UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

PLAN DE SEGURIDAD INFORMATICA EN EL MTC

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE :

INGENIERO ELECTRONICO

PRESENTADO POR :

VIRGINIA GENOVEVA ROMERO FUENTES

PROMOCIÓN
1977 - II

LIMA-PERU
2006

PLAN DE SEGURIDAD INFORMATICA EN EL MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Este trabajo lo dedico a mi hija

SUMARIO

Los riesgos a los que está sometida la información del Ministerio de Transportes y Comunicaciones (MTC) es permanente, los activos que se manipulan son importantes para el desempeño de las actividades que en ella se desarrollan. Los virus que proliferan en las redes conectadas a Internet y a través de los mensajes de correo electrónico, los hackers e intrusos que pudieran penetrar en el sistema informático del MTC podrían causar graves daños.

Este proyecto pretende implementar el sistema de seguridad Informática, para ello se propone las políticas de seguridad acordes con el análisis de riesgo tanto internos como externos, que puedan atentar contra la confidencialidad, la integridad y la disponibilidad de los recursos informáticos.

En el Capítulo I se plantea los conceptos básicos de seguridad de la información y un resumen de la Norma ISO/ IEC 17799:2002 y la norma técnica Peruana NTP-ISO/IEC 17799:2004- Tecnología de la Información. Código de buenas practicas para la gestión de la seguridad de la información" aprobada el 16 de Julio 2004 y que es de uso obligatorio para las entidades gubernamentales.

En el capitulo II se hace un diagnóstico de la red en sus aspectos físico y lógico.

En el capítulo III se analiza los diferentes sistemas con que se manejan la base de datos y describe las vulnerabilidades en cada uno de sus componentes.

En el capítulo IV se plantea un esquema de seguridad a corto, mediano y largo plazo.

En el Capítulo V se analiza las vulnerabilidades de la red de datos y se plantea la optimización de las herramientas de seguridad de la red LAN del Ministerio de Transportes y Comunicaciones – MTC.

Por último se define las conclusiones de ejecutar el plan de seguridad informática.

ÍNDICE

PROLOGO

La información es un recurso que, como el resto de los importantes activos, tiene valor para una organización y por consiguiente debe ser debidamente protegida. La seguridad de la información protege a ésta de una amplia gama de amenazas, con el objetivo de garantizar la continuidad del servicio, minimizar el daño al mismo.
La información puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

Los datos de los sistemas informáticos están en constante peligro por varias causas: errores de los usuarios, ataques intencionados ó fortuitos. Pueden producirse accidentes y ciertas personas con intención de atacar el sistema pueden obtener acceso al mismo e interrumpir los servicios, inutilizar los sistemas, alterar, suprimir o robar información.

Es de competencia de los administradores de seguridad el decidir el tiempo, dinero y esfuerzo que hay que invertir para desarrollar las directivas y controles de seguridad apropiados. El propósito de este trabajo es el de analizar las necesidades específicas y determinar los requisitos y limitaciones en cuanto a recursos. Si bien es cierto que cada sistema informático, entorno y directiva organizativa es distinta, lo que hace que cada servicio y estrategia de seguridad sean únicos, sin embargo, los fundamentos de una buena seguridad siguen siendo los mismos.

Aunque una determinada estrategia del plan de seguridad puede ahorrar mucho tiempo a la organización y proporcionar importantes recomendaciones de lo que se debe hacer, la seguridad no es una actividad puntual. Es una parte integrante del ciclo vital de los sistemas. En el presente trabajo se describen las actividades para una circunstancia en particular y requerirán actualizaciones periódicas, se realizarán cambios cuando las

configuraciones y otras condiciones y circunstancias cambien considerablemente. Este es un proceso iterativo, nunca termina y debe revisarse y probarse con periodicidad.

Se va a realizar un diagnóstico de las condiciones de seguridad en los niveles físico y lógico de la red, plantear o recomendar los cambios y de ser necesario proponer la adquisición de herramientas de seguridad, que permitan reducir los riesgos o las amenazas a los sistemas informáticos.

El propósito del presente trabajo es desarrollar un estudio completo del estado actual de la seguridad informática del MTC e intentar brindar las metodologías y estrategias a aplicarse concordante con los recursos de hardware y económicos que lo permita.

Este trabajo se pudo realizar gracias a la colaboración de los responsables de los diferentes sistemas, en la dirección de informática del MTC.

CAPITULO I
ASPECTOS GENERALES

1.1 Introducción

Mantener los sistemas informáticos a salvo se convierte en una necesidad básica para salvaguardar la información, que es un activo importante de cualquier empresa. La seguridad informática involucra la defensa en todos los niveles, desde la seguridad física hasta la recuperación de desastres.

Para llevar a cabo una adecuada política de seguridad informática se ha de tomar consciencia de los riesgos que implica tener los sistemas desprotegidos: pérdida de productividad, pérdidas y robo de información, pérdida de credibilidad, etc.

Si bien es cierto que en cada organización, la seguridad de la información, desde el punto de vista técnico, está en manos de sus directivos, también lo está en cada uno de los trabajadores, por lo tanto dependerá del grado de concientización que se tenga en este aspecto.

Los fundamentos de una buena seguridad siguen siendo los mismos, cualquiera que sea la organización o empresa que lo aplique, es por ello que en este capítulo se va a plantear un resumen de dichos principios.

1.2 Objetivo

Implementar el sistema de seguridad informática que permita asegurar la confidencialidad, la integridad y disponibilidad de los sistemas informáticos de modo tal que la información sea accesible solo a aquellos usuarios autorizados; garantizar la continuidad del servicio tratando de minimizar la vulnerabilidad de los sistemas a fin de proteger la red del MTC y sus recursos de ataques internos y externos.

Es por ello que se plantea previamente lo siguiente:

- Realizar un diagnóstico de la situación actual de la seguridad de la información del MTC.

- Determinar las vulnerabilidades de la infraestructura de la red de datos del MTC, evaluando el riesgo e impacto de su probable ocurrencia.
- Establecer procedimientos, políticas y mecanismos técnicos para atenuar o eliminar los riesgos.
- Analizar las herramientas de seguridad del MTC y proponer una solución de seguridad para la Infraestructura de la red de datos.
- Proteger y asegurar la red de datos y sus recursos de ataques internos y externos en el Ministerio de Transportes y Comunicaciones.
- Garantizar la continuidad del servicio minimizando la vulnerabilidad de los sistemas y/o de la información contenida en ella.
- Proponer políticas de seguridad informática interna basadas en Políticas y estándares sugeridos por la Norma Técnica Peruana.
- Proponer los términos de referencia para la adquisición de los recursos de seguridad informática.

1.3 Fundamento Teórico

1.3.1 Importancia de la Seguridad Informática

La seguridad puede entenderse como aquellas actividades y/o reglas técnicas, destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial. En este sentido, es la información el elemento principal a proteger, resguardar y recuperar dentro de las redes empresariales.

Seguridad Informática es también un estado de equilibrio con el entorno (conjunto de metodologías, documentos, programas y dispositivos físicos) que, para ser mantenido, requiere de la implantación de medidas auto - regulatorias continuas de protección, que respondan con acciones correctivas a las amenazas.

De este modo se logrará que los recursos de cómputo disponibles en un ambiente dado, sean accedidos única y exclusivamente por las personas autorizadas.
Consiste en establecer en que aspectos de la información requieren protección, para ello será necesario valorizar los datos de los sistemas informáticos.
La seguridad de la información se logra implementando un conjunto adecuado de controles, que abarca: políticas, prácticas, procedimientos, estructuras organizacionales y funciones del software. La seguridad informática es importante por la existencia de

personas ajenas a la información, también conocidas como piratas informáticos o hackers, que buscan tener acceso a la red empresarial para modificar, sustraer o borrar datos.
Ellos pueden, incluso, formar parte del personal administrativo o de sistemas, de cualquier compañía; de acuerdo con expertos en el tema, alrededor del 70 por ciento de las violaciones e intrusiones a los recursos informáticos se realiza por el personal interno, debido a que éste conoce los procesos, metodologías y tiene acceso a la información sensible de su empresa, es decir, a todos aquellos datos cuya pérdida puede afectar el buen funcionamiento de la organización.

Esta situación se presenta gracias a los esquemas ineficientes de seguridad con los que cuentan la mayoría de las empresas, y porque no existe conocimiento relacionado con la planeación de un esquema de seguridad eficiente, que proteja los recursos informáticos de las actuales amenazas combinadas.

1.3.2 Elementos de la Seguridad Informática

- Confidencialidad. El sistema contiene información que requiere protección contra la divulgación no autorizada. Por ejemplo, datos que se van a difundir en un momento determinado (como, información parcial de informes), información correspondiente al Despacho del Ministro y de Alta Dirección.

- Integridad. El sistema contiene información que debe protegerse de modificaciones no autorizadas, imprevistas o accidentales. Por ejemplo, información contable y sistemas de transacciones financieras, Resolución de Multas y Sanciones, Licencias de Conducir, Licencias de uso del espectro radioeléctrico.

- Disponibilidad. El sistema contiene información o proporciona servicios que deben estar disponibles puntualmente para satisfacer requisitos o evitar pérdidas importantes. Por ejemplo, sistemas esenciales de seguridad, Servicio de Correo electrónico por medio del cual se envía información voluminosa, sistemas de trámite documentario o licencias de conducir.

1.3.3 Amenazas al Sistema

Se entiende por amenaza una condición del entorno del sistema de información, persona, máquina, suceso o idea que, dada una oportunidad, podría dar lugar a que se produjese una

violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas, dependiendo del diseñador del sistema de seguridad especificar los servicios y mecanismos de seguridad necesarios.

Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como por ejemplo un fichero o una región de la memoria principal, a un destino, como por ejemplo otro fichero o un usuario.

Las amenazas afectan principalmente al Hardware, al Software y a los Datos.

Las cuatro categorías (ver fig. 1.1 y fig. 1.2) generales de amenazas o ataques son las siguientes:

a). Interrupción.- Un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad, su detección es inmediata.

Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros, borrado de programas y datos, fallos en el sistema operativo.

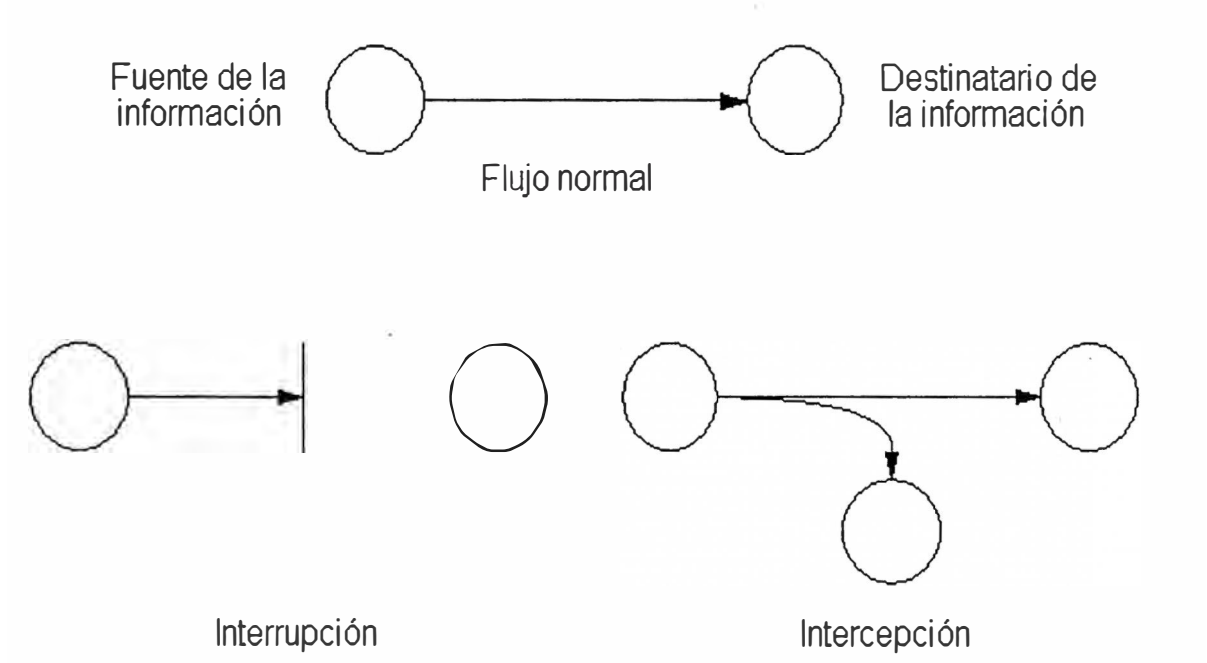


Fig.1.1 categorías de amenaza

b). Intercepción.- se entiende, como el acceso a la información por parte de personas no autorizadas, uso de privilegios no adquiridos, es un ataque contra la confidencialidad, el atacante no altera la comunicación, sino que únicamente la escucha o monitorea, para

obtener información que está siendo transmitida, son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos, no deja huellas.

Ejemplos de este ataque son: pinchar una línea para hacerse con datos que circulen por la red, escucha en línea de datos y la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

c). Modificación.- cuando una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad.

Ejemplos de este ataque son: el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

d). Fabricación.- cuando una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad, el delito es de falsificación. La detección es muy difícil.

Ejemplos de este ataque son: añadir transacciones en la red, la inserción de mensajes espurios en una red o añadir registros en base de datos.

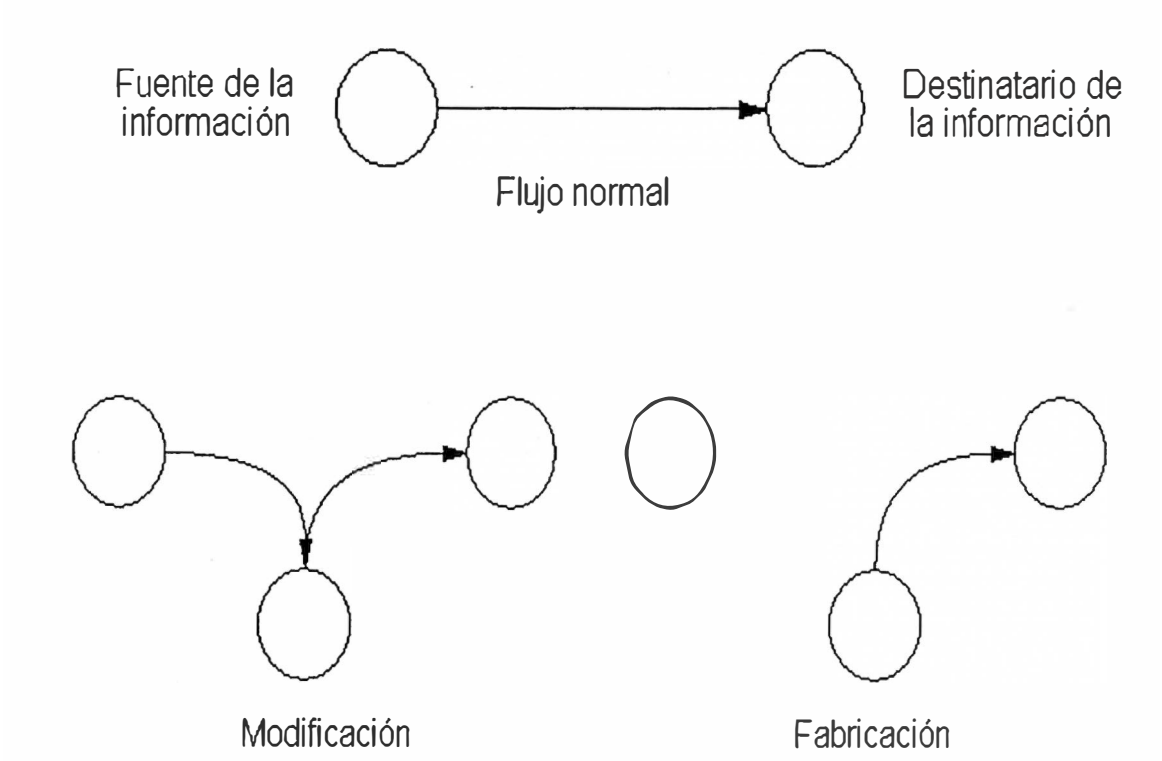


Fig.1.2 categorías de amenaza

1.3.4 Requerimientos de Seguridad

Es esencial identificar los requerimientos de seguridad, según la Norma ISO 17799, existen tres recursos principales para lograrlo.

El primer recurso consiste en evaluar los riesgos que enfrenta la organización. Mediante la evaluación de riesgos se identifican las amenazas a los activos, se evalúan las vulnerabilidades y probabilidades de ocurrencia, y se estima el impacto potencial.

El segundo recurso está constituido por los requisitos legales, normativos, reglamentarios y contractuales que deben cumplir la organización, sus socios comerciales, los contratistas y los prestadores de servicios.

El tercer recurso es el conjunto específico de principios, objetivos y requisitos para el procesamiento de la información, que ha desarrollado la organización para respaldar sus operaciones.

1.3.5 Tipos de Riesgo

Un riesgo es la probabilidad de que se materialice una amenaza, se clasifican en diferentes tipos:

a). Errores Humanos.- motivados por el desconocimiento ó por un simple descuido, son una de las principales causas de pérdida de información.

b). Fallos de los equipos.- afectan básicamente a la disponibilidad del sistema pudiendo provocar también una perdida de información.

c). Robo de la información contenida en el sistema o durante la transmisión. Puesto que el robo, normalmente, no supone la destrucción de la información original, el sistema no se vera afectada. Sus consecuencias serán de otro tipo: económicas, tácticas ó quizás una amenaza contra la intimidad de las personas.

d). Virus.- las consecuencias de que un virus entre en el sistema, con la posible destrucción de información y el invertir un tiempo para eliminarlo.

e). Sabotaje.- a un sistema informático, puede estar dirigido contra la información en forma de destrucción o manipulación, ó también tener como objetivo la destrucción de los equipos, por lo que puede afectar, tanto a la disponibilidad del sistema como a la integridad de la información contenida.

f). Fraude.- manipular la información con el fin de obtener un beneficio es lo que se conoce como fraude informático. Este tipo de fraude, frecuente hace unos años en entidades

financieras, es en la actualidad poco común por las avanzadas medidas de seguridad que se emplean. Sin embargo, en otros entornos donde no es factible establecer medidas tan sofisticadas, es un riesgo que debe tenerse en cuenta.

g). Desastres Naturales.- los desastres naturales como inundaciones, incendio, terremotos, etc. suelen tener consecuencias nefastas para los sistemas: daños en los equipos, pérdida de información y falta de disponibilidad. La ubicación y la geografía, son los factores que determinan el riesgo que se corre frente a cada desastre.

1.3.6 Valoración del Riesgo

Al evaluar un sistema se considera:

1. El valor intrínseco del producto a proteger.
2. Los costos derivados de su pérdida.
3. Costos ocultos inherentes a su pérdida.

Consiste en la determinación de lo que se necesita proteger y los niveles de protección a aplicarse y establecer el costo de implantar un sistema de Seguridad (análisis costo - beneficio).

Clasificar la instalación en términos de riesgo: alto, mediano, pequeño. Contar con sistemas duplicados (servidores, tarjetas de red, etc.)

Identificar las aplicaciones que tengan alto riesgo.

Formular medidas de seguridad.

1.3.7 Políticas de Seguridad Informática.

Tiene por objetivo definir las expectativas del MTC respecto al uso adecuado de los equipos de cómputo y de la red, así como definir los procedimientos para prevenir y responder a los incidentes de seguridad.

- Debe ajustarse a las políticas, normas, regulaciones y leyes existentes.
- Comprende la evaluación de las amenazas potenciales y los riesgos
- Comprende la prevención y detección de virus y programas maliciosos.
- Debe crearse un procedimiento de Auditoria que revise el uso de la red y servidores de forma periódica.
- Definición de responsabilidades generales y específicas en materia de gestión de la seguridad de la información.

1.3.8 Identificación de los Activos Organizativos

Consiste en la creación de una lista de todo lo que necesite protección, analizar las vulnerabilidades.
Hardware: ordenadores y equipos de Comunicación.
Software: programas fuente, utilitarios, Sistemas Operativos (Windows 95, 98, 2000, XP), programas de diagnóstico y de Comunicaciones.
Copias de seguridad, registros de auditoria, Base de datos.

1.3.9 Auditoria

Capacidad de determinar que acciones o procesos se han llevado a cabo en el sistema, quien y cuando las han llevado a cabo.
Se logra manteniendo un registro de las actividades del sistema y que esté protegido contra modificación. Para determinar si ha existido violación a la política de seguridad se analizan los eventos (logs), que vienen incluidos con el sistema operativo, ficheros de registro etc.

1.4 Norma ISO/IEC 17799

La Norma ISO 17799 tiene como objetivo proporcionar una base común para desarrollar normas de seguridad dentro de una organización.
En 1995 el British Standard Institute publica la norma BS 7799, un código de buenas prácticas para la gestión de la seguridad de la información.
En 1998, también el BSI publica la norma BS 7799-2, especificaciones para los sistemas de gestión de la seguridad de la información; se revisa en 2002.
Tras una revisión de ambas partes de BS 7799 (1999), la primera es adoptada como norma ISO en 2000 y denominada ISO/IEC 17799:
La norma ISO/IEC 17799 establece diez dominios de control que cubre la Gestión de la seguridad de la información y que se muestra en el gráfico de la fig. 1.3.

1. Política de seguridad.
2. Aspectos organizativos para la seguridad.
3. Clasificación y control de activos.
4. Seguridad ligada al personal.
5. Seguridad física y del entorno.

6. Gestión de comunicaciones y operaciones.
7. Control de accesos.
8. Desarrollo y mantenimiento de sistemas.
9. Gestión de continuidad del negocio.
10. Conformidad con la legislación.

Fig. 1.3 Dominios de Control

1) Políticas de seguridad.- tiene por objetivo dirigir y dar soporte a la gestión de la seguridad de la información, para ello:

- La alta dirección debe definir una política que refleje las líneas directrices de la organización en materia de seguridad, aprobarla y publicitarla de la forma adecuada a todo el personal implicado en la seguridad de la información.
- La política se constituye en la base de todo el sistema de seguridad de la información.
- La alta dirección debe apoyar visiblemente la seguridad de la información en la compañía.

2) Aspectos organizativos para la seguridad.- consiste en gestionar la seguridad de la información dentro de la organización, mantener la seguridad de los recursos de tratamiento de la información y de los activos de información de la organización que son

accedidos por terceros, así como mantener la seguridad de la información cuando la responsabilidad de su tratamiento se ha externalizado a otra organización.

3) Clasificación y control de activos.- Mantener una protección adecuada sobre los activos de la organización, asegurar un nivel de protección adecuado a los activos de información.

Debe definirse una clasificación de los activos relacionados con los sistemas de información, manteniendo un inventario actualizado que registre estos datos, y proporcionando a cada activo el nivel de protección adecuado a su criticidad en la organización.

4) Seguridad ligada al personal.- Las implicaciones del factor humano en la seguridad de la información son muy elevadas, todo el personal, tanto interno como externo a la organización, debe conocer tanto las líneas generales de la política de seguridad corporativa, como las implicaciones de su trabajo en el mantenimiento de la seguridad global.

Los procesos de notificación de incidencias deben ser claros, ágiles y conocidos por todos, con la finalidad de reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y los servicios.

Asegurar que los usuarios sean conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que estén preparados para sostener la política de seguridad de la organización en el curso normal de su trabajo.

Minimizar los daños provocados por incidencias de seguridad y por el mal funcionamiento, controlándolos y aprendiendo de ellos.

5) Seguridad física y del entorno.- Las áreas de trabajo de la organización y sus activos deben ser clasificadas y protegidas en función de su criticidad, siempre de una forma adecuada y frente a cualquier riesgo factible de índole físico (robo, inundación, incendio, etc.).

Evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización.

Evitar pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización.

Prevenir las exposiciones a riesgo o robos de información y de recursos de tratamiento de información.

6) Gestión de comunicaciones y operaciones.- Se debe garantizar la seguridad de las comunicaciones y de la operación de los sistemas críticos para el negocio, a fin de:

- Asegurar la operación correcta y segura de los recursos de tratamiento de información.
- Minimizar el riesgo de fallos en los sistemas.
- Proteger la integridad del software y de la información.
- Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación.
- Asegurar la salvaguarda de la información en las redes y la protección de su infraestructura.
- Evitar daños a los activos e interrupciones de actividades de la organización.
- Prevenir la pérdida, modificación o mal uso de la información intercambiada entre organizaciones.

7) Control de accesos.- se deben establecer los controles de acceso adecuados para proteger los sistemas de información críticos para el negocio, a diferentes niveles: sistema operativo, aplicaciones, redes, etc. Esto nos permitirá:

- Controlar los accesos a la información.
- Evitar accesos no autorizados a los sistemas de información.
- Evitar el acceso de usuarios no autorizados.
- Protección de los servicios en red.
- Evitar accesos no autorizados a ordenadores.
- Evitar el acceso no autorizado a la información contenida en los sistemas.
- Detectar actividades no autorizadas.
- Garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y teletrabajo.

8) Desarrollo y mantenimiento de sistemas.- debe contemplarse la seguridad de la información en todas las etapas del ciclo de vida del software en una organización, como la especificación de requisitos, desarrollo, explotación, mantenimiento con la finalidad de:

- Asegurar que la seguridad está incluida dentro de los sistemas de información.
- Evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones.

- Proteger la confidencialidad, autenticidad e integridad de la información.
- Asegurar que los proyectos de tecnología de la información y las actividades complementarias sean llevados a cabo de una forma segura.
- Mantener la seguridad del software y la información de la aplicación del sistema.

9) Gestión de continuidad del negocio.- Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente grandes fallos o desastres.
Todas las situaciones que puedan provocar la interrupción de las actividades del negocio deben ser prevenidas y contrarrestadas mediante los planes de contingencia adecuados.
Los planes de contingencia deben ser probados y revisados periódicamente.
Se deben definir equipos de recuperación ante contingencias, en los que se identifiquen claramente las funciones y responsabilidades de cada miembro en caso de desastre.

10) Conformidad con la legislación.- se debe identificar convenientemente la legislación aplicable a los sistemas de información corporativos, integrándola en el sistema de seguridad de la información de la compañía y garantizando su cumplimiento.
Se debe definir un plan de auditoria interna y ser ejecutado convenientemente, para garantizar la detección de desviaciones con respecto a la política de seguridad de la información.

CAPITULO II
DIAGNOSTICO DE LA RED

2.1 SEGURIDAD FÍSICA

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien se prevé, algunos de los aspectos tratados a continuación, otros como la detección de un atacante interno a la empresa, que intenta acceder físicamente a una sala de máquina de la misma, no se prevé. Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder de manera lógica a la misma.

La seguridad física consiste en la aplicación de controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicada la sala de máquina.
El objetivo es evitar accesos no autorizados, daños e interrupción del servicio, identificar los puntos vulnerables y medir el riesgo que éste representa.
La red física o recursos para el tratamiento de la información, está compuesto por los servidores, los equipos de comunicación, en el que esta incluido el cableado y los equipos de procesamiento automático de datos (PAD).

2.1.1 Respecto a los servidores.- los servidores se encuentran en una sala de máquina de un segundo piso, tiene instalado un falso piso sobre el piso real, con materiales incombustibles y resistentes al fuego. No está permitido fumar, no solo en este ambiente sino en todas las oficinas del Ministerio, por disposición de la Ley 25357.
Las oficinas y con mayor razón, la sala de máquina, están provistas de equipos para la extinción de incendios, se han instalado tres extintores manuales usando como sistema de protección contra incendios, el dióxido de carbono (CO2), que es la mas apropiada para

equipos de computo y cableado de energía; estos tanques son controlados permanentemente y se cambian cuando la vigencia esta por expirar. Existe un personal entrenado para usar estos extintores de fuego.

El acceso a la sala de máquina o cuarto de equipo es restringido (fig.2.1), solo pueden ingresar aquellos que están autorizados por el Director de Informática, esta relación se encuentra almacenada en un servidor conjuntamente con las huellas dactilares relacionados a una contraseña, el personal que solicita ingresar digita la contraseña y coloca su mano sobre el control de acceso biométrico, si ambos controles coinciden la puerta se abre.

Fig. 2.1 Puerta de acceso a la sala de servidores

El acceso al cuarto de equipo es restringido, solo están autorizados el personal de operaciones (operadores) y Director de Informática. Las visitas a esta área se realizan solo para propósitos específicos y es previamente autorizada y supervisada durante su permanencia.

La humedad relativa de esta sala es de 50%, cuenta con aire acondicionado que mantiene la sala a una temperatura entre 18 °C y 19 °C, que se encuentran dentro de los estándares de la TIA/EIA-569-A, estos parámetros son controlados mediante instrumentos de medición de humedad y temperatura (fig. 2.2). El TIA/EIA es un estándar para la Infraestructura de telecomunicaciones en edificios, reemplaza al estándar ANSI/TIA/EIA-606.

Fig. 2.2 Sala de Máquina: medidor de temperatura y humedad relativa.

Según el TIA/EIA-569-A el cuarto de equipo debe mantener una temperatura entre 18 °C y 24 °C con humedad relativa entre 30% y 55%.

La responsabilidad de la operatividad de los servidores y el control de las condiciones ambientales esta a cargo de cinco operadores quienes se turnan de modo tal, que cubren el servicio las 24 horas del día, cuentan con un cuaderno de bitácora en donde anotan las incidencias presentadas en cada turno, y un libro para el control de accesos

Asimismo en el primer piso, exactamente debajo del cuarto de equipos, se encuentra la cocina de la cafetería y el depósito de los balones de gas; aún no ha habido ningún incidente, pero esta considerado como de alto riesgo y es una amenaza permanente contra la seguridad física de la red. A fin de minimizar este riesgo se realicen simulacros de incendio una vez al año.

2.1.2 Respecto a los equipos de Comunicación.- los equipos de comunicación como los Switch y Router se encuentran ubicados en el cuarto de equipo ó sala de maquina, en gabinetes con puerta y asegurados con llave, en ambientes denominados cuarto de comunicaciones. Estos gabinetes (Fig. 2.3), cuentan con sistema de ventilación en la parte posterior y se localizan al costado del ascensor de cada uno de los cuatro pisos.

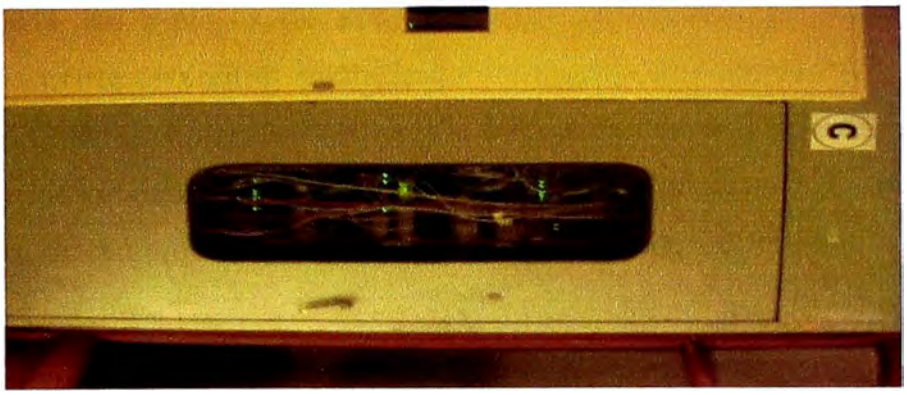


Fig. 2.3 Panel de Conexión de Switch protegidos por gabinetes.

2.1.3 Respecto al cableado.- en los gabinetes que se encuentran en los cuartos de telecomunicaciones, los cables de conexión cruzada conocido también como "patch cord", usados para conectar dos patch panel están sueltos y desordenados como se ve en la figura 2.4, por lo que se ha recomendado su reordenamiento.

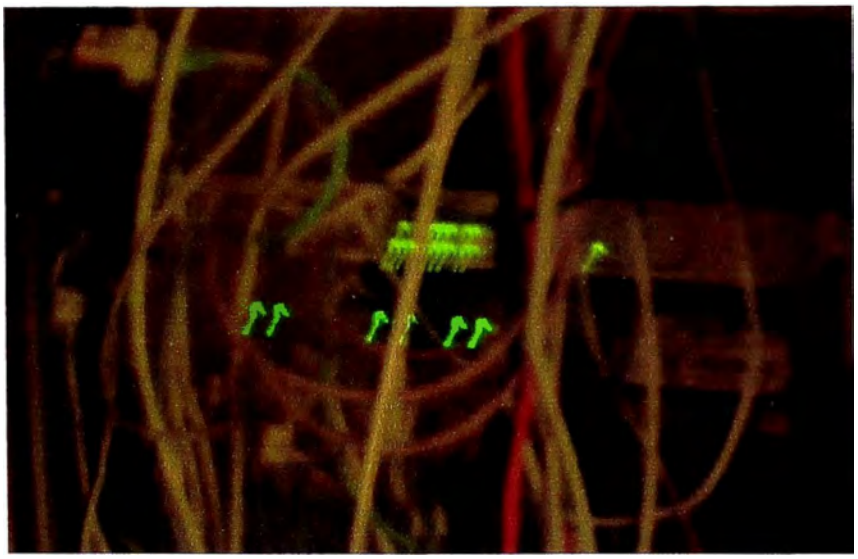


Fig. 2.4 Cableado en el gabinete

Asimismo en el cuarto de equipo o sala de máquina el cableado de red y el cableado de energía eléctrica estabilizada, pasan por un mismo ducto, éstos están ubicados debajo del falso piso, pudiendo estar expuesto a interferencias. La red cableada esta protegida mediante conductos blindados. Existe redundancia en el cableado que interconecta la sala de servidores con los IDF ubicados en los cuatro (04) pisos: un cableado es de fibra óptica y otro cableado es UTP CAT V los cuales están tendidos paralelamente.

El cableado desde el IDF hasta las computadoras es UTP CAT V, el 90 % el ducto es empotrado y el 10 % es adosado.

2.1.4 Respecto a los equipos de procesamiento automático de datos (PAD).- Se constató que no existe un control centralizado del ingreso de equipos PAD, debido a que cada Dirección General contaba con su propia oficina de compras y Area de informática. Con la política de modernización, las oficinas de compra pasaron a formar parte de la Oficina General de Administración (OGA) y la Dirección de Informática tomó el control de los activos.

Inventario físico manual.- el inventario de los recursos informáticos permite asegurar una protección adecuada de estos activos, porque identifica el propietario y la responsabilidad de la integridad del recurso.

En el MTC, el inventario se realiza una vez por año, para ello se utilizan formatos de recopilación de información, el inventario actualizado permite garantizar la vigencia de una protección eficaz de los recursos y además de identificar al propietario se obtiene la ubicación del equipo.

Tabla 2.1 Resumen de inventario físico de equipos PAD

TIPO I		TIPO II		TIPO III	
EQUIPO	**CANTIDAD**	**EQUIPO**	**CANT.**	**EQUIPO**	**CANTIDAD**
Computadora	**1650**	Servidor MTC4 Plataforma ALPHA	**01**	Impresora(Server)-Printronix	**11**
Servidor INTEL	**35**	Servidor - Plataforma ALPHA	**01**	********	******
Notebook	**55**	Impresora (Server) Digital	**02**		
Impresora láser	**285**	DecServer	**03**		
Impresora Inyección	**184**	*********	****		
Impresora Matricial	**224**				
Plotter	**12**				
Scanner	**57**				
Estabilizador	**59**				
Ups	**22**				
Switch	**66**				
Router	**05**				
Hub	**59**				

En la tabla Nº 2.1 se muestra el cuadro resumen del parque informático del 2005 del Ministerio de Transportes y Comunicaciones obtenida por la Dirección de Informática.

El parque informático se clasificó en tres tipos dependiendo de la plataforma y tecnología usada.

Inventario físico mediante software.- con la finalidad de tomar conocimiento de cambios no autorizados de partes y piezas, se ha instalado un software de inventario que permite de forma automatizada conocer el hardware y software instalado en cada CPU. En la fig. 2.5 se muestra el resultado del inventario, se observa detalles de las partes y piezas mas importantes de la CPU como son: tipo de procesador, capacidad de memoria, velocidad, capacidad del disco duro, características de las tarjetas de video, sonido y red, etc. Se ha previsto tambien el uso mediante disquetes, para aquellos equipos que no se encuentran conectados a la red del MTC.

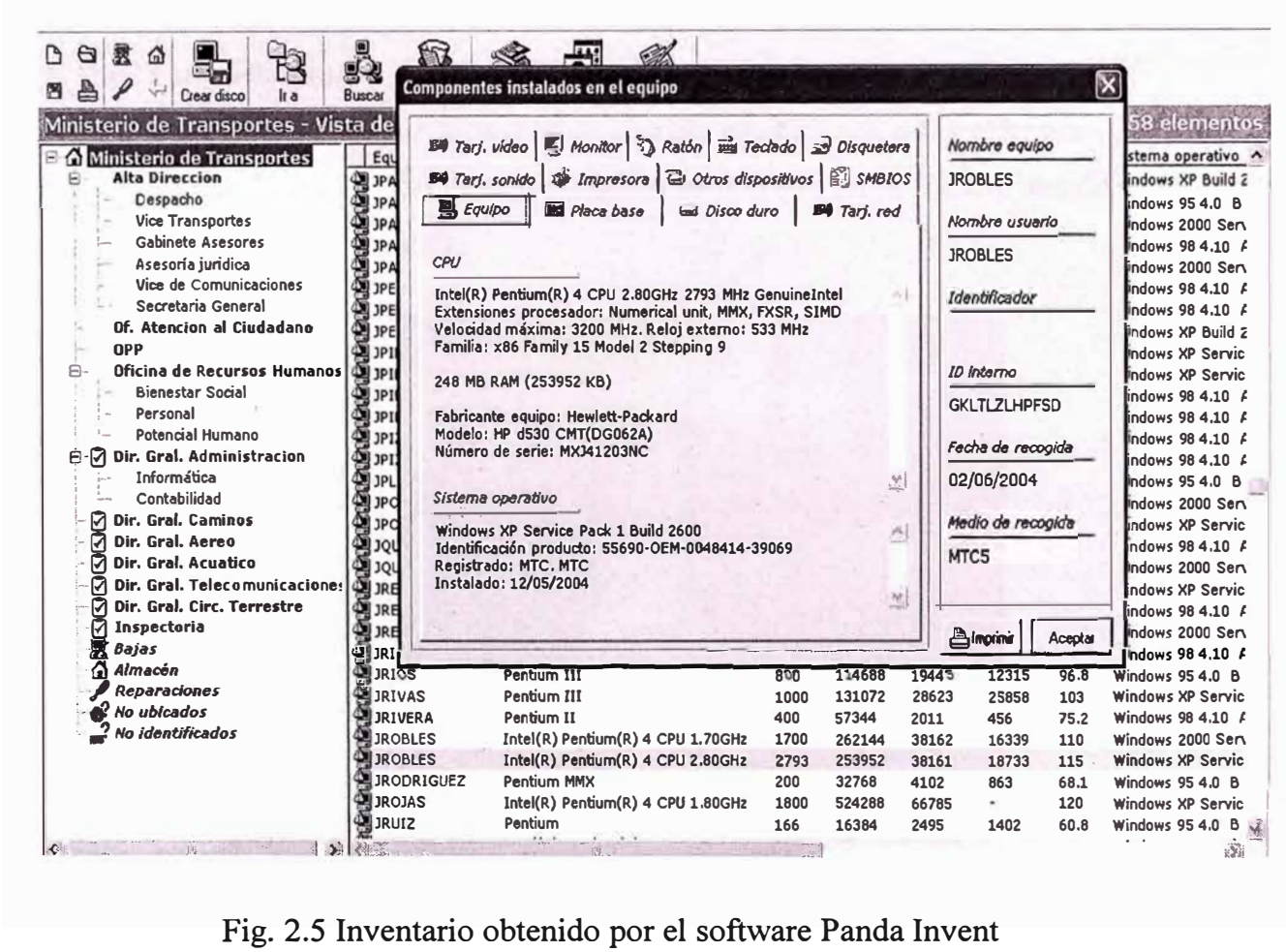


Fig. 2.5 Inventario obtenido por el software Panda Invent

Del Mantenimiento de equipos.- a fin de garantizar la continuidad en el servicio, los equipos de procesamiento automático de datos deben mantenerse en forma adecuada, es por esta razón que se ha considerado contar con el servicio de soporte técnico, que en este caso lo brinda empresas especializadas.

2.1.4 Respecto a los equipos de energía.- Se ha constatado que los equipos del MTC, se alimentan de dos tipos de energía.

La energía eléctrica proveniente de las empresas eléctricas ingresa al edificio por dos tableros de distribución:

a). La energía proveniente de un tablero alimenta el alumbrado eléctrico de las oficinas y exteriores así como las tomas de corriente de equipos como ventiladores, fax, y todo equipamiento que usan motores, existen tablero de distribución en cada piso.

b). La energía proveniente de un segundo tablero es convertida en energía estabilizada y alimenta a los equipos informáticos. Los equipos clasificados como críticos, servidores, equipos de comunicación, equipos de la alta dirección, están conectados previamente a los UPS. Existe un sensor con un panel digital que muestra el numero de piso en donde ocurre el corte de la energía estabilizada, al mismo tiempo emite una alarma, éste esta ubicado al exterior del cuarto de equipo,

Las llaves termomagnéticas que alimenta de energía estabilizada a los diferentes pisos del MTC se encuentran en el cuarto de equipo como se muestra en la fig.2.6, siendo esto una amenaza contra la seguridad física.

Fig. 2.6 Llaves termomagnéticas de la energía estabilizada.

2.2 SEGURIDAD LOGICA

La seguridad lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita su acceso, a las personas autorizadas para hacerlo.

El activo más importante en esta organización es la información, por lo que debe usarse técnicas que permita asegurarla, además de la seguridad física.
La seguridad informática se basa, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autentificación y autorización de accesos.

2.2.1 Política de control de acceso interno.- mediante la construcción de contraseñas en diversos niveles del sistema, donde permita solo el acceso en base a niveles de seguridad de usuarios con permiso

a). Administración de contraseñas.- Las contraseñas constituyen la primera y tal vez única manera de autenticación y, por tanto, la única línea de defensa contra ataques. Éstas establecen quién asignará la contraseña, qué longitud debe tener, a qué formato deberá apegarse, cómo será comunicada, etc.
Se han establecido las siguientes políticas:
En usuarios.-

- La longitud de una contraseña es verificada de manera automática al ser construida por el usuario.
- Todas las contraseñas deberán contar con al menos 06 caracteres.
- Está prohibido que los usuarios construyan contraseñas compuestas de algunos caracteres constantes y otros que cambien de manera predecible y sean fáciles de adivinar como la fecha de cumpleaños, nombre de los hijos, etc.
- Los usuarios no deben dejar sus contraseñas en lugar visible.
- La habilitación de la contraseña en el BIOS permite controlar el inicio del sistema, solo se realiza en caso de manejo de información delicada.

En servidores.- en el cuarto de equipo o sala de máquina se encuentran también los servidores de las Direcciones de Aviación Civil (DGAC) y la Dirección General de Circulación Terrestre (DGCT).
La contraseña de acceso a los servidores de la DGAC es de conocimiento de los operadores de la Dirección de Informática.
La contraseña de acceso a los servidores de la DGCT es de conocimiento únicamente del personal de sistemas de esta dirección, el ingreso a la sala de máquina del personal de sistemas se efectúa bajo la supervisión del operador de turno.

b). Administración de cuentas.- se manejan cuentas individuales de acceso, teniendo como estándar para asignar los nombres de cuenta, el siguiente patrón:

Vromero apellido paterno

Primer caracter del nombre

- Existe un procedimiento de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios.
- La identificación de usuarios se ha definido de acuerdo a una norma homogénea para toda la organización.
- No se realizan revisiones periódicas sobre la administración de cuentas y los permisos de acceso establecidos.

Del procedimiento de creación de cuentas de usuario para correo electrónico e Internet.- el responsable o Jefe del área solicitante envía su requerimiento mediante un mensaje por correo electrónico, al Director de Informática, especificando además las limitaciones en el uso y acceso por el usuario, a determinadas páginas de Internet.
Este procedimiento permite restringir los accesos a pagınas o URL de mediano y alto riesgo además de considerase como no productivas.

2.2.2 Políticas de Control de acceso externo.- Especifican cómo evitar que los intrusos como los Hacker, Craker accedan desde el exterior a nuestro sistema, Un sistema básico de seguridad, que debemos utilizar para la conexión a Internet, es la instalación de un Firewall o cortafuegos, opcionalmente el IDS (sistema de detección de intrusos), IPS (sistema de prevención de intrusos).

Sistema de Detección de Intrusos.- es un componente adicional en el modelo de seguridad, consiste en detectar actividades inapropiadas, incorrectas o anómalas desde el exterior o interior de una red de datos. Su función principal consiste en:

- Inspeccionar el tráfico de la red buscando posibles ataques
- Controlar el registro de los servidores para detectar acciones sospechosas.
- Mantener una base de datos con el estado de cada uno de los archivos del sistema para detectar la modificación de los mismos.

- Controla el ingreso de cada nuevo archivo al sistema para detectar caballos de Troya.
- Enviar reportes al administrador de red de cualquiera de las acciones

Firewall.- es un dispositivo de hardware y software que actúa como una barrera protectora, separando la red interna, de Internet, haciendo la red segura e invisible a usuarios de Internet, protegiéndonos de ataques externos, este sistema crea tres zonas diferenciadas, uno de ellos donde se pondrán los servicios públicos como Web y Correo Electrónico, otro el lado público Internet, y uno tercero que es la red interna o zona segura. Este tráfico entre la Red interna y la red de Internet es autorizado o denegado por el firewall (la "barrera"), siguiendo las instrucciones de configuración.

Estos sistemas permiten controlar que recursos de la red privada pueden ser accedidos desde el mundo exterior y cuales de afuera pueden ser accedidos por los usuarios internos. Todo tráfico de red será verificado y luego aceptado o rechazado sobre la base de una serie de condiciones, las mismas pueden basarse en dirección de origen y destino, servicio requerido, puertos, etc.

En la red LAN se ha instalado un Firewall (software) del fabricante Raptor V 6.5.0 funcionando sobre una plataforma Windows NT 4.0 SP 6a.
Este programa se ha instalado en una computadora PIII de 328Mb. de memoria Ram, 9Gb. de capacidad de disco duro y 3 tarjetas de red, fast ethernet 3COM Etherlink 10/100 PCI NIC 3C905B-TX, para sus tres niveles de interfaces de red (adaptadores virtuales): DMZ para la red segura, Interna y otra externa hacia Internet.
El esquema de seguridad planteado por el firewall para prevenir ataques desde Internet, segmenta la red LAN del MTC en tres componentes principales, de acuerdo al tipo de función que va a realizar.

Red Externa.- Segmento de salida a la red publica Internet con direcciones TCP/IP clase C públicas, asignadas por el proveedor de este servicio, Telefónica del Perú.
Red Segura.- Segmento en donde están ubicados los servidores, como se muestra en la figura 2.7, que van a ser accesados por usuarios anónimos desde Internet, servidor WEB, etc. Usa una red TCP/IP clase C con direcciones privadas.
Red Interna.- Propiamente la red Lan – Wan del MTC, servidores de aplicación, estaciones de trabajo, etc., sé están usando direcciones TCP/IP clase B privadas subneteada por cada dependencia local y una clase C para las remotas.

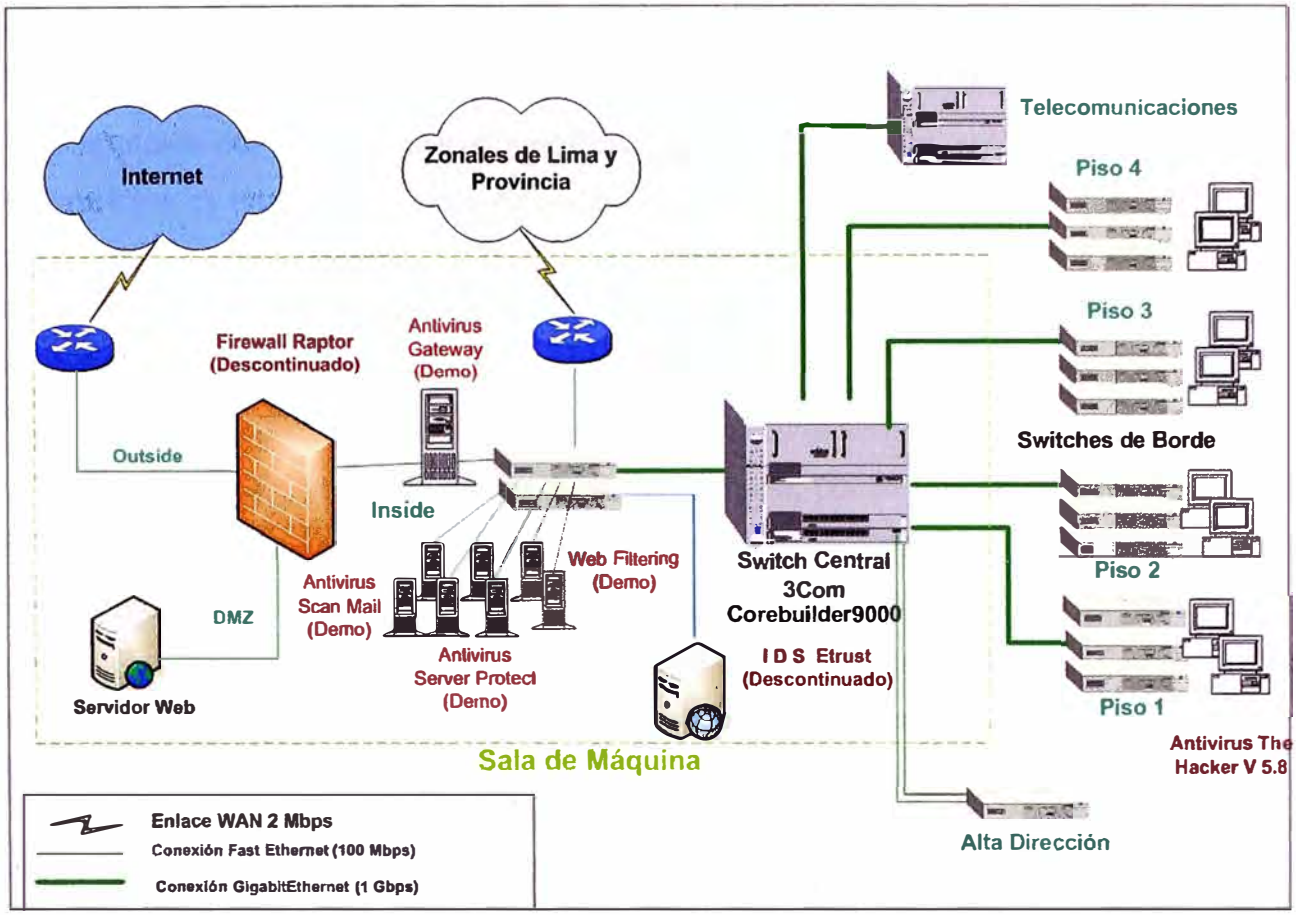


Fig. 2.7 Diagrama de acceso a Internet

2.2.3 Políticas de seguridad de la información.- Define políticas de protección contra los Virus, gusanos (worm) y caballos de troya; que ingresan a nuestra red a través del Correo Electrónico e Internet; instalando un antivirus legal y actualizado en las computadoras de los usuarios y en los servidores.

La política de seguridad debe especificar: las tareas a realizar, sus responsables, cómo se definen los niveles de acceso, cómo se auditan los planes operativos, cómo se realizará el seguimiento, dónde deben ponerse en marcha medidas específicas (firewall o cortafuegos, filtros, control de acceso, antivirus corporativos, entre otros), el plan de capacitación del personal de la organización.

La política de seguridad debe contemplar también, mecanismos que garanticen la seguridad en una organización.

Como consecuencia de ello, no existen políticas aisladas, sino políticas que integran planes y programas de seguridad para toda la institución, incluyendo a la seguridad

informática, éstos son: la administración de contraseñas de acceso, la gestión de criptografía o cifrado de mensajes, la administración de copias de seguridad.

La instalación de un sistema de programas antivirus y procedimientos es la medida más empleada por las empresas para protegerse de ataques virales.

El antivirus es una gran base de datos con la huella digital de todos los virus conocidos para identificarlos y también con las pautas que mas contienen los virus. Los fabricantes de antivirus avanzan tecnológicamente casi en la misma medida que lo hacen los creadores de virus.

En el Ministerio de Transportes la incidencia de virus provenientes de Internet, antes del 2005 fue tremenda, ya que no se le daba importancia, por lo que el servidor de Correo, sufrió el ataque de virus como: Melisa, I Love You, W32/Blaster, W32/Sober.P@mm, W32/MyDoom, Win32/Bagle, W32/Mytob, W32.Netsky, W32/Korgo, W32/BugBear, etc.

El antivirus instalado en una consola en calidad de evaluación, realizó un barrido en los servidores obteniéndose reportes de virus provenientes de Internet que intentaban ingresar la red LAN.

En la figura 2.8 se observa el cuadro de número de tipos de virus por día.

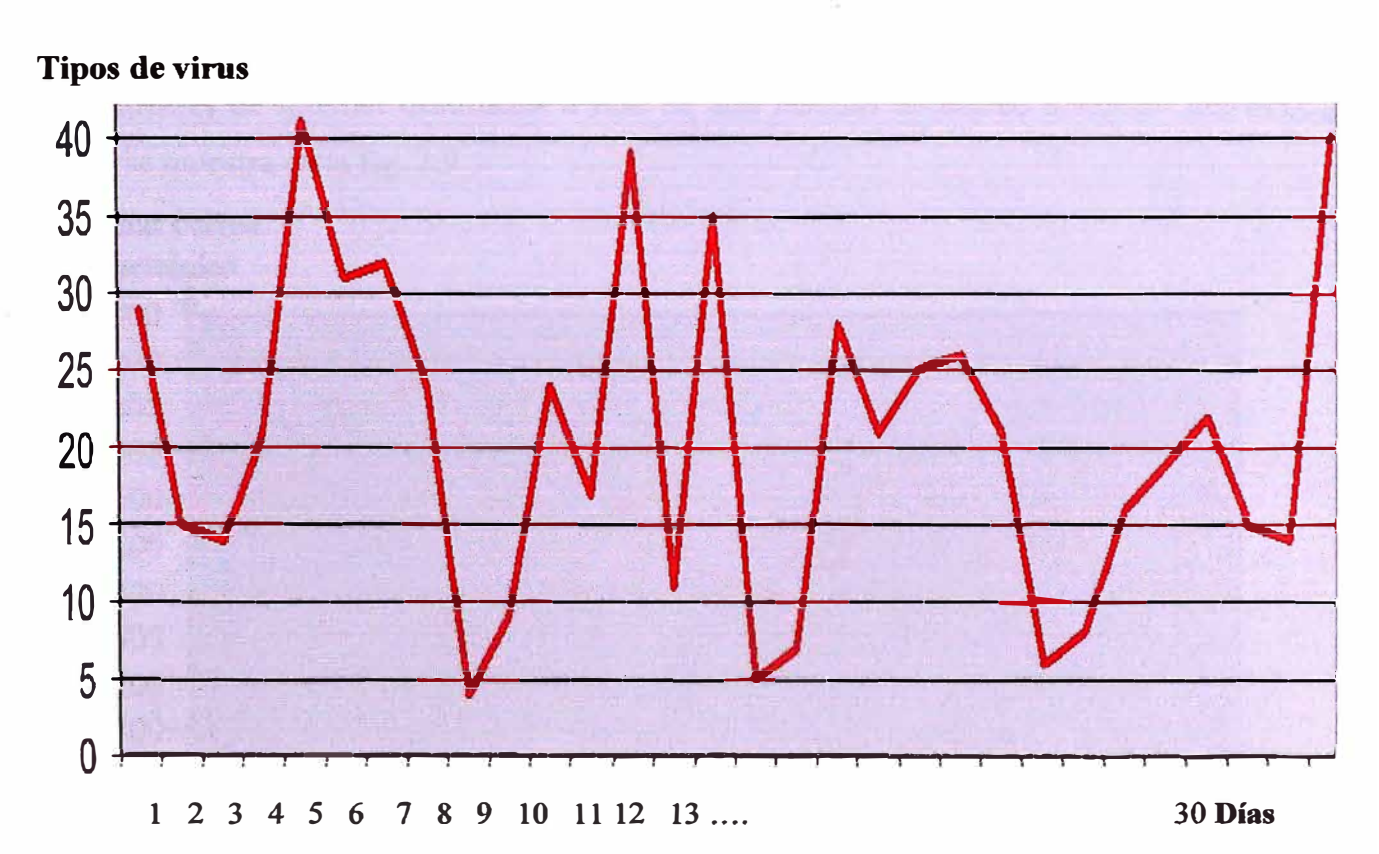


Fig. 2.8 Virus provenientes de Internet

Al cabo de un mes se obtuvo el siguiente resultado: se detectaron 586 virus pertenecientes a 18 tipos de virus, estos virus han sido detenidos en el perímetro antes de llegar al servidor de Correo Electrónico del MTC y a las computadoras de los usuarios finales, los correos con virus venían destinados a más de 600 cuentas válidas, de mensajes diferentes, que ingresarían al MTC.

Programas espías.- Es necesario proponer políticas de protección contra la instalación de programas denominados "espías", que pueden ser internas ó externas, por ejemplo el Gator, Precision Time, Hot Bar, que se instalan automáticamente, al instalarse los programas que ofrecen como calendarios, barras con figuritas y sonrisas (smile).

El Gator se instala automáticamente en los equipos de los usuarios como parte de alguna aplicación que es obtenida por el usuario desde Internet, se encarga de espiar la actividad de los usuarios, modifica las páginas Web que se muestran en los ordenadores donde se encuentra instalado, cambiando los banners de publicidad por propios, ingresa con los programas: Precision Time, Date Manager

Mensajes de correo electrónicos no deseados.- la incidencia de mensajes no deseados del correo electrónico del MTC, denominado también mensajes "Spam" es alta, en una prueba realizada durante treinta días se detectaron alrededor de 14,456 mensajes no deseados provenientes de Internet destinados a más de 800 cuentas de correo distintas del MTC, como se muestra en la fig. 2.9

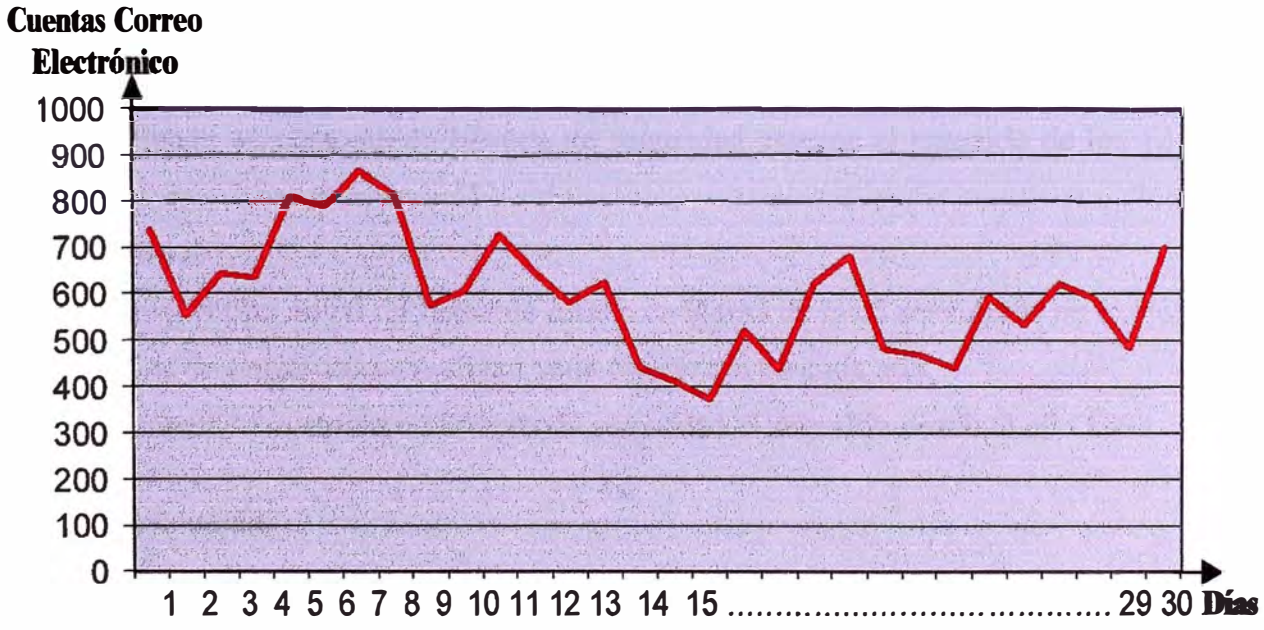


Fig. 2.9 Correo tipo spam proveniente de Internet

2.2.4 Política de resguardo de la Información

Se realizan copias de seguridad periódicas de la base de datos almacenada en los servidores.

Se han establecido procedimientos para llevar a cabo la estrategia de resguardo, realizando copias de respaldo de los datos, registrando eventos, fallas y asegurando la operatividad del equipo.

A fin de garantizar la integridad de la información que se maneja en los diferentes servidores de aplicación, se ha establecido la siguiente política de Copias de Seguridad:

Respaldo diario:

- Realizar en forma diaria, un respaldo total a cada uno de los 5 servidores en explotación, para ello se cuenta con un juego de cintas para cada servidor.
- Las copias de seguridad se inicia a las 24:00 horas de acuerdo al procedimiento establecido para este caso.
- Se mantendrá en custodia, en la bóveda de seguridad ubicada fuera del MTC, un primer juego de lo obtenido la semana anterior, mientras se respalda la semana en curso, es decir se cuenta con 13 días de respaldo diario
- Las cintas de backup diarios se rotan cada 13 días.

Respaldo mensual

- Realizar en forma mensual, un respaldo total a cada uno de los 5 servidores en explotación
- Las copias de seguridad se realizan cada ultimo día de cada mes
- Se mantienen en custodia en bóveda de seguridad externa el respaldo de los 12 meses del año.

Respaldo anual

- Realizar en forma anual un respaldo total a cada uno de los 5 servidores en explotación.
- Las copias de seguridad se realizan cada último día de cada año.
- Se mantienen en custodia en bóveda de seguridad el respaldo desde el año 1994.

2.2.5 De las licencias

a). Servicios de Correos Electrónico e Internet

El Servidor de Correo, cuenta con infinitas licencias del software de Exchange 5.5, y cuenta con licencias para su sistema operativo Windows NT4.0, los que proporcionan un

servicio deficiente, por que este sistema operativo está desactualizado, por lo que se ha recomendado el cambio de servidor y sistema operativo.

Actualmente el Servidor de correo se encuentra en estado crítico, tanto por espacio en el disco duro (70Gb), como en su funcionamiento. No hay espacio en el disco, debido a que la cantidad de usuarios creados supero las proyecciones del año pasado además la base de datos existente en el servidor de correo es inconsistente con la cantidad de usuarios que laboran en el MTC, es decir hay cuentas que ya no existen y no se han depurado por el desconocimiento de altas y bajas del personal.

La concurrencia de conexiones al servidor se realiza deficientemente, el servicio es cortado frecuentemente, pues el servidor de correo se satura y deja de funcionar.

Se ha recomendado la actualización permanente de la base de datos de usuarios en el servidor de correo electrónico, asimismo se ha efectuado el requerimiento de la adquisición de servidores de tecnología de punta.

b). De Sistema Operativo

Con la finalidad de contar con programas para el sistema operativo y aplicaciones como son los procesadores de texto y tablas, se ha previsto la adquisición de computadoras que incluyen el sistema operativo con licencias de 3 años.

En este capítulo se ha detallado las herramientas de seguridad lógica y las políticas de seguridad que se ejecutan en la red de datos del Ministerio de Transportes y Comunicaciones.

CAPITULO III
DIAGNOSTICO DEL DESARROLLO Y MANTENIMIENTO DE SISTEMAS

3.1 Introducción.- Los requerimientos de seguridad deben ser identificados y aprobados antes del desarrollo o mejora de los sistemas de información, el marco para analizar los requerimientos de seguridad e identificar los controles que los satisfagan son la evaluación y la administración de riesgo. Los controles introducidos en la etapa de diseño son mas baratos de implementar y mantener que aquellos que se incluyen durante o después de la implementación.

El objetivo de la implementación de los controles apropiados y pistas de auditoria o registros de actividad es el de prevenir la pérdida, modificación o uso inadecuado de los datos del usuario en los sistemas de aplicación.

3.2 Seguridad Física.- Con la finalidad de asegurar la base de datos, el área de desarrollo esta separada físicamente del área de Producción. Los servidores que manejan la base de datos de producción se encuentran ubicados en el cuarto de máquina con las seguridades anteriormente descritas, el área de Desarrollo donde se encuentran instalados físicamente los equipos de los programadores están ubicados en otra oficina, los programadores no tienen autorización de acceso al cuarto de equipo, sin embargo para efectos de prueba de los sistemas que los programadores están desarrollando o mejorando cuentan con un servidor de prueba con idénticas condiciones que el servidor de producción.

3.3. Sistemas desarrollados por personal del MTC.- En los diferentes programas que están a cargo de un personal selecto de la Dirección de Informática, se ha comprobado los niveles de seguridad y el registro de auditoria.

3.3.1 Sistemas de Licencias de Conducir.- consta del sistema de producción de licencias de conducir y la base de datos llamado LIRA.

a). El Sistema de Producción de Licencias de Conducir.- consta de dos módulos: sistema de Impresión de licencias de conducir que incluye la impresión de la imagen del rostro, imagen de la firma y la huella digital.

Acceso: solo pueden ingresar al sistema los operadores de la sedes de Antenor Orrego, Lince y Conchan autenticándose en el Dominio del servidor DTP

Interfase de integración de la Emisión de Licencias de Conducir
Esta aplicación fue concebida para integrar las zonales (fig. 3.1) de producción de Licencias de Conducir, y mantenerlas en línea con la finalidad de controlarlas y verificarlas.
Alcance: Las tres zonales de producción, la sede central del MTC y los departamentos: Arequipa, La Libertad, Tacna, San Martín, Huancavelica.
Acceso: Mediante autenticación de Intranet y lista de usuarios de Control de Conductores.

b). Base de datos: Lira

Sistema de Registro de Licencias de Conducir, donde se mantiene información de todas las licencias emitidas por el MTC; este sistema fue la base para soportar los otros sistemas.

- Sistema Operativo de Servidor: OPEN VMS
- Plataforma de base de datos: VMS COBOL
- Plataforma de interfase de usuario: OPEN VMS – VMS COBOL
  Acceso: Mediante TELNET
  Alcance: 14 departamentos
  Modalidad: Consulta y modificación

Niveles de seguridad.- Estos sistemas cuentan con varios niveles de seguridad:

1. Seguridad mediante Sistemas Operativos

El mantenimiento final se encuentra a cargo del administrador de usuarios del dominio de la entidad denominado también MTC.
Los sistemas con interfase Windows, requieren que el usuario esté autenticado primero en el dominio MTC.
En el dominio MTC se han creado perfiles o grupos de acceso para diversos tipos de usuarios:

- Usuarios de Producción: Producción LC
- Usuarios de Consulta de datos e Imágenes: Imágenes LC
- Usuarios de Consulta de datos: Licencias
  Los usuarios que producen la Licencia de Conducir requieren estar autenticados al dominio MIDIS.
- Los usuarios del sistema LIRA ingresan con autenticación de TELNET del OPEN VMS.

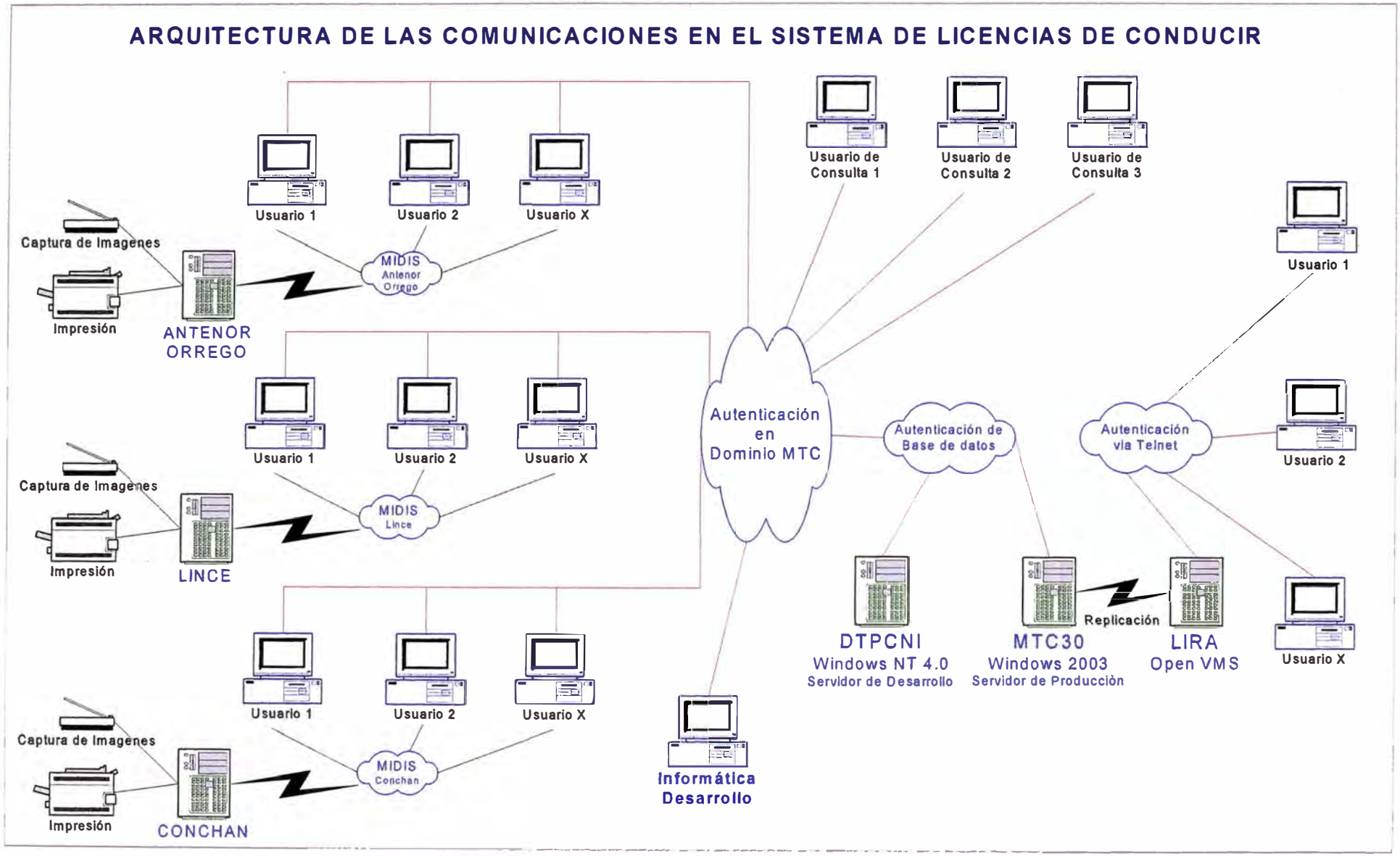


Fig.3.1 Arquitectura de comunicación del Sistema de Licencia de Conducir.

2. Seguridad de Segmentación de redes:

- Existe seguridad por el hecho que cada dominio (MIDIS) trabaja en forma independiente y excluyente, su administración es local a cargo de los administradores locales.
- El dominio MIDIS sirve únicamente como medio de producción, la configuración del respectivo acceso es por PC, debido a esta configuración es imposible que un operador o usuario fuera de este dominio realice la producción del documento (aunque tuviese el permiso de producción).

3. Seguridad mediante base de datos:

Todos los usuarios de la aplicación de Control de Conductores tienen autenticación de base de datos, el cuál contiene los siguientes perfiles de acceso:

- Consulta: Consulta de Licencias de Conducir,
- Producción Ventanilla : Impresión de Licencias de Conducir,
- Expedición batch de Licencias: Expedición de licencias en grandes bloques,
- Listado de Producción : Permite visualizar la producción diaria a los jefes zonales,
- Auditoria de Producción: Permite visualizar además de la producción a los operadores y zonales que han intervenido emisión del documento.

La administración se encuentra a cargo de la DGCT.

4. Seguridad en el módulo de seguridad de Control de Conductores

El módulo de seguridad consta de:

- Administrador de usuarios y perfiles: bajo la responsabilidad del administrador.
- Administración personal de contraseña: a cargo del propio usuario

3.3.2 Sistema de Concesión de Rutas de Transporte

Sistema Cliente/Servidor de uso exclusivo en la sede central del MTC por la Dirección General de Circulación Terrestre (DGCT).

Servidor de Desarrollo: MTC30

Servidor de Producción: DTP

En la tabla 3.1 se muestra un resumen del procedimiento para solicitar la instalación de los programas en la Dirección de Circulación Terrestre, así como los roles o función que se asignará al usuario que requiere acceder al programa.

Tabla 3.1 Resumen de autorización de instalaciones

	Solicitantes	**Tienen Instaladores**	**Autorización de Instalación**	**Perfiles de los usuarios**
Interfase Control de Conductores	Personal de la DGCT	El Coordinador autorizado por el Director de la DGCT cuenta con copia del instalador	Dirección de Circulación Vial mediante su director Luis Ortiz	Consulta Producción Expedición batch de Licencias Listado de Producción Producción Ventanilla Auditoria de Producción
Concesión de Rutas de Transporte	Personal de la DGCT	El Coordinador autorizado por el Director de la DGCT cuenta con copia del instalador	Direccion de Registros y Autorizaciones mediante su director Jesus Tapia	Consulta Registro de Empresas, Registro de Pólizas, Registro de Flota Empresa, Registro de Rutas, Registro de Conductores, Registro de Certificado de Operatividad, Registro de Exámenes Psicosomáticos.

Procedimiento para la creación de cuenta

Mediante correo electrónico o memorandum el Director de la DGCT solicita al Director de la Dirección de Informática la creación de un nuevo usuario en el Dominio MTC.

Seguidamente se le crea una cuenta para el uso del sistema respectivo, esta administración es compartida entre la Dirección de Informática y la Dirección de Circulación Terrestre quien se responsabiliza conjuntamente con el usuario por el uso de la cuenta asignada.

La eliminación de cuentas se procesa de igual forma, esto ocurre cuando el trabajador cesó en sus funciones o dejo de pertenecer al Ministerio.

El mantenimiento de las cuentas corre por cuenta del coordinador de la DGCT.

Vulnerabilidad encontrada con respecto a los Usuarios.- existen usuarios de base de datos sin límite de cuota de almacenamiento.

El rol (privilegio) otorgado como RESOURCE no limita al consumo de recursos de almacenamiento.

Propuesta alternativa.- la alternativa correctiva fue la de otorgar roles de select, insert, update, etc. en forma descriptiva y no vía RESOURCE ya que éste no controla el limite de espacio de uso en disco.

3.3.3 Materiales Aeronáuticos

Esta aplicación le pertenece a la Dirección de Seguridad Aérea, en ésta se registra el parque aéreo nacional (Modelos de aeronaves, propietarios, motores, etc.) así como el registro de las discrepancias u observaciones que realizan los inspectores de la DGAC a las aeronaves.

Procedimiento para el acceso a la aplicación Materiales Aeronáuticos

Los Coordinadores o el Jefe de la Unidad de Sistemas de la DGAC, puede solicitar el pedido de ingreso de nuevos usuarios a la aplicación, así como la instalación.

La aplicación cuenta con perfiles de usuarios y los accesos caducan los 31 de diciembre de cada año, es decir antes de finalizar el año se consultará quienes serán los usuarios que tendrán acceso a la aplicación el año siguiente.

a). Exámenes Aéreos

Esta aplicación pertenece a la Dirección de Instrucción Aérea, es usado por los pilotos y demás personal aeronáutico para rendir sus exámenes y obtener su licencia.

Esta aplicación permite el registro del banco de preguntas, temas y la configuración de lo anterior para la generación del examen.

Procedimiento para el acceso a la aplicación Exámenes Aéreos

La persona encargada de pedir ingreso de nuevos usuarios, así como la instalación es la jefa de la Dirección de Instrucción Aérea.

La aplicación cuenta con perfiles de usuarios y los accesos caducan los 31 de diciembre de cada año, es decir antes de finalizar el año se consultará quienes serán los usuarios que tendrán acceso a la aplicación el próximo año.

El usuario es el mismo de la red y la contraseña inicial que se les asigna, puede ser cambiada por el usuario.
Las Base de datos son administradas por el programador.

b). Seguros Aéreos

Aplicación que se encarga de ver todo lo referente a los seguros que deben de tener las aeronaves.

Procedimiento para el acceso a la aplicación Seguros Aéreos

La aplicación cuenta con perfiles de usuarios y los accesos caducan los 31 de diciembre de cada año, es decir antes de finalizar el año se consultará quienes serán los usuarios que tendrán acceso a la aplicación el próximo año.
El usuario es el mismo de la red y la contraseña inicial que se les asigna, puede ser cambiada por el usuario.
Las Base de datos son administradas por el programador.

3.3.4. Sistema de Administración y Trámite Documentario

a). Registro de Compras COA

Esta aplicación extrae información ingresada en la aplicación del COA de la Sunat y la junta con información adicional para la emisión de reportes de control interno.
El ingreso de usuarios esta a cargo de la Dirección de Contabilidad, así como la instalación.
El usuario es el mismo de la red y la contraseña inicial que se les asigna, puede ser cambiada por el usuario.
Las Base de datos son administradas por el programador.

b). SISTEMA SIGA

Procedimiento de acceso al sistema

1. El Director a Cargo envía a la Dirección de Informática, mediante el correo electrónico la relación de usuarios autorizando su inscripción al sistema, las opciones que debe tener y los privilegios que se le deben otorgar.
2. Verificando que las opciones pertenecen a su área se le instala el sistema, para ello se realiza lo siguiente:

Se registra en la base de datos al usuario y se asigna los roles correspondientes.
Cada responsable de módulo (programador), otorga las tablas que deben asignarse a cada rol para ser registrados en la base de datos.
En primer lugar el responsable debe verificar que el usuario este registrado dentro del grupo Gestor, si no lo está lo registra para que tenga acceso al Servidor correspondiente, esta operación lo debe coordinar con el Jefe responsable de la administración de redes.
3. En el Programa del SIGA, el responsable del módulo está asignando a cada usuario del sistema, las opciones que debe tener cada rol. En el inicio otorgan al usuario una contraseña fácil de memorizar y se habilita el programa para que automáticamente al ingresar al sistema por primera vez, se obliga al usuario a cambiar la contraseña y ésta no es validada a menos que la longitud de dicha contraseña sea mayor a 6 caracteres alfanuméricos.
Si las opciones solicitados por los directores no pertenecen a su área, el mismo director tiene que dirigir el documento, solicitando el permiso correspondiente de los responsables de la información (tesorería, contabilidad, abastecimiento, presupuesto, personal).
La oficina correspondiente envía la conformidad y se procede a instalar o completar las opciones requeridas.
4. Existe un procedimiento para el cambio de contraseña, cuando el usuario olvidó su contraseña y quiere cambiarlo se procede de la siguiente manera:
Puede realizar el requerimiento por el correo electrónico institucional ó el anexo o teléfono interno a la persona responsable de la base de datos correspondiente.
Luego de validado la solicitud, se procede al cambio siguiendo el mismo procedimiento que el aplicado al acceso de un nuevo usuario.
5. Las Altas y Bajas de los usuarios son comunicados por cada Jefe de oficina o Director General.

c) Sistema de Trámite Documentario (SID o SIDI)

El procedimiento para acceder al sistema existente permite asegurar que los accesos se restrinjan solo a un número de usuarios autorizados.
Procedimiento para acceder al sistema:
1. Solicitud del Jefe de la Unidad dirigida a la Dirección de Informática, quien autoriza la instalación del Sistema en la computadora de su personal, luego mediante el correo electrónico institucional el Jefe de la Unidad envía datos específicos como el nombre del

usuario, el área donde trabaja, que opciones tendrá habilitada en el sistema de trámite documentario (SID) o SIDI, puede autorizar el ingreso en ambos sistemas dependiendo de la función que desempeñe el usuario.

2. Cumplido el trámite anteriormente expuesto el responsable de la base de datos crea el usuario, en el Servidor Notes y asigna una clave temporal el área, que es cambiada al iniciar su acceso al programa.

d). Sistema de Registro de Visitas

El procedimiento para acceder al sistema permite asegurar que los accesos se restringen solo a un número de usuarios autorizados, el procedimiento es similar al anterior.

Contraseña de acceso.- las claves creadas tienen el siguiente parámetro.

El nombre de usuario asignado y las claves son administradas en el servidor, manteniéndose una copia en otra máquina, asimismo los instaladores están almacenados en una computadora.

3.4 Seguridad en base de datos de desarrollo y producción

La Dirección de Informática cuenta con dos Bases de Datos: desarrollo y producción.

a. Desarrollo

Esta base de datos se encuentra en la maquina del programador a cargo de desarrollar el programa o actualizarlo, en esta computadora se realiza algunas pruebas, se ha tomado en cuenta la seguridad en los accesos, para esto se manejan diferentes contraseñas de acceso personalizado y está habilitado solo para los programadores.

b. Producción

Existen otras modalidades de acceso especiales, que se incluyen en los sistemas de producción:

- Creación: permite al usuario crear nuevos archivos, registros o campos.
- Búsqueda: permite listar los archivos de un directorio determinado.
- Ubicación y Horario: el acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas. En cuanto a los horarios, este tipo de controles permite limitar el acceso de los usuarios a determinadas horas de día o a determinados días de la semana, de esta forma se mantiene un control más restringido de los usuarios y zonas de ingreso.

Estos dos tipos de controles siempre deben ir acompañados de alguno de los controles anteriormente mencionados.

En el caso del programa de tipo administrativo, solo están habilitados para actualizar las tablas en forma masiva las personas que tienen acceso al usuario SIGAAD.

Si el programador modificara la tabla, ésta se reflejaría automáticamente en el campo de auditoria, en este campo se verifica también, que usuario actualizó o modificó la información.

Se realiza el monitoreo de los accesos a la Base de Datos, con la auditoria de la misma Base de Datos.

Es fácil de comprobar, como se observará posteriormente, los siguientes datos: la computadora desde donde ingreso el usuario al sistema, el nombre o ID con el que ingreso el usuario, el día, la hora y las acciones de select , delete, update que realiza por cada tabla, como se muestran en las figuras 3.2 y 3.3

EL TERMINAL indica desde que maquina están ingresando

El USERNAME indica con que usuario de la BD ingresa

El TIMESTAMP indica la fecha y hora en que ingresa al sistema.

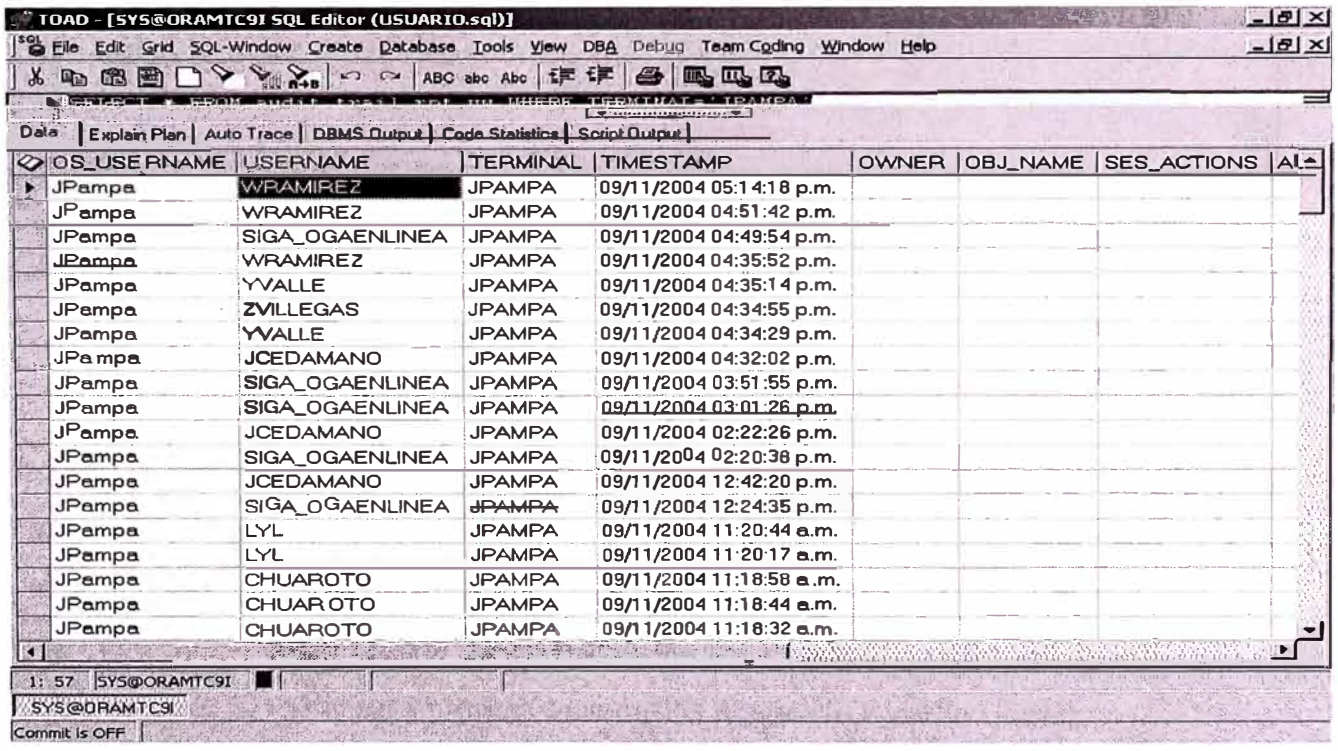


Fig. 3.2 La auditoria muestra el **SELECT** que esta utilizando el usuario Jpampa

Esta pantalla indica que proceso está realizando el usuario y el Select que está utilizando.

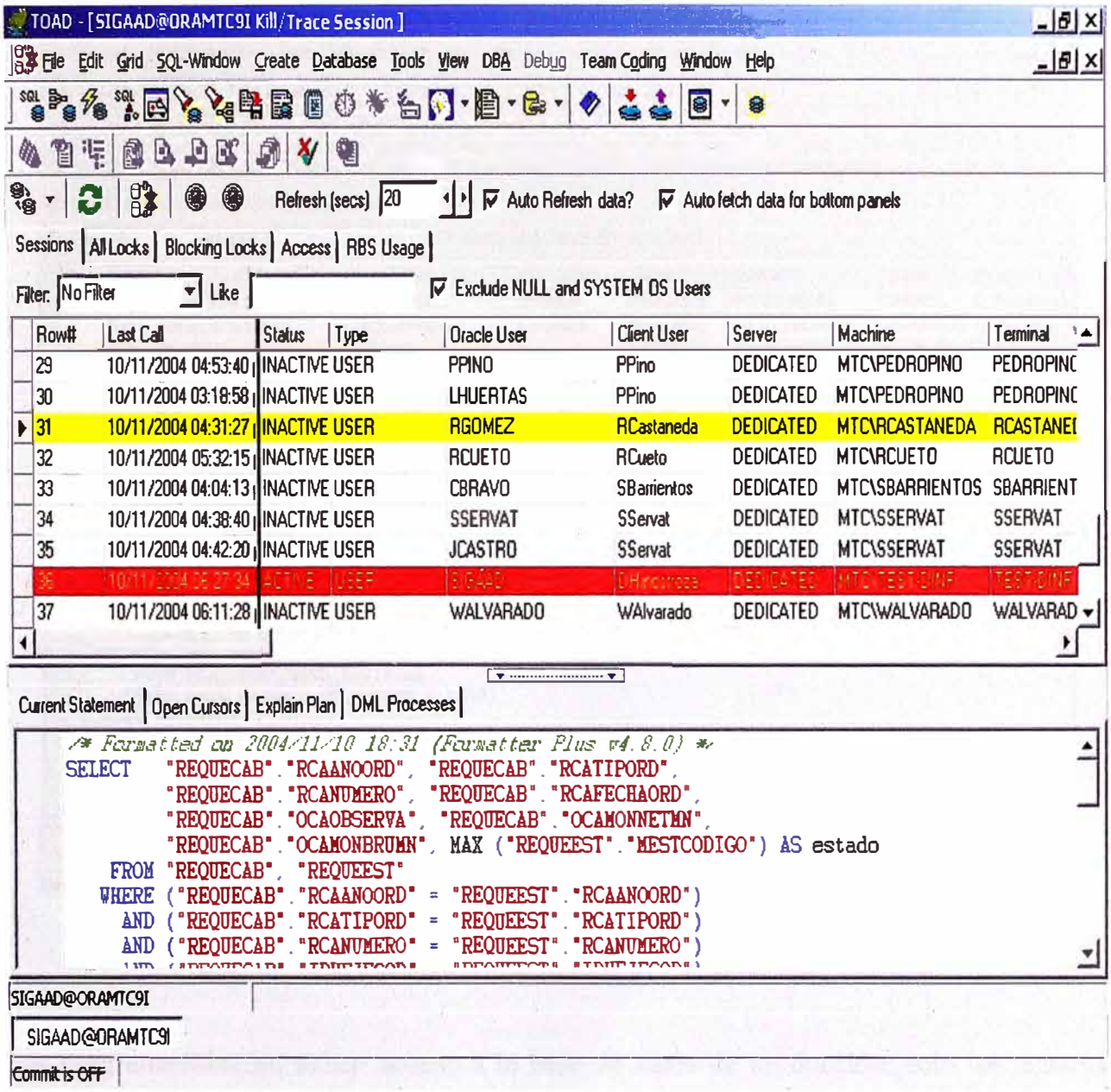


Fig. 3.3 Usuario RGOMEZ está ingresando al Gestor desde la PC de RCASTANEDA

En la fig. 3.3 se observa cuando un usuario usa el identificador Rgomez y la computadora desde donde ingresa corresponde a la asignada a la Sra. Rosa Castañeda, esto solo es posible si el Sr. Ricardo Gómez ha puesto en conocimiento de la Sra. Castañeda la clave de acceso al sistema, como ambos tienen instalados los sistemas, es probable que la usuaria Rosa Castañeda ha usado los privilegios asignados al usuario Ricardo Gomez.

Asimismo, es posible controlar, y determinar la herramienta que esta utilizando el usuario auditado para ingresar al **GESTOR** (Fig. 3.4). En la figura se puede observar que la administradora de la base de datos DHINOSTROZA está ingresando al Gestor, mediante el uso del programa Toad.exe.

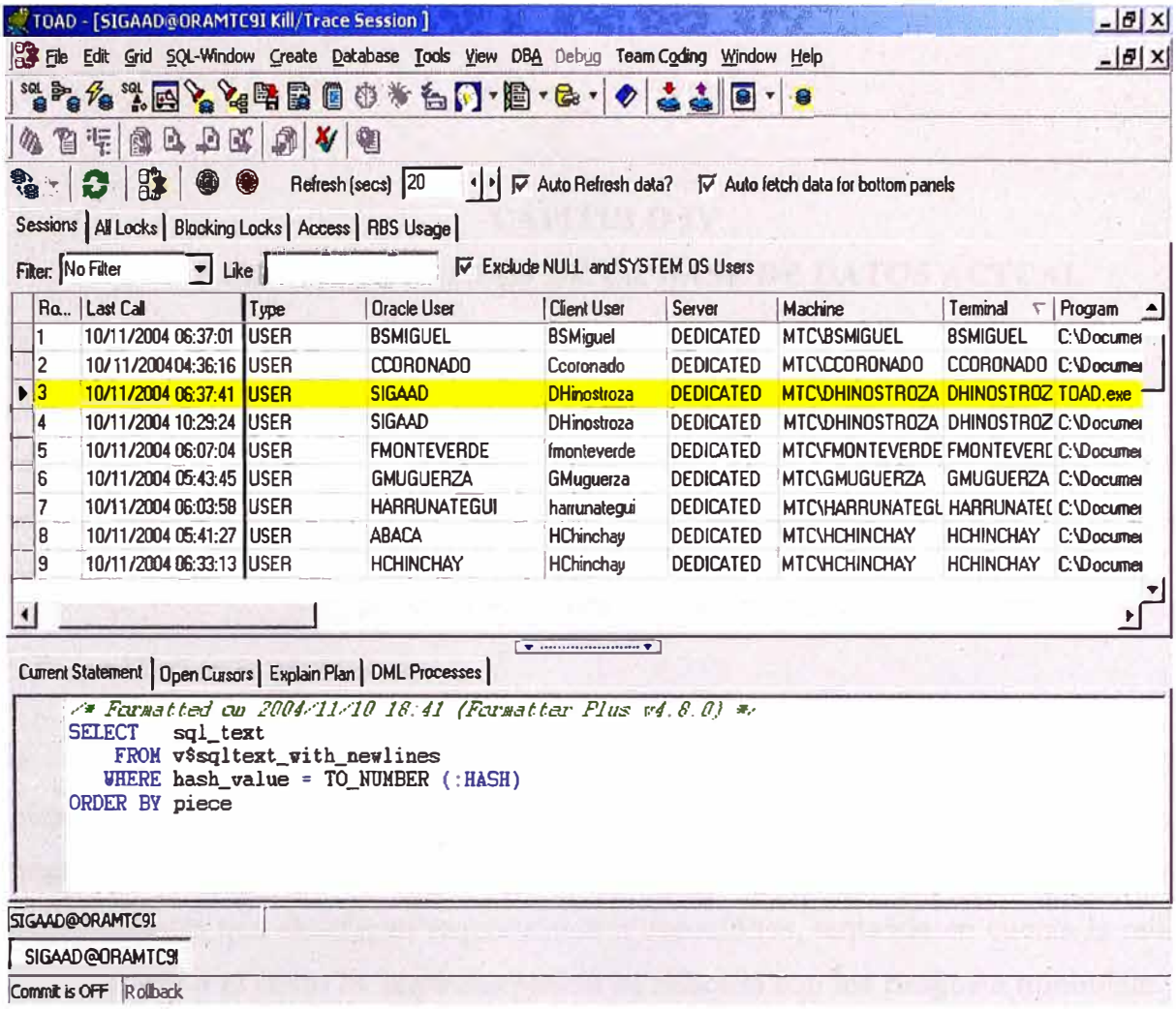


Fig. 3.4 Usuario Dhinostroza ingresa con el programa Toad.exe

Los programadores no tienen acceso a la base de datos de producción, solo los usuarios autorizados ingresan información.

CAPITULO IV
ANÁLISIS Y SEGURIDAD DE LA BASE DE DATOS ACTUAL

En este capítulo se hará énfasis a la base de datos Oracle, porque las bases de datos SQL Server cuentan con planes de migración a Oracle. El primer paso en la seguridad de la base de datos (BD) es asegurar considerando la plataforma en la que reside, luego se debe considerar la seguridad del sistema operativo.

4.1 Seguridad en la plataforma

Una vez identificados los requerimientos de seguridad, deben seleccionarse e implementarse controles para garantizar que los riesgos sean reducidos a un nivel aceptable. Los controles pueden seleccionarse en base a estándares o pueden diseñarse nuevos controles que satisfagan requerimientos específicos, teniendo en cuenta la relación costo beneficio o el costo de implementación en relación con los riesgos a minimizar y las pérdidas que podrían producirse de tener lugar una violación de la seguridad.
Algunos parámetros que se enuncian a continuación, pueden considerarse como rectores que proporcionan un punto de partida para la implementación de la seguridad de la información de la base de datos.

4.1.1 Seguridad de Cuentas.- Cada cuenta debe tener una palabra clave o password (diferentes del nombre). Una cuenta en una base de datos (BD), puede estar ligada con una cuenta de sistema operativo.

4.1.2 Seguridad de Objetos.- Los privilegios se pueden agrupar formando roles. La utilización de los roles simplifica la administración de los privilegios cuando tenemos muchos usuarios.
Los roles del sistema se pueden utilizar para gestionar los comandos de sistemas disponibles para los usuarios. Las acciones contra cada tipo de objeto son autorizadas por privilegios separados.

4.1.3 Creación de Usuarios.- El objetivo de la creación de usuarios es establecer una cuenta segura y útil que tenga los privilegios adecuados.

4.1.4 Eliminación de Usuarios.- Los usuarios pueden ser eliminados de la BD y a si dar mantenimiento de usuarios que ya no tengan acceso.

4.1.5 Privilegios del Sistema.- Los roles de sistema se utilizan para distribuir la disponibilidad de los comandos del sistema utilizados para gestionar la BD. Los privilegios se pueden agrupar en roles, para así satisfacer a distintos tipos de usuarios.

4.1.6 Perfiles de Usuario.- Los perfiles se utilizan para limitar la cantidad de recursos del sistema y de la BD disponibles para un usuario.

4.1.7 Cuentas de la base de datos sobre cuentas de sistema operativo.- Los usuarios pueden entrar en la base de datos una vez que han dado un nombre de usuario y una palabra clave o contraseña. Sin embargo, es posible aprovecharse del Sistema Operativo para obtener un nivel adicional de autentificación.
Protegidos por contraseña.
Las contraseñas pueden proteger tantas cuentas como roles.

4.1.8 Gestionando Privilegios.- Los privilegios dan acceso a los usuarios, a los datos que no poseen. Los roles con grupos de privilegios facilitan la administración de los privilegios.

- Listar Privilegios Otorgados
- La información de los privilegios otorgados se almacena en el diccionario de datos. Estos datos son accesibles por ello que se tiene que tener un control adecuado y específico.
- Encriptación de contraseñas.- conocer el modo en que se encriptan y se tratan las contraseñas puede posibilitar al administrador de la base de datos (DBA) la realización de ciertas tareas que de otro modo le resultarían imposibles.
  Almacenamiento de contraseñas.- cuando se especifica una clave o contraseña para un usuario y se asigna un rol, la base de datos almacena la versión encriptada del mismo en el diccionario de datos. la misma contraseña para diferentes usuarios genera diferentes versiones encriptadas.

- Convertirse en otro Usuario.- como se puede notar en la versión encriptada de una contraseña, es posible tomar una cuenta temporalmente, cambiando su clave original, para restaurarlo a continuación, esto permite que el administrador de la base de datos se convierta temporalmente en otro usuario.

4.2 Auditoria de Seguridad.- Capacidad de auditar todas las acciones que tienen lugar en la base de datos, como por ejemplo:

- Intentos de entrada en cuentas de la base de datos.
- Accesos a los objetos de la base de datos.
- Acciones sobre la base de datos.
- La base de datos registra todos los intentos de acción, tanto los exitosos como los infructuosos, aunque es un parámetro configurable.

4.2.1 Auditando Conexiones.- Todo intento de conexión con la base de datos será registrado por los siguientes mecanismos:

a). Auditando Acciones.- se puede auditar cualquier acción que afecte a cualquier objeto de la base de datos.

b). Auditando Objetos.- además de la auditoria de acciones sobre los objetos, se puede seguir el rastro a las operaciones de manipulación de tablas: SELECT, INSERT, UPDATE y DELETE. Estas auditorias se pueden hacer por sesión o por acceso.

10.3 Protegiendo los Registros de Auditoria.- la tabla que registra lo auditado puede ser objeto de intentos de acceso para eliminar los registros.

4.2.2 Auditoria externa de la base de datos en producción Oracle

Se realizó desde una estación cliente, accediendo a la base de datos con el ID de otro usuario escogido al azar, haciendo uso del software sqlplus (de Oracle) y toad que son aplicativos usados por desarrolladores con la base de datos Oracle.

a). Vulnerabilidad referida a los usuarios

Existen usuarios de base de datos sin límite de cuota de almacenamiento (fig.4.1). El rol privilegio otorgado como RESOURCE no limita al consumo de recursos de almacenamiento.

RESOURCE: conjunto de privilegios para usuario desarrollador quien puede almacenar datos sin restricción.

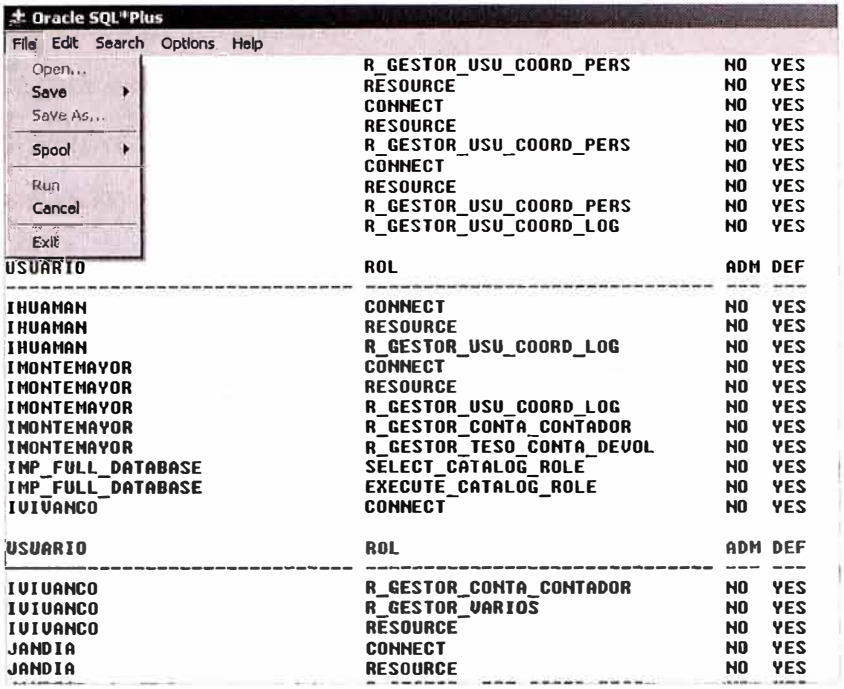


Fig. 4.1 Usuarios con privilegio Resource

Vemos en la fig. 4.2, que haciendo uso del privilegio de RESOURCE otorgado al usuario WRAMIREZ, también se pueden crear objetos de la base de datos, almacenar data sin ningún límite. Para los usuarios ubicados en el TABLESPACE SYSTEM, que forma parte de la base de datos, al llenarse éste, el TABLESPACE bloquearía al usuario SYSTEM y se detendría la base de datos.

TABLESPACE: Unidad lógica de la base de datos, la cual está conformada por datafiles (parte física) que almacena datos, usuarios etc., en general objetos de base de datos.

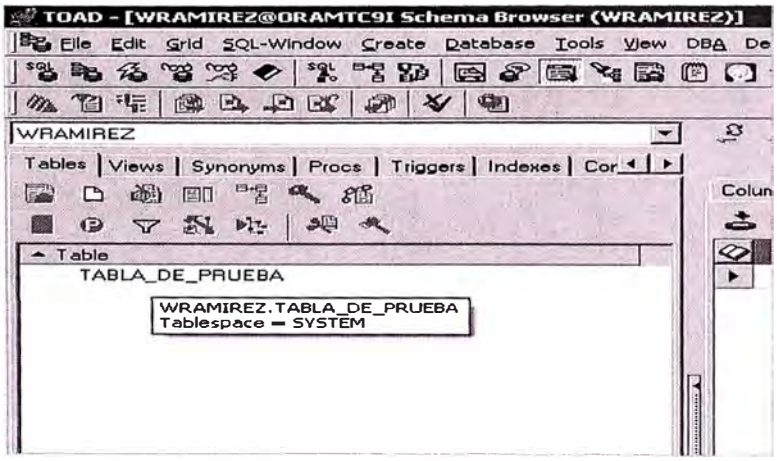


Fig. 4.2 Usuario ubicado en tablespace

b) Con respecto a la clave de los usuario

Existen muchos usuarios con igual clave de acceso.

Nombre de usuario = clave

SQL> connect usuario/clave@esquema

Connected.

Al resolver el acceso, la respuesta connected verifica que se ingreso a la base de datos.

Las pruebas se realizaron a usuarios que se muestran en la fig. 4.3

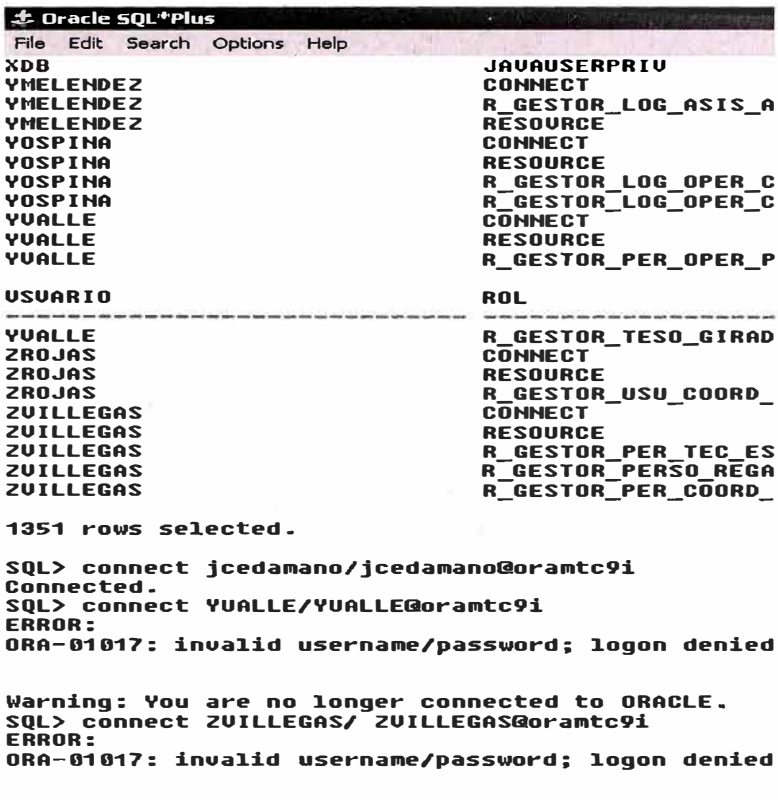


Fig. 4.3 Uso no autorizado contraseña no fue validada

SQL> CONNECT LMS/LMS@ORAMTC9I;
Connected.
SQL> CONNECT LLEY/LLEY@ORAMTC9I;
Connected.
SQL> CONNECT JRIOS/JRIOS@ORAMTC9I;
Connected.
SQL> CONNECT LAMES/LAMES@ORAMTC9I;
Connected.
SQL> CONNECT LPOLO/LPOLO@ORAMTC9I;
Connected.
SQL> CONNECT PVEGA/PVEGA@ORAMTC9I;
Connected.
SQL> CONNECT TRIOS/TRIOS@ORAMTC9I;

```
Connected.
SQL> CONNECT JCHUNG/JCHUNG@ORAMTC9I;
Connected.
SQL> CONNECT JLUJAN/JLUJAN@ORAMTC9I;
Connected.
SQL> CONNECT JPABLO/JPABLO@ORAMTC9I;
Connected.
SQL> CONNECT JPAVIC/JPAVIC@ORAMTC9I;
Connected.
SQL> CONNECT JPEREZ/JPEREZ@ORAMTC9I;
Connected.
SQL> CONNECT JPILCO/JPILCO@ORAMTC9I;
Connected.
SQL> CONNECT JSALAS/JSALAS@ORAMTC9I;
Connected.
SQL> CONNECT KROJAS/KROJAS@ORAMTC9I;
Connected.
SQL> CONNECT LORTIZ/LORTIZ@ORAMTC9I;
Connected.
SQL> CONNECT LRAMOS/LRAMOS@ORAMTC9I;
Connected.
```

c) Vulnerabilidad referida al Otorgamiento de Roles

Se detectó y luego se corrigió la falla en otorgamiento de roles, para esto se hizo una consulta como puede observarse en la fig. 4.4, es posible observar a los usuarios que acceden al sistema y los roles otorgados, esto ocurrió con todos los usuarios, incluidos del usuario SYS, SYSTEM.

select * from DBA_ROLE_PRIVS where grantee ='usuario'

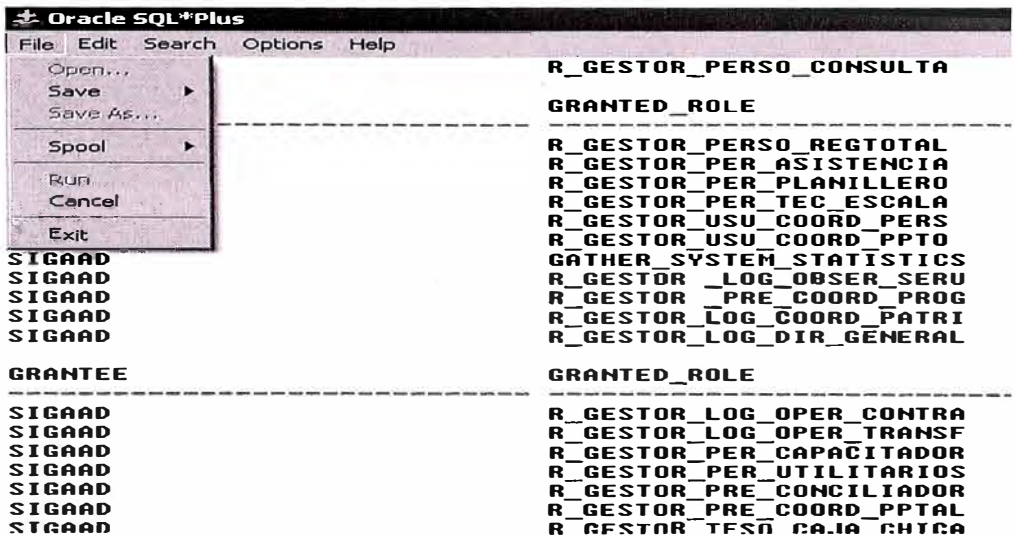


Fig. 4.4 Usuario observa roles de otros.

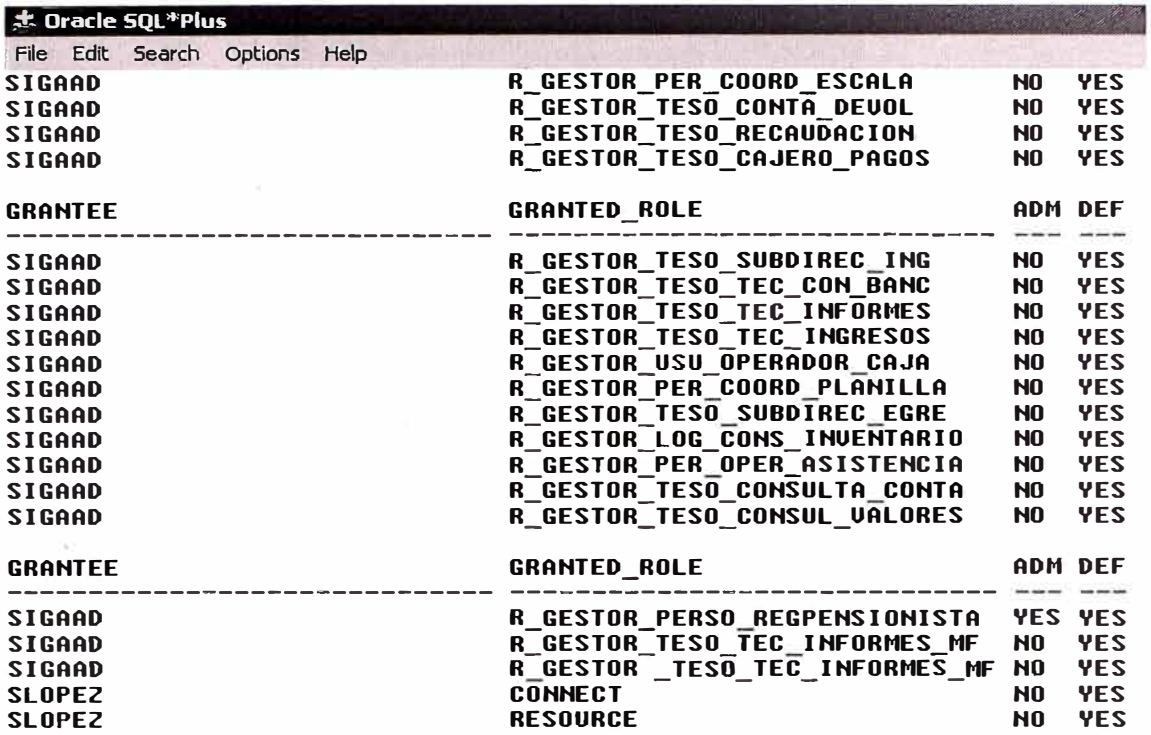


Fig. 3.5 Usuario observa roles de otros.

d) Vulnerabilidad referida a la Exportación de Datos

Se ha detectado que la herramienta de ayuda TOAD -que usan los desarrolladores- hace vulnerable la base de datos porque se puede exportar la estructura de la base de datos (diagrama entidad relación), la data de tablas y tener varios objetos de la base de datos (vistas, procedimientos y otros).

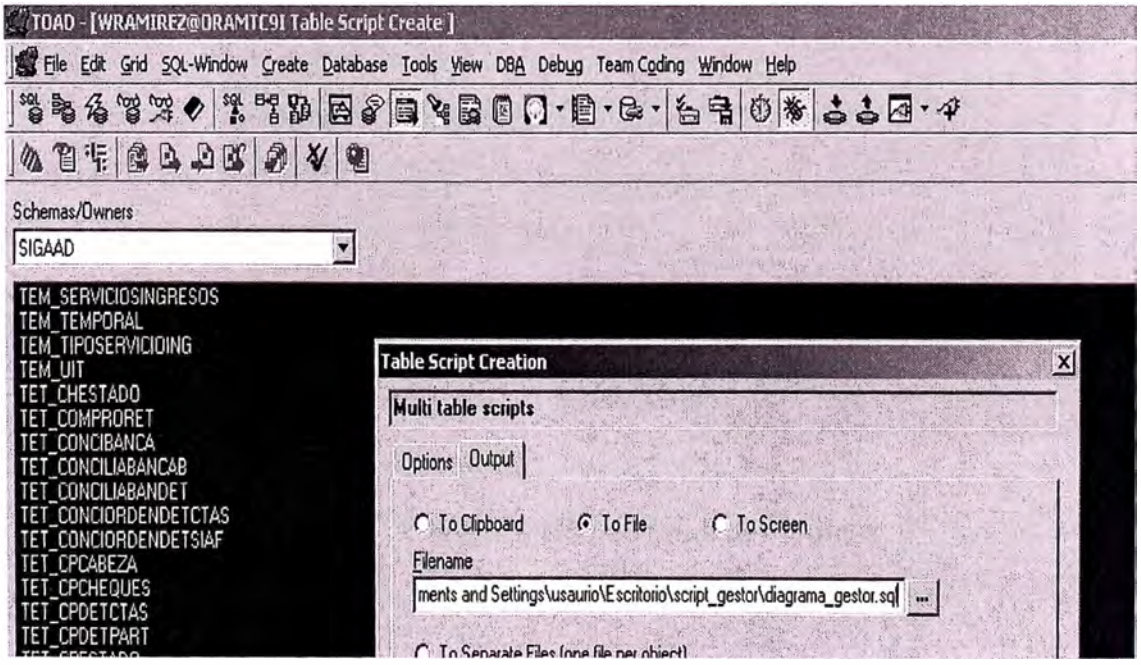


Fig. 3.6 Vulnerabilidad por uso del Toad

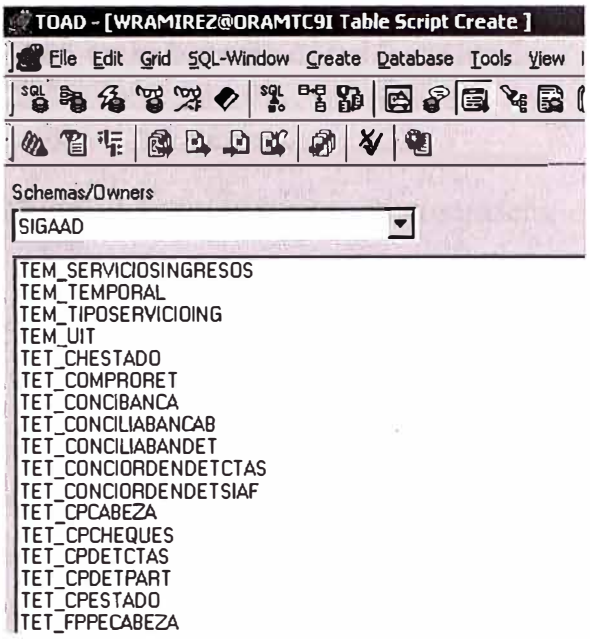


Fig. 3.7 Vulnerabilidad por uso del Toad

e)Vulnerabilidad referida a las Unidades Básicas de la Base de Datos

Se detecto solo dos unidades lógicas de almacenamiento de datos.

Cada unidad lógica de base de datos almacena datos (fig. 3.8), por lo que se hace necesario clasificarlos para un mejor control.

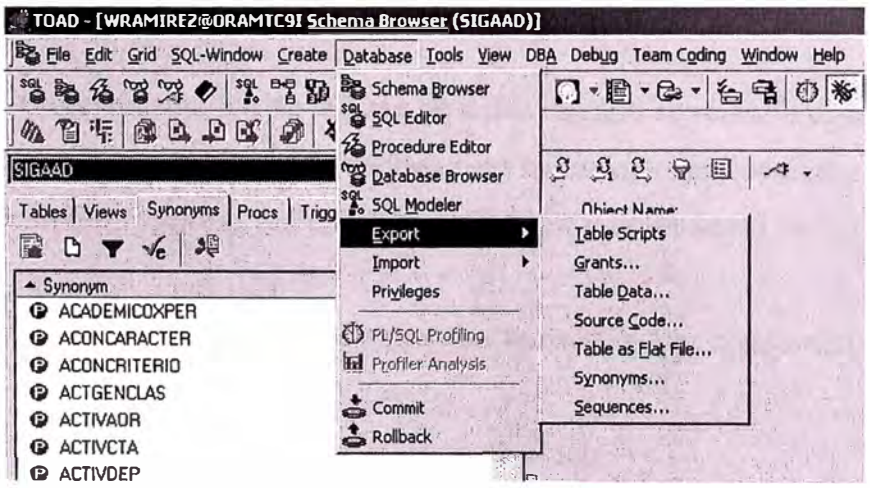


Fig. 3.8 Uso de unidades lógicas

4.3 Propuestas de seguridad en la base de datos a corto plazo

a) Automatizar otorgamiento y denegación de accesos.

b) Implementar la agregación y sincronización de contraseña del usuario para todos sus accesos.

c) Consolidar repositorio de almacenamiento de identidades (usuario-contraseña).

d) Mejorar la administración de contraseñas (letras, números, símbolos).

e) Autorización de acceso basada en roles.

f) Controlar los accesos por número de sesiones.

g) Usar políticas de restricción de software (Toad.exe=renombre1.exe= renombre2.exe).

h) Realizar pruebas de los backup.

i) Disponer visiblemente las alertas predeterminadas para bloquear los accesos no permitidos.

4.4 Propuestas de seguridad en la base de datos a mediano plazo

a) Separar los usuarios del tablespace system.

b) Revisar el otorgamiento de roles y corregir.

c) Crear "tablespace" de acuerdo a la clasificación de tablas con mayor cantidad de lecturas, cantidad de datos, funciones (personal, contabilidad, requerimientos. etc.) para auditar la cantidad de objetos específicos.

d) Configurar la carga automática de la base de datos cuando se reinicia el servidor.

e) Revisar y corregir las contraint (referencias) para la consistencia de datos.

f) Realizar afinamiento (mejorar las consultas y creación de índices) de las consultas a la base de datos.

g) Crear procedimientos almacenados de aquellas consultas que consumen mayor tiempo de respuesta.

h) Probar los backup para su posible puesta en producción.

i) Documentar los métodos de recuperación de datos y de los procedimientos antes mencionados.

4.5 Propuestas de políticas de contraseñas

El usuario de sistemas informáticos que disponga de una palabra clave de acceso es responsable del uso o mal uso que otras personas no autorizadas pudieran darle.

Una contraseña sencilla es fácil de determinar y una muy complicada resulta más peligrosa ya que el usuario para evitar olvidarse de ella, podría escribir en un papel y ubicarlo en su monitor.

Tomando en cuenta esto se ha planteado las siguientes recomendaciones:

a) Usar contraseñas con mas de 6 dígitos difíciles de averiguar, puede usar letras del alfabeto de la A a la Z, combinaciones de minúsculas con mayúsculas con números del 0 al 9 ó caracteres especiales: – ~, !: @, #, $, %, &, *, (;), +, =, [;], {; }, /, ?, <; > " De optar en usar una contraseña simple y fácil de recordar, también probablemente es fácil de adivinar por otros.

b) No comunicar a nadie la contraseña (password).

c) No escribir su contraseña por ningún lado.

d) Si por algún motivo (ejemplo.: soporte técnico) dio a conocer su contraseña de red, cámbielo por precaución.

e) No permita que le(a) observen al momento que usted digita su contraseña.

f) No usar una contraseña con datos conocidos por otros, como la fecha de nacimiento, número de seguro social, tarjeta de crédito, número de teléfono, una variación de su ID de usuario, nombre de familiares conocidos, etc.

g) Puede usar como contraseña, Nemónicos, por ejemplo: "TBONTB" que viene de " To Be Or Not To BE"; L3RM6002 que vienen de: Los tres Reyes Magos2006.

CAPITULO V
SEGURIDAD DE LA RED DE DATOS DEL MTC

5.1 OBJETIVO

Optimizar los niveles de Seguridad Informática en los principales segmentos de la Red de Datos de Informática, con la finalidad de:

a) Establecer una arquitectura de seguridad integral la cual comprenda el control del acceso externo e interno a los sistemas de información, logrando un adecuado nivel de confiabilidad, integridad y disponibilidad de los mismos.
b) Contar con una solución de seguridad que permita mejoras y cambios futuros en su diseño, y que además sea escalable, de alta disponibilidad y contar con parámetros de evaluación y monitoreo.
c) Garantizar conexiones seguras de entrada y salida a Internet, correo electrónico y cualquier tráfico de red.

5.2 ANTECEDENTES

En el campo virtual que está detrás del monitor se está expuesto a la mira de cualquier "husmeador" que por pericia o simples ganas de aprender o superarse vulneran la red, o personal de una empresa u organización, que por curiosidad vulneran la red de las instituciones, los portales y la privacidad de las computadoras. No sólo son los jóvenes inquietos los intrusos, sino también los individuos que detrás de un organismo gubernamental o detrás de un beneficio económico se infiltran en la privacidad de la red a través de Internet.

En un mundo globalizado donde la interacción de las comunicaciones ofrecen una vía de acceso fácil y rápida para los piratas o hackers, dejando expuestos los sistemas automatizados, como por ejemplo, de centrales nucleares, plantas potabilizadoras de agua, control de centrales hidroeléctricas, tráfico aéreo, banca privada y muchos sistemas más, es

muy probable que estos delitos informáticos sigan ocurriendo y que los hackers sigan realizando sus ataques más frecuentes.

Ante una medida de seguridad los hackers desarrollaran otra contramedida que vulnerará a la anterior y así sucesivamente se irán superando en capacitación y tecnología, para prevenir por un lado y vulnerar por el otro.

En el Ministerio de Transportes y Comunicaciones, en el segundo trimestre del año 2004 usuarios de alta dirección reportaron que sus fólderes o directorios de archivos, cuyos contenidos eran de índole reservados, estaban siendo compartidos hacia la red sin autorización del propietario en tanto otros usuarios comunicaron la aparición de un icono extraño en la barra de tarea de su estación de trabajo.

Ante esto la Dirección de Informática, con la autorización de la alta dirección tomó las siguientes acciones:

- Realizó una detección de vulnerabilidades en las Estaciones de Trabajo de Alta Dirección.
- Elaboró un Manual con Recomendaciones Básicas de Seguridad.

Los resultados obtenidos fueron:.

a) Se detectaron usuarios en la red que compartían sus recursos de disco en forma irrestricta como se muestran en las figuras fig. 5.1 y 5.2, así como también algunos usuarios de la red tenían contraseñas en blanco,

Fig.5.1 Usuario comparte totalmente su disco.

Un ejemplo es la Estación de Trabajo con IP 172.20.3.124 (Juan Escudero) cuya contraseña de administrador local esta en blanco, tal como se muestra en la figura 5.2.

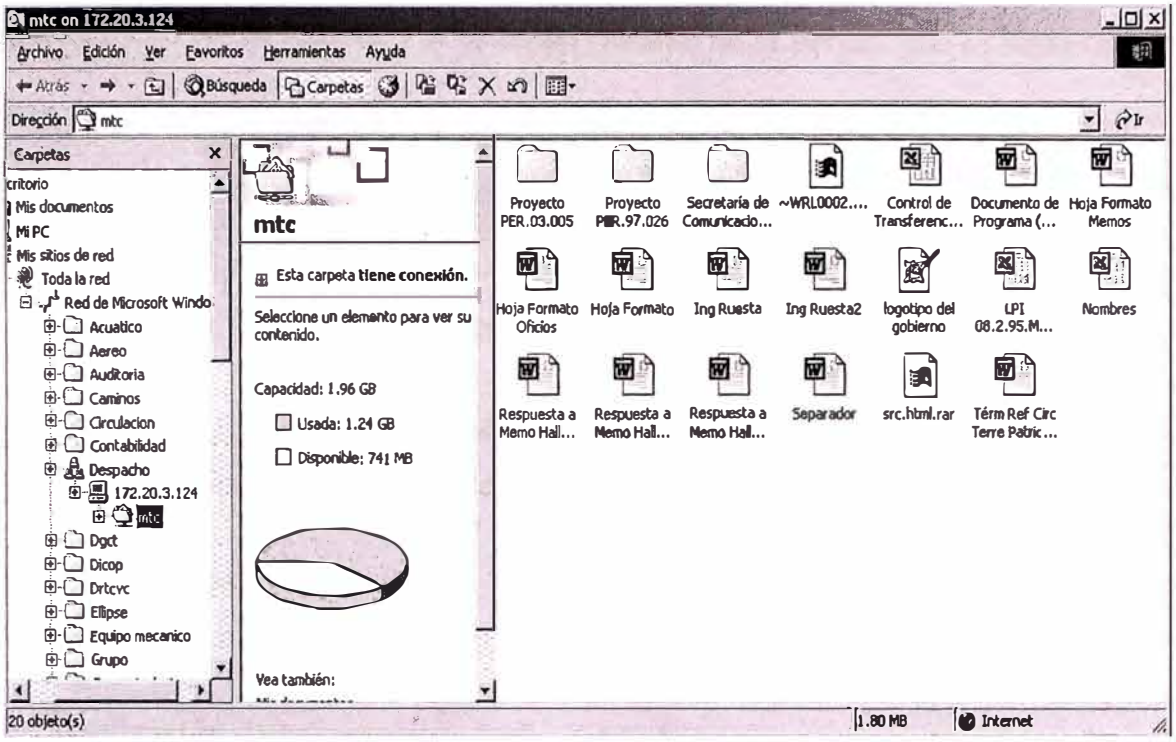


Fig.5.2 Usuario comparte totalmente su disco.

b) Se detectó que usuarios no autorizados de la red de datos del MTC ingresaban o trataban de ingresar a recursos compartidos de estaciones de trabajo.

Los indicios se detectaron fueron básicamente utilizando utilitarios de Monitoreo para Windows 95 y Windows 98 que se muestra en la fig. 5.3, en este caso la estación de trabajo de usuarios WHUAMANI y CEME están ingresando a la estación de trabajo del usuario Fernando Torres quien es personal del área de Sistemas del MTC.

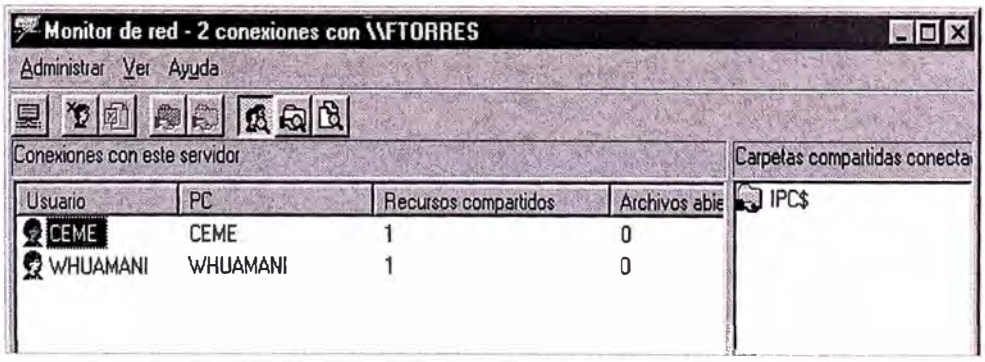


Fig. 5.3 Usuarios no autorizados que ingresan a una PC.

c) Se detectaron estaciones de trabajo, que tenían instalados intencionalmente y sin el conocimiento del propietario, un programa espía cuyo icono aparecía en la barra de tareas, como se muestra en la Fig. 5.4, este programa permite tener control total sobre una computadora en forma remota, y el usuario (víctima) no se percata que es observado.

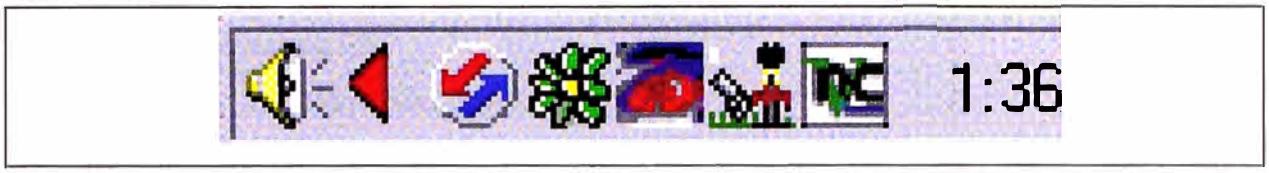


Fig. 5.4 Software VNC (último icono de izquierda a derecha)

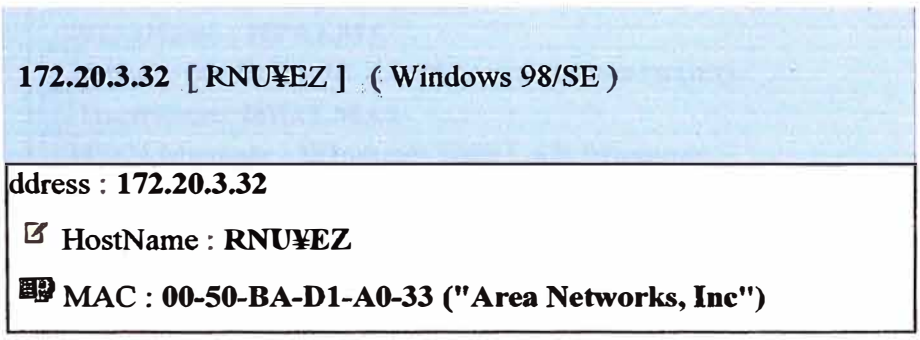
d) Se detectaron focos infecciosos de virus informático, en computadoras con carpetas compartidas de manera irrestricta, de cierto segmento de la Red de Datos del MTC.

5.3 Plan de trabajo

El plan de trabajo estuvo conformado por las siguientes etapas:

5.3.1 Realización de búsqueda de Vulnerabilidades a estaciones de trabajo de la Red Lan de Datos del MTC

Tuvo por finalidad la de identificar vulnerabilidades informáticas en las estaciones de trabajo de red Lan del MTC, las cuales pueden ser utilizadas por un intruso interno o externo para sustraer, alterar o eliminar información. Estas vulnerabilidades podrían consistir por ejemplo, en recursos de disco compartidos irrestrictamente como se muestra en la fig.5.5, existencia de programas espías (ver fig. 5.6), vulnerabilidades propias del sistema operativo (puertos abiertos), que pueden ser utilizados por intrusos para acceder a través de Internet a las computadoras, así como los virus tipo gusano, etc. Asimismo se analizó todos los recursos informáticos de la Red de Datos del MTC, con la finalidad de eliminar cualquier posibilidad de acceso a otras computadoras.



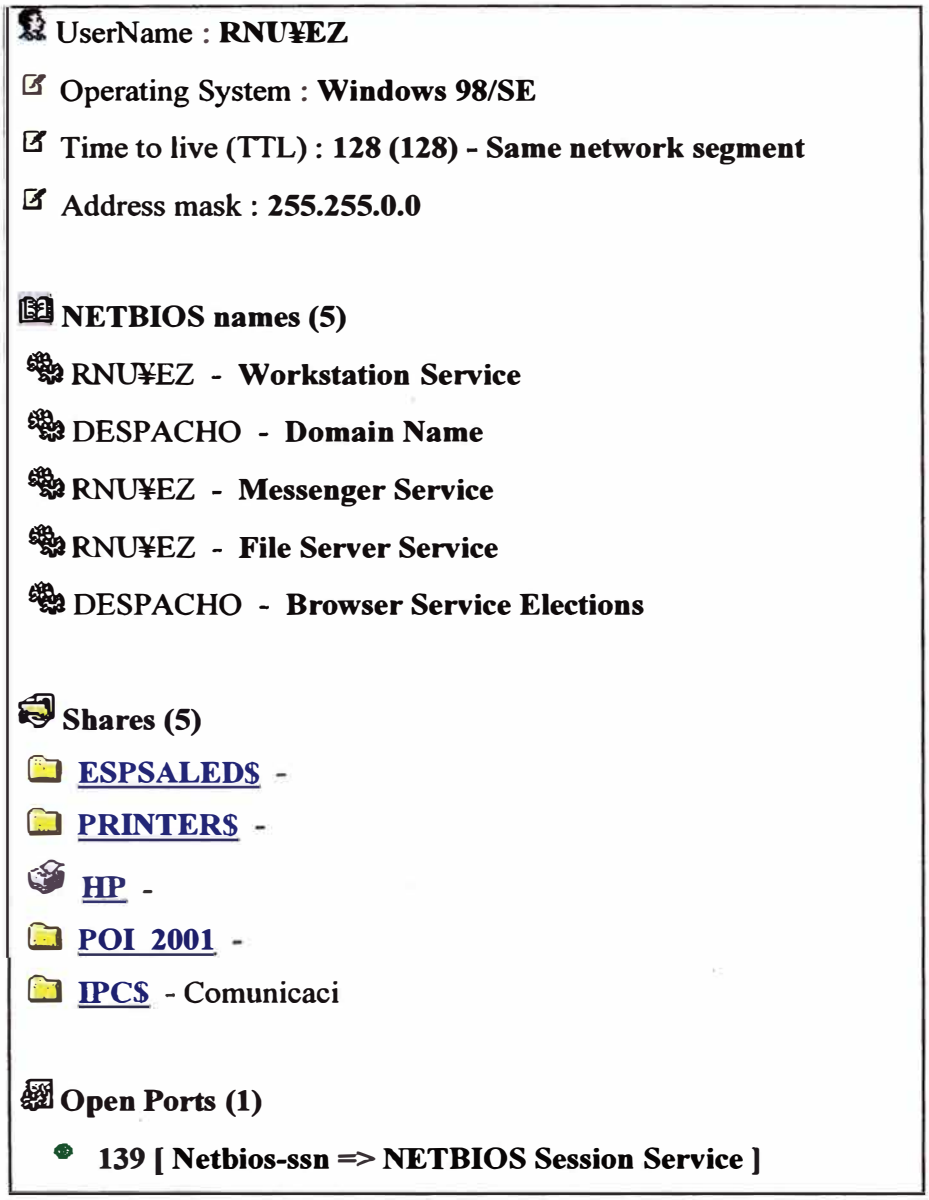
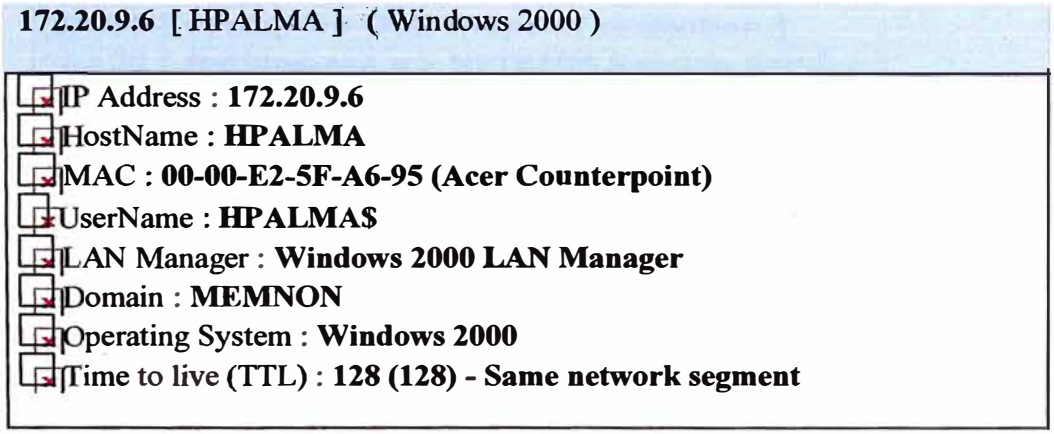


Fig. 5.5 Usuario comparte totalmente el disco

La usuaria Rnunez comparte las carpetas POI 2001 de manera irrestricta, IPC, ESPSALED.



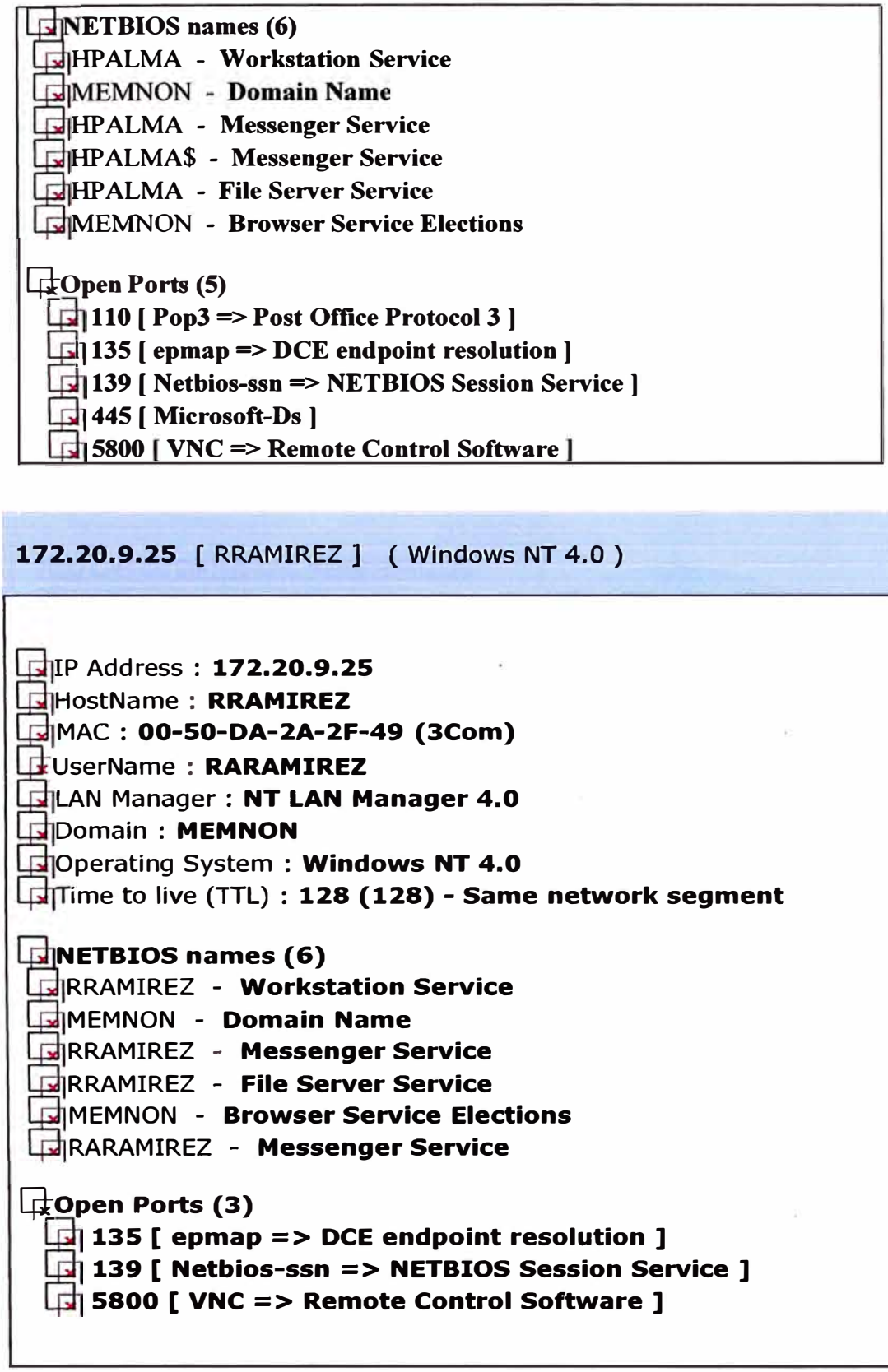


Fig. 5.6 Usuarios con software VNC instalado.

5.3.2 Creación y Monitoreo de VLANs .- Con la finalidad de poder identificar tráfico sospechoso o inusual hacia las estaciones de trabajo de Alta Dirección, se implementó:

a) Una red virtual que incluyó solamente las estaciones de trabajo de Alta Dirección (Vlan de alta dirección), lo que facilitaría la implementación de Sistemas de Seguridad Informático como IDS (Sistema Detector de Intrusos) o IDP exclusivamente para estos usuarios.

b) Una red virtual que incluyó todos los Servidores del MTC (Vlan de servidores), con la finalidad de identificar todo tráfico sospechoso o inusual hacia los Servidores del MTC, utilizando herramientas como el IDS o IDP.

Actualmente la red LAN de datos del MTC es un solo segmento lógico (red plana) como se muestra en la fig. 5.7, lo que dificulta el análisis del tráfico de datos de los segmentos mas críticos de la Red de datos del MTC.

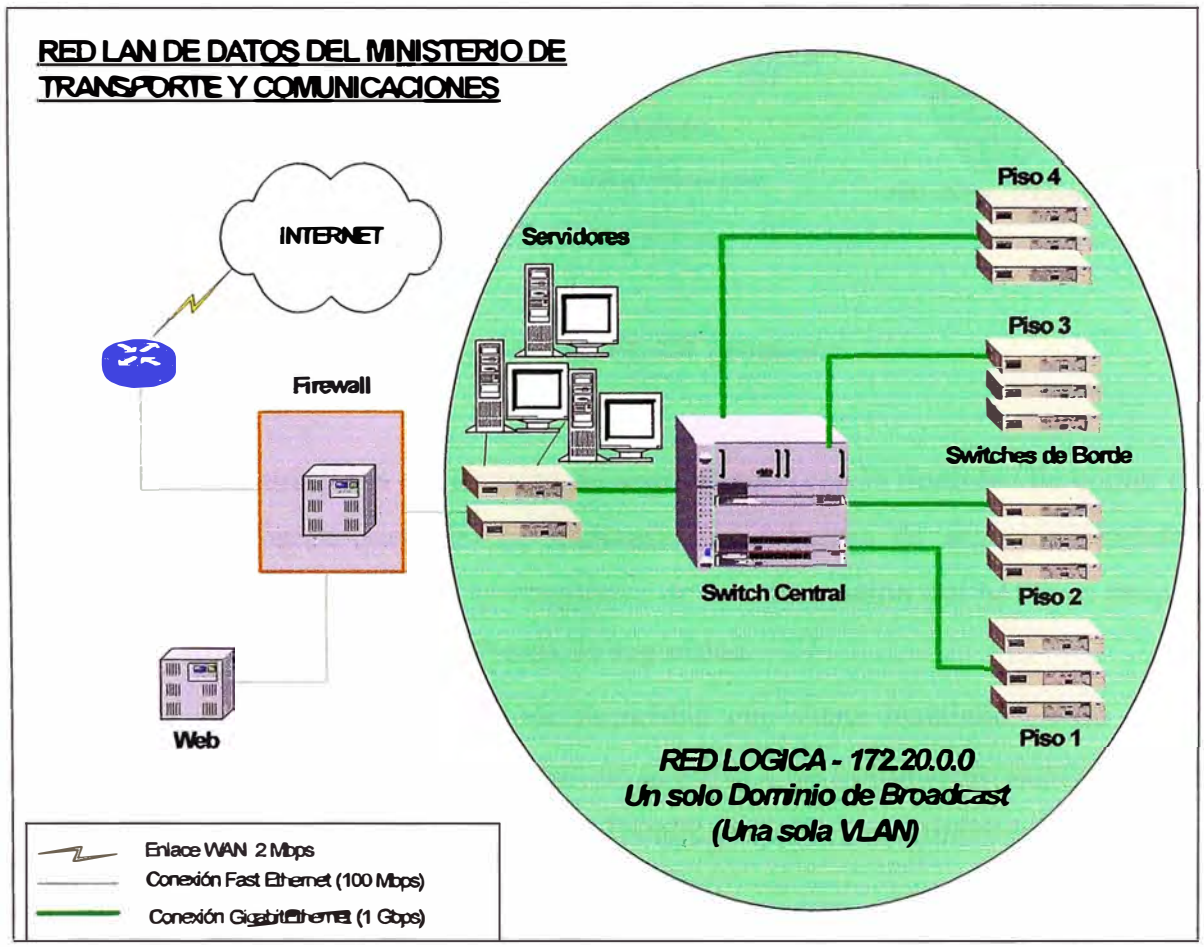


Fig. 5.7 Red antes de la creación de VLAN

Con la implementación de VLANs (fig. 5.8) podemos monitorear el trafico de red que fluye hacia / desde el segmento de los Servidores y segmento de Alta Dirección.

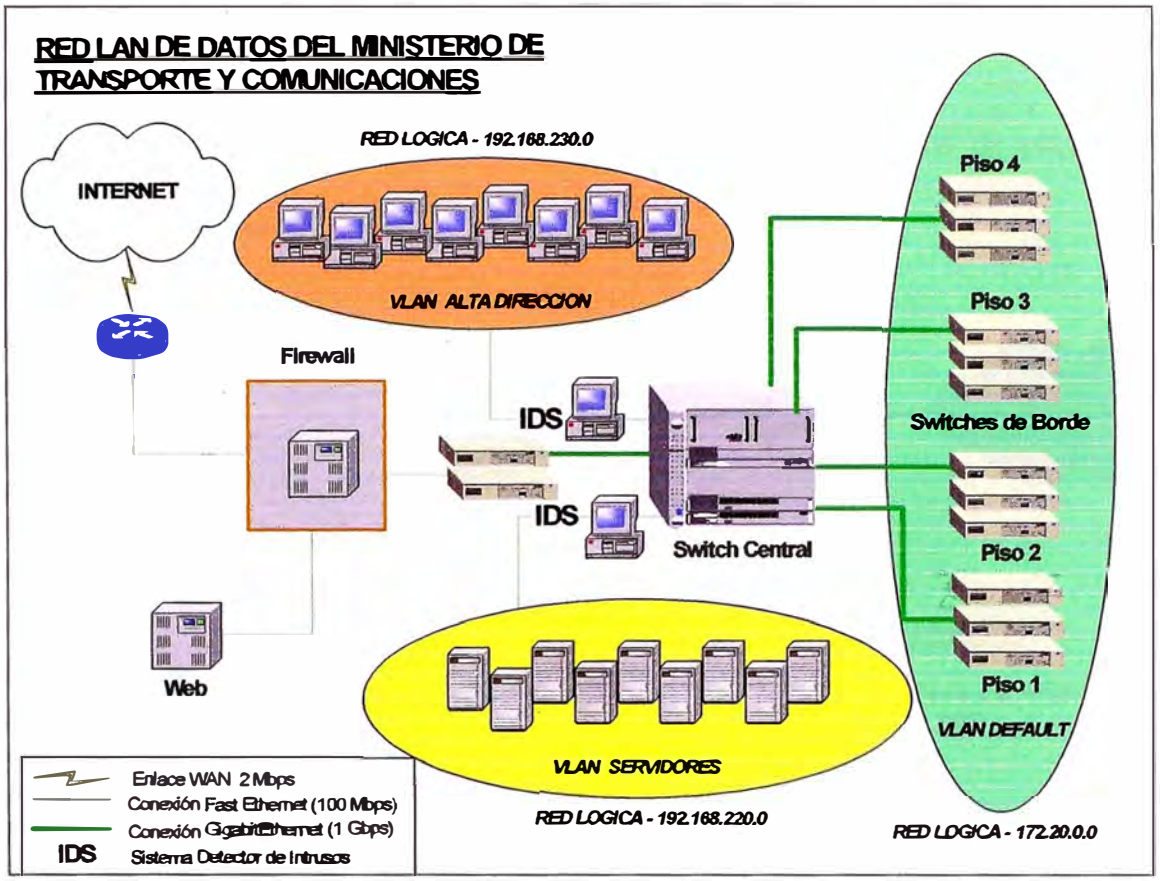


Fig.5.8 Red con VLAN propuesto

5.3.3 Requerimientos mínimos del sistema de seguridad.- con la finalidad de contar con una plataforma tecnológica que permita implantar un esquema de seguridad sólido y flexible a fin de proteger y mantener la integridad de la información del MTC se propone la adquisición de las siguientes herramientas de seguridad.

a) Firewall VPN Appliance.- Programa de seguridad que viene instalado en un equipo dedicado, destinado a filtrar protocolos de red de acuerdo a las políticas de seguridad de la Institución. Debe poder administrar: Ancho de Banda; creación y administración de Redes Privadas Virtuales.

Se ha considerado un Firewall de 08 puertos, para un crecimiento futuro de la red, con esta alternativa se bloquearía el acceso de los usuarios a la granja de servidores.

De adquirir un Firewall de 06 puertos, el acceso ó salida a la red Wan que viene realizándose a través de un Router, puede resolverse conectándose a un puerto del Switch principal en lugar de un puerto del Firewall, la misma consideración puede hacerse con la

salida hacia el MEF (Ministerio de Economía y Finanzas) que puede obtenerse de otro puerto del Switch, como se muestra en la fig. 5.9

El Firewall, el sistema de detección de intrusos (IDS) y/o el sistema de prevención de intrusos (IPS) deben ser considerados como una sola suite.

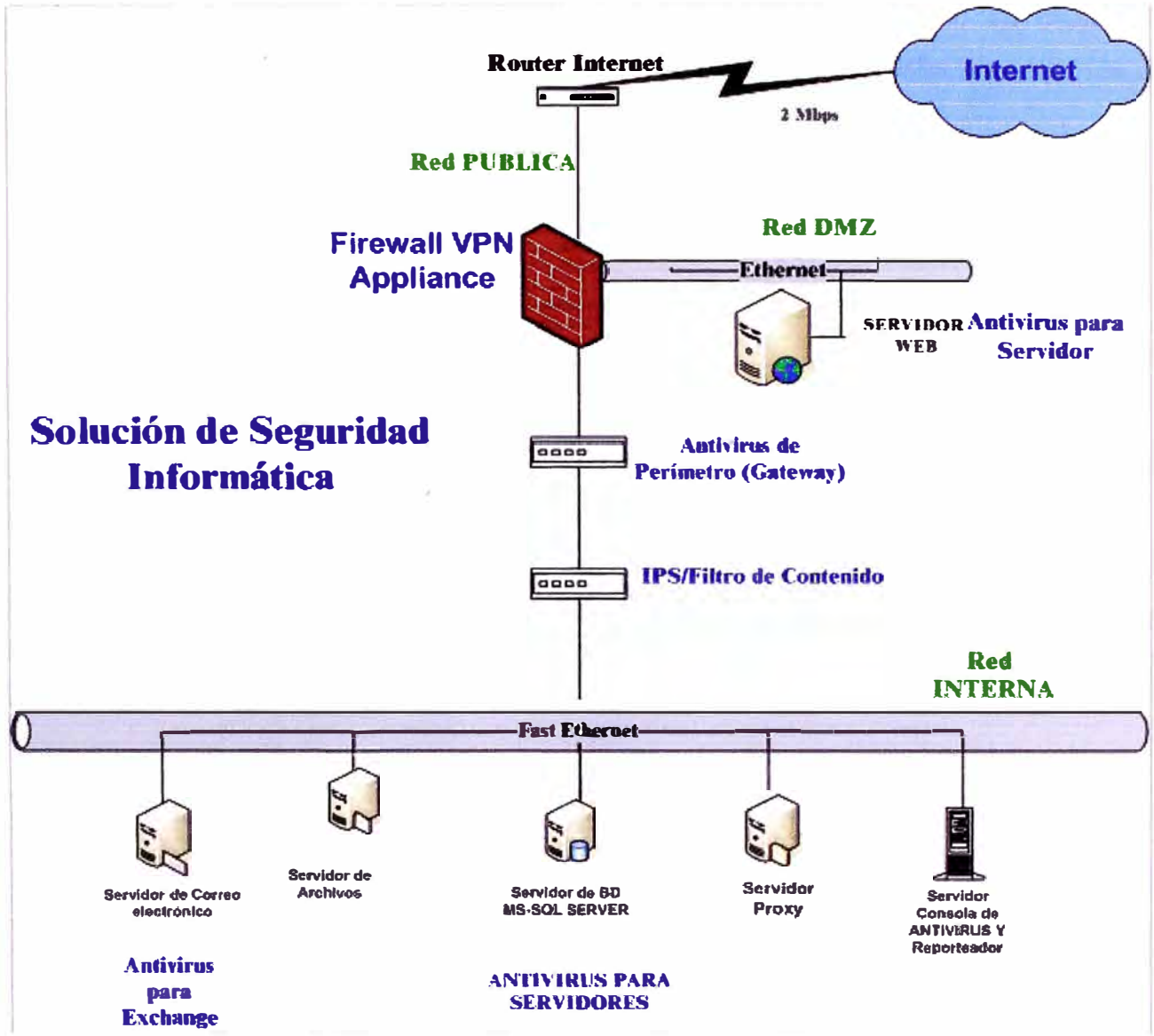


Fig. 5.9 Nueva plataforma de seguridad -Firewall

b) Antivirus Servidor Exchange (1,000 Licencias).- Software que permite filtrar cualquier tipo de archivo adjunto que pase a través del servidor.

Es urgente contar con una solución de antivirus que sea capaz de bloquear los mensajes tipo Spam y los adjuntos provenientes con virus. El antivirus que se aplique al servidor Exchange debe ser capaz de trabajar también sobre una plataforma Windows 2003.

Exchange debe ser capaz de trabajar también sobre una plataforma Windows 2003 y permita:

c) Sistema de detección y Prevención de Intrusos (IDS/IPS)

Este sistema es un complemento del Firewall, debe ser capaz de desechar los ataques, eliminar conexiones y paquetes malformados, terminar sesiones, remover cookies, reconfigurar el firewall, generar alertas, generar los registros (logs) en paquetes y proporcionar reportes mediante cuadros estadísticos. Este Modulo debe ser adquirido con el Firewall ó éste debe permitir incorporar el IDS/IPS posteriormente.

d) Seguridad – Antivirus para Servidores

Se requiere proteger a Servidores cuyo sistema operativo son: Nt 4.0, Windows Advance Server, Windows 2003 Server, para lograr una mayor eficacia es recomendable que el antivirus sea de diferente marca al instalado en las estaciones de trabajo.

d) Antivirus Gateway

Software que previene del ataque de virus a las páginas web visitadas, así como el correo electrónico y transferencia de archivos.

e) Filtro de Contenido

Software que asegura que el uso de Internet sea utilizado para fines de Trabajo, Investigación y otros relacionados con el giro de la Institución, optimizando el uso del Ancho de Banda de Internet.

CONCLUSIONES

La Seguridad Informática se basa, principalmente en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos y políticas de seguridad, esta administración abarca:

- Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios. Es necesario considerar que la solicitud de habilitación de un permiso de acceso para un usuario determinado, debe provenir de su superior y, de acuerdo con sus requerimientos específicos de acceso, debe generarse el perfil en el sistema de seguridad, en el sistema operativo o en la aplicación según corresponda.

- Además, la identificación de los usuarios debe definirse de acuerdo con una norma homogénea para toda la organización.

- Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos. Las mismas deben encararse desde el punto de vista del sistema operativo, y aplicación por aplicación, pudiendo ser llevadas a cabo por personal de auditoria o por el administrador del sistema; siempre sobre la base de que cada usuario disponga del mínimo permiso que requiera de acuerdo con sus funciones.

- Las revisiones deben orientarse a verificar la adecuación de los permisos de acceso de cada individuo de acuerdo con sus necesidades operativas, la actividad de las cuentas de usuarios o la autorización de cada habilitación de acceso.

- Detección de actividades no autorizadas. Además de realizar auditorias o efectuar el seguimiento de los registros de transacciones, existen otras medidas que ayudan a detectar la ocurrencia de actividades no autorizadas.

- Nuevas consideraciones relacionadas con cambios en la asignación de funciones del empleado. Para implementar la rotación de funciones, o en caso de reasignar funciones por

ausencias temporales de algunos empleados, es necesario considerar la importancia de mantener actualizados los permisos de acceso.

• Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización, llevadas a cabo en forma amistosa o no. Los despidos del personal de sistemas presentan altos riesgos ya que en general se trata de empleados con capacidad para modificar aplicaciones o la configuración del sistema. Para evitar estas situaciones, es recomendable anular los permisos de acceso a las personas que se desvincularán de la organización, lo antes posible. En caso de despido, el permiso de acceso debería anularse previamente a la notificación de la persona sobre la situación.

Política de Seguridad.- la política de seguridad, surge como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos.

La presidencia del Consejo de Ministros (PCM) desarrolla actividades relacionadas con la normatividad informática que son de uso obligatorio para los organismos del estado.

En relación a la seguridad informática, la PCM con fecha 23 de Julio del 2004 y Resolución Ministerial N° 224-2004-PCM aprobó el uso obligatorio de la norma técnica Peruana - NTP-ISO /IEC 17799-2004EDI – Tecnología de la Información: Código de Buenas Prácticas para la Gestión de la Seguridad de la Información, el que se viene implementando en el Ministerio de Transportes y Comunicaciones.

ANEXO A

GLOSARIO DE TERMINOS

Antivirus

Programa encargado de evitar que cualquier tipo de virus ingrese al sistema y se reproduzca.

Antivirus Gateway

Software que previene del ataque de virus a las páginas Web visitadas, así como el correo electrónico y transferencia de archivos. Analiza el tráfico, los datos para comprobar que están libres de virus y códigos maliciosos.

Antivirus para Exchange

Software que permite filtrar cualquier tipo de archivo adjunto que pase a través del servidor.

Base de datos

Conjunto de datos organizados entre los cuales existe una correlación y que están almacenados con criterios independientes de los programas que los utilizan. La filosofía de las bases de datos es la de almacenar grandes cantidades de datos de una manera no redundante y que permita las posibles consultas de acuerdo a los derechos de acceso.

Bug

Un error en un programa o en un equipo. Se habla de bug cuando es un error de diseño no cuando la falla es provocada por otro motivo.

Correo Electrónico.

Aplicación que permite enviar mensajes a otros usuarios de la red.

Cracker

Es un individuo que con su conocimiento penetra los sistemas informáticos y destruye a su antojo los programas y la información.

DHCP

Son las siglas en inglés para Protocolo de configuración dinámica de host. Éste es un protocolo utilizado para que los equipos de una red local puedan obtener la configuración

predeterminada de la red (dirección IP, máscara, puerta de enlace y otros parámetros) de forma automática.

DNS (Domain Name System)

Es un conjunto de protocolos y servicios (base de datos distribuida) que permiten a los usuarios utilizar nombres en vez de tener que recordar direcciones IP numéricas. Ésta es ciertamente la función más conocida de los protocolos DNS: la asignación de nombres a direcciones IP.

Filtro de Contenido

Software que asegura que el uso de Internet sea utilizado para fines de Trabajo, Investigación y otros relacionados con el giro de la Institución, optimizando el uso del Ancho de Banda de Internet.

Firewall o Cortafuegos

Barrera de protección entre una red segura y otra insegura. Software de seguridad que se instala en un Servidor o Estación de Trabajo.

Firewall VPN Appliance

Software de seguridad que viene instalado en un equipo dedicado, destinado a filtrar protocolos de red de acuerdo a las políticas de seguridad de la Institución. Debe poder administrar Ancho de Banda y creación y administración de Redes Privadas Virtuales.

Gateway

Dispositivo para fines especiales que convierte la información de la capa de aplicación de un stack de protocolo a otro.

Hacker

Una persona que busca el conocimiento y la libre difusión de la información para su propia superación intelectual.

Hardware

Componentes electrónicos, tarjetas, periféricos y equipo que conforma un sistema de computación.

Http

Abreviación de la designación inglesa para Protocolo de transferencia de hipertexto. Se trata del protocolo más utilizado para transferir datos entre un servidor y otra máquina.

ID

Identificación.

ICMP (Internet Control Message Protocol)

Es un protocolo de control usado en el nivel de red. Este protocolo es usado principalmente por los Routers de Internet, para informar de sucesos inesperados, errores, etc. También se usa para hacer pruebas sobre la red (local o Internet), por ejemplo enviando un comando de petición de eco a un ordenador, y esperar que responda.

Intruso

Aquella persona que con una variedad de acciones intenta comprometer un recurso de hardware o software.

LAN

Red de datos de alta velocidad y bajo nivel de error, que cubre un área geográfica relativamente pequeña.

OWA

Es programa de correo electrónico incluido en Exchange que se ejecuta en su navegador. El concepto de OWA es similar al popular servicio de Hotmail, pero tiene el aspecto y muchas de las funciones. Con OWA, un usuario móvil puede iniciar una sesión en el servidor de Exchange con su nombre de usuario y contraseña, en todo lugar y momento, usando dispositivos como un equipo portátil y un teléfono móvil.

Palabra clave (password)

Contraseña, palabra de paso. Palabra o código utilizado para identificar a un usuario autorizado; es normalmente provisto por el sistema operativo o por un Sistema de Gestión de Base de Datos (SGBD). Las contraseñas sirven como una medida de seguridad contra el acceso no autorizado a los datos; de todos modos, la computadora sólo puede verificar la legitimidad de la contraseña y no la legitimidad del usuario.

Respaldo

Se refiere a una copia extra, de un archivo o base de datos.

Sistema de Prevención de Intrusos -Appliance.

Software de seguridad que viene instalado en un equipo dedicado, destinado a detectar posibles intrusiones y tomar contramedidas para que no afecten la integridad y seguridad de nuestra información.

SMTP - Simple Mail Transfer Protocol

Protocolo Sencillo de transferencia de correo. El protocolo con el que se transmite un mensaje de correo electrónico de una máquina a otra.

TCP/IP

Es un conjunto de protocolos de comunicaciones que definen cómo se pueden comunicar entre sí ordenadores de distinto tipo. El nombre proviene de dos de esos protocolos: el protocolo de control de la transmisión (TCP, Transmision Control Protocol) y el protocolo de inter-red (IP, Internet Protocol).

Usuario

Cualquier persona que utiliza una computadora. Por lo general se refiere a las personas que no pertenecen al personal técnico y que proporcionan entradas y reciben salidas de la computadora.

Validación

Es la prueba de un programa que se ejecuta en un ambiente no simulado (es decir con datos reales) para hallar su errores.

Vulnerabilidad.

Hardware o software que contiene bugs que permite su explotación potencial

BIBLIOGRAFÍA

1. Anónimo, "Máxima Seguridad en Internet" Editorial Anaya Multimedia. ISBN 84-41503-88-5.1988.
2. Bace, Rebecca. An Introduction to Intrusion Detection. Infideli Inc. for ICSA Inc. EEUU. 1999.
3. Cisco Systems. Cisco Networking Academies. Curriculum Online version 1.1
4. Ludwig, Mark A. The Little Black Book of Computer Viruses. Volume One. Electronic Edition. American Eagle Publication, Inc. ISBN 0- 929408-02-0.
5. Nombella San Jose, "Seguridad Informática". Editorial Paraninfo. ISBN 84-283 - 2341-0-España, 1996.
6. Parmar, S.K. "An Introduction to Security". ISBN 250 -748-5522.
7. PCM, "Tecnología de la Información, Código de Buenas Prácticas para la Gestión de la Seguridad de la Información" – NTP-ISO/IEC 17799:2004.
8. PCM, "Tecnología de la Información Procesos del Ciclo de Vida del Software" – NTP ISO/IEC 12207.
9. PCM, "Guía para la Administración Eficiente del Software Legal" – R.M. N° 073-2004 - PCM.