como lo son: centros de esparcimiento, tiendas, agencia de viajes, entre otros; y a su vez se ha convertido en un ente financiero contable; la Asociación, está levantando el Servicio de 5 páginas de Internet, de cada una de sus empresas, esto primero con el fin de mantener informado a sus asociados; otra razón es también para que el asociado mediante la página de Internet pueda realizar diversas consultas de su estado de cuenta, tramites, reservaciones, e inclusive en el caso de la tienda comercial que posee, poder hacer compras.

La DMZ, es una zona desmilitarizada que parametriza el acceso a los servidores, delimitando las fronteras, tanto el acceso como la salida, marcando la zona donde solo se podrá acceder por medio de la Internet, y como efecto colateral protegiendo el resto de la red interna; también se hace mención de las vulnerabilidades presentes en la red de la Asociación, entre las que sobresale los huecos de seguridad encontrados en los puertos, ya que resultan ser puertas para el ingreso de algún intruso o amenaza. También se destaca que hay ciertas, medidas de seguridad que se deben retomar para restringir los accesos a dicha área.

El proceso de implementación requerirá de diversos elementos para la puesta en marcha, tales como equipos especializados en seguridad (firewall), servidor hosting, personal capacitado que pueda administrar y dar mantenimiento a la DMZ, el cual deberá de ser capacitado en manera constante en cuanto a la seguridad y las distintas amenazas se requiere, ya que siempre hay nuevas y más peligrosas.

De los 23000 asociados, un 80 % tiene conocimientos sobre Internet, a su vez un 89 % se encuentra de acuerdo en reforzar la seguridad de la red de datos de la Asociación, mientras que el 11 % no lo está. De manera curiosa, un 23 % realiza actualmente trámites por Internet, no obstante el 85% del total de la muestra declaró que sí le gustaría realizar diversos trámites con la Asociación por medio de la Internet una vez que se implemente dicho servicio, ya que sería un trámite más rápido, se ahorraría tiempo y dinero, y sería más confidencial y seguro.

Dedicatoria

Dedico este proyecto final de graduación, en primera instancia al Todopoderoso quien me ha dado la fortaleza suficiente para poder seguir adelante, inclusive en los momentos más difíciles,
Ha sido el creador de todas las cosas,
el que me ha dado fortaleza para continuar
cuando a punto de caer he estado ;
a mis padres y hermanas
quienes siempre han sido ejemplo en mi vida,
que con su amor, apoyo y preocupación han estado a mi lado siempre.
Y por último pero no menos importante,
a alguien que ha estado, siempre inquebrantable a mi lado,
dándome todo su apoyo, comprensión y cariño,
hasta quedar rendida en un apacible y profundo sueño,
alguien que le da a la palabra amor y compañía un nuevo significado,
mi alma gemela, Laura.

Agradecimientos

Deseo agradecer también enormemente a la Ing. Claudia Voysest por su apoyo, paciencia y conocimientos brindados durante todo el desarrollo del proyecto de graduación.

También, un agradecimiento muy especial, a todo el personal de la Asociación, por haberme proporcionado muy valiosa información para realizar mi trabajo de tesis.

INDICE

INDICE DE GRÁFICOS

CAPITULO I

INTRODUCCIÓN

"En el mundo de hoy de redes internacionales y correo electrónico, todos los sistemas de cómputo son un objetivo potencial. Se han parado computadoras, se han alterado registros en forma subrepticia, se han insertado "puertas traseras" en los programas normales, se ha copiado información privada sin permiso y se han capturado millones de contraseñas de usuarios despreocupados. Aún así si no se borra o altera nada, los administradores de sistemas han de pasar horas o días reparando y reconfigurando sistemas para recuperar alguna medida de confianza de su integridad. Si antes la seguridad en informática era cuestión de juego ahora ya no lo es".[1]

La seguridad en redes de computadoras actualmente es un tema muy común, debido a la gran importancia que ésta representa en el mundo de la informática, y por ende de todos los sistemas de información que se encuentran en ella; de esta manera, desde las grandes industrias a la vanguardia con la tecnología y los sistemas secretos de gobierno, hasta las pequeñas empresas y los millones de usuarios que dependen de esta, son vulnerables ya sea de manera directa o indirecta a las diferentes amenazas que atentan contra la seguridad de toda esta sistematización.

Hoy por hoy, Internet ha pasado de convertirse en una red de unos cuantos usuarios, en la red con más usuarios del mundo, y este número sigue en aumento.

A menor escala también existen las redes pequeñas o de menor tamaño en las empresas, en estas, varios usuarios se conectan entre si con el fin de

[1] Garfinkel, 1999, p. 3

transmitir datos e información, haciendo uso de diversos recursos, como lo son servidores, estaciones de trabajo, equipo especializado de redes, entre otros.

Las redes “locales” son redes de propiedad privada que se encuentran en un solo edificio o en un campus de pocos kilómetros de longitud[2]. En el mayor de los casos en estas redes, se suele consultar servidores de bases de datos, de los que se extrae la información que se necesita, entonces los administradores de la red tienen como responsabilidad proteger la información que se tiene resguardada en dichos servidores, con el fin de que no sea accesada por cualquier usuario, así como también, que los que la consulten y necesiten la tengan siempre a su alcance.

Ahora bien, ¿qué sucede cuando se desea unir la red más grande del mundo con una red interna?, y aparte a esto se desea que los usuarios puedan acceder a la información desde cualquier parte del mundo a través de una página de Internet.

En este mundo tan competitivo, toda empresa desea formar parte del basto mundo de Internet, facilitando a los usuarios los servicios que ésta brinda.

“Según un informe, del 20 noviembre del 2003, preparado por la Secretaría General de la Conferencia sobre Comercio y Desarrollo de las Naciones Unidas (UNCTAD), sobre el comercio electrónico y el desarrollo; Costa Rica está en el lugar cuarenta y nueve a nivel mundial, sétimo a nivel americano, quinto a nivel latinoamericano, y en lugar primero a nivel regional en cuanto al Índice de Preparación de la Red: (NRI – *Network Readiness Index*) definido como el “grado de preparación de una nación para participar y beneficiarse del desarrollo de las tecnologías de información y comunicación”. En el mundo, los primeros 10 países

[2] Tanenbaum, 2003.

latinoamericanos son: Brasil (lugar 29); Chile (35); Argentina (45); México (47); Costa Rica (49); República Dominicana (57); Colombia (59); Panamá (61); El Salvador (63); y Venezuela (66)."[3]

Todos estos datos e informes indican que Costa Rica, ha disminuido de gran forma la *"brecha digital"* que la separaba de los demás países del mundo; siendo esto una herramienta primordial y de apoyo con miras al progreso de un país en vías de desarrollo; claro está gracias a los esfuerzos que se realicen en todos los sectores productivos de bienes y servicios de la nación. De esta manera, es aquí donde las empresas, organizaciones, asociaciones, entre otros son pilares fundamentales para que esto se realice.

Con respecto a las asociaciones públicas o privadas, éstas se encargan de velar por el ahorro y bienestar de los empleados que laboran en ellas, mediante un conjunto de servicios establecidos para ofrecer una mejor calidad de vida a todos sus asociados.

Esta investigación se realizó en una asociación de un ente público, y debido a que el tema hace referencia a la seguridad de una empresa en específico, y por recomendación de terceros, no se hace mención del nombre completo del lugar en donde se elaboró la tesis, por lo que se identificará como Asociación de Empleados de un Ente Público. Según la base de datos de dicha institución, ésta cuenta actualmente con un aproximado de casi 23.000 asociados, los cuáles pueden hacer uso de diversos servicios tales como: financiero, crédito, vivienda entre otros. En las Oficinas Centrales, se encuentran laborando alrededor de 90 funcionarios en diversos departamentos. Actualmente la Asociación está implementando el servicio de hosting de sus sites de Internet, con el fin de que el asociado, pueda encontrar información acerca de sus dependencias, así también

[3] Radiográfica de Costa Rica, 2004.

como consultar su estado de cuenta e inclusive hasta en un futuro próximo revisar su correo electrónico o e-mail.

Es por tal motivo que resulta primordial la implementación de una DMZ, o Zona Desmilitarizada, para poder así parametrizar los servidores y servicios que pueden ser accesados desde la Internet, manteniendo totalmente aparte y segura la información que estos albergan, así como al resto de la red.

JUSTIFICACION

La Asociación Solidarista de Empleados del Ente Público en estudio, es una institución que a través de los 20 años que tiene de existir, ha venido innovando, y mejorando con nuevos servicios que brinda a sus asociados, es por esto que ahora dos décadas después, la Asociación cuenta con diversas dependencias, como lo son: centros de esparcimiento, tiendas, entre otros; y sin dejar de lado, el ente financiero contable en el que se ha convertido, en el cual el asociado puede solicitar créditos, así como realizar diversos tramites; debido a estas razones, resulta fundamental para la Asociación mantener informado a su asociado y a toda aquella persona que actualmente no lo sea, y con más razón en estos momentos, donde el acceso a la información es más fácil y eficiente.

Existen varias razones que motivan a la asociación a brindar los servicios por medio de la red de Internet, entre estas se puede mencionar:

- Aumentar la imagen institucional, dadas las expectativas que la tecnología de Internet ha causado.
- Estar “en punta” con la tecnología: Internet es la tecnología de moda, y existe la creencia de que quienes no la utilizan quedan rezagados.
- Ofrecer acceso a una gran cantidad de información y conocimiento a un costo muy bajo, lo que resulta muy atractivo.
- Aumentar la capacidad de comunicación desde y hacia la Institución al usar los nuevos canales disponibles, gracias a las tecnologías de telecomunicación digital.
- Brindar a través de Internet acceso a la información que la institución desee comunicar, por ejemplo: boletines, promociones, planes de ahorro, etc.

Actualmente la Asociación, está levantando el Servicio de 5 páginas de Internet (sites), de cada una de sus empresas, esto primero con el fin de mantener informado a sus asociados, así como lo hacen las grandes empresas que forman parte del gran mundo de Internet; otra razón es también para que el asociado mediante la página de Internet pueda realizar diversas consultas de su estado de cuenta, tramites, reservaciones, e inclusive en el caso de la tienda comercial poder realizar diversas compras.

Al implementar este novedoso servicio, resulta primordial para la Asociación, el salvo resguardo de la información de sus asociados, así como velar, para que la información que estos consulten, sea la única que les sea desplegada; en estos términos es en donde resulta necesario, hablar sobre la Seguridad de la Red, así como de la Información que en esta se encuentra, y que la misma, ha medida que sea posible no se encuentre al alcance de personas que puedan hacer un mal uso de ésta.

En la actualidad hablar de Seguridad, inclusive para los expertos o *"gurus"*, es algo que se torna un poco complicado, ya que según es sabido no existe una red 100% segura, no obstante lo que se pretende, es que sea lo más segura posible.

"Se puede invertir mucho tiempo, dinero y esfuerzo en la seguridad informática, pero nunca se resolverá realmente el problema de la pérdida intencional de datos o actividades. El trabajo de los profesionales en informática es ayudar a las organizaciones a decidir cuánto tiempo y dinero quieren gastar en la seguridad; deben cerciorarse que las empresas tengan políticas, recomendaciones y procedimientos vigentes para que el dinero que se gaste se gaste bien. Esto indica que la seguridad práctica es una cuestión de administración y manejo más que una cuestión de destreza técnica. Por lo tanto la

seguridad tiene que ser una de las prioridades de la administración de la empresa".[4]

Aún la más pequeña de las empresas no es inmune a las amenazas en Internet. Una sola grieta en la seguridad puede detener las operaciones de la empresa, disminuir la productividad y posiblemente comprometer la integridad de la información, la confianza de los clientes y el flujo de los ingresos. Las amenazas actuales pueden venir de cualquier parte: redes conectadas o inalámbricas, interna o externamente. Desaparecieron los buenos tiempos cuando se identificaba fácilmente el perímetro de las redes y se protegía con tan solo aplicar algunos dispositivos sencillos de seguridad.

La introducción de nuevas tecnologías, junto con la creciente sofisticación de las amenazas en Internet, exige una solución completa de protección.

Debido a esto, en Costa Rica poco a poco las empresas, principalmente las financieras, empiezan a invertir una gran cantidad de dinero en seguridad informática, tanto de sus sistemas, como de sus redes; y más aún cuando Internet se encuentra presente en ellas.

La Asociación, a pesar de ser un ente financiero no tan grande como un banco estatal, si tiene muy clara la importancia sobre la SEGURIDAD, para proteger la información que se encuentra almacenada en sus bases de datos.

La Seguridad de una Red, depende en gran medida, del control de acceso a los medios que tengan todos los usuarios de esta. Cuando una empresa cuenta con diversos Sites de Internet, hospedados en un servidor que se encuentre físicamente en sus propias instalaciones, las medidas de seguridad que esta ha de

[4] Garfinkel, 1999, p. 19

implementar, resultan primordiales, para poder delimitar el área hasta donde se desea que el usuario externo pueda acceder a la información de la institución.

Una de las medidas de seguridad más eficientes y utilizadas en los últimos años a nivel mundial en las grandes compañías extranjeras es la DMZ o zona desmilitarizada.

La DMZ, es una zona demarcada, la cual tiene como fin en específico parametrizar el área la cual va a estar expuesta a la red externa (área de alto riesgo), en este caso, Internet; en esta, el usuario solamente podrá acceder lo que se encuentra en ella, ya sea servidores de Hosting, FTP, E-mail, etc. Evitando de esta forma, exponerse a las diversas amenazas que se encuentran en movimiento por todo lo ancho de la Internet como: hackers, gusanos, virus, troyanos, sniffers, etc; el tema de seguridad, resulta ser una pieza clave para la protección ante éstas y otras amenazas.

PLANTEAMIENTO DEL PROBLEMA

La Asociación, cuenta con diversas empresas y servicios, los cuales se hallan al alcance de sus asociados, y a quienes no lo son, se les brinda la posibilidad de pertenecer a ésta, gracias a diversas campañas publicitarias que la institución ha venido realizando, la última de estas es la habilitación de diversas páginas de Internet, en las cuales, se puede encontrar información de las empresas y sus servicios, así como en un futuro cercano realizar diferentes tipos de consultas, tales como: estados de cuenta, excedentes, etc.

La Internet, es actualmente el medio número uno de comunicación y publicidad tanto de las personas, como de las empresas, las cuales hayan en está una ventana para presentar sus servicios a la población mundial.

Con lo que se refiere al proceso de implementación, al realizarse el servicio de hospedaje de las páginas de Internet propiamente en los servidores de la Asociación, y debido a la velocidad en que se está realizando este proceso, no se ha previsto del todo las posibles consecuencias de su puesta en marcha, y por ende de potenciales amenazas, ya que Internet en los últimos tiempos, no solo ha experimentado un gran aumento en el numero de usuarios, sino que también ha resultado ser uno de los principales "criaderos" de amenazas informáticas, las cuales han ido creciendo y evolucionando de manera constante.

Los problemas que se tienen con respecto a la habilitación de las páginas de Internet, son debido a que si cualquier usuario tiene acceso a éstas, podría infiltrarse en los demás servidores de la Asociación, los cuales poseen información de gran importancia y de mucha confidencialidad de todos sus asociados, convirtiéndose así en un grave problema, por lo tanto no se debe permitir el acceso a los demás servidores; es decir solamente pueden hacer uso del servidor

o del servicio que se tiene para dicho fin. Por este motivo, y debido a las amenazas que se encuentran en la Internet, es necesaria la implementación de una DMZ, para restringir el acceso y aumentar el nivel de seguridad de la red de la Institución.

El proceso de implementación de la DMZ, traerá consigo una serie de ventajas y beneficios, tanto para la Asociación como para los asociados, en este proceso se requerirá contar tanto con el apoyo del personal de soporte del área de informática, como también con el presupuesto para realizar dicha implementación, siendo necesaria la adquisición de equipos nuevos, entre otras cosas.

El departamento de Informática cuenta con el presupuesto necesario, previamente aprobado por la Junta Directiva, para llevar a cabo dicho proyecto; además los encargados de soporte técnico del departamento poseen los conocimientos básicos en redes, para administrar y dar seguimiento a la implementación de la DMZ.

FORMULACION DEL PROBLEMA

¿Cómo puede la implementación de una DMZ mejorar la seguridad de la red de la Asociación Solidarista de Empleados de un Ente Público?

MATRIZ DE OBJETIVOS

TEMA	PROBLEMA	OBJETIVOS	
		GENERAL	ESPECIFICOS
Análisis para implementar una DMZ en la red de la Asociación Solidarista de un Ente Público	¿Cómo puede la implementación de una DMZ mejorar la seguridad de la red de la Asociación Solidarista de Empleados de un Ente Público?	Esquematizar el estudio de la red de la Asociación Solidarista de Empleados del Ente Público, sin la implementación de la DMZ	- Definir la estructura actual de la red de datos de la Asociación. - Efectuar un análisis de vulnerabilidad de la red de datos de la Asociación. - Diseñar el diagrama de la red de datos de la Asociación, sin implementar la DMZ.

		Esquematizar la posible implementación de una DMZ en la red de la Asociación Solidarista de Empleados del Ente Público	-Analizar el equipo necesario para la implementación de la DMZ. - Describir el equipo que se posee para realizar la implementación de la DMZ. - Identificar las zonas de seguridad necesarias para implementar la DMZ. - Determinar el costo del equipo necesario para la implementación. - Diseñar el diagrama de la red de datos de la Asociación una vez implementada la DMZ. - Dar a conocer los posibles beneficios que podría obtener la Asociación de Empleados del Ente Público.

MATRIZ DE VARIABLES

Variables	Definición Conceptual	Definición Operacional	Indicadores	Instrumentos de recolección de datos
-Beneficios de contar con una DMZ	Beneficio que podría obtener la Asociación de Empleados con la implementación de la DMZ	Se propone implementar la DMZ, con sus respectivas políticas de seguridad		- Encuestas - Investigación
Conocimiento en redes	Conocimiento que poseen los técnicos de soporte en redes	Se analizará las destrezas, habilidades y conocimientos de los funcionarios del depto. Informática	- Nivel de conocimiento - Nivel de destrezas	- Encuestas
Conocimiento en seguridad de redes	Conocimiento que poseen los técnicos de soporte en seguridad de redes	Se analizará las destrezas, habilidades y conocimientos de los funcionarios del depto. Informática	- Nivel de conocimiento - Nivel de destrezas	- Encuestas
Tipos de equipos	Tipo de equipo con el que se cuenta para la implementación	Se revisará los equipos que cumplan con las características necesarias para la implementación	- Marca del equipo - Característi-cas del equipo - Funciones del equipo	- Investigación
Configuración de equipos	Configuración de los equipos	Se revisará configuración de los equipos SW y HW	- Nivel de seguridad - Funciones	- Investigación
Tipo de amenazas	El nivel de peligrosidad de las amenazas	- Se realizará monitoreo mediante SW especializado	- Número de amenazas - Tipos de amenazas	- Consulta a Bases de Datos

CAPITULO II

MARCO TEORICO

A) ASOCIACIONES SOLIDARISTAS

Las Asociaciones Solidaristas son organizaciones sociales que se inspiran en una actitud humana, por medio de la cual el hombre se identifica con las necesidades y aspiraciones semejantes, comprometiendo el aporte de sus recursos y esfuerzos para satisfacer esas necesidades y aspiraciones de manera justa y pacífica. Su gobierno y administración competen exclusivamente a los trabajadores afiliados a ellas.

Los fines primordiales de las asociaciones solidaristas son procurar la justicia y la paz social, la armonía obrero-patronal y el desarrollo integral de sus asociados.

Podrán constituirse asociaciones solidaristas como organizaciones sociales idóneas para el cumplimiento de los fines señalados en esta ley, en beneficio de los trabajadores de regímenes de empleo tanto público como privado.

“Las asociaciones solidaristas son entidades de duración indefinida, con personalidad jurídica propia, que, para lograr sus objetivos, podrán adquirir toda clase de bienes, celebrar contratos de toda índole y realizar toda especie de operaciones lícitas encaminadas al mejoramiento socioeconómico de sus afiliados, en procura de dignificar y elevar su nivel de vida. En tal sentido podrán efectuar operaciones de ahorro, crédito y de inversión, así como cualesquiera otras que sean rentables. Asimismo podrán desarrollar programas de vivienda, científicos, deportivos, artísticos, educativos, y recreativos, culturales, espirituales, sociales,

económicos, lo mismo que cualquier otro que lícitamente fomente los vínculos de unión y cooperación entre los trabajadores, y entre estos y sus patronos.” [5]

La estructura organizacional de la Asociación Solidarista del Ente Público referente a la administración, comprende una Gerencia General la cual ha dividido las tareas en cinco direcciones:

- Comunicación Corporativa
- Informática
- Operaciones
- Contabilidad
- Administrativa

[5] Ley de Asociaciones Solidaristas y su Reglamento, p 9. (Art.1- 4)

A.1) PRINCIPALES BENEFICIOS AL AFILIARSE

Los asociados cuentan con diversos beneficios, al formar parte de la Asociación, los más importantes son:

A.1.1. Ahorro Obrero 5%

- Crea una cultura de ahorro
- Previsión para el futuro
- Deducción automática de planilla
- Genera intereses (excedentes)
- Sirve como base para préstamos

A.1.2. Aporte patronal 2%

- Depósito de cesantía de la C.C.S.S a la ASOCIACION.
- Es un derecho con el cual cuenta cada trabajador
- Se retira al renunciar o ser despedido (con o sin responsabilidad patronal)
- Genera intereses
- Es 7inembargable

A.1.3. Excedentes

- El rendimiento es producto del ahorro y la cesantía
- Respaldo para Crédito
- Capitaliza un 20% anual
- Se entregan a fin de año
- Crecen anualmente

A.2) TIPOS DE TRAMITES

El asociado cuenta con la posibilidad de realizar diversos tipos de trámites, entre estos se encuentran:

- Afiliación: es el primer trámite a realizar por todo nuevo asociado.
- Crédito: en este tipo de trámite, el asociado cuenta con una gran variedad de planes de crédito según su condición económica lo permita.

- Vivienda: es una de las opciones de crédito más importantes para el Asociado, ya que gracias a este, puede contemplar la opción de comprar casa, terreno, modificar o ampliar su vivienda.
- Cobro: en este tramite la Asociación cobra al asociado los créditos pendientes o con mora que estos tengan directamente con la Asociación.
- Abonos: los abonos son regulados según el plan de crédito o préstamo que el asociado tenga.
- Consulta: los asociados cuentan con la posibilidad de consultar cualquier tipo de trámite, que este realizando o sencillamente consultar sus estados de cuenta.
- Planes de ahorro: la Asociación le brinda al asociado diversos tipos de planes de ahorro, a corto, mediano o largo plazo.
- Beneficios Sociales: el asociado, cuenta con diversos tipos de beneficios sociales, los cuales tienen como fin ayudarles con situaciones especiales, por ejemplo: becas, convenios universitarios.
- Retiro: es cuando el asociado no desea formar más parte de la Asociación y decide de esta forma terminar todo vínculo o relación con ella.

A.3) OPCIONES DE FINANCIAMIENTO

- Sobre Ahorro: Es un crédito sin fiadores y se otorga para cualquier trámite personal.

- Excedentes: Es un crédito sin fiadores, debido a que es un adelanto del excedente del respectivo periodo.

- Vivienda: Otorga vivienda digna a los asociados, debido a que se direcciona a la compra, construcción, cancelación de hipoteca y remodelación.

A.3.1. Fondos de inversión

- Ahorro Navideño:
  - Extraordinario quincenal, se devuelve en su totalidad en el mes de diciembre
- Ahorro a la Vista :
  - Tiene un plazo indefinido y se puede retirar en cualquier momento
- Capitalización Extraordinaria:
  - Para el mes de diciembre se puede capitalizar un porcentaje extraordinario de los excedentes desde un 5% hasta el 100%.

A.4) OTROS SERVICIOS

A.4.1. Asesoría Personalizada

- Traslado y seguimiento de documentos
- Entrega de estados de cuenta y comunicados
- Apoyo en la realización de actividades especiales

A.5) UNIDADES ESTRATÉGICAS DE NEGOCIOS

La Junta Directiva decidió crear diversas empresas, con base en lo dispuesto por el Artículo 4 de la Ley de Asociaciones Solidaristas que al efecto faculta a:

¨…realizar toda especie de operaciones lícitas encaminadas al mejoramiento socioeconómico de sus afiliados, en procura de dignificar y elevar su nivel de vida.¨ En tal sentido podrá efectuar operaciones de ahorro, de crédito y de inversión, así como cualesquiera que les sean rentables.¨

Por lo tanto se han venido desarrollando actividades empresariales que, una vez consolidadas, están destinadas a producir beneficios económicos y sociales para los Asociados.

Las actividades empresariales que emergen bajo la figura de Sociedades Anónimas, con el propósito de separar sus contabilidades, fueron convertidas en Unidades Estratégicas de Negocios por recomendación de la Price Waterhouse Cooper.

B) INTERNET

Internet no es del todo una red sino un inmenso conjunto de redes diferentes que utilizan ciertos protocolos comunes y proporcionan ciertos servicios comunes. Es un sistema poco común porque nadie lo planeó y nadie lo controla.

“Hoy en día Internet, es una red que engloba cientos de miles de computadoras y decenas de millones de usuarios a través del mundo. Similar al sistema telefónico, la Internet está bien conectada, es decir, hay robustez en cuanto a los enlaces y las rutas. Una persona, de esas decenas de millones de usuarios, puede enviar correo electrónico a otra, intercambiar archivos, o probar su suerte intentando corromper un sistema, si éste se está configurando de tal manera que permita el acceso necesario para lograrlo.” [6]

Por la red Internet circulan constantemente cantidades increíbles de información. Por este motivo se le llama también La Autopista de la Información. Hay aproximadamente 60 millones de "Internautas", es decir, de personas que "navegan" por Internet en todo el Mundo. Se dice "navegar" porque es normal el ver información que proviene de muchas partes distintas del Mundo en una sola sesión.

B.1) ANTECENDES DE LA RED MUNDIAL DE INTERNET

“Internet nació en EE.UU. hace unos 30 años como un proyecto militar llamado ARPANET (Advanced Research Projects Agency Network), el cual fue una red experimental diseñada para investigaciones militares y en particular para investigaciones sobre como construir redes que pudieran resistir daños parciales y que continuaran funcionando, a su vez se pretendía poner en contacto una

[6] Garfinkel, 1999, p. 390

importante cantidad de computadoras de las instalaciones del ejército de EE.UU. En este proyecto se gastó mucho dinero y recursos en construir la red de computadoras más grande en aquella época. Diez años más tarde aparecieron las "*Ethernet Local Area Networks*" (un estándar para redes locales de bajo costo), con lo que se planteó la necesidad de interconectar, no sólo computadoras, sino también diversos tipos de estas."[7]

Durante la década de los 80, se produce la primera explosión en números de usuarios conectados, primero en universidades, centros estatales, etc.; poco a poco, las empresas comienzan a acceder a estos servicios, además de ofrecer servicios de conexión, de carácter comercial, para usuarios finales. En 1989 se produce el nacimiento "oficial" de la Internet.

A finales de 1993, el número de computadoras conectadas estaba en aproximadamente los 2.200.000, con un total de 20 millones de usuarios conectados.

En la actualidad, Internet crece a un ritmo vertiginoso, las redes conectadas continúan creciendo a un ritmo aproximado del 10% mensual. Constantemente se mejoran los canales de comunicación con el fin de aumentar la rapidez de envío y recepción de datos. Cada día que pasa se publican en la Red miles de documentos nuevos, y se conectan por primera vez miles de personas. Con relativa frecuencia aparecen nuevas posibilidades de uso de Internet, y constantemente se están inventando nuevos términos para poder entenderse en este nuevo mundo que no para de crecer. Ver figura No. 1.

Internet crece exponencialmente, tanto en recursos como en usuarios.

[7] Garfinkel, 1999, p. 390

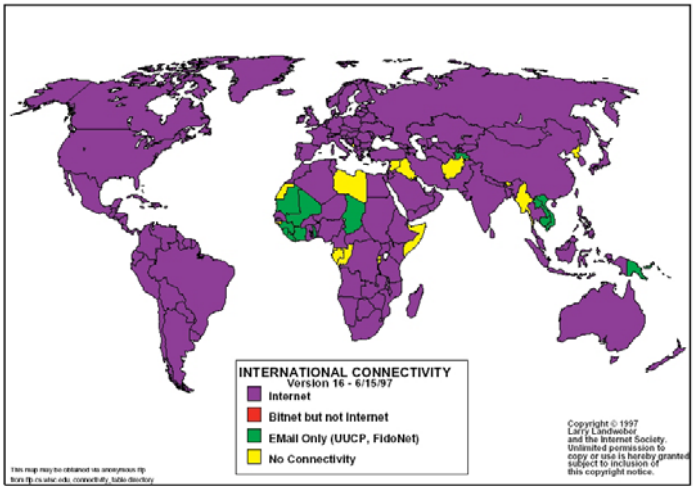


Figura No. 1. Países con acceso a Internet, 1997

Los países en morado disponían de acceso a Internet en el año de 1997

B.2) INTERNET EN COSTA RICA

El proceso de interconexión de Costa Rica a las grandes redes de investigación se inicia en 1990 con el establecimiento en la Universidad de Costa Rica (UCR) del primer nodo de la Red Bitnet en la región Centroamericana y su integración, dos años después, a la Red Internet.

En octubre de 1992, Costa Rica estaba lista para establecer un enlace de 64 kbps con la red Internet de los Estados Unidos de América, gracias a los fondos facilitados por la Agencia Internacional de Desarrollo (AID, por sus siglas en inglés) y la Organización de Estados Americanos (OEA). No obstante, el huracán Andrew truncó estos planes ya que destruyó las antenas receptoras.

Para finales del 26 de enero de 1993 se logra interconectar una docena de nodos ubicados en la Unidad de Redes, Centro de Informática, Escuela de

Geología y Escuela de Física de la Universidad de Costa Rica, con la red Internet, lo que permitió que Costa Rica se conectara a la Red.

En este mismo año se crea la Asociación CRNet (una red digital que utiliza enlaces de fibra óptica para interconectar las instituciones académicas y de investigación más importantes del país, permitiendo amplio acceso a la información y recursos computacionales del mundo), bajo los auspicios del Ministerio de Ciencia y Tecnología, la Universidad de Costa Rica y la Academia Nacional de Ciencias. CRNet se creó con el objetivo de administrar la Internet en el sector académico y de investigación en Costa Rica.

Estos logros importantes, no sólo permitieron la conectividad instantánea de un gran número de personas con el resto del mundo, sino que también introdujeron al país por primera vez en la tecnología inter-redes a gran escala.

“Radiográfica Costarricense S.A. (RACSA) inició en julio 1994 la operación de Internet para el sector comercial, luego posteriormente ofrece también servicios a particulares, realizando así las inversiones necesarias para responder a las necesidades del mercado en el acceso a este novedoso servicio. Desde su inicio de operación a la fecha, el crecimiento del servicio ha experimentado un comportamiento interesante, ya que se tienen registros que en menos de tres años el servicio había obtenido un crecimiento promedio de 10% a 13% mensual.”

“Un informe de diciembre 2003 de la Unión Internacional de Telecomunicaciones, (UIT), ubica a Costa Rica en un puesto privilegiado de las naciones en el mundo “mejor equipados con Internet y otras tecnologías de la información”, pues nos coloca en el puesto No. 58, siendo la segunda mejor de América Latina, sólo superados por Chile. Los 10 países del mundo, mejor ubicados son: Suecia, Dinamarca, Islandia, Corea del Sur, Noruega, Holanda, Hong Kong, Finlandia, Taiwán y Canadá.”

Otro informe, del 20 noviembre del 2003, preparado por la Secretaría General de la Conferencia sobre Comercio y Desarrollo de las Naciones Unidas (UNCTAD), sobre el comercio electrónico y el desarrollo, indica que Costa Rica se encontraba en el lugar No. 49 a nivel mundial en cuanto al Índice de Preparación de la Red (NRI – *Network Readiness Index)* definido como el "grado de preparación de una nación para participar y beneficiarse del desarrollo de las tecnologías de información y comunicación".

Para tener una referencia acerca de la posición de Costa Rica con la del resto de países americanos con respecto a dicho índice, se detalla que nuestro país estaba en el lugar sétimo a nivel americano, en lugar quinto a nivel latinoamericano, y en primer lugar a nivel regional. [8]

B.3) SERVICIOS DE LA INTERNET

Cada servicio es una manera de sacarle provecho a la Red, estos son independientes de los demás.

Hoy en día, los servicios más usados en Internet son: E-mail, World Wide Web, FTP y Servicios de Telefonía.

- El E-mail permite enviar cartas escritas con la computadora a otras personas que tengan acceso a la Red. Las cartas quedan acumuladas en Internet hasta el momento en que se piden. Es entonces cuando son enviadas a la computadora del destinatario para que pueda leerlas.

- La World Wide Web, o WWW como se suele abreviar, se inventó a finales de los 80 en el CERN, el Laboratorio de Física de Partículas más importante del Mundo. Se trata de un sistema de distribución de

[8] RACSA, 2004.

información tipo revista. En la Red quedan almacenadas lo que se llaman Páginas Web, que no son más que páginas de texto con gráficos o fotos. Aquellos que se conecten a Internet pueden pedir acceder a dichas páginas y acto seguido éstas aparecen en la pantalla de la computadora. Este sistema de visualización de la información revolucionó el desarrollo de Internet. A partir de la invención de la WWW, muchas personas empezaron a conectarse a la Red desde sus hogares, como entretenimiento.

Internet recibió un gran impulso, hasta el punto que hoy en día casi siempre que hablamos de Internet, nos referimos a la WWW.

- El FTP (File Transfer Protocol) permite enviar archivos por Internet. Ya no es necesario guardar la información en disquetes para usarla en otra computadora. Con este servicio, muchas empresas informáticas han podido enviar sus productos a personas de todo el mundo sin necesidad de gastar dinero en miles de disquetes, ni en envíos.

- Los Servicios de Telefonía son las últimas aplicaciones que han aparecido para Internet. Nos permiten establecer una conexión con voz entre dos personas conectadas a Internet desde cualquier parte del mundo sin tener que pagar lo que cuesta una llamada internacional. Algunos de estos servicios incorporan no sólo voz, sino también imagen. A esto se le llama Videoconferencia.

C) SEGURIDAD INFORMÁTICA

C.1) ANTECEDENTES DE LA SEGURIDAD INFORMÁTICA

En el inicio de la era de la computación, la seguridad informática no era un aspecto relevante, debido a que el número de computadoras y el número de personas con acceso a ellas era limitado. Sin embargo a principios del año 1950, surgió el primer problema de seguridad, cuando las computadoras comenzaron a ser usadas para guardar información confidencial, en donde el principal riesgo era el espionaje y la invasión de la privacidad. Desde ese tiempo y hasta hace poco, la seguridad de computadoras fue principalmente un tema militar, sumado a ello, el hecho de compartir recursos e información a través de una red local generó más problemas de seguridad; por tal motivo el tema ha sido un asunto de gran interés por la extensión de la microinformática y las redes de ámbito mundial, que ha provocado que las vías de acceso a estos sistemas se multipliquen, y como consecuencia que aparezcan nuevos riesgos relativos a la seguridad.

Por otra parte, la creciente aparición de nuevos usuarios que quieren acceder a Internet, también supone un riesgo añadido, ya que cuanto más usuarios haya, más posibilidades hay de que aparezcan nuevos usuarios maliciosos que hagan un uso inadecuado de las computadoras, como copia de programas para fines de comercialización sin reportar los derechos de autor, el acceso vía telefónica a bases de datos para realizar fraudes, hasta el uso de identidad para suplantar a usuarios legítimos.

C.2) ¿QUÉ ES LA SEGURIDAD INFORMÁTICA?

"Una computadora es segura si se puede confiar en que, junto con sus programas, funcione como se espera".[9]

Los términos seguridad de red y seguridad de información se refieren en sentido amplio, a la confianza de que la información y los servicios disponibles en una red no puedan ser accedidos por usuarios no autorizados. Seguridad implica protección de la información y debe cumplir con tres principios básicos:

- Integridad: la información debe ser oportuna, exacta completa y consistente.
- Disponibilidad: la información debe estar lista y disponible en cualquier momento que sea requerida, es decir que los recursos se encuentran libres de interrupciones en el servicio.
- Confidencialidad: La información debe ser conocida solamente por su propietario o por quienes el usuario desea compartirla, es decir que no existan accesos no autorizados a los recursos computacionales.

Por supuesto, así como la seguridad física no está absolutamente segura contra los delitos, ninguna red es absolutamente segura. Las organizaciones hacen un esfuerzo para lograr la seguridad de las redes, por la misma razón que se hace para mantener seguros edificios y oficinas: aun cuando una organización no pueda prevenir completamente los delitos, algunas medidas de seguridad básicas puedan disuadir a quienes los cometen, haciendo que los actos ilegales sean mucho más difíciles de realizar.

[9] Garfinkel, 1999, p. 5

Proporcionar seguridad de información requiere protección tanto de los recursos físicos como de los abstractos o lógicos. En un ambiente de red, la seguridad física se extiende a los cables, switches y enrutadores (routers) que comprenden la infraestructura de la red.

En la actualidad, la mayoría de las organizaciones cuentan con grandes dispositivos para la seguridad física de las computadoras y se tiene la idea de que los sistemas no puden ser violados si no se entra al centro de cómputo, olvidándose de la seguridad lógica que puede ser violentada. Consecuentemente la seguridad física como lógica debe ser considerada como una sola para establecer políticas, procedimientos y prácticas.

C.3) POLÍTICAS DE SEGURIDAD

Antes de que una organización implante un proyecto de seguridad de red, la organización debe asumir riesgos y desarrollar una política clara, considerando los accesos de información y protección. Las políticas deben especificar quienes tendrán garantizado el acceso a cada parte de la información y deben establecer las reglas individuales a seguir.

Al definir políticas de seguridad muy generales se corre el riesgo de que no sean entendidas por los empleados o que sean ignoradas por falta de conocimiento.

C.3.1. Consejos para desarrollar políticas prácticas

Existen algunas ideas claves para formalizar las políticas:[10]

- *Asignar un dueño:* el dueño debe ser la persona responsable de la información, y el que tiene cierta autoridad de otorgar acceso a ella.
- *Ser positivo:* la gente responde favorablemente a las informaciones positivas que a las negativas. En lugar de escribir una lista larga de frases que contengan “no se debe”, se debe pensar en decir lo mismo, pero de una manera positiva.
- *Concentrarse en la capacitación:* cada usuario debe tener una capacitación sobre la concientización de la seguridad, y tener alguna forma periódica de refrescar esa información.
- *Adoptar defensas a fondo:* deben establecerse varios niveles independientes y redundantes de protección. Esto incluye la vigilancia y auditoria para asegurar que las protecciones funcionen

[10] Garfinkel, 1999, p. 32- 33

D) AMENAZAS

Conforme se ha venido mencionando, no resulta ser un secreto la importancia tan grande que tiene implementar diversas medidas de seguridad en las redes de las empresas, más ahora que existe un termino para todos los peligros que pueden merodear la información y los datos de las empresas, ahora los tipos de peligros, son conocidos como “amenazas”. Adquirieron dicho término porque ya no es un tipo en específico de peligro, por el contrario, cada vez son más la variedad de “amenazas”, que circulan por toda la Red, los cuales fueron creados con un mismo fin, violentar y quebrantar la seguridad de los sistemas y las redes.

D.1) AMENAZAS MÁS COMUNES

D.1.1. Hackers:

El hacker es una de las denominaciones de mayor prestigio en el sentido del conocimiento tecnológico, sin embargo los hackers más famosos son quienes han cometido los delitos más grandes informáticos. Por lo tanto podría decirse que existen dos tipos de hackers, los buenos y los malos, los que colaboran en el crecimiento de la tecnología, y los que se aprovechan de sus conocimientos para llevar a cabo operaciones ilegales. Por otro lado, los crackers y script kiddies son en realidad quienes efectúan daños en las máquinas.

Un hacker investiga, trata de solucionar problemas y es precisamente un cracker, y en menor medida un script kidd, quien se dedica a ocasionarlos.

D.1.2. Virus:

Sólo mencionar la palabra virus provoca pánico en el usuario común de la Web, quien justamente suele ser la primer víctima dados sus escasos conocimientos de prevención. Los virus, se escriben para reproducirse a si mismos, cuando estos llegan, ya sea por medio de una página de Internet, un archivo adjunto de correo electrónico, o algún otro medio, por lo general inician infectando los programas ejecutables del disco.

"El martes 27 de enero surgía MyDoom, una de las especies de virus más peligrosos que sufrió Internet y que aún padece, siendo el virus de mayor velocidad de propagación de todos los tiempos habiendo afectado a más de 500.000 equipos. Las pérdidas, consecuencia de los ataques de MyDoom en sus distintas variantes superan los 3 billones de dólares según ha informado la consultora *mi2g*. Sin embargo a este le han seguido nuevos virus, más evasivos frente a las medidas de seguridad de los antivirus y con mayores recursos de reproducción." [11]

Los virus informáticos se aprovechan de las vulnerabilidades de las aplicaciones para infectar las computadoras y reproducirse, siendo indetectable a la visión del usuario hasta que se lleva a cabo el ataque. Existen distintos tipos de virus, según sus fines, pero las dos características que los unen son: reproducirse y/o sobrevivir, y cumplir sus misiones.

D.1.3. Troyanos:

Con una arquitectura similar a la de los virus, los troyanos actúan aprovechándose de los errores de programación, haciendo referencia principalmente al sistema operativo y clientes de e-mail de Microsoft Windows y Outlook respectivamente. La finalidad de los troyanos podría compararse a los

[11] Seguridad en la Red, 2004

spywares en el sentido de que se convierten en agentes de espionaje que buscan y transmiten datos de relevancia, tales como números de tarjetas de crédito y claves de acceso. [12]

Las amenazas combinadas emplean múltiples métodos para descubrir y aprovechar las vulnerabilidades de la red para luego poder autoreplicarse y autopropagarse, lo cual puede suceder sin que el usuario informático se entere.

Amenazas combinadas como el Código Rojo y Nimda tomaron las peores características de los virus, gusanos y caballos de Troya, y las combinaron con vulnerabilidades de los servidores y de Internet para iniciarse, transmitirse y propagarse. Las amenazas combinadas están diseñadas para aprovechar las vulnerabilidades de tecnologías de seguridad que funcionan independientemente y por separado, por lo cual la protección total es tan crucial para la seguridad de la empresa actual. La velocidad de distribución de las amenazas en Internet ha pasado de semanas a días y de días a horas.

D.1.4. Gusanos (Worms):

Son códigos malignos cuya principal misión es reenviarse a sí mismo. Son códigos víricos que en principio, no afectan a la información de los sites que contagian, aunque consumen amplios recursos de los sistemas, y los usan para infectar a otros equipos.

A diferencia de la mayoría de virus, los gusanos se propagan por sí mismos, sin modificar u ocultarse bajo otros programas. No destruyen información de forma directa, pero algunos pueden contener dentro de sí, propiedades características de los virus.

[12] Symantec, 2004

El mayor efecto de los gusanos es su capacidad para saturar, e incluso bloquear por exceso de tráfico los sites de Internet, aunque estos se encuentren protegidos por un antivirus actualizado.

D.1.5. Spywares:

"Los spywares son pequeños programas que se instalan en el sistema con la finalidad de robar los datos y espiar los movimientos del usuario por la red. Luego envían esa información a empresas de publicidad de Internet para comercializar con estos datos. Trabajan en modo 'background' (segundo plano) para que nadie se percate de su existencia, hasta que empiecen a aparecer los primeros síntomas." [13]

D.1.6. Sniffers:

"Un *sniffer* es un programa que se utiliza actualmente para monitorear y analizar el trafico en una red de computadoras, este puede ser utilizado de forma licita para detectar los cuellos de botellas y problemas que existan en ella, o de forma ilegal, que resulta en extremo peligroso para la seguridad de las redes, debido a que hace posible monitorear el tráfico de datos que circula por la red." [14]

Con tantas amenazas merodeando la Internet, y al estar expuesta una red corporativa o empresarial, a esta, lo que queda es primero aumentar el nivel de seguridad de toda la red, y posteriormente parametrizar el acceso de los usuarios externos a la red de una empresa, por ende implementar la DMZ, no es una posibilidad, más bien forma parte de la solución.

[13] Mastermagazine, 2004
[14] Mastermagazine, 2004

E) ZONA DESMILITARIZADA (DMZ)

"En los cincuenta se libró una de las guerras con mayor duración en la historia de Asia: la guerra de Corea. Para evitar enfrentamientos, una estrecha franja, de pocos kilómetros de anchura, quedó fijada como zona desmilitarizada, más conocida por sus iniciales en inglés como DMZ. A pesar de que fuese teóricamente un pasillo para la paz, en la realidad fue uno de los lugares más peligrosos del mundo. Tropas de Corea del Norte por un lado, y de la ONU, del otro, vigilando cualquier movimiento en la frontera. De esta forma DMZ ha quedado como sinónimo de un lugar altamente vigilado y peligroso." [15]

En términos informáticos DMZ, es la zona expuesta al exterior, donde se albergan los servicios que necesariamente tienen que ser accesibles desde afuera, tales como: servidores web, ftp o de correo. Estos servidores están expuestos al "fuego enemigo" de los posibles atacantes provenientes de la Internet, y por lo tanto, deben de ser vigilados de forma especialmente estricta. También deben de ser separados del resto de la red, para que en el caso de que un ataque contra los mismos fructificase, no hubiese posibilidad de usar esta máquina como vector de ataque al interior de la red. [16]

La existencia de una DMZ, donde poner los servidores expuestos nos proporciona un nivel extra de seguridad frente al caso de una única zona de red donde se junten los equipos de trabajo de la red interna con los equipos expuestos.

[15] About Inc., 2004
[16] Microsoft Corporate, 2004

En la actualidad, la mayor parte de las organizaciones desean que su infraestructura informática esté conectada a Internet ya que proporciona servicios valiosos a su personal y a sus clientes. Sin embargo, no siempre el uso de los servicios disponibles a través de una conexión a Internet es bienintencionado, lo que hace necesario el empleo de estrategias de seguridad de red. En una zona desmilitarizada es necesaria la inclusión de una serie de tecnologías que se puedan utilizar al planear la estrategia de seguridad de una red.

Estas tecnologías también pueden ser de utilidad si los problemas de seguridad de la red son internos a la organización o si las conexiones de red externas se establecen con redes distintas de Internet.

Una conexión a Internet permite al personal de una organización utilizar el e-mail para comunicarse con gente de todo el mundo para obtener información y archivos de un extenso número de orígenes. También posibilita que los clientes obtengan información y servicios de la organización en todo momento. Además, el personal puede utilizar recursos de la organización desde su casa, algún hotel o desde cualquier lugar donde se encuentren, y los socios pueden usar herramientas especiales que les permitan trabajar de forma más efectiva con la organización.

Al diseñar una red, puede ser aconsejable implementar las tecnologías de seguridad adecuadas para la organización. Solucionar en un primer momento estos asuntos garantiza que no se pueda infringir la seguridad y que se está preparado para proporcionar herramientas de red seguras siempre que sea necesario. Incluso aunque ya se cuente, probablemente, con un entorno de red seguro en la empresa, es importante revisar las estrategias de seguridad de la misma.

Por desgracia, la posibilidad de compartir y obtener información de los usuarios, conlleva algunos riesgos significativos. Los competidores podrían intentar hacerse con la información privada de los socios o alguien podría modificar las páginas Web con malas intenciones, así como sobrecargar los equipos y dejarlos inservibles. También existe la posibilidad de que los empleados pudieran obtener acceso a información que no les concierne. Lo que se desea es evitar éstos y otros tipos de riesgos de seguridad para garantizar que el trabajo en la empresa se desarrolle como se pretende.

Para asegurarse de que sólo las personas adecuadas tienen acceso a los recursos y datos, es importante analizar cuidadosamente las tecnologías de seguridad de red y planear las estrategias correctamente.

La zona desmilitarizada, igual que ocurre con los componentes de red internos, tiene que estar protegida físicamente contra el acceso del público. De este modo se asegura que nadie, ni siquiera alguno de los empleados, pueda reorganizar el cableado o utilizar inicios de sesión en las cuentas para debilitar la seguridad.

No es necesario independizar físicamente la zona desmilitarizada de otros equipos y equipamiento de red. Sin embargo resulta conveniente aplicar políticas y procedimientos especiales, ya que su función es decisiva en la seguridad de red. Los más pequeños cambios efectuados de forma inadecuada pueden ser suficientes para crear una grieta en la seguridad de la que puedan beneficiarse los intrusos. Por lo tanto, es necesario que sea imposible para el personal no calificado cambiar la zona desmilitarizada. La aplicación de seguridad física adicional a la zona, garantiza que esto se cumpla.

Se debe tener mucha precaución al administrar cuidadosamente las cuentas y los equipos cliente para asegurar que sólo los usuarios autorizados puedan utilizarlos para obtener acceso a la red.

En el capitulo cuatro se hace mención de cómo y que se recomienda para implementar la DMZ en la Asociación con diversos equipos y configuraciones, así como algunas políticas o medidas de seguridad necesarias para llevar a cabo dicho proyecto.

CAPITULO III

MARCO METODOLÓGICO

A) TIPO DE INVESTIGACION

En este proyecto se va a desarrollar, el tipo de investigación exploratoria, esto debido a que el tema de estudio de DMZ es hasta hace poco desconocido en algunos casos, sin embargo, en los últimos años la seguridad en redes, ha tomado un nuevo giro, y por ende se le está dando la consideración e importancia que ésta requiere.

La investigación implicará basar mucha de la información en consultas de diversos medios bibliográficos, siendo Internet la mayor fuente de estos, debido a lo actualizado de la información que se encuentra ahí.

B) TIPO DE MUESTRA

Elegir el tipo de muestra depende del enfoque y alcances de la investigación, objetivos y el diseño del tema seleccionado.

Por tal motivo se opto por implementar el prototipo de muestra probabilística ya que a primera instancia, toda la población, tiene la misma probabilidad de formar parte de la muestra, y en algunos casos se generalizará los resultados de la población.

En el caso de la encuesta a los asociados, el tamaño de la muestra fue obtenido gracias a la formula de Muestreo Simple al Azar, que resulta ser una fórmula para calcular el tamaño de la muestra cuando se desea estimar una proporción poblacional.

Se utilizaron diversos datos, mismos que fueron inferidos, mediante consultas a la base de datos de la Asociación.

- La cantidad de asociados activos hasta el día Jueves 10 de febrero del 2005 es de 22661 personas
- Como la población es un número muy grande y por ende la muestra quedaría con un tamaño muy superior, es que se opto por seleccionar, los asociados que residen en las provincias de Alajuela, San José, Cartago y Heredia hasta la fecha, estos sumados dan un total de 17278 personas.

- La fórmula de Muestreo Simple al Azar es la siguiente:

$$n_0 = \left(\frac{z_{\alpha/2}\sqrt{pq}}{d} \right)^2$$

$$n = \frac{n_0}{1 + \frac{n_0}{N}}$$

En donde:

N es igual al total de la población (22661)

P es el porcentaje de personas que si cumplen con las características de la muestra (76%), esto se obtuvo al realizar el siguiente calculo:

$\frac{17278 * 100}{22661}$ = 0.76

Z	1,96
p	0,76
q	0,24
d	0,05
N	22.661,00
n0	**280,28**
n	276,86

p = Proporción estimada en la población que SI cuentan con la característica de estudio

q = Proporción estimada en la población que NO cuentan con la característica de estudio

d = Error máximo permisible para la estimación (5%)

Z = Valor tabular de la normal estándar para el nivel de confianza (95%)

n0 = Tamaño de muestra sin aplicar factor de corrección por población finita. (cfp)

n = Tamaño de muestra aplicado factor de corrección por población finita. (cfp)

C) INSTRUMENTOS DE RECOLECCION DE DATOS

Para realizar dicha investigación se ha decidido que para poder realizar un análisis para implementar una DMZ en la red de la Asociación Solidarista de un Ente Público, se debe primero conocer la cantidad aproximada de usuarios que acceden los sites de Internet, así como los posibles usos que estos le dan a la misma, también los tipos de ataques que podría recibir la red, entre otros.

"La elección de recolección de datos es un aspecto crítico en el proceso de investigación; la decisión no es fácil, existen muchos factores por considerar, se debe seleccionar el mejor instrumento de medición, que es aquel que registra datos observables que representan verdaderamente los conceptos o las variables que el investigador tiene en mente, sin olvidar la validez y confiabilidad que este debe tener." [17]

El instrumento de medición por excelencia ha utilizar en esta investigación son las encuestas, mismas que estarán conformadas en su mayoría por preguntas de carácter cerrado, esto con el fin de que el asociado muestre interés y sienta que no se le está indagando más allá de asuntos personales y que pudiesen comprometerlos. De esta manera las interrogantes serán claras y concretas para que no se pierda el concepto de lo que se está solicitando, así como también para obtener información más veraz y confiable por parte de la muestra obtenida.

Las encuestas serán aplicadas tanto a los Asociados de la Institución, como a los encargados de soporte; esto como se mencionó anteriormente con el objetivo de recolectar información más confiable, que pudiera ser útil a la hora de desarrollar el problema de investigación.

[17] Hernández,, 2003

Así también como instrumentos de recolección de datos, se hará uso de investigaciones y recolección de diversas bases de datos; todos estos instrumentos se utilizarán con el fin de fortalecer la investigación, así también como de tener fuentes sólidas y actuales a la hora de realizar el análisis para implementar una DMZ.

D) ALCANCES Y LIMITACIONES

D.1) ALCANCES

Los alcances son resultados obtenidos, con el propósito de superar deficiencias y constituyen una etapa más de este proyecto, por lo tanto es aquí donde la magnitud del esfuerzo realizado puede visualizarse con mayor propiedad.

De manera que los alcances del proyecto se van a pretender que estén ligados y orientados hacia resultados positivos, que contribuyan a aumentar la seguridad de la red y de los datos de la Asociación que resulta ser al fin de cuentas la meta primordial del estudio.

D.2) LIMITACIONES

Las limitaciones son obstáculos que se contraponen en la continuidad y desempeño del proyecto, en este caso al ser el proyecto de investigación un tema, relativamente nuevo y por ende de poco estudio a nivel nacional, se presentan problemas tales como: la falta de documentación y recursos, lo cual impide un poco, realizar el estudio más en profundidad y con lleva también a realizar una búsqueda más exhaustiva de información que vaya a servir como referencia; entonces al existir poco material bibliográfico, es necesario que la mayoría de fuentes sean provenientes de la Internet.

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

A) SITUACIÓN ACTUAL DE LA RED DE DATOS DE LA ASOCIACION

A partir de finales del año 2004, la Asociación cuenta con nuevas instalaciones, ya que debido al crecimiento a nivel operativo y funcional que ésta ha tenido, fue necesaria la adquisición de otro edificio para beneficio tanto de los asociados, así también como de los 90 empleados que laboran en oficinas centrales, los cuales en su gran mayoría hacen uso de una computadora, y por ende de la red y los diversos sistemas que hay en ella.

A.1) ELEMENTOS FUNDAMENTALES PARA EL ESTABLECIMIENTO DE LA RED

De acuerdo a lo anterior, la red se encuentra desarrollada, con los siguientes elementos:

- Se utilizó cableado UTP CAT6.
- Cada planta del edificio, cuenta con un rack (IDF), en el cual desembocan todas las puntas.
- La estructura principal de red (BACKBONE) fue diseñada en fibra óptica.
- Cada piso del edificio cuenta con un Rack por piso
- Cada Rack de piso cuenta con 3 segmentos de red
- Cada segmento de red subdivide áreas de trabajo
- Cada área de trabajo se compone de fibra óptica independiente hasta el Rack principal.
- Cada Rack cuenta con tres líneas de respaldo de fibra óptica por cada segmento de red

- Cada fibra óptica cuenta con 24 hilos, los cuales el 50% está para desarrollo en cualquier campo de telecomunicaciones a futuro para la Asociación.
- Cada Rack cuenta con protección independiente en caso de caídas de voltaje, así como sobre voltaje, evitando interferencia en las comunicaciones de voz y datos.

En detalle el Rack principal cuenta con dispositivos de comunicación tales como:

- Switches 3COM Fibra Óptica / UTP → Core principal.
- Router CISCO 2600→ Enlace canalizado y principal con Sucursales y Unidades Empresariales.
- Router CISCO 1700 → Enlace dedicado de Internet a 512 Mbps.
- Otros equipos.

A.1.1. Puntos indispensables para la seguridad y funcionamiento de la red

- Como medida de seguridad, en algunos puntos críticos, se recubrió el cableado eléctrico con un material aislante conocido como BX, con el fin de evitar interferencia en las zonas donde no se podía corregir el problema de interferencia eléctrica; dando buenos resultados.
- Se tiraron puntos no previstos de red, que eran necesarios en algunos departamentos para cubrir las necesidades de instalar impresoras de red.
- Posteriormente, se separo cada piso del edificio en 3 segmentos de red, los cuales tienen como función, prever una eventual caída, previniendo que el daño sea menor, y que así se pueda aislar para resolverlo, sin detener la operativa completa.

- Se instaló en cada planta del edificio un IDF, (equipo en el cual convergen los puntos centrales de red, provenientes de cada segmento).
- En el Cuarto Piso, en el departamento de Informática, se montó el MDF dentro del área de telecomunicaciones, en este lugar convergen los puntos principales centrales de toda la estructura de red de datos (fibra óptica exclusivamente).
- El enlace que se realizó entre cada nivel del edificio, fue realizado con fibra óptica.
- Posterior al tiraje del cable UTP, se estableció la fibra óptica, está como se mencionó anteriormente, va desde el primer hasta el último piso, cubriendo el backbone de toda la red, hasta el cuarto de comunicaciones, terminando en los switches del CORE principal.
- También se montó varias líneas de respaldo de fibra óptica, esto como medida de contención, en caso de perder conectividad en una fibra, entraría la otra a funcionar.
- Posteriormente en el rack principal del área de comunicaciones en la oficina del departamento de Informática se instalaron los extremos finales de las fibras en los equipos respectivos.

A.2) SISTEMAS Y APLICACIONES

Tanto en oficinas centrales como en las sucursales, se utiliza un sistema propio de la Asociación, en el cual se maneja todo lo que se refiere a las cuentas corrientes de los asociados, este fue realizado bajo Visual Basic, que controla un motor de base de datos SQL Server. Así también, existe un sistema de mensajería a nivel interno, exclusivamente para los empleados; a parte a esto se desarrollan diversos sistemas a la medida tanto en el área financiero/contable, como en el área administrativa, adquiridos a diversas empresas; y por ultimo se utiliza un servidor Exchange para mensajería administrativa con oficinas centrales y las sucursales.

Actualmente la red cuenta con un aproximado de 100 estaciones de trabajo (sucursales, oficinas), enlazadas a los diversos servidores (producción, prueba, antivirus, Internet, etc), mediante switches, los cuales se encargan de segmentar toda la red, y por último se encuentran varios routers, que tienen funciones especificas; el primero de ellos, tiene la tarea de enlazar tanto las sucursales como las unidades empresariales; y el segundo se encarga de realizar el enlace hacia Internet.

A.2.1. Tipos de servidores implementados en la Asociación
(Plataforma Windows 2000 SP4)

Cada uno de los servidores de la Asociación tiene particularidades y funciones muy específicas, es decir que dependiendo de las tareas que realice así son las características técnicas que este tiene, como se podrá observar hay algunos que requieren más velocidad del procesador, otros más memoria, o inclusive más espacio de almacenamiento.

a) Servidor 1

- *SQL Server 2000 SP3 → Pruebas*
    i. Pentium 4 2.0GHZ
    ii. 1 GB RAM

Se utiliza para realizar diversas pruebas con los sistemas recientes o con alguno de los ya implementados, pero que necesitan realizar pruebas con la base de datos.

b) Servidor 2

- *SQL Server 2000 SP3 → desarrollo (menor escala)*
    i. Pentium 3 1.0GHZ
    ii. 128 MB RAM

Es utilizado para desarrollar e implementar sistemas de menor escala en el grado de complejidad, lo cual se ve claramente reflejado en las características que posee dicho equipo.

c) Servidor 3

- *Active directory*
- *SQL Server 2000 SP3*
- *Exchange 2000 SP3*
- *DHCP*
    i. ML530
        1. Pentium III XEON 1.0GHZ
        2. 4 GB RAM
        3. Raid 5 (18,2 GB)

En un principio fue utilizado como el servidor principal de producción, pero debido al crecimiento tanto de los sistemas, como de las funciones que estos realizan, se decidió entonces, dejar a este como el servidor de dominio principal y como el servidor de mensajería interna.

d) Servidor 4

- *ISA SP1 (Internet)*
  - i. Pentium 4 2.5 GHZ
  - ii. 512 MB RAM

Actualmente es utilizado como filtro que deniega o permite el acceso de los usuarios de Oficinas Centrales a la Internet, por medio de políticas y reglas de seguridad.

e) Servidor 5

- *Antivirus / Symantec Antivirus Corporate Edition*
- *Servidor* de Respaldo de Archivos
  - i. AMD Athlon XP 2.4 GHZ
  - ii. 1 GB RAM
  - iii. 200 GB

Se encarga de administrar el antivirus corporativo de toda la Empresa, así también como de fungir como servidor de respaldo de archivos de los usuarios.

f) Servidor 6

Servidor de base de datos PRODUCCIÓN (SQL SERVER 2000 SP3)

i. ML370 G3
   1. Intel XEON 3.2 GHZ - DUAL
   2. 4 GB RAM
   3. Raid 5 (72,2 GB)

De todos los servidores es el que tiene la función más importante, ya que se encarga de administrar las bases de datos principales, así como de los sistemas de producción; por las características que posee, es el más robusto de todos.

g) Servidor 7 (Proceso de Implementación)

Servidor Web / Email

- ii. Pentium 4 2.4 GHZ
- iii. 1 GB RAM

iv. SCSI
    1. 72 GB

Con los cambios que se están realizando, también se está montando un servidor que va a fungir con la función de Hosting o hospedaje de las páginas de la Asociación, así como del correo externo.

A.2.2. Estaciones de Trabajo

Una estación de trabajo, es toda aquella computadora, que se encuentra en un ambiente de red corporativo o empresarial.

En el caso de la Asociación, entre todos los funcionarios tanto de oficinas centrales como de las sucursales, existen un aproximado de 100 Computadoras (PC'S), de las cuales 20 tienen como sistema operativo Windows Millenium, 80 Windows XP SP2 y por último una computadora de diseño gráfico Macintosh, con sistema operativo OS X (Tiger).

A.2.3. Rack principal y secundario

A.2.3.1) Rack Principal o Armario Principal

(Cuarto de telecomunicaciones)

El rack principal de la Asociación, cuenta con los siguientes dispositivos de red:

- 2 Switch 3COM 4950 → Backbone de todo el edificio
- 1 Switch 3COM 4400 SE → DMZ (Proceso de Implementación)
- 1 Router Cisco 2600 → Sucursales, UE.
- 1 Router Cisco 1700 → Internet
- 2 Modem NTU → Sucursales, UE
- 1 Modem HDSL PairGain → Internet
- 1 Modem MDSL E1 → Canalizado E1.

A.2.3.2) Rack por Piso o Armario Secundario (Ubicados en los 4 pisos)

Los racks por piso de la Asociación, cuentan cada uno con los siguientes dispositivos de red:

- 3 Switch D-Link Gigabit DGS- 1224T
    - 24 PUERTOS / 2 F.O.

A.2.4. Función de los servidores con las sucursales

Con lo respecta a las sucursales, estas pueden acceder el servidor de producción de las oficinas centrales, mediante el sistema principal, además de realizar consultas al servidor del controlador de dominio, también el servidor antivirus los monitorea las 24 horas al día. Por otra parte se puede acceder el servidor de respaldo de archivos; pero no se les es permitido tener acceso a las estaciones de trabajo de las demás sucursales, así como de las oficinas centrales, todo esto por medidas de seguridad que se han ido implementado.

A.3) PUNTOS DEBILES EN LA SEGURIDAD FISICA DE LA RED DE LA ASOCIACIÓN

En la Asociación, se presentan algunos puntos débiles en la seguridad de los datos, así como de las comunicaciones, pasando tal vez desapercibidas por el personal de informática, entre los que se destacan los siguientes:

A.3.1. Acceso a áreas restringidas

Para acceder el cuarto de servidores, se cuenta con llavines ordinarios, a los cuales solamente los encargados de soporte del área de informática, tienen acceso; sin embargo, en algunas ocasiones debido a la necesidad de solventar algún inconveniente con el sistema, la red, o ayudar a algún usuario, dichos encargados, dejan sin restricción alguna el acceso al lugar lo cual podría facilitar el ingreso de personas no autorizadas.

En ocasiones, el cuarto de servidores, es visitado por algunos técnicos de otras empresas, que vienen a realizar soporte o algún trabajo en específico, y no se controla con ninguna bitácora o registro de dicha visita.

El lugar en donde se encuentra ubicado el *rack* del primer piso, posee también la caja interna de pares telefónicos del ICE; el acceso a este lugar es solo por llave, aunque en algunas ocasiones el personal del ICE, cuando debe realizar algún trabajo ahí, no obstante si ellos quisieran podrían tener acceso a lo que es el equipo de telecomunicaciones.

A.3.2. Cables expuestos

El cableado permanece a lo largo de las 4 plantas y diversos departamentos, este se encuentra montado en canaletas debidamente ubicadas, sin embargo en los departamentos que se encargan de atención al cliente, en varios puntos el cable de las estaciones de trabajo, se encuentran al alcance del público; siendo esto un problema, ya que en cualquier momento algún niño o asociado podría llegar a quitar o desconectar alguno de ellos.

A.3.3. Equipos ociosos

Actualmente la Asociación, cuenta como medida de seguridad ante alguna eventualidad con varios equipos de telecomunicaciones disponibles, en el caso que se deba sustituir alguno; no obstante con respecto a los servidores no sucede lo mismo, ya que por sus características no se cuenta con otro similar, ni con la función de equipo ocioso, es decir que en algún momento si el arreglo de discos duros, o ya sea la tarjeta madre, por ejemplo, se llegase a dañar, no existe otro servidor con las mismas características, para montar el respaldo del servidor dañado, y con esto reducir el tiempo de inactivad del servicio.

A.3.4. Línea de respaldo de Internet

La Asociación, cuenta con una línea dedicada a la red de Internet con un ancho de banda de 512 MB, no obstante si por alguna razón dicho enlace se dañara, no se cuenta con una línea redundante o de respaldo para solventar el problema, en el caso de los departamentos que hacen más uso de dicho servicio y que más lo requieren, sí se cuenta con alguna conexiones conmutadas pero no dan abasto en algunas ocasiones con la demanda del servicio.

A.4) RIESGOS DE SEGURIDAD EN LOS PUERTOS DE LA ASOCIACION (DEBILIDADES EN LA SEGURIDAD)

Utilizando el software especializado Tenable NeWT, mismo que se encarga de medir y analizar las vulnerabilidades existentes en la red, se obtuvo un reporte de seguridad de la red de la Asociación, en este se hace mención acerca de los huecos de seguridad mismos que resultan ser algunos puertos, los cuales son una eventual puerta para el acceso de algún tipo de amenaza, y con esto desencadenar consecuencias muy serias.

Por medidas de seguridad, solamente se van a mencionar algunos puertos encontrados en dicho reporte.

A.4.1. Puertos problemáticos encontrados en la red

- **Puerto 25:** Este puerto es utilizado por el servidor de mensajería interna, un sistema que en la actualidad es muy dado a contar con ataques, por contar entre sus funciones con la facilidad de propagar los mensajes a múltiples usuarios, entre otras cosas.

- **Puerto 110:** Al igual que el anterior, este puerto es utilizado por el servidor de mensajería interna, y cuenta con la misma vulnerabilidad.

- **Puerto 135:** El puerto 135 se utiliza para iniciar una conexión RPC con un equipo remoto. El bloqueo del puerto 135 en el servidor de seguridad ayudaría a evitar que los sistemas situados detrás de dicho servidor de seguridad fueran víctimas de cualquier ataque que intentara aprovechar este punto vulnerable.

- **Puerto 139:** El puerto 139 (netbios) está abierto por defecto en la mayoría de los sistemas operativos de Microsoft, permite compartir impresora y archivos. Aunque para la comunicación remota con la computadora es necesaria una clave, esta por un bug (fallo, error) es muy fácil de saltar, incluso para personas sin muchos conocimientos.

- **Puerto 443:** El puerto 443 es utilizado por el protocolo SSL (Secure Sockets Layer), una tecnología que proporciona comunicación segura de datos mediante el cifrado y descifrado de los mismos. SSL es ampliamente utilizado por aplicaciones y servidores que requieran un vínculo seguro, como los relacionados con el comercio electrónico; por tal motivo resulta muy llamativo para realizar algún tipo de violación a la seguridad, y con esto obtener información fidedigna.

- **Puerto 445:** Este puerto está habilitado por defecto en los sistemas de Microsoft, una consulta a este puerto hace posible conocer: el nombre del dominio de la red, así como conocer la versión y tipo del Sistema Operativo del administrador remoto de la red.

- **Puerto 6883:** Puerto desconocido, al parecer un servicio desconocido se encuentra corriendo en este puerto; los troyanos por lo general lo utilizan para obtener la información que requieren o realizar alguna acción en específico.

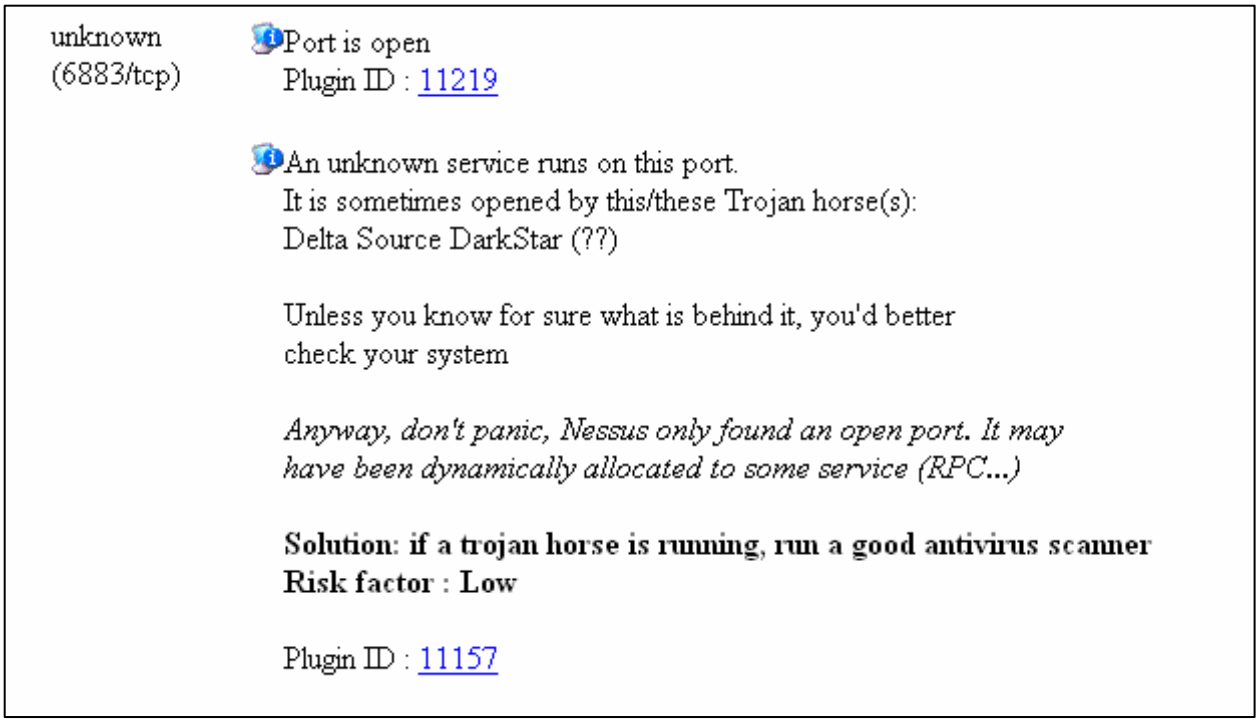


Figura No 2. Análisis de vulnerabilidades

En esta gráfica se muestra un ejemplo de los resultados obtenidos mediante el software de análisis de vulnerabilidades que se ejecuto en uno de los servidores de la red de la Asociación 2005.

Ver Anexo. No.1, para ejemplo de análisis de Vulnerabilidad a una estación de trabajo con el sistema operativo Windows XP y el Service Pack 2.

A.5) DIAGRAMA DE LA RED DE LA SITUACIÓN ACTUAL EN LA ASOCIACIÓN

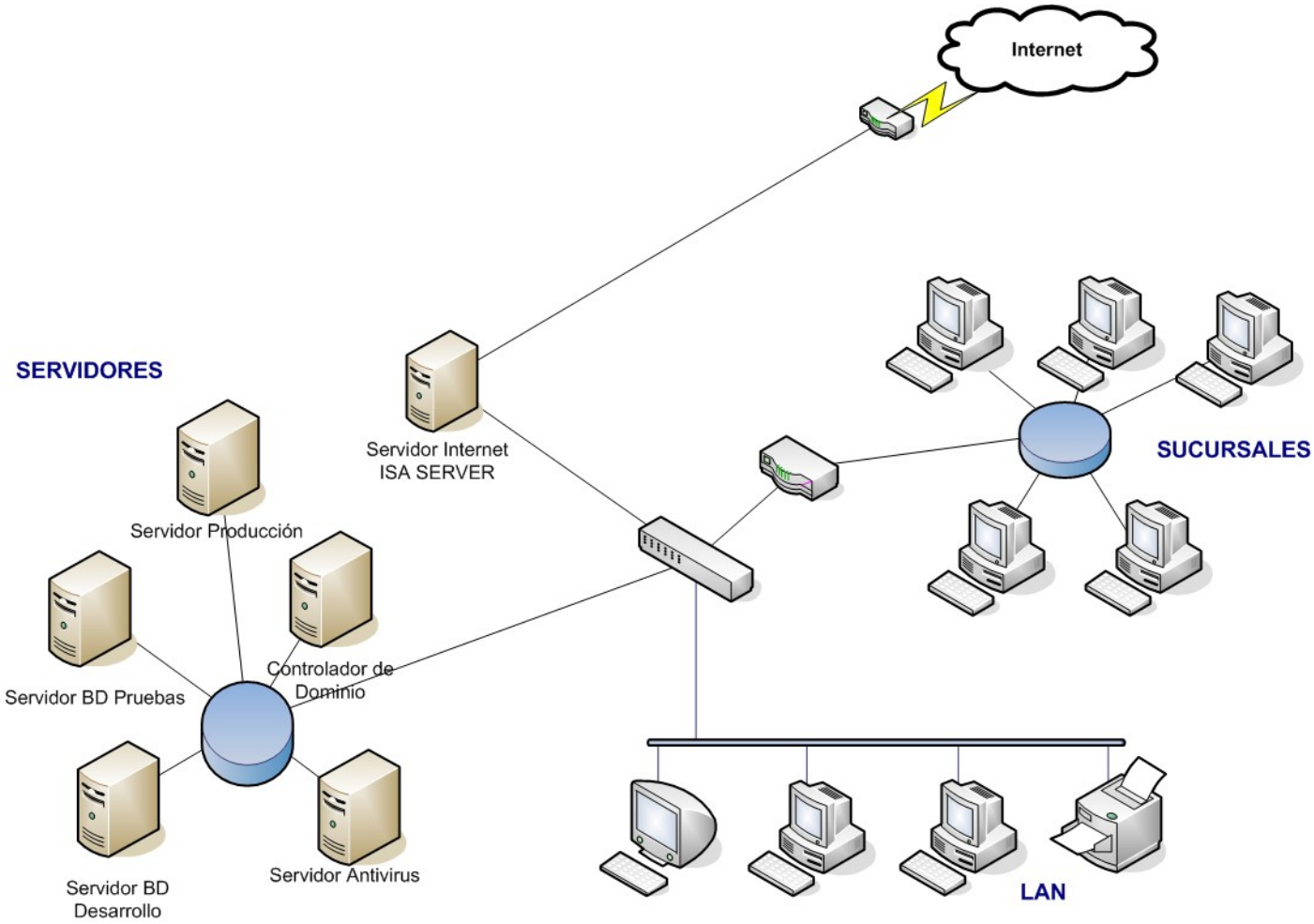


Figura No 3. Diagrama situación actual, sin implementar la DMZ. 2005.

B) SITUACIÓN DESEADA DE LA RED DE LA ASOCIACIÓN

Como se ha mencionado anteriormente, la DMZ o Zona Desmilitarizada es actualmente una de las herramientas más utilizadas a nivel mundial por las empresas como medida de seguridad en las redes de datos.

La DMZ en síntesis, termina siendo una red donde todos los servicios ubicados en ella, van a ser accesibles para las demás personas que vayan a acceder por medio de la Internet.

Existen diversas formas de diseñar una DMZ, el diseño final depende tanto de los recursos económicos con los que cuenta la empresa, así como también la estructura de red que ya se tiene establecida.

B.1) EQUIPOS QUE SE REQUIEREN PARA LA PUESTA EN MARCHA DE LA DMZ

A continuación se presentan los equipos que se requieren para poner en marcha la implementación de una DMZ

B.1.1. Firewall

Un cortafuegos o firewall en Inglés, es un equipo de hardware o software utilizado en las redes para prevenir algunos tipos de comunicaciones prohibidos por las políticas de red, las cuales se fundamentan en las necesidades del usuario.

B.1.1.1) Tipos de firewall

a) Firewall de capa de red.- Funciona al nivel de la red de la pila de protocolos (TCP/IP) como filtro de paquetes IP, no permitiendo que estos pasen el cortafuego a menos que se atengan a las reglas definidas por el administrador del firewall o aplicadas por defecto como en algunos sistemas inflexibles de cortafuego. Una disposición más accesible por ejemplo, podría permitir que cualquier paquete pase el filtro mientras que no cumpla con ninguna regla negativa de rechazo.

b) Firewall de capa de aplicación.- Trabaja a nivel de aplicación, todo el tráfico de HTTP, (u otro protocolo), puede interceptar todos los paquetes que llegan o salen de una aplicación. Se bloquean otros paquetes (generalmente sin avisar al remitente). En principio, los firewall de aplicación pueden evitar que todo el tráfico externo indeseado alcance las computadoras protegidas.

B.1.1.2) Ventajas de un firewall

- Protege de intrusiones.- Solamente entran a la red las personas autorizadas basadas en la política de la red en base a las configuraciones.

- Optimización de acceso.- Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa si así se desea. Esto ayuda a reconfigurar rápida y fácilmente los parámetros de seguridad.

- Protección de información privada.- Permite el acceso solamente a quien tenga privilegios a la información de cierta área o sector de la red.

- Protección contra virus.- Evita que la red se vea infestada por nuevos virus que sean liberados.

B.1.1.3) Función de los firewalls

Un Proxy Server, puede actuar como un firewall respondiendo a los paquetes de entrada como si fuera una aplicación mientras que bloquea otros paquetes.

Los firewalls tienen a menudo funcionalidad de traducción de direcciones de red (NAT) y es común utilizar el así llamado espacio de direcciones privadas en las computadoras detrás de ella. Este espacio de direcciones privadas se realiza como un intento (de eficacia discutible) de disfrazar las direcciones internas o de red.

La configuración correcta del firewall se basa en conocimientos considerables de los protocolos de red y de la seguridad de la computadora. Errores pequeños pueden dejar a un cortafuego sin valor como herramienta de seguridad.

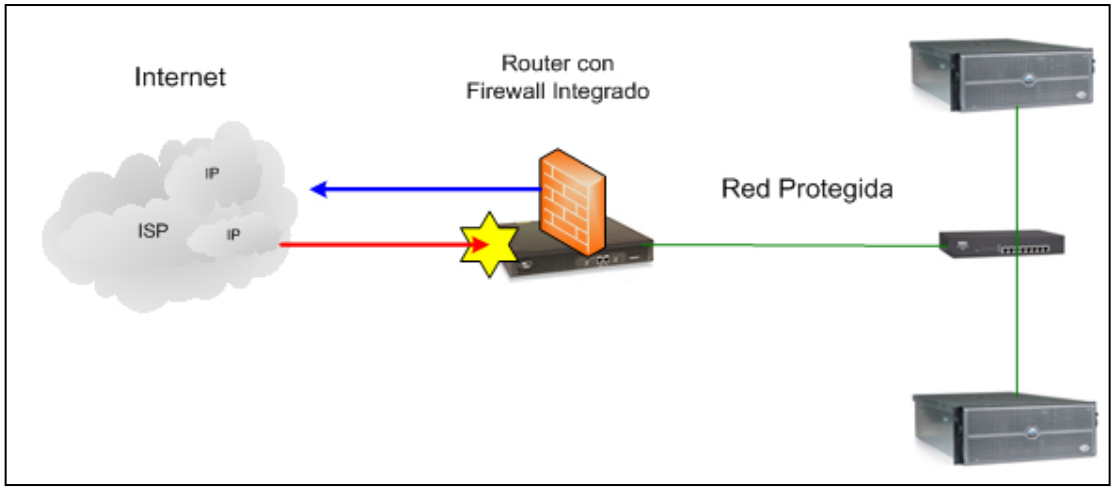


Figura No 4. Funcionamiento del Firewall

La imagen muestra el funcionamiento de un firewall de capa de [[red]], permitiendo el libre acceso de la red interna hacia otros dispositivos y al exterior mientras que el firewall restringe el acceso a ciertos servicios y usuarios de Internet.

B.1.1.4) Firewall propuesta para implementarlo a la DMZ

Como se mencionó anteriormente con lo que se refiere a dispositivos de seguridad, específicamente los firewalls, existen de dos tipos, la parte Hardware y la parte Software, es por eso que para la Asociación, se esta contemplando un firewall que cumple tanto la parte hardware como la de software, en esta línea de dispositivos de seguridad, el que se esta estimando es el Gateway Security 5420, de Symantec, una herramienta hardware-software de seguridad de red para protección perimétrica de entornos heterogéneos de comunicaciones TCP/IP (Internet/Extranet/Intranet) robusta, de gran efectividad, rica en funcionalidades, con balanceo de carga/alta disponibilidad que puede ser clasificada como pasarela de seguridad. Este firewall integra en un mismo dispositivo diversas tecnologías: cortafuegos-*proxy*, antivirus, detección y prevención de intrusiones, filtrado de

contenidos, anti-*spam*, detectándose una reducción significativa de la complejidad de la gestión global de la seguridad. Se puede colocar en diferentes puntos de la red corporativa, tanto en las fronteras con Internet como entre subredes de intranets o extranets.

El Symantec Gateway Security 5420, entre sus funciones como ya se ha mencionado anteriormente, provee firewall integrado, antivirus, detección y prevención de intrusos, filtra el contenido y también anti-spam.

El sistema operativo con el que cuenta el Symantec Gateway Security 5420 es una distribución personalizada de Linux (versión del kernel 2.4.18). Por las características propias que posee este Sistema Operativo es uno de los más robustos o menos atacados del mercado a nivel mundial.

Analizando más a profundidad, el tipo de firewall que utiliza es muy versátil en su funcionalidad. Este hibrido utiliza filtrado de paquetes para eliminar paquetes sospechosos rápidamente, a su vez que separa los segmentos de red para inspeccionarlos.

Con lo que se refiere a la prevención de intrusos es cuando ocurre un intento de quebrantar la seguridad, tan pronto como es identificada, este es bloqueado, aparte de dar la alerta sobre el intento, los paquetes que comprometieron la seguridad son destruidos.

La detección de intrusos es una manera de reconocer que alguien, en algún lado está intentando pasar trafico malicioso a la red. Esto podría significar que alguna persona, tal vez un hacker ha empezado un ataque con la esperanza de irrumpir en la red, o también dado el caso, podría significar que un usuario principiante y sin mala intensión, ejecutó un programa o aplicación que contiene

un código malicioso. La detección de intrusos no necesariamente indica que el ataque fue satisfactorio, solamente que este fue realizado. Existen otros factores que podrían determinarlo, tales como el sistema operativo de la maquina, la aplicación usada, los parches aplicados y las habilidades del atacante.

B.1.2. Servidores

Uno de los equipos o dispositivos más importantes que se van a encontrar dentro de la DMZ, son los servidores, ya que estos deben ser seleccionados de forma muy cuidadosa, debido a que de una u otra forma son los que van a estar expuestos a cualquier tipo de usuario externo.

B.1.2.1) Características que deben presentar los servidores de la Asociación

Los servidores que se van a encontrar dentro de la DMZ, no deben contener datos propietarios o críticos, es decir que no son únicos. Además que pueden ser reemplazados de forma rápida y fácil.

Según las características presentadas en la Asociación, y en base a los requerimientos que se tiene, los servidores que estarán dentro del perímetro de la DMZ, y por ende expuestos al exterior serían:

a) Servidor Web / Email
   Pentium 4 2.4 GHZ
   1 GB RAM
   SCSI
   72 GB

   Como se menciona anteriormente en el presente documento, este servidor va a fungir con la función de Hosting o hospedaje de las páginas de la Asociación, así también como del correo externo.

b) Servidor Internet
   ISA Server SP1 (Internet)
   Pentium 4 2.5 GHZ
   512 MB RAM

Al igual que el anterior, sus características y funciones ya fueron mencionadas, no obstante a la hora de implementarlo dentro de la DMZ, a parte a las funciones que tiene actualmente como filtro que deniega o permite el acceso de los usuarios de Oficinas Centrales a la Internet en forma de Proxy, también se va a encargar de publicar los servicios encontrados en los servidores de la DMZ, y va a proporcionar una mayor protección gracias a que controla el tráfico procedente de Internet; todas estas funcionalidades se van a dar mediante una nueva configuración y reestructuración de sus funciones.

La configuración, consiste principalmente en instalar tres tarjetas de red. Una de las tarjetas va a ser la tarjeta de red a Internet, la segunda va a estar conectada a un switch separado donde se va a poner todos los equipos públicos dentro del perímetro y por último la tercer tarjeta va a estar conectada a la red interna de la Asociación.

Cuando un usuario, acceda algunas de las páginas de Internet de la Asociación, por ejemplo: la página principal, en ella va a digitar tanto su usuario, como su password o contraseña, e inmediatamente accederá un menú en el cual va poder realizar diversas acciones, donde una de las más importantes sería la consulta de su estado de cuenta; técnicamente dicha consulta va a ser realizada dentro del servidor web y correo externo, posteriormente este va a realizar un túnel virtual con el servidor de producción en el cual se encuentra almacenados todos los datos de su cuenta, dicho túnel va a ser realizado mediante un puerto exclusivo (447), el cual permite solamente, en este caso, realizar consultas a la base de datos de su usuario en especifico.

B.2) ZONAS DE SEGURIDAD DESEADAS PARA IMPLEMENTAR LA DMZ

A parte a los equipos ya mencionados, también es necesario contar con diversas zonas de seguridad como:

B.2.1. La red exterior: Se refiere a lo que es Internet y cualquier otra red que quede fuera del control administrativo interno.

B.2.2. El backbone de la red corporativa: es la zona de la red bajo el control administrativo, pero no contiene servicios ni servidores "mission-critical". La zona de seguridad del backbone corporativo sirve como sistema de interconexión seguro entre todas las demás zonas de seguridad.

B.2.3. La red interna: esta zona de seguridad de la red contiene servidores y clientes que están completamente bajo el control administrativo. Todos los usuarios y computadoras que pertenecen al dominio corporativo de la Asociación, se localizan en la zona de la red interna. Los diversos segmentos LAN unidos por el backbone corporativo pertenecen todos a la misma zona de red interna.

B.2.4. Red de Administración: una zona de gestión de red dedicada a los clientes y servidores necesarios para llevar a cabo las tareas administrativas. Esta red ha de ser monitorizada y controlada muy estrechamente debido al alto nivel de privilegios asignados a los usuarios en esta red.

Una de las zonas más importantes es la red interna. Esta red está detrás de la red externa, del backbone corporativo y de la DMZ. La red interna es la zona de seguridad que necesita mayores defensas frente a los ataques externos.

B.3) POLÍTICAS DE SEGURIDAD

- La administración y el mantenimiento de la DMZ, es exclusivo de los encargados de soporte del departamento de Informática de la Asociación.

- El acceso al área del cuarto de telecomunicaciones (lugar donde se va a encontrar físicamente la DMZ), debe estar restringido para todo personal no autorizado.

- Se deberá llevar una bitácora formal de acceso al cuarto de telecomunicaciones por parte de terceros, en el cual se debe especificar quién fue la persona que ingreso, que tareas realizó, así como el tiempo que le llevo realizarlas.

- Se deberá establecer un plan de mantenimiento de la DMZ, por parte del personal a cargo; esto deberá incluir actualizaciones tanto de los sistemas operativos como de los demás sistemas de los servidores, así también como las actualizaciones del Symantec Gateway Security 5420, Antivirus, etc. Por a parte a esto, también se deberá dar mantenimiento físico.

- Se deberá establecer, un estricto plan de respaldos de toda la información contenida en los servidores, por consiguiente a esto, también:
    - Almacenar los respaldos en medios magnéticos, en un lugar seguro y fresco, libre de polvo y de señales electromagnéticas.

- Por a parte a las ya mencionadas políticas, de igual forma es primordial que en el área de telecomunicaciones, existan extintores especiales, para equipo de computo y eléctrico, así también la temperatura ambiente del lugar debe de estar menor a 21 grados Celsius.

B.4) DIAGRAMA DE RED DE LA SITUACIÓN DESEADA EN LA ASOCIACIÓN

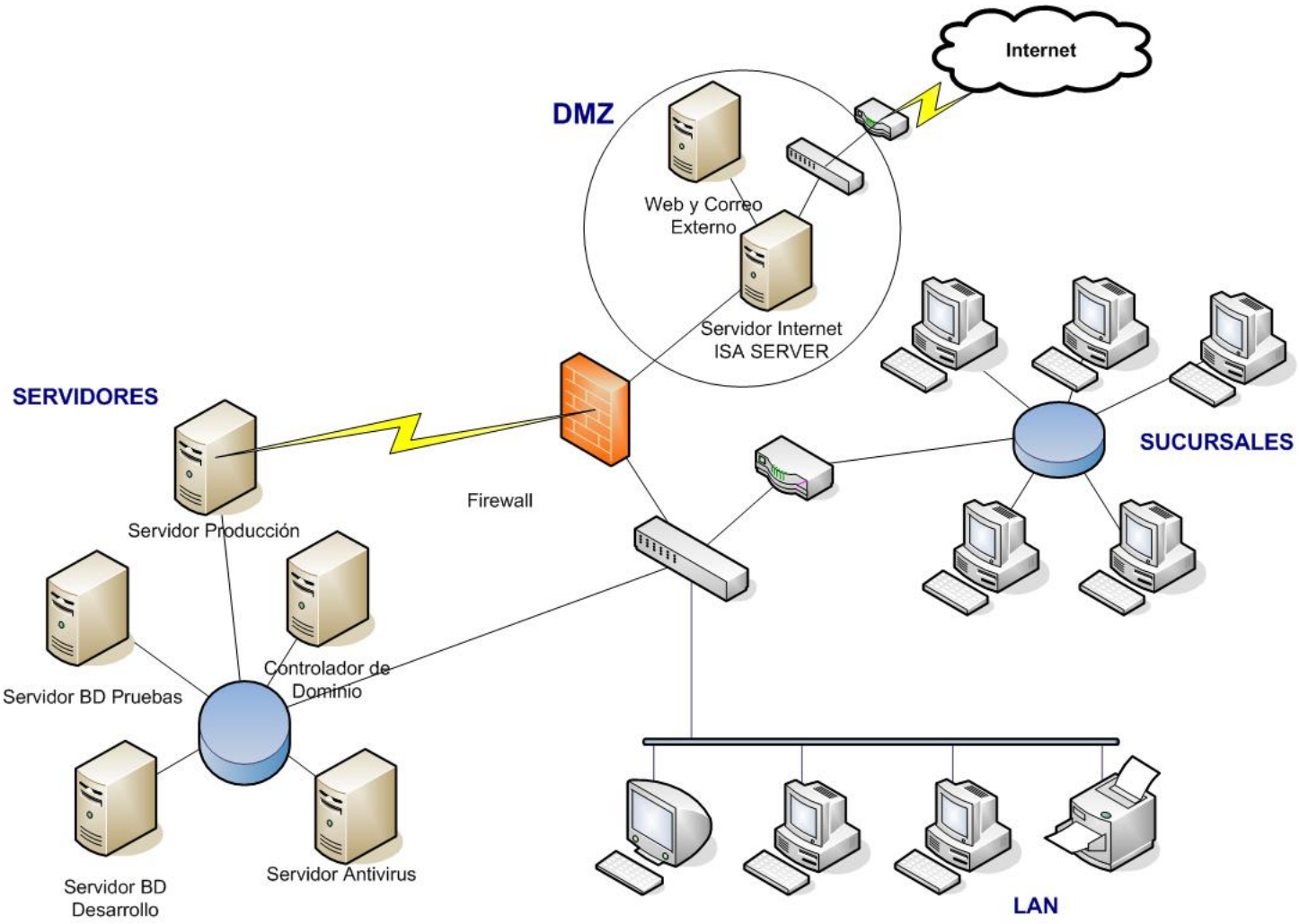


Figura No 5. Diagrama de la nueva estructura de la red, una vez implementada la DMZ. 2005.

B.5) COSTOS Y CARACTERISTICAS DE LOS EQUIPOS NECESARIOS PARA DESARROLLAR LA DMZ

TIPO DE EQUIPO	MARCA / MODELO	CARACTERISTICAS	PRECIO
FIREWALL	SYMANTEC SYMANTEC GATEWAY SECURITY 5420	Firewall-*proxy* Detección / prevención de intrusiones Filtrado de contenidos Anti-*spam* *Antivirus* -Actualizaciones 2 años -Licencias / 200 nodos -Instalación -Puesta en marcha	$10639.60
SERVIDOR		Mainboard INTEL D865GBF Proc. 2.4 ghz 533mhz Mem. Ddr 512mb 333 mhz Tarj. SCSI Adaptec 19160 PCI 64 bits Disco Duro 73GB SCSI Disco Duro 36GB SCSI Tarj. Red PCI 3COM Giga 3C2000-T Cd-rom 48x Monitor / Teclado /Mouse	$1780
TARJETAS DE RED	3COM 3C2000-T	3 Tarj. Red PCI 3COM Giga 3C2000-T	$225

Tabla No 1. Fuente: Entrevista realizada a los proveedores respectivos de cada equipo. Convexo S.A. y Allicon Internacional, S.A. 2005

C) RESULTADOS OBTENIDOS

Las encuestas para los Asociados fueron realizadas a 327 personas, una cantidad inclusive mayor al número obtenido por la fórmula para calcular la muestra; dichas encuestas fueron realizadas en diversas sucursales, ubicadas en las provincias de Alajuela, San José, Cartago y Heredia.

La encuesta contiene un total de 12 preguntas, de las cuales muy pocas son de carácter abierto, y la mayoría son preguntas cerradas, esto con el fin de que el asociado muestre interés y sienta que no se le está indagando más allá de asuntos personales y que pudiesen comprometerlos. De esta manera las interrogantes son claras y concretas para que no se pierda el concepto de lo que se está solicitando.

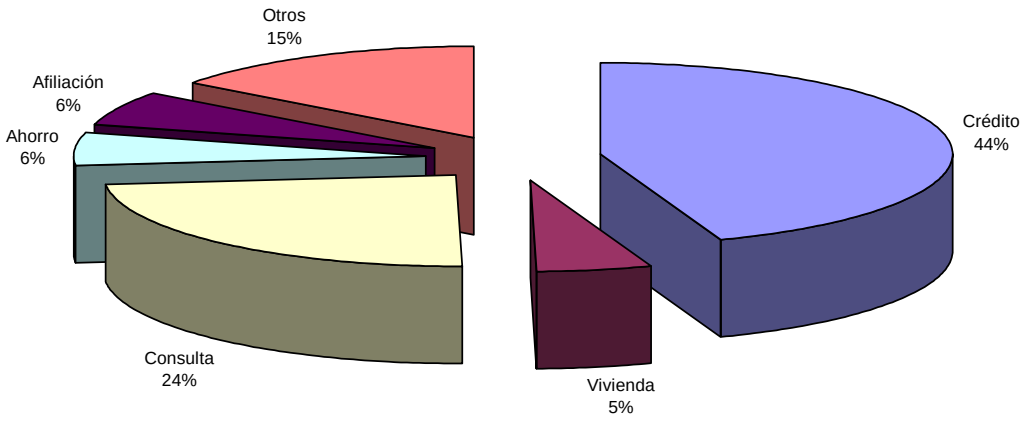
Los principales resultados obtenidos sobre las encuestas efectuadas a los asociados, son los siguientes:

De acuerdo a la primera pregunta, referente al tiempo de permanencia en la asociación, el 33% dijo que tenían menos de tres años de ser asociados, el 28% respondieron que tenían entre 4 a 7 años, el 21% se han mantenido de 8 a 11 años, el 8% de 12 a 16 años, y el 11% no quisieron dar respuesta. De esta manera, actualmente más del 80% de los asociados se han integrado durante la última década a la asociación, hecho que se puede interpretar como el respaldo que dichos miembros muestran para con ella; por ende cada vez más se hace indispensable fortalecer los sistemas informáticos que resguardan los intereses tanto de la asociación como de sus propios asociados.

De las actividades referentes a trámites (ver gráfico No.1), el 44% de la población realizan algún tipo de crédito; un 24 % hace consultas sobre sus estados de cuenta, 15 % gestionan asuntos de beneficio social, becas, ayudas de sepelio entre otros; un 6% de ahorro y afiliación respectivamente; y un 5% de vivienda.

Gráfico No.1

Tipo de trámite que realizan los Asociados en la Asociación Solidarista de Empleados de un Ente Público. Marzo 2005

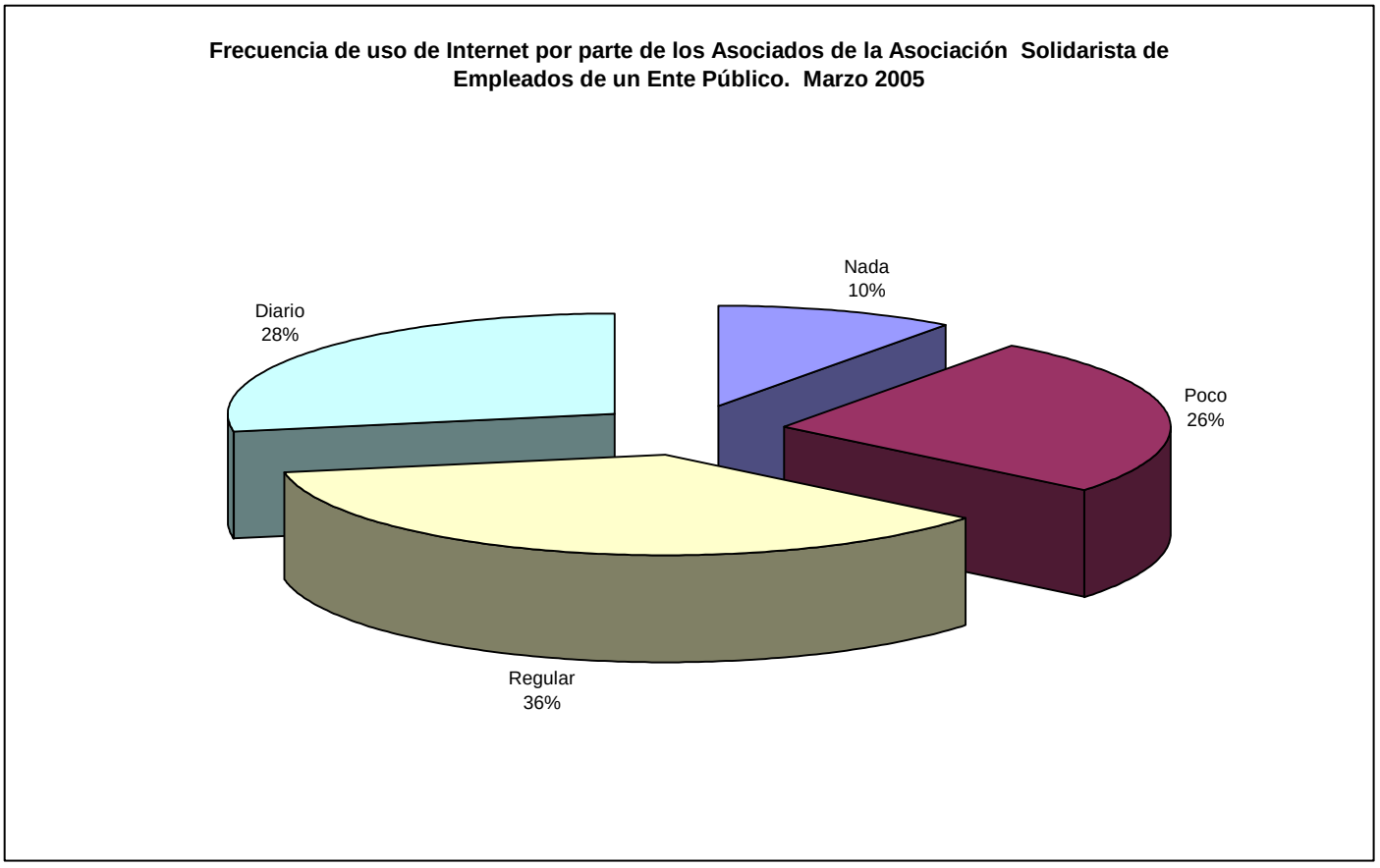


Otro componente importante que se tomó en cuenta fue el grado de conocimiento que poseen los asociados sobre el uso de la Internet; el 80 % de ellos indicaron que tenían conocimientos sobre Internet, mientras que el 20 % restante mencionaron que no lo tenía.

De acuerdo a ese 80% que si conocen Internet se obtuvo lo siguiente:

En cuanto al uso regular de dicho medio, el 36 % accedía regularmente, el 28 % lo hace a diario, el 26 % muy poco y el 10 % respondieron que no lo utilizaban. Ver gráfico 2.

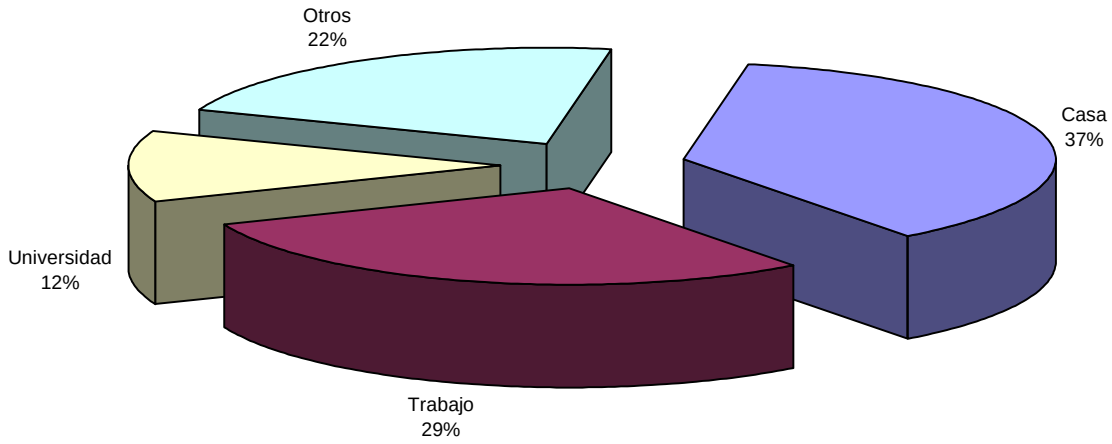
Gráfico No. 2



Con respecto a los puntos o lugares de acceso que los asociados utilizan para ingresar a la red, el 37 % tenían lo hacen desde sus casas, el 29 % desde el trabajo, un 22 % lo hace desde algún lugar tipo Internet Café, y un 12 % desde la universidad. Ver gráfico No.3.

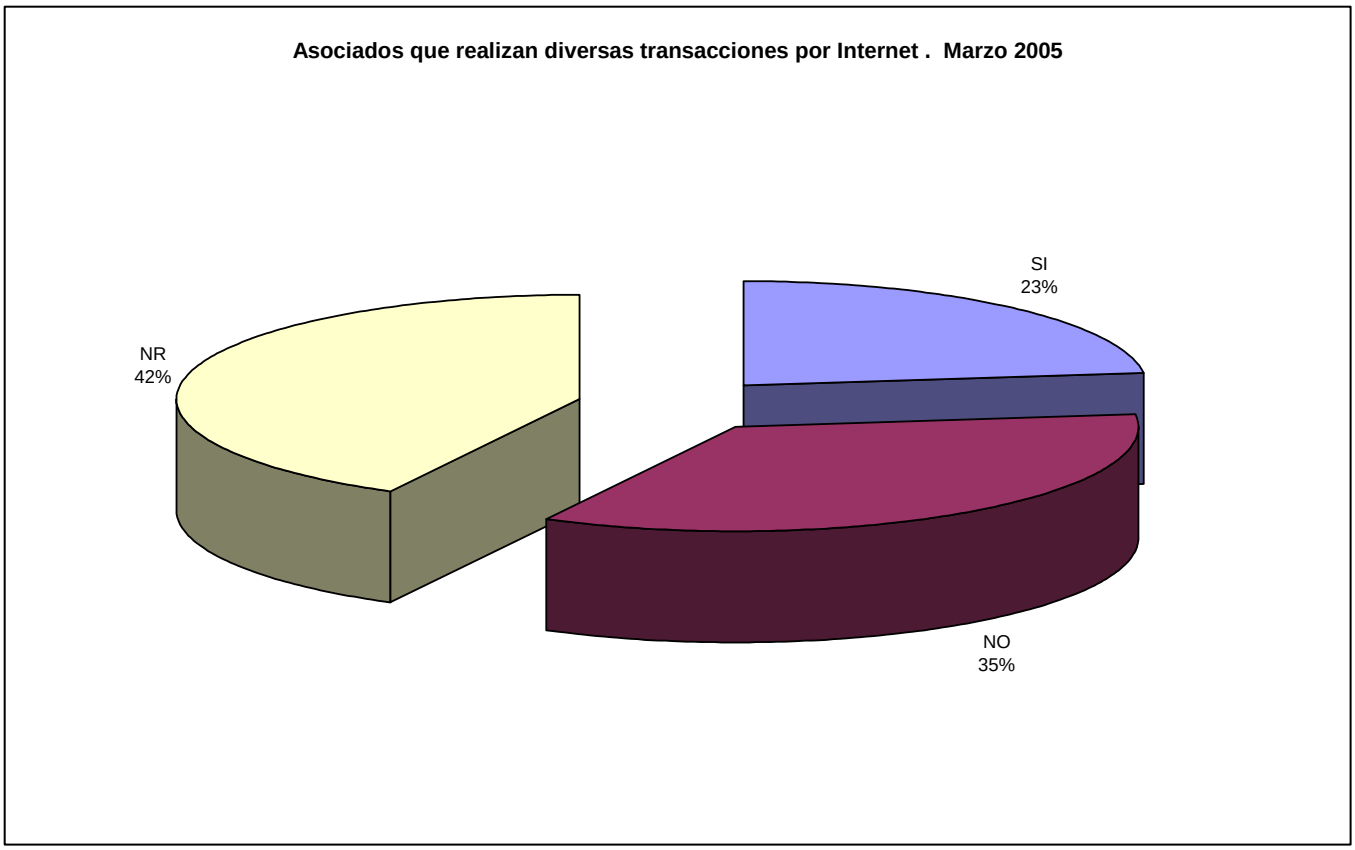
Gráfico No. 3

Lugar de donde acceden a Internet los Asociados de la Asociación Solidarista de Empleados de un Ente Público. Marzo 2005



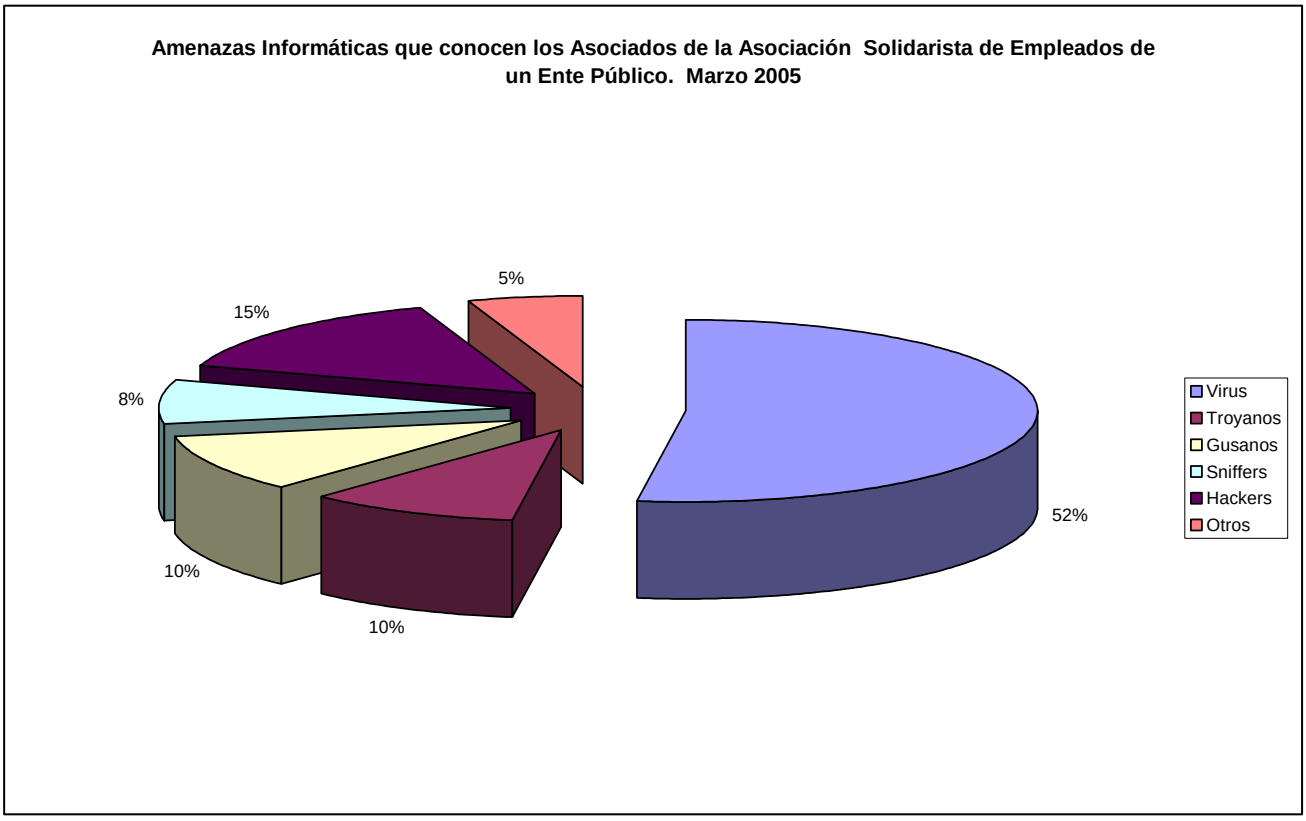
Se les preguntó a los asociados, si actualmente realizan algún tipo de trámite por medio de la Internet, un 42 % decidió no responder, 35 % no realiza ningún trámite, y un 23 % sí utiliza este servicio. Ver gráfico No.4.

Gráfico No .4



Otro aspecto importante que cabe destacar es sobre el conocimiento que se tiene sobre el tipo de amenazas que existen en la red de Internet, los resultados obtenidos demuestran que un 52 % han escuchado o tienen alguna idea con respecto a los virus, 15 % están al corriente de lo que son los Hackers, 10 % sobre los troyanos y gusanos respectivamente, un 8 % sobre sniffers, y un 5 % sobre otros. Ver gráfico No.5.

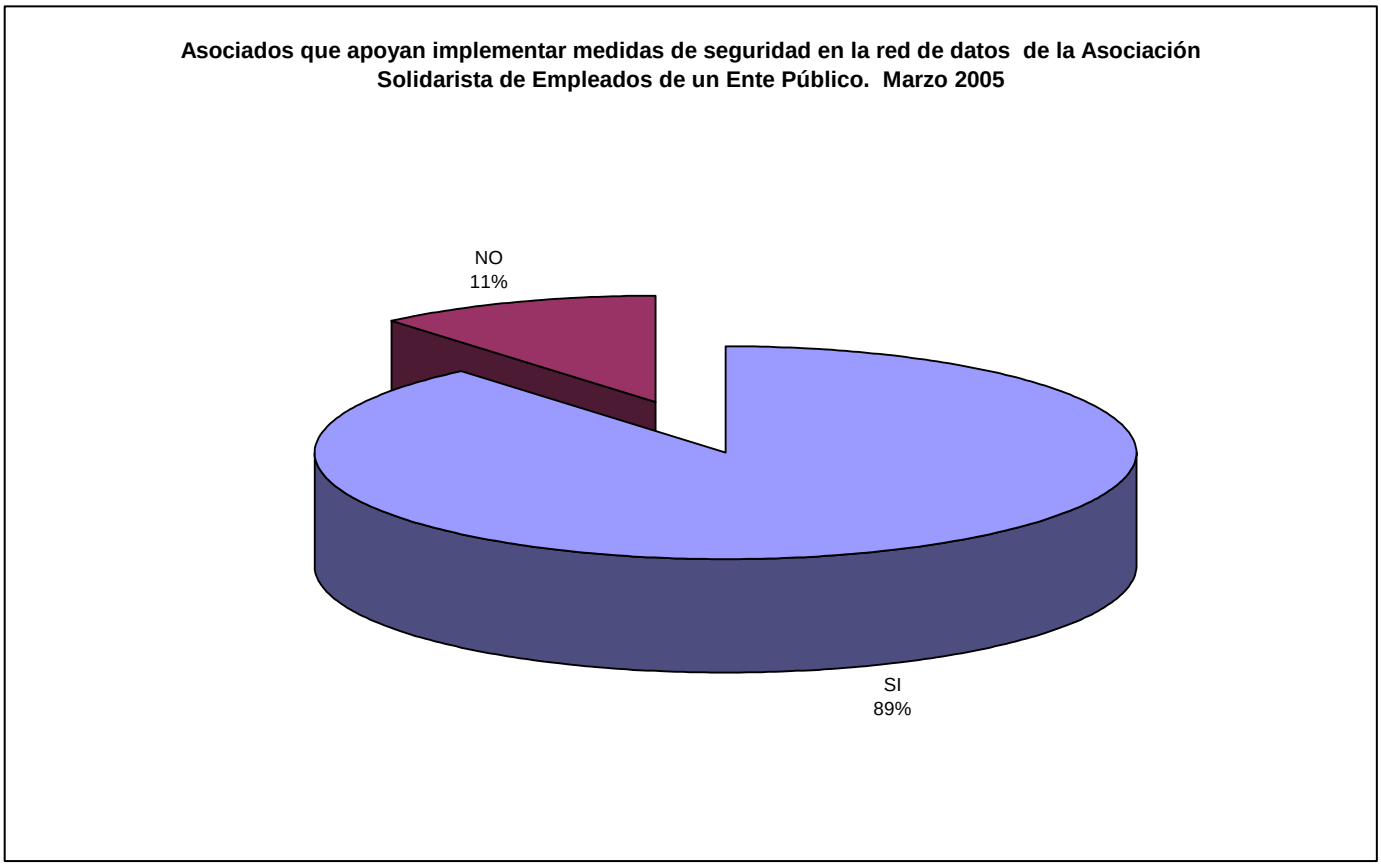
Gráfico No. 5



También, se les preguntó a los asociados, que si conocen los diversos sistemas de seguridad en la parte de informática que está implementando la Asociación; en este ítem un 100% de la muestra, indicaron no tener conocimiento alguno de los sistemas de seguridad, que se han implementado.

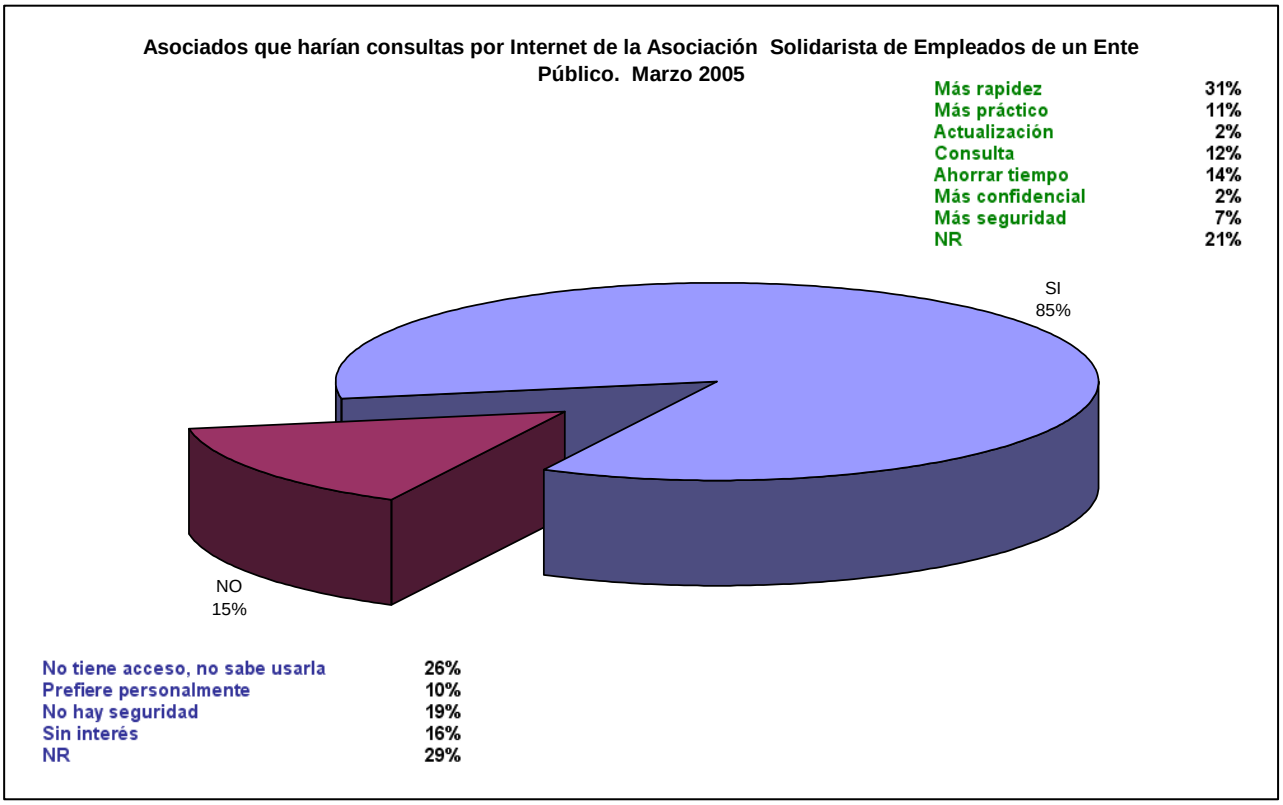
Se les realizó la pregunta que si apoyarían la implementación de diversas medidas de seguridad en el área de los sistemas informáticos de la asociación, y un 89 % se encuentra totalmente de acuerdo; mientras que un 11 % no lo están. Ver gráfico No.6

Gráfico No. 6



Una de las últimas preguntas que se les realizó consistía en averiguar si en un futuro en las páginas de Internet de la Asociación, se pudiera realizar diversos trámites para brindar un servicio más eficiente a los usuarios; a lo que un 85 % contesto que sí, dando razones tales como: que sería más rápido realizar dicho tramite y con esto se ahorrarían tiempo, también que sería más práctico, más confidencial e inclusive más seguro, entre otros; mientras que un 15 % asintieron negativamente, diciendo que no tienen acceso, y que no sabrían como usarla dicho servicio, también mencionaron que prefieren realizar los trámites personalmente, y que no existe mucha seguridad. Ver gráfico No.7

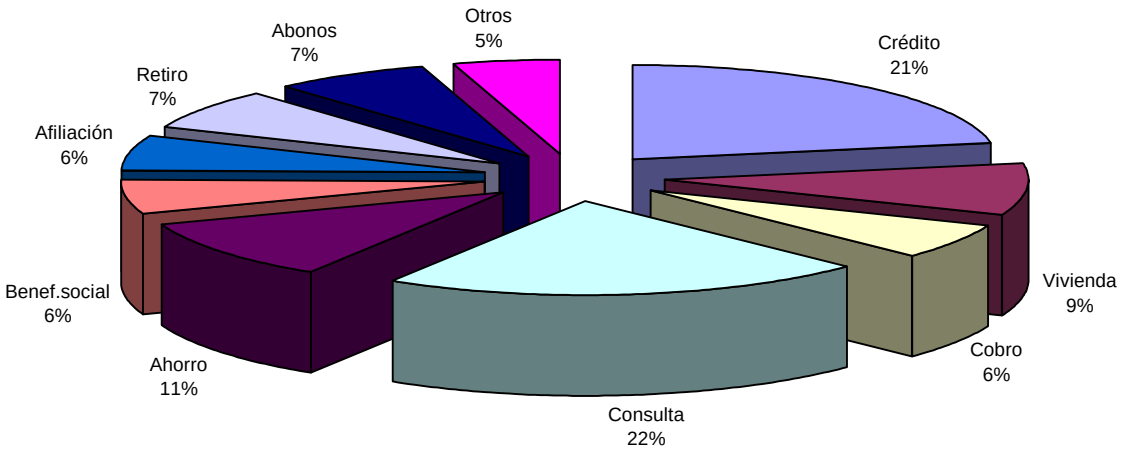
Gráfico No. 7



Por último se les preguntó que sí en un futuro se implementara los servicios de las páginas de Internet, ¿Que servicios de la Asociación le gustaría acceder por medio de esta?, (ver gráfico No.8); un 22% indicaron que para realizar trámites de crédito, un 22% para consulta de estados de cuenta, un 11 % para Ahorro, un 9 % para Vivienda, un 7 % para retiros o renuncia, otro 7 % para abono, un 6 % para cobro, beneficios sociales y afiliación respectivamente, y un 5 % para otros servicios.

Gráfico No. 8

Tipo de consulta que harían en un futuro los Asociados de la Asociación Solidarista de Empleados de un Ente Público. Marzo 2005



En base a los resultados obtenidos en las encuestas realizadas a los encargados de soporte técnico de la Asociación, se obtuvo como resultado lo siguiente:

Los tres encargados de soporte, cuentan con título de Bachiller en Ingeniería en Informática, uno de ellos se encuentra terminando la licenciatura.

Dos de los encargados cuentan con diversos estudios en el campo de las telecomunicaciones, entre estos CCNA (Cisco Certificate Network Academy), y como se mencionó anteriormente uno de ellos está terminando la licenciatura en redes y sistemas telemáticos.

Por parte de la empresa, ninguno de los funcionarios a recibido ningún tipo de capacitación en el área de telecomunicaciones. No obstante dos cuentan con experiencia en utilización de equipos de telecomunicaciones, tales como routers, firewall, switiches, hubs, entre otros.

En la parte de seguridad en redes de la encuesta, dos de los encargados de soporte, indicaron haber recibido una muy breve capacitación en seguridad en redes de datos.

Entre los equipos o dispositivos de seguridad de redes, que conocen los encargados se encuentran los firewalls y los proxys.

Entre los tipos de amenaza que conocen los encargados de soporte que acechan las redes empresariales, ellos mencionaron virus, gusanos, hackers, troyanos, sniffers, crackers, spywares, etc.

Entre los tipos de amenazas que más se han presentado en la red de datos de la Asociación según lo indicaron, se encuentran: los Virus, gusanos y troyanos.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

La Asociación Solidarista, es una empresa que conforme pasa el tiempo ha ido evolucionando, por lo tanto se ha dado a la tarea de reforzar ciertas áreas (en este caso la de informática), para brindar nuevos y mejores servicios.

La tecnología se ha vuelto un factor dominante en el acontecer diario de la Institución, más especialmente por el tipo de comunicación tan avanzada, en el cual la red de Internet es una herramienta que lleva la batuta, con un sin fin de beneficios y ventajas que ofrece tanto a los usuarios como a las empresas.

Internet, no solamente cuenta con cosas buenas o beneficios para las empresas, también tiene sus defectos, como lo son: las ya mencionadas amenazas, mismas que ponen en jaque la seguridad de la empresa, entre las que se pueden mencionar: hackers, virus, gusanos, troyanos, etc.

Según los resultados obtenidos a lo largo de este proyecto de investigación, se puede inferir que la implementación de la DMZ, es un proyecto que traerá sin duda alguna una gran serie de ventajas para la Asociación, la más importante de todas es la seguridad, ya que vendrá a reforzar la ya existente, cerrando los perímetros de la red y con esto delimitar el acceso a la misma, haciendo uso de diversas técnicas tales como: implementación de políticas de seguridad; configuración y puesta en marcha de diversos equipos, con la finalidad de dar acceso solamente a los servicios que a si lo requieran, en este caso en específico será el servidor Web, ya que al cumplir este con la función de hospedar y publicar tanto las páginas de Internet, como el correo electrónico, cualquier usuario externo, sea quién sea accederá solamente a este servidor de toda la empresa, sin poner en peligro algún otro elemento de la red interna, así como a los datos que circulan por esta.

Se recomienda realizar el proceso de implementación, lo más pronto posible, en vista de que se dispone tanto con la disposición así como del

presupuesto para realizar dicho proyecto, y sin dejar de lado la necesidad casi inmediata de iniciar este proceso.

Por otro lado, en este estudio, a parte de realizar todo un análisis con lo que respecta a la DMZ, requerimientos, necesidades, y recomendaciones de la misma; también se realizó un análisis de vulnerabilidad en la seguridad tanto de los datos como de las redes, no solo lógica sino también física.

La zona desmilitarizada o DMZ, igual que ocurre con los componentes de red internos, tiene que estar protegida físicamente contra el acceso del público. De este modo se asegura que nadie, ni siquiera alguno de los empleados, pueda reorganizar el cableado o utilizar inicios de sesión en las cuentas para debilitar la seguridad; tampoco es necesario independizar físicamente la zona desmilitarizada de otros equipos y equipamiento de red; sin embargo, se recomienda aplicar políticas y procedimientos especiales, ya que su función es decisiva en la seguridad de la red.

Se recomienda también, realizar un análisis a profundidad de las vulnerabilidades de la red, a nivel interno, porque según lo que se indicó en el estudio que se realizó, uno de los principales problemas de seguridad es a nivel de puertos, tanto para tráfico entrante, como saliente.

Gracias al análisis realizado a la seguridad de la red, la Asociación cuenta con un reporte a groso modo de los niveles de la seguridad de ésta, así también como de sus posibles amenazas.

Entre los últimos puntos, al estudiar los resultados obtenidos de las encuestas, se puede concluir que los asociados, están dispuestos a hacer uso de los servicios que la Asociación podría poner al alcance, por medio de la Internet, y

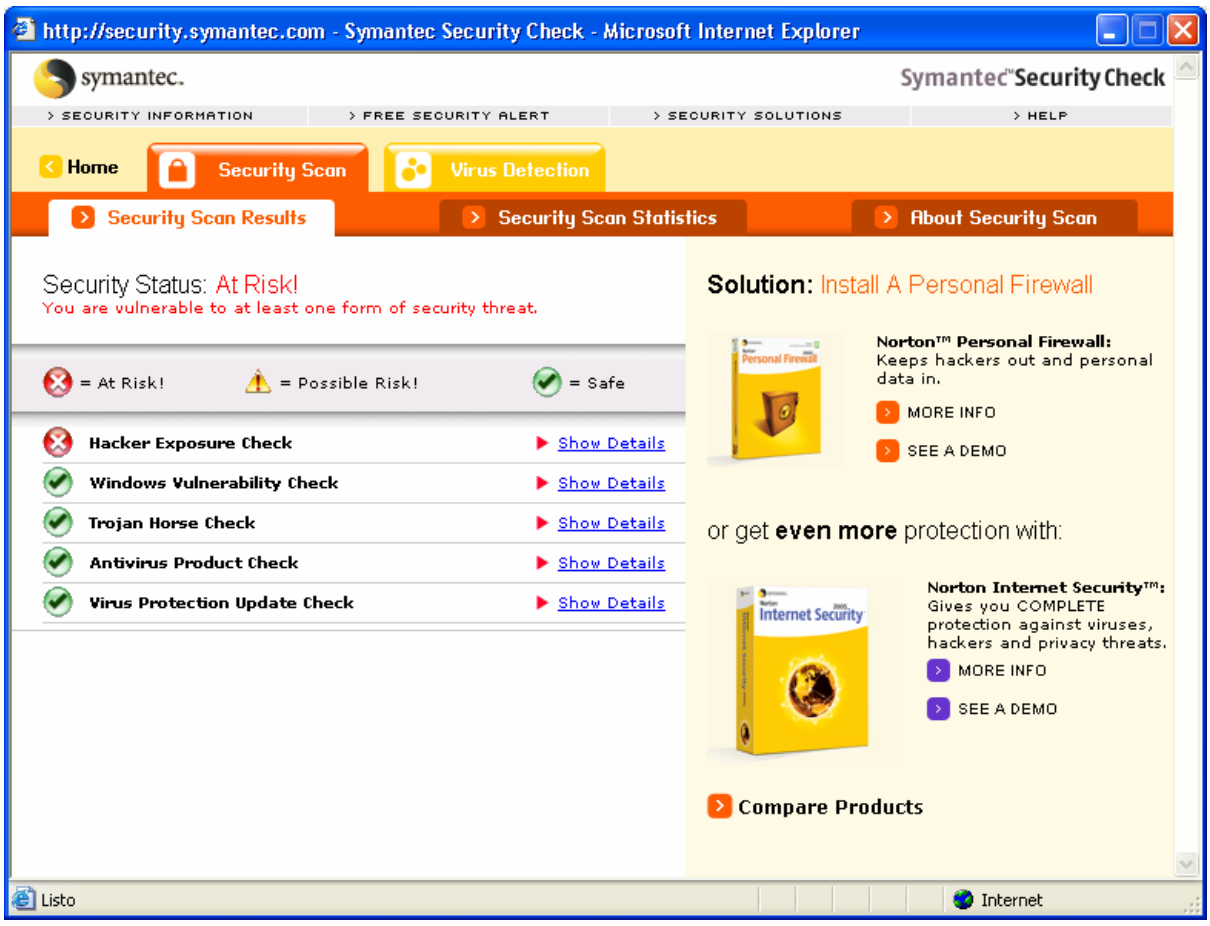
al mismo tiempo la mayoría se encuentra de acuerdo a que se invierta en la seguridad de las redes de datos de la Asociación.

Con respecto al personal de la Asociación, sería conveniente que se capacite a los encargados de soporte en el área de seguridad de redes, aunque bien es cierto tienen un alto conocimiento en redes, resulta primordial, capacitarlos en la parte de seguridad, a parte a esto, estar actualizando los conocimientos, con respecto a las amenazas actuales, así como la forma adecuada de evitarlas, y de cómo eliminarlas.

Se recomienda tomar en cuenta que conforme al número actual de usuarios, se debe visualizar los que se tendrían en un futuro, es decir, en el caso que el número fuera a aumentar, hay que contemplar la posibilidad que el acceso y la consulta hacia las páginas, aumentaría, y en base a esto, sería importante tomar las medidas del caso, tal y como puede ser implementar un mayor ancho de banda en el enlace de Internet, tanto de bajada, como de subida.

ANEXOS

Anexo No. 1. Análisis de Seguridad de una estación de Trabajo bajo Windows XP



The Hacker Exposure Check tests whether ports commonly used by Internet applications are open, closed, or stealth

Understanding your results:

open	An **open** port responds to port probes and acknowledges the port's availability. Open ports are dangerous because they're an easy and attractive means of entry for hackers.
closed	A **closed** port is visible but not open to attack. Although this is a safe state, a hacker can use closed ports to detect the existence of your computer and potentially target it for attack.
stealth	A **stealth** port is safest of all. Stealth means your computer doesn't respond to port probes and you are virtually invisible to hackers scanning the Internet for potential targets. Although this is a very safe result, a stealth port may cause performance problems for some Internet applications.

Your Results:

Port	Description	Status
ICMP Ping	**Ping.** Ping is a network troubleshooting utility. It asks your computer to acknowledge its existence. If your computer responds positively to a ping, hackers are more likely to target your computer.	stealth
21	**FTP (File Transfer Protocol).** FTP is used to transfer files between your computer and other computers. Port 21 should be open only if you're running an FTP server.	stealth
22	**SSH.** TCP connections to this port might indicate a search for SSH, which has a few exploitable features. SSH is a secure replacement for Telnet. The most common uses of SSH are to securely login and copy files from a server.	stealth
23	**Telnet.** Telnet can be used to log into your computer from a terminal anywhere in the world. This port should be open only if you're running a Telnet server.	stealth
25	**SMTP (Simple Mail Transfer Protocol).** A protocol for host-to-host mail transport. This port should be open only if you're running a mail server.	open
79	**Finger.** Finger is an Internet utility that allows someone to obtain information about you, including your full name, logon status, and other profile information.	stealth
80	**HTTP (Hypertext Transfer Protocol).** HTTP is used to transfer Web pages over the Internet. Port 80 should be open only if you're running a Web server.	open
110	**POP3 (Post Office Protocol).** Internet mail servers and mail filter applications use this port. This port should be open only if you're running a mail server.	open

113	**Ident / Authentication.** This service is required by some mail, news, or relay chat servers to allow access. A stealth result on this port could cause performance problems.	
119	**NNTP (Network News Transfer Protocol).** A service used by News servers to distribute Usenet articles to newsreader applications and between other servers.	
135	**Location service (loc-srv).** This port is used to direct RPC (Remote Procedure Calls) services to the appropriate dynamically mapped ports. Hackers can use this to determine which port is used by several Windows services. This port should not be visible from the Internet.	
139	**NetBIOS.** NetBIOS is used for Windows File & Print sharing. If port 139 is open, your computer is open to sharing files over the Internet. Other components of NetBIOS can expose your computer name, workgroup, user name, and other information. To learn more about preventing connections to your NetBIOS ports, see: NetBIOS Information and Configuration Instructions	
143	**IMAP (Internet Message Access Protocol).** IMAP is a sophisticated protocol for electronic mail delivery. This port should be open only if you're running an IMAP server.	
443	**HTTP over TLS/SSL.** A protocol for providing secure HTTP communication. It should be open only if you're running a Web server.	
445	**Windows NT / 2000 SMB.** A standard used to exchange Server Message Blocks, and can be exploited in multiple ways, including gaining your passwords.	
1080	**SOCKS.** This protocol allows computers access to the Internet through a firewall. It is used when one IP address is shared among several computers. Generally this protocol only allows access out to the Internet. However, it is frequently configured incorrectly to allow hackers to pass traffic inwards through the firewall.	
1723	**PPTP (Point-to-Point Tunneling Protocol).** This service is used for virtual private networking connections.	
5000	**UPnP (Universal Plug and Play).** This service is used to communicate with any UPnP devices attached to your network.	
5631	**pcAnywhere.** This port is used by Symantec pcAnywhere when in host mode.	

Anexo No 2.
ENCUESTA

CUANTO SABE EL ASOCIADO DE LA SEGURIDAD QUE EXISTE EN LOS SISTEMAS INFORMATICOS DE LA ASOCIACION

La presente, es una encuesta que tiene como fin medir, el nivel de conocimiento de los asociados así como los posibles beneficios con los que podrían contar al implementar nuevas medidas de seguridad en la red de datos.

Favor marcar con una X, la respuesta que considere apropiada, así como rellenar los espacios en blanco

1- ¿Cuanto tiempo tiene de ser Asociado?

_____

2- ¿Que tipo de tramites realiza con la Asociación?

☐ Crédito ☐ Consulta ☐ Afiliación
☐ Vivienda ☐ Planes de ahorro ☐ Retiro
☐ Cobro ☐ Tramite / Beneficio Social ☐ Abonos
☐ Otros

_____

3- Conoce usted, que es Internet?

☐ SI ☐ NO

4- Cuenta usted con la facilidad de tener acceso a Internet?,

Si la respuesta es NO, pase a la pregunta 8

☐ SI ☐ NO

5- ¿Qué tan a menudo hace usted uso de la Internet?

☐ Nada ☐ Poco ☐ Regular ☐ Diario

6- En que lugar tiene acceso a ella

☐ Casa ☐ Trabajo ☐ Universidad☐ Otros

_____

7- ¿Ha realizado usted alguna transacción por medio de la Internet?

☐ SI ☐ NO

Cual/

_____

8- ¿Cuáles tipos de amenazas informáticas ha escuchado usted que existen en la actualidad?

☐ Virus ☐ Gusanos ☐ Hackers

☐ Troyanos ☐ Sniffers ☐ Otros

_____

9- ¿Conoce los sistemas de seguridad que está implementando la Asociación?

☐ SI ☐ NO

10- Apoyaría usted la implementación de diversas medidas de seguridad en el área de los sistemas informáticos de la asociación?

☐ SI ☐ NO

11- Si en un futuro en las páginas de Internet de la Asociación, usted pudiera consultar sus datos, haría usted uso de dicho servicio?

☐ SI ☐ NO

Porque/

_____

_____

12- En un futuro, Que servicios de la Asociación le gustaría acceder por medio de la Internet?

☐ Crédito	☐ Consulta	☐ Afiliación
☐ Vivienda	☐ Planes de ahorro	☐ Retiro
☐ Cobro	☐ Tramite / Beneficio Social	☐ Abonos
☐ Otros		

_____

_____

Anexo No 3.

ENCUESTA

CONOCIMIENTOS Y DESTREZAS EN REDES Y SEGURIDAD

La presente, es una encuesta que tiene como fin medir, el nivel de conocimiento de los encargados de soporte técnico, tanto en redes como en la seguridad de estas.

Favor marcar con una X, la respuesta que considere apropiada, así como rellenar los espacios en blanco

Conocimiento en redes

1- ¿Cuantos años tiene de laborar para la Asociación en el área de soporte del departamento de Informática?

_____

2- Que tipo de estudio posee en el área de informática?

☐ Técnico ☐ Diplomado ☐ Bachiller ☐ Licenciatura
☐ Otros

_____

3- Posee usted algún tipo de estudio en el campo de las telecomunicaciones?

Si la respuesta es NO, pase a la pregunta 6

☐ SI ☐ NO

4- Que tipo de estudio posee en el área de las telecomunicaciones?

☐ Técnico ☐ Diplomado ☐ Bachiller ☐ Licenciatura
☐ Otros

_____

5- Ha recibido algún tipo de capacitación por parte de la empresa en el área de las telecomunicaciones?

☐ SI ☐ NO

Cual / _____

6- Tiene experiencia en la utilización de equipos de redes?

Si la respuesta es NO, pase a la pregunta 8

☐ SI ☐ NO

7- En que tipo de equipo de redes tiene experiencia?

☐ Routers ☐ Switches
☐ Firewall ☐ Hubs
☐ Otros

_____

Conocimiento en seguridad de redes

8- Ha recibido alguna capacitación en el área de seguridad en las de redes de datos?

☐ SI ☐ NO

Cual /

_____

9- Que tipo de equipos o dispositivos de seguridad conoce usted que existen para las redes de datos ?

_____

_____

10- Que tipos de amenazas conoce usted que acechan las redes empresariales?

☐ Virus ☐ Gusanos ☐ Hackers
☐ Troyanos ☐ Sniffers ☐ Otros

_____

_____

9- Cual es el tipo de amenaza que más se ha presentado en la red de datos de la Asociación?

☐ Virus ☐ Gusanos ☐ Hackers
☐ Troyanos ☐ Sniffers ☐ Otros

_____

_____

GLOSARIO

AID Agencia Internacional de Desarrollo

ARPA Advanced Research Projects Agency (Agencia de Proyectos de Investigación Avanzada). Nombre actual del organismo militar norteamericano.

ARPANET Advanced Research Projects Agency Network. Red pionera de larga distancia financiada por ARPA. Fue la base inicial de la investigación sobre redes y constituyó el eje de estas durante el desarrollo de Internet. ARPANET estaba constituida por ordenadores de conmutación individual de paquetes, interconectados mediante líneas telefónicas.

BACKBONE Es una zona de seguridad que sirve como sistema de interconexión seguro entre todas las demás zonas de seguridad.

C.C.S.S. Caja Costarricense de Seguro Social.

CRNeT Red Nacional de Investigación en Costa Rica.

DMZ Zona expuesta al exterior, donde se albergan los servicios que necesariamente tienen que ser accesibles desde afuera, tales como: servidores web, FTP.

E-MAIL Capacidad para redactar, enviar y recibrir correo electrònico.

FIREWALL (Cortafuegos). Sistema que se coloca entre una red local e internet. La regla básica es asegurar que todas las comunicaciones entre dicha red e internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además estos sistemas suelen incorporar elementos de privacidad, autenticación, etc.

FTP File Transfer Protocol (Protocolo de Transferencia de Archivos). Protocolo que permite a un usuario de un sistema acceder y transferir desde otro sistema de una red.

GATEWAY SECURITY 5420

Es una herramienta hardware-software de seguridad de red para protección perimétrica de entornos heterogéneos de comunicaciones TCP/IP robusta, de gran efectividad, rica en funcionalidades, con balanceo de carga, alta disponibilidad que puede ser clasificada como pasarela de seguridad.

HARDWARE Conjunto de elementos materiales que componen una computadora. Se incluyen los dispositivos electrónicos y electromecánicos, circuitos, cables, tarjetas, armarios, etc.

HOSTING Servicio que es conocido como dar hospedaje a una página de Internet, esto conlleva mantenimiento y mejora.

ICE Instituto Costarricense de Electricidad.

INTERNET Conjunto de redes y ruteadores (routers) que utilizan el protocolo TCP/IP para formar una sola red virtual cooperativa a nivel mundial. Es la mayor red interna del mundo.

NRI Network Readiness Iden (Indice de Preparación de la Red).

OEA Organización de Estado Americanos.

RACSA Radiográfica Costarricense S.A. Proveedora de servicios de comunicación de Costa Rica.

SERVIDORES "Computadoras Poderosas". Con frecuencia están alojados en una central y un administrador de sistemas les da mantenimiento.

SITES Término que se utiliza para referirse a las páginas de Internet.

SSL (Secure Sockets Layer), Capa de Sockets Seguros, una tecnología que proporciona comunicación segura de datos mediante el cifrado y descifrado de los mismos.

TCP/IP Es un protocolo, que proporciona transmisión fiable de paquetes de datos sobre redes. El nombre TCP / IP proviene de dos protocolos importantes de la familia, el Transmission Control Protocol (TCP) y el Internet Protocol (IP). Todos juntos llegan a ser más de 100 protocolos diferentes definidos en este conjunto.

El TCP / IP es la base de Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos.

Tenable NeWT Software especializado que se encarga de medir y analizar las vulnerabilidades existentes en la red.

UIT Unión Internacional de Telecomunicaciones.

UNCTAD Secretaría General de la Conferencia sobre Comercio y Desarrollo de las Naciones Unidas.

WWW Word Wide Web (www o w3), (Telaraña o maya mundial). Sistema de información distribuido, con mecanismos de hipertexto creado por investigadores en Suiza.

SOFTWARE Se conoce como la parte lógica de la computadora, esto es, el conjunto de instrucciones (programas) que puede ejecutar el hardware para la realización de las tareas de computación a las que se destina.

PROTOCOLOS Conjunto de reglas que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red.

PROXY Es un servidor que se utiliza para almacenar la información que es consultada con mayor frecuencia en páginas de Internet, por un período de tiempo, con el fin de aumentar la velocidad de acceso.

SWITCHES Es un dispositivo de red, capaz de buscar y seleccionar el camino correcto para enviar una serie de datos a su próximo destino.

ROUTERS Es una pieza de hardware o software que conecta dos o más redes. Asegura que estas redes puedan mantener una comunicación constante.

RACK Armario en el cual se encuentran ubicados diversos equipos de telecomunicaciones tales como: Routers, Switches.

PUERTOS Son los puntos de enlace para cada conexión de red que se realiza, existen mas de 65.000 para los diferentes servicios y comunicaciones que se realizan (FTP, web, telnet, etc).

REFERENCIAS BIBLIOGRÁFICAS

Garfinkel Simson. Seguridad Práctica en Unix e Internet. Segunda edición, México, McGrawHill, 1999.

Hernández, Fernández y Batista. Metodología de la Investigación, Tercera edición, México, McGrawHill, 2001

Ley de Asociaciones Solidaristas y su Reglamento, pag 9. (Art.1- 4)

Mediavilla Manuel. Seguridad en Unix. Madrid - España , Editorial RA-MA, 1998.

Tanembaum, Andrew .Redes de Computadoras. Cuarta edición, Mexico, Pearson Educación, 2003

White B. Gregory, Fisch A. Eric, Pooch Udo W., Computer System and Network Security , CRC Press, 1996.

Microsoft Corporate. (2004). *Microsoft TechNet Latinoamerica.* Recuperado el 27 de octubre del 2004.
http://www.microsoft.com/latam/technet/implantacion/cap17.asp

IsaServer.Org (2004). *ISA Server DMZ Scenarios*. Recuperado el 20 de octubre del 2004. http://www.isaserver.org/tutorials/ISA_Server_DMZ_Scenarios.html

About, Inc. (2004). *DMZ – Demilitarized Zone in Computer Networking*. Recuperado el 25 de octubre del 2004.

http://compnetworking.about.com/cs/networksecurity/g/bldef_dmz.htm

RACSA. (2004). *Historia de Internet en Costa Rica*. Recuperado el 13 de octubre del 2004.
http://www.racsa.co.cr/conociendo_Internet/historia_Internet_costa_rica.htm

RACSA. (2004). *Disminuye brecha Digital de Costa Rica*. Recuperado el 25 de noviembre del 2004.
http://www.racsa.co.cr/racsa_noticias/disminuye_brecha_digital.htm

E-commerce and Development Report 2003. *Electronic Commerce Branch UNCTAD.* Recuperado el 25 de noviembre del 2004.
http://r0.unctad.org/ecommerce/ecommerce_en/edr03_en.htm

UACA. (2004). *Como establecer una Presencia Internet en Costa Rica.* Recuperado el 25 de noviembre del 2004
http://www.uaca.ac.cr/acta/1998nov/virthtm.htm

Symantec (2004). *América Latina Biblioteca de seguridad para pyme.* Recuperado el 27 de noviembre del 2004.
http://www.symantec.com/region/mx/smallbusiness/articles/

Seguridad en la Red (2004). *Amenazas de Internet.* Recuperado el 27 de noviembre del 2004.
http://www.seguridadenlared.org/amenazas/intrusiones/default.htm

MasterMagazine (2004). *Amenazas de Internet.* Recuperado el 2 de febrero del 2005.
http://www.mastermagazine.info/informes/Internet_amenazas_b.htm

Fisterra (2004).Metodología de la Investigación. Recuperado el 16 de febrero del 2005.http://www.fisterra.com/mbe/investiga/poder_estadistico/poder_estadistico.htm#tabla%203

Wikipedia (2005). *Cortafuegos(Firewall)*. Recuperado el 14 de marzo del 2005. http://es.wikipedia.org/wiki/Firewall

Tenable Network SecurityTM (2004). Recuperado el 25 de marzo del 2005. http://www.nessus.org/