CAPÍTULO I
INTRODUCCIÓN

1.1 Tema

Implementación de normas y políticas de seguridad ante el uso de Internet como herramienta de información en empresas públicas de San José.

1.2 Antecedentes

La ciencia y la tecnología evolucionan a pasos agigantados. El concepto “Internet” hace referencia a una gran red mundial de computadoras conectadas mediante diferentes tipos de enlaces (satélites, radios, o incluso submarinos).

Este recurso que se ha incorporado paulatinamente en empresas públicas y debido a su provecho es fuente de conocimiento consistente, siempre y cuando se mantengan controles que permitan el manejo de la información de modo seguro y se cuente con un alto grado de vulnerabilidad para mantener medidas de protección en la red.

Ya que sabemos que hoy en día la seguridad de los datos es el recurso primordial de las entidades y con base en hechos que han surgido de accesos no autorizados sin saber con qué tipo de pretensiones, obligan a establecer parámetros con el fin de evitar este tipo de casos.

En consecuencia las instituciones buscan implementar mayor seguridad y a su vez mejoras con el fin de evitar trasiego de información no permitida. Es muy importante manejar con discreción los resultados que se obtengan de los aspectos de seguridad, su mala difusión podría causar daños mayores. Esta información no debe ser divulgada y se debe mantener como reservada, para eludir aspectos de irregularidades en cuanto a robo, alteración, fraude y pérdida de información.

1.3 Problema

¿Cuáles son los pasos que se deben realizar para obtener seguridad en el manejo de la información por medio del servicio que ofrece Internet en las instituciones públicas?

1.4 Objetivo General

Objetivo Diagnóstico

Investigar las normas y políticas para mantener la seguridad del servicio de Internet en las instituciones públicas.

Objetivo Solución

Proponer metodologías para implementar normas y políticas para el mejoramiento de la seguridad.

Objetivos Específicos

Diagnóstico

- Analizar el hardware para ver si cumple con las técnicas de seguridad.
- Evaluar el software para ver si cumple con la seguridad necesaria.
- Identificar las leyes actuales de la seguridad en Internet.
- Comentar el entorno actual de Internet como herramienta.
- Describir el nivel actual de conocimiento que debe contar el Recurso Humano para el uso de la Internet.

Solución

- Aplicar los pasos para implementar mecanismos o políticas de seguridad.
- Determinar posibles sistemas de seguridad para contrarrestar el acceso sin autorización en Internet.

1.5 Justificación

Se pretende realizar la investigación de normas y políticas de seguridad ante el uso de Internet como herramienta de información en instituciones públicas para enriquecimiento personal y luego compartirlo. La seguridad en los sistemas de información y de cómputo se ha convertido en uno de los problemas más grandes desde la aparición de Internet. Dada la potencialidad de la herramienta y de sus innumerables aplicaciones, las empresas sienten la necesidad de conectarse a este mundo. Debido a lo anterior, debemos conocer un poco más al respecto de seguridad en los sistemas de información con la idea de establecer los puntos débiles de Internet ante un mal uso y cómo prevenirlos y así obtener una amplia gama de parámetros que permitan controlar la red mediante una metodología específica.

1.6 Alcances y Limitaciones

La investigación pretende dar una visión acerca de los pasos necesarios para la seguridad de los datos, generados por la popularidad o uso de Internet como herramienta de información en empresas públicas ubicadas en San José para evitar principalmente de los ataques externos a redes locales. Esto se hará analizando rubros de seguridad: medidas de control de acceso a intrusos, seguridad en el correo electrónico, planeamiento de una política de seguridad, riesgos y amenazas a la privacidad de las redes e implementación de controles costeables para la seguridad de información. Sin embargo, se debe mencionar que una limitante que surgió en el desarrollo de la tesis fue que entidades contempladas dentro de la muestra inicial no brindaron información; no obstante, otra entidad, también de índole pública, dio la ayuda necesaria.

1.7 Variables

Hardware

- Conceptual

  Todos los componentes físicos de la computadora y sus periféricos.

- Operacional

  Dispositivos físicos que con los requerimientos necesarios, proporcionan un mejor nivel de seguridad y permiten incorporar mayores herramientas de protección de información en nuestra red.

Software

- Conceptual

  Soporte lógico. Término general que designa los diversos tipos de programas usados en computadora.

- Operacional

  Son las aplicaciones internas que se manejan en el computador a través de las cuales se implementan medidas de seguridad para su acceso mediante protocolos de comunicación, principalmente el TCP/IP que proporciona compatibilidad y facilidad para estar a la vanguardia en accesos no autorizados. Sin embargo, se debe de evaluar el software para ver la operatividad y funciones que ofrece.

Ley (es)

- Conceptual

  Conjunto de todas las leyes que rigen la vida social, política y económica de un país o comunidad.

- Operacional

  Es cada una de las normas o preceptos de obligado cumplimiento que una autoridad establece para regular o prohibir una cosa, en relación con la justicia y la ética. Serán de importancia para saber los deberes y obligaciones como usuarios ante el uso de Internet en las instituciones, las cuales indicarán los requerimientos mínimos para contar con seguridad.

Entorno de Internet

- Conceptual

  Conjunto de redes que se conectan a través de un protocolo en común de comunicación.

- Operacional

  Es un conjunto de ordenadores conectados entre sí dentro de Internet que comprende la World Wide Web reconocida como www, que permite que la información de cualquier red interconectada a Internet pueda ser localizada sin importar su ubicación física, como una manera de aprovechar sus servicios para el intercambio de información.

Conocimiento del Recurso Humano

- Conceptual

  Facultad de entender y juzgar las cosas.

- Operacional

  Contar con personal calificado favorece el obtener un mejor grado de productividad y certidumbre en la toma de decisiones debido a la experiencia y aporte en cuanto a la protección de información.

CAPÍTULO II
MARCO TEÓRICO

2.1 Historia y Antecedentes de Internet

Hoy en día, las compañías necesitan de las redes para compartir recursos, como archivos e impresoras. También dan la facilidad de transportar paquetes a mayores velocidades debido al ancho de banda que ofrecen los proveedores de servicios. Así mismo, permiten contar con redundancia en los enlaces de comunicación de datos a fin de que siempre se mantenga la productividad en la empresa, aprovechando el avance de las diversas tecnologías, para mejorar la calidad de los servicios ofrecidos por las empresas así como la satisfacción de los usuarios, utilizando la capacidad y flexibilidad de las redes. De esta manera, es necesario fortalecer e integrar la gestión de red y servicios, debido a que toda compañía necesita mover información entre sus sucursales, además a otras empresas y países con el fin de ceder y mantener datos actualizados. Por lo tanto, se necesita usar la plataforma que ofrece Internet la cual consiste en un conjunto de ordenadores que se conectan a través de un protocolo común de comunicación que es el TCP/IP (Protocolo de Control de Transmisiones/ Protocolo de Internet) mediante el cual se asignan direcciones IP. En consecuencia, la dirección IP es la dirección de un ordenador conectado a Internet y gracias a ella otro ordenador sabe a dónde tiene que enviar la información.

Sin duda alguna, la sociedad en general se ha visto influenciada de una u otra forma por el uso de Internet. A través de ella es posible encontrar toda clase de software para una gran variedad de computadoras y sistemas operativos, además, pueden consultarse los catálogos de las bibliotecas más importantes del mundo, acceder a bases de datos con los temas más diversos y transferir copias de los documentos encontrados; es posible visualizar y copiar archivos de imágenes con fotografías de todo tipo o reproducciones; pueden hacerse cosas como conversar dos o más personas en tiempo real. Otra de las ventajas de utilizar la red de redes para estos fines son los siguientes: la rapidez con que se puede encontrar la información; la gran cantidad de datos que se pueden

conseguir acerca de un mismo tema de interés; el bajo costo que significa el no tener que comprar determinado libro, también la Internet ha hecho que la distancia haya dejado de ser un elemento importante en diferentes actividades por ejemplo, en lugar de tener que esperar por un curso programado durante tres meses y en otra ciudad, el mismo conocimiento se puede obtener el día de hoy y sin la necesidad de viajar, de tal manera Internet se ha convertido en la última década en un fenómeno que ha revolucionado la sociedad. Dentro de las comunicaciones no se ha observado otro fenómeno social de tal envergadura que evolucione tan rápido. Existen tres factores por los cuales este nuevo fenómeno ha evolucionado en forma masiva en la sociedad actual:

1. La expansión de los ordenadores en todos los ámbitos de la sociedad (empresas, universidades, gobiernos) ha contribuido a informatizar casi cualquier aspecto de nuestra vida.
2. La rápida evolución de la tecnología de comunicaciones (debido a enlaces más rápidos, baratos y con mejor rendimiento) que han acelerado aún más el auge de Internet.
3. El carácter universal de Internet que permite la conectividad global y permanente con todos los países de forma económica y prácticamente instantánea, la convierten en una herramienta imprescindible para cualquier tipo de comunicación.

2.2 Auge o Toma de Fuerza de Internet

Hoy en día, este tipo de comunicación necesita seguridad a la hora de mover información, ya que cientos de millones de entidades en todo el mundo utilizan Internet como parte de su trabajo y entretenimiento. De acuerdo con los estándares de seguridad desarrollados en el libro naranja del Departamento de Defensa de los Estados Unidos, se dice que se utilizan varios niveles de seguridad. Para el caso de estudio, se analizará el nivel B de seguridad que tiene tres sub niveles:

B1 o protección de seguridad etiquetada: se considera como primer nivel que soporta seguridad de multinivel. Parte del principio de que un objeto bajo control de acceso obligatorio no puede aceptar cambios en los permisos establecidos por el dueño del archivo.

B2 conocido como protección estructurada, requiere que todos los objetos estén etiquetados, los dispositivos como discos, cintas y terminales pueden tener asignado uno o varios niveles de seguridad. Este es el primer nivel en el que se aborda el problema de la comunicación de un objeto con otro que se encuentra en un nivel de seguridad inferior.

B3 o nivel de dominios de seguridad, en donde se refuerzan los dominios con la instalación del hardware. Requiere que la terminal del usuario se conecte al sistema por medio de una ruta de acceso segura. Posteriormente, el nivel A se utiliza como parte del complemento para evitar violaciones a los sistemas de seguridad. Se considera el nivel más elevado de seguridad, ya que componentes de niveles inferiores se incluyen. Se cree que es de distribución confiable, es decir, que el hardware y el software han sido protegidos ya que los activos de información y los equipos informáticos son recursos importantes y vitales de nuestra compañía por lo que se deben preservar, utilizar y mejorarlos. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad, intrusos, interrupción de servicio, accidentes y desastres naturales ya que se sabe que hay gente mal intencionada que quiere hacer uso indebido de la información, como lo son los hackers. Eric Raymond, en su libro “Diccionario del hacker” define este término como un programador hábil; sin embargo, Raymond no sólo se queda en la conceptualización, también señala cinco características posibles que lo definen:

a) Una persona que disfruta al aprender los detalles de un lenguaje o sistema de programación.

b) Una persona que disfruta al hacer la programación real en vez de sólo Teorizar en ella.
c) Una persona capaz de apreciar el hackeo de otro
d) Una persona que aprende rápidamente a programar
e) Una persona que es experta en un lenguaje o sistema de programación específico, como por ejemplo "un hacker de UNIX".

Sin embargo, las más importantes aclaratorias que hace Raymond en relación con el término es desligarlo de cualquier acto delictivo. También se hace referencia al término **cracker** como un grupo de expertos informáticos atraídos por el “lado oscuro de la fuerza”. Estos tratan de entrar en los sistemas de otras personas usando sus conocimientos de programación. Los conceptos mencionados anteriormente se relacionan con **personas externas** que tratan de ingresar a la red. En un **entorno interno** los **vándalos** quienes entran a las redes y se encargan de alterar, modificar, borrar información de grado potencial para la empresa; posteriormente se encuentran los **espías** son personas que con disimulo y secreto observan o escuchan lo que pasa, para comunicarlo al que tiene interés en saberlo, la mayor parte de las veces son empleados despedidos, descontentos o simplemente sabotajes, puesto que conocen perfectamente el funcionamiento del sistema. Adicionalmente existen “sniffing” (Intrusos) que son herramientas mediante software utilizadas para capturar información que pasa en la red. Los sniffers representan un alto nivel de riesgo, ya que: pueden capturar contraseñas, atrapar información confidencial o patentada u obtener acceso por la fuerza. Ante estás circunstancias es necesario implementar herramientas y técnicas de seguridad para el trato de la información que permitan detectar intrusos en la red.

2.3 ¿Cómo se pretende resolver?

Algunos aspectos que podrían ayudar a resolver el problema son la seguridad por hardware mediante dispositivos como el Firewall (muros de fuego) Estos sistemas o grupos de sistemas que imponen una política entre una red privada e Internet, determinando qué servicios de red pueden ser accesados por usuarios externos e internos. También es un filtro que controla todas las comunicaciones que pasan de una red a otra y en función de lo que sean, permiten o deniegan el paso. Para permitir o denegar una comunicación, el Firewall examina el tipo de servicio al que corresponde, como puede ser el web (Internet) correo. Según, el Firewall decide si lo permite o no, además examina si la comunicación es entrante o saliente y dependiendo de su dirección puede dejarla pasar o no. Otro dispositivo es Pix Firewall, que es una línea de productos líder en el mercado. Ofrece poderosos recursos de seguridad y de redes privadas virtuales para empresas de todos los tamaños y presupuestos", dijo Richard Palmer, vicepresidente y gerente general de una unidad de negocios VPN (red privada virtual) y servicios de seguridad de Cisco. Otra técnica de seguridad sería la Seguridad por Software, aquí entran en funcionamiento los sistemas de IDS (sistemas de detección de intrusos) que tienen como fin examinar y supervisar los recursos tanto a ordenadores como a redes de computadoras. En el caso de los ordenadores se realiza a nivel del sistema operativo para controlar los accesos de los usuarios, modificación de ficheros del sistema, uso de recursos, memoria y disco, con el objetivo de detectar cualquier comportamiento anómalo que pueda ser indicativo de un abuso del sistema. Para el caso de redes de ordenadores se puede monitorear el uso de ancho de banda, acceso a direcciones no permitidas, uso de direcciones falsas, con el propósito de encontrar comportamientos indebidos en la red. Otra de las técnicas de seguridad que complementan a los sistemas de detección de intrusos son los "honeypots" y "honeynets" (redes de miel o tarros de miel).Estos se consideran como un recurso de red destinado a ser atacado o comprometido en cualquier momento por un atacante. Los "honeypots" no tienen en ningún caso la

finalidad de resolver o arreglar fallas de seguridad en la red, son los encargados de proporcionar información valiosa sobre los posibles atacantes en potencia a las redes antes de que comprometan los sistemas reales, de está forma son vitales para conseguir un sistema de seguridad fiable y eficaz. Por lo tanto, mantener distintas vulnerabilidades en forma controlada ayuda a que se ofrezca información confusa y engañosa para el atacante, cosa que dificultará su trabajo. Así mismo, la detección de una vulnerabilidad en la red no tiene que implicar su caída; al contrario, permite descubrir a un intruso y tomar las medidas oportunas antes de que entre realmente en nuestra red. También se utiliza la Protección de virus. Los virus son programas que tratan de espaciarse de una computadora a otra, usualmente a través de correo electrónico, a un programa huésped. Puede dañar el hardware, software o datos. En comparación con el término gusano el cual es un programa que se mantiene y duplica solo, usualmente consume memoria, causando por lo tanto que el equipo deje de responder. Por lo tanto, es importante escoger la mejor herramienta actual de seguridad contra virus. Luego está la Protección del correo electrónico. Con el sistema electrónico de correo es relevante aclarar al usuario de la empresa qué se puede hacer y qué no. Se debe además notificarle sobre los actos que van en contra del funcionamiento óptimo del correo y mencionar las responsabilidades en distintos grados, de la seguridad. La Gerencia de Informática es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la organización, todo esto en coordinación con la Junta Directiva y la Gerencia de Telecomunicaciones. El Jefe de Seguridad es responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad, así como recomendar las medidas pertinentes. El Administrador de Sistemas es responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administra, como por ejemplo, aplicar inmediatamente los parches correctivos cuando le

llegue la notificación del fabricante del producto o de un ente como el CERT (Computer Emergency Response Team). Los usuarios son responsables de cumplir con todas las políticas de la compañía relativas a la seguridad informática y en particular conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos. No divulgar información confidencial de la compañía a personas no autorizadas, ni permitir o facilitar el uso de los sistemas informáticos a personas no autorizadas. No deben utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo. Deben proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida; seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas; reportar inmediatamente a su jefe inmediato o a un funcionario de Seguridad Informática cualquier evento que pueda comprometer la seguridad de la compañía y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales. En las Políticas de seguridad para redes el propósito es establecer las directrices, los procedimientos y los requisitos para asegurar la protección apropiada de la compañía al estar conectada a redes de computadoras, mencionando aspectos que se deben de tomar en cuenta a la hora elaborar una política. Un ejemplo de posible planteamiento para el desarrollo de una política podría ser el siguiente:

¿Qué recursos se quieren proteger?

¿De cuáles personas se necesitan proteger los recursos?

¿Qué tan importante es el recurso?

¿Qué tan reales son las amenazas?

¿Qué medidas se pueden implantar para proteger sus bienes, de una manera económica y oportuna?

Examine con frecuencia su política de red para verificar si han cambiado los objetivos y circunstancias en la red.

Al crear una política de seguridad se debe conocer cuáles recursos de la red vale la pena proteger y así entender que algunos son más importantes que otros.
El análisis de riesgos implica determinar lo siguiente:
¿Qué necesita proteger?
¿De quién debe protegerlo?
¿Cómo debe protegerlo?

Algunos ejemplos de recursos son los siguientes:
Estaciones de trabajo.
Dispositivos de interconexión, compuertas, enrutadores, puentes, repetidores.
Software para red y aplicaciones.
Información de archivos y bases de datos.

Finalmente, la Seguridad Física se refiere a todos aquellos elementos de control tangibles que de una u otra forma limitan el acceso a un recurso o la ejecución de una tarea. Se puede citar como ejemplo: una puerta, un vigilante, un detector de humo.
Todos los aspectos mencionados anteriormente se pueden incorporar e ir implementando para evitar problemas de seguridad de información en la empresa, debido a que la administración de seguridad debe considerar rubros físicos, lógicos y procedimientos, normas y políticas institucionales. Las organizaciones deben tener políticas de seguridad que permitan incluir controles o medidas para minimizar los riesgos asociados al acceso y manejo de información, además tomar en cuenta que las medidas y políticas la aseguren ante accidentes, vandalismos y robos.

Por lo tanto, se deben considerar aspectos como la confidencialidad e integridad que se ven reflejadas en el beneficio de contar con una plataforma confiable de seguridad, con lo que se obtiene aumento de productividad y a su vez un incremento en la motivación del personal. De esta manera, se logran mejores relaciones humanas que ayudan a desarrollar equipos de trabajo competentes y proporcionan un ambiente laboral agradable para el recurso humano de la empresa. Además se debe ser conciente del grado de importancia que tiene contar con personal capacitado debido a la experiencia acumulada y aporte que son de peso en la toma de decisiones para dar estabilidad y seguir evolucionando en pro de la seguridad de la empresa.

CAPÍTULO II
MARCO METODOLÓGICO

3.1 Tipos de Investigación

Metodología por emplear

Explicativa y Descriptiva

Explicativa

Hernández, Fernández y Baptista (2004) establecen que “los estudios explicativos pretenden establecer las causas de los eventos, sucesos o fenómenos que se estudian.” (página 113)

La metodología explicativa pretende dar un enfoque de ubicación, saber si el tema de investigación ha sido tratado con anterioridad, para obtener conclusiones y buscar mejoras, con el objetivo de implementarlas.

Descriptiva

“Hernández, Fernández y Baptista (2004) afirman que este tipo de investigación “Busca especificar propiedades, características y rasgos importantes de cualquier fenómeno que se analice.”

Es decir busca la descripción y características de la seguridad de la información para determinar las causas su vulnerabilidad, desarrollarlas y minimizar el riesgo de seguridad de información cuando se ingresa a la Internet, en el contexto de entidades públicas de San José.

3.2 Sujetos de Investigación

Jefe del Departamento de Informática

Encargado de planificar, organizar y coordinar las actividades. Dirige la selección, instalación, utilización y mantenimiento de las computadoras y programas, es responsable de dirigir los proyectos que desarrolla su departamento, administra los recursos humanos del sector (evaluaciones anuales, capacitaciones, entre otras), además administración de recursos financieros y materiales, negocia con otros departamentos las prioridades en cuanto al desarrollo de sistemas.

Jefe del Departamento de Soporte-Técnico

Dirige y coordina las actividades relacionadas con el soporte a los usuarios, brinda ayuda técnica en sistemas a usuarios finales de la organización, realiza labores asistenciales en el Departamento de Sistemas, lleva un registro de anotaciones sobre las solicitudes de requerimientos nuevos o modificaciones que los usuarios soliciten.

Encargado de Administración de la Red

Administra a los usuarios, políticas, perfiles, grupos y derechos, administra la Internet, ancho de banda, mantenimientos de accesos, actualizaciones y rendimiento de la red, aadministra los servicios de correo, revisa periódicamente los servidores, migraciones, lleva la agenda de soporte diario(mantenimiento preventivo, service packs, parches, respaldos), custodia las licencias de los sistemas operativos, se encarga de la optimización de la Red Física (planes de contingencia, diagnósticos y reestructuración.)

3.3 Población y Muestra

Muestreo No probabilístico (conveniencia)

Para efectos de está investigación se utilizará como **unidad de estudio** las siguientes instituciones públicas: ICE, MUNICIPIO, INS, CCSS, AyA, Fuerza y Luz, Registro Nacional, Contraloría General, Magisterio Nacional, UNED, ubicadas en San José, que cuenten con algún tipo de topología de red, y herramientas de seguridad implementadas o en desarrollo, también que tengan acceso a Internet. Se utilizará el tipo de **muestreo no probabilístico** por razones de tiempo, costo y conveniencia para extraer información sobre seguridad en la red. Debido a esto se aplicaran los diferentes instrumentos de investigación (entrevista, cuestionario) a perfiles específicos de las áreas de coordinación, red y soporte técnico para extraer información sobre seguridad en los datos. Además, se selecciono como población la parte técnica de la empresa, en el área de Informática, quienes serán los beneficiados con el producto final del trabajo. De los entes mencionados anteriormente se cuenta con el aporte de: 10 Jefes del Departamento de Informática, 10 encargados de soporte técnico y 10 responsables de administrar la red. Estos llevarán a una investigación causal que busca explicar las relaciones entre las diferentes variables, identificando las fortalezas y debilidades para mejorar el grado de vulnerabilidad de la red empresarial.

3.4 Fuentes de Información

Primarias

Cruz, Paz, Andrés. (1994) dice que “es aquella que genera, contiene, transfiere o suministra información original; resultante de un proceso intelectivo de investigación, creación o desarrollo.”
www.uh.cu/facultades/fcom/portal/interes_glosa_fuentes.htm

Es la información suministrada de primera mano, debido a que se cuenta con sujetos de investigación que brindan la información requerida y con originalidad y veracidad con respecto al tema de la seguridad de información. Están conformadas por la información que proporciona los **encargados del departamento de cómputo** quienes debido a su conocimiento y experiencia ayudan a visualizar el entorno actual de la institución para así compartir sus ideas con respecto al tema: normas y políticas de la Internet como herramienta de información. Los encargados de **soporte técnico** facilitan información en cuanto al hardware, para ver si es necesario hacer cambios en los equipos, los cuales son de gran importancia para la implementación y actualización de herramientas que permitan estar al día a la hora de entrar en la Internet. También los **administradores de red** mencionan aspectos que se deben de tener en consideración para control, mantenimiento, tráfico y funcionamiento de la red, valiosos en la operación de la red y acceso a la Internet.

Secundarias

Sampieri R.H y Collado C.F. (2003) establecen que “ayudan a detectar las referencias necesarias, permiten localizar las fuentes primarias y habitualmente es la estrategia más frecuentemente utilizada. Son compilaciones, resúmenes y listados de referencias publicadas en un área del conocimiento en particular.” http://med.unne.edu.ar/revista/revista126/como_esc_articulo.htm

Dentro de las fuentes secundarias de información que se utilizarán están los diferentes documentos y resúmenes que se encuentran en Internet, que serán de mucho provecho para el desarrollo de esta metodología.

3.5 Descripción de los instrumentos de investigación

Entrevista

Es una técnica importante para recolectar hechos y opiniones que orientan sobre los requerimientos del proyecto. Los principales objetivos de la entrevista son:

1. Reunir percepciones de hechos relevantes de los individuos involucrados en el proyecto.
2. Aumentar la comprensión y compromiso de las personas que participan en el proyecto.
3. Proporcionar una base común para el análisis posterior.

Se eligió aplicar **entrevistas** a los encargados de proyectos relacionados con el tema de seguridad de información en los entes públicos, debido a que estas personas tienen influencia en la gestión y toma de decisiones de la empresa.

Para recolectar la información se elaboraron preguntas abiertas y cerradas

Las preguntas abiertas se realizaron para que el entrevistado aporte su conocimiento, mediante opiniones, consideraciones y criterios relacionados con el tema de investigación. Además, para tomar en consideración aspectos que fueron omitidos así obtener un mejor análisis de los datos.

En el caso de las preguntas cerradas, su elaboración permite tener un control sobre los datos obtenidos, mediante el desarrollo de preguntas concisas para evitar obtener sesgo en los datos de investigación.

Cuestionario

Consiste en un conjunto de preguntas de varios tipos, de forma sistemática y cuidadosa, sobre hechos y aspectos que interesan en una investigación. Será aplicado al personal encargado de Redes y Soporte Técnico de los entes públicos. También es un instrumento muy útil para la unificación de los datos, lo que ayudara a contar con datos tangibles y representativos basados en el tema de investigación, a través de la elaboración de preguntas cerradas, cerradas de selecciones múltiples y abiertas.

Las preguntas cerradas y cerradas de selección múltiple permiten mayor facilidad en la comprensión de los datos y comparaciones, por lo tanto no se salen del tema de estudio y con ello se obtienen datos relevantes en cuanto a la investigación. Por ello, es más factible este tipo de preguntas debido a que las personas tienden a brindar a contribuir para obtener resultados importantes para el análisis de los datos.

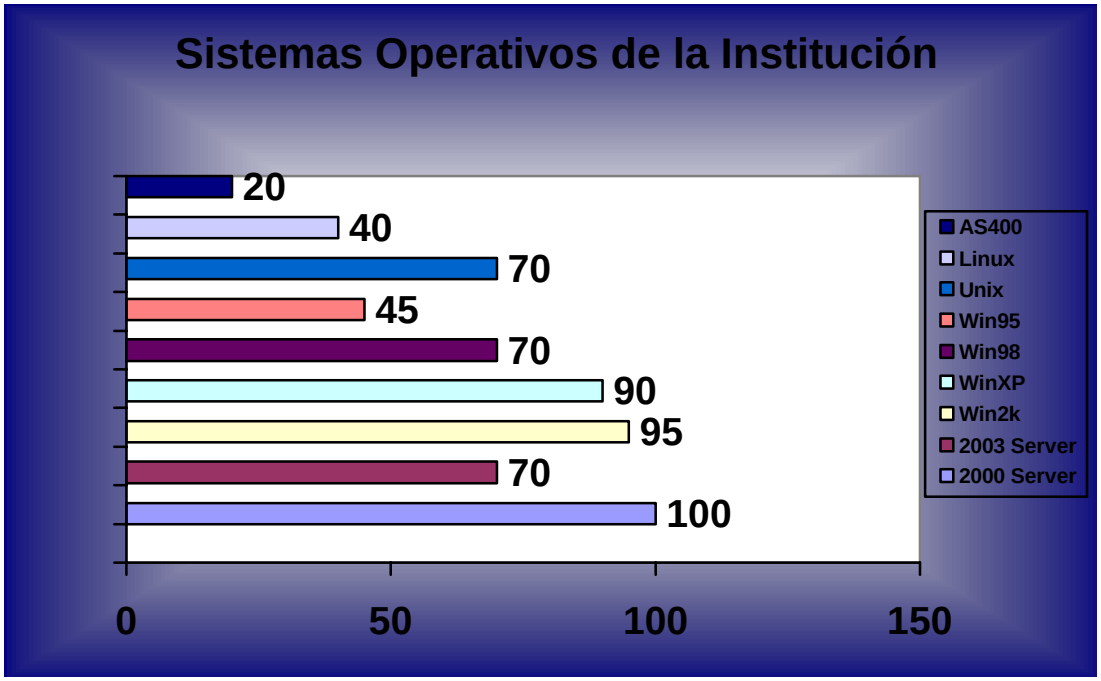
Las preguntas abiertas permiten incrementar detalles importantes de la investigación que posteriormente ayudarán a un mayor análisis en la investigación. Pero se aplicaron en menor proporción debido a que las personas no tienden a mencionar detalles de las entidades o por seguridad de la empresa. Sin embargo, siempre aportan un valor agregado.

CAPÍTULO IV
ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

4.1 Análisis de los datos

Se utilizarán dos cuestionarios, uno dirigido al Encargado de Red y el otro al Encargado de Soporte Técnico; de 10 instituciones públicas, para un total de 20 cuestionarios. De ellos se extrae la siguiente información.

Gráfico #1



Fuente: cuestionario aplicado.

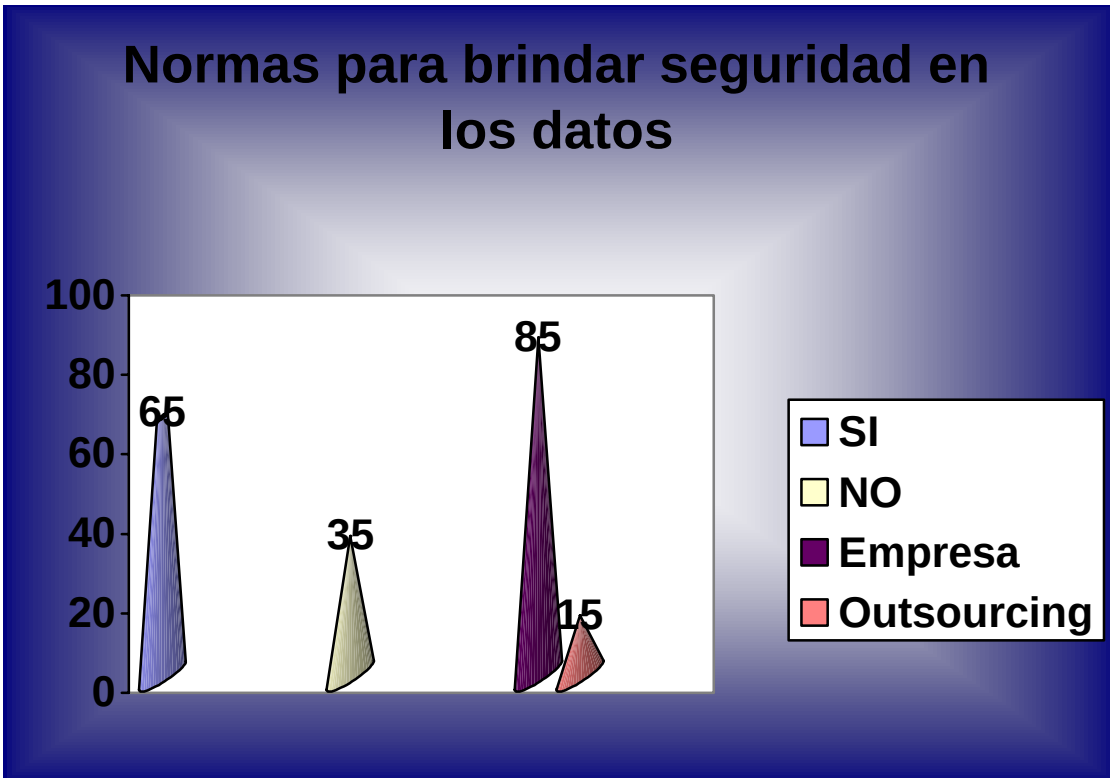
Como se puede observar en el cuadro anterior, el diagnóstico sobre los Sistemas Operativos que se han implementado en las instituciones públicas se refleja sobre la plataforma de Microsoft. Partiendo de este hecho se buscarán herramientas para ofrecer seguridad en los datos sobre esta plataforma.

Gráfico #2

Fuente: cuestionario aplicado.

Se denota que la compra de equipo de comunicaciones se realiza por compra directa. Sin embargo, otra opción importante se da por medio de Leasing; de tal que manera el hardware es un aspecto idóneo para el desarrollo de las empresas.

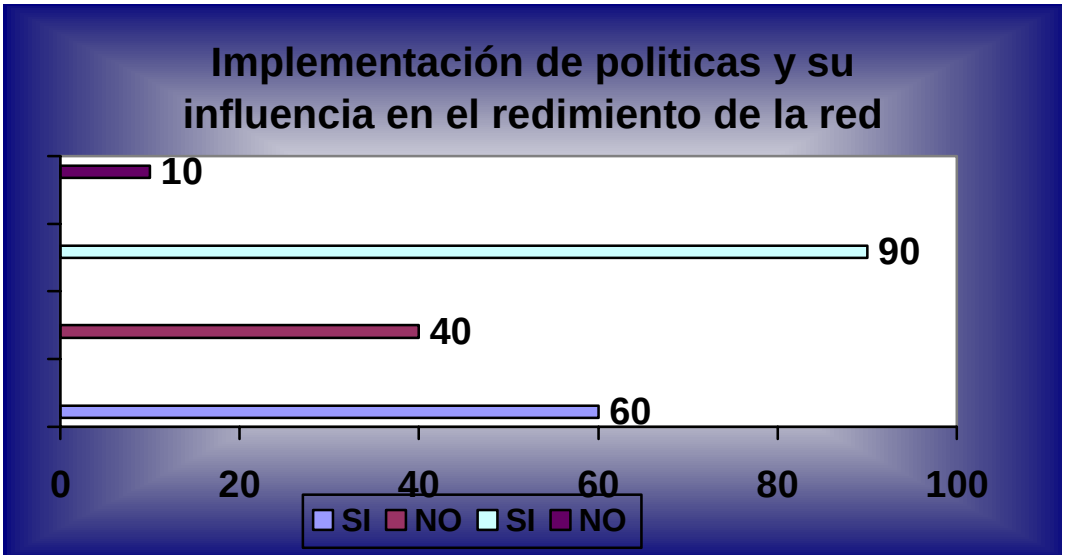
Gráfico #3



Fuente: cuestionario aplicado.

En el cuadro anterior se demuestra que la mayoría de los entes públicos utilizan normas para la administración de seguridad en los datos y se deben considerar aspectos de seguridad física, lógica (Claves), además políticas preferiblemente desarrolladas por personal de la empresa.

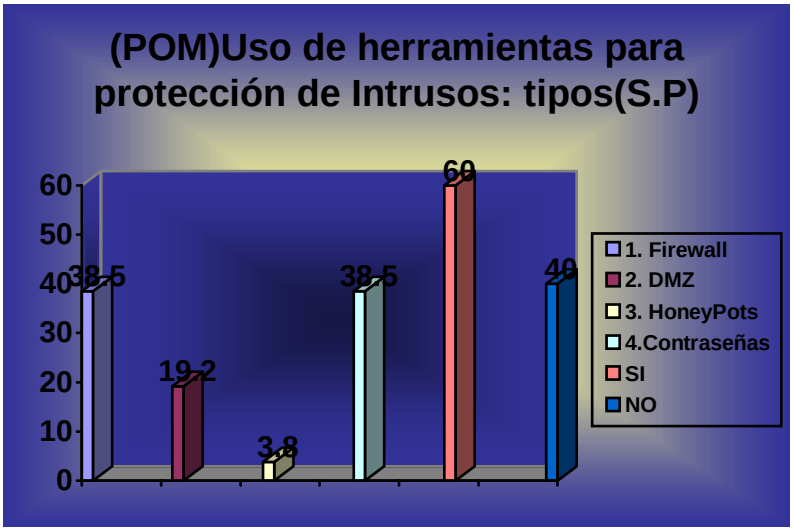
Gráfico #4



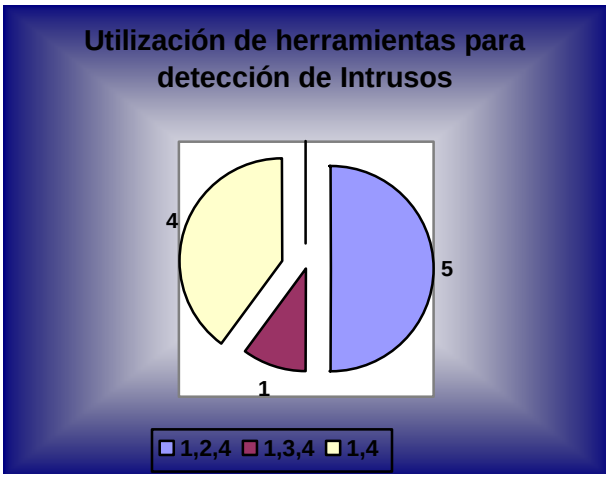
Fuente: cuestionario aplicado.

Como se refleja en el grafico anterior, la implementación de **políticas en la red** sí ha influido en su rendimiento; por lo cual ha sido necesario ampliar el **ancho de banda** en la red para lograr estabilidad.

Gráfico #5



SI	1,2,4	5
	1,3,4	1
NO	1,4	4

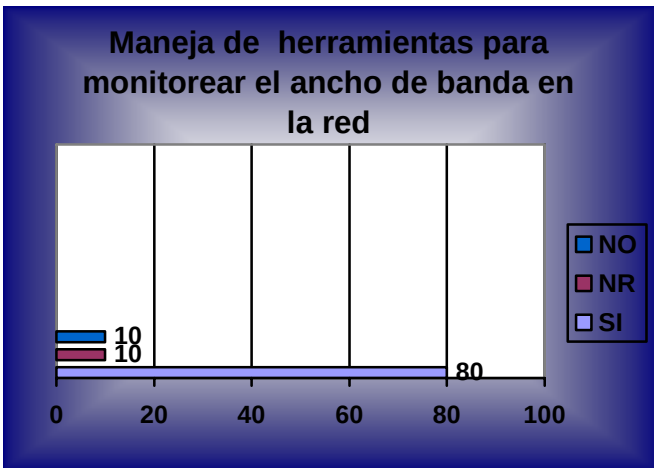


Fuente: cuestionario aplicado.

En este cuadro se determina la relación de los criterios institucionales por parte de los Encargados de Redes y Soporte Técnico con respecto a si cuentan con herramientas para detección de intrusos para determinar las herramientas de detección intrusos. Se desglosa de la siguiente manera: interpretación del cuadro anterior.

.

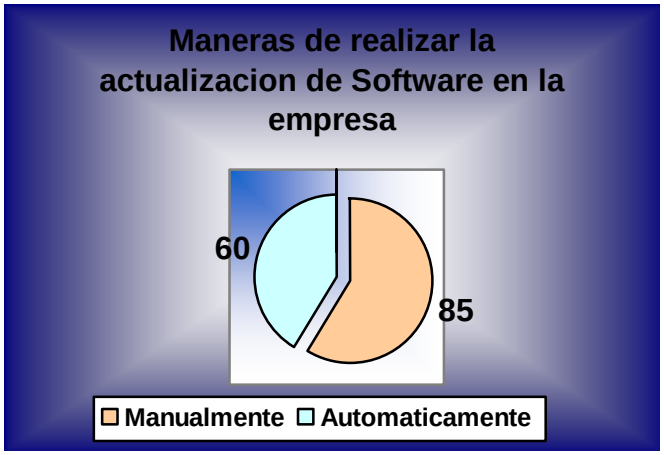
Gráfico #6



Fuente: cuestionario aplicado.

La mayoría de las instituciones públicas sí utilizan alguna herramienta para monitorear el ancho de banda. Dentro de estas se mencionan: IPSWITCH, GFILANGUARD, SolarWinds Network Performance Monitor.

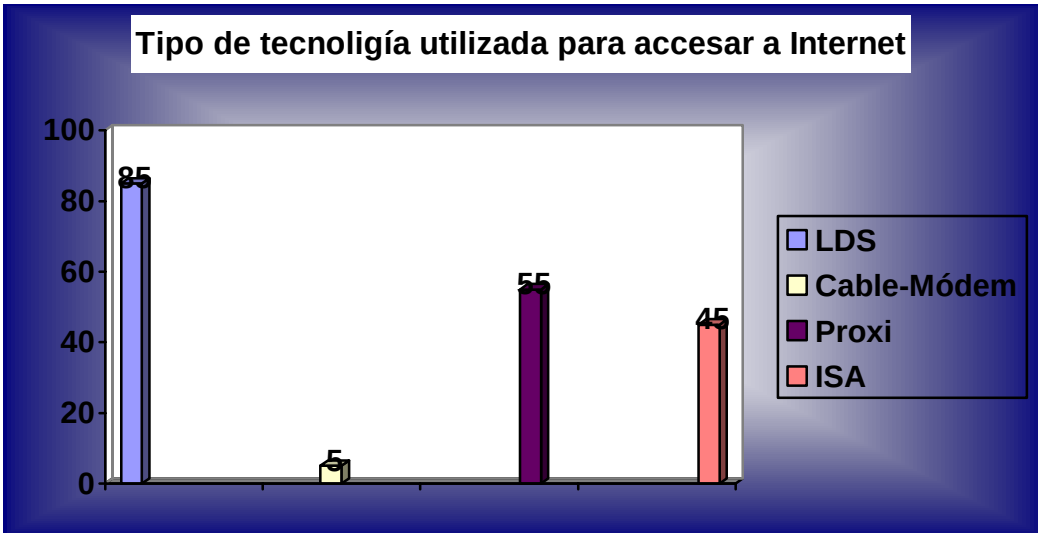
Gráfico #7



Fuente: cuestionario aplicado.

Sin embargo, existe una herramienta gratuita llamada SUS y otra denominada GFILANGUARD que permiten estar en la medida de lo posible, al día con las actualizaciones por medio de parches a nivel de servidores que se aplican de forma manual y terminales generalmente automáticamente y antivirus para optar por un mayor grado de integridad en los datos.

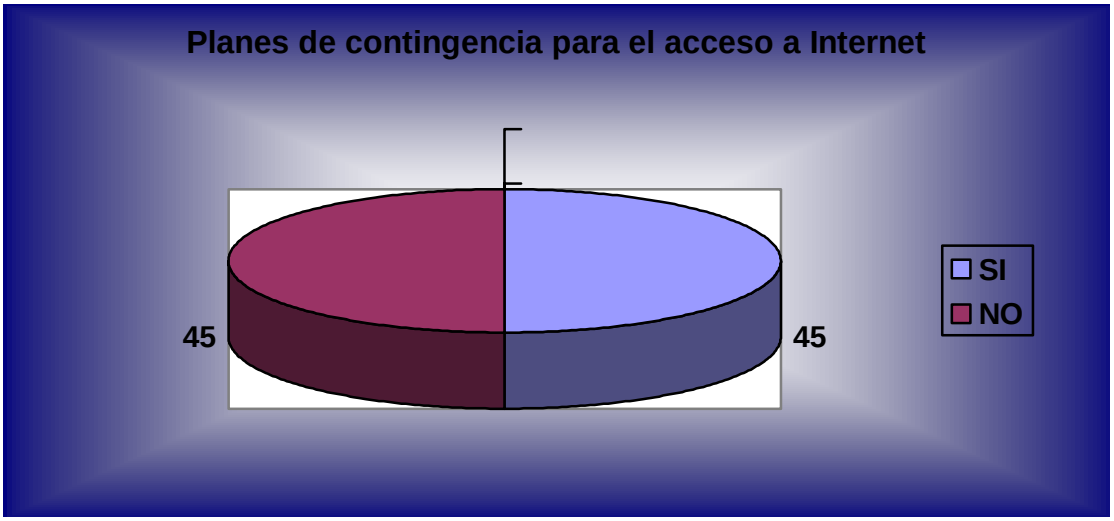
Gráfico #8



Fuente: cuestionario aplicado.

Del cuadro anterior se puede determinar que la mayoría de las instituciones públicas cuentan con la tecnología de línea dedicada: Conmutada (ADSL, RDSL), F.O, VPN y el acceso a Internet se hace por medio de Proxi para transferencia de datos.

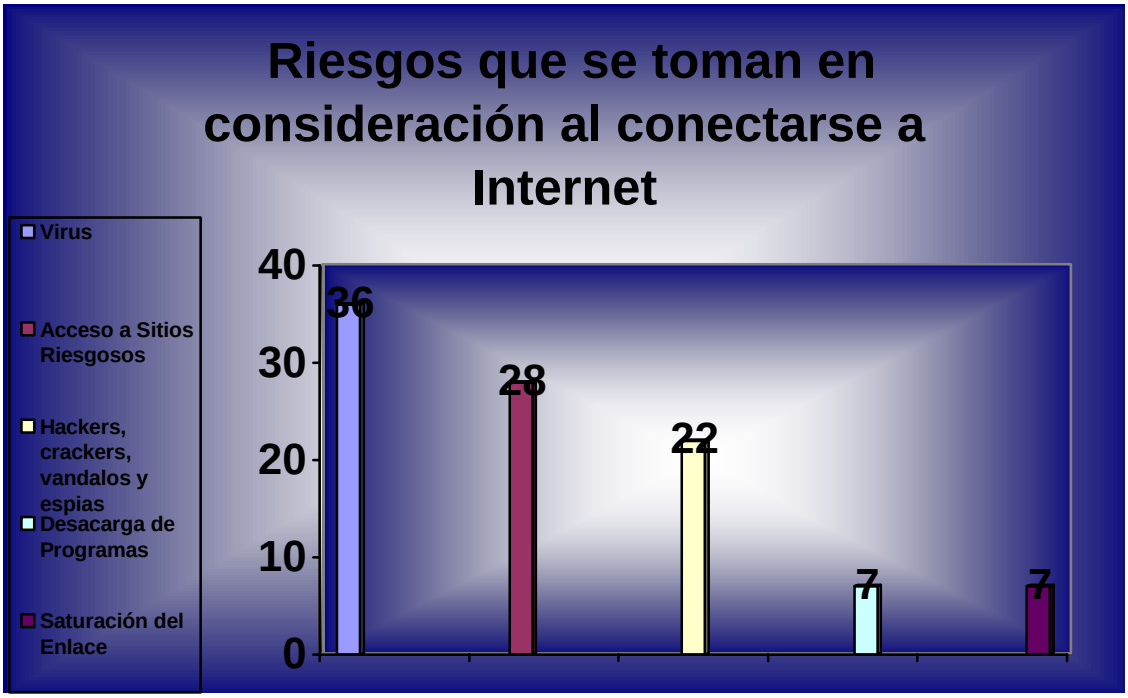
Gráfico #9



Fuente: cuestionario aplicado.

En el cuadro anterior se muestra que hay paridad en cuanto a planes de contingencia de acceso a Internet y como contingencia se utilizan tasas de transferencia de 2Mbps y posteriormente 10Mbps para mantener activo el enlace.

Gráfico #10



Fuente: cuestionario aplicado.

De acuerdo con las repuestas, todos se consideran relevantes como riesgos en cuanto a la conexión a Internet. Sin embargo, se logran destacar dos labores importantes como lo son protección a virus y restricción a sitios potencialmente peligrosos en cuanto a la confidenciabilidad de los datos institucionales.

Cuadro #1

Opinión de los Encargados de Redes sobre la forma de implementar seguridad en la Empresa	**#**	**%**
1. Conformación de Departamento de Control y Gestión de políticas	6	46
2. Definición de usuarios con determinados atributos según funciones	2	15
3. Protección externa contar con PIX y Proxi	2	15
4. Respaldo de Bases de Datos y custodia de los mismos en diferentes lugares	1	8
5. Definición de Claves	1	8
6. Seguridad Física	1	8
Total	13	100

Fuente: cuestionario aplicado.

Cuadro #2

Aspectos importantes en la elaboración de políticas de red	**#**	**%**
1. Definición del tipo de servicio **vrs** vulnerabilidades	6	42
2. Entorno definido y sus interacciones interno/externo	5	36
3. Toma de decisiones e información ágil y oportuna(para resguardar la integridad y Confidencialidad de los datos)	3	22
TOTAL	14	100

Fuente: cuestionario aplicado.

Cuadro #3

Factores que pueden ayudar a contar con seguridad en la red	**#**	**%**
1. Mantenimiento y Actualización de Equipo	7	20
2. Políticas, seguimiento adecuado	6	18
3. Protección en el correo-electrónico	5	15
4. Prevención y Pro actividad de Sistemas de Detección de Intrusos	4	12
5. Concientización al usuario	3	8
6. Bitácoras y Registro	2	6
7. Capacitación del personal	2	6
8. Parches para prevenir vulnerabilidades en la red	1	3
9. Cable y equipos idóneos ajustados a normas	1	3
10. Asesorías Externas	1	3
11. Administración Ancho de banda	1	3
12. Antivirus	1	3
TOTAL	**35**	**100**

Fuente: cuestionario aplicado.

Cuadro #4

Posibles requerimientos para obtener seguridad en la red	**#**	**%**
1. Sistemas de Detección de Intrusos	8	19
2. Contar con el Hardware adecuado	7	16
3. Capacitación de los encargados de Redes	6	14
4. Cumplimiento de política institucional	5	12
5. Planes de contingencia y recuperación de los datos	5	12
6. Análisis de vulnerabilidades	4	9
7. Administración del Ancho de Banda	3	7
8. Control de uso de computadoras y Programas que funcionan como espías en la red	3	7
9. Documentación de la Red	2	5
TOTAL	**43**	**100**

Fuente: cuestionario aplicado

Cuadro #5

Beneficios de contar con una red óptima en cuanto a seguridad	**#**	**%**
1. Gestionamiento de la Red	6	25
2. Estabilidad	5	21
3. Evitar accesos no-autorizados	4	17
4. Aprovechamiento del ancho de banda	3	13
5. Minimización de riesgos de pérdida de información y caídas del sistema	2	8
6. Integridad y confidenciabilidad de los datos	2	8
7. Protección de los recursos de la institución	1	4
8. Menor grado de virus	1	4
TOTAL	**24**	**100**

Fuente: cuestionario aplicado.

CAPÍTULO V

HERRAMIENTAS PARA IMPLEMENTAR SEGURIDAD EN LAS REDES

Las herramientas que se desarrollarán estarán divididas en tres etapas: **herramientas para monitoreo de la red en el entorno externo; monitoreo de virus** y **monitoreo interno**. Estas detallarán todo el proceso que conlleva la implementación de seguridad en las Redes Lan con acceso a Internet en el contexto de las instituciones públicas, teniendo en cuenta herramientas actuales.

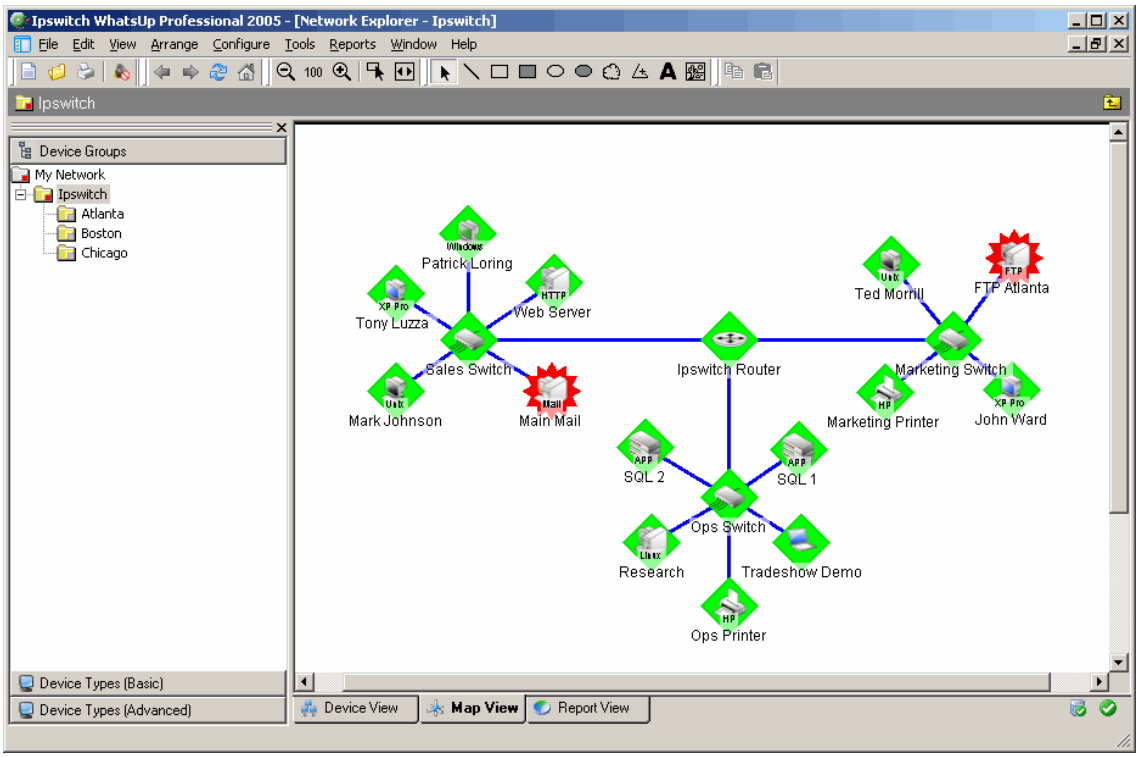
5.1 Monitoreo de la red en el entorno externo

5.1.1 IPSWITCH

Es una solución para pequeñas y medianas organizaciones y proporciona nuevos niveles de escalabilidad, utilidad, y extensibilidad. Esta herramienta permite:

Identificación de la Topología de Red

Descubre los dispositivos de la red automáticamente para crear vistas lógicas de la red. Almacena todos los datos en una base de datos de SQL 2000 que guarda todos los dispositivos de red, registros y datos de configuración. Soporta veinte dispositivos como máximo para escanear, permite explorar la red a través de una tabla de direcciones IP de routers, identifica los tipos de dispositivos, las subredes de la red y funcionamiento crítico de los servidores.



IPSWITCH permite ver:

Lista de dispositivo: brinda una lista de información que muestra el nombre, ip address, tipo y estado del dispositivo.

Enlaces activo y estático: identifican rápidamente cuando la conexión entre los dispositivos está activa o encendida. Las líneas verdes del gráfico indican las interfaces activas, rojo indican que una interfaz ha fallado o se ha apagado.

Opinión del mapa: exhibe la infraestructura de la red en forma gráfica, los íconos del dispositivo personalizados, las líneas de acoplamiento y las herramientas de dibujo avanzadas crean un diagrama verdadero de la red.

IPSWITCH y sus funciones de monitoreo

- **Supervisión portuaria de TCP/UDP:** comprueba el estado de puertos individuales en la red y evita faltas de comunicación en la misma.

- **Registro de los acontecimientos:** identifica acontecimientos potenciales como faltas de autentificación o tarjetas red mediante el registro de syslog de Windows en caso de necesitarse.

- **Supervisión del recurso de sistema:** utiliza la reasignación de los recursos de la red necesarios, tales como CPU, espacio en disco duro, memoria o ancho de banda por medio del escáner y detecta inmediatamente si hay inconvenientes con alguno de estos recursos.

- **Modo de Mantenimiento:** permite programar el mantenimiento de los dispositivos para asegurar la supervisión y un uso adecuado de los recursos.

IPSWITCH y sus funciones de alerta

Ipswitch ejecuta acciones específicas cuando falta un dispositivo o se ha comprometido el funcionamiento del sistema, informando al administrador de la red de estas alteraciones por medio de notificaciones o a través de alarmas y políticas individuales de la acción del sistema.

- **Alerta robusto**: envía un correo, mensaje sms o sonido como señal de notificación.
- **Modifica las alarmas individuales del servicio para requisitos particulares:** puede seleccionar un tipo de acción por ejecutarse basado en el tipo de dispositivo o de servicio individual que ha fallado.

IPSWITCH y sus funciones de reporte

Analiza las tendencias de la red, las cuales se reflejan a través de informes de los dispositivos y servicios. Estos se pueden generar por mes, semana, día u hora, según el interés de la administración.

5.1.2 GFILANGUARD

¿Por qué utilizar GFI Languard S.E.L.M.?

- Supervisa los sucesos de seguridad críticos en toda la red, detecta ataques y usuarios de red maliciosos.
- Recibe alertas sobre sucesos críticos de Exchange, ISA, SQL y Servidores IIS.
- Hace copia y limpia los registros de sucesos de toda la red y los almacena en una base de datos central.
- No se necesita software/agente cliente para su funcionamiento.

¿Por qué escoger GFI Network Server Monitor?

- Supervisa la red y servidores buscando fallos del software y hardware.
- Proporciona una lista para la supervisión de Exchange, ISA, SQL y servidores Web.
- Vigila el espacio en disco, servicios y procesos de servidores y estaciones de trabajo.
- Fácil de aprender y utilizar y sencillo de implementar.
- Vigila automáticamente su red y servidores en busca de fallos y permite a los administradores solucionar e identificar los problemas antes de que los usuarios los informen.
- Las alertas pueden enviarse por correo, buscapersonas o SMS.
- Las acciones, tales como reiniciar el equipo, reiniciar un servicio o ejecutar un script, pueden hacerse automáticamente.

- Permite identificar las tendencias de seguridad, por medio de informes estándar. Además se pueden crear informes personalizados o utilizar los informes estándar que incluyen:
    1. Todas las entradas al sistema (logon) fallidas.
    2. Usuarios que no pudieron entrar debido a un nombre de usuario o contraseña erróneos.
    3. Todas las cuentas bloqueadas durante un período de tiempo.
    4. La hora diaria de entrada al sistema por cada usuario durante un período de tiempo.
    5. En qué equipos iniciaron sesión los usuarios.
    6. Posible manipulación de registros de seguridad durante un período de tiempo.
    7. Sucesos de accesos fallidos a objetos (p.ej. archivos seguros).
    8. Sucesos de seguridad alta del pasado día, semana o mes.

¿Por qué utilizar GFI LANguard Network Security Scanner (GFI LANguard N.S.S)?

- Audita la red buscando debilidades de seguridad.
- Detecta recursos compartidos innecesarios, como puertos abiertos y cuentas de usuario sin utilizarse en las estaciones de trabajo.
- Comprueba e implementa parches de seguridad que falten y service packs a nivel de Sistemas Operativos y en Office.
- Analiza los métodos potenciales que un hacker podría utilizar para atacar la red, mediante el análisis del sistema operativo y de las aplicaciones que se están ejecutando sobre los equipos de red.
- Identifica todas las posibles brechas de seguridad, y alerta al administrador de las debilidades antes de que un hacker pueda encontrarlas, permitiendo que la organización se ocupe de estos casos antes de que un hacker pueda aprovecharlas.

Precios

Starter Packages

		Price
2 servers and 25 workstations *	LANSELMSRV2WKS25	$ 375
5 servers and 50 workstations *	LANSELMSRV5WKS50	$ 750

* Starter packages cannot be combined.

Servers

		Price			Price
3 servers	LANSELMSRV3	$ 395	25 servers	LANSELMSRV25	$ 1995
5 servers	LANSELMSRV5	$ 495	50 servers	LANSELMSRV50	$ 3495
10 servers	LANSELMSRV10	$ 950	100 servers	LANSELMSRV100	$ 6500

Workstations

		Price			Price
25 workstations	LANSELMWKS25	$ 195	250 Workstations	LANSELMWKS250	$ 750
50 workstations	LANSELMWKS50	$ 350	500 workstations	LANSELMWKS500	$ 995
100 Workstations	LANSELMWKS100	$ 595	1000 Workstations	LANSELMWKS1000	$ 1495

Upgrades

Server upgrades

		Price			Price
3 servers	LANSELMSRVVU3	$ 195	25 servers	LANSELMSRVVU25	$ 995
5 servers	LANSELMSRVVU5	$ 250	50 servers	LANSELMSRVVU50	$ 1750
10 servers	LANSELMSRVVU10	$ 475	100 servers	LANSELMSRVVU100	$ 3250

Workstation upgrades

		Price			Price
25 workstations	LANSELMWKSVU25	$ 95	250 workstations	LANSELMWKSVU250	$ 375
50 workstations	LANSELMWKSVU50	$ 175	500 workstations	LANSELMWKSVU500	$ 495
100 workstations	LANSELMWKSVU100	$ 295	1000 workstations	LANSELMWKSVU1000	$ 750

5.1.3 Altiris

Es una herramienta de inventario flexible, como por ejemplo de computadoras, servidores y sistemas remotos que permite administrar eficazmente su empresa. Gracias a la Opción de Inventario se puede implementar y recopilar los datos de equipos que necesiten actualizaciones.

Igualmente es importante mencionar que esta herramienta es compatible con los Sistemas Operativos Windows y Unix.

Con la ayuda de la instalación de un cliente (Client Mgmt Suite), a través de una consola basada en Web, permite que los administradores de TI (Tecnologías de Información) implementen y administren los PC, notebooks y handhelds desde una ubicación central. Client Mgmt Suite permite que los administradores de TI asuman el control de cada PC mediante herramientas que eliminan la necesidad de ir físicamente a cada sistema para implementar, administrar y diagnosticar los problemas.

Client Mgmt Suite contiene:

- Application Metering Solution
- Inventory Solution
- Deployment Solution
- Carbon Copy(Control Remoto)
- SW Delivery Solution

Con este paquete, Altiris es capaz de implementar y migrar sistemas locales u operativos, realizar inventario de hardware y software, rastrear e informar sobre el uso de aplicaciones, distribuir software con base en políticas y control remoto sensible al ancho de banda a nivel de empresa.

Implementación de sistemas:

Client Mgmt Suite proporciona las funciones de clonación, configuración, empaquetamiento e implementación de software y migración de las características personales de los PC para cualquier sistema operativo Windows. También permite instalar sistemas operativos o locales en caso de que la conexión se pierde durante la descarga.

Rastreo del uso de aplicaciones:

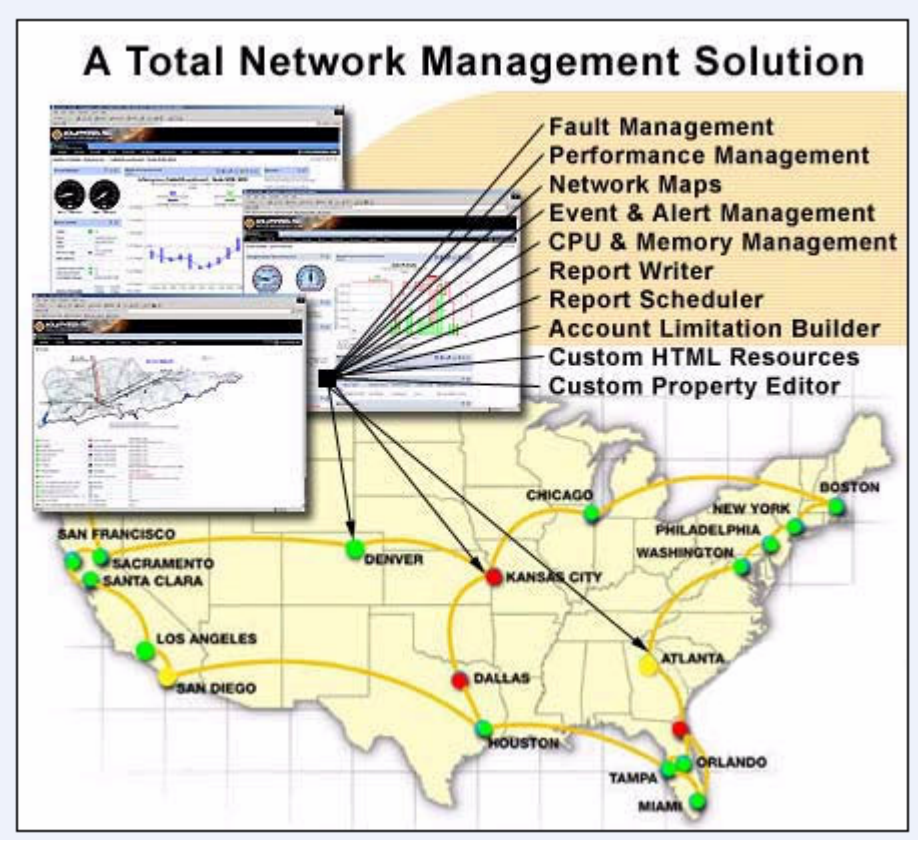
Client Mgmt Suite va un paso más allá de la recopilación de inventarios; también incluye el rastreo y la generación de informes sobre las aplicaciones que se encuentran en ejecución en los sistemas cliente y monitorea el uso de dichas aplicaciones. Al contar con estos datos, la administración se encuentra mejor capacitada para redistribuir las licencias no utilizadas o de uso poco frecuente, para determinar las compras futuras de software y para monitorear pro activamente las aplicaciones no aprobadas que puedan existir en la empresa.

Beneficios

- Rastrea los activos en toda la empresa.
- Crea rápidamente informes detallados y personalizados.
- Detecta e incluye en el inventario virtualmente cualquier sistema que utilice un sistema operativo Windows de 32 bits o Unix.
- Soporte integrado para Microsoft SMS.
- Incluye funciones potentes para actualización por Web.
- Recopila los números de serie y las direcciones MAC para simplificar el rastreo de activos.
- Fácil de implementar y configurar.
- Tecnología integrada de implementación y migración que brinda soporte para PCs, notebooks y handhelds.
- Inventario automatizado de hardware y software con informes basados en Web.

- Visualización detallada de las propiedades de computadores remotos junto con un control remoto sensible al ancho de banda.
- Entrega de software basada en políticas (a solicitud del cliente) o entrega de software en tiempo real.
- Notificación de correo electrónico incorporada.
- Recuperación de puntos de verificación, limitación de ancho de banda, compresión, bloqueo de red y programación de entrega de software
- Brinda soporte para WAN, LAN y clientes móviles y handheld

5.1.4 SOLARWINDS



Características

Herramientas de la gerencia y de la disponibilidad de avería

Analiza el estado de miles de nodos y de interfaces de un sitio Web, mostrando el estado del dispositivo (encendido o apagado), ancho de banda y tráfico de los enlaces.

CPU, memoria y supervisión de espacio de disco

Muestra la carga del CPU, utilización de memoria, uso del ordenador y espacio de disco disponible para los dispositivos, por ejemplo: Linux, Solaris, Windows.

Mapas De la Red

Permite agregar cualquier mapa existente de la red para hacer las modificaciones convenientes con opción de realizar los cambios en “caliente” (arrastrando nodos sobre él) para mantener un diagrama actualizado de la red, agrupando la red en regiones o subredes.

Acontecimientos y herramientas de gerencia alertas

Con Orión usted puede fijar parámetros para alertar cuando un dispositivo está encendido o apagado, los porcentajes de ancho de banda utilizados, memoria, CPU y espacio en disco duro para ser divulgados o notificados por medio de correo a cualquier dispositivo compatible.

Vistas personales / Menús / Barra de herramientas

Cuentan con opiniones de personalización según los requerimientos y necesidades del usuario.

Requerimientos del sistema

	SL100	SL250	SL500	SL2000	SLX
Operating System	 **Windows 2000 Server or Adv. Server** **Service Pack 3** **Internet Information Services (IIS) 5.0**				
Database	Microsoft SQL Server 2000 *				
CPU	800 MHz		1.2 GHz	2.0 GHz	
RAM	256 MB	512 MB		1 GB	
HDD	10 GB available disk space			20 GB	
Network	Network card				

Información General

Razón Social: ALFA GPR TECNOLOGÍAS S.A.®

Empresa registrada en la República de Costa Rica en la Oficina de Registro Público en el tomo 1216, Folio 220, Asiento 275 desde el 15 de Octubre de 1999 y cuya cédula jurídica es 3-101-252838.

Teléfax: (506) 263-61-73 / 262-78-09

Inversión Económica

La presente oferta económica detalla los productos solicitados por su representada:

Número Parte	Producto / Descripción	Cantidad	Costo Unitario	Total
LANSSUNL	GFI NSS Análisis y parchado ilimitado de direcciones IP en toda la LAN *	1	$985.00	$985,00
Orión SL100-Part#3931	ORION Network Perf Monitor - SL100	1	$2.510,00	$2.510,00
CONSUL2H	Instalación y Configuración 2 horas	1	0	0
	TOTAL EXENTO DE IMPUESTO			
	TOTAL GENERAL			

* La licencia de análisis y parchado ILIMITADO de IP es por estación de administrador. Si utiliza múltiples copias del GFI LANguard N.S.S., se deben adquirir múltiples licencias. Como por ejemplo, si analiza o parcha 3000 máquinas en su red y 4 administradores utilizan GFI LANguard N.S.S. diariamente en sus máquinas, entonces usted requeriría de 4 licencias de LNSS.

5.1.5 RAdmin

Es un programa que crea una estación de trabajo a distancia, que le permite trabajar en una o más computadoras. Es una solución completa del mando a distancia con las características dominantes: transferencia de archivo y seguridad del NT.

Cómo Trabaja

Se ve el escritorio de la computadora con la que se estableció conexión en su monitor local y tiene una visión completa de los elementos de pantalla. Todos los movimientos realizados se transfieren directamente a la computadora alejada.

Este constituye una herramienta de soporte necesaria en la empresa por motivos de distancia y tiempo de respuesta del equipo de cómputo y usuarios.

Características

Seguridad y confiabilidad

RAdmin es fácil de utilizar y muy seguro por que se basa en un protocolo de TCP/IP. Este es el protocolo más extenso usado en las redes de área ancha y área local, lo cual significa que usted puede controlar una computadora situada en cualquier lugar del mundo. Cuando se está conectado se puede tener control completo del equipo, como por ejemplo transferir archivos, cerrar sesiones o reiniciar el equipo.

Requisitos del Sistema

1. Windows 95 en adelante
2. 32Mb de memoria Ram
3. 2Mb de espacio de disco duro.

La versión de evaluación se puede conseguir en: **ftp://ftp.ttp.co.uk/radmin21.exe**

5.1.6 SUS (Servicios de Actualización de Software)

El servicio de la actualización de software SUS es libre y brindado por Microsoft Windows. Esta herramienta proporciona soluciones de actualización de software para las empresas.

Para ello pueden consultar la página de Microsoft donde existe una guía de referencia del proceso de instalación y configuración que permite evitar posibles vulnerabilidades en la red.

Requerimientos del servidor y cliente

Servidor

- Windows 2000 Server SP4 o Windows Server 2003
- Microsoft Internet Servicios Información (IIS) 5.0 o Microsoft Internet Explorer 6.0

Cliente

- Windows 2000 Service Pack 3 (SP3) o Windows XP, o Windows Server 2003

5.1.7 WINPROXY

WinProxy permite monitorear el acceso a internet debido a que posee características de firewall o cortafuego y servidor proxy, por lo tanto, puede parar virus antes de que ingresen en la red. Además filtran hacia fuera el Spam de su correo y bloquean sitios indeseables de que no deben ser vistos por los empleados o niños.

Características

- La conexión de Internet es rápida debido a una sola conexión.
- Soporta todas las conexiones de Internet (DLS, Cable, ISDN, Frame Relay, Inalámbrico).
- Protección de antivirus siempre activa.
- Firewall de seguridad.

- ❖ Bloqueo de sitios indeseables o riesgosos.
- ❖ Memoria rápida (para peticiones y consulta).
- ❖ Rápido scanner de todos los archivos salientes de la red.
- ❖ Elimina la necesidad de reconfigurar aplicaciones o instalar software especial en cada cliente.

Requisitos del sistema

Requisitos del sistema de WinProxy para 50 usuarios y arriba		
Número de usuarios	Requisitos Mínimos	Recomendado
50 – 100	Máquina Dedicada OS Windows NT4 CPU 600MHz(P3) o mejor 512MB del ESPOLÓN 50MB liberan la espacio de disco	Máquina Dedicada OS Windows 2000 o XP CPU 1.7GHz(P4) 1GB del ESPOLÓN 10GB liberan la espacio de disco
250 – 500	Máquina Dedicada OS Windows 2000 o XP CPU 1.7GHz(P4) o mejor 768MB del ESPOLÓN 5GB liberan la espacio de disco	Máquina Dedicada OS Windows 2000 o XP CPU 1.7GHz (P4) o mejor 1.5GB del ESPOLÓN 20GB liberan la espacio de disco Adaptadores con los almacenadores intermediarios grandes (eg. Intel, los 3Com) Perro guardián apoyado del PCI
1,000 - 2,500	Máquina Dedicada OS Windows 2000 o XP CPU 1.7GHz(P4) - 2.0GHz(Xeon) o mejor 1GB del ESPOLÓN 10GB liberan la espacio de disco, SCSI	Máquina Dedicada OS Windows 2000 o XP CPU 1.7GHz (P4) - 2.0GHz (Xeon) o mejor 2GB del ESPOLÓN 30GB liberan la espacio de disco Adaptadores con los almacenadores intermediarios grandes (eg. Intel, los 3Com) Perro guardián apoyado del PCI

5.1.8 ISA-SERVER 2004

Características

Inspección con estado

ISA Server 2004 realiza una inspección de estado dinámica e inteligente a través del nivel de aplicación del tráfico que atraviesa el servidor de seguridad, el cual inspecciona los protocolos http y ftp del cliente para garantizar la integridad de las comunicaciones e impedir infracciones de seguridad.

Filtrado inteligente de las aplicaciones

ISA Server 2004 va más allá del filtrado básico de las aplicaciones al controlar el tráfico específico de una aplicación, por medio de filtros de datos, comandos, aplicaciones y el filtrado inteligente de VPN, HTTP, FTP, SMTP, POP3, DNS, conferencia y transmisión de multimedia. El ISA Server 2004 puede aceptar, rechazar, redirigir y modificar el tráfico en función de su contenido.

Publicación segura en servidores

La publicación segura en los servidores ayuda a proteger frente a ataques externos los servidores Web, servidores de correo electrónico y aplicaciones de comercio electrónico. ISA Server 2004 puede agregar un nivel de seguridad al suplantar al servidor de publicación. Las reglas de publicación en Web protegen los servidores Web internos gracias a que permiten especificar los equipos a los que se puede tener acceso. Las reglas de publicación en servidores protegen los servidores internos del acceso no deseado por parte de usuarios externos. El filtrado inteligente de aplicaciones protege a todos los servidores publicados de ataques procedentes del exterior.

Detección de intrusos

Mediante las capacidades integradas de detección de intrusos basadas en la tecnología de los sistemas de seguridad de Internet, ISA Server 2004 puede generar una alerta y ejecutar una acción si detecta un intento de invasión en la red, por ejemplo, el examinar determinado puerto para saber si hay vulnerabilidades.

Redes privadas virtuales integradas

Al integrar sus servicios con los servicios VPN de Windows 2000 y Windows Server 2003, ISA Server 2004 permite proporcionar acceso remoto seguro basado en estándares para conectar las sucursales y los usuarios remotos a las redes corporativas. Puede aplicar la directiva de servidor de seguridad de ISA Server a las conexiones VPN para obtener un control más minucioso de los recursos y protocolos a los que pueden tener acceso los usuarios de VPN.

Transparencia del servidor de seguridad

SecureNAT proporciona un acceso transparente al servidor de seguridad y protección para todos los clientes IP, sin que sea necesario realizar ninguna configuración ni software de cliente, sustituyendo por una dirección IP válida globalmente las direcciones IP internas. Los sofisticados filtros del nivel de aplicación incluyen capacidades de administración de conexiones que proporcionan una compleja funcionalidad de protocolos para permitir el uso de clientes SecureNAT.

Autenticación de usuarios segura

ISA Server 2004 permite una autenticación de usuarios segura gracias a la autenticación de Windows integrada (Windows NT, LAN Manager y Kerberos) para su servidor de seguridad y sus clientes proxy Web. Para los clientes proxy Web, el producto permite el uso de certificados de cliente además de admitir una autenticación implícita, básica y anónima en Web que se basa en el uso de formularios. ISA Server puede autenticar a los usuarios con la base de datos de usuarios locales en el servidor de seguridad o Active Directory (Directorio Activo).

5.2 Para monitoreo de Virus

Protección a Virus

Los virus son una amenaza real para la red, los cuales se adquieren fácilmente de discos desconocidos que dañan archivos de servicios interactivos, listas de distribución y de Internet.

Cualquiera de los usuarios de red puede infectarse con un virus y propagarlo por la red. Estos suelen ser difíciles de detectar, por lo que podrían permanecer dentro del sistema sin ser encontrados antes de ser ejecutados.

Usuarios vigilantes o administradores de la red podrían detectar cualquier actividad no habitual o notar un incremento en el tamaño de los archivos al indicar un peligro de infección.

Se pueden localizar en los sistemas al detectar signos inhabituales de actividad, tales como tamaños de archivos muy grandes, cambios de sellado temporal de los archivos, actividad de disco extraña o un descenso abrupto en el espacio de disco.

Se considera conveniente instalar un software de detección de virus que realice la acción automáticamente. Los administradores y usuarios deben conocer acerca de estas técnicas, con el objetivo de poder detectar y evitar virus.

Al detectarse y limpiar una infección por virus, se considera posible que el virus todavía esté en algún lugar de la organización listo para reinfectar los sistemas, por lo que podría incluso haber infectado las copias de seguridad.

Ante la necesidad de contar con una aplicación que nos brinde seguridad ante estos casos de infección se mencionarán algunas herramientas.

5.2.1 Solución Antivirus Symantec

Permite controlar la protección frente a un virus en servidores y estaciones de trabajo, mediante una consola de administración central. Gracias a esta solución es posible identificarlos y replicar actualizaciones con el fin de scanear los archivos para eliminar los infectados por el virus.

La instalación **Symantec Antivirus Solución** incluye cuatro componentes:

- **Consola de Administración**

  Se ejecuta en máquinas que tengan NT /2000. Permite administrar servidores y estaciones de trabajo que tengan instalado Norton Antivirus Corporación Edición y la central de Quarentena, así como gestionar el envío de alertas por medio de correo.

- **Protección frente a virus para servidores**

  Protege los servidores de NT/2000 y NetWare. Además puede enviar valores de configuración y actualización de definición de virus a las estaciones de trabajo.

- **Protección para virus frente a estaciones de trabajo**

  Protege las máquinas con Windows 95/98/NT/2000 y Windows 3.1., incluyendo funciones de actualización y envío de alertas.

- **Symantec Central de Cuarentena**

  Proporciona una respuesta automática frente a los virus nuevos o irreconocibles detectados heuristicamente. Los elementos infectados quedan aislados en los servidores y estaciones de trabajo para posteriormente ser enviados al sitio de Central de Cuarentena.

Requisitos mínimos para la instalación

1. 64Mb de memoria Ram con el módulo integrado de la consola central.
2. 128Mb de memoria Ram con el módulo integrado de central de Cuarentena
3. Procesador Pentium 166 o superior.

5.2.2 Sistema de protección McAfee

McAfee Group Shield for Microsoft Exchange

McAfee GroupShield 6.0 brinda una completa protección antivirus contra amenazas para el correo electrónico y otros contenidos que ingresan y abandonan el entorno Microsoft Exchange Server 2000/2003. El escaneo antivirus proactivo y un administrador automático de contagio evitan que los códigos maliciosos interrumpan el sistema, mientras que el avanzado filtro de contenidos permite a los administradores establecer reglas para los contenidos inapropiados.

Beneficios

Protección proactiva contra amenazas: GroupShield utiliza la avanzada detección heurística y genérica del renombrado motor de exploración McAfee para proteger por adelantado a Microsoft Exchange Server 2000 y Microsoft Exchange Server 2003 contra virus nuevos y desconocidos.

Filtro avanzado de contenidos: el filtro granular del contenido de los archivos adjuntos del correo electrónico ofrece una defensa contra las amenazas destructivas más recientes; es posible aplicar reglas predefinidas o personalizadas para archivos de contenido indeseable a nivel de departamentos o de grupo de usuarios.

Requisitos mínimos para la instalación

1. 256 de Memoria RAM
2. Procesador Pentium 133Mhz en adelante
3. Espacio libre en disco de 800Mb
4. 2000 Server con Service Pack4
5. Internet Explorer 5.5

5.3 Para control interno

Debemos tener en consideración lo siguiente:

5.3.1 Planeación de seguridad en redes

Es importante tener una política de seguridad de red bien concebida y efectiva que pueda proteger la inversión y los recursos de información valiosos de la compañía. La mayoría de las organizaciones tienen en sus redes información secreta o discrecional u otros bienes valiosos como la propiedad corporativa y los edificios de oficinas, por lo que estos deben protegerse del acceso indebido.

La mayoría de los diseñadores de redes por lo general empiezan a implementar soluciones de Firewall antes de que se haya identificado un problema particular de seguridad en la red. Quizá una de las razones de esto es idear una política de seguridad de red efectiva.

Si actualmente sus usuarios tienen acceso irrestricto a la red, puede ser difícil aplicar una política que limite ese acceso. También debe tomar en cuenta que la política de seguridad que debe usar no debe disminuir la capacidad de su organización. Una política de red que impida a los usuarios cumplir efectivamente con sus tareas puede traer consecuencias indeseables, por lo que los usuarios de la red quizá encuentren la forma de eludir la política de seguridad volviéndola inefectiva.

Una política efectiva de seguridad en redes es algo que todos los usuarios y administradores de redes pueden aceptar y están dispuestos a aplicar.

5.3.2 Identificación del uso adecuado de recursos

Es indispensable determinar los usuarios autorizados a tener acceso a los recursos de la red, usted debe establecer los lineamientos del uso aceptable de dichos recursos. Los lineamientos dependen de la clase de usuarios, como desarrolladores de software, estudiantes, profesores, usuarios externos entre otros, por lo que debe tener lineamientos distintos para cada clase. La política debe establecer qué tipo de uso es aceptable y cuál es inaceptable, así como qué tipo de uso esta restringido. La política que elabore será la de Uso Aceptable (AUP) de esa red. Si el acceso a un recurso de la red esta restringido, debe considerar el nivel de acceso que tendrá cada clase de usuario.

Su AUP debe establecer con claridad que cada usuario es responsable de sus acciones. La responsabilidad de cada usuario existe al margen de los mecanismos de seguridad implementados, por ello no tiene caso construir costosos mecanismos de seguridad con firewalls si un usuario puede revelar la información copiando archivos en disco o cinta y poner los datos a disposición de individuos no autorizados.

Evaluar los puntos débiles de la seguridad y tomar las medidas adecuadas puede ser eficaz para evitar ataques de intrusos en la red.

5.3.3 Plan de acción cuando se viole la política de seguridad

Cada vez que se viola la política de seguridad, el sistema está sujeto a amenazas. Si no se producen cambios en la seguridad de la red cuando ésta sea violada, entonces debe modificarse la política de seguridad para eliminar aquellos elementos que no sean seguros.

La política de seguridad y su implementación deben ser lo menos obstructivas posibles. Si la política de seguridad es demasiado restrictiva, o está explicada inadecuadamente, es muy probable que sea violada o desactivada.

Al margen del tipo de política que se implemente, algunos usuarios tienen la tendencia a violarla. En ocasiones las violaciones a la política son evidentes, pero otras veces estas infracciones no son detectadas, por lo que los procedimientos de seguridad que usted establezca deben reducir al mínimo la posibilidad de que no se detecte una infracción de seguridad.

Cuando usted detecte una violación debe determinar si esta ocurrió debido a la negligencia de un individuo, a un accidente o error por ignorancia de la política vigente o si deliberadamente la política fue pasada por alto. En este último caso, la violación quizás haya sido efectuada no sólo por una persona, sino por un grupo que a sabiendas realiza un acto de violación directa a la política de seguridad. En cada una de estas circunstancias ésta debe contar con los lineamientos requeridos acerca de las medidas que se deben tomar.

Debe llevarse a cabo una investigación para determinar las circunstancias en torno a esta violación. Es razonable esperar que el tipo y severidad de la acción dependan de la gravedad de la violación.

5.3.4 Lineamientos de acceso físico

Se debe designar una persona que se encargará de administrar el acceso físico al centro de cómputo, la cual deberá llevar los mecanismos de control necesarios que garanticen los esquemas de seguridad de los equipos ubicados en esta área.

- El control de acceso al centro de cómputo debe tener no sólo la capacidad de identificación, sino también asociarla a la apertura o cierre de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector, horarios semanales y días feriados.

- El sistema de control de acceso debe contar con capacidad para llevar el control de ingreso de usuarios a las áreas asignadas y poder exportar el archivo a otros formatos que puedan ser leídos fácilmente por otros programas.
- El sistema de control de acceso debe poder ser monitoreado por módem externo, de manera que permita ante eventuales incidentes de seguridad ser revisado por la persona asignada por la Unidad de Sistemas y Tecnología de Información vía remota.
- El sistema de control de acceso deberá proveer un mecanismo que permita ante emergencias naturales o por eventos imprevistos que pongan en peligro la integridad física de las personas en las áreas restringidas, poder desactivar los mecanismos de apertura de puertas para la inmediata evacuación del sitio.
- El control de acceso al centro de cómputo deberá contar con cámaras de vigilancia ubicadas estratégicamente dentro del centro de cómputo que permitan llevar a cabo un control más estricto del ingreso de personas al recinto y su futura identificación.
- La tarjeta o mecanismos de control de acceso es el medio de identificación de cualquier funcionario del centro de cómputo y no podrá bajo ningún motivo prestarlo, reproducirlo o violentarlo. Su naturaleza es intransferible.
- Si dos o más funcionarios ingresan simultáneamente al centro de cómputo, deberá cada uno marcar su ingreso dentro del sistema de control de acceso.
- El control de acceso a los equipos de seguridad (firewalls, detector de intrusos o servidor antivirus) deben tener como función mínima la capacidad de validar al usuario basado en una tarjeta de acceso y un PIN numérico ingresado por teclado que identifique al usuario.

- El ingreso de los operadores al centro de cómputo será registrado en un archivo de eventos (logs) del sistema y este registro será cuidadosamente revisado por la jefatura de la Unidad de Sistemas y Tecnología de Información.
- El sistema de control de acceso debe poseer mecanismos que permitan activar alarmas si se violenta el acceso de una puerta en forma mecánica sin haber validado a ningún usuario previamente.
- Cuando se retiren funcionarios claves, deben cambiarse sus códigos de acceso, retirarse su tarjeta de acceso y sacarlo de la base de datos del sistema de control de accesos. Todos los funcionarios con acceso al centro de cómputo son responsables de aplicar adecuadamente los procedimientos de seguridad de acceso físico y de informar cualquier sospecha de violación de las medidas a su jefe inmediato.
- Todos los funcionarios y personal de empresas suplidoras de mantenimiento o limpieza que deban ingresar al centro de cómputo, deberán firmar un libro o bitácora de control de entrada y salida del centro. Con este procedimiento se llevará un mejor control de los funcionarios que se encuentran en el centro de cómputo y permitirá contar con un mecanismo de verificación alternativo al sistema de control de acceso.

5.3.5 Directrices para protección de contraseñas

- No lo escriba en papel ni lo almacene en su oficina
- No almacene estas contraseñas en NINGUNA computadora de la oficina (incluyendo Palm Pilots o dispositivos similares sin encriptación).
- No se debe permitir compartir las contraseñas con otros funcionarios, ya que estas deben ser tratadas como sensitivas y de información confidencial de la empresa.
- No se permite utilizar las funciones de “recordar password” de aplicaciones que permitan esta facilidad, como por ejemplo Eudora, Outlook, Netscape y Messenger.
- No se permite realizar ninguna de las siguientes condiciones ya que estas atentan contra la confidencialidad de las contraseñas:
    1. Revelar una contraseña en una conversación telefónica.
    2. Revelar una contraseña en un mensaje de correo.
    3. Revelar una contraseña a terceras personas.
    4. Hablar de una contraseña en frente de otros.
    5. Dar pistas sobre el formato de una contraseña (Ej.: “Mi apellido paterno”).
    6. Revelar una contraseña en un cuestionario o formularios de seguridad.
    7. Compartir las contraseñas con miembros de la familia.
    8. Revelar una contraseña a un compañero de trabajo mientras está de vacaciones.

Todos los usuarios deben conocer cómo elegir contraseñas robustas.

Las contraseñas robustas tienen las siguientes características

Contienen letras en mayúscula y en minúscula (Ej.: a-z, A-Z)
Tienen dígitos y caracteres de puntuación, así como letras, por ejemplo, 0-9!,@#$%^&*()_+|~=\`{}[]:";'<>?,./)
Son de por lo menos ocho caracteres alfanuméricos.
No son una palabra en ningún lenguaje, dialecto, muletilla o jerga cotidiana.
No están basados en información personal, o nombres de familiares.

CAPÍTULO VI
CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

Seguidamente se describen las conclusiones a las que se llega al finalizar este trabajo de investigación sobre el tema: Seguridad en Redes Lan con acceso a Internet en las instituciones públicas de San José.

- La totalidad de las empresas públicas trabajan con la plataforma de Microsoft en un mayor grado, en relación con sistemas operativos e inclusive herramientas en pro de la seguridad en las redes locales y con acceso a Internet.

- Para adquirir el hardware se requiere seguir alguna opción de adquisición, entre las que están: compra directa que es la compra de un equipo, desembolso el precio en el momento de realizar el contrato. El leasing o alquiler con opción de compra que permite que el equipo sea alquilado con miras a adquirirlo en un futuro, debido a que cualquier adquisición de tecnología informática, dentro de la que se ubica el hardware, debe tener un proceso lógico y ordenado que considere aspectos técnicos y administrativos para garantizar que los niveles de inversión que se realizan responden a la calidad del producto que se va adquirir en la institución.

- Se investigó sobre el tema de la seguridad en las redes LAN con acceso a Internet y se refleja que es necesario contar con normas para la seguridad de las empresas y posteriormente considerar aspectos de seguridad física, lógica (Claves) además la implementación de políticas por personal interno para resguardar la protección de los datos organizacionales.

- Los encargados de redes entrevistados consideran necesaria la conformación de un departamento de control y gestión de politicas también la definición de usuarios con determinados atributos según sus funciones en el entorno interno. Por otra parte en el externo se debe contar con PIX o Proxi según los requerimientos de la empresa.

- La correcta implementación de políticas sí ha influido en el rendimiento de la red. Sin embargo, se refleja un efecto secundario como lo es un mayor consumo de ancho de banda. Ante tal evento, las instituciones tendrán en cuenta las consideraciones pertinentes para el funcionamiento competitivo y exitoso de las empresas.

- Los aspectos importantes en la elaboración de políticas de red traen como consecuencia los siguientes aspectos: la definición del tipo de servicio y sus vulnerabilidades además conocer en entorno y sus interacciones tanto internas y externas, para lograr definir un mejor aporte al gestionamiento de la red.

- Se determina que la mayor parte de las empresas cuentan con herramientas para la protección de intrusos unificando criterios por parte de los encargados de redes y soporte técnico para dar a conocer las herramientas disponibles en el mercado.

- Casi la totalidad de la muestra de los encargados de redes utiliza alguna herramienta para monitorear el ancho de banda en las empresas, dentro de las que mencionaron se encuentran SolarWinds Network Performance Monitor para lograr obtener un mayor control de la red empresarial.

- Se debe controlar y administrar la manera en que se realiza la actualización de software en la empresa. Por lo tanto, es importante saber que existen herramientas que nos permiten estar a la vanguardia como lo son: SUS (Subscripciones de Actualización de Software) la cual es gratuita y por otra parte GFILANGUAR.

- El grado de satisfacción de las instituciones públicas se inclina por la tecnología de línea dedicada Conmutada (ADSL, RDSI), F.O o VPN y el acceso a Internet se hace por medio de Proxy para la transferencia de los datos.

- Dentro de los planes con que se cuenta con respecto a la contingencia del acceso a internet hay igualdad de criterios por parte de las empresas lo que se denota son las variaciones de velocidades necesarias para cada organización para mantener el enlace activo.

- Dentro de los riesgos más comunes y peligrosos que pueden tomarse en consideración al conectarse a Internet se encuentran: la protección de virus y la restricción a sitios potencialmente perjudiciales para la confidenciabilidad de los datos empresariales.

- Es necesario contar con factores que puedan ayudar a contar con seguridad en la red, según lo expresado por los encargados de redes y soporte técnico. Entre las principales opiniones están: mantenimiento y actualización de equipo de computo, politicas y seguimiento adecuado, protección en el correo electrónico, prevención y pro actividad de sistemas de detección de intrusos, concientización a los usuarios, capacitación del personal para lograr obtener mejor control e integridad de los datos.

- Los requerimientos para obtener seguridad en la red constituyen la razón de ser del proyecto de seguridad en las redes LAN con acceso a Internet por lo que se procede a mencionarlos: sistemas de detección de intrusos, contar con el hardware adecuado, capacitación de los encargados de redes, cumplimiento de la política institucional, planes de contingencia y recuperación de datos, análisis de vulnerabilidades, administración del ancho de banda, control del uso de computadoras y programas que funcionan como espías en la red, documentación de la red, que darán un grado optimo de estabilidad y administración.

- Dentro de los beneficios de contar con una red óptima en cuanto a seguridad, según los encargados de red y soporte técnico, cabe resaltar las siguientes: gestionamiento de la red, estabilidad, evitar accesos no-autorizados, aprovechamiento del ancho de banda disponible, minimizar los riesgos de perdida de información y caídas del sistema, integridad y confidenciabilidad de los datos, protección de los recursos de la institución, menor grado de virus. Así, se logrará ir hacia un proceso de éxito.

6.2 RECOMENDACIONES

A partir de las conclusiones, se pueden establecer las siguientes recomendaciones:

- Considerar qué se debe tomar en cuenta para llevar a cabo dicho proceso lógico durante la adquisición o revalorización de equipo de cómputo, dependiendo de las necesidades del mercado que son muy variadas, y orientadas al tipo de servio que brinden las empresas.

- Definir normas y políticas institucionales que permitan resguardar los datos con el fin de establecer límites y protección de los recursos de la empresa y mantener las actualizaciones correspondientes para lograr los objetivos de las entidades.

- Analizar y revisar la tecnología existente de la empresa antes de definir cambios necesarios en la red, para que no se incurra en gastos innecesarios y obtener el mejor funcionamiento y aprovechamiento posible.

- La proyección de herramientas estimadas en la investigación para la detección de intrusos en la red son de tomar en cuenta como es el caso de IPSWITCH y WinProxy además Honey Pots. Las dos primeras herramientas se puede tomar como referencia a la empresa sispam disponibles para controlar el ancho de banda y estado de los enlaces, transferencia de datos en el caso de la última herramienta que funciona para verificar el ingreso de posibles intrusos en la red pueden comunicarse con ITS.

- Es recomendable que se brinden asesorías integrales que se ajusten a los requerimientos de la empresa, en cuanto a actualización de software como el caso de Alfa Group Tecnologías con excelentes niveles de calidad y ventaja competitiva para que las empresas. Además pueden comunicarse también con Microsoft ofrece una herramienta gratuita para actualizaciones como lo es SUS (Subscripciones de actualización de Software)

- Se debe evaluar y tomar en cuenta las influencias del mercado en cuanto a las tecnologías de contingencia del acceso a Internet y posteriormente las velocidades con que van a contar; cuanto sean, mayores dividendos traerá para la empresa y sus trabajadores.

- Se debe tener en consideración que cuando ingresamos a la Internet nos exponemos a una serie de riesgos y peligros propensos a dañar la integridad de los datos institucionales por lo cual es indispensable contar con alguna herramienta para la protección de virus y posteriormente restringir el ingreso a sitios potencialmente dañinos.

- La etapa de planeamiento del proyecto debe contemplar actividades con factores que puedan ayudar a contar con seguridad en la red que permitan tener un mayor control e integridad en los datos de la empresa.

- Se deben definir los requerimientos de la mejor forma posible, en cuanto a la seguridad de los datos en la red, con la ayuda de instrumentos de investigación que ayuden a la identificación de los requerimientos como lo puede ser la entrevista, las cuales son permiten tener una relación directa, al realizar consultas y preguntas personales para obtener un gestionamiento dirigido hacia un proceso exitoso.

- Según el grado de seguridad que resguardan las empresas, a favor de ello se reflejan los beneficios y así se obtiene el mayor aprovechamiento para la empresa. Otro aspecto importante de recalcar es la documentación, que sirva como respaldo y justificación de cada etapa, para lectura de nuevos integrantes del grupo al proyecto de la seguridad en las redes LAN con acceso a Internet.

GLOSARIO

Browser Término aplicado normalmente a los programas que permiten acceder al servicio de Internet.

CERT Equipo de Respuestas de Emergencias de Cómputo

DMZ Zona desmilitarizada. Red de computadoras localizada en un ambiente de Internet, en donde se localizan equipos de una u otra forma expuestos públicamente. Los servidores WEB generalmente están en la DMZ.

Firewall Tecnología de software y hardware diseñada para proteger la información almacenada en cualquiera de los componentes tecnológicos de una organización. Usualmente el firewall está compuesto por elementos físicos de control de acceso a servicios y puertos de un servidor, sensores de detección de intrusos, tecnología de acceso encriptado a servidores, programas de control de virus informáticos, firewalls personales instalados en las estaciones de trabajo.

Hardware Todos los componentes electrónicos, eléctricos y mecánicos que integran una computadora, en oposición a los programas que se escriben para ella y la controlan software

Host Computador conectado a Internet. Computador en general, anfitrión.

HTML Lenguaje de Marcas de Hipertexto. Lenguaje para elaborar páginas Web, desarrolladas en el laboratorio CERN en Ginebra, Suiza.

HTTP HyperText Transfer Protocol. Protocolo de Transferencia de Hipertexto.

IDS Sistema de detección de intrusos, compuesto generalmente de una consola de administración, sensores de red (físicos o lógicos) y sensores de host (instalados sobre el sistema operativo de los servidores institucionales.

ISDN Integrated Services Digital Network. Red Digital de Servicios Integrados. En español RDSI. En Costa Rica un buen ejemplo de la utilización de la ISDN es el modelo de tele conferencia que tiene la CCSS, mediante el cual, utilizando conexiones ISDN, establecen videoconferencias entre diversos hospitales.

POP Post Office Protocol. Protocolo de Oficina de Correos. Protocolo usado por computadores personales para manejar el correo, sobre todo en recepción.

Protocolo Conjunto de reglas definidas para realizar la comunicación entre dos o más dispositivos que se encuentren en una misma red. El ejemplo más común de un protocolo es el de TCP/IP.

Protocolo POP3 Es uno de los más conocidos para recibir mensajes electrónicos por Internet. Es inseguro desde el punto de vista de que los datos que se transmiten viajan sin ningún tipo de cifrado.

Protocolo SMTP Es uno de los más conocidos para transmitir mensajes electrónicos por Internet. Un servidor de correo electrónico deberá al menos tener los dos protocolos (POP3 y SMTP) activos para operar adecuadamente. Existen otros como el IMAP4 que son más seguros para el envío y recepción de correo electrónico.

Protocolo TCP/IP Conjunto de protocolos utilizados por todos los dispositivos que se interconecten a Internet.

Proveedor de Acceso o ISP Centro servidor que da acceso lógico a Internet, es decir, sirve de enlace (Gateway) entre el usuario final e Internet. También se conoce como ISP.

Proveedor de Conexión Entidad que proporciona y gestiona enlace físico a Internet, por ejemplo, telefónica. En Costa Rica el ICE y las cableras (Cable

PROXY Servidor Cache. El Proxy es un servidor que, conectado normalmente al servidor de acceso a la WWW de un proveedor de acceso, almacena toda la información que los usuarios reciben de la WEB, por lo tanto, si otro usuario accede por medio del proxy a un sitio antes visitado, recibirá la información del servidor Proxy en lugar del servidor real de conexión.

Seguridad de correo electrónico Garantía de que un mensaje de correo Electrónico no ha sido visto por terceras personas.

Sensores de detección de intrusos es uno de los componentes de un sistema de firewall institucional, que consiste de dispositivos físicos o lógicos que tienen como objetivo analizar el tráfico de datos y emitir una alerta si se considera “sospechoso”, con base en patrones preestablecidos de posibilidades de violaciones o hackeos. Estos sensores se comunican con una consola de administración, la cual puede tomar varias acciones, entre ellas, enviar mensajes de radiolocalización o reconfigurar dinámicamente las listas de acceso a los enrutadores. Adicionalmente existen los sensores de host, componentes de software que se instalan para que operen en conjunto en el sistema operativo y detecten cualquier anomalía que se pueda presentar ante cambios no autorizados en la configuración del sistema operativo del servidor.

SMPT Simple Mail Transfer Protocol. Protocolo de Transferencia Simple de Correo. Es el protocolo usado para transportar el correo por Internet.

Sniffer "Husmeador". Pequeño programa que busca una cadena numérica o de caracteres en los paquetes que atraviesan un nodo, para conseguir información

Spam / Spammer "Bombardeo" con correo electrónico, es decir, grandes cantidades de correo o mensajes muy largos, generalmente no solicitados por el destinatario.

TCP Transmisión Control Protocol. Protocolo de Control de Transmisión. Uno de los más usados en Internet; en la capa de transporte.

Vulnerabilidad Problema de seguridad debidamente documentado, relacionada con algún componente (hardware o software) de los sistemas informáticos. Se utiliza por terceras personas para dañar los sistemas.

WWW, World Wide Web. Telaraña mundial, para muchos la WWW es Internet, para otros es solo una parte de esta. La WEB es la parte de Internet a la que se accede por medio del protocolo HTTP y gracias a browsers normalmente gráficos, como Netscape o Internet Explorer.

REFERENCIAS BIBLIOGRÁFICAS

Hernández Sampieri, Roberto; Fernández Collado, Carlos y Baptista Lucio, Pilar (2003). *Metodología de la Investigación.* México: Mc Graw Hill.

Malean, H.G. (2004). *Metodología para el desarrollo de un Datawarehousing.* Tesis de licenciatura no publicada, ULACIT, San José, Costa Rica.

Rodríguez, Nuria y Martínez, Wuillian (1998). *Planificación y Evaluación de Proyectos Informáticos*. San José: EUNED.

Altiris. (2004). *Solución de Desarrollo Altiris*. Recuperado el 25 de octubre de 2004, de www.altiris.com

Microsoft. (2004). *Vista de la actualización de Servicios y Características de ISASERVER 2004*. Recuperado el 25 de octubre de 2004, de www.microsoft.com

IPSWITCH. *Introducción de la herramienta Ipswitch*. Recuperado 26 de octubre de 2004, de www.ipswitch.com

WinProxy. *Total protección de la red*. Recuperado 28 de octubre 2004, de www.winproxy.com

GFI. *Supervisión de los registros de sucesos*. Recuperado 30 de octubre de 2004, de www.gfi.com

SOLARWINDS ORION. *Características del Monitor de funcionamiento de la Red Orion*. Recuperado 4 de noviembre 2004, de www.rootaccount.net/solarwinds

Cappuccio, Victor, E. *Políticas y Procedimientos en la seguridad de la información*. Recuperado 15 de abril de 2004, de www.ilustrados.com

TechNet de Microsoft. *Información de service packs*. Recuperado 20 de abril 2004, de www.technet.com

ABCDATOS. *Información sobre Honey Posts*. Recuperado 22 de junio 2004, de www.abcdatos.com o www.honeypots.net

Symantec. *Utilidad de está herramienta de antivirus*. Recuperado 20 de diciembre 2004, de www.symantec.com

McAfee. *Funciones de está herramienta de antivirus*. Recuperado 21 de diciembre 2004, de www.mcafee.com

ANEXOS

Universidad Latinoamericana de Ciencia y Tecnología
Ingeniería en Informática

Cuestionario para los Encargados de Redes

Fecha: _____

Revisado por: Douglas Miranda Méndez

Objetivo: Obtener información valiosa y concisa de los Encargados de proyectos como de Soporte Técnico y Administradores de Redes de las instituciones públicas del país, sobre el proceso de implementación de normas o politicas en las redes LAN que cuentan con acceso a Internet.

Instrucciones: Marque con una (x) en caso de pregunta(s) cerradas. En caso de preguntas cerradas con opción múltiple marque con una (x) las opciones que considere correctas en su caso. Para el caso de las preguntas abiertas, favor ser breve y conciso.

Nombre la Empresa o Institución en la que labora

---

1. ¿Indique el número de personas que conforman el departamento de Informática?
   _____
2. ¿Cómo esta dividido este grupo en la realización de sus actividades?
   _____
   _____
   _____
3. ¿Existe un departamento de tecnologías de información en la institución? (SI / NO)
4. ¿Marca(s) de equipo(s) de computo que trabajan en la empresa?
   a). Dell b). Compaq c). Everest d). H.P
   e). Aopen f). Macintosh g). Genericos
   h). Otro: Especifique _____
5. ¿Cuáles sistemas operativos se manejan en la institución?
   a). win95 b). win98 c). win2000 d). winXP
   e). 2000Server f). 2003Server g). Unix h). Linux
   i). Otro: Especifique _____
6. ¿Cuál es el equipo activo de comunicaciones que poseen actualmente?
   a). Firewall b). Router c). Switch d). Hub
   e). Access_Point f). Otro: Especifique _____
7. ¿Condición del equipo de comunicaciones actualmente de la empresa?
   a). Comprado b). Alquilado c). Prestado d). Leasing
   e). Todos f). Otro: Especifique _____ ___

8. ¿En caso de que el equipo de comunicaciones se dañe o esté en reparación el proveedor de servicios les da opción de préstamo? (SI / NO)

9. ¿Los medios existentes para la transmisión de datos en la institución?
   a). Cable coaxial b). Cable UTP c). Fibra Óptica d). Antenas
   e). Redes_Inalambricas (aire) f). Otro: Especifique _____

10. ¿La empresa cuenta con alguna norma para brindar seguridad en los datos? (SI / NO)

11. ¿Actualmente de que forma implementan la seguridad en la empresa?
    _____
    _____
    _____
    _____

12. ¿La implementación de politicas en la red fue desarrollada por?
    a). personal de la empresa b). Outsourcing

13. ¿Considera usted que cuenta con una política de red efectiva? (SI / NO)

14. ¿El desarrollo de politicas, ha influido en el rendimiento de la red? (SI / NO)

15. ¿En algún momento se ha solicitado ampliar en ancho de banda de la red? (SI / NO)

16. ¿Mencione aspectos importantes en la elaboración de politicas de seguridad en la red?
    _____
    _____
    _____
    _____
    _____

17. ¿Han realizado medidas de corrección para que la política de red se ajuste a los Requerimientos de los usuarios? (SI / NO)

18. ¿Cuentan con herramientas para la detección de intrusos? (SI / NO)

19. ¿Cuenta con alguna metodología para evitar el ingreso de intrusos en la red? (SI / NO)
    Si su pregunta es afirmativa pase a la siguiente pregunta, de lo contrario pase la pregunta Número 21.

20. ¿Mencione aspectos importantes de está metodología utilizada?
    _____
    _____
    _____
    _____
    _____

21. ¿Maneja una herramienta para monitorear el ancho de banda consumido en la red? (SI / NO)

22. ¿En caso de ser afirmativa su respuesta, comente la herramienta y de que forma de ha Ayudado?

_____
_____
_____
_____

23. ¿De que manera se realiza la actualización de software(Terminales o Servidores) en la empresa?

a). Automáticamente b). Manualmente c). Ninguna

24. ¿Basado en la pregunta # 22 indique las herramienta(s) y en que se basaron para su escogencia?

_____
_____
_____
_____
_____

25. ¿Qué tipo de tecnología utiliza para accesar a Internet?

a). Cable _ módem b). ASDL c). ISA d). DLS
e). Proxy f). Otro: Especifique _____

26. ¿Tiene planes de contingencia para la recuperación de fallos del acceso a Internet? (SI / NO)

27. ¿Tasa de transferencia del enlace de Internet que maneja la empresa? _____

28. ¿Ha participado en capacitaciones que lo mantienen actualizado sobre la seguridad en la red? (SI / NO)

29. ¿Realiza campañas para la concientización de la seguridad en Internet a sus usuarios finales? (SI / NO)

30. ¿Mantiene perfiles definidos para los usuarios que tienen acceso a Internet? (SI / NO)

31. ¿Utiliza alguna herramienta que permita filtrar el acceso a sitios no permitidos de Internet? (SI / NO)

32. ¿Se realizan auditorias a los usuarios con respecto al acceso a Internet? (SI / NO)

33. ¿Qué riesgos se toman en consideración al conectarse a Internet?

_____
_____
_____
_____

34. ¿Mencione factores que nos pueden ayudar a contar con seguridad en la red?

_____
_____
_____
_____
_____

35. ¿Comente posibles requerimientos para obtener seguridad en la red?

_____
_____
_____
_____
_____

36. ¿Cite los beneficios de contar con una red óptima en cuanto a seguridad?

_____
_____
_____
_____
_____

Universidad Latinoamericana de Ciencia y Tecnología
Ingeniería en Informática

Entrevista dirigida a Encargados de Proyectos

Fecha: _____

Revisado por: Douglas Miranda Méndez

Objetivo: Obtener información valiosa y concisa de los Encargados de proyectos como de Soporte Técnico y Administradores de Redes de las instituciones públicas del país, sobre el proceso de implementación de normas o politicas en las redes LAN que cuentan con acceso a Internet.

Entrevista:

1. Indique el número de personas que conforman el departamento de informática
2. Como esta divido este grupo en la realización de actividades
3. Existe departamento de tecnologías de información en la institución
4. Trabajan con una marca especifica o varias de equipo de computo
5. Cuales sistemas operativos se manejan dentro de la empresa
6. Equipo activo de comunicaciones dentro de la institución
7. Actualmente el equipo de comunicaciones de la empresa es:
   a). Comprado b). Alquilado c). Prestado
   d). Leasing e). Todos f).Otro: Especifique _____
8. En el caso de que el equipo de comunicaciones este en reparación el proveedor de servicios les da opción de préstamo.
9. Los medios existentes para la transmisión de datos en su empresa:
   a). Cable Coaxial b). Cable par trenzado (UTP)
   c). Cable Fibra Óptica d). Redes Inalámbricas (aire)
   e). Otro: Especifique _____
10. la empresa cuenta con alguna norma para brindar seguridad en los datos
11. Actualmente de que manera implementa la seguridad en la empresa
12. La implementación de politicas en la red fue desarrollada por:
    a) personal de la empresa b) Outsourcing
13. Considera que cuenta con una política de seguridad de red efectiva
14. Mencione aspectos importantes en la elaboración de políticas de seguridad en la red
15. Han realizado medidas de corrección para que la política de red se ajuste a los requerimientos de los usuarios.
16. Cuentan con herramientas para la detección de intrusos IDS
17. Cuenta con alguna metodología para evitar el ingreso de intrusos en la red
18. Mencione aspectos importantes de está metodología utilizada
19. De que manera se realiza la actualización de software (Terminales o Servidores) en la empresa. (Automática, Manual, Ninguna).
20. En que se basaron para la escogencia de estas herramientas.
21. Tipo de tecnología utilizada para accesar a Internet (Pq)
22. Tiene planes de contingencia para la recuperación de fallos del acceso a Internet
23. Tasa de transferencia del enlace de Internet que maneja la empresa
24. Mantiene un rol de actualización en capacitación del personal encargado de la seguridad de Internet
25. Realiza campañas de concientización de la seguridad en Internet a sus usuarios finales
26. Se realizan auditorias a los usuarios con respecto al acceso a Internet
27. Que riesgos se toman en consideración al conectarse a Internet
28. Mencione factores que nos pueden ayudar a contar con seguridad en red

29. Comente posibles requerimientos para obtener seguridad en la red
30. Cite algunos beneficios de contar con una red óptima en cuanto a seguridad

Universidad Latinoamericana de Ciencia y Tecnología
Ingeniería en Informática

Cuestionario para los Encargados de Soporte Técnico

Fecha: _____

Revisado por: Douglas Miranda Méndez

Instrucciones: Marque con una (x) la opción que considere correcta en su caso.

1. ¿Cómo realiza sus labores?:
   a). Solo b). Con ayuda de otra persona(s)
2. ¿Existe Departamento de Tecnologías de Información? (SI / NO)
3. ¿Número de veces en las que ha participado en capacitaciones esté año? _____
4. ¿Qué tipo de topología es utilizada en la empresa?
   a). Eterneth b). Bus c). Anillo d). Anillo _ doble
   e). Estrella f). Otro: Especifique _____
5. ¿La empresa cuenta con alguna marca específica de equipo de cómputo?
   (Selección Única o Múltiple)
   a). Genéricos b). Aopen c). Compaq o HP
   d). Dell e). Everest f). Macintosh
   g). Otro: Especifique _____
6. ¿Cuentan con los siguientes sistemas operativos dentro de la institución?
   a). win95 b).win98 c). win2000 d). winXP
   e). 2000Server f). 2003Server g). Unix h). Linux
   i). Otro: Especifique _____
7. Equipo de comunicaciones dentro de la empresa
   a). Firewall b). Router c).Switch d). Hub
   e). Access_Point f). Otro: Especifique _____
8. El equipo de comunicaciones es:
   a). Comprado b). Alquilado c). Prestado d). Leasing
   e). Donado f). Todos g). Otro: Especifique _____
9. ¿Actualmente los usuarios tienen acceso irrestricto a la red? (SI / NO)
10. ¿Cuentan con políticas de seguridad en la red institucional? (SI / NO)
12. La implementación de políticas la realizo:
    a). personal de empresa b). Outsourcing
13. En cuanto a los requerimientos de los usuarios consideran las políticas de red:
    a). Rígidas b). Flexibles
14. Estas políticas han ayudado a:
    (Califique de 1 al 5, donde 1 es muy importante y 5 poco importante)
    a). _____ Permiten obtener un mayor control en la red
    b). _____ Ahorro de tiempo y recursos
    c). _____ Mayor productividad en los usuarios
    d). _____ Disminución de la carga de trabajo en red
    e). _____ Menos riesgos en el manejo de información
15. ¿En circunstancias en las que el equipo de comunicaciones falle o este en reparación, el Proveedor de servicios da opción de préstamo? (SI / NO)
16. Medios existentes para la transmisión de datos en la empresa
    a). Cable Coaxial b). Fibra Óptica c). UTP(cable par trenzado)
    d). Access_Point e). Otro: Especifique _____

17. ¿Cómo se realiza la actualización de software (Terminales, Servidores) en la empresa?
    a). Automáticamente b). Manualmente c). Ambos d). Ninguno
18. Los tiempo de caída o fuera de servicio de Internet son:
    a). Mínimos b). Cortos c). Largos
19. Cuál es el medio utilizado por la organización para accesar a Internet
    a). DLS (línea dedicada) b). ISA c). Proxy d). ASDL
    e). Otro: Especifique _____
20. ¿Tiene planes de contingencia en caso de que el acceso a Internet este caído?
    a). Si (Mencione) _____
    b). No
21. ¿Indique el ancho de banda disponible en la red? _____
22 ¿Qué tipo de herramientas utilizan para proteger la red de intrusos?
    a). Firewall b). DMZ c).honey Pots d). Contraseñas
    e). Todas f). Ninguna g). Otro: Especifique _____
23. ¿Han solicitado ampliar el ancho de banda al proveedor de servicios? (SI / NO)
24. ¿Cuál antivirus es utilizado en la institución?
    a). McAfee b). Norton_Antivirus (Symantec) d.) Panda
    e). Ninguno f). Otro: Especifique _____
25. Las actualizaciones del antivirus se realizan
    a). Automáticamente b). Manualmente c). Ambos d). Ninguno
26. ¿Está actualización se realiza?:
    a). En línea b). Día por medio c). Cada 3 días d). Cada 8 días
    e). Otro: Especifique _____
27. ¿ Realizan campañas de concientización de la seguridad en Internet a los usuarios finales (SI / NO)
28. ¿Qué riesgos se toman en consideración al conectarse a Internet?
    a). Intrusos(hacker, cracker, espias, vandalos) b). virus
    c). Otro: Especifique: _____
29. Mencione factores que nos pueden ayudar a contar con seguridad en la red
    _____
    _____
    _____
    _____
    _____
30. Comente posibles requerimientos para obtener seguridad en la red
    _____
    _____
    _____
    _____
    _____
31. Cite algunos beneficios de contar con una red óptima en cuanto a seguridad
    _____
    _____
    _____
    _____
    _____