UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

FACULTAD DE CIENCIAS

Modelo de Seguridad Computacional para el Sistema Global de Información Académica y de Apoyo

TESIS

Que para obtener el título de

Licenciado en Ciencias Computacionales

presenta:

Alma Rocío Cabazos Marín

Ensenada, B.C. Febrero 1999

Agradecimientos

Gracias a Dios por concederme la vida y la fuerza para realizar este trabajo.

Gracias a mis padres por su tolerancia y amor en cada una de las etapas que me llevaron hasta esta meta.

Gracias a mi esposo por su apoyo, amor, aliento y comprensión durante todo el tiempo de mi trabajo.

Gracias a mi hija que es la inspiración y la alegría de mi vida.

Gracias a mi director de tesis Leopoldo Morán por su guía, apoyo y amistad brindados durante el desarrollo de este trabajo.

Gracias a mi asesora y amiga "Conchita" Mendoza quien me brindó su apoyo y motivación en la realización de esta tesis.

Gracias a mi asesor Dr. Jesús Favela por sus atenciones, a quien admiro por su dedicación en el área científica.

Gracias a quienes fueron mis maestros y me transmitieron su conocimiento durante mis estudios en esta Universidad.

Resumen

de la tesis de **Alma Rocío Cabazos Marín**
presentada como requisito parcial
para la obtención de la
Licenciatura en Ciencias Computacionales.

Ensenada, Baja California, México. Febrero 1999

Modelo de Seguridad Computacional para el

Sistema Global de Información Académica y de Apoyo.

Resumen Aprobado:

En este trabajo se desarrolló un Modelo de Seguridad Computacional -MSC- para el Sistema Global de Información Académica y de Apoyo -SGIAA-.

El MSC se desarrolló con base en la Metodología para Sistemas Suaves, considerando como aspectos relevantes el análisis de riesgos para determinar el nivel de seguridad requerido por cada uno de los recursos, y la implantación de medidas de prevención y de protección para la seguridad de dichos recursos, considerando como recurso relevante la información, de acuerdo a los objetivos del SGIAA.

El modelo propuesto establece un equilibrio entre seguridad y utilidad en el sistema. Considera tanto las necesidades del *factor humano* como los requerimientos del *factor técnico* para que el sistema sea productivo y confiable a la vez, evitando que una de estas dos características limite a la otra.

Alberto Leopoldo Morán y Solares.
Director de tesis

Contenido

VI. Desarrollo de las medidas de seguridad

Figuras

Tablas

I Introducción

1.1 Importancia de la Seguridad Computacional

Para la mayoría de los sistemas de cómputo, el interés en seguridad computacional es proporcional al grado de riesgo que corre su sistema (Dereck, 1993).

En algunas organizaciones es común encontrar computadoras que están en oficinas y laboratorios privados, sin embargo, corren el riesgo de ser accesadas por cualquier otra persona ajena al departamento. La recomendación más común es tener bajo llave la oficina o edificio y además se requiera de una clave de acceso para usar el sistema (Sun, 1994).

Actualmente, con el incremento del uso de redes locales y su interconexión a redes de cobertura amplia, la necesidad de establecer parámetros de seguridad se hace inminente (Camacho et. al., 1995).

Una gran cantidad de sistemas de cómputo están conectados a una red de cobertura mundial llamada Internet. Con estas conexiones al exterior se corre el riesgo de que cualquier usuario de un sistema de cómputo externo, desde

cualquier lugar del mundo, pueda entrar a nuestro sistema e irrumpir en él, aún cuando tengamos clave de acceso y el edificio esté cerrado bajo llave (Sun, 1994).

"A pesar de la importancia de la seguridad en un sistema de cómputo, es común todavía no prestarle la debida atención, no por falta de interés, sino que al ser un problema a veces 'oculto', es fácil que se vea opacado por el requerimiento incesante de otras tareas de la administración del sistema" (Camacho et. al., 1995).

La conciencia sobre este problema puede surgir temporalmente en caso de desastre o abuso en los recursos de computación. Sin embargo, es importante tener conciencia de los riesgos que amenazan al sistema y tomar las medidas de seguridad adecuadas antes de que éste o alguno de sus recursos se vean afectados (Sun, 1994).

1.2 Necesidad de un Modelo de Seguridad Computacional para el SGIAA

El propósito principal de este trabajo es desarrollar un modelo de seguridad computacional para el Sistema Global de Información Académica y de Apoyo.

"El Sistema Global de Información Académica y de Apoyo -SGIAA-, es un sistema que ha de implantarse en la Universidad Autónoma de Baja California, unidad Ensenada -UABC/uE- con la finalidad automatizar el manejo

de los bancos de información de docencia, investigación y difusión de la unidad Ensenada, bajo un ambiente integrado común, en el cual el acceso a los bancos de información sea en forma intra e interinstitucional utilizando la infraestructura de redes actual de la UABC/uE y su entorno" (Morán et.al.,1995).

Dada la importancia del papel que desempeña el SGIAA en el manejo de información, existe la necesidad de que el sistema sea confiable y satisfaga los requerimientos del usuario en el momento solicitado. Por ello es indispensable contar con un modelo de seguridad que respalde la integridad y funcionalidad del sistema (Sun, 1994).

Con el Modelo de Seguridad Computacional -MSC- para el SGIAA se pretende establecer las medidas de prevención y protección necesarias, considerando el nivel de riesgo que amenaza a dicho sistema en particular.

II Antecedentes

2.1 Aspectos históricos de seguridad computacional

El mundo de las computadoras ha cambiado drásticamente en los últimos años. Hace veinticinco años, la mayoría de las computadoras eran administradas de manera centralizada, estaban encerradas en cuartos y eran usadas por personal especializado y de confianza. Los riesgos eran mínimos y los daños al sistema estaban directamente relacionados con los usuarios internos. Estos daños se podían evitar fácilmente teniendo las puertas bajo llave y asignando cuentas para cada uno de los usuarios (Holbrook, et. al., 1991).

"Tradicionalmente la seguridad en computación se enfocaba a los aspectos de seguridad física y contra incendios, sin embargo, los riesgos que amenazan a los sistemas computacionales en la actualidad van más allá del aspecto físico" (Fine, 1990).

Por otro lado, las redes internacionales de computadoras han propiciado una apertura al intercambio de servicios entre sistemas de cómputo, influyendo

positivamente en la comunicación y el desarrollo de las empresas o instituciones conectadas. Desafortunadamente, hay quienes abusan de esta apertura accesando información confidencial o afectando de alguna manera el funcionamiento de los recursos, sin autorización, lo cual representa una amenaza a la integridad de los sistemas conectados. Los mecanismos técnicos y políticas de seguridad son indispensables para superar esta adversidad (Zamboni, 1995).

2.2 Conceptos básicos de seguridad computacional

Seguridad en computación se refiere a la prevención y protección en contra de:

a) acceso a la información por usuarios no autorizados;

b) alteración o destrucción de la información sin autorización.

La seguridad pretende resguardar la información confidencial del intento de acceso, alteración o destrucción, ya sea deliberado o no intencionado, por entidades no autorizadas. Los conceptos de seguridad, privacidad e integridad van ligados entre sí (Computing, 1995).

Un modelo de seguridad es el establecimiento formal de los aspectos intrínsecos de seguridad proporcionados por un sistema (Computing, 1995).

El análisis de riesgos se refiere a reconocer las amenazas y las vulnerabilidades que pueden afectar al sistema durante su desempeño (Computing, 1995). Tres preguntas son el punto de partida en el análisis de riesgos (Holbrook, 1991): ¿Qué se va a proteger?, ¿De qué se va a proteger? y ¿Cómo se va a proteger?.

a) *Qué se va a proteger.* El elemento vulnerable en un sistema computacional son los recursos del sistema (Derek, 1993), estos recursos se clasifican en tres partes:

- *Hardware.*
- *Software.*
- *Datos.*

b) *De qué se va a proteger.* Los riesgos que amenazan a cada uno de estos recursos son (Derek, 1993) :

- *Uso NO autorizado*
- *Cambios NO autorizados*
- *Destrucción.*

c) *Cómo se va a proteger.* Para reducir los riesgos que enfrenta cada uno de los recursos es necesario establecer medidas de seguridad, éstas se pueden resumir en dos grupos (Zamboni, 1995):

- *Políticas de seguridad.*
- *Mecanismos técnicos de protección.*

Se requiere que el SGIAA sea un sistema seguro a nivel intra e interinstitucional, por lo que es necesario contar con las medidas de seguridad adecuadas y la participación de las entidades que intervienen directa o

indirectamente en el sistema. Las tres entidades que participan en la seguridad de un sistema son (Zamboni, 1995):

- *Administradores del sistema,* implantando las medidas de seguridad.
- *Directivos de la institución,* apoyando dichas medidas.
- *Usuarios directos del sistema,* considerando las medidas establecidas cuando se dé uso al sistema.

Con base en lo anterior se desarrolla un modelo que considera estos conceptos y los resultados de la investigación de la problemática actual del sistema en estudio, SGIAA.

2.3 Objetivos

Objetivo General: Desarrollar un Modelo de Seguridad Computacional -MSC-, que establezca las medidas de seguridad que van a proteger a cada una de las partes que componen el SGIAA.

Objetivos Específicos:

- Identificar los riesgos que amenazan la seguridad en cada uno de los *recursos* del SGIAA (hardware, software, datos).
- Establecer las políticas de seguridad para los usuarios directos del sistema.
- Determinar los mecanismos técnicos de seguridad que permitan monitorear, controlar y evaluar periódicamente la seguridad del SGIAA.

III Metodología

3.1 Desarrollo del MSC con base en la Metodología para Sistemas Suaves

En la actualidad no existe una metodología establecida para el análisis y desarrollo de modelos de seguridad. El presente trabajo se desarrolló con base en la Metodología para Sistemas Suaves, MSS, (Checkland, 1993) ya que, puede adaptarse de manera flexible al estudio de cualquier sistema, asimismo permite conocer la problemática y resolverla con base en la situación real (Figura 1). La MSS considera un sistema de aprendizaje que utiliza ideas de sistemas para formular cuatro procesos: percibir (estadios uno y dos), predecir (estadios tres y cuatro), comparar (estadio cinco) y decidir sobre la acción a ejecutar (estadio seis). El resultado conduce a una situación cambiada (estadio siete) (Ramírez, 1996).

Estadio 1: Situación del problema: no-estructurado

En esta etapa se busca conocer la problemática actual, para ello se recurrió al análisis y recopilación de información necesaria para reconocer los distintos aspectos que afectan la seguridad del sistema.

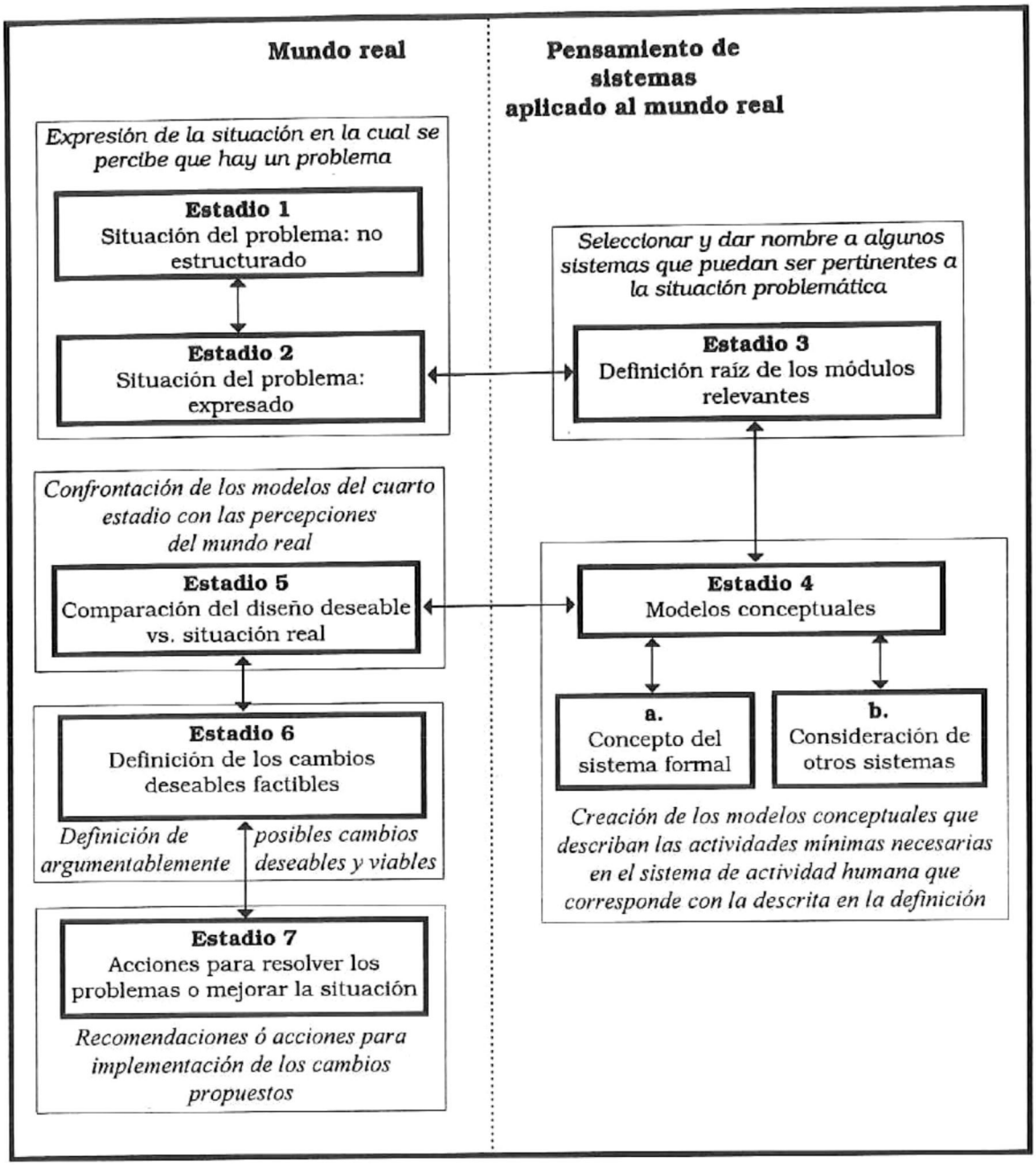


Figura 1. Estadios de la Metodología para Sistemas Suaves.

Los instrumentos empleados en esta primera etapa fueron:

- *Entrevista guiada,* aplicada al responsable de cada área de cómputo.
- *Cuestionarios,* se aplicaron a usuarios directos del sistema *(Anexo A).*
- *Consulta de Bibliografía especializada,* se empleó para el estudio de problemáticas similares de seguridad computacional, en distintos ambientes de cómputo.

Con dichos instrumentos se lograron identificar los problemas que existen en los siguientes aspectos:

- Infraestructura del SGIAA.
- Seguridad computacional del sistema actual.

Estadio 2: Situación del problema: expresado

El propósito de esta parte del trabajo fue construir un *modelo simbólico* que represente gráficamente la situación en la que se percibe el problema. La finalidad de este modelo es hacer explícitas las suposiciones hechas en el primer estadio mediante un diagrama. La ventaja de una exhibición pictográfica es que la información ahí contenida puede visualizarse en su conjunto, mientras que la información contenida en prosa sólo puede ser interpretada en serie. (Ramírez, 1996).

Además del "Modelo Simbólico de la problemática actual" se describen los riesgos a que se ve expuesto el sistema ante esta situación:

- Riesgos que amenazan al sistema.

Estadio 3: Definición raíz de los módulos relevantes

En esta etapa de la metodología, el objetivo es obtener una formulación explícita de algunos módulos que formarán parte relevante del modelo general, para resolver los problemas identificados o mejorar la situación actual.

Se identificaron y definieron como módulos relevantes:

- Diseño de los niveles de acceso a los recursos del sistema.
- Estructuración de las políticas de seguridad.
- Estructuración de los mecanismos técnicos de seguridad que deben aplicarse para la seguridad del SGIAA.

Estadio 4: Modelos conceptuales

En esta etapa se desarrolla cada uno de los módulos relevantes como modelo conceptual. El modelo conceptual es la descripción de las actividades que el módulo debe hacer para convertirse en el sistema nombrado en la definición. Es decir, el modelo conceptual describe qué actividad y en qué secuencia tiene que llevarse a cabo para que cumpla con la definición del módulo descrito. Los modelos conceptuales realizados son:

- Modelo conceptual del análisis de riesgos.
- Modelo conceptual para el diseño de los niveles de acceso a la información.
- Modelo conceptual del ciclo de vida de las políticas de seguridad.
- Modelo conceptual del ciclo de vida de los mecanismos técnicos de seguridad.

Estadio 5: Comparación del diseño deseable vs. situación real (4 vs. 2).

A este estadio se le denomina de *comparación* debido a que en él, la *situación problema* analizada en el segundo estadio se compara con los *modelos conceptuales* del cuarto estadio. Para el desarrollo de este trabajo, la comparación se realiza a través de una tabla (Ramírez, 1996) que contiene preguntas respecto a la actividad propuesta, los resultados al cuestionamiento, la valoración de dichos resultados y la posible solución a la problemática (Tabla I).

Actividad	Existe o no	Mecanismo presente	Valoración	Cambio propuesto
... *(Lista de actividades conforme al modelo* conceptual*)*	... *(Existe dicha actividad o no)*	... *(Cómo se realiza actualmente dicha actividad)*	... *(Valoración del mecanismo presente con base en los riesgos)*	... *(sugerencia de cambios para minimizar riesgos)*

Tabla I Formato de la tabla de comparación del diseño deseable vs. situación real.

Estadio 6: Definición de los cambios deseables factibles.

Las comparaciones de la etapa anterior dieron como resultado un conjunto de recomendaciones o *cambios propuestos.* Los cambios deben ser

deseables y factibles para los interesados en la situación problemática, para ello fue necesario establecer estos cambios con el acuerdo de las personas que se encuentran involucradas en la situación problemática y quieren hacer algo al respecto. Los cambios propuestos son establecer las siguientes medidas de seguridad:

- Políticas de seguridad para el SGIAA.
- Mecanismos técnicos de seguridad a aplicarse en el SGIAA.
- Modelo general de Seguridad Computacional para el SGIAA.

Estadio 7: Acciones para resolver los problemas o mejorar la situación.

En esta etapa se presenta una *lista de recomendaciones,* que se consideran adecuadas para resolver los problemas más comunes de Seguridad Computacional, y en particular se hacen recomendaciones para minimizar los riesgos en el SGIAA.

3.2 Área de estudio

El área de estudio para el presente trabajo son los departamentos y unidades académicas, de investigación y de desarrollo que se consideran en el

Sistema Global de Información Académica y de Apoyo, las cuales se listan en la Figura 2.

Departamentos	• Departamento de Asuntos Académicos. • Departamento de Extensión Universitaria. • Departamento de Investigación y Posgrado. • Departamento de Vinculación y Egresados.
Unidades Académicas, de Investigación y Desarrollo	• CECUUE, Centro de Cómputo Universitario Unidad Ensenada. • Facultad de Ciencias • IIO, Instituto de Investigaciones Oceanológicas.

Figura 2 Departamentos y Unidades Académicas evaluadas.

3.3 Aspectos evaluados

Con ayuda de los *cuestionarios* se evaluaron los aspectos de seguridad computacional que se listan en la Figura 3. En las *entrevistas guiadas* se investigaron aspectos de infraestructura, seguridad a nivel intra e internet, y se consideraron las experiencias de la administración con respecto a problemas de seguridad.

Aspectos Evaluados	• Características del Equipo. • Calidad de Claves de acceso. • Virus Informáticos en el sistema. • Respaldo de Información. • Políticas de Seguridad que se aplican. • Medidas de Seguridad en transacciones de información con el exterior de la red.

Figura 3 Aspectos considerados para la evaluación.

IV. Seguridad Computacional del Sistema de Cómputo UABC/uE

4.1 *Estadio 1:* Situación del problema: no estructurado

En esta primera etapa se realizó el análisis de la infraestructura y la seguridad computacional de la red actual (Marzo 96), con la finalidad de conocer los problemas de seguridad existentes en el sistema. Los resultados de este análisis se presentan a continuación.

4.1.1 Infraestructura del SGIAA.

El SGIAA ha de implantarse sobre la infraestructura de redes actual de la UABC/uE, los mecanismos técnicos de seguridad deben considerar las características de la misma.

a. Descripción general de los sistemas en red y sus conexiones.

La red UABC/uE emplea la tecnología Ethernet, usando los protocolos *IPX/SPX (Internetwork Packet eXchange / Sequenced Packet eXchange)* y *TCP/IP (Transmision Control Protocol / Internet Protocol)*. La red UABC/uE es una red heterogénea, los sistemas que emplea se describen en la Tabla II.

Sistema	Unidades
HP-9000 (HP-UX)	3
SUN (Solaris, Sun Os)	
SPARC 20	6
SPARC 2	1
SPARC Server	1
Servidores PC's X86 (Free BSD)	10
Servidores Pentium, Vectra, SLC3,(Novell)	10
Estaciones de trabajo PC's X86	+400
Macintosh	2
HP-3000	1
Enrutadores	1

Tabla II Descripción de los sistemas con que cuenta actualmente la red UABC/uE.

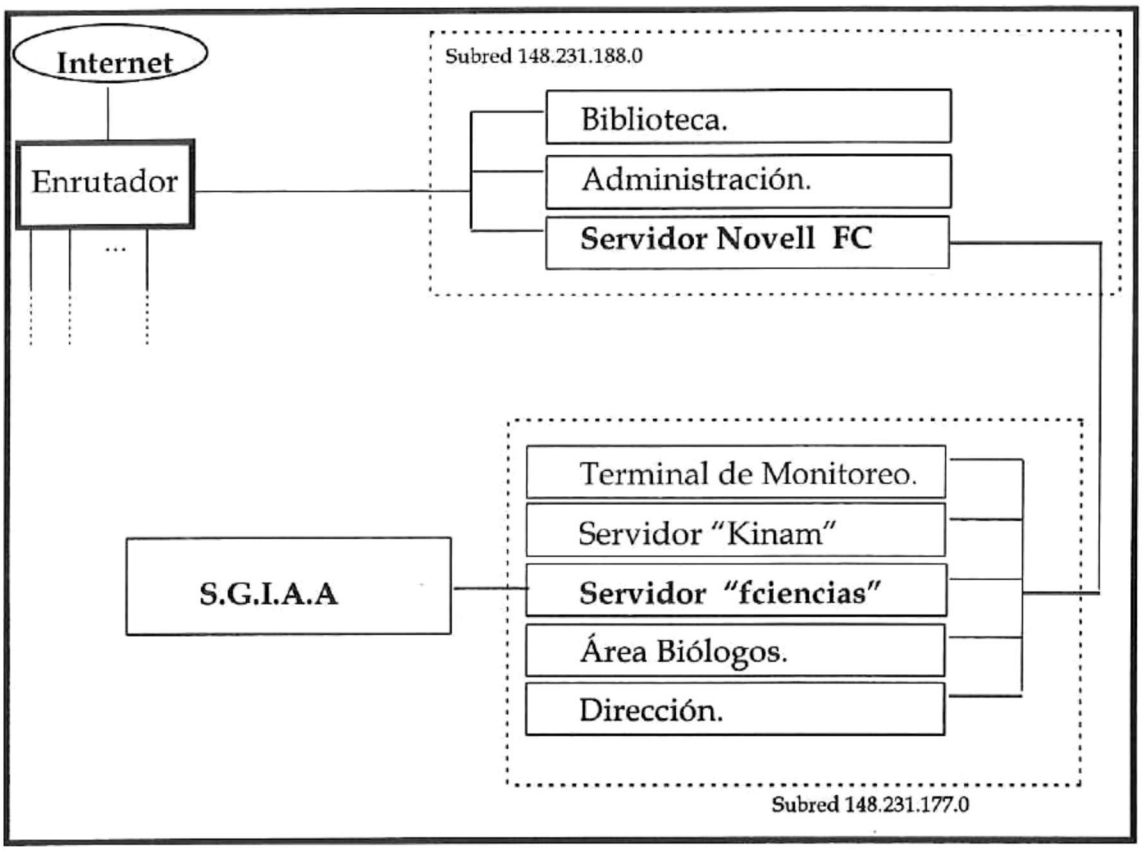


Figura 4 Ubicación del SGIAA en la red UABC/uE.

La ubicación del SGIAA en la red (Figura 4), se describe de acuerdo a los mapas y la información proporcionados por los administradores de la red.

Se hace una descripción general de las conexiones entre los edificios de la UABC/uE, éstos se conectan entre sí mediante fibra óptica. Las conexiones internas son con cable coaxial o mediante par trenzado. Sus conexiones al exterior, se hacen vía microondas.

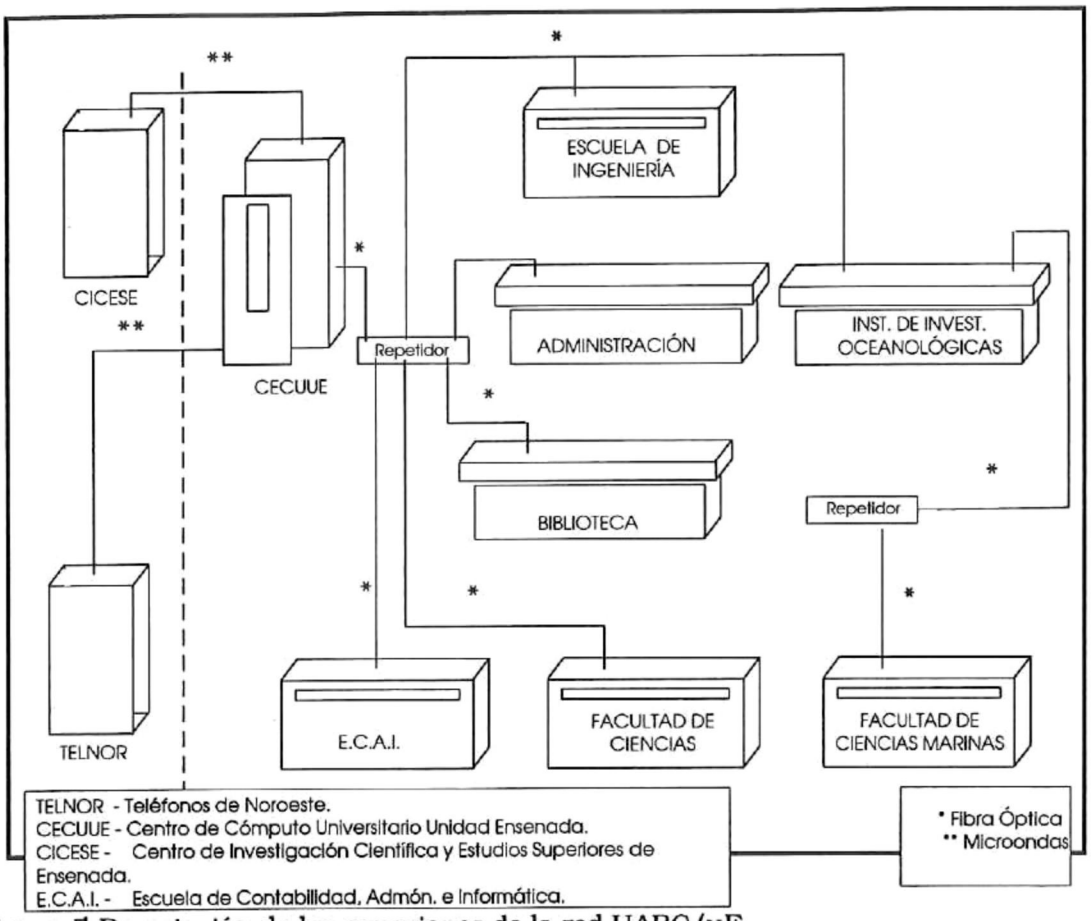


Figura 5 Descripción de las conexiones de la red UABC/uE.

La red UABC/uE está registrada con el número de Internet 148.231.0.0, su dominio es *ens.uabc.mx*. Se conecta a las subredes de las unidades de Mexicali, Tijuana y Tecate ; siendo la salida principal a Internet por la subred en Mexicali, mediante una línea privada rentada a *Teléfonos del Noroeste*, (TELNOR). Cuenta con una salida de respaldo a través de CICESE, vía microondas.

b. Características básicas del equipo

Uno de los aspectos importantes que deben considerarse para que un sistema sea confiable es que el equipo esté en buenas condiciones, y cuente con las características necesarias para satisfacer los requerimientos de las aplicaciones que se van a utilizar.

En la presente etapa se hizo el estudio del equipo con que cuenta cada departamento y la aplicación que se le da a dicho equipo. Los resultados se presentan en las Tablas III-XI. Además de contar con el equipo adecuado, otro aspecto importante es el mantenimiento del equipo. El mantenimiento abarca aspectos preventivos, correctivos y de actualización, tales como, limpieza de los componentes del equipo, revisión, reparación o sustitución de dispositivos y software que presenten fallas (aún cuando dichas fallas aparenten ser poco relevantes), actualización de equipo y software, antes de que éstos sean obsoletos para los requerimientos del departamento o unidad.

El mantenimiento periódico del equipo previene el riesgo de que repentinamente el equipo falle por causas que podrían haberse evitado oportunamente. Los resultados de este estudio se presentan en la Tabla XII.

Departamento de Asuntos Académicos /uE		
Máquina	**1AA**	**2AA**
Tipo	PC	PC
Procesador	486DX	386
Capacidad Disco Duro	80 MB	40 MB
RAM	7MB	4 MB
Servidor	No conectada a red	CECUUE-4
Sistema Operativo y Versión	MS-DOS v.6.22	MS-DOS v.6
Función del equipo	• Control de plantas docentes. • Cursos de Asuntos Académicos. • Edición de textos.	• Manejo de base de datos. • Edición de textos.

Máquina	**3AA**
Tipo	PC
Procesador	386
Capacidad D.D.	40 MB
RAM	4 MB
Servidor	CECUUE-4
Sistema Operativo y Versión	MS-DOS v.6
Función del equipo	• Manejo de base de datos. • Elaboración de oficios. • Edición del material de diplomados y talleres.

Tabla III Descripción básica del equipo del Departamento de Asuntos Académicos/uE.

Departamento de Extensión Universitaria /uE		
Máquina	1EX	2EX
Tipo	PC	PC
Procesador	486	486
Capacidad Disco Duro	80 MB	80 MB
RAM	2 MB	8 MB
Servidor	No conectada a red	No conectada a red
Sistema Operativo y Versión	MS-DOS v.6.22	MS-DOS v.5
Función del equipo	• Elaboración de documentos administrativos. • Diseño gráfico. • Diseño de formatos.	• Planta docente. • Manejo del sistema académico. • Diseño de publicidad.

Tabla IV Descripción básica del equipo del Departamento de Extensión Universitaria unidad Ensenada.

Departamento de Investigación y Posgrado /uE		
Máquina	1IP	2IP
Tipo	PC	PC
Procesador	486DX	486DX
Capacidad Disco Duro	80 MB	80 MB
RAM	8 MB	8 MB
Servidor	CECUUE-6	CECUUE-1, CECUUE-2, CECUUE-4
Sistema Operativo y Versión	MS-DOS v.6.22	MS-DOS v.6.22
Función del equipo	• Alimentar base de datos del sistema de Investigación y Posgrado. • Elaboración de tablas.	• Desarrollo de sistemas. • Consulta a base de datos del sistema de Investigación y Posgrado.

Tabla V Descripción básica del equipo del Departamento de Investigación y Posgrado /uE.

Departamento de Vinculación y Egresados /uE		
Máquina	1VE	2VE
Tipo	PC	PC
Procesador	386	486
Capacidad Disco Duro	No tiene disco	No tiene disco
RAM	3 MB	3 MB
Servidor	HP-3000	CECUUE
Sistema Operativo y Versión	MS-DOS v.5	MS-DOS v.5
Función del equipo	• Actualización del padrón de egresados. • Elaboración de credenciales. • Radiotón.	• Sistema de bolsa de trabajo. • Padrón de la asociación de egresados estatal. • Elaboración de oficios.

Tabla VI Descripción básica del equipo del Departamento Vinculación y Egresados /uE.

CECUUE, Centro de Cómputo Universitario Unidad Ensenada (Servidores Novell)		
Máquina	CECUUE-1	CECUUE-2
Tipo	Servidor	Servidor
Procesador	Pentium	Pentium
Cap. Disco Duro	2 GB	3 GB
RAM	64 MB.	64 MB
Nodos	85	98
S. O. Versión	Novell 3.11	Novell 3.11
Función del equipo	• Servidor del *tercer nivel de las instalaciones de CECUUE.*	• Servidor del *segundo nivel y sala B de las instalaciones de CECUUE.*
Máquina	CECUUE-3	CECUUE-4
Tipo	Servidor	Servidor
Procesador	SLC3	Vectra 28
Cap. Disco Duro	2 GB	1 GB
RAM	64 MB	28 MB
Nodos	58	28
S. O. Versión	Novell 3.11	Novell 3.12
Función del equipo	• Servidor del *Instituto de Investigaciones Oceanológicas.*	• Servidor del *área administrativa y área académica.*
Máquina	CECUUE-5	CECUUE-6
Tipo	Servidor	Servidor
Procesador	Vectra 16	Vectra 28
Cap. Disco Duro	1.5 GB	1 GB
RAM	16 MB	28 MB
Nodos	62	28
S. O. Versión	Novell 3.12 (50)	Novell 3.11
Función del equipo	• Servidor de la *sala A y sala C del CECUUE.*	• Servidor de uso indeterminado. (se emplea eventualmente para: cursos, talleres, etc.).

Tabla VII Descripción básica de los servidores Novell en CECUUE.

Dirección de la Facultad de Ciencias /uE		
Máquina	1FC	2FC
Tipo	PC	PC
Procesador	286	386
Capacidad Disco Duro	20 MB	40 MB
RAM	4MB	4 MB
Servidor	No conectada a red	No conectada a red
S. O. Versión	MS-DOS v.5	MS-DOS v.5
Función del equipo	• Edición de documentos.	• Edición dedocumentos.

Máquina	3FC
Tipo	PC
Procesador	386
Capacidad D.D.	40 MB
RAM	4 MB
Servidor	No conectada a red
S. O. Versión	MS-DOS v.5
Función del equipo	• Horarios de planta docente. • Edición de textos. • Diseño gráfico.

Tabla VIII Descripción básica del equipo de la Dirección de Facultad de Ciencias /uE.

Aula Equipada de la Facultad de Ciencias /uE		
Máquina	1AFC	2AFC
Tipo	PC	PC
Procesador	486	486
Capacidad Disco Duro	20 MB	20 MB
RAM	4MB	4 MB
Servidor	FC	FC
S. O. Versión	MS-DOS v.6	MS-DOS v.6
Función del equipo	• Laboratorio de computación para alumnos, maestros e investigadores de la Facultad.	• Laboratorio de computación para alumnos, maestros e investigadores de la Facultad.

Máquina	3AFC
Tipo	PC
Procesador	Pentium
Capacidad D.D.	40 MB
RAM	4 MB
Servidor	FC
S. O. Versión	MS-DOS v.6
Función del equipo	• Laboratorio de computación para alumnos, maestros e investigadores de la Facultad.

Tabla IX Descripción básica del equipo del Aula Equipada de la Facultad de Ciencias /uE.

Servidores de la Facultad de Ciencias		
Máquina	PC	KINAM
Tipo	Servidor	Servidor
Procesador	Pentium	SPARC
Cap. Disco Duro	8 GB	2 GB
RAM	16MB	MB
S. O. Versión	Novell Netware 3.11	UNIX Solaris
Función equipo	• Servidor Novell del aula equipada, sala de maestros y área de biología.	• Servidor UNIX del aula equipada, sala de maestros y área de Biología..
Máquina	FCIENCIAS	COLECCIONES
Tipo	Servidor	Servidor
Procesador	Pentium	HP Vectra 486
Cap.Disco Duro	1.2 GB	2 GB
RAM	32 MB	16MB
S. O. Versión	Free BBD 2.1.5.	Novell Netware 3.11
Función equipo	• Servidor del SGIAA.	• Servidor para consulta de base de datos de colecciones científicas de la Facultad de Ciencias

Tabla X Descripción básica de los servidores de la Facultad de Ciencias /uE.

IIO, Instituto de Investigaciones Oceanológicas			
Máquina	SERVIDOR-IIO	2IIO	3IIO
Tipo	Servidor	PC	PC
Procesador	486	486	Pentium
Capacidad D.D.	1.5 GB	16 MB	2 MB
RAM	16 MB	8 MB	8 MB
S. O. Versión	Novell 3.11	MS-DOS v.6	SERVIDOR-IIO
Función equipo	• Servidor del IIO.	• Apoyo para la Investigación.	
Máquina	4IIO	5IIO	
Tipo	PC	PC	
Procesador	386	486	
Cap. Disco Duro	2 MB	2 MB	
RAM	8 MB	8 MB.	
Servidor	SERVIDOR-IIO	SERVIDOR-IIO	
S. O. Versión	MS-DOS v.5	MS-DOS v.6.2	
Función equipo	• Apoyo para la investigación.	• Base de datos, diseño, edición de textos y uso de servicios de red.	
Máquina	6IIO	7IIO	
Tipo	PC	PC	
Procesador	486	Pentium	
Cap. Disco Duro	2 MB	1 GB	
RAM	6 MB.	16 MB	
Servidor	SERVIDOR-IIO	SERVIDOR-IIO	
S. O. Versión	MS-DOS v.5	MS-DOS v.6.2	
Función del equipo	• Captura de texto y diseño de revista especializada.	• Apoyo para la investigación.	

Tabla XI Descripción básica del equipo del IIO.

Departamento	Asuntos Académicos			Extensión Universitaria		Investigación y Posgrado		Vinculación	
Máquina	1AA	2AA	3AA	1EX	2EX	1IP	2IP	1VE	2VE
Responsables del mantenimiento	CECUUE			CECUUE		CECUUE		CECUUE	
Periodicidad del mantenimiento	Se da mantenimiento cada vez que hay problemas con el equipo.					Semestral.		Se da mantenimiento cada vez que hay problemas con el equipo.	
Periodicidad en la actualización del equipo	Cada vez que sea necesario y en la medida que lo permita el presupuesto.					Semestral.		Cada vez que sea necesario.	

Departamento	Cecuue						Facultad de Ciencias			IIO						
Máquina	CEC-1	CEC-2	CEC-3	CEC-4	CEC-5	CEC-6	1FC	1FC	1FC	SIIO	2IIO	3IIO	4IIO	5IIO	6IIO	7IIO
Responsables del mantenimiento	CECUUE						Aula Equipada de la Facultad de Ciencias.			CECUUE						
Periodicidad del mantenimiento	Semestral						Semestral			Se da mantenimiento cada vez que hay problemas con el equipo						
Periodicidad en la actualización del equipo	Cada vez que sea necesario y en la medida que lo permita el presupuesto.															

Tabla XII Mantenimiento del sistema UABC /uE (Muestra: 25 máquinas).

4.1.2 Seguridad computacional del sistema actual

Durante esta etapa se investigaron cuales eran las medidas de seguridad que se aplican actualmente, en las áreas de cómputo conectadas a la red UABC/uE. Se analizaron las áreas de cómputo pertenecientes a aquellos departamentos y unidades académicas descritas en la Figura 2.

Actualmente, el sistema en red de la UABC/uE, no cuenta con una política global de seguridad establecida. Los mecanismos técnicos de seguridad existentes en el sistema son insuficientes comparados con la cantidad de riesgos que lo amenazan.

En esta etapa se aplicaron encuestas a los usuarios del sistema, considerando los departamentos y unidades académicas, de investigación y desarrollo especificados, así mismo, se llevaron a cabo entrevistas con los responsables de cada área del sistema de cómputo para tener una visión general de sus características y su estado actual. Los resultados de este análisis se describen a continuación.

a. Calidad de Claves de Acceso

La clave de acceso, "password", de los sistemas de cómputo fue creada con el fin de tener control sobre el acceso al sistema, brindando, en cierta medida, privacidad a la cuenta del usuario y evitando riesgos de intrusión por parte de usuarios ajenos a la cuenta, quienes pudieran enmascararse para

realizar actividades mal intencionadas, para experimentar o para beneficiarse accesando información o recursos sin autorización.

La calidad de una clave de acceso es tan importante como el hecho de que ésta exista. Si una clave es poco sofisticada, entonces se corre el riesgo de que sea descubierta por intrusos que se dedican a romper barreras de seguridad para ganar acceso a los recursos de los sistemas. Por ejemplo, si la calidad del password es pobre y se conoce el nombre de la cuenta, "*login name*", bastaría teclear algunas palabras, ya sean relacionadas con el nombre de la cuenta, datos ó nombres relevantes para el propietario o expresiones populares, para adivinar la clave. Intrusos expertos en la ruptura de claves encuentran más sencillo el empleo de programas dedicados a generar entradas para password, el programa prueba con palabras de diccionario, frases populares, algunas combinaciones y permutaciones de éstas, hasta coincidir con la clave de entrada.

Los usuarios del sistema en red UABC/uE, no aplican ninguna estrategia de seguridad en la elección de su password, se presentan los resultados del análisis realizado al respecto en las Tablas XIII y XIV. Este análisis está basado en los parámetros de un estudio realizado por Daniel V. Klein en Carnegie Mellon University, de Pittsburg (Klein, 1991).

La información fue obtenida mediante una encuesta *(Anexo A)*, la muestra fue tomada aleatoriamente entre los usuarios directos del sistema. La valoración de los resultados se realiza posteriormente, en el punto 4.2.2. de este capítulo.

Características de Passwords vulnerables	Frecuencia	Porcentaje
Basado en el nombre de su cuenta de usuario	2	2.859 %
Está basado en sus iniciales o nombre	8	11.429 %
Nombres comunes o de lugares.	12	17.145 %
Palabras de diccionario	4	5.716 %
Palabra conjugada	1	1.429 %
Secuencia de caracteres según el patrón del teclado	1	1.429 %
Secuencia de solo números	4	5.716 %
No contiene mayúsculas y minúsculas mezcladas	10	14.287 %
No contiene números y letras mezcladas	6	8. 565 %
No contiene letras y puntuaciones mezcladas	12	17.145 %
Combinación de letras y números a semejanza de placas de auto	4	5.716 %
Total de passwords vulnerables	**64**	**91.436%**
No entran en esta clasificación	**6**	**8. 564%**
Total de muestras	**70**	**100 %**

Tabla XIII Resultados de la evaluación de calidad de passwords.

Longitud de password	Frecuencia	Porcentaje
- de 3 Caracteres	0	0 %
4 Caracteres	8	12.5 %
5 Caracteres	0	0 %
6 Caracteres	20	31.25 %
7 Caracteres	32	50%
8 Caracteres	0	0 %
+ de 8 Caracteres	4	6.25%
Total de muestras	**64**	**100%**

Taba XVI Evaluación de la longitud de password.

b. Virus Informáticos en el sistema

La existencia de los virus informáticos fue postulada teóricamente por Von Neumann a fines de los años cuarenta en su libro *Theory and Organization of Complicated Automata*. Sin embargo, los virus de computadora aparecieron mucho después. En 1983 Fred Cohen experimentó con virus en su laboratorio de

investigación y en 1984 hubo incidentes aislados con virus en computadoras Apple II . Los virus informáticos existen virtualmente en todas las arquitecturas computacionales, desde la ubícuita PC hasta los sistemas UNIX y los mainframes IBM (Mallén-Fullerton, 1995).

"La palabra virus es un término biológico que se refiere a una núcleo - proteína submicroscópica conocida por su habilidad para invadir una célula huésped, alterar su DNA para producir más de su propio núcleo - proteína, y finalmente, libera estas nuevas versiones de sí misma para invadir células de los alrededores. Haciendo una analogía de un virus computacional con uno del mundo de la biología, muchas de las propiedades en los estados o fases de un virus biológico son idénticas a aquellas de un virus computacional" (Dereck, 1993). Las fases de los virus biológicos e informáticos se contrastan en la Tabla XV, destacando las analogías entre ambos.

El nombre de virus informático se debe al paralelo que existe entre los virus biológicos y los computacionales. "Se encuentra que los virus biológicos invaden las células del cuerpo y utilizan sus recursos para reproducirse. De manera similar, los virus de computadora se alojan en los programas y usan los recursos ordinarios del sistema para reproducirse. Así mismo, existen tanto virus computacionales como biológicos que producen enormes daños mientras que hay otros que podemos considerar como benignos.

Fases	Virus Biológico	Virus computacional
Contagio	El virus (núcleo - proteína) puede ser contagiado mediante algún vector, este vector es el transmisor del virus desde un agente infeccioso a un huésped receptivo. El aire, contacto físico, comida y agua, son los vectores más comunes.	El virus (segmento de código) se esparce entre sistemas de computadoras mediante algún vector. Cualquier forma de intercambio de información puede ser usada como vector para esparcir un virus. Estos pueden ser discos flexibles, cintas y, más notablemente, una red de computadoras.
Infección	El virus invade las células del huésped. Inserta su DNA en el DNA de la célula invadida.	El virus se adhiere a un programa del sistema, insertando su código en el código del programa invadido.
Activación	Las porciones de DNA son insertados por el virus sólo en sitios receptores del DNA de la célula. Si la célula no usa ese segmento de su DNA , entonces el virus se considera como durmiente. Sólo cuando condiciones externas causan que la célula use el segmento infectado entonces el virus se vuelve activo replicándose a sí mismo.	La fase de activación está codificada e insertada en el código del programa huésped. Esto significa que cuando el programa huésped es ejecutado el virus necesita ser llamado para su activación, y luego retornar a la programación original del huésped para evitar ser detectado.
Replicación	Una vez activado, el virus usa los recursos de la célula para replicarse a si mismo. Comúnmente esto degrada la ejecución de la célula. Si el virus usa demasiados recursos, la célula puede dañarse ó romperse. Las consecuencias de éste daño son la razón por la que el sistema invadido se ve afectado.	En esta fase el virus usa los recursos del huésped para crear copias de sí mismo. Los daños que causa son aquellos programados en su código.

Tabla XV Descripción de analogías entre las fases de un virus biológico y un virus computacional (resumido de: Dereck, 1993).

Otro fenómeno que nos hace notar las similitudes de ambos tipos de virus es el hecho de que hay mayor número de infecciones entre las personas 'promiscuas', al igual que quienes intercambian programas y discos indiscriminadamente -promiscuidad informática - tienen mayores problemas con virus informáticos." (Mallén-Fullerton, 1995).

En la lucha contra los virus se han creado diversos programas "antivirus", los cuales detectan y eliminan sólo a virus conocidos, por lo que los de nueva creación son pasados por alto. Hasta la fecha, no es posible inmunizar completamente un sistema, sin embargo, se realizan investigaciones al respecto (Mallen-Fullerton, 1995).

Los beneficios que proporcionan los actuales antivirus se están viendo opacados, básicamente, "por el rápido crecimiento del número de virus diferentes en circulación y debido a la conducta de los usuarios, que no llevan a la práctica las medidas preventivas recomendadas" (Mallén-Fullerton, 1995).

Para evaluar la problemática de virus informáticos en el sistema en red UABC/uE se realizó una "auditoría antivirus", en dicha auditoría se revisaron los sistemas empleando los antivirus F-PROT y Scan de McAfee, para detectar si había virus, y se aplicó un cuestionario al responsable de cada computadora *(Anexo)*, los resultados se presentan en la Tabla XVI.

Depto. ó Unidad Acad.	PC's Independientes	PC's en red	Antivirus Residente	Periodicidad de Búsqueda	Máquinas Infectadas
Asuntos Académicos	3	Ninguna	NO	CUANDO HAY SOSPECHA	0%
Extensión Universitaria, Centro de Idiomas	2	Ninguna	NO	CUANDO HAY SOSPECHA	0%
Extensión Universitaria, Vinculación y Posgrado	Ninguna	2	NO	CUANDO HAY SOSPECHA	0%
Facultad de Ciencias, Dirección.	4	Ninguna	SI	SÓLO EN DISCOS EXTERNOS	0%
Facultad de Ciencias, Aula Equipada.	Ninguna	5	NO	CADA VEZ QUE SE ACCESE AL SISTEMA	0%
Facultad de Ciencias, Cubículos.	2	2	NO	NINGUNA	1%
Investigación y Posgrado	Ninguna	2	NO	CUANDO HAY SOSPECHA	0%
Instituto de Investigaciones Oceanológicas	Ninguna	10	NO	CUANDO HAY SOSPECHA	20%

Tabla XVI Resultados de la auditoría "antivirus" en las áreas de cómputo en estudio (los números representan el tamaño de la muestra).

c. Respaldo de Información

El usuario guarda sus archivos en el sistema esperando que éstos se mantengan *íntegros*. La integridad de cualquier archivo se ve amenazada por cambios o destrucción, causados por errores del sistema ya sean de hardware o software, o por los usuarios que intervienen en el sistema, incluso el propietario del archivo, pueden causar daño a la información, intencional o accidentalmente. Considerando que los errores ocurren en cualquier momento,

la administración del sistema debe actuar de manera preventiva al respecto. La prevención, en este caso, consiste en que siempre exista una copia de respaldo de la versión reciente de los archivos en el sistema.

Se aplicó un cuestionario a los responsables de cada área[1] del sistema UABC/uE. Los resultados de este análisis están descritos en las Tablas XVII y XVIII.

	Asuntos Académicos	Extensión Universitaria	Investigación y Posgrado	Vinculación y Egresados
Forma en que se respalda la información	Total (en discos flexibles)	Incremental (en discos flexibles)	Total (en discos flexibles)	Total (en Mexicali)
Información que se respalda	Datos	Programas, Datos y Proyectos	Datos, oficios, tablas y Programas del sistema	Datos
Periodicidad de los respaldos	Semestral	Cuando se considere necesario	Semanal (datos) mensual (progrs.)	Diaria (incremental) y Semanal (Total)
Tiempo que se conserva el respaldo	Años	Años	Meses	Meses

Tabla XVII Descripción de los procesos de respaldo por departamento.

	CECUUE (Admon.)	Facultad de Ciencias (Direccion)	IIO
Forma en que se respalda la información	Total Disco Duro	Parcial (en discos flexibles)	Parcial (en discos flexibles)
Información que se respalda	Directorios, Datos y programas.	Datos y Cartas	Datos y Programas del sistema
Periodicidad de los respaldos	Diario (Directorios y Datos)	Cuando se considere necesario	Cuando se considere necesario
Tiempo que se conserva el respaldo	Indefinido	Indefinido	Meses

Tabla XVIII Descripción de los procesos de respaldo por unidad académica.

[1] Se consideran sólo las áreas en estudio, descritas en la Figura 2, Capítulo III.

d. Políticas que se aplican

La finalidad de las políticas de seguridad es establecer las medidas, específicamente operacionales, que han de ser tomadas para proteger el sistema de cualquier acción que intente violar su seguridad e integridad (Computing, 1995).

- Política o Reglamentos

El sistema computacional actual en red de la UABC/uE no tiene una política global establecida, cada una de las áreas equipadas con un sistema de cómputo ha implantado sus propias reglas de seguridad computacional de acuerdo a experiencias en el departamento o unidad académica. La política que prevalece en la mayoría de los departamentos es mantener el área de cómputo bajo llave cuando no hay nadie que se haga responsable de ella.

Hasta el momento del presente estudio, el Aula Equipada de la Facultad de Ciencias fue el único sitio donde existe un reglamento para el usuario, más no es un reglamento específico en aspectos de seguridad.

- Políticas para uso del Hardware

En la mayoría de los departamentos se considera que cada usuario es responsable del equipo que maneja, de los recursos que emplea y de las aplicaciones que le da al sistema.

- Políticas para uso del Software

No existe una política que exija la instalación de paquetes de software original. La adquisición de programas originales para cada departamento no es económicamente factible, por lo que los programas originales adquiridos se conservan en CECUUE o en las distintas aulas equipadas de cada escuela o facultad, así los departamentos pueden solicitar el original a estas unidades cada vez que se requiera la instalación de un paquete.

Con respecto a las Bases de Datos no todas requieren de clave de acceso para ser ejecutadas, siendo que muchas de estas Bases de datos tienen información confidencial para el departamento o unidad académica.

- Políticas de aplicación

Es común que en los departamentos existan paquetes de software sin relación alguna con el trabajo que se realiza (por ejemplo: juegos, imágenes,etc.) No hay una regla que establezca que tipo de aplicaciones son permitidas en cada departamento, por ello el usuario puede instalar y usar lo que él guste, aún cuando se vea afectado el espacio en disco y sus horas de trabajo.

e. Medidas de seguridad en transacciones al exterior

La UABC mantiene relación con diversas instituciones externas a través de Internet, algunas de estas transacciones se describen en la Tabla XIX. Estas transacciones se consideran de alto riesgo, ya que se trata de información

confidencial, la cual podría ser interceptada en su trayecto por algún experto en intrusión.

Además de las transacciones señaladas en la Tabla XIX, están las que realizan otros usuarios, los cuales sirviéndose de Internet pueden enviar y recibir toda la información que requieran (vía *ftp, e-mail, navegador de Internet,* etc.), sin embargo hay que considerar que una vez que se recibe y almacena la información, ésta ocupará un espacio en la memoria secundaria del sistema, por lo tanto debe existir un control, no en contenido de la información, ya que con ello se violaría la confidenciabilidad; sino en cantidad de información, asignando al usuario una cantidad limitada de espacio en memoria, de acuerdo a su función en el sistema.

Otro aspecto importante de interacción con el exterior es el uso que se da a la red UABC/uE desde un sistema remoto mediante los servicios de *telnet, rlogin* y *ftp* los cuales se encuentran activados sin restricciones, beneficiando al usuario externo y arriesgando en el mismo grado al sistema de red local. Estas funciones permiten al usuario externo trabajar en el sistema UABC/uE, con los mismos derechos de un usuario interno, lo cual sería una ventaja tanto para un alumno que trabaja en su cuenta desde su casa, como para un intruso que logra entrar a una cuenta ajena y explotar los recursos a su conveniencia.

Departamento que hace la transacción	Institución con la que se hace la transacción	Transacción	Riesgo
Instituto de Investigaciones Oceanográficas	Instituciones Educativas Superiores alrededor del mundo	Recepción de artículos de fondo para la revista vía e-mail. (sin encriptación)	Se pone en riesgo los derechos de autor de los colaboradores, ya que la información puede ser interceptada en el trayecto.
Vinculación	UABC, Mexicali	Envío de los datos de egresados para actualizar la Base de Datos de Egresados en Mexicali. (sin encriptación)	La información viaja sin protección, los datos son relevantes y confidenciales.

Tabla XIX Transacciones de información al exterior de la red.

Actualmente no se emplea ningún tipo de protección de la información que viaja a través de la red, ni se protege al sistema de la información que se recibe.

Con esto se concluye la identificación de la problemática actual la cual es resumida en el siguiete estadio.

4.2 *Estadio* 2: Situación del problema expresado

En esta segunda etapa se pretende expresar, de forma gráfica, la problemática del sistema actual. Considerando los resultados obtenidos en el estadio anterior se identifican los riesgos a los que se enfrenta el sistema actual y se elige una representación gráfica de la situación, con el fin de dar a conocer y hacer explícitos cada uno de estos problemas, mediante el uso de imágenes.

Se considera como parte de la problemática todo aquello que implique un riesgo que amenace la disponibilidad, integridad y privacidad; características que hacen al sistema útil y seguro.

4.2.1 Modelo Simbólico de la Problemática Actual

La imagen simbólica de la problemática actual se presenta en la Figura 6, posteriormente se analizan con mayor detalle los riesgos que esta situación implica.

4.2.2 Riesgos que amenazan al sistema

Se considera como riesgo todo aquel factor que represente una amenaza contra la seguridad de un sistema. El factor de riesgo se incrementa conforme mayor sea el valor de los elementos que lo componen, por lo tanto, el nivel de protección debe ser proporcional al factor de riesgo.

En el caso de un sistema computacional tenemos como elementos el equipo, los programas, la información y las conexiones, todos ellos valorados según la función principal del sistema en particular.

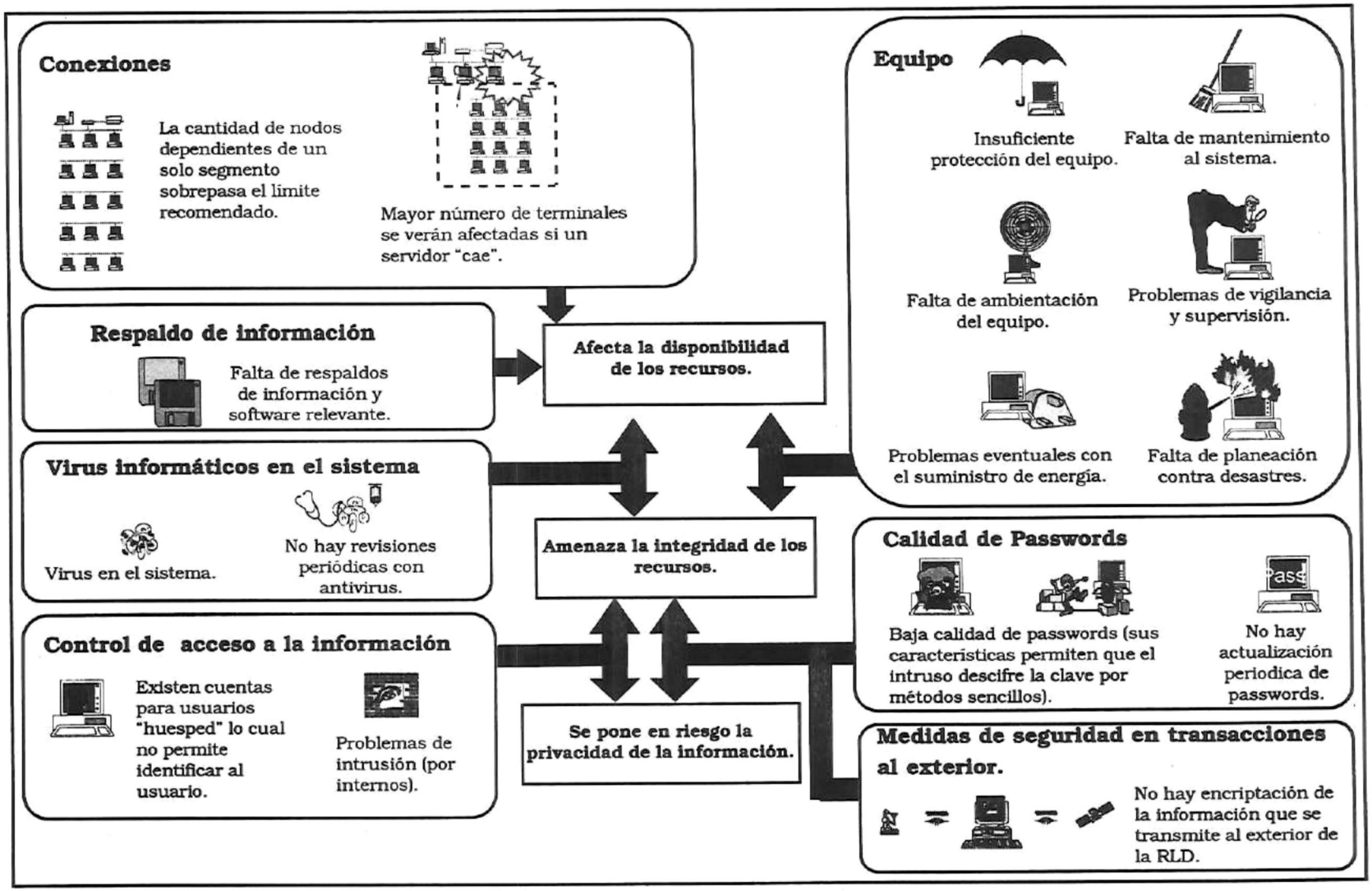


Figura 6 Modelo Simbólico de la Problemática actual.

En el Sistema Global de Información Académica y de Apoyo, como su nombre lo indica, el elemento información tiene un valor importante, aunque el resto de los elementos también juegue un papel imprescindible, el hecho de poner en riesgo la información del SGIAA sería como poner en riesgo al sistema en sí. Debido a lo anterior, la seguridad de este sistema se enfoca principalmente a este elemento, la *información*.

El análisis de riesgos realizado abarca los principales factores que amenazan la seguridad del SGIAA, como podrían ser un equipo con características inadecuadas para la aplicación que se le da, baja calidad en claves de acceso, virus en el sistema, inexistencia de respaldos de información, transacciones de información al exterior sin protección, falta de políticas de seguridad o indeterminación en éstas.

Se consideran los aspectos que amenazan la funcionalidad e integridad del sistema en red, dentro de lo que puede ser resuelto de acuerdo a los objetivos del trabajo.

4.2.2.1 Riesgos que amenazan el buen funcionamiento del sistema en red

a. Conexiones. La red UABC/uE emplea la tecnología de transmisión de datos Ethernet 10Base2 (10 Mbits/seg. banda base, 180 mts.); tomando en cuenta que de acuerdo a las especificaciones para esta tecnología de transmisión se recomienda un máximo de treinta nodos por segmento; en la red UABC/uE se

sobrepasa dicho número, en su mayoría, con más de cuarenta nodos por segmento. Existe, por lo tanto, una cantidad excesiva de nodos dependientes de un segmento. Cuanto más nodos estén conectados a un solo servidor, mayores serán las consecuencias, ya que cuando un servidor "caiga", mayor número de terminales serán afectadas, así mismo, el desempeño del sistema en general se verá afectado.

b. Equipo. Con el fin de valorar si el equipo es el adecuado para la función asignada, se hizo un estudio del equipo empleado en cada área de cómputo, se obtuvieron las características básicas del equipo y su función principal (punto 4.1.1, b.). De acuerdo a los resultados de cuestionarios y entrevistas, los riesgos que amenazan al equipo se describen en los siguientes puntos:

- *Protección.* No obstante que el equipo cumple con las características necesarias para cada aplicación, existen áreas en las que el equipo carece de protección, lo que amenaza la funcionalidad del sistema, por ejemplo, las computadoras no se cubren con forros para evitar la acumulación de polvo sobre la periferia e interior de los dispositivos.
- *Mantenimiento.* No se da un mantenimiento periódico al sistema en todas las áreas de cómputo, éste sólo es atendido en casos en que algo esté fallando o algún dispositivo esté descompuesto.

- *Medio Ambiente.* El sistema actual podría verse afectado por el medio ambiente, pues no todas las áreas de cómputo cuentan con extractor de humedad o aire acondicionado lo que puede provocar el sobrecalentamiento del equipo. Además, dada la proximidad de las instalaciones de la UABC/uE con la bahía de Ensenada, aproximadamente a cien metros de la orilla del mar, un factor importante que influye en el deterioro del sistema en cuestión es la brisa marina, la cual además de aumentar el grado de humedad en el ambiente es altamente oxidante, por lo que una ventana abierta en un área de cómputo puede ser una amenaza a mediano plazo.
- *Suministro de energía.* Algunos departamentos corren el riesgo de verse afectados por fallas eléctricas, debido a que no tienen los reguladores de corriente adecuados o existen fallas en las conexiones de corriente, varios departamentos han sufrido daños por sobrecargas. Con respecto a la amenaza de perder información en el caso de que hubiera suspensión del suministro de energía no se corre gran riesgo pues los principales servidores tienen un sistema de respaldo que funciona con baterías, por un lapso aproximado de cinco horas, tiempo suficiente para dar de baja el sistema de manera adecuada e incluso realizar un respaldo general.
- *Supervisión y vigilancia.* Otro aspecto que debe considerarse parte de la seguridad del equipo de un sistema es la protección contra robo o

destrucción, ya sea intencionada o accidental, lo cual puede lograrse con vigilancia, supervisión y medidas de control de acceso a los edificios o salas donde se encuentra el equipo, así como el control de uso de los dispositivos del sistema (impresoras, digitalizadores (*scanners*), ratones (*mouse*), monitores, etc.). Al respecto, el sistema actual en la red UABC/uE se muestra un tanto vulnerable, tal vez por el hecho de ser una institución educativa las restricciones de acceso no son tan estrictas. A pesar de contar con un número considerable de vigilantes, ha habido casos aislados de robo de equipo desde ratones, tarjetas de red o de video, hasta computadoras completas (CPU, monitor, teclado, ratón, etc.). En el aspecto de supervisión cada departamento se adapta a sus necesidades, algunas unidades académicas han adoptado sistemas de control sobre horarios de acceso, uso de dispositivos y de material.

- *Planeación contra desastres.* Los desastres naturales (sismos, incendios, inundaciones, etc.) ocurren con poca frecuencia, por lo que no es común contar con las medidas preventivas y de acción, sin embargo, dado que un desastre de esta naturaleza puede dañar o destruir todo un sistema de cómputo, es conveniente contar con un área física protegida (como una caja fuerte) donde se almacenen los respaldos de información relevante. Además se debe contar con extinguidores en cada área para el caso de incendio,

verificar si las estructuras del edificio están en buenas condiciones y si fueron planeadas contra sismos, entre otros; estos aspectos corresponden a otra área de conocimiento, seguridad industrial, por lo que no se pretende establecer políticas al respecto, pero cabe mencionarlo como punto importante dentro de la seguridad del equipo de cómputo y sus recursos.

- *Instructivos y lineamientos para el uso del equipo.* No existe un lineamiento establecido en el uso del equipo, los usuarios tienen la responsabilidad del uso, aplicación y cuidado que le den, aún cuando muchos de ellos no hayan sido instruidos con respecto a como proteger el equipo, paquetería e información del sistema que manejan, amenazando así la seguridad del mismo. Por lo tanto, existe el riesgo de que se dañe el equipo por no conocer las limitaciones del mismo.

4.2.2.2 Riesgos que amenazan la integridad de la información

a. Calidad de claves de acceso. Los resultados indican vulnerabilidad en las claves de acceso. El **91.43%** de la muestra tienen características de claves vulnerables, de acuerdo a lo descrito por Klein (1991). Es recomendable que una clave de acceso tenga una longitud mínima de ocho caracteres, sin embargo, en la mayoría de las claves de la muestra tomada (93.75%) la longitud en caracteres es menor.

La baja calidad de las claves en el sistema representa un riesgo que amenaza la integridad de la información particular de cada usuario, y en general, de toda aquella información a la que éste tiene acceso desde su cuenta. Así mismo, existen cuentas a las que el propietario nunca ha accesado y por lo tanto no ha actualizado su clave de acceso, manteniéndose aquella clave de acceso asignada por el administrador, la cual es conocida por la mayoría de los usuarios.

b. Virus. El comportamiento predominante entre los usuarios ante el problema con virus informáticos es actuar una vez que el sistema ya ha sido infectado, los usuarios del sistema en la red UABC/uE no son la excepción. En los departamentos que no están conectados a la red, las infecciones por virus se dan muy rara vez, esto se debe a que no hay mucho intercambio de información y programas de una máquina a otra que esté fuera de ese departamento, es decir el área de cómputo se encuentra aislada de este tipo de contagio, sin embargo en cualquier momento algún disco o paquete de software comercial que se instale puede contener un virus y éste no será detectado si no se hacen revisiones periódicas. En las unidades académicas que se encuentran en red y en las áreas de cómputo no restringidas, existe una mayor posibilidad de contagio, sin embargo, en estas áreas es común encontrar antivirus residentes o se hacen revisiones antivirus por lo menos cuando se sospecha de alguna infección, éstas

son las razones por las que en el estudio realizado los departamentos no estaban infectados con virus y en las unidades académicas el porcentaje de infección fue mínimo, sin embargo, dado que estas máquinas infectadas están conectadas a la red, la amenaza es considerablemente grande, pues desde una máquina infectada conectada a la red se pueden infectar todos los nodos que pertenezcan a la misma.

Las afecciones que un virus puede causar, van desde el envío de un mensaje hacia una de las salidas del sistema (análogo a un grafitti en las bardas, no perjudica pero es una molestia), hasta la inutilización del sector de arranque de un disco duro, o de un servidor de red. Sin embargo, las afecciones más comunes son la alteración o destrucción de archivos.

c. Respaldos. Los resultados (4.1.2) indican que sí se respalda la información relevante en cada uno de los departamentos y unidades evaluados, sin embargo, los usuarios directos no acostumbran realizar respaldos de su información, por lo tanto, en el caso de pérdida de información en su directorio, disco duro o flexible, por causas físicas o por infección con virus, no hay manera de recuperar sus archivos que son de gran valor para sus fines.

d. Control de acceso a la información. En seguridad computacional el control de acceso a la información se refiere a la asignación de permisos para manipular la información. Estos permisos son establecidos en el sistema y pueden ser

permisos de: lectura, escritura, y ejecución. Cada tipo de usuario debe poseer un límite de permisos sobre los recursos en el sistema, de lo contrario, éste podría accesar cualquier archivo, directorio o cuenta, situación que amenazaría la integridad del mismo.

La administración de la red UABC/uE, clasifica a los usuarios y los divide por grupos, estos grupos tienen un nivel de acceso (permisos determinados) de acuerdo a su función dentro de la institución. Sin embargo, hasta la fecha en que se hizo este estudio existen cuentas a las que puede accesar cualquier usuario (tipo huésped, invitado o anónimo), la amenaza que esto representa es que el usuario que accese esta cuenta puede hacer "cualquier cosa" desde ésta y no ser reconocida su identidad, sobre todo, si no están estrictamente limitados los permisos sobre los recursos del sistema. Así un usuario ajeno a la institución tendría la oportunidad de alterarlo.

e. Transacciones al exterior de la red. A la fecha del presente estudio, en la red UABC/uE se hacen transmisiones de información vía Internet sin emplear ningún mecanismo de protección, como lo es la *encriptación*, esto es, codificar la información con base en un algoritmo determinado, tanto el emisor como el receptor pueden decodificar dicha encriptación por medio de otro algoritmo específico para ello. La información confidencial que viaja a través de la red corre el riesgo de ser interceptada, sin embargo, la encriptación impide que la

información sea entendible para el interceptor. Tampoco se tienen *firewalls* "paredes de fuego" en las entradas a la red, que permitan entradas selectivas y seguras desde el exterior al interior de la red UABC/uE. Por lo tanto, no se pueden considerar seguras las transacciones que se realizan al exterior actualmente. La integridad de la información que viaja a través de *internet* se pone en riesgo, también se pone en riesgo el sistema debido a que se recibe información sin ser previamente evaluada como segura.

El riesgo que corre la *información confidencial* que viaja a través de Internet, es que en el transcurso del viaje, la información puede ser accesada ilegalmente, quien la accesa puede leer, modificar o destruir dicha información a su conveniencia. El riesgo que se corre al recibir información es que ésta puede contener segmentos de código dañinos, virus, instrucciones que afecten el sistema o servidor, código que permita a un usuario externo convertirse en super-usuario, crear directorios para sí mismo, robar información confidencial y explotar los recursos del sistema, entre otras actividades posibles.

V. Modelos Conceptuales de Seguridad Computacional

5.1 *Estadio 3.* Definición raíz de los módulos relevantes.

En esta etapa el objetivo es definir los módulos que formarán parte relevante del modelo general, para resolver los problemas identificados en las etapas anteriores (Capítulo IV).

a. Elementos del sistema

En el presente trabajo los elementos del SGIAA son divididos en dos ramas principales, el *Factor Humano* y el *Factor Técnico* (Figura 7). El Factor Humano se refiere a los ***usuarios*** *directos e indirectos* del sistema, y el Factor Técnico se refiere a los ***recursos*** del sistema.

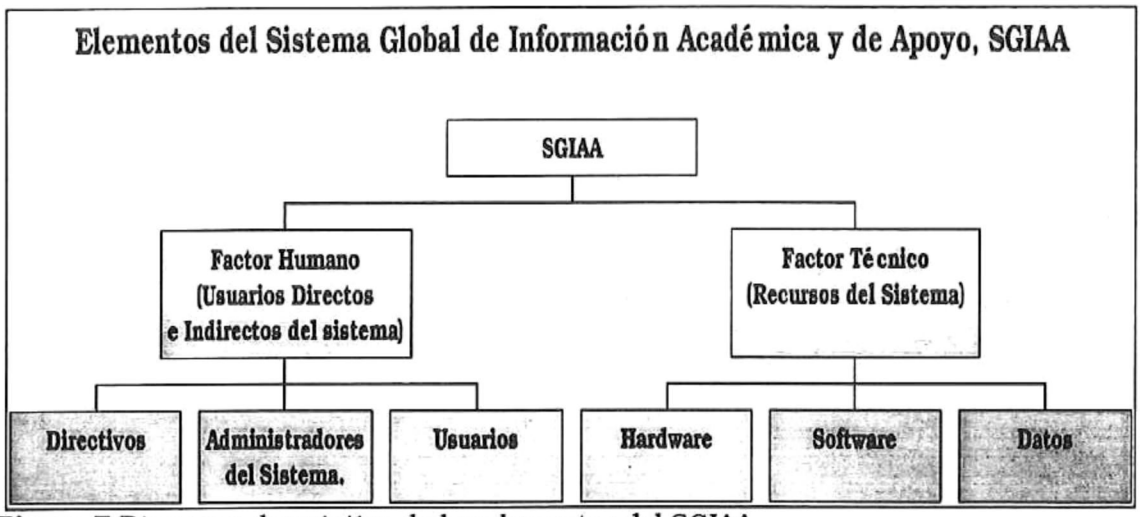


Figura 7 Diagrama descriptivo de los elementos del SGIAA.

Podemos decir que el Factor Humano es quien *usa* los recursos del sistema y el Factor Técnico es la herramienta que proporciona una *utilidad* al usuario (Figura 8).

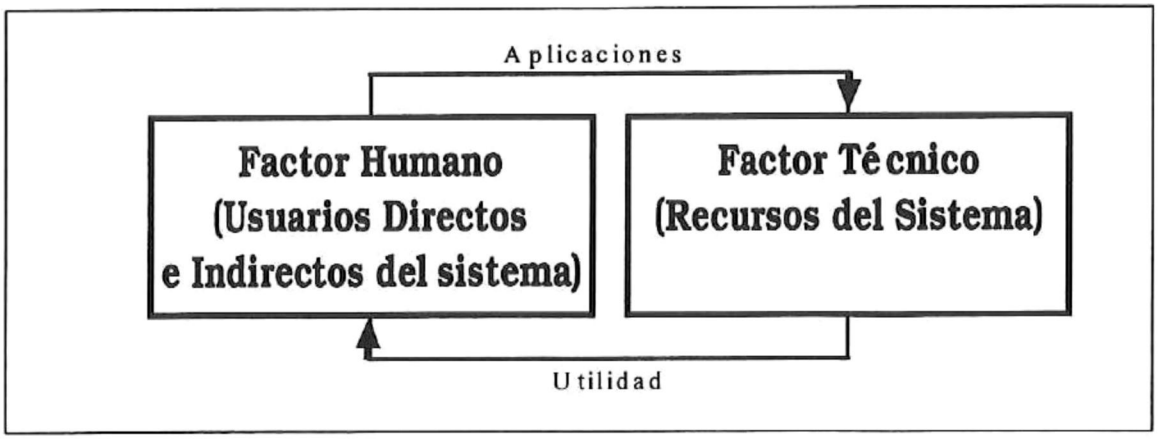


Figura 8 Interacción entre el Factor Humano y el Factor Técnico.

En un *sistema de información*, como lo es el SGIAA, la ***aplicación*** principal que se da a los recursos es la manipulación de información, lo cual consiste básicamente en *transmisión, almacenamiento y procesamiento* de datos (McCumber, 1991).

En cada *aplicación* el usuario espera una *utilidad*, la *seguridad computacional* incrementa la confianza del usuario en que el sistema le brindará una *utilidad* satisfactoria. En términos de seguridad el grado de *privacidad* de un sistema de información dependerá de las características de *confidenciabilidad, integridad y disponibilidad* que posean sus recursos. "Estas *características* son consideradas

como *críticas"* (McCumber, 1991) ya que son los puntos vulnerables que ponen en riesgo a los recursos.

Aún cuando no puede decirse que exista un sistema cien por ciento seguro (Robinson, 1995) es posible implantar *medidas de seguridad* que minimicen la vulnerabilidad de dicho sistema. Una *utilidad* satisfactoria sólo puede garantizarse en un *sistema seguro* y *confiable.*

b. Equilibrio entre utilidad y seguridad del sistema

Más que un porcentaje de seguridad, es necesario que exista un equilibrio entre utilidad y seguridad del sistema , éste puede lograrse con el correcto *análisis de riesgos* que amenazan al sistema y el análisis de las necesidades de los usuarios (Figura 9).

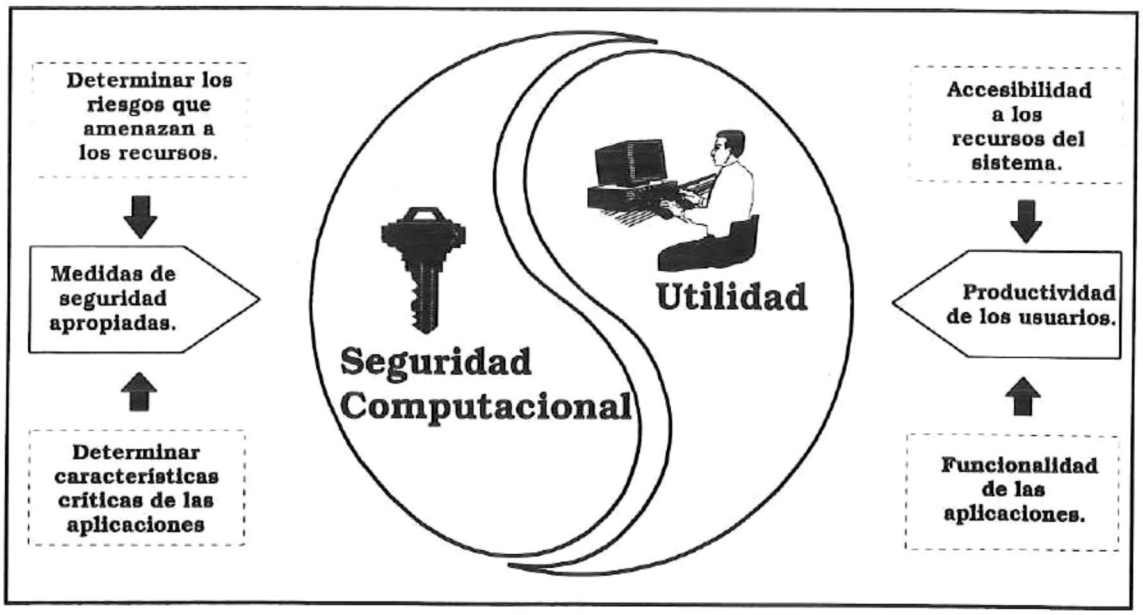


Figura 9 Balance entre utilidad y seguridad computacional.

La seguridad en un sistema debe ser proporcional al grado de riesgo que corre dicho sistema. Si las medidas de seguridad son extremas, las limitaciones de uso también serán extremas. Con estas limitaciones el usuario puede hallar el sistema tedioso, complejo e improductivo, el usuario no se hallará satisfecho al usar ese sistema, y no lo considerará útil para sus fines.

c. Determinar los grados de seguridad

Antes de establecer cualquier medida de seguridad es necesario analizar el grado de riesgo que corre cada uno de los recursos del sistema. Dado que el recurso "información" en el SGIAA es el recurso de mayor importancia y de alto riesgo (4.2.2), se considera como módulo relevante el *diseño de los niveles de acceso a la información del sistema.*

Una vez que se conocen los riesgos a los que se enfrenta cada parte es necesario determinar los grados de prevención y protección apropiados, además, es recomendable elaborar un plan de acción para el caso en que ocurra una violación del sistema (Figura 10).

En el presente trabajo, como medida de *prevención* se establecen *políticas de seguridad,* en donde se determina qué es lo que el usuario debe hacer para evitar incidentes que violen la seguridad del sistema. Como medidas de *protección* se establecen los *mecanismos técnicos,* los cuales se implantan en el mismo para

brindar protección durante cualquier proceso. Por lo tanto se eligieron y definieron como módulos relevantes:

- *Diseño de los niveles de acceso a la información del sistema.*
- *Estructuración de las políticas de seguridad.*
- *Estructuración de los mecanismos técnicos de seguridad que deben aplicarse para la seguridad del SGIAA.*

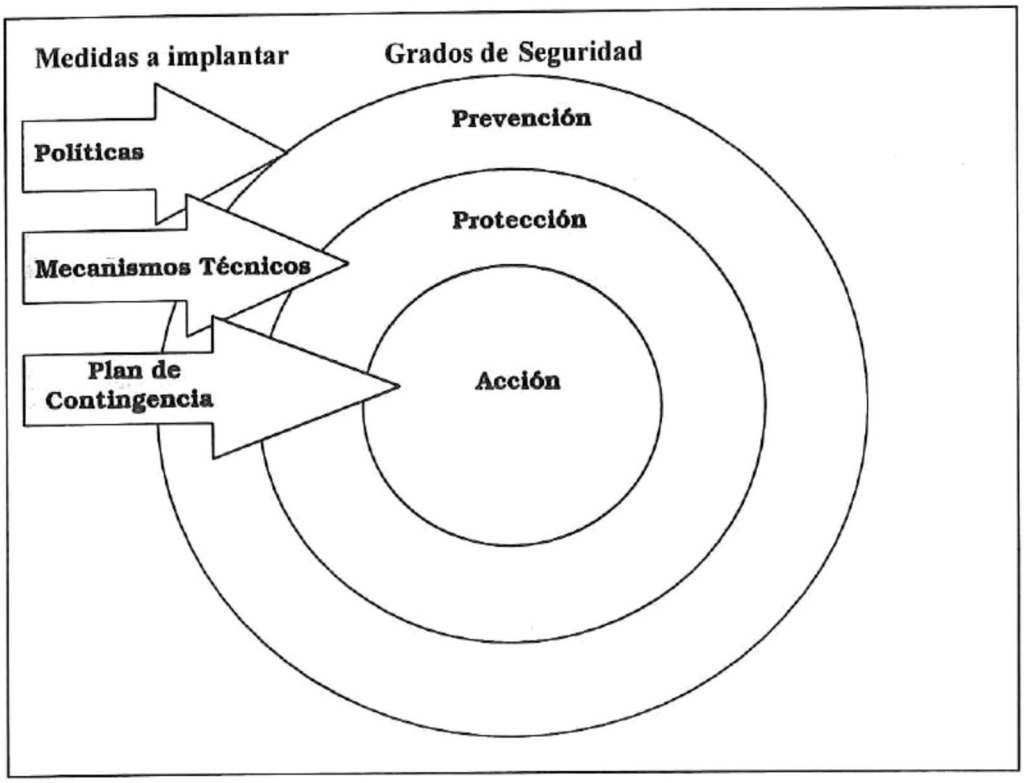


Figura 10 Representación de los grados de seguridad y las medidas a implantarse.

Ante situaciones inesperadas, la toma de decisiones se dificulta, por ello es recomendable contar con un plan de contingencia, en el cual se enlisten todas

aquellas situaciones posibles que pudieran atentar contra la seguridad del sistema, y se describan las acciones a tomar ante un problema específico. Un plan de contingencia requiere de la experiencia de un administrador de sistemas y la de los directivos de la institución, quienes finalmente toman las decisiones y aprueban las estrategias de respuesta ante cualquier situación que afecte considerablemente la institución. El desarrollo de un plan de contingencia queda fuera del alcance del presente trabajo.

5.1.1 Diseño de los niveles de acceso a la información del sistema.

De acuerdo a lo descrito en los antecedentes (2.2), el primer paso para establecer los niveles de seguridad, es responder a tres preguntas básicas:

- **¿Qué se va a proteger?**

  Respuesta: Lo que se desea proteger son los recursos, ya que son esenciales para que el sistema sea útil y cumpla su objetivo (Tabla XX).

- **¿De qué se va a proteger?**

  Respuesta: De aquello que pueda alterar el estado actual del sistema sin autorización o sin derecho (Tabla XX).

- **¿Cómo se va a proteger?**

  Respuesta: Empleando las medidas de seguridad apropiadas para prevenir, proteger y actuar en contra de violaciones en el uso del sistema (Tabla XX).

¿Qué se va a proteger? (RECURSOS)	¿De qué se va a proteger? (RIESGOS)	¿Cómo se va a proteger? (MEDIDAS de SEGURIDAD)
Hardware	• Uso No autorizado de Hardware. • Cambios No autorizados de Hardware. • Destrucción de Hardware valioso.	• Políticas de seguridad • Mecanismos técnicos de seguridad.
Software	• Uso No autorizado de Software. • Cambios No autorizados del software. • Destrucción de software valioso.	• Políticas de seguridad • Mecanismos técnicos de seguridad.
Datos	• Uso No autorizado de los Datos • Cambios No autorizados de los datos. • Destrucción de datos valiosos.	• Políticas de seguridad • Mecanismos técnicos de seguridad.

Tabla XX Preguntas y respuestas básicas para establecer los niveles de seguridad.

En términos generales y considerando los conceptos que se exponen en el capítulo II, debemos responder a estas preguntas con el fin de tener una base para el análisis de los riesgos y de los niveles de protección que se requieren. El *"Modelo Conceptual del análisis de riesgos" (5.2.1)* se propone como guía para responder a estas preguntas.

Para un sistema de información como lo es el SGIAA, el recurso información es uno de los más vulnerables. Dado que la información es un recurso relevante dentro de los objetivos del sistema, los riesgos que ésta corre

se acentúan. Un gran número de usuarios emplearán la información a nivel intra e interinstitucional, por lo que es necesario establecer los niveles de acceso a dicha información. Los niveles de acceso fueron clasificados de acuerdo a lo siguiente:

- *Nivel Público Externo:* Toda aquella información de interés público que pueda ser empleada a nivel externo de la RLD de la UABC/uE, vía Internet.
- *Nivel Público Interno:* Aquella información que está destinada exclusivamente para usuarios pertenecientes a la institución.
- *Nivel Privado:* Es la información que se considera propiedad de un sólo usuario o de un grupo de usuarios determinado, la cual no debe ser empleado por ningún otro usuario que no sea el propietario o propietarios.

En el diseño de los niveles de acceso a la información se consideraron:

- La información que será manipulada dentro del sistema SGIAA.
- La forma en que se presenta dicha información.
- Quién la genera y quién la recibe (Medina, 1997).

Estos aspectos se integraron en el *"Modelo Conceptual para el diseño de los niveles de acceso a la información"* (5.2.2), con la finalidad de que el administrador de sistemas conozca los niveles de protección que requiere cada tipo de información del SGIAA.

5.1.2 Estructuración de las políticas de seguridad.

La meta de la seguridad computacional es garantizar las características de *privacidad, integridad y disponibilidad* de los recursos del sistema, las políticas de seguridad son una medida de prevención contra incidentes que puedan afectar estas características.

Las políticas de seguridad especifican qué debe hacer un usuario para evitar incidentes que afecten al sistema (Holbrook, 1991). Considerando los riesgos identificados durante el análisis de la problemática actual (Capítulo IV), se propone una estructura que determine los puntos que se consideran relevantes para el establecimiento de las políticas para el SGIAA, posteriormente se hacen las especificaciones respecto a cada uno de estos puntos (Capítulo VI). La estructura para las políticas de seguridad para el SGIAA es la siguiente:

Política para...

1. Obtener una cuenta en el sistema.
2. Uso de hardware.
3. Uso de software.
4. Manejo de información.
5. Elección de password.
6. Prevención contra virus informáticos.
7. Acceso al exterior de la RLD.

Una vez que son implantadas las políticas de seguridad de manera específica,deben ir evolucionando conforme a las necesidades y al nuevo nivel de

riesgo a que se enfrente el sistema, por esta razón se propone un ciclo de vida para las políticas. Este ciclo de vida inicia a partir de que las políticas de seguridad han sido establecidas, continuando con puntos de cuestionamiento y acción en caso de que sea necesario algún cambio en éstas.

Sin embargo, el contar con políticas de seguridad establecidas no garantiza que todos los usuarios las apliquen, pues dependerá en gran parte de la ética y profesionalismo del propio usuario.

5.1.3 Estructuración de los mecanismos técnicos de seguridad que deben aplicarse al SGIAA.

Además de las medidas de prevención es necesario establecer medidas de protección. Los mecanismos técnicos de protección que aquí se proponen, están directamente relacionados con la administración del sistema, pues son los administradores quienes deben implementarlos como parte del sistema.

La estructura general propuesta hace mención de los puntos relevantes a considerar en el establecimiento de los mecanismos técnicos de protección.

1. Implantación de *herramientas de seguridad* con las cuales se puedan realizar las siguientes actividades:
    - Reportes del estado actual de seguridad.
    - Monitoreo de usuarios y procesos.
    - Rastreo de intrusos.
    - Control de acceso.

- Control de usuarios.
- Encriptación de información sensible del sistema.
- Control de calidad de claves de acceso.

2. Mantenimiento y actualización de la Infraestructura.
3. Implantación y actualización de antivirus.
4. Medidas de protección en transacciones al exterior.
    - Encriptación.
    - *Firewalls* ("Paredes de fuego") y filtros de paquetes.

De acuerdo a esta estructura general los mecanismos técnicos se especifican detalladamente en el Capítulo VI.

Los mecanismos técnicos de seguridad al igual que las políticas requieren de cambios conforme pasa el tiempo, por lo que se propone también un ciclo de vida para éstos, este ciclo de vida debe tener cierta semejanza con el de las políticas, con las variantes propias de esta medida de protección.

5.2 *Estadio 4.* Modelos conceptuales

En esta etapa el propósito es presentar los modelos conceptuales de los que se parte para el desarrollo de las medidas de seguridad para el SGIAA.

5.2.1 Modelo Conceptual del análisis de riesgos

Este modelo conceptual aplica las tres preguntas básicas, (5.1.1), para el análisis de riesgos y de los niveles de protección. Los cuestionamientos se enfocan al SGIAA y a su problemática en particular (Figura 11).

Figura 11 Modelo Conceptual del Análisis de Riesgos.

Este modelo podrá ser empleado por los responsables del área de seguridad en cómputo en coordinación con los directivos del SGIAA.

5.2.2 Modelo conceptual para el diseño de los niveles de acceso a la información

Este modelo pretende ser una guía para la representación de la información, el módulo que la genera, el usuario que la emplea, los permisos de acceso que tienen las entidades que la manejan, la forma en que se presenta, y el nivel de protección que requiere, basándose en los niveles establecidos en el capítulo anterior.

Esta representación gráfica de los niveles de acceso a la información del SGIAA facilitará a los administradores del sistema el establececimiento y control de acceso apropiado a dicha información y conocer claramente los flujos que ésta debe tener (Figura 12).

5.2.3 Modelo conceptual del ciclo de vida de las políticas de seguridad

El modelo conceptual representa el ciclo de vida de las políticas para que éstas sean actualizadas cada vez que sea necesario. Se recomienda seguir este modelo cada vez que las políticas actuales sean insuficientes para los riesgos a que se somete el sistema, o cuando dichas políticas limiten la productividad de nuevas aplicaciones dentro del SGIAA (Figura 13).

Los responsables de actualizar dichas políticas, serán los administradores del sistema y los responsables del área de seguridad en cómputo, en coordinación con los directivos del SGIAA y en caso necesario con los directivos de la institución.

5.2.4 Modelo conceptual del ciclo de vida de los mecanismos técnicos de seguridad

Este modelo representa el ciclo de vida de los mecanismos técnicos de seguridad, ya que se requerirá que haya cambios de acuerdo a la evolución del SGIAA y de los nuevos riesgos que lo amenacen (Figura 14).

Los mecanismos técnicos de seguridad se especifican en el Capítulo VI. Éstos serán actualizados por los responsables del área de seguridad computacional en coordinación con los administradores del sistema conforme sea necesario.

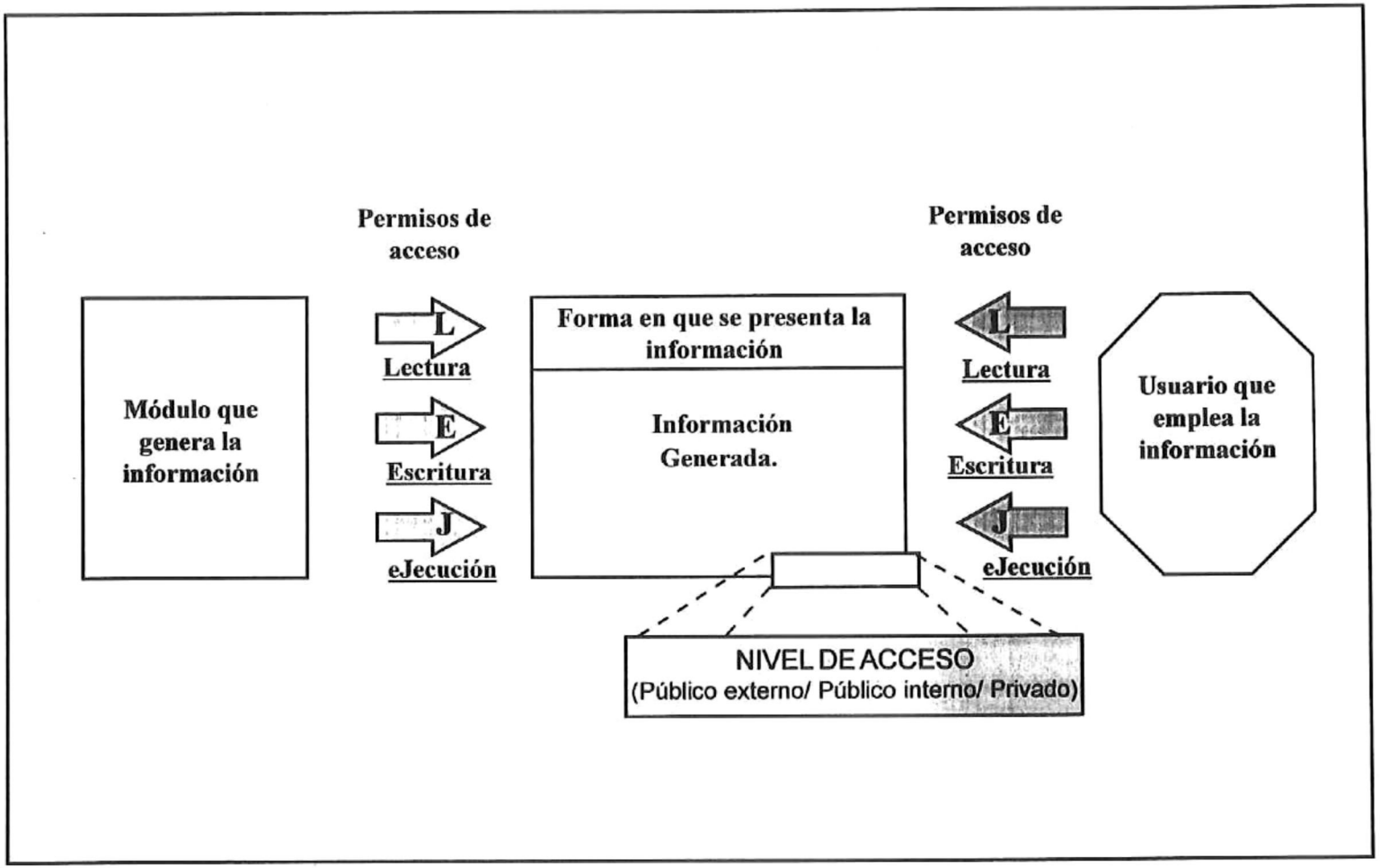


Figura 12 Modelo Conceptual para el Diseño de los Niveles de Acceso a la Información.

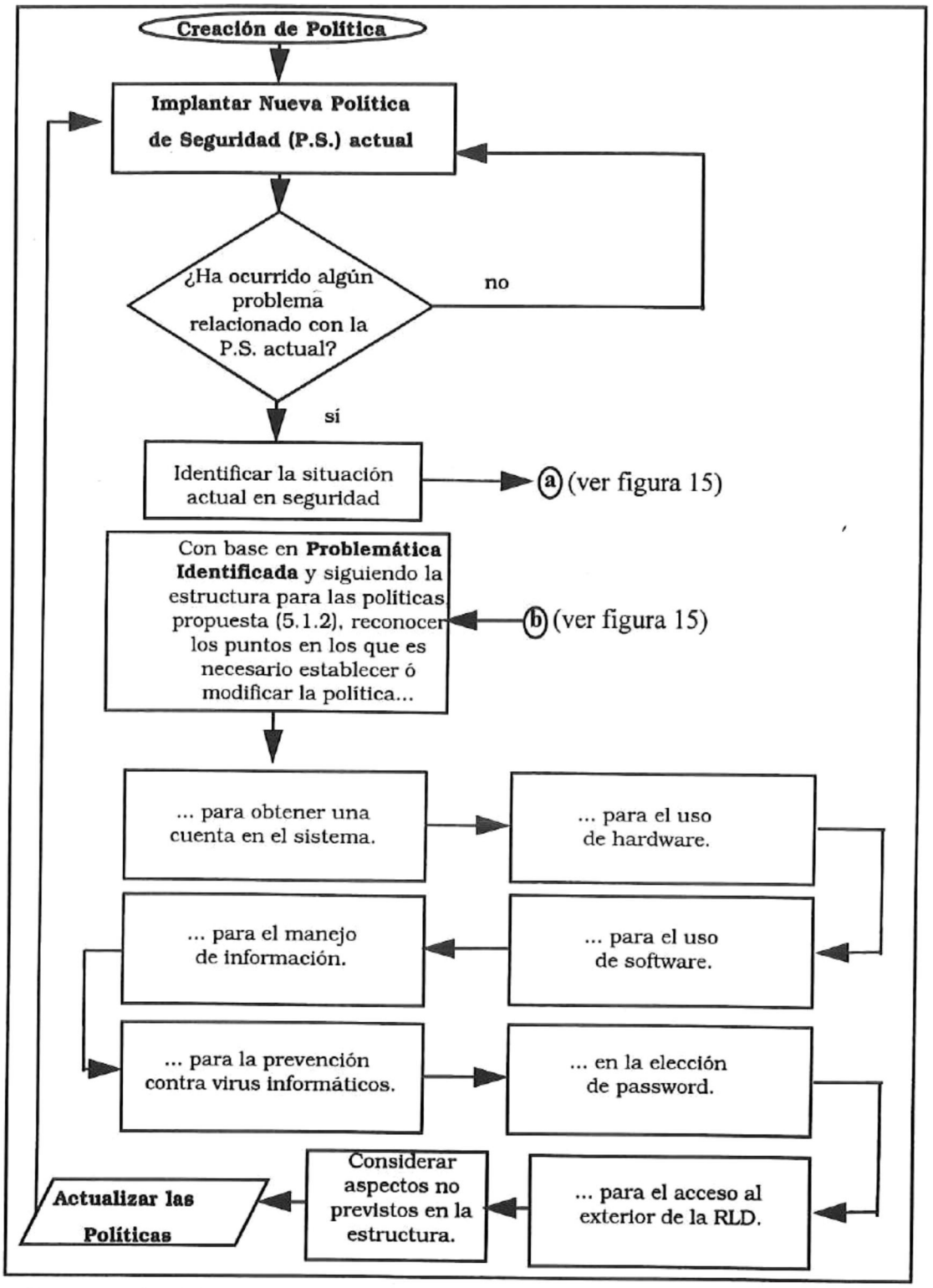


Figura 13 Modelo conceptual del ciclo de vida de las Políticas de Seguridad.

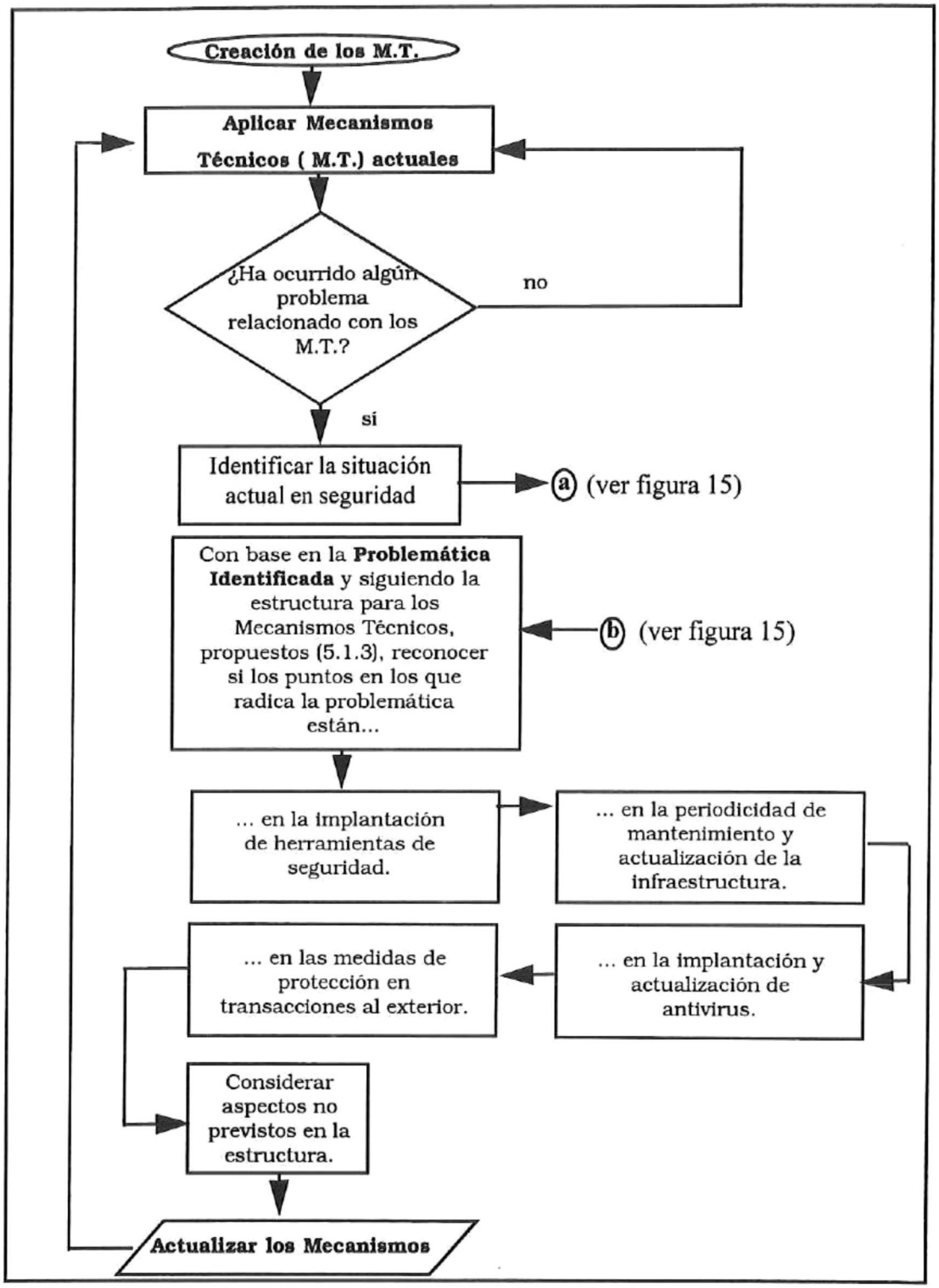


Figura 14 Modelo conceptual del ciclo de vida de los Mecanismos Técnicos de Seguridad.

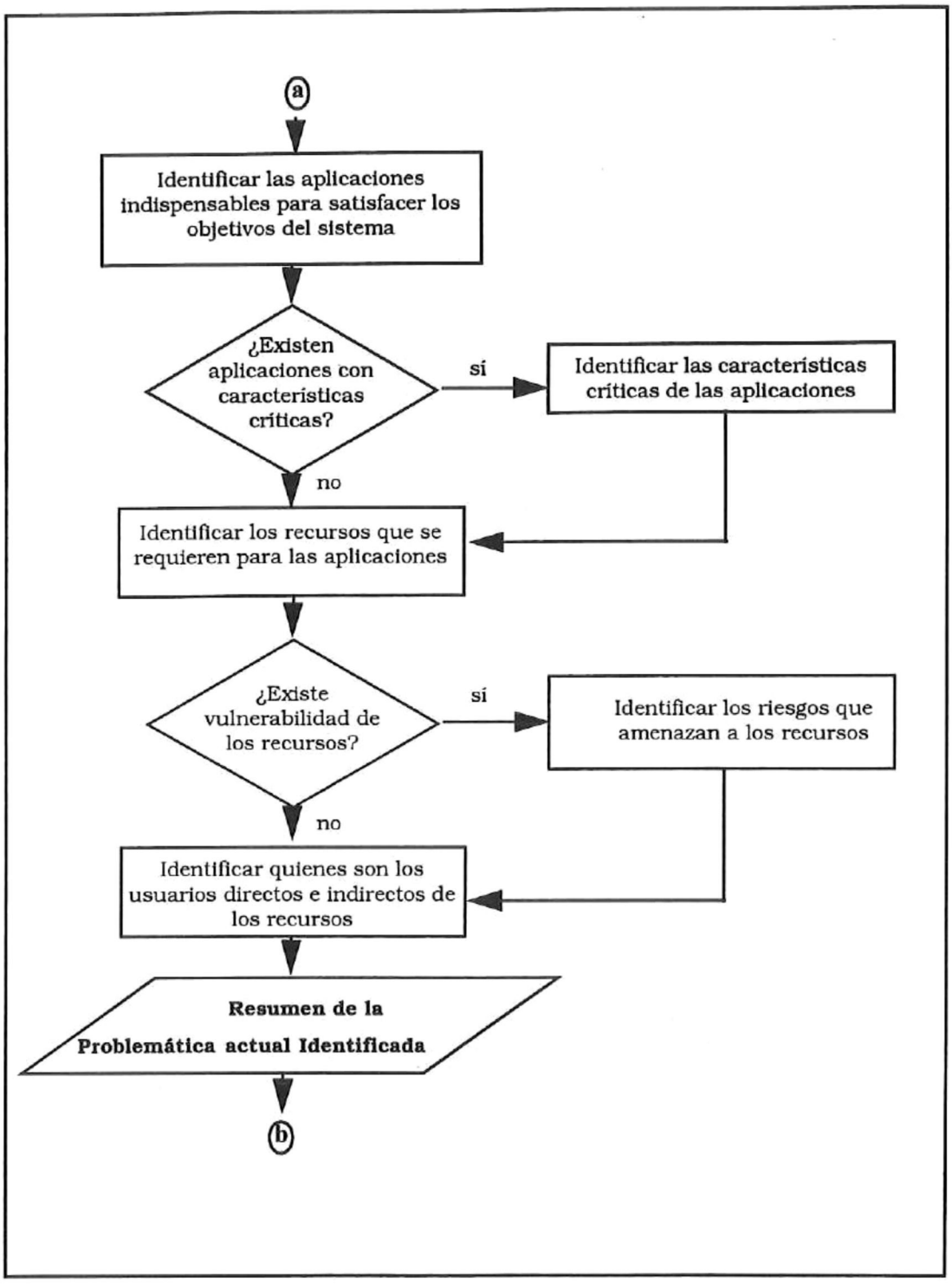


Figura 15 Complemento de los Modelos Conceptuales de los ciclos de vida de las Políticas y de los Mecanismos Técnicos de Seguridad.

VI. Desarrollo de las Medidas de Seguridad

6.1 *Estadio 5.* Comparación del diseño deseable vs. situación real

En este estadio denominado de comparación, la situación problema analizada en el segundo estadio se examina a la par de los modelos conceptuales (Ramírez, 1996), obteniendo una propuesta de los posibles cambios a realizar para resolver la situación problemática.

6.1.1 Tablas comparativas de la situación problema y los modelos conceptuales

La comparación se describe a través de las tablas XXI-XXIII, de acuerdo al formato establecido en la Tabla I.

En estas tablas, la primer columna presenta una lista de las actividades propuestas en el modelo conceptual, la segunda columna cuestiona si existe o no dicha actividad actualmente, la tercera indica qué se realiza actualmente para sustituir la actividad dada, en la cuarta columna se describe el criterio para la valoración de la existencia o ausencia de determinada actividad y la quinta presenta el cambio propuesto para mejorar la situación.

Actividad	¿Existe?	Mecanismo presente	Valoración de la actividad	Cambio propuesto
1) **Especificar las aplicaciones que se consideren indispensables para la productividad del sistema.**	1) *Se conocen, mas no están especificadas*	1) *Son identificadas formalmente, cuando es necesario (inicio de semestre).*	1) *Consultando dichas especificaciones antes de implantar las medidas de seguridad se evita que éstas limiten las aplicaciones indispensables.*	1) *Especificar en un documento las aplicaciones consideradas indispensables.*
2) **Especificar los recursos que se consideren indispensables para obtener la utilidad esperada durante las aplicaciones.**	2) *Se conocen , mas no están especificados*	2) *El usuario dispone de los recursos indispensables y tiene acceso restringido a recursos limitados.*	2) *Se evita que las medidas de seguridad limiten la disponibilidad de los recursos indispensables.*	2) *Especificar en un documento los recursos considerados indispensables.*
3) **Mantener las características que garanticen confidenciabilidad, integridad y disponibilidad de los recursos durante las aplicaciones.**	3) *Se aplica sólo en la administración del sistema.*	3) *La administración del sistema procura mantener dichas características, sin embargo los usuarios las desconocen.*	3) *Manteniendo dichas características se brinda confiabilidad en el sistema.*	3) *Mantener las características de confiabilidad dando a conocer y aplicando las medidas necesarias para ello.*

Tabla XXI Comparación del Modelo Conceptual del Análisis de Riesgos vs. situación real.

Actividad	¿Existe?	Mecanismo presente	Valoración de la actividad	Cambio propuesto
4) Identificar los riesgos que puedan amenazar la utilidad y confiabilidad del sistema.	4) *No están identificados.*	4) *Se van conociendo los riesgos conforme a las experiencias del sitio.*	*4) Identificando los riesgos las medidas de seguridad serán establecidas en proporción a dichos riesgos.*	4) *Hacer análisis periódicos de los riesgos que amenazan al sistema.*
5) Identificar las medidas de seguridad, prevención, protección y acción necesarias.	5) *No están especificadas.*	5) *Se da prioridad a la protección de recursos y aplicaciones.*	5) *Estableciendo medidas en distintos grados de seguridad, se asegura una mayor confiabilidad.*	5) *Identificar el nivel de prevención y protección adecuado para el sistema y las acciones a tomar en caso de violación al mismo.*
6) Especificar e Implantar las medidas de seguridad apropiadas para el sistema. (políticas, mecanismos técnicos y plan de contingencia)	6) *No están establecidos*	6) *Los usuarios son responsables del uso que dan al sistema, los administradores protegen el sistema conforma vaya siendo necesario, y los problemas se van resolviendo conforme ocurren.*	6) *Al contar con medidas de seguridad se cuenta con los tres principales niveles de seguridad.*	6) *Especificar e implantar dichas medidas y actualizarlas periódicamente.*

(Continuación Tabla XXI) Comparación del Modelo Conceptual del Análisis de Riesgos vs. situación real.

Actividad	¿Existe?	Mecanismo presente	Valoración de la actividad	Cambio propuesto
1) **Determinar los permisos de acceso para cada tipo de información dentro del sistema.**	1) *Se aplica sólo a información restringida*	1) *Se asignan permisos de acceso (lectura, escritura y ejecución) a las aplicaciones y a información relevante para el sistema.*	1) *La información tendrá el nivel apropiado de protección minimizando riesgos de acceso no autorizado.*	1) *Documentar el tipo de información que maneja cada módulo en el sistema determinando los permisos de acceso correspondientes.*
2) **Clasificar la información de acuerdo al nivel de acceso permitido (pública externa, pública interna ó privada).**	2) *No se tiene clasificada.*	2) *Se generan grupos de usuarios para determinadas aplicaciones e información.*	2) *Los permisos de acceso pueden ser asignados más acertadamente si la información puede ser identificada como pública externa, pública interna ó privada.*	2) *Clasificar y documentar la información determinando el nivel de acceso.*

Tabla XXII Comparación del Modelo Conceptual para el Diseño de los Niveles de Acceso a la Información vs. situación real.

Actividad	¿Existe?	Mecanismo presente	Valoración de la actividad	Cambio propuesto
1) **Revisar periódicamente las políticas y adecuarlas a los nuevos requerimientos de seguridad cuando sea necesario.**	1) *No existe una política determinada.*	1) *Los usuarios son responsables del uso que dan al sistema.*	1) *La revisiones periódicas, de acuerdo al ciclo de vida propuesto, permiten captar nuevas necesidades de seguridad en el sistema.*	1) *Implantar Políticas de Seguridad y aplicar periódicamente el ciclo de vida para éstas.*
2) **Revisar periódicamente los mecanismos técnicos y adecuarlos a los nuevos requerimientos de seguridad cuando sea necesario.**	2) *Las revisiones se hacen cada vez que ocurre algún incidente.*	2) *Se emplean los mecanismos que vienen integrados al sistema y se van adaptando a las necesidades.*	2) *La revisiones periódicas, de acuerdo al ciclo de vida propuesto, permiten captar nuevas necesidades de seguridad en el sistema.*	2) *Implantar los Mecanismos Técnicos de Protección y aplicar periódicamente el ciclo de vida para éstos.*

Tabla XXIII Comparación de los Modelos Conceptuales del Ciclo de Vida de las Políticas y Mecanismos Técnicos vs. situación real.

6.2 *Estadio 6.* Definición de los cambios deseables factibles

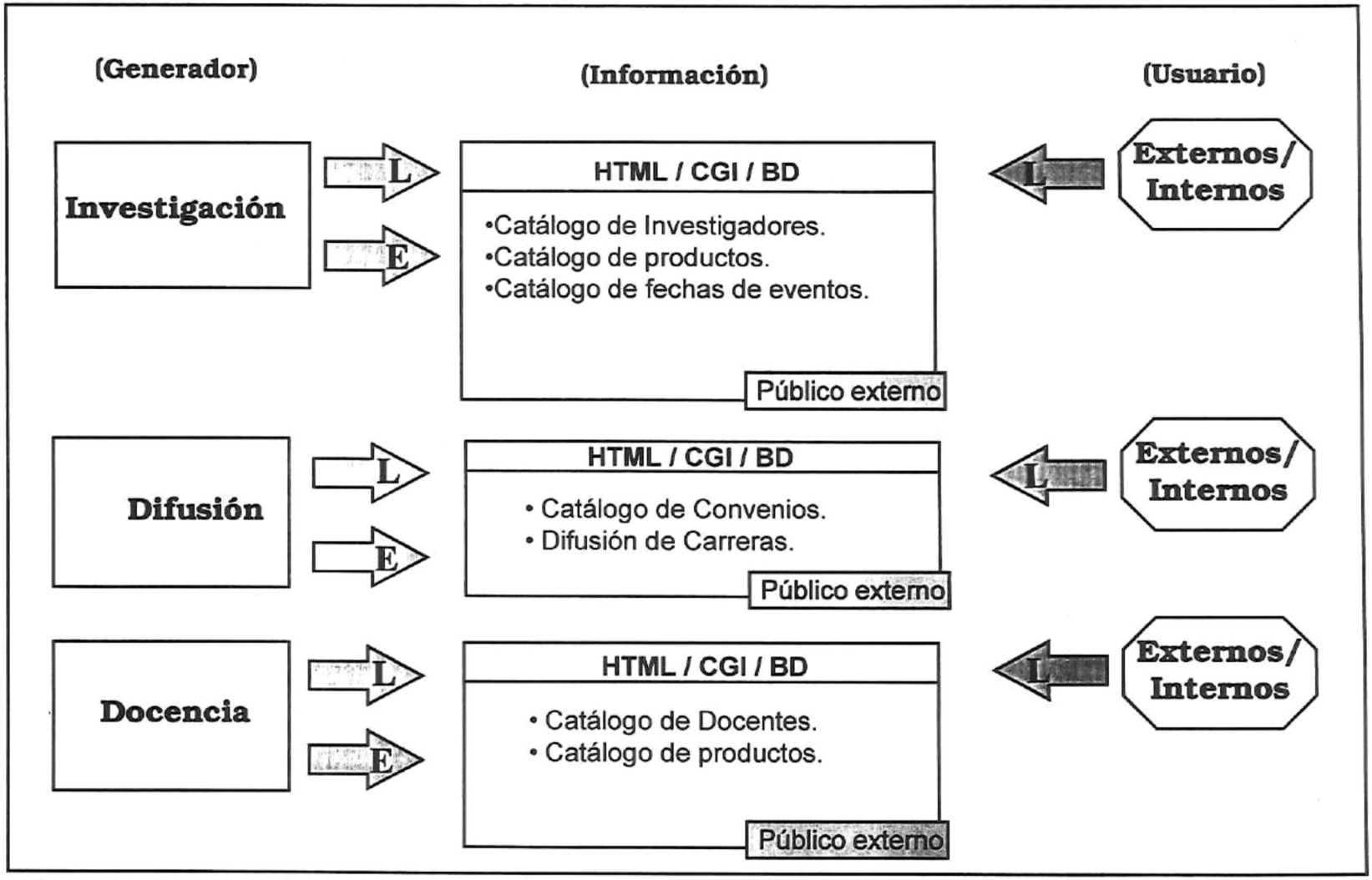
En el presente estadio se pretende establecer los cambios deseables y factibles de la situación problemática actual. Esto con base en los resultados de las comparaciones de la etapa anterior *(Estadio 5)* y los cambios propuestos. Los cambios son, establecer las medidas de seguridad que se describen en los puntos 6.2.1, 6.2.2 y 6.2.3; llegando finalmente a la propuesta de un modelo general de seguridad para el SGIAA (6.2.4) .

6.2.1 Diseño de los niveles de acceso a la información

Con base en el *"Modelo conceptual para el diseño de los Niveles de Protección de la Información"*, se describen los niveles de protección correspondientes a la información que manejará el SGIAA (Figuras 16-19). Los niveles de protección se establecen de acuerdo a lo descrito en el punto 5.1.1.

Como punto de partida se considera aquella información que es generada por los módulos de:

- Investigación,
- Difusión y
- Docencia.



Figuara 16 Descripción de los permisos de acceso a la información de Nivel Público.

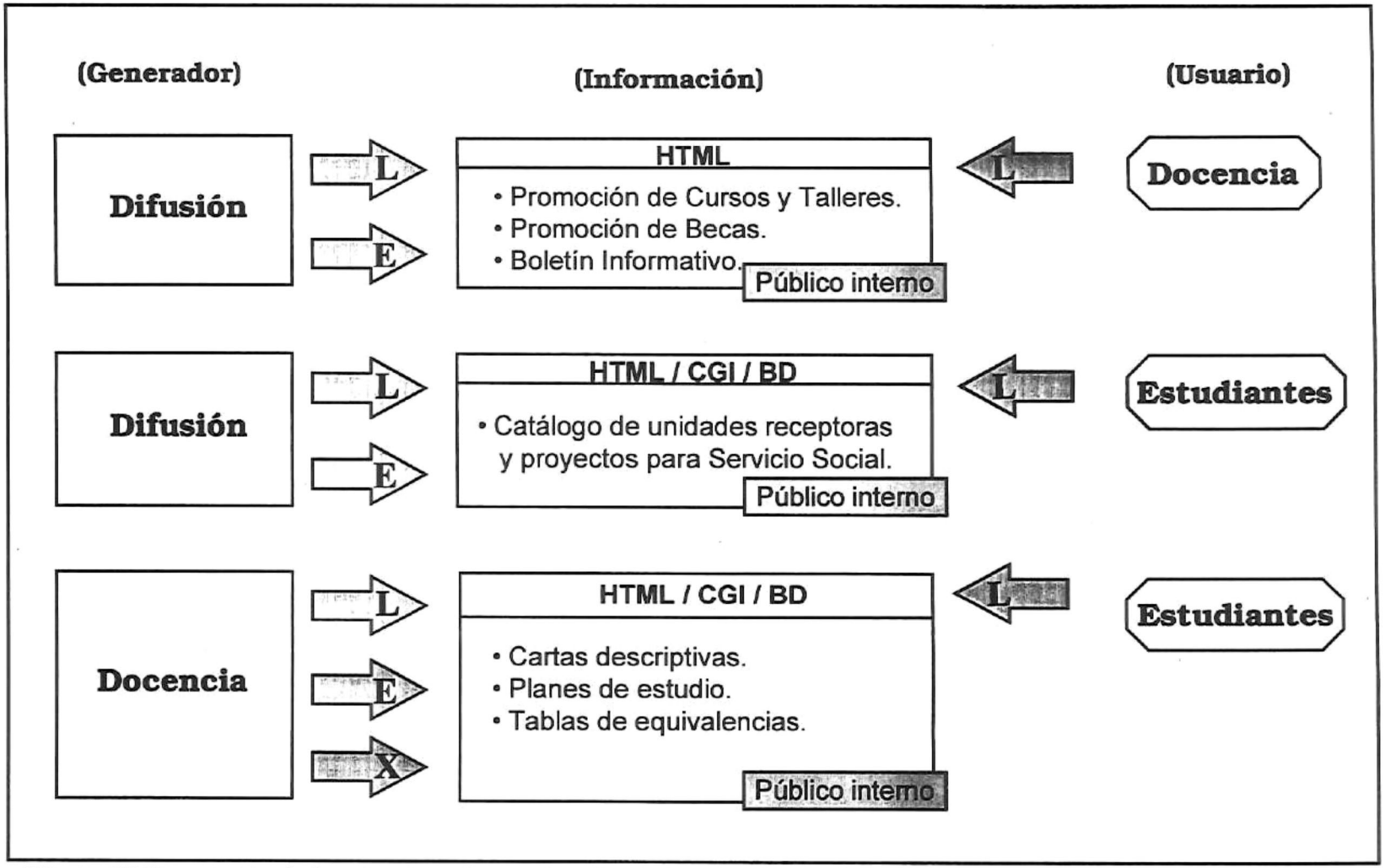


Figura 17 Descripción de los permisos de acceso a la información de Nivel Interno.

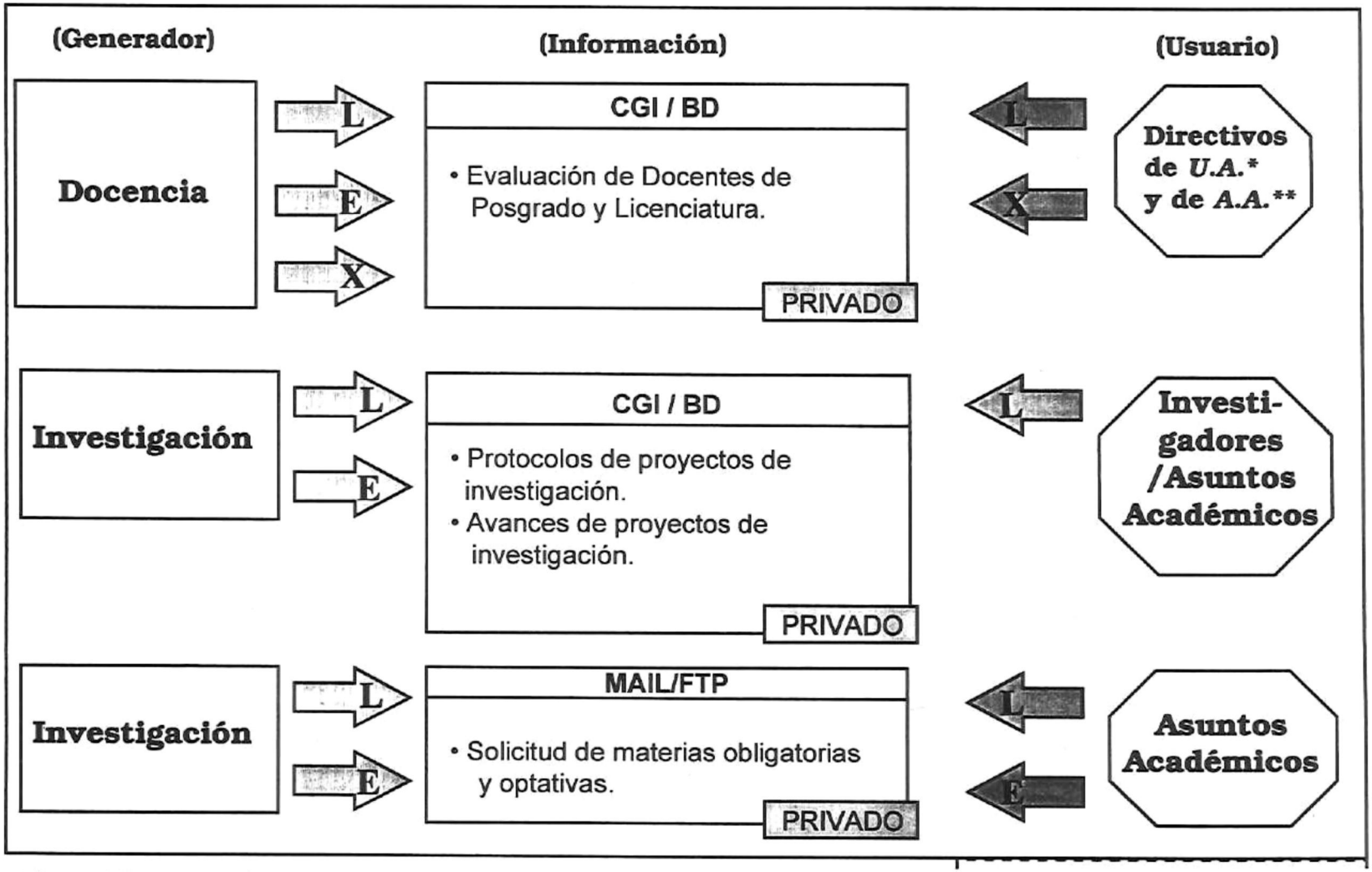


Figura 18 Descripción de los permisos de acceso a la información de Nivel Privado.

* ***U. A.*** *Unidad Académica.*

** ***A.A.*** *Asuntos Académicos.*

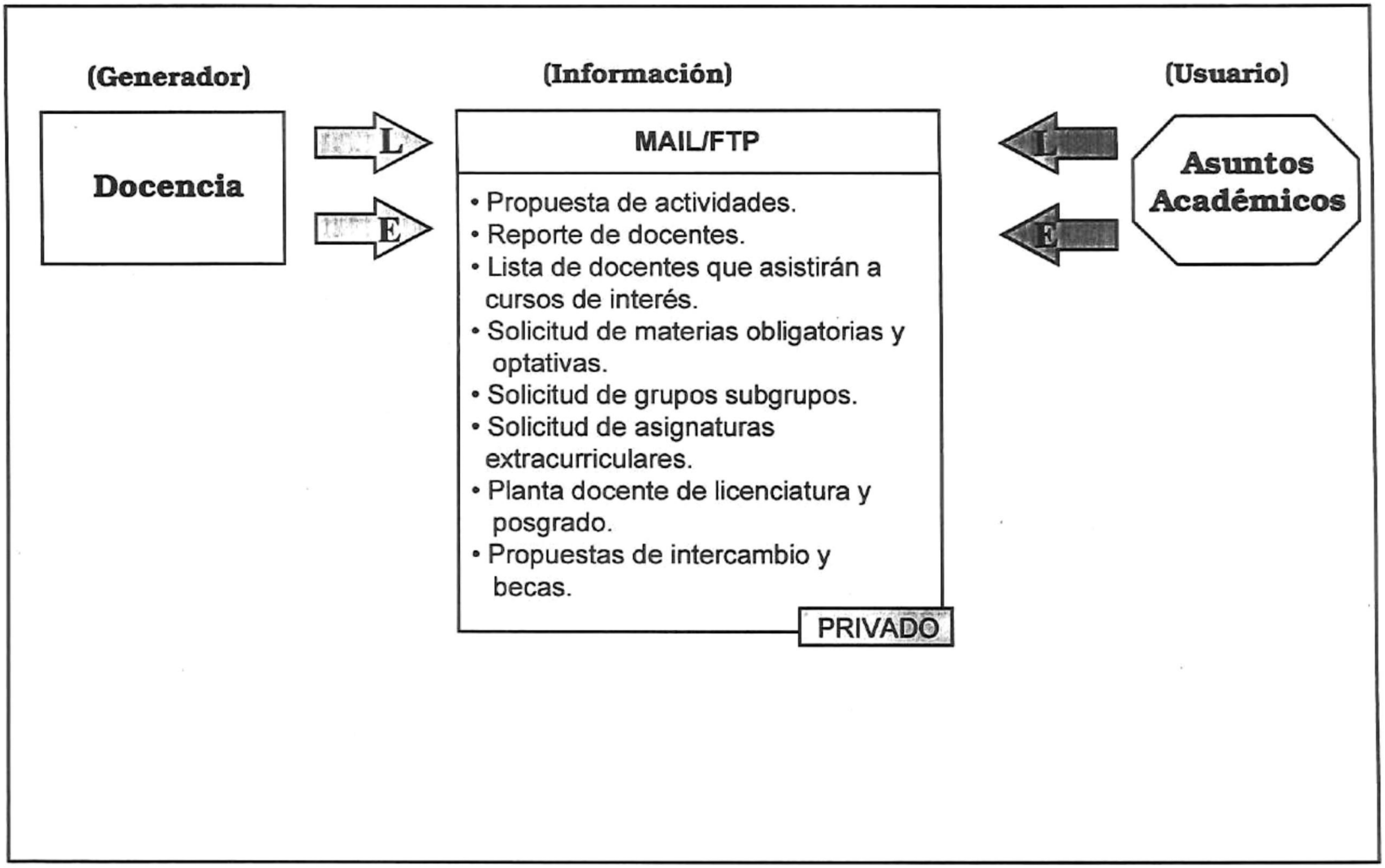


Figura 19 Descripción de los permisos de acceso a la información de Nivel Privado.

6.2.2 Políticas de Seguridad para el SGIAA

Para desarrollar las políticas se consideran tres aspectos (Holbrook, 1991), la meta y enfoque del *sitio* (en este caso el sitio es el SGIAA), políticas y reglamentos a que está sujeto actualmente el sistema en el que se desarrolla el SGIAA, y la implicación a nivel global que puede tener el contar o no con una política de seguridad computacional preestablecida.

- **Meta y enfoque del SGIAA**, la meta principal del SGIAA es desarrollar un sistema automatizado que permita manejar los bancos de información de docencia, investigación y difusión, y que permita accesar los bancos de información en forma intra e interinstitucional utilizando la infraestructura de redes actual de la UABC/uE y su entorno (Morán, et al., 1996). El SGIAA se enfoca a dos principales formas de acceso a la información, intra-institucional, que corresponde a toda aquella información de interés interno, e interinstitucional, toda aquella información de interés global.
- **Políticas y reglamentos a las que está sujeto el SGIAA y su entorno, antes de determinar la nueva política**, puesto que el SGIAA será implantado sobre el sistema de redes de la UABC/uE actual, se considera cualquier política, reglamento, regulación o ley que rija esta red, igualmente se considera cualquier regla que el SGIAA haya implantado en cualquiera de sus módulos. Los Módulos que componen el SGIAA son: Facultad de

Ciencias, Investigación y Posgrado, Asuntos Académicos, Vinculación, y Extensión Universitaria. Actualmente, no existe un reglamento oficial a nivel general de la red, sino que se mantiene realizando las acciones necesarias conforme surgen los problemas de seguridad en el mismo. Estas regulaciones están directamente relacionadas con mecanismos técnicos que mantienen la funcionalidad del sistema, mientras que la interacción con el usuario respecto al uso adecuado del mismo, consiste en mensajes ocasionales que le instruyen para resolver algún incidente por el que se está pasando. Estas son dos buenas estrategias que deben permanecer dentro de las nuevas políticas. Mientras que esto se da a nivel general, a nivel departamento o unidad académica (U.A.) la situación es similar, con excepción de la unidad académica de la Facultad de Ciencias, ninguna de los departamentos o U.A. tienen un reglamento establecido para los usuarios. En particular, el aula equipada de la Facultad de Ciencias tiene un reglamento para los usuarios el cual es mostrado por escrito en un lugar público.

- **Implicaciones a nivel global**. El sistema de red de la UABC/uE está enlazada a Internet, por lo tanto deben considerarse las implicaciones que esto tiene a nivel global. Un *sitio* universitario comúnmente se considera fuera de peligro en cuestiones de seguridad, comparado con un *sitio* de una

base militar por ejemplo. Sin embargo, una universidad también corre riesgos al estar conectada al exterior, pues la integridad y confidenciabilidad de la información de interés interno es valiosa para ella y sus elementos, si el sistema se viera afectado, todos los usuarios que dependen del mismo también se verían afectados. Sin embargo, los riesgos no se limitan a tener daños internos por causa de intrusos externos, sino que viceversa, usuarios internos pueden causar daños en sistemas externos, lo cual puede causar graves problemas en la relación con otras organizaciones, y de prestigio para la misma Universidad.

- **Políticas de Seguridad para el Usuario:**

I. Condiciones para obtener una cuenta en el sistema

I.I El usuario que desee darse de alta en el sistema deberá formar parte activa de la Universidad Autónoma de Baja California, unidad Ensenada, es decir, todo aquel que desarrolle alguna actividad como docente, alumno, tesista, egresado, investigador, directivo o trabajador, dentro de la institución.

I.II El usuario proporcionará sus datos llenando una forma con las características establecidas en la Tabla XXIV.

I.III Dichos datos pasarán a una base de datos donde permanecerán hasta que el usuario se dé de baja definitiva del sistema.

<table>
<tr><td colspan="3">UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA
Forma de Registro para el Usuario
(Nombre del aula equipada)</td></tr>
<tr><td colspan="2">Datos del usuario
Matricula: (matrícula del usuario)
Nombre: (apellido paterno, apellido materno y nombres del usuario)</td><td rowspan="5">Aplicaciones que dará al sistema:</td></tr>
<tr><td colspan="2">Usuario
◊ Interno ◊ Externo
Escuela ó Facultad: Institución:</td></tr>
<tr><td colspan="2">Función que desempeña dentro de la institución:
◊ académico ◊ alumno ◊ otros (especificar):
◊ administrativo ◊ egresado</td></tr>
<tr><td colspan="2">Tipo de usuario:
◊ Administrador del sistema. ◊ Usuario</td></tr>
<tr><td colspan="2">Servidor:
Nombre de la cuenta:
Tipo de cuenta:
◊ Individual ◊ Grupo</td></tr>
<tr><td>Firma del Responsable
(Nombre del Responsable)</td><td>Firma del Usuario</td></tr>
</table>

Tabla XXIV Características de la forma que el usuario llenará para su registro

I.IV El usuario del sistema se apegará al presente reglamento; cuando utilice cualquiera de los recursos de la red local de la UABC/uE.

II. Reglamento en el uso de hardware

II.I El usuario debe tener autorización previa para el uso de los dispositivos de las áreas de cómputo, sobre todo cuando se trate de dispositivos especiales, o limitados en existencia, como impresoras láser, *scanners* (digitalizadores de imágenes), cámaras, bocinas, y otros dispositivos especializados.

II.II El hardware y dispositivos no deberán ser modificados por el usuario, sin la previa autorización por parte del responsable del sistema. Esto se refiere a que el usuario:

II.II.I no hará cambios en la configuración y características del equipo, sin previa autorización;

II.II.II no hará cambios en la ubicación del equipo dentro del área de cómputo, ni al exterior de ésta, sin previa autorización;

II.II.III no añadirá ningún dispositivo externo al sistema sin previa autorización.

II.III Si el usuario daña o destruye el equipo o cualquiera de sus partes se atendrá a las sanciones que la administración disponga.

II. Cualquier problema o falla en el hardware notificarlo de inmediato al encargado del sistema local.

III. Reglamento en el uso de software

III.I No se hará uso del software sin previa autorización.

III.II El software no deberá ser modificado ni reconfigurado de su forma original, sin previa autorización.

III.III El usuario no destruirá ni borrará ningún programa del sistema.

III.IV El software comercial original no deberá ser copiado por ningún usuario.

III.V El usuario no instalará ningún paquete de software en el sistema sin previa autorización.

III.VI Cualquier software que se instale en el sistema deberá ser original, no se instalarán copias, ni software de dominio público que no esté certificado por alguna agencia profesional de seguridad de software, como lo es "Computer Emergency Response Team" (CERT) *(Anexo B)*.

IV. Reglamento en el manejo de información

IV.I El usuario es responsable de proteger la información de su propiedad, por medio de respaldos, clave de acceso y asignación de permisos de lectura/escritura/ejecución.

IV.II El usuario no hará uso de la información del sistema a menos que sea de su propiedad, o esté autorizado para ello.

IV.III El usuario no destruirá o borrará información del sistema a menos que sea de su propiedad, o esté autorizado para ello.

IV.IV El usuario no modificará la información del sistema a menos que sea de su propiedad, o esté autorizado para ello.

V. Reglamento para la elección de claves de acceso

V.I El usuario está obligado a tener una clave de acceso para garantizar la privacidad de su cuenta, se recomienda elegirla con las siguientes características:

V.II la clave de acceso debe tener ocho o más caracteres,

V.III debe consistir en una combinación única de caracteres, letras, números o símbolos especiales, que NO sea palabra común, y pueda ser recordada fácilmente por el propietario.

V.IV NUNCA escribir la clave en ningún lugar, sólo memorizarla.

V.V No compartir la clave con NADIE o cambiarla en cuanto alguien la descubra.

V.VI Cambiar la clave cada mes, como mínimo, o cuando le sea indicado por el responsable del sistema.

VI. Reglamento Antivirus

VI.I El usuario será responsable de proteger sus archivos y sistemas de almacenamiento, contra virus informáticos.

VI.II Revisar con un programa antivirus actualizado el disco duro y la memoria residente de la computadora que vaya a utilizar cada vez que vaya a emplear el sistema.

VI.III Revisar con un programa antivirus actualizado los discos flexibles y otros sistemas de almacenamiento que se vayan a utilizar, cada vez que accese el sistema.

VI.IV Si se encuentran virus después de la revisión, desinfectar los archivos afectados. En el caso de encontrar algún virus en el sistema, reportarlo al encargado del mismo.

VI.V Cuando el sistema se vea afectado y se desconoce la causa, puede sospecharse de la existencia de un virus nuevo que no sea detectado por los antivirus, en este caso el usuario deberá reportar esta situación al encargado del sistema.

VII. Reglamento en el acceso al exterior de la RLD.

VII.I Cuando el usuario emplee los servicios de Internet deberá ser cuidadoso y responsable de la seguridad de su sitio.

VII.II El usuario tendrá acceso moderado a Internet en los horarios establecidos por el responsable del sistema.

VII.III Sus sesiones estarán relacionadas directamente con su labor y dentro del contexto universitario.

VII.IV El usuario no realizará actividades que puedan perjudicar a sistemas internos o externos.

Responsabilidades del área de seguridad en la implantación de políticas:

- Asegurarse de que todos los usuarios conocen su responsabilidad de mantener la seguridad del sistema.

- Dar a conocer las políticas actuales por escrito a todos los usuarios.
- Notificar cualquier renovación en las políticas.

El que una política de seguridad sea eficiente es responsabilidad no sólo de quienes la elaboran o de los que las implantan, la mayor parte de la responsabilidad la tienen los usuarios directos del sistema.

6.2.3 Mecanismos técnicos de seguridad a aplicarse en el SGIAA

La propuesta de los mecanismos técnicos a implantar en el SGIAA se especifican de acuerdo a la estructura determinada en el capítulo anterior (5.1.3).

1. ***Implantación de herramientas de seguridad***

Existen varios procedimientos que pueden ser utilizados para detectar la mayoría de los casos de uso no-autorizado de un sistema de cómputo. Estos procedimientos emplean herramientas, que bien pueden venir incluidas con el sistema operativo, o ser adquiridas con proveedores (Hoolbrook, 1991). Otra forma de adquirir herramientas de seguridad es mediante el servicio de Internet "ftp", en sitios dedicados a la investigación de seguridad computacional (*Anexo B*) donde se encuentran herramientas de dominio público y se pueden adquirir gratuitamente. En este último punto hay que resaltar que es recomendable que no se obtengan programas de cualquier sitio, sino sólo de aquellas instituciones que garanticen ser un sitio serio y

confiable. También se debe asegurar de que los programas estén certificados por compañías prestigiadas dedicadas a la seguridad computacional.

En el *Anexo B* se lista una serie de direcciones en las cuales pueden adquirirse las herramientas de seguridad más popularmente empleadas.

Algunos de las procedimientos que deben realizarse son los siguientes:

- *Reportes del estado actual de seguridad.* Es importante la supervisión periódica para detectar si existen "huecos" en el sistema. Dicha supervisión puede ser realizada por software especializado que analiza el estado actual en seguridad. Dichos programas generan un reporte con los resultados del análisis de permisos de acceso a directorios, existencia de claves de acceso para cada una de las cuentas y permisos de uso de comandos de alto riesgo, entre otros.
- *Monitoreo.* Monitorear un sistema es un procedimiento que tiene como meta el reconocer actividades no autorizadas dentro del mismo. Esto puede hacerse directamente por el administrador del sistema o por software especializado para este propósito.
- *Rastreo.* En el momento que ocurre una intrusión en el sistema el administrador puede realizar un rastreo del intruso apoyándose en herramientas especializadas, sin embargo, el rastreo no es siempre la manera óptima de salvar al sistema de una violación. Dependerá del

criterio del administrador y de la actividad que esté realizando el intruso. Por ejemplo, si se sorprende al intruso realizando actividades que no afecten el funcionamiento del sistema principal se puede hacer la persecución del mismo y encontrarlo antes de que éste realice alguna fechoría, en cambio, si el intruso ya realizó alguna violación grave (robar o alterar información confidencial), o la funcionalidad del sistema está a punto de verse afectada, lo mejor sería proteger el sistema de inmediato y evitar que el intruso siga trabajando en él.

Existen grupos de respuesta especializados en seguridad, a los cuales se puede recurrir para el servicio de rastreo e investigación después de ocurrida una intrusión, es recomendable notificar a tales grupos cuando ha habido una violación del sistema por externos, sin embargo, si se sospecha que la intrusión fue realizada por internos es preferible que la investigación se lleve a cabo por los responsables del sistema local.

2. ***Aspectos de administración de sistemas***

El ochenta por ciento de las violaciones de seguridad están basadas en los permisos. Establecer adecuadamente los permisos de acceso puede salvar al sistema de la mayoría de los problemas de seguridad que lo amenazan (Dereck, 1995).

Independientemente de que un intruso sea interno o externo los permisos de acceso son la clave para proteger los recursos del sistema. En efecto, la mayoría de las violaciones son realizadas por usuarios autorizados para usar el sistema (internos), ya que tienden a exceder dicha autorización aprovechándose de la apertura que se les brinda.

- *Control de acceso a la información.* La información puede ser utilizada con tres fines, lectura, escritura o ejecución, por lo tanto los permisos se centran en estos tres aspectos.

  - *Permiso de lectura.* Mediante este permiso un archivo puede ser abierto y los datos contenidos pueden ser leídos por el usuario que obtenga este permiso. Si el usuario fuera un intruso la confidenciabilidad se vería afectada.

  - *Permiso de escritura.* El permiso de escritura implica modificación de los datos. Esta modificación puede consistir en agregar, borrar o actualizar los datos. Por lo tanto, el abuso de este permiso sería una amenaza a la confidenciabilidad, integridad y disponibilidad de los datos.

  - *Permiso de ejecución.* La ejecución de los datos implica que el archivo será ejecutado como un programa, si se trata de un archivo en texto éste será ejecutado como un programa BATCH. Abusar de este

permiso podría provocar que el intruso ejecute programas para los que no está autorizado, pudiendo con ellos obtener ventajas en el sistema.

- *Control de usuarios.* Deben conocerse las clases de usuarios del sistema, (administrativos, académicos, administradores del sistema, etc.), formar grupos específicos de usuarios, asignar el nivel de acceso permitido a cada grupo y las aplicaciones que requieren y que les son permitidas, lo anterior conlleva a que la administración de los recursos sea adecuada.
- *Encriptación de información sensible del sistema.* Toda aquella información que se considere confidencial, como el archivo de claves de acceso entre otros, debe ser sometida a algún algoritmo de encriptación, de esta manera la información será ilegible a quien logre accesarla.
- *Sistema de respaldo.* Contar con un sistema de respaldo nos garantiza que aún cuando la integridad de los datos haya sido afectada, ya sea por error, fallas en el sistema o intrusión, aún así, podemos recuperar los datos e integrarlos nuevamente al sistema. Los respaldos deben realizarse periódicamente, los periodos no deben ser muy largos.

Control de calidad de Passwords. Además de la existencia de una política que recomiende al usuario la elección de un password de calidad debe existir un control que verifique si realmente existe dicha calidad. Existen programas que empleando palabras de diccionario, permutaciones, combinaciones de letras y números, y otras variantes, revisan todas las claves de acceso y detectan aquellas que son vulnerables, generando un reporte con los porcentajes correspondientes a las claves de calidad y a las vulnerables.

3. ***Mantenimiento y actualización de la Infraestructura***

Antes de implantar cualquier mecanismo técnico es importante conocer la infraestructura actual del sistema. Además de implantar mecanismos técnicos, es importante integrar en la infraestructura dispositivos físicos y lógicos que protejan a la red local de violaciones de seguridad desde el exterior (routers, firewalls, etc.).

4. ***Implementación y actualización de antivirus***

Debe contarse con antivirus residentes en cada máquina con disco duro. Es importante también hacer revisiones periódicas con distintos antivirus. La actualización de los antivirus es indispensable ya que día a día surgen

nuevos virus. En resumen pueden considerarse tres formas de prevención antivirus para los que existen programas especializados (García, 1996):

- *Monitoreo general:* Estos intentan prevenir la actividad viral antes de que ésta tenga algún efecto, como amenazar con escribir en otro programa ejecutable, dar nuevo formato al disco duro, etc.
- Búsqueda de virus (*Scanners*): Consisten en el reconocimiento de patrones o secuencias de *bytes* de virus conocidos, sin embargo, existen algunos que emplean técnicas heurísticas para reconocer un código de virus. La mayoría de los "scanners" incluyen removedores de virus.
- *Supervisión de integridad o detección de modificaciones en el sistema:* Este tipo de programa realiza una revisión del sistema, denominada "*checksum*", comparando los valores originales almacenados contra los nuevos valores calculados y verifica si hubo alguna modificación. Esto puede detectar virus desconocidos lo mismo que conocidos, y provee una detección "genérica". Por otro lado, las modificaciones pueden haberse hecho por razones distintas a los virus. Usualmente corresponde al usuario determinar que modificaciones fueron realizadas intencionalmente y cuales pueden ser atribuidas a los virus,

sin embargo existen algunos productos que ayudan al usuario en tomar esta decisión.

5. ***Medidas de protección en transacciones al exterior***

- *"Paredes de fuego", Firewalls.* El principal objetivo de las "paredes de fuego" es proteger una red de otra. Éste termino es empleado generalmente para describir una extenso rango de funciones y arquitecturas de dispositivos que protegen la red. En general, la "pared de fuego" es colocada entre la red interna y la externa. Ésta actúa como un punto de choque que monitorea y rechaza niveles de aplicación en el tráfico de la red (Siyan, 1995).
- *Encriptación.* La información que viaja a través de las redes internacionales puede ser interceptada en cualquier punto de la red, por ello cualquier información que se considere secreta o que pone en riesgo la competitividad de la institución y sea transferida por medio de los servicios de Internet, deberá ser sometida a algún algoritmo de codificación criptográfica.

Es importante que los mecanismos técnicos de seguridad al igual que las políticas cumplan con el ciclo de vida propuesto anteriormente.

6.2.4 Modelo General de Seguridad Computacional -MSC- para el SGIAA

Aquí se establece un modelo general de seguridad computacional aplicable al SGIAA. En éste se resumen las partes desarrolladas en los capítulos anteriores.

El modelo general integra las etapas relevantes del análisis de riesgos, esto es, la descripción de los **recursos** con que cuenta el sistema, de los **riesgos** que amenazan a dichos recursos y de las **medidas de seguridad** que deben tomarse para prevenir y proteger los recursos contra tales riesgos; así como el análisis de las necesidades básicas del usuario, el cual describe quienes son los **usuarios** del sistema, cuales son las **aplicaciones** indispensables que dan al sistema, y la **utilidad** que esperan. A continuación se describen las seis partes principales que conforman el modelo:

- **Recursos.** Esta parte del modelo la conforma el Factor Técnico del sistema, los elementos son:

- *Hardware,* conformado por los dispositivos físicos del sistema (discos, conexiones, dispositivos de E/S, etc.).

- *Software,* conformado por dispositivos lógicos ejecutables (sistema operativo, programas y aplicaciones).

- *Datos,* en este elemento se considera la información.

- **Riesgos.** Aquí se consideran los principales riesgos que pueden afectar al Factor Técnico:

- Uso no autorizado. *- Cambios no autorizados.* *- Destrucción.*

- **Medidas.** Menciona las medidas de seguridad a implantarse para la seguridad del sistema, estas son:

- Políticas de Seguridad, las cuales sirven como un medio de prevención dando a conocer la forma de evitar incidentes comunes.

- Mecanismos técnicos de seguridad, se implementan como medida de protección, impidiendo en un grado determinado acciones que puedan amenazar al sistema.

- Plan de contingencia, es un plan de acción en el caso de que haya ocurrido una violación en contra de la seguridad del sistema.

- **Usuarios**. Esta conformado por el Factor Humano:

- Directivos. *- Administradores del Sistema.* *- usuarios directos.*

- **Aplicaciones**. Se refiere al uso primordial que el usuario da a la información del SGIAA:

- Transmisión. *- Almacenamiento.* *- procesamiento.*

- **Utilidad**. Considerada el objetivo primordial del sistema, desde el punto de vista de seguridad computacional, la utilidad del sistema depende de las características de:

- *privacidad,* que los recursos conserven su calidad de confidencial o privado cuando así lo requiera el propietario del mismo.

- *Integridad,* que los recursos estén completos y sin alteraciones.

- *Disponibilidad,* que el usuario encuentre accesible aquellos recursos que le son indispensables para su labor.

Con el fin de dar una apariencia simétrica y equilibrada al MSC, concediendo la misma importancia a cada una de sus partes, éste se representa como un cubo en el que cada una de las caras tiene asignada una de las partes que lo conforman, subdivididas en los aspectos esenciales para cada parte. (Figuras 20 y 21).

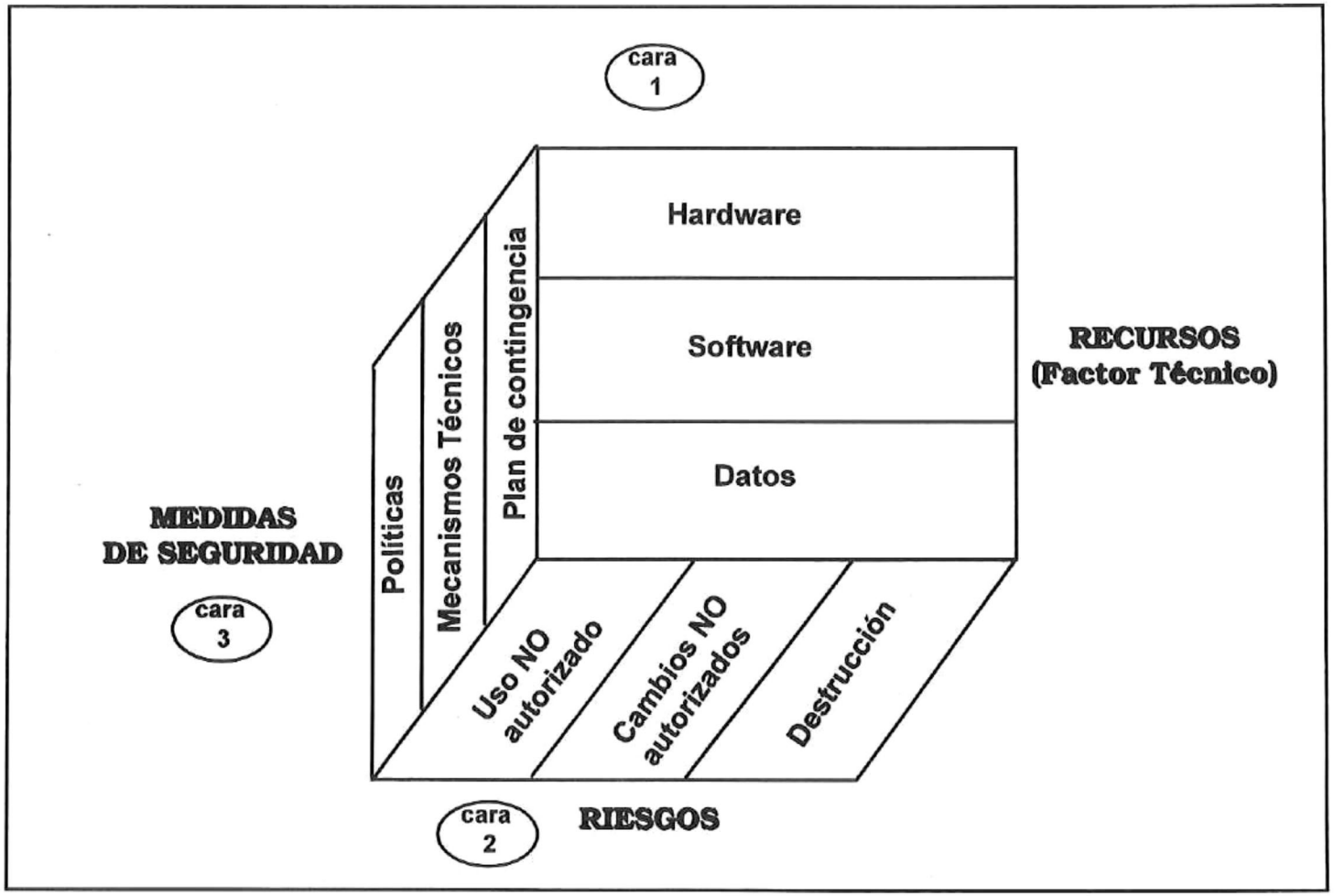


Figura 20 Modelo de seguridad Computacional para el SGIAA (Sección I)

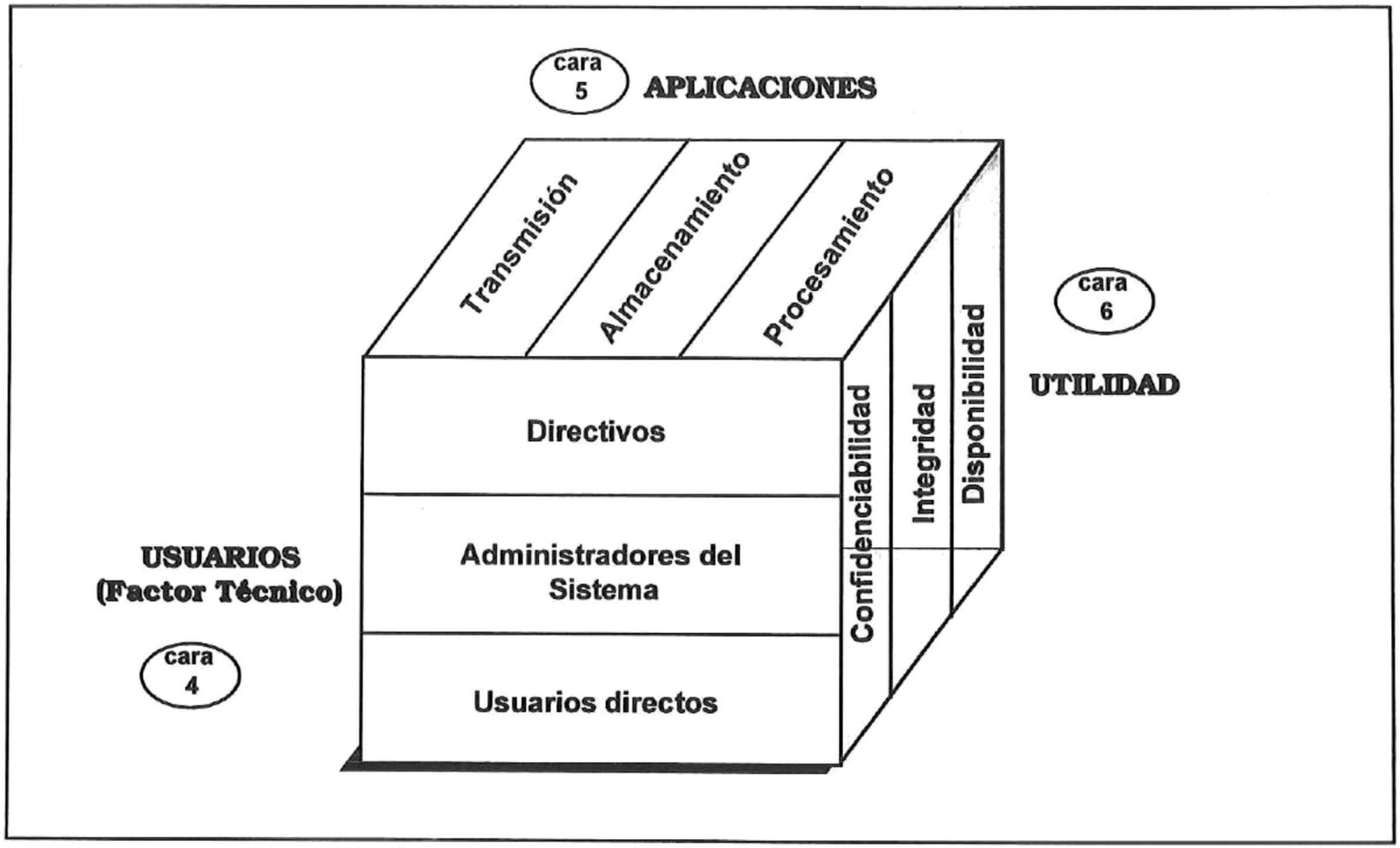


Figura 21 Modelo de seguridad Computacional para el SGIAA (Sección II)

VII Recomendaciones

7.1 *Estadio 7.* Acciones para resolver los problemas o mejorar la situación.

De acuerdo a los estudios realizados se ha detectado énfasis en la actualización de los recursos del sistema de acuerdo a las necesidades de aplicación, en cambio, se han pasado por alto las necesidades de protección. Es necesario tomar conciencia de la problemática actual en seguridad, y realizar las acciones necesarias para evitar que el sistema se vea afectado por las diferentes amenazas detectadas.

Con base en el trabajo previo (Estadios 1-6) se recomienda realizar las siguientes acciones:

7.1.1 Promover la seguridad en las áreas de cómputo

- Instruir a los usuarios en aspectos básicos de seguridad (Calidad de passwords, protección de archivos, virus, responsabilidades de usuario, riesgos en transferencia de datos, entre otros).

- Actualización de la administración de sistemas en aspectos de seguridad avanzada. (control de información, comandos de alto riesgo, firewalls, encriptación, etc.)
- Solicitar a los directivos los requerimientos para la implantación y mantenimiento de medidas de seguridad.

7.1.2 Implantar Políticas de Seguridad

- Implantar las políticas de seguridad propuestas, y realizar las especificaciones particulares para cada subred.
- Promover y dar a conocer por escrito dichas políticas.
- Seguir el ciclo de vida propuesto para las políticas de seguridad y mantenerlas en constante evolución a la par con los objetivos del sistema.

7.1.3 Implementar Mecanismos técnicos de Seguridad

- Implementar los mecanismos técnicos propuestos.
- Seguir el ciclo de vida propuesto para los mecanismos técnicos de seguridad y actualizarlos de acuerdo a la tecnología actual y a las necesidades de la administración.
- Tener un control de los recursos con que cuenta el sistema.

7.1.4 Creación de un Área de Seguridad Computacional

- Crear un Área de Seguridad Computacional dentro de UABC o de la Facultad de Ciencias, que trabaje en coordinación con la Administración de Sistemas en aspectos específicos de seguridad.
- Estar a la vanguardia en aspectos de seguridad, organizando cursos internos de actualización, en coordinación con otras instituciones que tienen experiencia en aspectos de seguridad computacional
- Suscribirse a grupos de discusión y listas especializadas en seguridad computacional.
- Elaborar un plan de contingencia, que describa las acciones a tomar en distintos casos de intrusión, fallas, errores o desastres; el cual servirá como auxiliar en la toma de decisiones, cuando llegue a presentarse alguno de los casos previstos.

Es importante dar continuidad a la actividad que en cuanto a seguridad se ha iniciado en la institución, así mismo, es indispensable promover la ética computacional entre las nuevas generaciones de usuarios, pues de ello depende el respeto que merecemos como "seres usuarios" en esta nueva era cibernética.

VIII Resultados

- Se obtuvo el Modelo de Seguridad Computacional para el Sistema Global de Información Académica y de Apoyo, SGIAA, en el que se exponen los elementos que deben considerarse para implantar las medidas de seguridad, como son: Factor Humano, Factor Técnico, Aplicaciones, Riesgos, Utilidad y Medidas de Seguridad (Capítulo VI).
- El modelo se desarrolló empleando la Metodología para Sistemas Suaves (Capítulo III).
- Se identificó la problemática en seguridad computacional que existe en la red UABC/uE, encontrando puntos vulnerables en la infraestructura, en el control de acceso a los recursos y en las políticas de uso y protección del sistema (Capítulo IV).
- Se detectaron los riesgos que amenazan al sistema (4.2.2).
- Se determinaron las medidas a implantarse en los distintos grados de seguridad: prevención, protección y acción contra cualquier incidente (Figura 10).
- Se propuso un modelo conceptual para el análisis de riesgos (Figura 11).

- Se determinaron los niveles de acceso a la información, clasificándose en: Nivel Privado, Nivel Público Interno y Nivel Público Externo, (5.1.1) de acuerdo a sus características, también, se establecieron los permisos de acceso a la información de acuerdo a su nivel de acceso (Figuras 16,17,18 y 19).
- Se definieron los cambios deseables factibles con base en los resultados de la comparación del diseño deseable vs. situación real (Tablas XXI,XXII,XXIII) y (6.2).
- Se elaboraron las estructuras para el establecimiento de las políticas de seguridad (5.1.2) y de los mecanismos técnicos de seguridad (5.1.2), proporcionando los parámetros que deben considerarse en la elaboración de los mismos.
- Se diseñaron los modelos conceptuales del ciclo de vida a que están sujetas las políticas y los mecanismos técnicos (Figuras 13, 14 y 15).
- Se desarrollaron: la política de seguridad y los mecanismos técnicos a aplicarse en el SGIAA (6.2.2 y 6.2.3).

IX. Discusión

La seguridad computacional, en la actualidad, no es una aplicación más, sino una necesidad inminente, todo sistema computacional corre cierto grado de riesgo y su vulnerabilidad amenaza la utilidad del mismo. El número de usuarios especializados se incrementa día con día; la competencia, la ambición, el desempleo, la experimentación o el no tener algo mejor que hacer con el conocimiento adquirido, lleva a ciertos usuarios a utilizar o crear aplicaciones que perjudican a terceros y que de alguna manera benefician o satisfacen al autor de la intrusión. No obstante, la seguridad de un sistema no sólo se ve amenazada por la intrusión, sino también por daños accidentales, los cuales pueden ser ocasionados por error del usuario, errores o fallas del sistema o por desastres naturales.

En el presente trabajo se aborda el problema de seguridad para el Sistema Global de Información Académica y de Apoyo, dado que, es un sistema de alcance global, implantado dentro de una red heterogénea, que maneja información a niveles intra en interinstitucionales y en el cual los usuarios tienen

distintos derechos de acceso. Estas y otras características hacen del SGIAA un caso interesante de estudio desde el punto de vista de la seguridad computacional, además, al tratarse de un sistema en proceso de implantación representa otra ventaja, ya que, puede ajustarse a las medidas de seguridad necesarias con más aceptación.

Para la implantación de las medidas de seguridad en el SGIAA se propuso un modelo que muestre cuáles son las vulnerabilidades y amenazas, y cómo pueden evitarse, involucrando a quiénes toman parte en este problema.

Algunas de las razones de proponer un modelo son:

- en el SGIAA participan distintos departamentos y unidades académicas, cada uno de ellos tiene requerimientos diferentes en cuanto a seguridad;
- el modelo permite establecer un estándar al implantar las medidas de seguridad, adecuándose a las necesidades individuales de cada área;
- el grado de riesgo que amenaza a un sistema es variable conforme pasa el tiempo;
- el modelo puede ser empleado para mantener el ciclo de vida de las medidas de seguridad y adaptarlas a tales cambios.

Actualmente no existe una metodología establecida para el análisis y desarrollo de modelos de seguridad, para el presente trabajo se empleó la Metodología para Sistemas Suaves, (Checkland, 1993). Se eligió esta metodología

metodología por adecuarse a las necesidades para desarrollar el modelo de seguridad, ya que permite, *percibir* la problemática actual y las partes involucradas en ella, *predecir* las situaciones que pudieran amenazar al sistema, *comparar* las condiciones de seguridad actuales con las que se proponen, y *decidir* cuales serán los niveles de seguridad apropiados para cada parte del sistema, como resultado el sistema enfrentaría una situación cambiada con respecto a seguridad.

Por otro lado, los trabajos realizados sobre seguridad son relativamente pocos y recientes, si se comparan con la cantidad de trabajos en otras áreas de cómputo. Cada uno de los trabajos tomados como referencia, tienen un enfoque distinto sobre seguridad, pero todos coinciden en que la seguridad es indispensable y particular para cada sistema. Se realizó una selección de las propuestas de diferentes autores: Holbrook,1991; McCumber,1991; Derek,1993; Zamboni,1995; entre otros, las cuales se integraron a este modelo de manera que se obtuviera una propuesta única, proponiendo la metodología, los procesos, las entidades y equilibrio entre seguridad y utilidad, para la futura implantación de medidas de seguridad en el SGIAA.

Por tratarse de un sistema de información perteneciente a una institución académica, UABC/uE, podría considerarse razonable sacrificar la seguridad del sistema y procurar dar un máximo de facilidades al usuario para que emplee el

mayor provecho; esto sería benéfico si todos los usuarios internos y externos respetaran los derechos de otros usuarios, desafortunadamente esto no siempre es así, ya que existen quienes se aprovechan del hecho de que no existan restricciones de uso y realizan actividades que pueden perjudicar al sistema interno o a otros sistemas externos, poniendo en riesgo la integridad no sólo del sistema afectado, sino la de la institución desde la cual se realizó la intrusión; por lo tanto, el hecho de ser una institución académica brinda la oportunidad de formar al usuario dentro del marco de una ética computacional y concientizarlo de la necesidad de tomar las medidas de seguridad computacional y los beneficios que esto conlleva. Además, procurar que el sistema sea seguro no implica que el sistema no sea útil como muchos creen, en cambio, no garantizar un sistema seguro provocaría que el usuario evitara su uso, convirtiéndolo en un sistema "inútil", debido al grado de riesgo que representaría trabajar en él.

En este estudio, el SGIAA se dividió en dos factores: el Factor Humano y el Factor Técnico (Zamboni, 1995). Ésto permitió identificar las entidades que participan en el sistema, quiénes usan directa o indirectamente el sistema (Factor Humano) y cuáles son los recursos que lo conforman (Factor Técnico). Esta división fue determinante en el estudio y desarrollo de este modelo, ya que una vez ubicados los elementos del sistema en el factor correspondiente fue

sencillo reconocer las interacciones, entre ambos, y la manera en que afectan la seguridad y utilidad del sistema.

Las aplicaciones de *transmisión, almacenamiento y procesamiento de información* (McCumber, 1991) son la base en todo sistema de información, por lo tanto lo son para el SGIAA, en el MSC se considera que la seguridad del sistema depende de cómo se utilicen dichas aplicaciones.

Las características de *integridad, disponibilidad y privacidad* (McCumber, 1991) pueden ser garantizadas si las aplicaciones se rigen por las medidas de seguridad adecuadas, en términos de seguridad, puede decirse que el resultado de una aplicación es la utilidad sólo si cumple con dichas características. Brindar una utilidad satisfactoria es el propósito principal de todo sistema, por ello el Modelo de Seguridad Computacional para el SGIAA se enfoca en este término como una de sus partes más importantes, así mismo, se determina un equilibrio entre utilidad y seguridad, ésto con la finalidad de que las medidas de seguridad no interfirieran con la utilidad del sistema. Ésto se logró analizando las necesidades de aplicación de los usuarios y los principales riesgos que corre el sistema.

El modelo conceptual utilizado para el diseñar los niveles de acceso a la información (5.2.2), permite "etiquetar" la información del SGIAA de acuerdo a la privacidad de su contenido, dado que, los niveles se clasifican en: nivel

público externo, nivel público interno y nivel privado; por lo cual es más claro y sencillo identificar los permisos de acceso que deben asignarse a cada usuario o grupo de usuarios.

El medio para obtener la utilidad con las características antes mencionadas, además de una buena administración del sistema, fue proponer la implantación de medidas de seguridad que garanticen la prevención y protección contra los riesgos que amenazan el sistema, estas estructuras son las políticas de seguridad y de los mecanismos técnicos (5.1.2. - 5.1.3.). La ventaja de contar con éstas es que se marcan los lineamientos a seguir en la elaboración y actualización de dichas medidas. También, estas medidas deben mantener un ciclo de vida (5.2.3), de manera que no se hagan obsoletas en un tiempo determinado; ya que los riesgos a que se enfrenta el SGIAA, son cambiantes y en constante evolución.

Se desarrollaron las políticas de seguridad y los mecanismos técnicos particulares para el SGIAA, con base en las estructuras propuestas, con la finalidad de tener una pauta de cómo pueden emplearse dichas estructuras y ser adaptadas a cualquier otra área vinculada con el SGIAA, adecuándose a las necesidades particulares.

A manera de sinopsis, el diseño del Modelo General de Seguridad Computacional para el SGIAA, reúne los conceptos fundamentales

desarrollados en el presente trabajo. Su representación gráfica, en un cubo, plasma la idea del equilibrio que existe entre las partes que interactúan en el modelo, como fue detallado a lo largo del desarrollo.

Un resumen del presente trabajo fue enviado al FOndo para la Modernización de la Educación Superior (FOMES) como parte del reporte sobre el proyecto SGIAA. Las propuestas sobre las clasificaciones de la información (6.2.1) fueron consideradas en el diseño de las bases de datos del SGIAA. Las medidas de seguridad fueron aplicándose conforme el desarrollo del SGIAA, sin embargo, no se han implantado en su totalidad, esto se debe a la necesidad de un área de seguridad computacional, dentro de la administración de cómputo, la cual sea responsable de estas funciones específicas.

La realización de este trabajo influyó no sólo en el SGIAA, sino en distintas áreas de la red UABC/uE, dado que se comparten los mismos recursos, pero una contribución de gran importancia fue la de concientizar a la mayoría de los usuarios en la necesidad de la seguridad computacional, pues al realizar las encuestas personalmente en cada uno de los departamentos, se despertó el interés en la seguridad computacional, tema desconocido por muchos usuarios, y se adoptaron medidas de seguridad básicas para todo sistema (respaldo de información, instalación de antivirus, etc.)

X Conclusiones

I. La Metodología para Sistemas Suaves fue el adecuado para el estudio, desarrollo y diseño del Modelo de Seguridad Computacional para SGIAA debido a su flexibilidad, adaptabilidad y a su evolución por estadios.

II. Los conceptos de seguridad computacional y de sistemas de información citados fueron la base de las propuestas del MSC para el SGIAA.

III. Los modelos conceptuales diseñados de acuerdo al análisis de resultados, llevaron a una propuesta única que se integra en el MSC que servirá de guía durante la implemetación de herramientas y políticas de seguridad en el SGIAA; este modelo es de utilidad, también, para otros sistemas que tengan características similares a las del SGIAA.

IV. El modelo desarrollado establece un equilibrio entre la utilidad y la seguridad del sistema, considerando tanto las necesidades del Factor Humano como las del Factor Técnico. La característica de este equilibrio radica en conocer los objetivos para los que fue creado el sistema, satisfacer dichos objetivos y prevenir todas aquellas acciones que amenacen con hacerlos fallar.

XI Bibliografía

(Camacho, et al., 1995) Camacho L. Sylvia, Mendoza D. Concepción. 1995. Memorias del "Día Internacional de la Seguridad en Cómputo 1995: Recomendaciones de Medidas de Seguridad en una LAN de Sistemas Heterogéneos Conectada a Internet. Experiencias en Red-CICESE". Centro de Investigación Científica y de Educación Superior de Ensenada. México. p. 1-3.

(Checkland, 1990) Checkland, P. & Scholes. 1990. "Soft Systems Methodology in Action". Wiley. England.

(Derek, 1993) N. Derek Arnold. 1993. "UNIX Security, a practical tutorial". ITDC. McGraw Hill. USA.

(Fine, 1990) Fine Leonard H. 1998. "Seguridad en Centros de Cómputo: Políticas y Procedimientos". Trillas. 2a. Edición. México.

(Holbrook, et al., 1991) P. Holbrook, CICNet; J. Reynolds. 1991. "Site Security Handbook". ISI. USA.

(Johnson, 1995) Johnson Johna Till. 1995. "Enterprise Security: Better Safe Than Sorry". March, 1995: 114.

(Klein, 1995) Klein Daniel V. 1995. "Foiling the Craker: A Survey of, and Improvements to, Password Security". Carnegie Mellon University. USA.

(Mallén-Fullerton, 1995) Mallén - Fullerton Guillermo M. 1995. "Epidemiología de Virus Informáticos". Universidad Iberoamericana. México.

(McCumber, 1992) John McCumber. 1992. "Information Systems Security: a Comprehensive Model". PRC Enterprise Assurance Group. USA.

(Medina, 1997) Medina R. Laura E. 1997. "Análisis y Diseño del Sistema de Información de la Facultad de Ciencias de la UABC". Universidad Autónoma de Baja California. México.

(Miller, 1996) Miller Stewart. 1996."Secure Your Data: Web Site Attacks On The Rise!". Interactive Week, Jan. 1996: 37-39.

(Moran, et al., 1995) Morán y S. A. Leopoldo; Luna S. Judith; Alvarez Omar; Martínez Evelio. 1995. "Proyecto FOMES: Sistema Global de Información Académica y de Apoyo". Universidad Autónoma de Baja California. Ensenada, B.C. . México.

(Oxford, 1991) Oxford Paperback Reference. 1991."Dictionary of Computing". Oxford University Press. 3rd Edition.

(Ramírez, 1996) Ramírez Barreto María Elizabeth. 1996. "Aplicación de una Metodología de Sistemas Suaves para el Mejoramiento de un Programa de Posgrado". Instituto Politécnico Nacional. México.

(Robinson, 1995) Robinson Teri. 1995. "Security Overkill?". CommunicationsWeek, Nov. 1995 : 63-74.

(Siyan, et al., 1995) Siyan Karanjit, Ph. D.; Hare Chris. 1995. "Internet Firewalls and Network Security". NRP. USA.

(Sun, 1994) "System & Network Administration", Rev. A. Sun Microsystem.

(Zamboni, 1995) Zamboni Diego. 1995. Memorias del "Día Internacional de la Seguridad en Cómputo 1995: Experiencias en la formación del Área de Seguridad en Cómputo de la DGSCA". Universidad Autónoma de México. México.

XII

Anexo A

Cuestionarios Aplicados

I. Características Básicas del Equipo

Departamento: **Evaluación:**

1. Máquina: _____ ☐ PC. ☐ Estación de trabajo. ☐ _____.	☐ Conectada a Red_____ (RED) ☐ Independiente:_____ (Prop.)
2. Procesador:	
3. Capacidad Disco Duro:	4. RAM:

5. Función del equipo:
6. Usuarios del equipo:
7. Permisos de acceso:
8. Servidor:

9. Sistema Operativo:	10. Versión:

11. Observaciones:

II. Calidad de Passwords

1. Indique con una **X** si su password está basado en uno de los siguientes tipos:

- ☐ Basado en el nombre de su cuenta de usuario.
- ☐ Esta basado sus iniciales o nombre.
- ☐ Nombres comunes (masculino o femenino) o de lugares.

- ☐ Palabra del diccionario:
  - ☐ escrita tal y como aparece en éste.
  - ☐ con alunas o todas las letras mayúsculas.
  - ☐ en orden invertido.
  - ☐ palabra de diccionario en orden invertido con algunas o todas las letras mayúsculas.
  - ☐ con una letra arbitraria convertida en caracter de control.
  - ☐ con números (0,1,2,5) sustituyendo las letras (O,I,Z, S).
- ☐ Conjugada (plural,gerundio,pasado,etc)
- ☐ Secuencia de caracteres según el patrón del teclado.(ej. "aaaa", "lolo","qwerty",etc.)
- ☐ Secuencia de solo números (ej. Número de seguro social, número de teléfono, núm. De casa, etc.)
- ☐ No contiene mayúsculas y minúsculas mezcladas.
- ☐ No contiene números y letras mezcladas.
- ☐ No contiene letras y puntuaciones mezcladas
- ☐ Combinación de letras y números a semejanza de placas de auto.

2. Longitud del password que usa (# de caracteres):_____.
3. Periodicidad con la que cambia su password:_____veces cada _____.
4. Cuantas personas conocen su password: _____.

Observaciones:

III. Virus en el sistema

Evaluar con:

1. *Scan (Ultima Versión).*
2. *F-Prot (Ultima Versión).*
3. *Antivirus para Windows 95 (en caso necesario).*

4. Antivirus Instalados en el sistema:
☐ F-PROT ☐ SCAN ☐ CPAV ☐ Otros:

5. Periodicidad con la que se actualizan las versiones:
☐ semanal ☐ mensual ☐ semestral ☐ otra:

6. ¿Existe copia de los antivirus en disco flexible con sistema de arranque?
☐ SI ☐ NO

Nota: Imprimir reporte o tomar los datos de éste.

7. Observaciones:

IV. Respaldo de Información

1. Forma en que se respalda la información:		2. Información que se respalda:	
☐ Total	☐ Incremental	☐ Datos	☐ Programas
☐ Otros:		☐ Otros:	

3. Periodicidad de los respaldos:			
☐ Diaria	☐ Semanal	☐ Mensual	☐ Otra:

4. Tiempo durante el que se guarda el respaldo:
____dias. ____semanas. ____meseses. ____años.

5. Observaciones:

V. Políticas de Seguridad que se aplican

Mecanismos de seguridad que se aplican en:

1. Hardware

Actividad:	*Periodicidad:*			
☐ Inventario.	☐ Semanal.	☐ Mensual.	☐ Anual	☐ Otro:
☐ Mantenimiento.	☐ Semanal.	☐ Mensual.	☐ Anual	☐ Otro:
☐ Actualización de equipo	☐ Semanal.	☐ Mensual.	☐ Anual	☐ Otro:

2. Software

☐ Respaldos:	Periodicidad:
Programas con Licencia:	%
Programas copia:	%
Sistema de arranque en: ☐ Disco duro. ☐ Disco flexible.	
Permisos de acceso a los programas:	

3. Datos

Citar el tipo de protección que se da a:

Bases de Datos: ☐ Ninguna ☐ Clave.	☐ Encriptación ☐ Archivo oculto.	☐ Permisos especiales.	☐ Otros:
Información confidencial: ☐ Ninguna ☐ Clave.	☐ Encriptación. ☐ Archivo oculto.	☐ Permisos especiales.	☐ Otros:
Información general: ☐ Ninguna ☐ Clave.	☐ Encriptación. ☐ Archivo oculto.	☐ Permisos especiales.	☐ Otros:

4. Usuarios

¿Quienes son los usarios directos del sistema?

☐ Directivos ☐ Becarios ☐ Maestros ☐ Investigadores ☐ Otros:

☐ Secretarias ☐ Servicios Sociales ☐ Alumnos ☐ Externos

¿Que aplicaciones se utilizan en el sistema?

☐ Editores de texto. ☐ Compiladores. ☐ Navegador de internet. ☐ Juegos.

☐ Hoja Electrónica. ☐ Procesamiento de Imágenes. ☐ Transferencia de archivos (ftp, etc.) ☐ Otros (esp.):

☐ CAD. ☐ Multimedia. ☐ Correo electrónico.

Mencione las aplicaciones que se prohiben en el sistema y porqué:

Aplic.- ?: Aplic.- ?: Aplic.- ?:

Aplic.- ?: : Aplic.- ?: Aplic.- ?:

Aplic.- ?:

¿Cuales son los horarios en que se permite usar el sistema?:

¿Existe permiso para usar el sistema fuera de este horario?

☐ NO

☐ SI, ¿bajo qué condiciones?:

5. Documentación

Documentos que apoyen al usuario para el uso apropiado del equipo:

☐ Manuales.
☐ Instructivos.
☐ Reglamentos.
☐ Resúmenes de Cursos.

6. Materiales

Políticas de protección en materiales de uso frecuente en el sistema:

Papel	☐ No hay control. ☐ Sí hay control; especifique:
Formas impresas	☐ No hay control. ☐ Sí hay control; especifique:
Cintas para impresora	☐ No hay control. ☐ Sí hay control; especifique:
Toner para impresora.	☐ No hay control. ☐ Sí hay control; especifique:
Discos y cartuchos	☐ No hay control. ☐ Sí hay control; especifique:

7. Personal que se encarga del mantenimiento y asesoría:

☐ Aula Equipada ☐ C.E.C.U.U.E. ☐ Ninguno ☐ Otros;especifique:

8. Actividades realizadas que apoyen al usuario en el conocimiento y uso adecuado del sistema:

☐ Ha asistido a cursos. ☐ Ha recibido instrucción.

Cuales: Por parte de quien:

☐ Otros; especifique:

9. Protección del equipo contra: *(Relacionar ambas columnas.)*

☐ Desastres naturales.
☐ Robo.
☐ Mal funcionamiento o fallas físicas.
☐ Cambios de lugar de los dispositivos.
☐ Acceso de usuarios no autorizados.
☐ Maltrato de equipo.

10. Medidas de protección:

☐ _____.
☐ _____.
☐ _____.
☐ _____.
☐ _____.
☐ _____.
☐ _____.

11. Observaciones:

Anexo B

Direcciones en Internet con información sobre Seguridad Computacional

a) Equipos de Respuesta

Distintas organizaciones han formado grupos especializados para tratar con problemas de seguridad. Estos equipos reúnen información sobre los "hoyos" de seguridad que existen en ciertos programas ó sistemas y lo difunden a aquellos interesados, también, dan asistencia para restaurar los daños ocasionados después de una violación de seguridad. Los equipos cuentan con distribución de listas por correo electrónico así como un número telefónico al cual se puede llamar para solicitar información o reportar un problema. A continuación se enlistan algunos de estos equipos más reconocidos y la dirección WWW (World Wide Web):

CERT (Computer Emergency Response Team):

http://www.cert.org/

info.cert.org/pub/

COAST (laboratorio de investigación de tecnología y herramientas de seguridad computacional de "Purdue University"):

http://www.cs.purdue.edu/coast/199

ftp://coast.cs.purdue.edu/pub

CIAC (Computer Incident Advisory Capabily):

http://ciac.llnl.gov/

ftp://ciac.lllnl.gov/pub/ciac/bulletin/

b) Listas de correos y Boletines

En Internet aparecen regularmente noticias, boletines y avisos, sobre lo último en herramientas y "hoyos" en seguridad algunos de los más reconocidos son:

COAST Newsletter "Coast Watch":

http://www.cs.purdue.edu/coast/coast-news.html

IEEE-CS TC on Security and Privacy letter

http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher

NetWatchers Front Page

http://www.ionet.net/-mdyer/netwatch.shtml

Nota: (Las direcciones pueden cambiar en el transcurso del tiempo)