UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO

FACULTAD DE INGENIERÍA

# POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD PARA LA RED SIAE

TESIS

**Que para obtener el título de**

INGENIERO EN COMPUTACIÓN


**Presenta**
**SANDRA GARCÍA RESÉNDIZ**
**Director**
**ING. ARMANDO VEGA ALVARADO**
**Coodirectora**
**M.C. MARIA JAQUELINA LÓPEZ BARRIENTOS**



México, D.F. Octubre del 2003

# INDICE

## Prefacio

Hoy en día el uso de sistemas de información en todos los ámbitos (militar, comercial, financiero) se ha incrementado, la mayoría de empresas e instituciones basan gran parte de su productividad en dichos sistemas.

El principio de la seguridad de una red es proteger el entorno de cualquier tipo de amenaza mediante servicios de seguridad, mecanismos y técnicas para hacer cumplir una política de seguridad.

Las políticas de seguridad informática definen de manera clara y formal todo aquello que se considera valioso para la organización y especifican las medidas que se deben tomar para proteger dichos activos, aclaran qué se protege y porqué, establecen las responsabilidades de la protección y ponen las bases para resolver conflictos posteriores.

Los procedimientos de seguridad son pasos secuenciales que se llevan a cabo para la prevención y corrección de posibles ataques o desastres que pudiera llegar a sufrir el sistema de información.

En base a lo anterior la creación de las Políticas y Procedimientos de Seguridad que se pretenden implantar en la Red del Sistema Integral de Administración Escolar (SIAE) son de vital importancia, ya que la protección del entorno es vital tanto como para la supervivencia del sistema como para evitar pérdidas económicas y/o pérdidas horas-hombre.

## Objetivo

Crear e implementar las políticas y procedimientos de seguridad, para garantizar la integridad, confidencialidad y disponibilidad de los recursos que componen el Sistema Integral de Administración Escolar (SIAE) de la Dirección General de Administración Escolar (DGAE).

## Contenido

**Capitulo 1.** En este capitulo se encuentran los antecedentes de la Dirección general de Administración Escolar (DGAE) su objetivo, su misión y sus funciones así como su estructura interna.

Se explica lo que es el Sistema Integral de Administración escolar (SIAE) el cual permite la simplificación, agilización y descentralización de los trámites para todos

los alumnos que se encuentran inscritos ya sea en escuelas, facultades, escuelas preparatorias y CCHs, esta información debe ser de carácter seguro y confiable.

También es este capitulo se definen los conceptos que se consideraron esenciales para una mejor comprensión del tema y del objetivo al que se quiere llegar.

**Capitulo 2.** Este capitulo trata de todo el análisis que se le tuvo que hacer al sistema para poder redactar las políticas de seguridad.

Para el análisis en primer instancia, se tuvo definir la misión o propósito con el fin de identificar el objetivo de seguridad, se enlistaron los elementos lógicos y físicos con los que cuenta el sistema, por último se hizo un análisis de riesgos y vulnerabilidades para detectar los activos más importantes del sistema informático, sus posibles riesgos y consecuencias.

**Capitulo 3.** En este capitulo se plasmaron las políticas ya redactadas que requiere el sistema.

El objetivo general consiste en la realización de un **Plan de Seguridad Informática** para **La Red SIAE**, en donde se definen los lineamientos para promover la planeación, el diseño e implantación de un modelo de seguridad en la misma con el fin de establecer una cultura de la seguridad en la organización. Asimismo, la obliga a redactar sus propios procedimientos de seguridad, los cuales deben estar enmarcados por este plan.

La definición de la presente política de seguridad informática y de los estándares asociados es esencial para hacerles saber a todos los empleados de la  y personas que utilicen los servicios que brinda el SIAE lo que pueden hacer y lo que no, para salvaguardar los activos informáticos de la **Subdirección de Sistemas de Registro Escolar**.

Sobre lo que pueden hacer, las políticas les señalan como hacerlo y sobre lo que no deben hacer les marca claramente sus responsabilidades.

**Capitulo 4.** Dentro de este capitulo se llevaron a cabo algunos de los procedimientos que requieren las políticas antes redactadas.

Los procedimientos de seguridad de la Red SIAE se describen en el siguiente capitulo, con la finalidad de indicar cómo hay que llevar a cabo la protección. Estos procedimientos como se dijo antes también constituyen los mecanismos para hacer cumplir las políticas. Además resultan útiles pues indican detalladamente qué hay que hacer cuando sucedan incidentes específicos, son referencias rápidas en caso

de emergencia y ayudan a eliminar los puntos de falla críticos, además de indicar quien va a realizar cada uno de los procedimientos aquí enlistados.

**Capitulo 5.** Por último en este capitulo se enlistan las principales características de algunas de las herramientas de seguridad informática que se utilizan los administradores de la base de datos.

Estas herramientas de seguridad son programas diseñados para ayudar al administrador ya sea alertándolo o realizando por sí mismo las acciones necesarias a mantener su sistema seguro.

# 1 Antecedentes

## 1.1 ¿Qué es la Dirección General de Administración Escolar (DGAE)?

La Dirección General de Administración Escolar (DGAE) es una dependencia normativa y de dirección dependiente de la Secretaría General de la UNAM, es el instrumento administrativo capaz de traducir los ordenamientos contenidos en la legislación universitaria y las disposiciones emitidas por la autoridad en esta materia, a planos operativos de la administración escolar.

### Organigrama

La DGAE depende jerárquicamente de la Secretaría General de la UNAM, la cual a su vez depende directamente de la Rectoría. De la Secretaria General, la DGAE recibe las políticas generales para su funcionamiento.

La DGAE está integrada por cuatro subdirecciones, tres coordinaciones y dos unidades administrativas como se aprecia en la fig. 1.1.

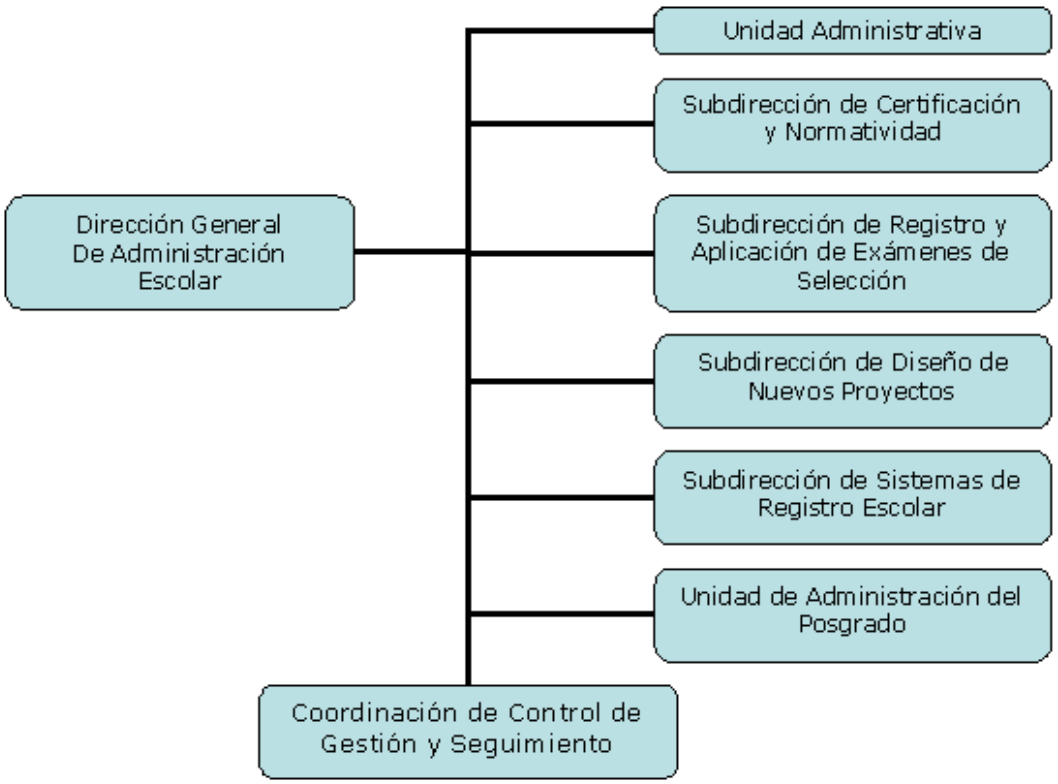



Fig. 1.1. Organigrama de la DGAE

**Subdirección de Sistemas de Registro Escolar**

Dirigir, supervisar, coordinar, resguardar y evaluar la sistematización y emisión de la documentación computarizada relacionada con el registro escolar y el historial académico de los alumnos de la UNAM, niveles bachillerato, técnico y licenciatura, bajo el marco legal que rige la Legislación Universitaria en este ámbito.

## 1.1.2 ¿Qué es el Sistema Integral de Administración Escolar (SIAE)?

La Dirección General de Administración Escolar, a través de la Subdirección de Sistemas de Registro Escolar (SSRE), desarrolló el Sistema Integral de Administración Escolar (SIAE), para otorgar un servicio de calidad y eficiencia a cada miembro que integra nuestra máxima casa de estudios, en todo lo referente al registro y seguimiento académico de la trayectoria escolar de los alumnos de la UNAM

Tiene como objetivo lograr dentro de la Administración Escolar de la UNAM, la simplificación, agilización y descentralización de los trámites académico-administrativos de los alumnos en todas las escuelas y facultades, integrando información confiable y consistente como el producto de la coordinación de todos los elementos de la Institución.

**Servicios que ofrece la SSRE a través del SIAE**

*Actualización*

De carreras, planes de estudio, asignaturas y planteles que se ofrecen en la UNAM En este apartado, es el Departamento de Planes y Programas de Estudio y con base en la autorización del Consejo Universitario a un plan de estudios, el que asigna claves a las nuevas carreras y asignaturas, en respuesta a un requerimiento de alguna facultad o escuela.

*Consulta*

A planes de estudio, proporciona acceso a escuelas, facultades, alumnos y público en general para consulta sobre asignaturas, créditos, seriación, equivalencia de asignaturas entre diferentes planes de estudio de una misma carrera, así como consulta de los requisitos de ingreso y titulación a la carrera.

*Solicitud y autorización de trámites*

El plantel tiene acceso para la actualización del registro del alumno, a través de los siguientes trámites: cambios de unidad, y cambios internos de carrera. Asimismo, el alumno puede solicitar la corrección de datos personales como nombre, fecha de nacimiento, nacionalidad, domicilio y teléfono en su plantel y tiene acceso al seguimiento de su solicitud en forma automatizada (vía Internet); así como solicitud de segunda carrera y simultánea.

*Registro y auditoría*

De la reinscripción e inscripción a cursos ordinarios, exámenes extraordinarios, que se efectúen en los sistemas locales del plantel.

- *Registro de Información* desde el plantel hacia el SIAE correspondiente a profesores, grupos, alumnos asignaturas, reinscripción, inscripción a exámenes extraordinarios. El registro garantizará el cumplimiento de los Reglamentos generales de Inscripciones y Exámenes

- *Validación* de la reinscripción contra el plan de estudios en el cual el alumno se encuentra registrado, por lo que al momento de que el alumno la solicita, se verifica: seriación, acreditación anterior de asignaturas, doble inscripción en ordinario y límite de tiempo para cursar en ordinario.

- *Autorización de extraordinarios*: para la inscripción a exámenes extraordinarios, la respuesta es inmediata para conocer si el alumno ya acreditó anteriormente la asignatura o la autorización para inscribir más de dos exámenes.

*Consulta a la trayectoria académica del alumno*

El SIAE cuenta con información de alumnos en relación a todos los movimientos académicos dentro de la UNAM, como es el tipo de ingreso al ciclo, los cambios de plantel, sistema (escolarizado o abierto) carrera o plan de estudios que el alumno realiza, así como su situación actual y su ubicación en el plan de estudios de la carrera que cursa, ya sea como primera o segunda carrera o carrera simultánea dando el acceso a las escuelas y facultades y al propio alumno.

*Consulta de la historia académica del alumno*

El alumno cuentan con un número de identificación personal (número de cuenta), con el cual pueden accesar al sistema para conocer su avance académico mediante

la consulta de su historia académica, así como la información referente a su inscripción y a sus datos personales. (Vía Internet).

*Obtención de estadísticas*

El acceso a información actualizada y en forma expedita es una de las principales características que ofrece la Subdirección de Sistemas a través del SIAE por lo que el plantel tiene la posibilidad de contar con estadísticas sobre los diferentes eventos que se lleven a cabo; reinscripción. Inscripción a extraordinarios, control de cupos y grupos, estadísticas de aprobación y reprobación, por asignatura, etc.

## 1.2 Definiciones

### 1.2.1 Seguridad Informática

Hoy en día el uso de sistemas de información en todos los ámbitos (militar, comercial, financiero) se ha incrementado, la mayoría de empresas e instituciones basan gran parte de su productividad en dichos sistemas.

*En un sistema de información se dice que la Seguridad Informática es un conjunto de estructuras de control establecidas con la finalidad de mantener la confidencialidad, integridad y disponibilidad de la información, mediante políticas y procedimientos de seguridad.*

La seguridad informática es, sin lugar a dudas, una de las mayores preocupaciones de las organizaciones en la actualidad. Todos los esfuerzos se encaminan hacia las políticas, normas, procedimientos y mecanismos que garanticen la protección de los recursos informáticos.

### 1.2.2 Amenazas a la Seguridad Informática

Se entiende por amenaza una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). La política de seguridad y el análisis de riesgos habrán de identificar las amenazas que han de ser contrarrestadas, y dependerá del diseñador del sistema de seguridad especificar los servicios y los mecanismos de seguridad necesarios.

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

**Clasificación de Amenazas**

| **CLASIFICACIÓN DE AMENAZAS** | |
|---|---|
| **TIPO** | **FACTORES** |
| HUMANO | Desconocimiento, fraude, venganza. |
| HARDWARE | Equipo en mal estado |
| SOFTWARE | Virus, gusanos, caballo de troya. |
| INSTALACIONES | Mala calidad de cable, mala instalación, etc.. |
| DESASTRES | Falta de energía, incendios, terremotos, etc... |

### 1.2.3 Ataques a la Seguridad Informática

#### Tipos de Ataque

**Interrupción:** un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro o cortar una línea de comunicación (ver fig. 1.2.3.1.a).

**Intercepción:** una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o una computadora. Ejemplos de este ataque son pinchar una línea para hacerse con datos que circulen por la red y la copia ilícita de archivos o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad) ver fig. 1.2.3.1.b.

**Modificación:** una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red (ver fig. 1.2.3.1.c).

**Suplantación o Fabricación:** una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes en una red o añadir registros a un archivo (ver fig. 1.2.3.1.d).

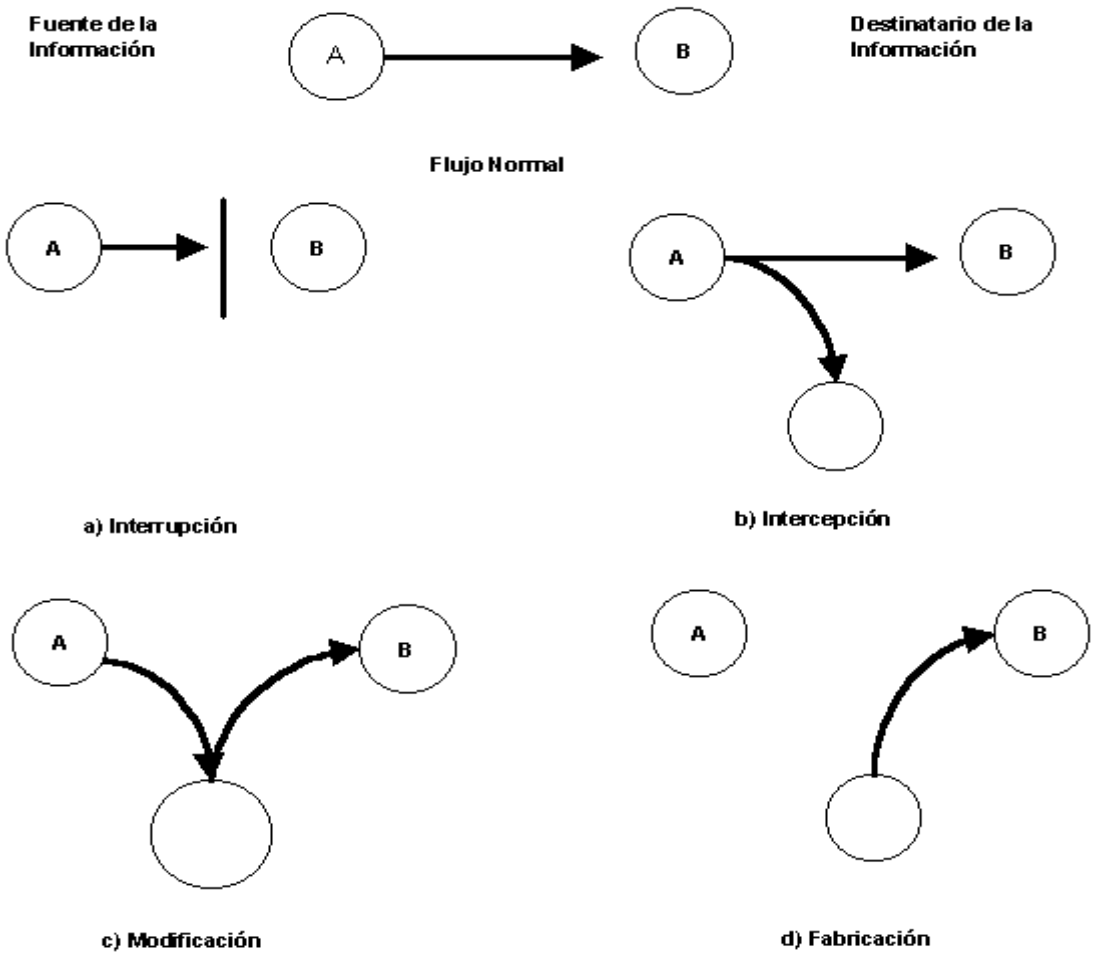



Fig. 1.2.3.1 Tipos de ataque

Un ataque no es más que la realización de una amenaza. Los factores por los que se puede llevar a cabo un ataque es la motivación, capacidad y oportunidad. Los ataques también los podemos clasificar por el daño a la información en activos y pasivos.

### Ataques pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida.

Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

- **Obtención del origen y destinatario** de la comunicación, leyendo las cabeceras de los paquetes monitorizados.

- **Control del volumen de tráfico** intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.

- **Control de las horas habituales** de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante.

**Ataques activos**

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos.

Pueden subdividirse en cuatro categorías:

- **Mascarada***.* Tiene lugar cuando se pretende tomar el lugar de otro. Generalmente incluye alguna de las otras formas de ataques activos.
- **Repetición***.* Involucra la captura pasiva de datos y su retransmisión para producir un resultado no autorizado.
- **Modificación de mensajes***.* Significa que una parte de una mensaje legítimo es alterado, o que el mensaje es demorado para producir un resultado determinado.
- **Impedir acceso al servicio.** Impide el normal uso o administración de las facilidades de comunicación.

Los ataques activos presentan características opuestas a los ataques pasivos. Es bastante difícil prevenir en forma absoluta los ataque activos, ya que habría que obtener una protección física de todas las facilidades de comunicación en todo momento. En cambio, la meta es detectarlos y tomar las medidas que correspondan.

### 1.2.4 Servicios de Seguridad

Para hacer frente a las amenazas a la seguridad del sistema se definen una serie de servicios para proteger los sistemas de proceso de datos y de transferencia de información (mensaje) de una organización. Estos servicios hacen uso de uno o varios mecanismos de seguridad. Una clasificación útil de los servicios de seguridad es la siguiente:

**Confidencialidad**: requiere que la información sea accesible únicamente por las entidades autorizadas. La confidencialidad de datos se aplica a todos los datos intercambiados por las entidades autorizadas o tal vez a sólo porciones o segmentos seleccionados de los datos, por ejemplo mediante cifrado. La confidencialidad de flujo de tráfico protege la identidad del origen y destino(s) cuando se lleva a cabo una comunicación o transferencia de datos.

**Autenticación**: requiere una identificación correcta del origen cuando se requiere comunicación entre dos entidades autorizadas, asegurando que la entidad no es falsa. Se distinguen dos tipos:

- *De entidad*: que asegura la identidad de las entidades participantes en la comunicación, mediante biométrica (huellas dactilares, identificación de iris, etc.), tarjetas de banda magnética, contraseñas, o procedimientos similares.
- *De origen:* de información, que asegura que una unidad de información proviene de cierta entidad, siendo la firma digital el mecanismo más extendido.

**Integridad**: requiere que la información sólo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación de la información transmitida. La integridad de datos asegura que los datos recibidos no han sido modificados de ninguna manera, por ejemplo mediante un hash criptográfico con firma, mientras que la integridad de secuencia de datos asegura que la secuencia de los bloques o unidades de datos recibidas no ha sido alterada y que no hay unidades repetidas o perdidas.

**No repudio**: ofrece protección a un usuario frente a que otro usuario niegue posteriormente que en realidad se realizó cierta comunicación. Esta protección se efectúa por medio de una colección de evidencias irrefutables que permitirán la resolución de cualquier disputa.

El *no repudio de origen* protege al receptor de que el emisor niegue haber enviado el mensaje, mientras que el *no repudio de recepción* protege al emisor de que el receptor niegue haber recibido el mensaje. Las firmas digitales constituyen el mecanismo más empleado para este fin.

**Control de acceso** requiere que el acceso a los recursos (información, capacidad de cálculo, nodos de comunicaciones, entidades físicas, etc.) sea controlado y limitado por el sistema destino, mediante el uso de contraseñas o llaves hardware, por ejemplo, protegiéndolos frente a usos no autorizados o manipulación.

**Disponibilidad**: requiere que los recursos del sistema informático estén disponibles a las entidades autorizadas cuando los necesiten.

### 1.2.5 Mecanismos de Seguridad

No existe un único mecanismo capaz de proveer todos los servicios anteriormente citados, pero la mayoría de ellos hacen uso de técnicas criptográficas basadas en el cifrado de la información. Los más importantes son los siguientes:

**Intercambio de autenticación**: corrobora que una entidad, ya sea origen o destino de la información, es la deseada, por ejemplo, A envía un número aleatorio cifrado con la clave pública de B, B lo descifra con su clave privada y se lo reenvía a A, demostrando así que es quien pretende ser. Por supuesto, hay que ser cuidadosos a la hora de diseñar estos protocolos, ya que existen ataques para desbaratarlos.

**Cifrado**: garantiza que la información no es inteligible para individuos, entidades o procesos no autorizados (confidencialidad). Consiste en transformar un texto en claro mediante un proceso de cifrado en un texto cifrado, gracias a una información secreta o clave de cifrado. Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el criptosistema es *simétrico*. Estos sistemas son mucho más rápidos que los de clave pública, resultando apropiados para funciones de cifrado de grandes volúmenes de datos.

Se pueden dividir en dos categorías:

- **Cifradores de bloque**, que cifran los datos en bloques de tamaño fijo (típicamente bloques de 64 bits).
- **Cifradores en flujo**, que trabajan sobre flujos continuos de bits.

Cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado, se dice que el criptosistema es *asimétrico* o de clave pública. Una clave, la privada, se mantiene secreta, mientras que la segunda clave, la pública, puede ser conocida por todos. De forma general, las claves públicas se utilizan para cifrar y las privadas, para descifrar. El sistema tiene la propiedad de que a partir del conocimiento de la clave pública no es posible determinar la clave privada. Los criptosistemas de clave pública, aunque más lentos que los simétricos, resultan adecuados para las funciones de autenticación, distribución de claves y firmas digitales.

**Integridad de datos**: este mecanismo implica el cifrado de una cadena comprimida de datos a transmitir, llamada generalmente valor de comprobación de integridad (Integrity Check Value o ICV). Este mensaje se envía al receptor junto con los datos ordinarios. El receptor repite la compresión y el cifrado posterior de los datos y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados.

**Firma digital**: este mecanismo implica el cifrado, por medio de la clave secreta del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se envía junto con los datos ordinarios. Este mensaje se procesa en el receptor, para verificar su integridad. Juega un papel esencial en el servicio de no repudio.

**Control de acceso**: esfuerzo para que sólo aquellos usuarios autorizados accedan a los recursos del sistema o a la red, como por ejemplo mediante las contraseñas de acceso.

**Tráfico de relleno**: consiste en enviar tráfico espurio junto con los datos válidos para que el atacante no sepa si se está enviando información, ni qué cantidad de datos útiles se está transmitiendo.

**Control de encaminamiento**: permite enviar determinada información por determinadas zonas consideradas clasificadas. Asimismo posibilita solicitar otras rutas, en caso que se detecten persistentes violaciones de integridad en una ruta determinada.

**Unicidad**: consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores, que se incluyen en la firma digital o integridad de datos. De esta forma se evitan amenazas como la reactuación o resecuenciación de mensajes.

Los mecanismos básicos pueden agruparse de varias formas para proporcionar los servicios previamente mencionados. Conviene resaltar que los mecanismos poseen tres componentes principales:

- Una información secreta, como claves y contraseñas, conocidas por las entidades autorizadas.
- Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado, hash y generación de números aleatorios.
- Un conjunto de procedimientos, que definen cómo se usarán los algoritmos, quién envía qué a quién y cuándo.

Asimismo es importante notar que los sistemas de seguridad requieren una gestión de seguridad. La gestión comprende dos campos:

- Seguridad en la generación, localización y distribución de la información secreta, de modo que sólo pueda ser accedida por aquellas entidades autorizadas.
- La política de los servicios y mecanismos de seguridad para detectar infracciones de seguridad y emprender acciones correctivas.

### 1.2.6 Seguridad de Red

La seguridad en los sistemas informáticos cobra mucha mas importancia desde el momento que incorporamos sistemas de red y posibilitamos el acceso de manera remota a nuestra computadora. Con el auge de Internet si nuestro servidor está accesible en la "red de redes" podrá ser accedido por millones de personas de todo tipo desde miles de lugares a lo largo del mundo, de ahí la importancia que tiene asegurar una máquina contra posibles intrusos o ataques.

Resguardar la información de intrusos o ataques, es prevenir y proteger a través de ciertos mecanismos para evitar de manera accidental o intencional, la transferencia, fusión, modificación o destrucción no autorizada de la información.

Seguridad informática es la colección de herramientas diseñadas para la protección de los sistemas de cómputo a fin de evitar amenazas de confidencialidad, integridad y/o disponibilidad.

*El principio de seguridad de red es proteger el entorno de cualquier tipo de amenaza, mediante servicios, mecanismos y técnicas, para hacer cumplir una política de seguridad.*

### 1.2.7 Políticas de seguridad

Los recursos de cómputo actuales resultan caros y algunas veces insuficientes para una organización determinada, por lo cual se hace necesario explotarlos al máximo para obtener el mayor beneficio de ellos. Para lograr esto, deben establecerse estándares aceptables de uso de los mismos. El hacer entender a la gente que interactúa con estos sistemas (usuarios, administradores, directores, operadores, etc.) la importancia de respetar estos estándares de uso es una labor más difícil de lo que pudiera parecer a primera vista, ya que a las personas normalmente les resulta incómoda la existencia de este tipo de estándares. Existen varios métodos para intentar concienciar a la gente sobre la importancia de respetar estas normas de conducta, pero lo que nos ayuda son las Políticas de Seguridad.

Antes de continuar es necesario definir el significado de misión de seguridad informática, ya que una vez que se ha establecido dicha misión se identificará el objetivo de seguridad y entonces podrá darse paso a redactar las políticas en que se basará el cumplimiento de la misión.

La *misión* de seguridad informática debe de definir claramente qué es lo que se quiere proteger y porqué, para que cada uno de los cuales pueda plasmarse en una o más políticas de seguridad.

*Política de seguridad son los documentos que describen, principalmente, la forma adecuada de uso de los recursos de un sistema de cómputo, las responsabilidades y derechos que tanto usuarios como administradores tienen.*

#### Ventajas de las Políticas de Seguridad

- Ayuda a tomar decisiones con respecto a la adquisición de hardware o software, ya que contiene guías con respecto a los estándares de protección requeridos en ciertos tipos de sistemas de cómputo.

- Permite decidir que acciones llevar a cabo en circunstancias particulares, como en el caso de una violación de la seguridad, donde la Política indica lo que las personas con autoridad para la toma de decisiones deben hacer para minimizar el impacto de tal violación, cómo prevenir futuras violaciones de seguridad, y cómo identificar y sancionar a quiénes resulten responsables de dicha violación.

- Habla muy bien del profesionalismo de la organización.

- Es indispensable en caso de una auditoria a la organización.

**Características de una Política de seguridad**

- Debe considerarse como un documento de referencia con un periodo de vigencia largo, pero debe ser revisada en intervalos de tiempo regulares, o en cualquier ocasión que lo requiera, modificándose en caso necesario.

- Debe servir como referencia para otros tipos de seguridad, tal como la seguridad física de los activos con que cuenta la organización.

- Debe ser única, pues los requerimientos de seguridad de los sistemas de cómputo de una organización generalmente son distintos de los de otras organizaciones.

- Debe estar estructurada de tal forma que sea posible encontrar fácilmente secciones específicas dentro de ella.

- Tanto los formatos iniciales como las actualizaciones posteriores deben contener la fecha y el número de versión.

- Para tener autoridad debe ser aceptada como documento oficial por las autoridades correspondientes dentro de la organización.

- Debe ser escrita cuidadosamente (la clave para preparar un documento de políticas es asegurarse de que todos los términos están definidos de una manera exacta y precisa, por ejemplo, sí una política establece "la revelación de información confidencial será castigada severamente", será necesario definir de forma precisa que entendemos por "confidencial" y "severamente").

- No sólo debe establecer condiciones de uso aceptables, sino también condiciones de uso no aceptables, pueden considerarse dos enfoques aquí:

    1) "Todo lo que no está estrictamente permitido está prohibido"
    2) "Todo lo que no está estrictamente prohibido está permitido".

- Debe ser dada a conocer y aprobada por todas las personas afectadas (directa o indirectamente) por ella.

- No debe ser simplemente una política de uso aceptable (esto es, una política sobre el comportamiento aceptable de los usuarios del sistema de cómputo), sino también debe referirse a los derechos y obligaciones que los

administradores y usuarios tienen con respecto al uso de los sistemas de cómputo.

- La redacción de una regla o norma debe usarse la frase en afirmativo no en negativo, es decir evitar la palabra "NO".

- Considerar la jerarquía de los usuarios.

## Partes Principales de las Políticas de Seguridad

Generalmente están formadas por tres partes:

- La primera parte se refiere a los parámetros dentro de los cuales operará la política, esto es, el ámbito dentro del cual tendrá vigencia.

- La segunda parte consiste esencialmente de un análisis de riesgos, donde se discute qué activos o bienes deben ser protegidos, las amenazas que pueden causar daño a estos activos (esto es, de qué debemos protegerlos) y los mecanismos que pueden usarse para reconocer estas amenazas. El material de esta parte constituye el fundamento lógico para las políticas de seguridad definidas en la siguiente sección.

- La tercera parte define formalmente las reglas y guías que constituyen las políticas de seguridad en sí.

## Redacción de las políticas

La elaboración de políticas de seguridad es una tarea muy difícil e importante como para ser asignada a una sola persona, dadas las consecuencias potenciales que se encuentran implícitas en éstas, por lo que se recomienda la formación de un equipo de trabajo con diferentes puntos de vista con respecto a la seguridad de un sistema de cómputo para la realización de esta tarea.

Entre las personas que podrían formar parte de este equipo podemos mencionar:

- Un administrador de sistemas experimentado que esté bien enterado acerca de las políticas de seguridad y que sepa cuáles de ellas se encuentran ya en uso (en su caso) dentro de la organización.

- Alguien con la autoridad para tomar decisiones y hacerlas respetar (es decir, alguien con una buena posición administrativa).

- Un representante jurídico o bien, el abogado de la compañía.

- Una persona con buena redacción.

- Un usuario típico, quien representará a todas las personas afectadas por las políticas a desarrollar.

Todas estas personas pueden hacer comentarios con el fin de llegar a un acuerdo con respecto a cada una de las políticas, si bien no todos (a excepción del escritor o redactor) estarán involucrados en el establecimiento de todas las políticas.

**Metodología para el desarrollo de las Políticas de Seguridad**

Un esquema de políticas de seguridad debe llevar ciertos pasos, para garantizar su funcionalidad y permanencia en la institución. Nuestra propuesta es seguir los pasos que detallamos a continuación:

- **Preparación** - La recopilación de todo tipo de material relacionado con cuestiones de seguridad en la organización: Manuales de procedimientos, planes de contingencia, cartas compromiso, etc.

- **Redacción** - Escribir las políticas de una manera clara, concisa y estructurada. Requiere de la labor de un equipo en el que participen abogados, directivos, usuarios y administradores.

- **Edición** - Reproducir las políticas de manera formal para ser sometidas a revisión y aprobación

- **Aprobación** - Probablemente, la parte más difícil del proceso, puesto que es común que la gente afectada por las políticas se muestre renuente a aceptarlas. En esta etapa es fundamental contar con el apoyo de los directivos.

- **Difusión** - Dar a conocer las políticas a todo el personal de la organización mediante proyecciones de video, páginas Web, correo electrónico, cartas compromiso, memos, *banners*, etc.

- **Revisión** - Las políticas son sometidas a revisión por un comité, que discutirá los comentarios emitidos por las personas involucradas.

- **Aplicación** - Es peor tener políticas y no aplicarlas que carecer de ellas. Una política que no puede implementarse o hacerse cumplir, no tiene ninguna utilidad. Debe predicarse con el ejemplo.

- **Actualización** - En el momento requerido, las políticas deberán ser revisadas y actualizadas, respondiendo a los cambios en las circunstancias. El momento ideal es justo después de que ocurra un incidente de seguridad.

**Políticas necesarias**

Al diseñar un esquema de políticas de seguridad, conviene que dividamos nuestro trabajo en varias diferentes políticas específicas a un campo - cuentas, contraseñas, control de acceso, uso adecuado, respaldos, correo electrónico, contabilidad del sistema, seguridad física, personal, etc.

- **Políticas de cuentas:** Establecen qué es una cuenta de usuario de un sistema de cómputo, cómo está conformada, a quién puede serle otorgada, quién es el encargado de asignarlas, cómo deben ser creadas y comunicadas.

- **Políticas de contraseñas:** Son una de las políticas más importantes, ya que por lo general, las contraseñas constituyen la primera y tal vez única manera de autenticación y, por tanto, la única línea de defensa contra ataques. Éstas establecen quién asignará la contraseña, qué longitud debe tener, a qué formato deberá apegarse, cómo será comunicada, etc..

- **Políticas de control de acceso:** Especifican cómo deben los usuarios acceder al sistema, desde dónde y de qué manera deben autentificarse.

- **Políticas de uso adecuado:** Especifican lo que se considera un uso adecuado o inadecuado del sistema por parte de los usuarios, así como lo que está permitido y lo que está prohibido dentro del sistema de cómputo.

- **Políticas de respaldos:** Especifican qué información debe respaldarse, con qué periodicidad, qué medios de respaldo utilizar, cómo deberá ser restaurada la información, dónde deberán almacenarse los respaldos, etc.

- **Políticas de correo electrónico:** Establece tanto el uso adecuado como inadecuado del servicio de correo electrónico, los derechos y obligaciones que el usuario debe hacer valer y cumplir al respecto.

- **Políticas de contabilidad del sistema:** Establecen los lineamientos bajo los cuales pueden ser monitoreadas las actividades de los usuarios del sistema de cómputo, así como la manera en que debe manejarse la contabilidad del sistema y el propósito de la misma.

### 1.2.8 Procedimientos de seguridad

Una vez que se han determinado las políticas de seguridad que especifican lo que hay que proteger, es necesario elaborar los procedimientos de seguridad, que indican cómo hay que llevar a cabo la protección. Estos procedimientos también constituyen los mecanismos para hacer cumplir las políticas. Además resultan útiles pues indican detalladamente qué hay que hacer cuando sucedan incidentes específicos, son referencias rápidas en caso de emergencia y ayudan a eliminar los puntos de falla críticos.

**Procedimientos necesarios**

- **Auditoria de seguridad de los sistemas:** Dado que los datos que se almacenan sobre el uso de los sistemas son la principal herramienta para detectar violaciones a las políticas, es necesario especificar detalladamente qué es lo que se desea almacenar. Cómo se resguarda estas bitácoras y quién tiene acceso a ellas. Otro componente de estos procedimientos se relaciona con precisar qué mecanismos de verificación de la integridad de los archivos binarios ejecutables que contiene un sistema de información, o en varios sistemas, qué algoritmos criptográficos se emplearán, y cómo se resguardan los códigos de identificación correspondientes.

- **Administración de cuentas:** Abarca desde cómo se tiene que solicitar una cuenta en un sistema de información, o en varios sistemas, hasta qué tiene que hacer el departamento de personal antes de despedir un empleado. También lo que debe de hacerse para cambiar los privilegios de una cuenta o cancelarla. Específica cómo se documenta el manejo de las cuentas y cómo se vigila el cumplimiento de las políticas correspondientes.

- **Administración de autenticadores:** Los sistemas de control de acceso, en general deben emplear por lo menos dos autenticadores de tipos distintos para cada usuario. Estos procedimientos indican cómo deben obtenerse los autenticadores, cómo deben resguardarse, la vigencia de los mismos y las características que deben de tener.

- **Administración de las configuraciones de los sistemas:** Define cómo se instala y prueba un equipo o un programa nuevo, cómo se documentan los cambios de los equipos, los programas y su configuración, a quién se debe informar cuando hagan cambios y quién tiene la autoridad para hacer cambios de equipo, programas y configuración.

- **Respaldos y acervos de datos y programas:** Define qué sistemas de archivos hay que respaldar, cuándo hagan los cambios y quién tiene la autoridad para hacer cambios de equipo, programa configuración.

- **Manejo de incidentes:** Defino cómo se manejan las intrusiones, delimita las responsabilidades de cada miembro del equipo de respuesta, indica qué información hay que anotar e investigar, a quién hay que notificar y cuándo, determina quién, cuándo y cómo se hará el análisis posterior del incidente.

- **Escalamiento de problemas:** Es una colección de recetas para el personal de soporte de primera línea. Define a quién hay que llamar y cuando, indica qué pasos iniciales hay que dar, y qué información inicial hay que anotar.

- **Planes de respuesta:** Un desastre es un evento de gran escala que afecta a grandes secciones de la organización. El plan debe delinear qué acciones hay que tomar para que los recursos críticos sigan funcionando y se minimice el impacto del desastre. Debe indicar qué hay que tener listo fuera de sitio y fácilmente disponible para emplearlo después de un desastre. Hay que estratificar el plan para responder a distintos niveles de daño. Definirá si se requiere sitios alternos "calientes o frios". Se debe establecer cada cuando se harán simulaciones para probar el plan.

## 2. Análisis y requerimientos de seguridad de la red SIAE

Para redactar las Políticas de Seguridad de la red SIAE se tuvo que hacer un análisis de toda la red. Para el análisis en primer instancia, se tuvo definir la misión o propósito con el fin de identificar el objetivo de seguridad, se enlistaron los elementos lógicos y físicos con los que cuenta el sistema, por último se hizo un análisis de riesgos y vulnerabilidades para detectar los activos más importantes del sistema informático, para esto se tuvieron que hacer una serie de preguntas (que se muestran con más detalle en el Anexo I) a los encargados de llevar todo el proceso de la información y así poder detectar aquellos problemas en donde los activos estén con más riesgo a ser atacados.

### 2.1 Misión o propósito

El SIAE tiene como objetivo lograr dentro de la Administración Escolar de la UNAM, la simplificación, agilización y descentralización de los trámites académico-administrativos de los alumnos en todas las escuelas y facultades, integrando información confiable y consistente como el producto de la coordinación de todos los elementos de la Institución, para otorgar un servicio de calidad y eficiencia a cada miembro que integra nuestra máxima casa de estudios, en todo lo referente al registro y seguimiento académico de la trayectoria escolar de los alumnos de la UNAM.

Para poder lograr el objetivo la Subdirección de Sistemas de Registro Escolar cuenta con los departamentos que se muestran en la fig. 2.1.1

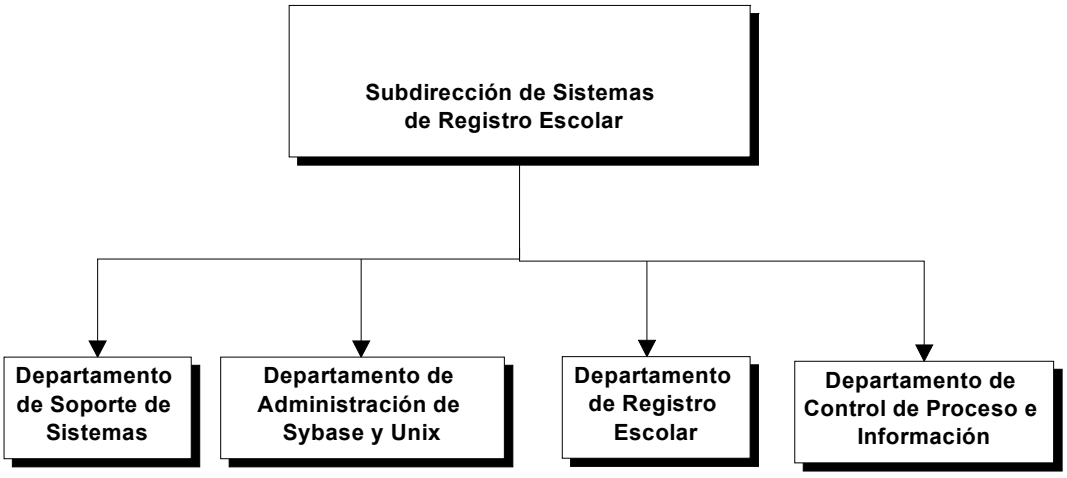



**Fig. 2.1.1 Organigrama**

## 2.2 Entorno Físico y Lógico

Es necesario conocer el entorno de seguridad al que vamos o queremos proteger, ya que de esto depende que nuestras políticas de seguridad informática contemplen todos y cada uno de los recursos con los que cuenta el sistema.

### Entorno Lógico

El entorno lógico nos muestra la relación que existe entre los distintos usuarios que pueden acceder o que integran al sistema con la base de datos (B.D.) que en nuestro caso es uno de los activos más importantes de la subdirección (fig. 2.2.1).

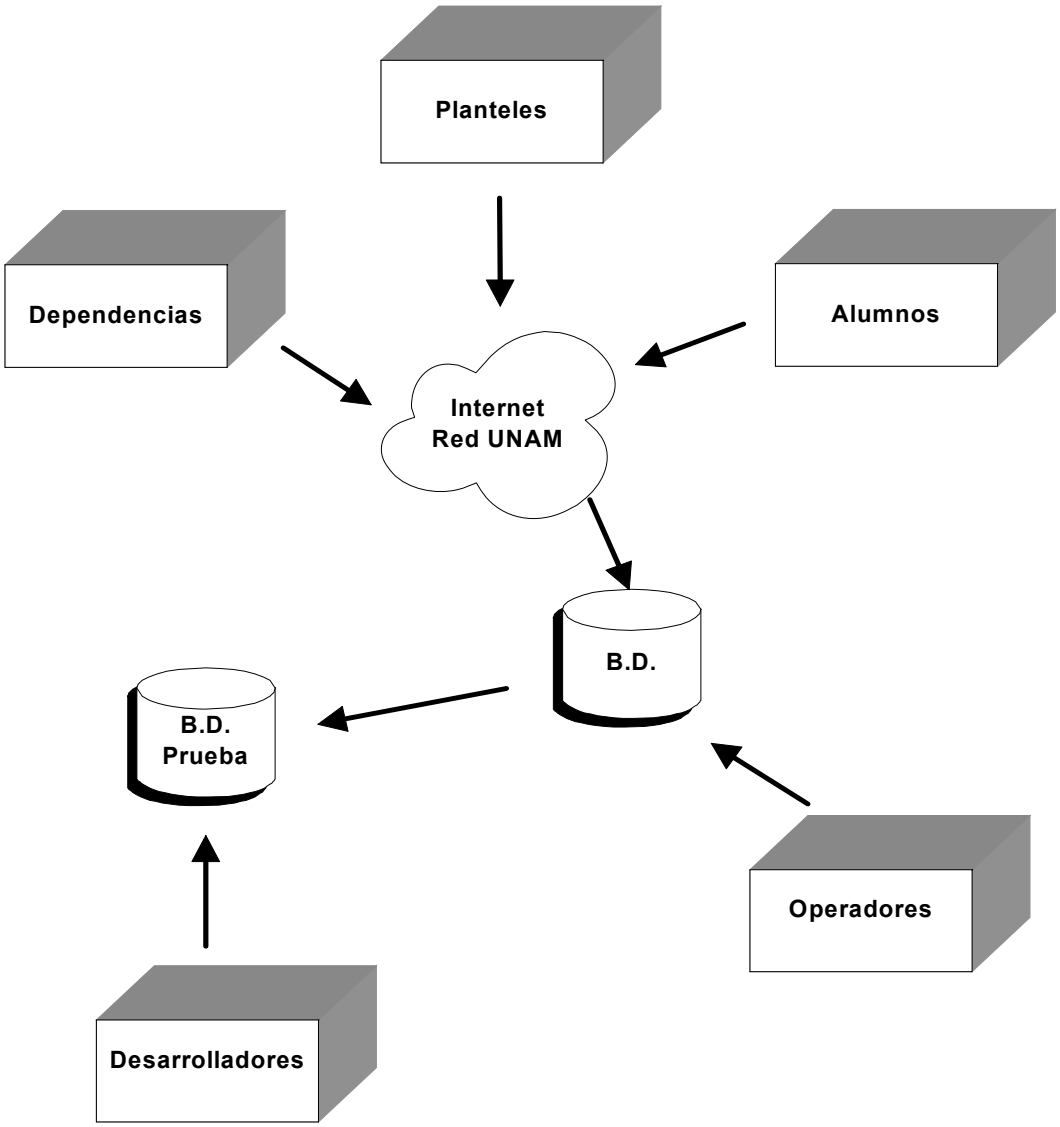
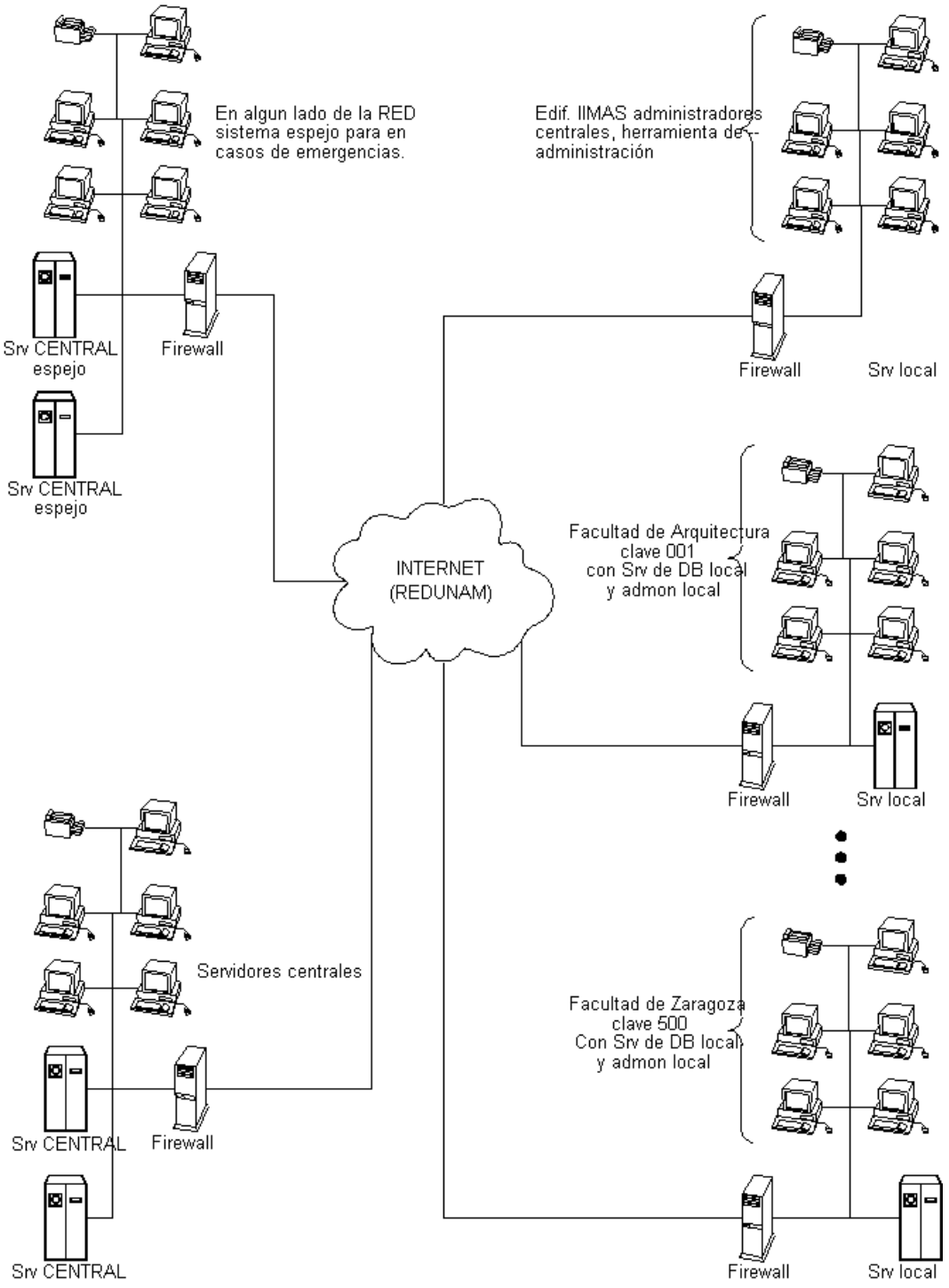



**Figura 2.2.1.**

## Entorno Físico

El entorno físico es el conjunto de hardware con que cuenta el sistema informático y su relación entre ellos.



## 2.3 Recursos disponibles.

a) Hardware:

- 3 Servidores SUN 2 G en RAM
- 1 SUN Blade 2000 1 G de RAM
- 1 SUN Blade 1000 512K RAM
- 30 PC's Pentium III MMX, 300Mz en RAM
- 7 concentradores de 10/100 con 24 puertos
- cable trensado tipo 5

b) Software:

**Sybase V. 12**

Adaptive Server Enterprise es la porción del software más importante de un sistema de base de datos, es una colección de numerosos elementos de software interrelacionados, cada uno de los cuales es responsable de alguna tarea específica.

**WindowsX, WindowsXP**

Sistema operativo de Microsoft que trabaja mediante ventanas. Se trata de un entorno gráfico con capacidades multitarea.

**Linux Redhat V. 7.2**

Un sistema operativo multiusuario y multitarea basado en UNIX.

**PowerBuilder V. 6.X**

Es una herramienta gráfica de desarrollo extremadamente flexible, es posible desarrollar poderosas aplicaciones gráficas con acceso a bases de datos, proporciona todas las herramientas necesarias para la construcción de aplicaciones sólidas.

**gcc V. 3.2**

Es una colección de compiladores y admite diversos lenguajes: C, C++, Objetive C, Chill, Fortran, y Java para plataforma Unix.

**DBlibrary V. 10.X**

Contiene varios archivos de cabecera (include) que definen estructuras y valores usados por las rutinas.

**Apache V. 1.3.9**

Es un servidor de web libre, estable, fiable y veloz para plataformas Unix.

**SSH V. 2**

Es un software que permite realizar comunicaciones o transferencia de datos de manera segura.

**PHP V. 4.X**

PHP es el acrónimo de Hipertext Preprocesor. Es un lenguaje de programación del lado del servidor gratuito e independiente de plataforma, rápido, con una gran librería de funciones y mucha documentación.

**HTML V. 4**

(Lenguaje de Marcas de Hipertexto) Lenguaje utilizado para crear páginas Web.

c) Humano:

- **DASSU**

  Dentro de este grupo se encuentran los usuarios avanzados, en este caso los que administran el servidor de bases de datos, y el nombre esta formado por las siglas del departamento al que pertenecen cuyo nombre es Departamento de Administración de Servidores Sybase y UNIX (DASSU), ellos tienen diferentes roles que son privilegios asignados a un "login"; los roles son:

  *sa (System Administrator)* el cual tiene a su cargo:

  - Instalación del Servidor
  - Asignación de recursos de disco
  - Manejo del almacenamiento en disco
  - Crear usuarios de bases de datos y otorgar permisos a ellos
  - Privilegios de accesos, modificar, borrar y bloquear "logins"
  - Crear grupos
  - Auditar la integridad de la base de datos y de información

*SSO (System Security Officer)* el cual tiene a su cargo:

- Crear "logins" y asignar passwords
- Modificar "logins"
- Cambiar passwords
- Manejo del sistema de auditoría
- Bloquear y desbloquear "logins"

*OPER (Server Operator)* el cual tiene a su cargo:

- Respaldo y recuperación de bases de datos

## 2.4 Usuarios

### *SSRE*

En este grupo se encuentran aquellos usuarios que pueden hacer modificaciones a todas las bases de datos cuyas acciones son inserción de nuevos registros, actualización y consulta de los mismos, el nombre del grupo se formo por las siglas de la Subdirección de Sistemas de Registro Escolar (SSRE), los usuarios del grupo SSRE pertenecen a esta subdirección. Además aquí se encuentran los desarrolladores de todas las aplicaciones que se necesitan para interactuar con la base de datos.

Para poder realizar estos procedimientos se requiere del uso de aplicaciones, que interactúan con la base de datos.

### *PLANTEL*

Los usuarios que se encuentran dentro de este grupo, son aquellos que pueden realizar modificaciones a los datos de la base que pertenecen a su plantel (PLT).

Este grupo también requiere del uso de aplicaciones, que interactúan con la base de datos.

### *CONSULTA*

Este grupo de usuarios sólo puede consultar información dentro de la base de datos, aquí podemos encontrar a los alumnos y dependencias.

## 2.5 Riesgos

El presente análisis de riesgo fue desarrollado con el propósito de determinar cuáles de los activos de la dependencia tienen mayor vulnerabilidad ante factores externos o internos que puedan afectarlos, identificando las causas potenciales que faciliten o impidan alcanzar los objetivos, calculando la probabilidad de su ocurrencia, evaluando sus probables efectos, y considerando el grado en que el riesgo puede ser controlado.

Para generar esta información se desempeñaron las siguientes actividades:

1. Listado de los activos de la organización: se evaluaron los distintos activos físicos y de software de la organización, generando un inventario de aquellos que son considerados como vitales para su desenvolvimiento seguro.

2. Asignación de prioridades a los activos: los activos fueron clasificados según el impacto que sufriría la organización si faltase o fallara tal activo.

3. Definición de factores de riesgos: acto seguido se listaron los factores de riesgo relevantes a los pueden verse sometidos cada uno de los activos arriba nombrados.

4. Descripción de consecuencias: teniendo presente el listado anterior, se generó una descripción de las consecuencias que podría sufrir la empresa si los activos son afectados por sus respectivos factores de riesgo, detallando la manera en que se protege al activo contra ese ataque en particular, y puntualizando en qué grado son efectivas estas medidas.

5. Asignación de probabilidades de ocurrencia de los factores de riesgo: teniendo en cuenta los datos arriba mencionados fue posible estimar la probabilidad de ocurrencia que cada uno de los factores de riesgo representaba con respecto a los activos listados, considerando para esta estimación las medidas tomadas por la empresa para mitigar su acción.

6. Cálculo de niveles de vulnerabilidad: una vez identificados los riesgos, se procedió a su análisis. Con toda la información recolectada, se determinó el nivel de vulnerabilidad que se asocia con cada activo listado.

7. Conclusiones: a partir de las actividades anteriormente descritas se pudo evaluar la situación actual de la empresa en relación a los incidentes que pueden afectarla, calculando el porcentaje de los riesgos cubiertos y descubiertos, y un análisis sobre la escala de importancia de los activos.

8. Consecuencias: luego de identificar, estimar y cuantificar los riesgos, los directivos de la organización deben determinar los objetivos específicos de control y, con relación a ellos, establecer los procedimientos de control más convenientes, para enfrentarlos de la manera más eficaz y económica posible. En general, aquellos riesgos cuya concreción esté estimada como de baja frecuencia, no justifican preocupaciones mayores. Por el contrario, los que se estiman de alta frecuencia deben merecer preferente atención. Entre estos extremos se encuentran casos que deben ser analizados cuidadosamente, aplicando elevadas dosis de buen juicio y sentido común.

## ACTIVOS Y FACTORES DE RIESGOS

Presentamos los distintos activos reconocidos en la organización. La importancia de estos activos refleja el nivel de impacto que puede tener la empresa si un incidente afecta a dichos activos, sin considerar las medidas de seguridad que existan sobre los mismos.

| ACTIVOS A PROTEGER |
|---|
| Servidores |
| Bases de datos. |
| Software de aplicación, programas fuente, sistemas operativos. |
| Backup. |
| Datos en tránsito, datos de configuración, datos en medios externos. |
| Administrador de sistemas (Departamento de sistemas). |
| Cableado, conectores. |
| Red. |
| Usuarios. |
| Documentación de programas, hardware, sistemas, procedimientos,administrativos locales, manuales, etc |
| Hardware (teclado, monitor, unidades de discos, medios removibles, etc.). |
| Insumos (cintas, cartuchos de tinta, toner, papel, formularios, etc.) |
| Datos de usuarios. |

A continuación se listan los factores de riesgo que pueden afectar a dichos activos.

| FACTORES DE RIESGO PROBABLE |
|---|
| Abuso de puertos para el mantenimiento remoto |
| Acceso no autorizado a datos (borrado, modificación, etc.) |
| Almacenamiento de passwords negligente |
| Ancho de banda insuficiente |
| Aplicaciones sin licencia |
| Ausencia o falta de segmentación |
| Borrado, modificación o revelación inadvertida de información |
| Complejidad en el acceso a las redes de sistemas de IT |

Condiciones de trabajo adversas
Conexión de cables inadmisible
Conexiones todavía activas
Configuración inadecuada de componentes de red
Conocimiento insuficiente de los documentos de requerimientos en el desarrollo
Copia no autorizada de un medio de datos
Corte de luz, UPS descargado o variaciones de voltaje.
Daño de cables inadvertido
Deficiencias conceptuales en la red
Descripción de archivos inadecuada
Destrucción negligente de equipos o datos
Destrucción o mal funcionamiento de un componente
Documentación deficiente
Documentación insuficiente o faltante, Funciones no documentadas
Denial of service
Entrada sin autorización a habitaciones
Entrenamiento de usuarios inadecuado
Errores de configuración y operación
Errores de software
Errores en las funciones de encriptación
Factores ambientales
Huelga de estudiantes o trabajadores
Falla en medios externos
Falta de auditorias
Falta de autenticación
Falta de compatibilidad
Falta de confidencialidad
Falta de cuidado en el manejo de la información (Ej. Password)
Falta de espacio de almacenamiento
Ingeniería social
Interferencias
Límite de vida útil - Máquinas obsoletas
Longitud de los cables de red excedida
Mal interpretación
Mal mantenimiento
Mal uso de derechos de administrador
Mal uso de servicios de mail
Mala administración de control de acceso (salteo del login, etc.)
Mala evaluación de datos de auditoría
Mala integridad de los datos
Mantenimiento inadecuado o ausente
Medios de datos no están disponibles cuando son necesarios
Modificación de paquetes
Modificación no autorizada de datos
No-cumplimiento con las medidas de seguridad del sistema
Penetración, intercepción o manipulación de líneas
Pérdida de backups
Perdida de confidencialidad en datos privados y de sistema

| |
|---|
| Pérdida de confidencialidad o integridad de datos como resultado de un error humano en el sistema |
| Pérdida de datos |
| Perdida de datos en tránsito |
| Desvinculación del personal |
| Poca adaptación a cambios en el sistema |
| Portapapeles, impresoras o directorios compartidos |
| Prueba de software deficiente |
| Recursos escasos |
| Reducción de velocidad de transmisión |
| Reglas insuficientes o ausencia de ellas |
| Riesgo por el personal de limpieza o personal externo |
| Robo |
| Robo de información |
| Rótulos inadecuados en los medios de datos |
| Sabotaje |
| Seguridad de base de datos deficiente |
| Sincronización de tiempo inadecuada |
| Software desactualizado |
| Spoofing y sniffing |
| Transferencia de datos incorrectos o no deseados |
| Transporte inseguro de archivos |
| Transporte inseguro de medios de datos |
| Uso de derechos sin autorización |
| Uso descontrolado de recursos (DoS) |
| Uso sin autorización |
| Virus, gusanos y caballos de Troya |

## Posibles consecuencias

En el presente cuadro se listan las consecuencias que puede acarrear la ocurrencia de estos factores de riesgo.

## Servidores

| **Factor de riesgo** | **Consecuencia** |
|---|---|
| Acceso no autorizado | Robo, modificación de información. |
| Corte de luz, UPS descargado o variaciones de voltaje | Falta de sistema. |
| Destrucción de un componente | Pérdida de tiempo por necesidad de reemplazo |
| Error de configuración | Aumento de vulnerabilidades e inestabilidad en el sistema |
| Factores ambientales | Falta de sistema y destrucción de equipos |
| Límite de vida útil Máquinas obsoletas | Deterioro en la performance del sistema |
| Mal mantenimiento | Interrupciones en el funcionamiento del sistema. |
| Modificación no autorizada de datos | Inconsistencia de datos, mala configuración, fraude. |

| | |
|---|---|
| Robo | Pérdida de equipamiento e información |
| Virus | Fallas generales del sistema y en la red. |

## Bases de Datos

| **Factor de riesgo** | **Consecuencia** |
|---|---|
| Base de datos compleja | Desarrollo complejo de sistemas. |
| Copia no autorizada de un medio de datos | Divulgación de información |
| Errores de software | Inconsistencias en los datos |
| Falla de base de datos | Inconsistencias en los datos |
| Falla en medios externos | Perdida de backup |
| Falta de espacio de almacenamiento | Falla en la aplicación |
| Mala configuración del schedule de backups | Datos sin backup |
| Mala integridad de los datos | Inconsistencias y redundancia de datos |
| Medios de datos no están disponibles cuando son necesarios | Pérdida de tiempo y productividad. |
| Pérdida de backups | Incapacidad de restauración |
| Perdida de confidencialidad en datos privados y de sistema | Divulgación de información |
| Perdida de datos en tránsito | Inconsistencia de datos y divulgación de información |
| Portapapeles, impresoras o directorios compartidos | Divulgación de información |
| Robo | Divulgación de información |
| Sabotaje Pérdida o modificación de datos | Pérdida de tiempo y productividad |
| Spoofing y sniffing | Divulgación y modificación de información |
| Transferencia de datos incorrectos | Inconsistencia de datos |
| Virus | Pérdida, modificación o divulgación de datos, pérdida de tiempo, y productividad |
| | |

## Software de Aplicación, programas fuentes y sistema operativo

| **Factor de riesgo** | **Consecuencia** |
|---|---|
| Acceso no autorizado a datos (borrado, modificación, etc.) | Modificación del software en desarrollo |
| Aplicaciones sin licencia | Multas y problemas con Software Legal |
| Conocimiento insuficiente de los documentos de requerimientos en el desarrollo | Sistema inestable y excesivos pedidos de cambios |
| Error de configuración | Mal funcionamiento de los sistemas |
| Errores en las funciones de encriptación | Problemas en la recuperación de archivos encriptados o divulgación de información |
| Falla del sistema | Falta de sistema y posibles demoras |
| Falta de compatibilidad | Datos erróneos e inestabilidad del sistema |
| Falta de confidencialidad | Divulgación de información |
| Mala administración de control de acceso (salteo del login, etc.) | Divulgación y modificación de información |
| Pérdida de datos | Divulgación de información |

| | |
|---|---|
| Poca adaptación a cambios del sistema | Sistema inestable y de difícil modificación |
| Prueba de software deficiente | Sistema poco confiable |
| Software desactualizado | Probabilidad incremental de vulnerabilidades y virus |
| Virus | Inestabilidad y mal funcionamiento de sistemas |

## Backup

| | |
|---|---|
| Copia no autorizada a un medio de datos | Robo de información |
| Errores de software | Error en la generación o en la copia de backups a medios externos |
| Falla en medios externos | Pérdida de backups |
| Falta de espacio de almacenamiento | Falla en la generación del backup |
| Mala configuración del schedule de backups | Falta de copias de respaldo de datos |
| Mala integridad de los datos resguardados | Errores durante la restauración de datos |
| Medios de datos no están disponibles cuando son necesarios | Pérdida de backup y retraso del sistema |
| Pérdida de backups | Falta de datos, incapacidad de restaurarlos y divulgación de información |
| Robo | Incapacidad de restaurarlos y divulgación de información |
| Rótulos inadecuado en los medios de datos | Errores durante la restauración de datos |
| Sabotaje | Pérdida o robo de información |
| Spoofing y sniffing | Divulgación, modificación y robo de información |
| Virus | Pérdida de datos de backup |

## Datos en tránsito, datos de configuración, datos en medios externos.

| **Factor de riesgo** | **Consecuencia** |
|---|---|
| Copia no autorizada de un medio de datos | Robo de información |
| Errores en las funciones de encriptación | Divulgación de información (passwords) |
| Falla en medios externos | Pérdida de datos en medios externos |
| Mala integridad de los datos | Inconsistencia de información |
| Medios de datos no están disponibles cuando son necesarios | Pérdida de tiempo y productividad por falta de datos |
| Perdida de confidencialidad en datos privados y de sistema | Divulgación de información |
| Perdida de datos en tránsito | Divulgación de información |
| Portapapeles, impresoras o directorios compartidos | Divulgación o robo de información |
| Sabotaje | Pérdida o robo de información |
| Spoofing y sniffing | Divulgación, modificación y robo de información |
| Virus | Pérdida, modificación o divulgación de datos, pérdida de tiempo, y productividad |

## Administrador de sistemas (Departamento de Sistemas).

| Factor de riesgo | Consecuencia |
|---|---|
| Administración impropia del sistema de IT (responsabilidades y roles del personal de sistemas) | Asignación de responsabilidades impropia |
| Almacenamiento de passwords negligente | Divulgación de password y uso indebido de derechos de usuarios |
| Errores de configuración y operación del sistema | Inestabilidad del sistema, reducción de la performance y aumento de las vulnerabilidades |
| Falta de auditorías en sistema operativo | Imposibilidad del seguimiento de usuarios y de la generación de reportes |
| Mala evaluación de datos de auditoría | No se analizan los logs y por lo tanto no hay evaluación de los resultados |
| Mal uso de derechos de administrador | Mala distribución de los permisos y de las cuentas de administrador |

## Cableado.

| Factor de riesgo | Consecuencia |
|---|---|
| Ancho de banda insuficiente | Transmisión pesada en la red o imposibilidad de utilizar el sistema online |
| Conexión de cables inadmisible | Pinchaduras de cables, robo de datos, spoofing y sniffing |
| Factores ambientales | Pinchaduras de cables, robo de datos, spoofing y sniffing |
| Interferencias o daños de equipamiento | Errores en los datos de transmisión o imposibilidad de utilizar el sistema online |
| Límite de vida útil de equipos | Equipos obsoletos e imposibilidad de utilizar el sistema |
| Longitud de los cables de red excedida | Transmisión lenta o con interferencias, o imposibilidad de utilizar el sistema on-line |
| Mal mantenimiento | Errores de transmisión o interrupción del servicio de red |
| Reducción de velocidad de transmisión | Pérdida de tiempo de los usuarios, o imposibilidad de utilizar el sistema online |
| Riesgo por el personal de limpieza o personal externo | Daño en cables o equipos, interrupción del sistema on-line |

## Red

| Factor de riesgo | Consecuencia |
|---|---|
| Abuso de puertos para el mantenimiento remoto | Posibles intrusiones y robo o divulgación de información |
| Ausencia o falta de segmentación | Tramos de red extensos y dificultades en la comunicación |
| Complejidad en el diseño de las redes de sistemas de IT | Dificultad en la administración y en el mantenimiento |
| Conexiones todavía activas | Intrusión de usuarios no autorizados al sistema |
| Configuración inadecuada de componentes de red | Errores de transmisión, interrupción del servicio de red |
| Denegación de servcio | Interrupción de todos o algunos de los servicios de red |
| Errores de configuración y operación | Inestabilidad del sistema, reducción de la performance y aumento de las vulnerabilidades |
| Falla en la MAN | Una o más redes incomunicadas |
| Falta de autenticación | Posibles intrusiones y robo o divulgación de información |
| Mal uso de servicios de mail | Disminución de la performance del ancho de banda |
| Sincronización de tiempo inadecuada | Inconsistencia en datos |
| Spoofing y sniffing | Divulgación, modificación y robo de información |
| Transporte inseguro de archivos | Divulgación de información |
| | |

## Usuarios

| Factor de riesgo | Consecuencia |
|---|---|
| Acceso no autorizado a datos | Divulgación o robo de información |
| Borrado, modificación o revelación desautorizada o inadvertida de información | Inconsistencia de datos o datos faltantes |
| Condiciones de trabajo adversas | Predisposición a distracción, bajo rendimiento de usuarios |
| Destrucción de un componente de hardware | Pérdida de tiempo por necesidad de reemplazo |
| Destrucción negligente de datos | Pérdida de información |
| Documentación deficiente | Mayor probabilidad de errores por falta de instrucciones |
| Entrada sin autorización a habitaciones | Robo de equipos o insumos, divulgación de datos |
| Entrenamiento de usuarios inadecuado | Predisposición a errores y bajo rendimiento de usuarios |
| Falta de auditorías | Predisposición a un rendimiento mediocre y falta de concienciación sobre responsabilidades y seguridad |
| Falta de cuidado en el manejo de la información (Ej. Password) | Divulgación de datos |
| Ingeniería social | Robo o modificación de información |
| Mal uso de derechos de administrador (sesiones abiertas) | Divulgación o robo de información, sabotaje interno |

| | |
|---|---|
| No-cumplimiento con las medidas de seguridad del sistema | Medidas correctivas tomadas por la gerencia, según la gravedad del incidente |
| Pérdida de confidencialidad o integridad de datos como resultado de un error humano | Error en la información |
| Desvinculación del personal | Robo o modificación de información, sabotaje interno |
| Uso descontrolado de recursos (DoS) | Retraso en las actividades o falta de sistema |

## Documentación de programas, hardware, sistemas, procedimientos administrativos locales, manuales, etc.

| | |
|---|---|
| Acceso no autorizado a datos de documentación | Divulgación, robo o modificación de información |
| Borrado, modificación o revelación desautorizada de información | Documentación incorrecta |
| Browsing de información | Divulgación de información |
| Copia no autorizada de un medio de datos | Divulgación de información |
| Descripción de archivos inadecuada | Documentación incorrecta |
| Destrucción negligente de datos | Documentación incorrecta |
| Documentación insuficiente o faltante, funciones no documentadas | Entorpecimiento de la administración y uso del sistema |
| Factores ambientales | Destrucción de datos |
| Mal interpretación | Entorpecimiento de la administración y uso del sistema |
| Mantenimiento inadecuado o ausente | Documentación incorrecta, redundante y compleja |
| Medios de datos no están disponibles cuando son necesarios | Entorpecimiento de la administración y uso del sistema |
| Robo | Divulgación de información |
| Uso sin autorización | Divulgación, robo o modificación de información |
| Virus, gusanos y caballos de Troya | Pérdida, modificación o divulgación de datos, pérdida de tiempo, y productividad |
| | |

## Hardware (teclado, monitor, unidades de discos, medios removibles, etc.)

| **Factor de riesgo** | **Consecuencia** |
|---|---|
| Corte de luz, UPS descargado o variaciones de voltaje | Interrupción del funcionamiento de equipos |
| Destrucción o mal funcionamiento de un componente | Interrupción de la tarea del usuario |
| Factores ambientales | Destrucción o avería de equipos |
| Límite de vida útil | Avería de equipos |
| Mal mantenimiento | Avería de equipos e incremento en el costo de equipamiento de respaldo |
| Robo | Pérdida de equipamiento e interrupción de la tarea del usuario |

## Insumos (cintas, cartuchos de tinta, toner, papel, formularios, etc.)

| | |
|---|---|
| Factores ambientales | Destrucción de insumos |
| Límite de vida útil | Destrucción o avería de insumos |
| Recursos escasos | Interrupción en el funcionamiento normal de la empresa |
| Uso descontrolado de recursos | Incremento no justificado del gasto de insumos |
| Robo | Pérdida de insumos e incremento en el gasto |
| Transporte inseguro de medios de datos | Pérdida de datos, de insumos, e incremento en el gasto |

## Datos de usuarios.

| **Factor de riesgo** | **Consecuencia** |
|---|---|
| Falta de espacio de almacenamiento | Retraso de las actividades |
| Mala configuración del schedule de backups | Pérdida de datos del usuario |
| Medios de datos no están disponibles cuando son necesarios | Retraso en las actividades |
| Pérdida de backups | Pérdida de datos del usuario y retraso de la tarea |
| Perdida de confidencialidad en datos privados y de sistema | Divulgación de información |
| Portapapeles, impresoras o directorios compartidos | Divulgación de información |
| Robo | Divulgación de información |
| Sabotaje | Pérdida, modificación o divulgación de datos |
| Spoofing y sniffing | Divulgación, modificación y robo de información |
| Virus | Pérdida, modificación o divulgación de datos, pérdida de tiempo, y productividad |

## 2.6. Amenazas y Vulnerabilidades

Ya que se han detectado los activos se calculan los niveles de vulnerabilidad (o niveles de riesgo) en los que incurre cada activo arriba mencionado. Para esto se tiene en cuenta el nivel de importancia asignado a cada uno y la probabilidad de ocurrencia de estos riesgos. Para realizar dicho cálculo se desarrollaron las siguientes operaciones:

**PROBABILIDAD DE OCURRENCIA**: representan la probabilidad de que ocurran los factores de riesgo mencionados, en una escala del 1 al 3. Esta probabilidad fue evaluada teniendo en cuenta las medidas de seguridad existentes en la organización.

**PORCENTAJE DE LA PROBABILIDAD DEL RIESGO**: se calcula el porcentaje de probabilidad de que ocurra un determinado factor de riesgo, con respecto a la cantidad de factores de riesgo que intervienen para dicho activo. Esto es debido a que cada activo está afectado por un número diferente de riesgos posibles, de manera que este cálculo sirve para obtener un porcentaje de probabilidades equilibrado por igual para cualquier activo, independientemente de la cantidad de factores de riesgo que lo afecten.

**NIVEL DE VULNERABILIDAD**: en este momento interviene el nivel de importancia, multiplicando al porcentaje de probabilidad del riesgo. De esta forma se obtiene el nivel de vulnerabilidad de cada activo con respecto a un factor de riesgo. La suma de estos valores es el nivel de vulnerabilidad total que corresponde a cada activo.

**NOTA:**

> Por razones de seguridad y a petición de los directivos de la subdirección los datos que arrojaron las operaciones anteriores junto con las conclusiones y consecuencias no se mostraran en esta tesis, ya que se considera un documento de orden público.

**3. Políticas de seguridad de la red SIAE**

## Objetivo General de las Políticas de la Red SIAE

El objetivo general consiste en la realización de un **Plan de Seguridad Informática** para **La Red SIAE**, en donde se definen los lineamientos para promover la planeación, el diseño e implantación de un modelo de seguridad en la misma con el fin de establecer una cultura de la seguridad en la organización. Asimismo, la obliga a redactar sus propios procedimientos de seguridad, los cuales deben estar enmarcados por este plan.

La definición de la presente política de seguridad informática y de los estándares asociados es esencial para hacerles saber a todos los empleados de la  y personas que utilicen los servicios que brinda el SIAE lo que pueden hacer y lo que no, para salvaguardar los activos informáticos de la **de Sistemas de Registro Escolar**.

Sobre lo que pueden hacer, las políticas les señalan como hacerlo y sobre lo que no deben hacer les marca claramente sus responsabilidades.

## Disposiciones generales

Toda persona que utilice cualquier servicio que ofrece la  de Sistemas de Registro Escolar deberá conocer las políticas de seguridad de la red SIAE así como el reglamento vigente sobre su uso. El desconocimiento del mismo no exonera de las responsabilidades asignadas.

Los casos no previstos por el presente reglamento serán resueltos por la  de Sistemas de Registro Escolar. Si la situación lo amerita se procederá en conjunto con al menos dos personas representantes de la Dirección General  de Administración Escolar (DGAE), dos personas representantes de las autoridades de plantel y si el caso lo requiere con dos representantes de la Dirección General de Computo Académico; o garantizando una representación análoga por las partes involucradas.

## Vigencia

El presente Plan de Seguridad Informática es de aplicación a partir del  de  de 2003.

## Autoridad de emisión

Este documento es emitido por la alumna de la Facultad de Ingeniería UNAM a ser presentado como Tesis de la carrera de Ingeniería en Computación.

Además este documento es publicado por la  de Sistemas de Registro Escolar (SSRE), cuyos servicios han sido autorizados por la Dirección General de Administración Escolar (DGAE) de la Universidad Nacional Autónoma de México (UNAM).

## Contenido

Este Plan presenta las **Políticas de Seguridad Informática** cuyo contenido se agrupa en los siguientes aspectos:

1. Seguridad Lógica.
2. Seguridad en las Comunicaciones.
3. Seguridad de las Aplicaciones.
4. Seguridad Física.
5. Administración del Centro de Cómputos.
6. Auditorias y Revisiones.
7. Plan de Contingencia.
8. Reglamento y Uso de la Red SIAE

## Desarrollo

En este Plan de Seguridad Informática se desarrollan normas y procedimientos que pautan las actividades relacionadas con la seguridad informática y la tecnología de información. Este deberá ser aprobado por los directivos de  de Sistemas de Registro Escolar, para su implantación.

Estas políticas de seguridad informática y las medidas de seguridad en ellas especificadas deben ser revisadas periódicamente, analizando la necesidad de cambios o adaptaciones para cubrir los riesgos existentes y auditando su cumplimiento.

## 3.1 Seguridad Lógica

### 3.1.1 Identificación de ID's

Deberá existir una herramienta para la administración y el control de acceso a los datos.

Debe existir una **política formal de control de acceso** a datos donde se detalle como mínimo:

- el nivel de confidencialidad de los datos y su sensibilidad
- los procedimientos de otorgamiento de claves de usuarios para el ingreso a los sistemas
- los estándares fijados para la identificación y la autenticación de usuarios.

Para **dar de alta un usuario** al sistema debe existir un procedimiento formal, por escrito, que regule y exija el ingreso de los siguientes datos: identificación del usuario, deberá ser única e irrepetible,

- password, debe ser personal y asignado por el dba(administrador de base de datos)
- nombre y apellido completo
- departamento al que pertenece
- grupo de usuarios al que pertenece
- fecha de expiración del password
- fecha de anulación de la cuenta
- contador de intentos fallidos

Deben asignarse los **permisos mínimos** y necesarios para que cada usuario desempeñe su tarea.

Debe existir una manera de **auditar (lista de control de acceso)** todos los requerimientos de accesos y los datos que fueron modificados por cada usuario, y si este tiene los permisos necesarios para hacerlo.

Deberá restringirse el acceso al sistema o la utilización de recursos en un **rango horario definido**, teniendo en cuenta que:

- las cuentas de los usuarios no deben poder acceder al sistema en horarios no laborales, de acuerdo al grupo al que pertenezcan
- durante las vacaciones o licencias las cuentas de usuarios deben desactivarse

- en días feriados las cuentas de usuarios, a excepción de los del departamento de DASSU, deben permanecer desactivadas.

Deben restringirse las conexiones de los usuarios sólo a las **estaciones físicas autorizadas**.

El **administrador debe poder acceder al sistema** solamente desde las terminales que se encuentren en el centro de cómputos.

El administrador del sistema deberá realizar un **chequeo mensual de los usuarios** del sistema, comprobando que existen solo los usuarios que son necesarios y que sus permisos sean los correctos.

Para **dar de baja un usuario** deberá existir un procedimiento formal por escrito, a través del cual los datos del usuario no se eliminarán sino que se actualizará la fecha de anulación de su cuenta, quedando estos datos registrados en el histórico.

Además, se debe llevar a cabo una **política de desvinculación del personal**, a través de la cual se quitan permisos al empleado paulatinamente, evitando un posible acto de vandalismo por insatisfacción con la decisión de la subdirección.

El sistema deberá **finalizar toda sesión interactiva** cuando la terminal desde donde se esté ejecutando no verifique uso durante un período de cinco minutos, deberá deslogear al usuario y limpiar la pantalla.

Las PC´s deben tener instalado un **protector de pantalla con contraseña**.

Los usuarios del sistema solamente podrán abrir **una sesión de cada aplicación**, y no podrán abrir dos sesiones del mismo menú en diferentes terminales ni en la misma terminal.

Se deberá impedir la existencia de **perfiles de usuarios genéricos**, en todos los sistemas operativos y en el sistema informático.

Se deberá minimizar la generación y el uso de perfiles de **usuario con máximos privilegios**. Todos los usos de estas clases de perfiles deberán ser registrados y revisados por el administrador de seguridad.

Deberá existir un **administrador total del sistema** (sa), que deberá estar resguardado en un sobre cerrado bajo adecuadas normas de seguridad. En caso que sea necesaria su utilización se deberá proceder de acuerdo con un procedimiento de autorización estipulado a tal fin.

Un **segundo administrador** (un súper-usuario) debe ser creado con privilegios similares al anterior. Se creará un **tercer** perfil de administrador del sistema, con los permisos mínimos necesarios para la realización de tareas cotidianas del administrador. Ninguno de estos usuarios tendrá permitida la eliminación del usuario sa.

Los administradores que realizan tareas de mantenimiento, deberán tener otro perfil, con un nivel de acceso menor, denominado **mantenimiento***,* para ser utilizado en tareas cotidianas que no requieran privilegios de súper usuario.

Periódicamente el administrador del sistema deberá **chequear** las acciones desempeñadas con las cuentas de administradores y de mantenimiento.

### 3.1.2 Autenticación

La **pantalla de acceso** del sistema deberá mostrar los siguientes datos:

- nombre de usuario
- password
- periodo o plantel

Mientras el usuario está **ingresando su contraseña**, esta no debe ser mostrada por pantalla.

Cuando el **usuario logra acceder** al sistema deberán registrarse los siguientes datos:

- nombre de usuario
- fecha y hora de la última conexión
- localización de la última conexión (Ej. número de terminal)
- cantidad de intentos fallidos de conexión de ese ID de usuario desde la última conexión lograda.

La **aplicación para administrar los datos de usuarios** solo deberá ejecutarse en máquinas designadas del centro de cómputos.

Deberán **encriptarse**:

- la lista de control de accesos
- los passwords y datos de las cuentas de usuarios
- los datos de autenticación de los usuarios mientras son transmitidos a través de la red.

### 3.1.3 Password

Los passwords deberán tener las siguientes **características**:

- conjunto de caracteres alfa-numérico
- longitud definida internamente

La **fecha de expiración** del password deberá ser de cuatro meses. El sistema exigirá automáticamente el cambio, una vez cumplido el plazo.

El password **no deberá contener** el nombre de la subdirección, el nombre del usuario, ni palabras reservadas.

Bloquear el perfil de todo usuario que haya intentado **acceder al sistema en forma fallida** por más de **cinco** veces consecutivas.

Controlar que el password ingresado sea **diferente a los últimas cinco utilizados**.

El password deberá tener un **período de duración mínimo** de 5 días. El sistema no permitirá el cambio de password si este período no se ha cumplido.

Si un usuario **olvida el password**, el administrador permitirá que ingrese cuando intente acceder de nuevo al sistema, proporcionándole otro password.

### 3.1.4 Segregación de funciones

Debe existir una adecuada y documentada **separación de funciones** dentro del centro de cómputos.

El área de sistemas debe encontrarse ubicada en el **organigrama** de la subdirección en una posición tal que garantice la independencia necesaria respecto de las áreas usuarias.

## 3.2 Seguridad de las comunicaciones

### 3.2.1 Topología de red

Se deberá asegurar la **integridad, exactitud, disponibilidad y confidencialidad** de los datos transmitidos, ya sea a través de los dispositivos de hardware, de los protocolos de transmisión, o de los controles aplicativos.

Deberá existir **documentación** detallada sobre los diagramas topológicos de las redes, tipos de vínculos y ubicación de nodos.

Deberán existir **medios alternativos de transmisión** en caso de que alguna contingencia afecte al medio primario de comunicación.

### 3.2.2 Conexiones externas

Asegurar la definición e implementación de procedimientos pertinentes para el **control de las actividades de usuarios externos** del organismo a fin de garantizar la adecuada protección de los bienes de información de la organización.

La conectividad a Internet será otorgada para propósitos relacionados con el SIAE y mediante una **autorización de la Subdirección**. Los usuarios no autorizados deberán estar imposibilitados de conectarse al exterior.

Los usuarios de la dependencia que utilicen Internet deben recibir **capacitación específica** respecto a su funcionalidad y a los riesgos y medidas de seguridad pertinentes.

Debe asegurarse que la totalidad del tráfico entrante y saliente de la red interna, sea filtrado y controlado por un **firewall** prohibiendo el pasaje de todo el tráfico que no se encuentre expresamente autorizado.

Todas las conexiones a Internet de la dependencia deben traspasar un servidor **Proxy** una vez que han traspasado el firewall.

Deben documentarse los **servicios provistos** a través de Internet y definirse las responsabilidades en cuanto a su administración. No se publicarán en Internet datos referidos a las cuentas de correo de los empleados.

La información enviada a través de equipos de comunicaciones de la  se considera **privada**. Cabe aclarar que la información no es pública, a menos que en forma expresa se indique lo contrario.

El uso de Internet debe ser **monitoreado** periódicamente. Si existe alguna razón para creer que la seguridad está siendo violada, la  puede revisar el contenido de las comunicaciones de Internet.

El acceso casual a los mensajes de correo electrónico por los administradores y similares, se considera una violación a la política de seguridad de la información. Sin embargo, la  tiene el **derecho de examinar** cualquier información, sin previo consentimiento o notificación del empleado, en caso que se considere que se está utilizando inadecuadamente los activos de la dependencia.

De ser necesario realizar **mantenimiento remoto** a los servidores, se utilizarán protocolos y servicios de comunicación que garanticen la seguridad de los datos que se transmiten a través de la red, utilizando encriptación.

Deberán documentarse cada una de las actividades que el personal externo realice sobre los equipos utilizando acceso remoto. Para llevar a cabo estas tareas, el encargado del mantenimiento deberá solicitar formalmente la dirección IP del servidor de Internet y el password de la cuenta de mantenimiento al administrador del centro de cómputos.

### 3.2.3 Configuración lógica de red

El riesgo aumenta con el número de conexiones a **redes externas**; por lo tanto, la conectividad debe ser la mínima necesaria para cumplir con los objetivos de la dependencia.

El esquema de direcciones de la **red interna** no debe ser visible ante las conexiones externas.

Deberá asegurarse que la **dirección IP** de la dependencia sea confidencial.

Los **recursos lógicos** o físicos de los distintos **puestos de trabajo** no deben ser visibles en el resto de la red informática. Los recursos de los **servidores** serán visibles solo en los casos necesarios y con las medidas de seguridad correspondientes.

### 3.2.4 Mail

La  determinará que empleados deben contar con una **cuenta** de correo electrónico, según lo amerite su tarea.

Deberá existir un **procedimiento** formal para dar de alta y de baja las cuentas de correo electrónico en el sistema informático.

La subdirección deberá contar con un sistema de **mail externo y uno interno**, con diferentes dominios. De esta manera, las comunicaciones entre el personal de la dependencia se realizarán sin exponer los mensajes a Internet.

Los **aplicativos** de correo electrónico deben brindar las condiciones de seguridad necesarias para evitar los virus informáticos o la ejecución de código malicioso, deben brindar la facilidad de impedir que un usuario reciba correos de un remitente riesgoso para los recursos de la dependencia.

El servidor de mail no debe ser utilizado para enviar correo basura (**SPAM**).

Los mensajes de correo electrónico deben ser considerados como **documentos formales** y deben respetar todos los lineamientos referentes al uso inapropiado del lenguaje.

El correo electrónico no debe ser utilizado para enviar **cadenas de mensajes,** no debe relacionarse con actividades ilegales y no éticas o para mensajes no relacionados con los propósitos de la dependencia.

Los datos que se consideraron "confidenciales" o "críticos" deben **encriptarse**.

Debe existir un procedimiento de **priorización** de mensajes, de manera que los correos electrónicos de prioridad alta sean **resguardados**.

Deberá asignarse una **capacidad de almacenamiento** fija par cada una de las cuentas de correo electrónico de los empleados.

### 3.2.5 Antivirus

En todos los **equipos** de la subdirección debe existir una herramienta antivirus ejecutándose permanentemente y en continua actualización.

Deberá utilizarse más de una herramienta antivirus en las PC's clientes, para así disminuir el riesgo de infección.

Deberán existir **discos de rescate** de los antivirus, tanto para los servidores como para las PC's clientes, que sean capaces de realizar escaneos de virus a bajo nivel y restaurar los sistemas.

La **actualización** de los antivirus de todos los equipos de la subdirección deberá realizarse a través de un procedimiento formal y, si es posible, automático, a cargo de un empleado del centro de cómputos designado por el administrador.

Deberán programarse **escaneos** periódicos de virus en todos los equipos de la dependencia; esta tarea estará a cargo de personal designado por el administrador del centro de cómputos.

Deberá existir un **procedimiento formal** a seguir en caso que se detecte un virus en algún equipo del sistema.

### 3.2.6 Firewall

El firewall de la dependencia debe presentar una postura de negación preestablecida, configurado de manera que se prohíban todos los **protocolos y servicios**, habilitando los necesarios.

Los servicios o protocolos que solo sean necesarios esporádicamente deberán habilitarse **bajo petición expresa y autorizada del jefe inmediato**. Aquellos que sean considerados riesgosos deberán habilitarse bajo estrictas limitaciones de uso, considerando el equipo desde el que se utilizará, hacia qué destino, las fechas y los horarios para dichas conexiones.

El **encargado de mantenimiento** debe controlar periódicamente la configuración del firewall y los servicios de red, documentando los resultados de dichas pruebas.

De haber una falla en el firewall, debe ser una "**falla segura**", lo que significa que todos los accesos al servidor de Internet deben bloquearse.

### 3.2.7 Ataques de red

Toda la información que se considere confidencial deberá **encriptarse** durante la transmisión, o viajar en formato no legible.

Deben existir **procedimientos** formalmente documentados destinados a prevenir los ataques de red más frecuentes.

Se deberá usar algún sistema de detección de intrusos (**IDS**), tolerantes al fallo, utilizando los mínimos recursos posibles.

Deberá utilizarse una herramienta que monitoree la red, con el fin de evitar el ataque de denegación de servicio (**DoS**).

Para disminuir el riesgo de **sniffing**, la red de la subdirección deberá segmentarse física y/o lógicamente.

Con el fin de disminuir la posibilidad de **spoofing** el firewall deberá denegar el acceso a cualquier tráfico de red externo que posea una dirección fuente que debería estar en el interior de la red interna.

Los **archivos de passwords** y datos de usuarios no deberán almacenarse en el directorio por default destinado a tal fin. Además deberán estar encriptados utilizando encriptación en un solo sentido ("one way"), con estrictos controles de acceso lógico, de manera de disminuir la posibilidad de ataques.

## 3.3 Seguridad de las aplicaciones

### 3.3.1 Software

El **sistema operativo** de los servidores deberá presentar las siguientes características:

- alta confiabilidad
- equilibrio en costo y beneficio
- compatibilidad e interoperatividad con los sistemas operativos de las PC´s y demás sistemas usados en la
- escalabilidad
- disponibilidad de software de aplicación y actualizaciones
- buena administración y generación de logs
- cumplir con los requerimientos funcionales impuestos por la
- amigable con el usuario
- disponibilidad de documentación

Además deberá presentar las siguientes características en lo relativo a la **seguridad**:

- identificación y autenticación
- control de acceso
- login
- incorruptibilidad
- fiabilidad
- seguridad en la transmisión
- backup de datos
- encriptación
- funciones para preservar la integridad de datos
- requerimientos sobre privacidad de datos

### 3.3.2 Seguridad de bases de datos

El administrador de sistemas deberá confeccionar un **Plan de Migración** desde archivos indexados a bases de datos relacionales, una vez que el sistema esté desarrollado en su totalidad.

Los archivos fuentes y ejecutables de la dependencia, las carpetas donde se encuentran almacenados y las aplicaciones que los administran deberán tener **controles de acceso**, de forma tal que la única persona que pueda tener acceso a estos recursos sea el administrador del centro de cómputo.

Debe existir una aplicación que registre las siguientes **ocurrencias**:

- tiempo y duración de los usuarios en el sistema
- número de conexiones a bases de datos
- número de intentos fallidos de conexiones a bases de datos
- ocurrencias de deadlock con la base de datos
- estadísticas de entrada-salida para cada usuario
- modificación de datos

Deberán hacerse **chequeos regulares** de la seguridad de la base de datos, en los que se deberá verificar que:

- se hacen y son efectivos los backups y los mecanismos de seguridad
- no haya usuarios de la base de datos que no tengan asignado una contraseña
- se revisen los perfiles de los usuarios que no han usado la base de datos por un período largo de tiempo
- nadie, además del administrador de datos, ha accedido a los archivos del software de base de datos y ha ejecutado un editor de archivos indexados
- solo el administrador de datos tiene acceso de lectura y escritura en los archivos de programa
- la base de datos y las aplicaciones que la administran tiene suficientes recursos libres para trabajar eficientemente.

Deben mantenerse registros de todas las transacciones realizadas en la base de datos, de manera que éstas puedan revertirse en caso de surgir un problema.

Deberá existir una **clasificación de los datos** en base a su sensibilidad para definirlos como críticos y así determinar controles específicos. Se deberán definir tres niveles de información:

- *Crítica*:

    - la no-disponibilidad de esta información ocasiona un daño en los servicios por los que fue creado el SIAE.
    - se considera recurso crítico a aquel recurso interno que debe estar disponible solamente para un conjunto determinado de personas, debe ponerse un cuidado especial en información que por ley o que por políticas de la dependencia debe permanecer confidencial; la clasificación de un recurso como crítico deberá incluir los criterios para determinar quienes tienen acceso a él. De ser necesaria su transmisión por redes externas o su almacenamiento en sistemas de la red perímetro, deberán tomarse medidas de seguridad extremas, la información deberá encriptarse.

- *Confidencial*:

    - en poder de personas no autorizadas compromete los intereses de los alumnos y planteles.
    - Se considera recurso confidencial a todo aquel que solo deberá utilizarse y ser del conocimiento de miembros de la dependencia y por defecto todo aquel recurso que no haya sido explícitamente clasificado como disponible al público.

- *Pública*:

    - información de libre circulación
    - se considera recurso disponible al público aquel que no requiere permanecer como de uso interno y que explícitamente se ha clasificado como un recurso público.

Esta clasificación deberá ser documentada e informada a todo el personal de la organización, y deberá evaluarse y actualizarse periódicamente.

Deberá existir un **responsable** en cada área de la dependencia, que responda por la información que se maneja en dicho sector. Deberá definir la clasificación de los datos y los controles de acceso que son necesarios, junto con el administrador del sistema.

### 3.3.3 Control de las aplicaciones en PC's

Deberán existir **estándares de configuración** de los puestos de trabajo, servidores y demás equipos de la red informática.

En base al estándar se deberá generar un **procedimiento** donde se especifique qué aplicaciones deben instalarse de acuerdo al perfil de cada usuario y con qué frecuencia se harán las actualizaciones de dichas aplicaciones.

Las **aplicaciones solo se actualizarán** debido al reporte de algún mal funcionamiento o a un nuevo requerimiento por parte de los usuarios o del personal del centro de cómputo.

Antes de hacer un cambio en la configuración de los servidores se deberá hacer un **backup de la configuración existente**. Una vez que el cambio ha resultado satisfactorio deberá almacenarse la configuración modificada.

Se deberá establecer un **procedimiento de emergencia** para dejar sin efecto los cambios efectuados y poder recuperar las versiones autorizadas anteriores en el caso de generarse problemas.

Se deberán **documentar** no solo el procedimiento de instalación y reparación de equipos, sino además cada uno de los mantenimientos que se les realicen.

Deberán generarse historiales y así calcular datos estadísticos de los cambios realizados y los errores reportados.

En el momento en que un nuevo usuario ingrese a la Subdirección, se lo deberá **notificar y deberá aceptar** que tiene prohibida la instalación de cualquier producto de software en los equipos.

Se deberán realizar **chequeos periódicos** en las PC´s, los servidores y demás equipos, en búsqueda de aplicaciones instaladas no autorizadas o innecesarias.

### 3.3.4 Control de datos en las aplicaciones

Los **datos de entrada y salida** del sistema deberán poseer controles donde se verifique su integridad, exactitud y validez.

Los datos de salida del sistema de la dependencia deben restringirse con **controles lógicos**, de acuerdo a los permisos de acceso.

Deberán protegerse con **controles de acceso** las **carpetas** que almacenen los archivos de las aplicaciones, y sólo el administrador de sistemas tendrá acceso a ellas.

### 3.3.5 Ciclo de vida

Deberá utilizarse un **plan detallado de sistemas**, donde se definan las asignaciones de recursos, el establecimiento de prioridades y responsabilidades, la administración de tiempos y la utilización de métricas de software. Esta norma deberá aplicarse tanto para el desarrollo de las aplicaciones como para las modificaciones que se realicen.

Antes de realizar alguna modificación en el sistema, deberá realizarse un **análisis del impacto** de este cambio.

Se deberá implementar un sistema de configuración de versiones de aplicación, y deberán documentarse los cambios desarrollados en las mismas.

Deberá existir un **documento formal de solicitud de cambios**, donde quede reflejado el motivo y la solicitud del cambio, allí se agregarán los requerimientos de seguridad necesarios, definidos por el responsable de la información y el administrador de sistemas. La documentación de los cambios debe incluir:

- sistema que afecta
- fecha de la modificación
- desarrollador que realizó el cambio
- empleado que solicitó el cambio
- descripción global de la modificación

El formulario anterior se utilizará para actualizar la **documentación del desarrollo** y de los distintos manuales generados.

Deberán realizarse **pruebas del software** desarrollado, para esto se generarán planes y escenarios de prueba y se documentarán los resultados.

Todo nuevo desarrollo o modificación deber estar **probado y aprobado** por los usuarios del mismo antes de su instalación en el ambiente de trabajo.

La metodología para el desarrollo y mantenimiento de sistemas debe contemplar una **revisión de post-implantación** del sistema en operación, que deberá determinar si se han logrado los objetivos previstos, y si se ha alcanzado la satisfacción de las necesidades planteadas por los usuarios.

Se deberá informar por escrito la importancia de la seguridad de la información a todo el personal contratado. El administrador del centro de cómputo, junto con los directivos, serán quienes:

- especifiquen los requerimientos de seguridad
- determinen los pasos a seguir en caso que no se respete lo establecido en el reglamento de uso de la Red SIAE
- establezcan cláusulas sobre confidencialidad de la información
- exijan al tercero en cuestión que informe posibles brechas de seguridad existentes.

# 3.4 Seguridad física

## 3.4.1 Equipamiento

Deberá existir una adecuada **protección física y mantenimiento** permanente de los equipos e instalaciones que conforman los activos de la dependencia.

## 3.4.2 Control de acceso físico al centro de cómputo

El **control de acceso** se será por medio de una tarjeta electrónica. Todo el personal deberá acceder a las instalaciones con su tarjeta de acceso que será personal y única para cada uno de los que laboren en la Subdirección.

Se deberá restringir el acceso físico a las **áreas críticas** a toda persona no autorizada, para reducir el riesgo de accidentes y actividades fraudulentas.

Se deberá asegurar que todos los **individuos** que entren a áreas restringidas se identifiquen y sean autenticados y autorizados para entrar.

Cualquier **persona ajena a la** que necesite ingresar al centro de cómputos deberá anunciarse en la puerta de entrada.

El **área del centro de cómputos** donde se encuentran los servidores y demás equipamiento crítico solo debe tener permitido el acceso a los administradores.

Se debe realizar un adecuado mantenimiento y **prueba de los procedimientos** para la restricción de acceso físico, así como de los dispositivos de seguridad para la prevención, detección y extinción del fuego.

## 3.4.3 Cableado estructurado

El cableado debe seguir las normas del **cableado estructurado**, que garantizan el funcionamiento eficiente de la red.

Se deberá **documentar** en planos los canales de tendidos de cables y las canaletas de red existentes.

Debe existir tendido de **cableado redundante** para futuros puestos de trabajo. Estos cables no deben tener los ductos de red instaladas.

Deberá medirse periódicamente el **nivel de interferencia** que existe en la red. Si este nivel excede un mínimo permitido, deberán tomarse las acciones correctivas necesarias.

Ante un **corte del suministro de energía** eléctrica deberán apagarse los equipos del centro de cómputo de forma segura, como medida de prevención.

## 3.5 Administración del centro de procesamiento de datos

### 3.5.1 Administración del CDP

La  deberá asegurar la correcta **organización y administración** del área de sistemas a fin de que ésta brinde condiciones generales de operación que posibiliten un ambiente adecuado de control.

Se deberá designar en la dirección del área un **profesional** que acredite experiencia en el manejo de los recursos informáticos y comprenda los riesgos y problemas relativos a la tecnología y sistemas de información. Es su obligación y responsabilidad el mantener seguros los sistemas que operan.

Deberá designarse un **encargado de la seguridad** del sistema, que coordine las tareas correspondientes, haciendo cumplir las políticas de seguridad en toda la subdirección.

Deberá existir una **planificación** formalizada y completa de las actividades que se desarrollan normalmente. Deberán designarse responsabilidades claras y documentadas para actividad.

Deberá desarrollarse un plan de sistemas a **corto plazo**, que contenga un cronograma de las actividades, asignación de prioridades, recursos, sectores involucrados y la totalidad de las tareas a llevarse a cabo durante un periodo de un año.

Deberá desarrollarse de un plan estratégico a **largo plazo**, que contenga los proyectos principales y los cronogramas de su implementación, para un periodo de por lo menos 3 años.

**Ambos planes** deben tener objetivos concordantes con los de la organización, y deben supervisarse continuamente permitiendo su actualización en caso de ser necesario.

Deberán generarse **reportes** trimestrales dirigidos al Subdirector de la dependencia, informando sobre las actividades en el centro de cómputo, el progreso de los planes propuestos y el cumplimiento de las políticas impuestas.

El equipo de sistemas debe hacer hincapié en la concienciación de todos los usuarios, generando una **cultura de la seguridad**, haciéndolos partícipes de las medidas de seguridad, tanto los usuarios actuales como los que se incorporen en el

futuro. El proceso de concientización debe ser renovado y transmitido a los usuarios en forma anual.

Los usuarios solicitarán **asesoramiento** o servicios al centro de cómputo a través de mails, de manera que se genere un registro de los trabajos efectuados por los empleados del centro de cómputo y de las solicitudes de los empleados.

Deberá implementarse un **buzón de sugerencias** donde los usuarios recomienden mejoras o realicen comentarios, expresando sus inquietudes.

Deberá existir un procedimiento para realizar la **publicidad** de políticas, planes o normas de la dependencia y sus modificaciones.

Deberá existir un encargado de llevar a cabo el **mantenimiento preventivo** el equipamiento informático de la dependencia, monitorizando, chequeando y auditando las PC´s y demás dispositivos que conforman la red.

Los administradores deberán informar en tiempo de **suspensiones** en el servicio necesarias por mantenimiento, especificando fecha, hora y duración de la suspensión.

Deberá generarse un **inventario** detallado donde se describan los sistemas de información y de los equipos de cómputo utilizados en la organización.

Deberá asignarse un responsable de mantenerlo actualizado y de realizar controles periódicos.

Deberán existir procesos para **rotular**, manipular y dar de baja el equipamiento informático.

Los **medios de instalación originales** del software deberán respaldarse y resguardarse adecuadamente, en caso de que no sean de solo lectura, siempre se mantendrán con las protecciones contra escritura que estén disponibles para el medio. En la medida de lo posible se evitará instalar el software directamente de los medios originales.

Debe existir un procedimiento para controlar que en el organismo solamente se utilicen productos de **software** adquiridos por vías oficiales.

### 3.5.2 Capacitación

El **personal del centro de cómputo** debe mantenerse capacitado respecto de las tecnologías utilizadas en la organización.

Debe **impartirse capacitación** a los usuarios finales a efectos de que puedan operar adecuadamente los recursos informáticos.

El personal debe ser entrenado respecto al cumplimiento de lo especificado en la **política de seguridad** informática. Se debe entregar una copia de la misma a cada empleado.

Se debe obtener un **compromiso firmado** por parte del personal respecto al cumplimiento de las medidas de seguridad definidas en la política de seguridad informática, destacando específicamente el mantenimiento de la confidencialidad de las claves de acceso, la no-divulgación de información de la organización, el cuidado de los recursos, la utilización de software sin licencia y el reporte de situaciones anormales. Debe confirmarse este compromiso anualmente o cada vez que se produzcan cambios en las funciones asignadas al personal.

Asegurar que los empleados reciban **capacitación continua** para desarrollar y mantener sus conocimientos, competencia, habilidades y concientizarlos en materia de seguridad informática dentro del nivel requerido a fin de lograr un desempeño eficaz.

### 3.5.3 Backup

Se deberá asegurar la existencia de un **procedimiento** aprobado para la generación de copias de resguardo sobre toda la información necesaria para las operaciones de la organización, donde se especifique la periodicidad y el lugar físico donde se deben mantener las copias generadas.

La **periodicidad** de la generación de los resguardos debe ser acorde a que tan crítica sea la información y la frecuencia de cambios.

La **ubicación** de los backups debe contar con adecuadas medidas de seguridad, sin estar expuestos a las mismas contingencias que el centro de cómputo, es decir que deberán almacenarse en el exterior de la subdirección, y ser transportados en un medio resistente que los proteja. Debe designarse un **responsable** y un suplente encargados de su custodia, y se generará un registro de los **movimientos** de estos medios.

Los archivos de backup deben tener un **control de acceso** lógico de acuerdo a la sensibilidad de sus datos, además de contar con protección física.

El administrador del centro de cómputo debe designar un **responsable** de la realización de las copias de seguridad y de su restauración, y un suplente de éste primero.

Deberán realizarse chequeos para comprobar el funcionamiento correcto de los **medios externos** donde se realizan las copias de respaldo. Además debe existir una política de reemplazo de medios externos de almacenamiento de backups, de manera de sustituirlos antes de su degradación física, y deberán poseer rótulos para identificarlos.

Deberá existir un **procedimiento de recuperación** de copias de respaldo, donde se incluya la metodología a seguir y el responsable de la realización. Deberán realizarse **chequeos** para comprobar que los procedimientos de restauración son eficientes.

Debe existir una **política de documentación** de copias de respaldo, donde se registren todos los datos necesarios para la gestión del procedimiento de backup. Se deberá llevar un **inventario** actualizado de las copias de respaldo.

Deben generarse copias de respaldo de las **configuraciones de los servidores**, documentando las modificaciones realizadas para identificar las distintas versiones. Se deberá establecer un procedimiento de emergencia para dejar sin efecto los cambios efectuados y poder recuperar las **versiones autorizadas anteriores.**

No deberán utilizarse los **servidores** de la subdirección como medios de almacenamiento de las copias de respaldo de ningún sistema.

Se deberá generar una copia de respaldo de toda la **documentación** del centro de cómputo, incluyendo el hardware, el software, y el plan de contingencias, la cual deberá ser de acceso restringido y estar físicamente en un lugar distinto a los centros de procesamiento.

### 3.5.4 Documentación

Deberá generarse un **soporte** de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en el centro de cómputo.

Deberán existir una documentación y un registro de las **actividades** del centro de cómputo (procesos normales, eventuales y excepcionales) que se desarrollan diariamente, que incluya como mínimo el detalle de los procesos realizados.

Deberá desarrollarse documentación detallada sobre el equipamiento informático, que consista en diagramas y distribución física de las instalaciones, **inventarios** de hardware y software, diagramas topológicos de las redes, tipos de vínculos y ubicación de nodos. Esta documentación comprende tanto al centro de procesamiento de datos principal, como a los secundarios y las redes departamentales.

Deberá existir un registro de los eventos, **errores** y problemas del hardware y el software utilizados en las operaciones de procesamiento de datos.

La metodología para el **desarrollo** y mantenimiento de sistemas debe incluir estándares para la documentación de las aplicaciones y las actividades. Esta documentación deberá mantenerse actualizada y abarcar todas las fases del ciclo de vida del desarrollo de los sistemas.

## 3.6 Auditorias y revisiones

### 3.6.1 Chequeos del sistema

La dependencia debe asegurar que los sistemas provean las herramientas necesarias para garantizar un correcto control y auditabilidad para asegurar la integridad, confidencialidad y disponibilidad de la información. Para ello deben existir:

- **Herramientas que registren** todos los eventos relacionados con la seguridad de la información procesada por el centro de cómputo de la dependencia.

- **Herramientas que analiza los registros** generando reportes, estadísticas, gráficos con relación a los datos recogidos, con distintas frecuencias (diarios, semanales, mensuales y anuales). Deberá tener la capacidad de generar alarmas teniendo en cuenta la severidad de los eventos acontecidos.

- **Procedimientos de revisión** de los eventos registrados, a cargo de un empleado designado por el administrador, de forma de detectar anomalías y tomar las acciones correctivas necesarias.

Se deberán **registrar**, mediante logs de auditoría, aquellos eventos relacionados con la seguridad de la información. Dichos registros deberán contener como mínimo:

- fecha y hora del evento
- fuente (el componente que disparó el evento)
- ID del evento (número único que identifica el evento)
- equipo (máquina donde se generó el evento)
- usuario involucrado
- descripción (acción efectuada y datos asociados con el evento)

Se deberán registrar como mínimo los siguientes **eventos respecto a los servidores**:

- los servicios de mail
- servicios de red
- configuración de los servidores

- utilización del CPU
- reinicio de servidores

Deberán **actualizarse continuamente las herramientas** de análisis de logs, asignándole la responsabilidad de esta tarea a una persona en particular.

Deberá existir un proceso encargado de la **rotación y eliminación** de logs. Se deberá conservar esta información al menos durante tres meses.

Deberán generarse **líneas de base** que contengan información sobre las PC´s, los servidores y el sistema informático en su totalidad, con datos históricos obtenidos de los registros de auditoría, que sirvan para el cálculo de estadísticas y la generación de reportes diarios, semanales, mensuales y anuales.

Estas líneas de base deben ser **resguardadas** en medios de almacenamiento externo no reutilizables, antes de la eliminación de los logs.

Deberán **actualizarse** las líneas de base cada vez que se modifique la configuración del sistema.

Deben programarse **auditorías periódicas y chequeos aleatorios**, para controlar las áreas o funciones críticas con respecto a la seguridad de los datos de la dependencia, documentando la ejecución y los resultados de dichas pruebas.

Se deberán **analizar periódicamente** los siguientes eventos específicos como mínimo:

- controles de acceso y permisos de los usuarios
- uso de recursos informáticos
- operaciones de borrado o modificación de objetos críticos
- intentos de ingreso al sistema fallidos

Se deberán **documentar** las revisiones y controles efectuados, y **comunicar** las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

### 3.6.2 Responsabilidad de los encargados de seguridad

El administrador del sistema o un **encargado de auditorias** designado por él, deberá:

- determinar qué logs se generarán
- determinar qué eventos de seguridad se auditarán
- determinar qué datos se recogerán de estas auditorias
- administrar, desarrollar e implementar los procedimientos de auditoría y revisión
- monitorizar y reaccionar a los avisos (warnings) y reportes
- chequear aleatoriamente para verificar el cumplimiento de los requerimientos y procedimientos de seguridad
- revisar los reportes de auditorias cuando es advertido de anomalías

El **encargado del mantenimiento** de los servidores debe encargarse de actualizar las herramientas de análisis de logs.

### 3.6.3 Auditorias de control de acceso

Los **logs** deben almacenarse en carpetas de los servidores protegidas con contraseña. Esta contraseña debe ser desconocida para todos los usuarios del sistema, excepto para el administrador, por lo que debe conservarla un miembro del Directorio.

Deberán generarse logs referidos al **acceso a datos**, identificando los archivos abiertos por usuario.

Deberán generarse logs referidos a la **modificación de datos**, identificando los datos modificados por cada usuario y el valor anterior de dicho dato.

Deben generarse logs cuando un usuario **modifica su contraseña**, con datos sobre la aplicación desde la que se realizó el cambio y, en caso que el cambio resulte fallido, el motivo del fallo.

Deben generarse logs cuando hubo un **fallo en el acceso al sistema** de un usuario, indicando el motivo del fallo.

Debe generarse un logs cuando se produzca el **bloqueo de un usuario** avisando al administrador por medio de un sistema de alerta.

### 3.6.4 Auditoria de redes

Debe generarse un **plan de monitorización de red** utilizando algún escáner de seguridad integral (Overall security scanner).

Con respecto a las **conexiones a Internet** deben almacenarse datos sobre:

- número IP de la máquina conectada
- dirección de las páginas visitadas
- cookies guardadas
- archivos descargados
- servicios utilizados
- aplicaciones utilizadas

Con respecto a la utilización de la **red informática** deben almacenarse datos sobre:

- ancho de banda utilizado y cuellos de botella en el tráfico de red
- tráfico generado por las aplicaciones
- recursos de los servidores que utilizan las aplicaciones
- el estado de cada aplicación, (en cola, ejecutándose, esperando una respuesta)
- intentos de intrusión
- uso de los protocolos
- solicitudes de impresión de datos de la subdirección.

## 3.7 Plan de contingencia

### 3.7.1 Plan de administración de accidentes

Se deberá asegurar la continuidad de la recolección de datos y su procesamiento ante cualquier contingencia que afecte al centro de procesamiento. Para ello se deberá:

- generar **procedimientos manuales** de respaldo para cada una de las actividades desarrolladas en la dependencia

- preparar, probar y mantener actualizado un **plan de contingencias**, coordinando el mismo con los procedimientos de copias de respaldo y almacenamiento externo. Dicho plan deberá ser desarrollado de forma tal que cubra las distintas áreas de riesgo

- definir y asignar claramente las **responsabilidades** de las tareas detalladas en el plan

- prever un programa de **entrenamiento** para el personal involucrado en el plan de contingencias

Deberá almacenarse una **copia del plan** de contingencias en el exterior de la dependencia, protegiéndola contra su divulgación y actualizándola permanentemente.

### 3.7.2 Backup de equipamiento

El equipamiento informático de la dependencia debe contar con **dispositivos de respaldo**, ante cualquier tipo de incidente.

Los **mecanismos de recuperación** de los dispositivos de respaldo deben ser probados periódicamente comprobando su buen funcionamiento.

El sistema informático no deberá verse afectado ante una contingencia en el centro de cómputo, por lo que el equipamiento informático debe distribuirse en **lugares físicos diferentes**, contando ambos con las medidas y condiciones de calidad y seguridad especificadas en esta política, distribuyendo de esta manera el equipamiento redundante.

### 3.7.3 Estrategias de recuperación de desastres

Debe conformarse un **grupo de desarrollo** encargado de concebir, probar e implementar el plan de contingencias. Éste debe estar a cargo del administrador del centro de cómputo, e integrado por los líderes de cada área de la organización.

Debe asignarse un **orden de importancia** a los sistemas de información y a los equipos de la red informática, de acuerdo al análisis de riesgo y al impacto que representaría para la subdirección su ausencia.

Los equipos deberán estar **señalizados** o etiquetados de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación.

Deberán definirse las funciones o **servicios críticos** de la subdirección, junto con los
recursos mínimos necesarios para su funcionamiento, asignándoles una prioridad en el plan de contingencia.

Deberán identificarse las **contingencias** que podrían ocurrir para cada nivel de servicio crítico definido.

Deberá conformarse un **plan de emergencias**, determinando los procedimientos a llevar a cabo para cada contingencia identificada, considerando los distintos escenarios posibles. Cada procedimiento deberá estar claramente definido, y tener asignado un responsable para su ejecución.

Para el desarrollo del plan de contingencias deben contemplarse las siguientes pautas:

- Deberá estar **documentado** y **testeado** antes de su puesta en práctica
- Deberá basarse en un **análisis de riesgo**, determinando que acciones merecen estar incluidas
- Deberá **abarcar** la totalidad de la subdirección
- Deberá mantenerse **actualizado** de acuerdo a nuevos puestos de trabajos y funciones.
- Deberá ser **probado** frecuentemente
- Deberá **contener** la siguiente información:

    - objetivo del plan
    - modo de ejecución
    - tiempo de duración
    - costes estimados
    - recursos necesarios

- evento a partir del cual se pondrá en marcha el plan

Debe definirse hasta cuanto tiempo se aceptará estar en **condición de emergencia**.

Debe documentarse la realización de las siguientes actividades **después de un incidente**:

- determinar la causa del daño
- evaluar la magnitud del daño que se ha producido
- que sistemas se han afectado
- qué modificaciones de emergencia se han realizado
- que equipos han quedado no operativos
- cuales se pueden recuperar y en cuanto tiempo

Cada una estas actividades deberán ser reportadas por los líderes de cada área a un miembro de la Gerencia.

Deberá asignarse el papel de **coordinador** a un empleado, que se encargará de las operaciones necesarias para que el sistema funcione correctamente después de la emergencia. Éste deberá determinar las acciones a seguir basándose en el plan de emergencias.

Deberá **retroalimentarse** el plan luego de una contingencia, ajustando las directivas en consecuencia.

Deben establecerse planes de prueba periódicos que incluyan **simulacros de siniestros** para evaluar la eficacia y eficiencia del plan.

### 3.8. Reglamento y Uso de la Red SIAE

## I. Conexión a otras redes

Se permite conexión entre todas las máquinas que queden dentro del dominio "dgae.unam.mx" y hacia redes que queden fuera de este dominio, pero **NO** se permite conexión de otros dominios hacia "dgae.unam.mx" a excepción de autorización de la SSRE.

Cuando la DGAE brinde el acceso a otras redes a través de un convenio establecido con otra entidad, el usuario de ésta se sujetará a las normas de este reglamento y las violaciones al mismo serán penalizadas de acuerdo al reglamento.

## II. De los derechos y responsabilidades de los usuarios

1. Los usuarios internos del SIAE tienen derecho a utilizar todos los recursos de la Red-SIAE con las limitantes expresadas en el apartado I.

2. Los usuarios externos tienen derecho a utilizar únicamente los recursos que se le asignen y en la cantidad que se determine para cada caso.

3. Los usuarios tienen derecho a la privacidad de información personal, con la salvedad de aquellos casos en que se detecten acciones que pongan en riesgo la seguridad tanto de la Red-SIAE como cualquier otra red.

4. El usuario del plantel tiene derecho a contar con la información de los alumnos de su plantel en el momento solicitado.

5. El usuario del plantel tiene derecho a contar con disponibilidad de recursos de la Red-SIAE para realizar sus actividades laborales.

6. Los Administradores de Servicios Escolares del plantel tienen derecho a intercambiar información referente al alumnado entre sus similares de otros planteles, siempre y cuando estos pertenezcan al dominio "dgae.unam.mx", previo conocimiento de los Secretarios de Servicio Escolares de los dos planteles.

7. Es responsabilidad del administrador local el buen funcionamiento tanto de software como del hardware que pertenece a servicios escolares del plantel.

8. Es responsabilidad del usuario asegurarse que sus archivos cuenten con las protecciones para escritura, lectura y ejecución adecuadas.

9. Es responsabilidad del usuario asegurarse que la programática (software) y medios que introduzcan en la Red-SIAE no contengan virus.

10. Los usuarios deben ser respetuosos del trabajo de los demás absteniéndose de destruir, alterar o corromper información ajena.

11. Es responsabilidad del usuario contribuir en la protección de su información, evitando dejar la consola u otra terminal mientras tenga una sesión de trabajo.

12. Es responsabilidad del usuario realizar el respaldo de su información.

13. Es responsabilidad del administrador local del plantel garantizar respaldo seguros de la información de usuarios del sistema.

14. Es responsabilidad del administrador de Servicios Escolares del plantel implementar medidas de seguridad adicional a este reglamento.

15. Es responsabilidad del administrador de Servicios Escolares del plantel hacer respaldos a cinta de la información del servidor Sybase.

16. Es responsabilidad del administrador de Servicios Escolares del plantel que si requiere recuperar algún tipo de respaldo UNIX avisar a los administradores de la SSRE para coordinar una recuperación integra.

17. Es responsabilidad del administrador de Servicios Escolares del plantel prender y apagar correctamente el equipo UNIX.

18. Es responsabilidad del administrador de Servicios Escolares del plantel avisar a la SSRE de nuevas direcciones IP que requieran entrar a la Red-SIAE y dar de baja las que ya no sean responsabilidad de Servicios Escolares.

## III. De las restricciones

Siendo limitada la cantidad de recursos informáticos con que se cuenta en la dependencia, también lo es el uso que de ellos pueden hacer los usuarios, los limites establecidos se estarán adecuando continuamente acorde a la situación de la DGAE. Al momento de la creación de este reglamento se tiene definidas las siguientes restricciones.

A. Los usuarios

1. Ninguno de los recursos deber ser usados para transmisión de información de terceros (fttp, correo electrónico, etc...) sin una autorización previa.

2. Ninguno de los recursos deben ser usados para recibir o enviar material ofensivo o no solicitado, ni realizar actos de difamación, ni publicidad.

3. No se puede hacer uso de la red para transmitir información de carácter comercial o cualquier otra forma que represente un lucro para la persona que lo origina, excepto en caso de que el DGAE se involucre en proyectos de este tipo.

4. Ningún usuario de la red está facultado para otorgar acceso a terceros quedando como responsable de esta actividad el administrador local.

5. Ninguno de los recursos de Red-SIAE deberá utilizarse con fines políticos, ni religiosos, expresa aclaraciones de que es una opinión de carácter personal y que no representa a la dependencia.

6. No se permite la transferencia de información que afecte los derechos de autor o propiedad intelectual.

7. No podrá ningún login del plantel entrar desde otro dominio que no sea de la DGAE o previo aviso por escrito al subdirector de SSRE con copia a los administradores de la misma área.

8. El login es personal y será utilizado únicamente por el usuario autorizado y no deberá ser prestado o transferido por ningún motivo.

9. No podrá ningún login del plantel entrar desde una sesión UNÍX al servidor de base de datos.

10. En ningún caso el login root podrá entra a sesión (fttp, telnet, pop3, etc...) de otra dirección IP que no sea la consola, lo mismo aplica para el super usuario.

11. Un login no deberá modificar archivos que no sean de su propiedad.

12. Ningún login incluyendo root podrá modificar archivos de login sybase.

13. Estudiantes, profesores, investigadores o personas de centros de cómputo locales NO podrán utilizar los recursos de cómputo de la DGAE, solo en el caso de que estos trabajen en la misma.

14. No esta permitido usar equipo de la Red-SIAE para atacar equipos del misma red u otras redes.

B. Espacio en disco

1. El espacio del directorio /export/home será asignado a los usuarios siendo este comunitario y es responsabilidad tanto del administrador local como de los usuarios que éste sea aprovechado adecuadamente y nunca podrá tomar más espacio de otro directorio que no sea el mencionado.

C. Estaciones y computadoras personales

1. Las máquinas PC asignadas directamente a la DGAE podrán ser utilizadas libremente por cualquier usuario de la Red-SIAE, con apego a lo impuesto en este reglamento. De registrarse una saturación continua en el uso de las mismas se establecerán horarios para su utilización, los cuales se darían a conocer con la debida anticipación por parte del plantel.

2. Está definida una prioridad en el uso de las máquinas y demás recursos de la red (siempre y cuando sea para fines de la administración escolar) de acuerdo al orden siguiente:

   - Atención al alumnado
   - Técnicos del plantel
   - Administradores de la SSRE
   - Usuarios externos
   - De requerirse el uso de una máquina y/o algún dispositivo, un usuario podrá pedirle a otro con una menor prioridad la

libertad para emplear el recurso en cuestión. Bajo condiciones especiales, tales como problemas en la comunicación, o necesidad de prestar algún tipo de mantenimiento a nodos o impresoras, etc..., el personal de la SSRE tendrá la mayor prioridad en la utilización de la infraestructura.

D. Servicios de red

1. Los usuarios podrán utilizar libremente los servicios de red (fttp, mail, telnet, talk y sus variantes), pero en caso necesario el administrador local y la SSRE estará regulando la utilización que se haga de los mismos.

2. Esta prohibido el uso de telnet a los servidores bbs desde las estaciones de trabajo de uso común.

## IV. Del equipo y paquetes

1. El Secretario Escolar del plantel queda como responsable de la integridad física de los equipos SUN y PC's aportadas por DGAE.

2. El personal técnico del plantel queda como responsable de la administración de las máquinas PC's y la administración UNIX de las máquinas SUN.

3. A partir de la fecha que entre en operación la SSRE en el plantel y el dominio para ser reconocido en el servidor de nombres de la UNAM.

4. La máquinas PC serán utilizadas para la Administración Escolar quedarán físicamente dentro de Servicios Escolares.

5. Únicamente el personal de la SSRE y los administradores locales están autorizados para mover de lugar el equipo, conectar/desconectar o inicializar nodos y periféricos, realizar modificaciones en el equipo, y otros elementos de la Red-SIAE.

6. La adquisición de paquetes de licencia se determinará en base a necesidades actuales de los distintos planteles y de acuerdo con las normas establecidas por el departamento de compras locales.

7. La instalación de paquetes y programas en los servidores DUN de la red se llevará a cabo por el personal de la SSRE y en el caso de que el administrador local requiera instalar algún paquete o software adicional será

previo aviso y autorización por escrito del subdirector de SSRE con copia a los administradores de la misma.

8. Tiene prioridad de funcionamiento el servidor de base de datos, y es responsabilidad del administrador local poner todos los recursos y medios (memoria, espacio y red) para que el servidor tenga un buen funcionamiento.

9. Todos los derechos de Autor del SIAE-Windows pertenecen a la DGAE y el plantel NO puede tener los archivos fuente ni modificar los ejecutables, y solo se les permite sacar tantas copias que considere necesarias para ser instalados en equipos de Servicios Escolares del plantel.

10. Si cualquier Módulo del SIAE-Windows es instalado en algún equipo fuera de Servicios Escolares del plantel está será considerada un elemento más de la Red-SIAE y se aplicará este reglamento.

11. Es responsabilidad del plantel tener la licencia de SYBASE actualizada a la versión que requiere el SIAE para su correcto funcionamiento y será bajo las especificaciones de la DGAE.

## V. De las sanciones

1. En caso de que se comprobara actividades delictivas de un usuario y que comprometen la seguridad de la Red-SIAE será dado de baja como login del sistema SIAE, y se avisará al Secretario de Servicios Escolares del plantel para que éste tome las medidas adecuadas.

2. La falta del cumplimiento de alguno de los artículos de este reglamento cuya sanción no este especificada en los incisos siguientes 3, 4 o 5 de este apartado conlleva, en la primera ocasión, que el usuario reciba un mensaje recordatorio sobre el mismo, en el mejor de los casos, o en los casos no previstos por el presente reglamento serán resueltos por la área de Sistemas de Registro Escolar. Si la situación lo amerita se procederá en conjunto con al menos dos personas representantes de la Dirección General de Administración Escolar (DGAE), dos personas representantes de las autoridades de plantel y si el caso lo requiere con dos representantes de la Dirección General de Computo Académico; o garantizando una representación análoga por las partes involucradas.

3. A aquel usuario que llegará a incurrir en el incumplimiento de los artículos III.1, III.2, III.11, II.13, II.19 o si reincidiera en aquellos señalados en el

artículo anterior se le hará una llamada de atención tanto a la persona que incurra en la falta como al responsable directo previo aviso verbal del Secretario de Servicios Escolares y si no existiese este a el subdirector del SSRE.

4. A aquel usuario que incurra en el incumplimiento de los artículos III.3, III.4, III.8, III.12, III.14 o reincida en las fallas señaladas en el artículo anterior se le suspenderá el login de manera definitiva en la máquina SUN y quedará como responsable el Secretario de Servicios Escolares para aplicar la sanción administrativa que considere necesaria. Si adicionalmente existiera una queja justificada de algún usuario de nuestra red o de cualquier otra de haber obrado de mala fe se pasara el caso a Tribunal Universitario para su evaluación o la autoridad correspondiente.

5. Si un usuario incurre en el incumplimiento del artículo III.7, III9, III.10 su caso será manejado acorde a las circunstancias y después de una investigación por parte de los administradores de la SSRE, se aplicará sanciones, si es necesario, por parte de la SSRE, previo aviso verbal al Secretario de Servicios Escolares del plantel.

**4. Procedimientos de seguridad**

## Introducción del Manual de Procedimientos

La Subdirección de Sistemas de Registro Escolar(SSRE), como parte de la Dirección General de Administración Escolar(DGAE), tiene como función la sistematización de los procesos de registro escolar.

Los procedimientos de seguridad de la Red SIAE se describen en el siguiente manual, con la finalidad de indicar cómo hay que llevar a cabo la protección. Estos procedimientos también constituyen los mecanismos para hacer cumplir las políticas. Además resultan útiles pues indican detalladamente qué hay que hacer cuando sucedan incidentes específicos, son referencias rápidas en caso de emergencia y ayudan a eliminar los puntos de falla críticos, además de indicar quien va a realizar cada uno de los procedimientos aquí enlistados.

"El manual no podrá ser sacado de las instalaciones de la Subdirección de Registro Escolar y sólo podrá ser utilizado, consultado y actualizado por el personal de los departamentos DASSU, DSS y de la jefatura de la subdirección"

Cabe señalar que los procedimientos que aquí se enlistan y se describen por motivos de seguridad solo son a manera de ejemplo y en consecuencia se describirán de forma muy general y sin entrar en detalles.

## Objetivo del Manual

Darle seguimiento a las políticas de seguridad de la Red SIAE estableciendo los procedimientos que nos indicarán como hacer cumplir dichas políticas.

## Índice del Manual

## 4.1. Procedimiento para instalar el Firewall

### Objetivo

Este documento tiene como objetivo principal dar las indicaciones básicas requeridas para la instalación del Firewall Tool Kit. Describiendo las políticas a seguir y expone en una secuencia ordenada las principales operaciones o pasos de que se compone el procedimiento y la manera de realizarlas, además contiene diagramas de flujo, que expresan gráficamente la trayectoria de las distintas operaciones.

### Normas de Operación

1.- Antes de realizar este procedimiento deberá asegurarse de que se cuenta con una máquina con los requerimientos mínimos que a continuación se especifican:

- CPU Intel 4 80386 como mínimo
- Como mínimo 2 MB RAM (cuanto más memoria tenga más rápido será el sistema)
- Mínimo 2 GB de disco duro

Requerimientos Sugeridos

- Procesador Pentium III a 500 Mhz
- 128 MB RAM
- 4 GB en disco duro

2.- Para hacer uso de este documento se requiere cierto conocimiento previo de UNIX, LINUX y Hardware (para bootear la máquina y realizar particiones) por lo que no está orientado a alguien que recién esté comenzando. El contenido de este manual debiera ser útil para el personal que labora en el Departamento de Administración de Servidores Sybase y UNIX (DASSU).

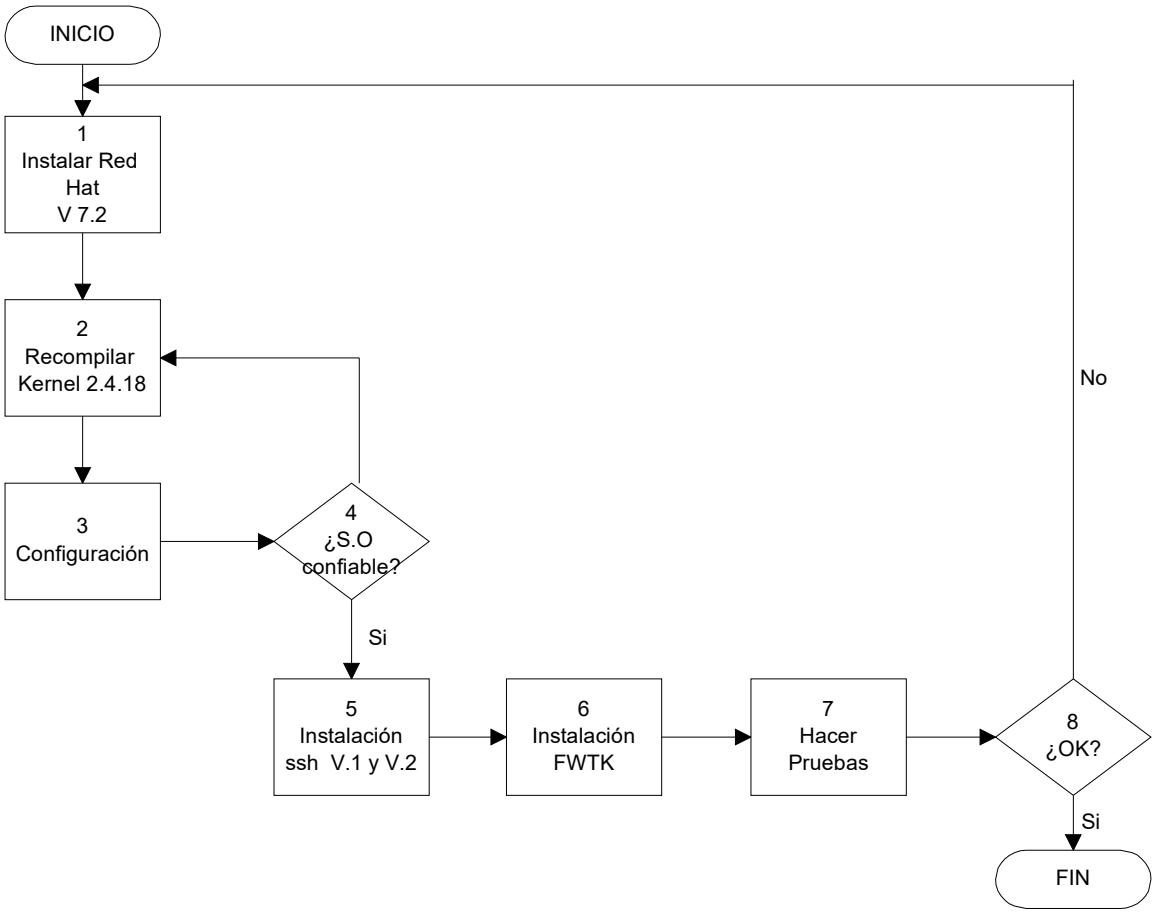
3.- Para que tenga validez y cumpla de la mejor manera con su objetivo, este Manual de Procedimientos radica en la veracidad y actualidad de su información; por lo que se requiere de revisiones periódicas para mantenerlo actualizado, cualquier cambio debe ser sugerido al Administrador de Unix, responsable de este manual, para su análisis y en su caso posterior corrección.

### Diagramas

**DEPARTAMENTO DE ADMINISTRACIÓN DE SERVIDORES SYBASE Y UNIX**

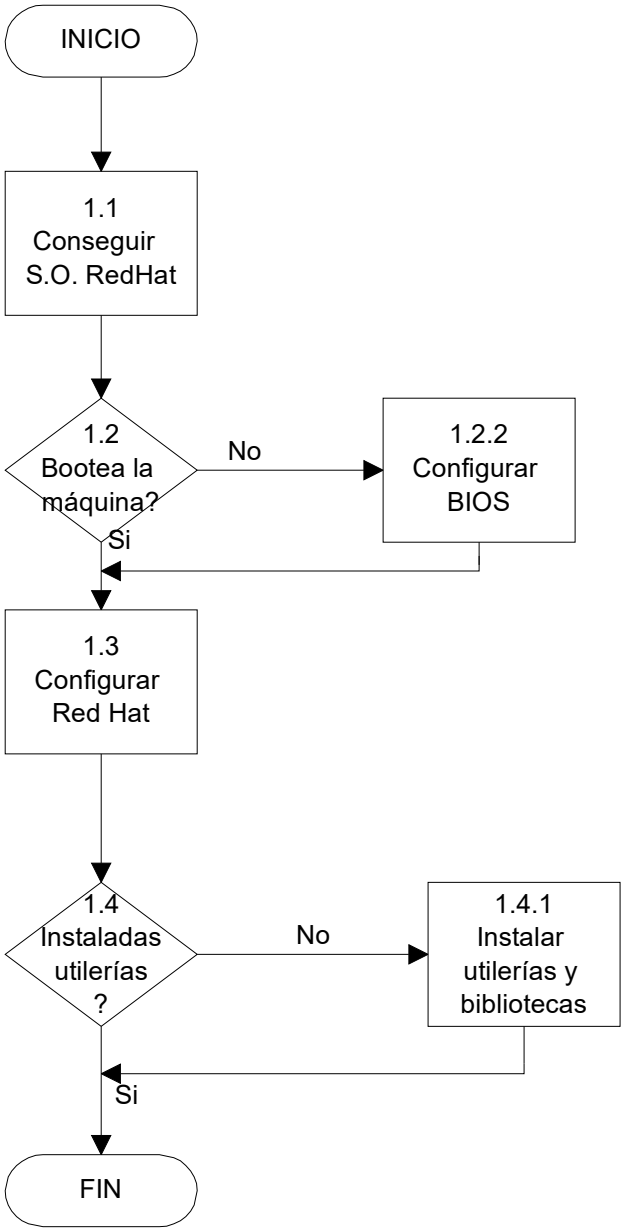
**PROCEDIMIENTO: PARA LA INSTALACIÓN DEL FIREWALL TOOL KIT.**

**DIAGRAMA GENERAL DE LA INSTALACIÓN DE FIREWALL**



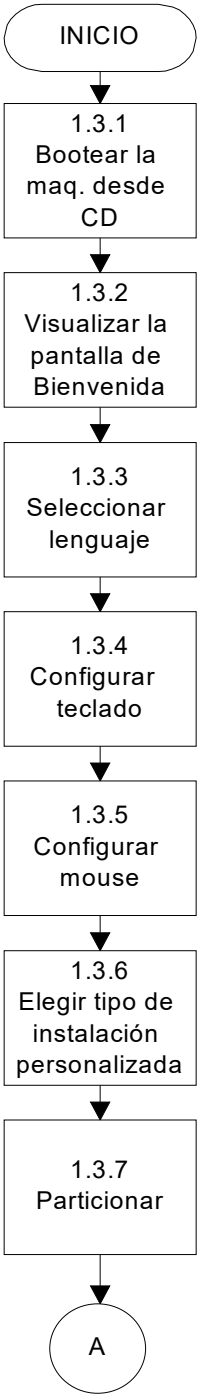
## PROCEDIMIENTO: PARA LA INSTALACIÓN DEL FIREWALL TOOL KIT.

**Diagrama del Procedimiento de Instalación de RedHat (1)**



## PROCEDIMIENTO: PARA LA INSTALACIÓN DEL FIREWALL TOOL KIT.

**Diagrama de Configuración para la Instalación de RedHat (1.3)**

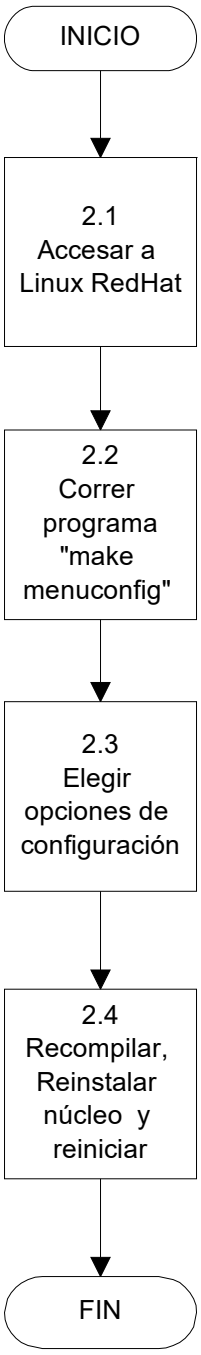


## PROCEDIMIENTO: PARA LA INSTALACIÓN DEL FIREWALL TOOL KIT.

**Diagrama de Configuración para la instalación de RedHat**
**Continuación (1.3)**

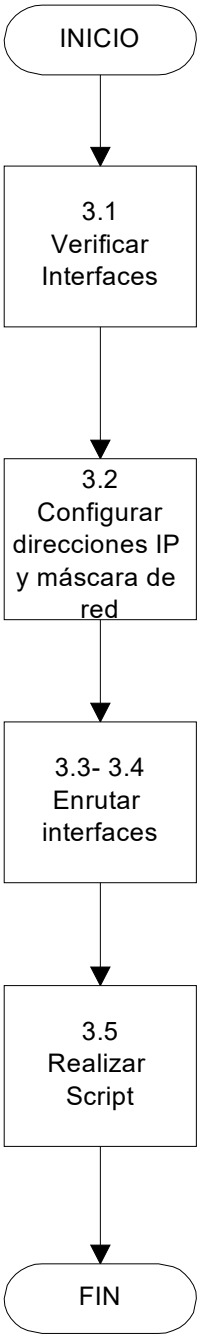

## PROCEDIMIENTO: PARA RECOMPILAR EL KERNEL

**Diagrama de Procedimiento para recompliar el KERNEL (2)**



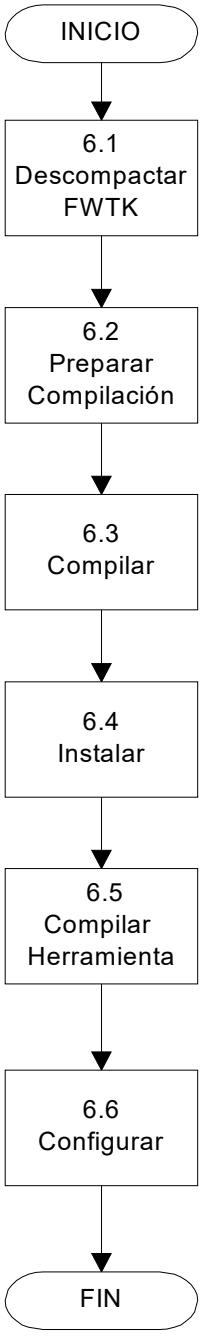

## PROCEDIMIENTO: PARA CONFIGURACIÓN

**Diagrama del Procedimiento para Configuración (3)**



## PROCEDIMIENTO: PARA INSTALACIÓN DE FWTK

**Diagrama para la Instalación de FWTK (6)**



| **PROCEDIMIENTO : PARA LA INSTALACIÓN DEL SISTEMA OPERATIVO LINUX REDHAT versión 7.2** | |
|---|---|
| **INTERVENCIÓN** | **ACTIVIDAD** |
| ADMINSITRADOR DE UNIX | 1.1 Conseguir el Sistema Operativo. Es importante que sea una versión estable. El tiempo promedio de este proceso es de doce horas. No hay que olvidar que será utilizado para la seguridad por lo que se pide que la fuente sea confiable.<br><br>1.2 Verificar que la computadora donde se instalará RedHat bootea desde la unidad de CD<br><br>1.2.1 En caso de bootear ir al paso 1.3<br>1.2.2 En caso de no bootear deberá configurarse la BIOS de la computadora para que lo haga. Se puede entrar a la BIOS <Supr> aunque a otras BIOS con <ALT>+<F1><br><br>1.3 Durante la instalación se tendrá que configurar el Hardware y se deberán realizar los siguientes pasos:<br><br>1.3.1 Para iniciar la instalación de Linux RedHat (2 discos) es necesario bootear el CD1. Aparecerá una pantalla de bienvenida en inglés. Teclear *text* para iniciar una instalación de modo texto.<br><br>1.3.2 Visualizar la pantalla de Bienvenida<br><br>1.3.3 Escoger idioma a usar en la instalación. Elegir Español (Spanish). Es recomendable escoger español ya que es el lenguaje por omisión que se utilizará en el sistema después de la instalación. Oprimir *Ok*.<br><br>1.3.4 Ahora los menús y la ayuda aparecen en Español. El programa de instalación detecta y selecciona automáticamente el teclado.<br>Seleccionar: es<br>Oprimir *Ok*<br>1.3.5 El paquete reconoce el mouse y espera la confirmación. Escoger emular tres botones. Si el ratón es de dos botones oprimir *Ok*.<br><br>1.3.6 Dentro de la pantalla de opciones de instalación existen varias opciones: |

Estación de trabajo

Servidor

Personalizada

Elegir la opción *Personalizada.*

1.3.7 Elección de una estrategia de particionamiento:

1.3.7.1 Al entrar se pide seleccionar:

Particionar de forma automática

Partición manual de Disk Druid

Partición manual con fdisk

Seleccionar *fdisk*. Para configurar el disco, elija *modificar*

1.3.7.2 Al entrar a fdisk puede teclear *m,* para ver un menú de ayuda. El menú es el siguiente:

*m* ayuda

*p* muestra contenido

*d* borra particiones (en caso de que el disco tenga información)

*w* escribir, guardar cambios

*n* hacer nueva partición

1.3.7.3 Se recomienda hacer las particiones como sigue:

/root o superusuario y Kernel

/var para arh.log

/usr para programas de FWTK y ssh

/swap para memoria virtual

aunque el mínimo de directorios que se necesitan es / y */swap*

Para discos IDE existe la limitación con respecto al número de particiones que se pueden tener en un disco duro.

La primera partición debe ser primaria para el KERNEL y es mínimo de 150 megas.

Para crear una nueva partición:

- Teclear *n*
- *p* (partición primaria)
- aparece cilindro 1 (teclee *enter*)
- aparece cilindro fin (teclee *+150 M enter*)

Se hará lo mismo para crear las cuatro particiones. El tamaño dependerá del espacio disponible en el disco duro.

Se recomienda que home tenga el mínimo posible y el directorio donde se ubicarán las bitácoras sea de tamaño razonable.

La partición para memoria virtual /swap debe ser al menos el doble de la cantidad de memoria RAM que tenga la computadora.

1.3.7.4 Revisar cuidadosamente la configuración de las particiones.

1.3.7.5 Para terminar con fdisk y grabar lo realizado, teclear *w*

1.3.7.6 Ahora el programa irá a una pantalla de configuración del disco duro donde se nombran las particiones que se crearon en el paso 1.3.6.3. Seleccionar la primera partición con las teclas de dirección y luego pulsar la opción de modificar. Aparecerá una ventana donde hay que especificar el punto de montaje y seleccionar el sistema de archivos de esta partición.

Nota: En la partición /swap no se modifica

Finalmente seleccionar *aceptar* para continuar.

1.3.7.7 Configurar LILO

1.3.7.8 Nombrar Host

1.3.8 Si el programa detecta alguna tarjeta de red se deberá configurar declarando *dirección IP, máscara, red, broadcast, nombre, host, getway o puerta de enlace y DNS.*

| | |
|---|---|
| | 1.3.9 Elegir zona horaria (México, centro), fecha normal no UTC<br><br>1.3.10 Dar el password de root o administrador del sistema (poner un password que tenga mayúsculas, minúsculas y/o números u otros signos para hacerlo difícil de romper) pulsando añadir agregar cuentas de nuevos usuarios. Dar username como UNICO y password. Pulsar *aceptar.*<br>Nota: Es importante agregar una sola cuenta ya que es una de las medidas de seguridad que se deben tomar.<br><br>1.3.11 Ahora se deberá escoger el software que desea instalar en Linux.<br>Como medida de seguridad se tiene que instalar el mínimo de software posible.<br>Para evitar aplicaciones y servicios inoperantes y/o no necesarios en el sistema que pudieran disminuir la capacidad de desempeño y almacenamiento en el mismo.<br><br>Otra medida de seguridad es no instalar modos gráficos como por ejemplo KDE, GNOME<br><br>1.3.12 Sigue la pantalla de selección y configuración de la tarjeta de video. El paquete detecta automáticamente la tarjeta y la cantidad de memoria en ella.<br><br>Habrá que esperar aproximadamente 20 minutos para que Linux termine de instalarse. Durante el proceso se pedirá que se introduzca el CD2.<br>Durante el proceso de instalación puede teclear C*trl Alt F1, Ctrl Alt F2* o bien *Ctrl Alt F3* para ver en otra pantalla que está sucediendo con la instalación o teclear comandos, para volver a la instalación normal teclee C*trl F7*<br><br>1.3.13 Antes de terminar la instalación se pedirá introducir un diskette para grabar el diskette de rescate.<br><br>1.3.14 Para la resolución de la pantalla se puede apretar la tecla |

| | |
|---|---|
| | de *Probar* la configuración, pero no es necesario que se hagan esas pruebas en este momento ya que dentro de Linux se puede cambiar dicha configuración.<br><br>1.4 Como último paso se deberá verificar que se han instalado las siguientes utilerías que serán necesarias para la instalación de FWTK y ssh.<br><br>- Kernel<br>- bin utils<br>- utilería Make<br>- net-tools<br>- netcfg<br>- net kit – base<br>- wu-ftp<br>- ipchains<br>- bibliotecas standar<br><br>1.4.1 En caso de no estar instalado usar el siguiente comando:<br>rpm –Uhv <nombre de la utilería><br><br>1.4.2 Con las utilerías antes mencionadas ya instaladas, se finalizará el proceso de instalación de RedHat. |

| | | | |
|---|---|---|---|
| ELABORÓ | FECHA<br>11 – ABRIL - 2002. | APROBÓ | FECHA<br>18 – ABRIL - 2002 |

| **PROCEDIMIENTO: PARA RECOMPILAR EL KERNEL** | |
|---|---|
| **INTERVENCIÓN** | **ACTIVIDAD** |
| ADMINSITRADOR DE UNIX | 2.1 Accesar a Linux RedHat con la clave de root<br><br>2.2 Correr el programa “make menuconfig” que se encuentra en: /usr/scr/linux<br><br>2.3 Elegir las siguientes opciones marcadas con *<br><*> Packet socket<br>[ ] Kernel/User netlink socket<br>[*] Network firewalls<br>[ ] Socket Filtering<br><*> Unix domain sockets<br>[*] TCP/IP networking<br>[ ] IP: multicasting<br>[*] IP: advanced router<br>[ ] IP: kernel level autoconfiguration<br>[*] IP: firewalling<br>[?] IP: always defragment (required for masquerading)<br>[?] IP: transparent proxy support<br>[?] IP: masquerading<br>--- Protocol – specific masquerading support will be built<br>[?] IP: ICMP masquerading<br>--- Protocol – specific masquerading support will be built<br>[ ] IP: masquerading special modules support<br>[*] IP: optimize as router not host<br>< > IP: tunneling<br>< > IP: GRE tunnels over IP<br>[?] IP: aliasing support<br>[*] IP: TCP syncookie support (not enabled per default)<br>--- (it is safe to leave these untouched) |

< > IP: Reverse ARP

[*] IP: Allow large windows (not recommended if <16Mb of

< > The IPv6 protocol (EXPERIMENTAL)

---

< > The IPX protocol

< > Appletalk DDP

< > CCITT X.25 Packet Layer (EXPERIMENTAL)

< > LAPB Data Link Driver (EXPERIMENTAL)

[ ] Bridging (EXPERIMENTAL)

[ ] 802.2 LLC (EXPERIMENTAL)

< > Acorn Econet/AUN protocols (EXPERIMENTAL)

< > WAN router

[ ] Fast switching (read help!)

[ ] Forwarding between high speed interfaces

[ ] PU is too slow to handle full bandwidth

QoS and/or fair queueing --->

2.4 Deberá recompilar, reinstalar el núcleo y reiniciar. Para ello se deberá teclear la siguiente orden:

make dep;make clean;make bzlilo;make modules;make modules_install; init6

para llevarlo a cabo en un solo paso.

| ELABORÓ | FECHA<br>11 – ABRIL - 2002 | APROBÓ | FECHA<br>18 – ABRIL - 2002 |
|---|---|---|---|

| **PROCEDIMIENTO: CONFIGURACIÓN** | |
|---|---|
| **INTERVENCIÓN** | **ACTIVIDAD** |
| ADMINSITRADOR DE UNIX | 3.1 Verificar estado de interfaces con el siguiente comando: dmesg \| grep eth<br><br>Si el o los módulos están insertados (es decir, las tarjetas de red levantadas), tendremos algo parecido al siguiente resultado:<br>*3c59x.c:v0.99H 27May00 Donald Becker http://cesdis.gsfc.nasa.gov/linux/drivers/vortex.html*<br>*eth0: 3Com 3c905B Cyclone 100baseTx at 0x9400, 00:50:da:0d:0e:d5,*<br>*IRQ 11*<br>*8K byte-wide RAM 5:3 Rx:Tx split, autoselect/Autonegotiate interface.*<br>*MII transceiver found at address 24, status 786d.*<br>*MII transceiver found at address 0, status 786d.*<br>*Enabling bus-master transmits and whole-frame receives.*<br><br>3.2 Con las tarjetas levantadas, habrá que configurar su dirección IP y máscara de red, a manera de ejemplo supondremos la dirección IP 132.248.78.36 por lo que sería de la siguiente manera:<br><br>/sbin/ifconfig eth0 132.248.78.36 netmask 255.255.255.0 broadcast 132.248.78.255 up<br><br>/sbin/ifconfig eth1 132.248.78.36 netmask 255.255.255.0 broadcast 132.248.78.255 up<br><br>3.3 El enrutamiento es donde indicamos cuales paquetes deben ser direccionados por cual tarjeta de red, para ello tecleamos el siguiente comando sin parámetros:<br><br>$ /sbin/route |

La tabla de enrutamiento (la cual es estática) es la siguiente:

Kernel IP routing table

| Destination | Gateway | Genmask | Flags | Metric | Ref | Use | Iface |
|---|---|---|---|---|---|---|---|
| 132.248.78.60 | * | 255.255.255.255 | UH | 0 | 0 | 0 | eth1 |
| 132.248.78.40 | * | 255.255.255.255 | UH | 0 | 0 | 0 | eth0 |
| 132.248.78.254 | * | 255.255.255.255 | UH | 0 | 0 | 0 | eth0 |
| 132.248.78.58 | * | 255.255.255.255 | UH | 0 | 0 | 0 | eth0 |
| 132.248.78.0 | * | 255.255.255.0 | U | 0 | 0 | 0 | eth1 |
| 127.0.0.0 | * | 255.0.0.0 | U | 0 | 0 | 0 | lo |
| default | 132.248.78.254 | 0.0.0.0 | UG | 1 | 0 | 0 | eth0 |

Lo que esta tabla nos indica, es por medio de que interfaz de red será por la que alcanzaremos determinados destinos; ya sean hosts o redes completas.

La forma "manual" de enrutar las interfaces, es con los siguientes comandos, ejecutados como usuario root:

$ route add 132.248.78.36 eth1

$ route add 132.248.78.100 eth0

$ route add 132.248.78.254 eth0

$ route add 132.248.78.43 eth0

$ route add -net 132.248.78.0 netmask 255.255.255.0 eth1

$ route add -net 127.0.0.0 netmask 255.0.0.0 lo

$ route add default gw 132.248.78.254 eth0

3.4 Para automatizar el enrutamiento de estas interfaces, incluso tiempo de booteo, hay que modificar los siguientes archivos:

/etc/sysconfig/network-scripts/ifcfg-eth0

cuyo contenido debe quedar así:

DEVICE=eth0

BOOTPROTO=static
IPADDR=132.248.78.36
NETMASK=255.255.255.0
GATEWAY=132.248.78.254
ONBOOT=yes

/etc/sysconfig/network-scripts/ifcfg-eth1

DEVICE=eth1
BOOTPROTO=static
IPADDR=132.248.78.36
NETMASK=255.255.255.0
ONBOOT=yes

3.5 Por último realizar un script en /etc/rc.d/init.d/network2

route del 132.248.78.36 eth0
route del -net 132.248.78.0 netmask 255.255.255.0 eth0
route del default eth0
route add 132.248.78.254 eth0

ipchains -P forward DENY
ipchains -A forward -s 132.248.78.0/24 -j MASQ

Para ver de forma esquemática esta configuración ir al
ANEXO 1

| ELABORÓ | FECHA<br>11 – ABRIL - 2002 | APROBÓ | FECHA<br>18 - ABRIL - 2002 |
|---|---|---|---|

**PROCEDIMIENTO: PARA LA VERIFICACIÓN DE LA CONFIABILIDAD DEL SISTEMA OPERATIVO**

| INTERVENCIÓN | ACTIVIDAD |
|---|---|
| ADMINSITRADOR DE UNIX | 4.1 En xinetd vienen abiertos varios servicios como chargen, echo, telnet, ftp, rsh, rexec, rwho, talk, finger, ident.<br><br>Éstos además de ser innecesarios, pueden ser muy peligrosos. Varios de estos demonios también han presentado casos de buffer overflows<br><br>Hacer un netstat para ver los servicios disponibles<br>netstat -atu\|grep '*:*' \|more<br><br>La columna LocalAdress nos dice el nombre del servicio, o en otro caso aparecerá el número de puerto en el que el servidor se encuentra a la escucha. |

| Servicio/Puerto/Protocolo | Descripción | ¿Mantener? |
|---|---|---|
| /pd/515/tcp | Servicio de impresión | No |
| syslogd/514/udp | Syslog | Si |
| nfsd/2049/udp | NFS | No |
| smbd/137-138-139-tcp-udp | Samba | No |
| sendmail/25/tcp | Correo SMTP | No |
| http-innd-named/80-119-53 | Web,news,DNS | No |
| echo/7/tcp-udp | Todo lo que se envía a este puerto lo devuelve | No |
| daytime/13/tcp-udp | Devuelve la hora y la fecha del sistema | No |
| ftp/21/tcp | Servidor FTP | Quizás/restringir |
| telnet/23/tcp | Permite conectarnos y abrir una consola remotamente | Sí/restringir |
| finger/79/tcp | Devuelve información sobre los usuarios del sistema | No |
| linuxconf/98/tcp | Sistema de configuración remota | No |
| pop2/109/tcp | Servidor de correo Pop versión 2 | No |
| pop3/110/tcp | Servidor de correo Pop versión 3 | No |
| auth(ident)/113/tcp | Identifica y registra a los usuarios que hacen | Sí |

| | | | |
|---|---|---|---|
| | uso de servicios tcp | | |
| imap2/143/tcp | | | |
| login/513/tcp | | | |
| | Servidor de correo Imap versión 2 | | No |
| shell/514/tcp | Permite logins remotos (rlogin) a usuarios autorizados | | No |
| uucp/540/tcp | Permite Shells remotos (rshell) a usuarios autorizados | | No |
| x-windows/600 | Antiguo protocolo de comunicación de Unix | | No |
| | Acepta conexiones de servidores autorizados | | Sí/restringir |

Otros servicios que no deben instalarse:

| | | | |
|---|---|---|---|
| bootparamd | snmpd | cgd | rstatd |
| dhcpd | squid | mountd | timed |
| gated | xntpd | named | xntpd |
| routed | ypbind | nfsiod | netstat |
| rusersd | yppasswdd | pcnfsd | systat |
| rwalld | ypserv | portmap | bootp |
| rwhod | | printer | |

4.2.1 Eliminar los servicios entrando con la clave de root

4.2.2 Buscar todos los archivos de nombre

/etc/rc.d/rc*.d/s* xxx

donde xxx es:

| | |
|---|---|
| nfsfs, nfs | NFS |
| smb | Samba |
| httpd | Web |
| innd | News |
| sendmail | SMTP |
| named | DNS |

4.2.3 Renombrar cada uno de los archivos anteriores, poniendo una K mayúscula (“K”) en lugar de la S, por ejemplo:

mv /etc/rc.d/rc3.d/s50nfs /etc/rc.d/rc3.d/K50nfs

4.2.4 Los cambios tendrán efecto a partir del siguiente rebooteo de la máquina. Si se quiere pararlo de forma inmediata, se puede teclear:

/etc/rc.d/init.d/xxx stop

donde xxx es el nombre del servicio

4.3 Seguridad de las cuentas

4.3.1 No olvidar eliminar las cuentas que ya no se vayan a usar. Recuerde que sólo se debe tener al usuario UNICO.

4.3.2 El archivo /etc/securetty establece la lista de las terminales desde las cuales el root puede hacer login.

| | | | |
|---|---|---|---|
| ELABORÓ | FECHA<br>17 – MAYO – 2002 | APROBÓ | FECHA<br>4 – JULIO - 2002 |

| **PROCEDIMIENTO: PARA LA INSTALACIÓN DEL SECURE SHELL CLIENTE/SERVIDOR** | |
|---|---|
| **INTERVENCIÓN** | **ACTIVIDAD** |
| ADMINSITRADOR DE UNIX | 5.1 Instalar SSH1. Después de obtener el programa de Secure Shell se descompacta en el directorio /usr/src<br>gunzip ssh-x.x.x.tar.gz<br>tar –xvf ssh-x.x.x.tar<br><br>Donde x.x.x es la versión.<br>La última versión es : ssh1: 1.2.31 y ssh2:2.4.0<br><br>5.2 En este punto obtendremos un directorio ssh-x.x.x. Desde aquí se ejecuta el script de configuración:<br><br>CC=gcc./configure --with-etcdir=/etc/ssh1<br><br>Esto genera los cambios necesarios en los archivos de código fuente para su correcta compilación.<br><br>5.3 Compilar los binarios de secure shell. Para ello basta con ejecutar<br><br>make<br><br>5.4 Instalación de Secure Shell. Para poder ejecutar la instalación es necesario estar dentro de la cuenta de root. Teclear:<br><br>make install<br><br>Los archivos de configuración de secure shell ( ssh_host_key y sshd-config) quedan localizados en el directorio "/etc" los programas clientes (ssh y scp) quedan en /usr/local/bin.<br>Finalmente el programa servidor o demonio de secure shell (sshd) queda localizado en /usr/local/sbin<br><br>5.5 Instalar SSH2. Las operaciones necesarias son las mismas que |

| | |
|---|---|
| | las requeridas para SSH1. Por lo que se repetirán los pasos 5.2 al 5.4<br><br>5.6 Ahora se configurará para que haya compatibilidad entre SSH1-SSH2<br>En el archivo:<br>/etc/ssh2/ssh2_config<br>Agregar las siguientes líneas:<br><br>Ssh1Compatibility yes<br>Ssh1Path /usr/local/bin/ssh1<br>AllowHosts 132.248.78.*<br><br>5.7 En el archivo:<br>/etc/ssh2/sshd2_config<br><br>Agregar las siguientes líneas:<br><br>Ssh1Compatibility yes<br>Ssh1Path /usr/local/sbin/sshd1<br>AllowHosts 132.248.78.*<br><br>Nota: En el archivo de configuración de ssh1 los nombres de los hosts están separados por espacios solamente. En el de ssh2, debe haber comas entre cada nombre.<br><br>5.8 Hacer un Script en /etc/rc.d/init.d/sshd2<br>---<br>#!/bin/sh<br>#<br># chkconfig: 345 55 45<br># description: sshd (secure shell daemon) is a server part of the ssh suite.<br># Ssh can be used for remote login, remote file copying, TCP port |

```
#       forwarding etc. Ssh offers strong encryption and
authentication.
#


# Source function library.
. /etc/rc.d/init.d/functions


# See how we were called.
case "$1" in
  start)
        echo -n "Starting sshd: "
        if test -r /var/run/sshd2_22.pid  && kill -0 `cat
/var/run/sshd2_22.pid`
        then echo "already running according to
/var/run/sshd2_22.pid. Not started."
        else /usr/local/sbin/sshd2
                echo "sshd2"
        fi
        touch /var/lock/subsys/sshd
        ;;
  stop)
        echo -n "Stopping sshd: "
        [ -f /var/run/sshd2_22.pid ] || exit 0
        kill -TERM `cat /var/run/sshd2_22.pid`
        rm -f /var/run/sshd2_22.pid
        rm -f /var/lock/subsys/sshd
        echo "sshd2"
        ;;
  restart)
        $0 stop
        $0 start
        ;;
  status)
```

```
        status sshd2
        ;;
  *)
        echo "Usage: $0 {start|stop|restart|status}"
        exit 1
esac

exit 0
```

---

5.9 Hacer una liga en:

etc/rc.d/rc3d

que apunte a

/etc/rc.d/init.d/sshd2

para que este servidor se levante al iniciar la máquina. Por lo que la liga se llamará:

ln –s ../init.d/sshd2 S55sshd2

| ELABORÓ | FECHA<br>17 – MAYO – 2002 | APROBÓ | FECHA<br>4 – JULIO - 2002 |
|---|---|---|---|

| **PROCEDIMIENTO: PARA LA INSTALACIÓN DEL FWTK** | |
|---|---|
| **INTERVENCIÓN** | **ACTIVIDAD** |
| ADMINSITRADOR DE UNIX | 6.1 Destarear - descomprimir el fwtk-2.1<br>tar xzvf fwtk-2.1.tar.gz -c /usr/src<br><br>6.2 Preparar la compilación<br><br>6.2.1 Editar el archivo Makefile<br>DIRS= smap smapd net acl plug –gw ftp-gw<br>tn-gw http –gw x-gw<br><br>6.2.2 Renombrar el archivo Makefile.config.linux como Makefile.config y editarlo:<br><br>#Your C compiler (eg, “cc” or “gcc”)<br>CC = gcc<br>#Destination directory for installation of binaries<br>DEST = /usr/fw/bin<br><br>Las siguientes líneas fueron cambiadas para construir binarios estáticos. Por lo que se tendrán que descomentar las siguientes dos líneas<br><br>LDFL = -g -static<br>XLDFL= -g<br>#Location of the fwtk sources [for #include by any external tools needing it]<br>FWTKSRCDIR=/usr/src/fwtk<br><br>Para constriur el binario de gateway para el servidor X, será necesario que las siguientes líneas sean modificadas: |

| | |
|---|---|
| | #Location of X libraries for x-gw<br><br>XLIBDIR =/usr/x11/lib<br>#Xlibraries<br>XLIBS = -L$(XLIBDIR) -\|Xaw -\|Xmu -\|Xt -\|Xext -\|X11 -\|c<br><br>#Location of x include files<br>XINCLUDE = /usr/X11/include |
| | 6.2.3 Editar el archivo firewall.h<br>Con define se especificará la localización de la tabla de permisos del FWTK<br><br>#ifndef PERMFILE<br>#define PERMFILE "/usr/fw/tablas/netperm-table" |
| | 6.2.4 También hay que cambiar el log facility que es el nivel de lo que reportará el FWTK en sus archivos logs. Se cambiará a nivel 6 el cual hace un loggeo mas detallado<br><br>#ifndef LFAC<br>#define LFAC LOG_LOCAL6<br>#endif |
| | 6.2.5 Aplicar el siguiente parche al proxy de http<br>Simplemente hay que insertar este pedazo de código en la línea 1362 del archivo /http/http.c<br><br>}else<br>break;<br>}<br>/*check if there is a CRLF left in the buffer<br>*Netscape send CRLF on the end of POST<br>*TRG – 19990817 |

```
*/
    char  str[2];
    int count;
    if (ioctl (rfd, FIONREAD,&count)==0){
        if (count ==2) {
        if (recv(rfd,str,2,MSG_PEEK)==2){
            if((str[0] =='\r')&&(str[1]=='\n'))
             read (rdf,str,2);
                                }
                            }
                        }
                    }
                }
                    return 0;
            }
```

6.3 Ejecutar make en el directorio /usr/src/fwtk
make

6.4 Para instalar:
Make install

6.5 Compilar portscan con el comando make que se encuentra en el directorio admin/tools/portscan

6.6 El archivo de configuración se encuentra en:

/usr/fw/tablas/netperm-table

el cual debe tener las siguientes líneas:

| | | |
|---|---|---|
| http–gw:userid | unico | #Lista de usuarios a quienes se les otorga el permiso de usar el servicio http-gw |
| http–gw:permit-host | 132.248.78.* | #Direcciones IP que tienen permiso de usar el servicio http-gw |
| http–gw:deny-hosts | * | #Lista de hosts a quienes se les niega el uso del servicio http |
| | | |
| ftp-gw:userid | unico | |
| ftp-gw:denial-msg | /usr/fw/tablas/ftp-deny | #En esta línea se especifica el archivo que contiene el mensaje de negación del servidor ftp |
| ftp-gw:welcome-msg | /usr/fw/tablas/ftp-welcome | |
| ftp-gw:permit-hosts | 132.248.78.* | |
| ftp-gw:deny-hosts | * | |
| | | |
| tn-gw:userid | unico | |
| tn-gw:help-msg | /usr/fw/tablas/tn-help | |
| tn-gw:permit-host | 132.248.78.* | |
| tn-gw:deny-host | * | |
| | | |
| plug-gw:port 9120 132.248.78.* -plug to 132.248.103.70 –port21 | | #Permite una conexión ssh del segmento de red 132.248.78 al host 132.248.103.70 por el puerto 21 |

6.7 Hacer el siguiente script en el directorio /etc/rc.d/initd
Para que se levanten los demonios en el momento de arranque

**<plugs-bases>**

```
#!/bin/bash
# Este script arranca los plugs para servicios de consultas
# a la base de datos en la intranet dgae.unam.mx
#
# Ultima modificacion  13 Abril 2000
#
#

echo -n "Arrancando Enlaces con los servidores de base de datos "
/usr/fw/bin/plug-gw -daemon 8100
echo -n "8100 alta "
/usr/fw/bin/plug-gw -daemon 8101
echo -n "8101 alta"
```

**<plugs-webserver>**

```
#!/bin/bash
# Este script arranca los plugs para servicios de consultas
# a la base de datos en la intranet dgae.unam.mx
#
# Ultima modificación  14 Abril 1999
#
# Serchkat!

case "$1" in
```

```
start)
echo -n "Arrancando Enlaces con el servidor WEB:"
/usr/fw/bin/plug-gw -daemon AL-WWW
echo -n "AL, "
/usr/fw/bin/plug-gw -daemon ALD-WWW
echo -n "AL-WWWD"
/usr/fw/bin/plug-gw -daemon BUZON-WWW
echo -n "BUZON, "
/usr/fw/bin/plug-gw -daemon TRAMI-WWW
echo -n "TRAMI"
/usr/fw/bin/plug-gw -daemon TRAMICOR-WWW
echo -n "TRAMICOR, "
/usr/fw/bin/plug-gw -daemon DIAG-WWW
echo -n "DIAGNOSTICO, "
#/usr/fw/bin/plug-gw -daemon EST-WWW
#echo -n "EST, "
/usr/fw/bin/plug-gw -daemon GRAL-WWW
echo -n "GRAL, "
/usr/fw/bin/plug-gw -daemon HIST-WWW
echo -n "HIST, "
/usr/fw/bin/plug-gw -daemon TIT-WWW
echo -n "TIT, "
/usr/fw/bin/plug-gw -daemon OFERPI-WWW
echo -n "OFERPI, "
/usr/fw/bin/plug-gw -daemon PI-2KD-WWW
echo -n "PI-2KD-WWW"
#/usr/fw/bin/plug-gw -daemon PI2K-WWW
#echo -n "PI2K, "
/usr/fw/bin/plug-gw -daemon PI2K1-WWW
echo -n "PI2K1"
/usr/fw/bin/plug-gw -daemon PI2K-D-WWW
echo -n "PI2K-D"
#/usr/fw/bin/plug-gw -daemon PI-WWW
```

```
#echo -n "PI, "
/usr/fw/bin/plug-gw -daemon TITD-WWW
echo -n "TITD, "
#/usr/fw/bin/plug-gw -daemon REGASPI-WWW
#echo -n "REGASPI, "
#/usr/fw/bin/plug-gw -daemon MASPI-WWW
#echo -n "MASPI, "
#/usr/fw/bin/plug-gw -daemon REGISTRO-WWW
#echo -n "REGISTRO, "
#/usr/fw/bin/plug-gw -daemon TIT-WWW (Nota: Ya existe otro TIT-WWW)
#echo -n "TIT, "
/usr/fw/bin/plug-gw -daemon TITCOR-WWW
echo    "TITCOR"
# Plug agregado 13 Abril 2000. Pruebas CGI:
/usr/fw/bin/plug-gw -daemon 5575
echo -n "PTO 5575 de pruebas"


echo -n "Arrancando Enlaces SSH con el servidor WEB: "
/usr/fw/bin/plug-gw -daemon ssh-web-gw
echo "ssh-web-gw"
/usr/fw/bin/plug-gw -daemon ssh-web-gw2
echo -n "Subiendo ssh para el LOCAL :"
/usr/fw/bin/plug-gw -daemon ssh-local
echo -n "circ"
/usr/fw/bin/plug-gw -daemon circ
# Puertos de prueba de Carolina :
/usr/fw/bin/plug-gw -daemon UNO-WWW
echo -n "UNO-WWW"
# Puerto de Carolina de circe a leibniz :
/usr/fw/bin/plug-gw -daemon DOS-WWW
echo -n "DOS-WWW"
    ;;
```

```
    status)
ps xfe | grep WWW | grep -v grep > /tmp/web

 if [ -s /tmp/web ];then
  echo "Enlaces con el servidor WEB funcionando!"
 else
  echo "Enlaces con el servidor WEB apagados!"
 fi
    ;;

    stop)
echo -n "Cerrando Enlaces con el servidor WEB: "
for i in `ps xfe | grep WWW | grep -v grep |awk '{print $1}'
`;do kill -9 $i; done
echo "Apagados!"
echo -n "Cerrando enlaces SSH con el servidor WEB: "
for i in `ps xfe | grep -v grep | grep 'ssh-web' | awk '{print $1}'`;
do kill -9 $i;done
echo "Apagados!"
    ;;

    *)
echo "Utiliza: $0 {start|status|stop}"
    exit 1

esac

exit 0
```

**<proxies>**

```
#!/bin/bash
```

```
#
# Script de arranque para demonios Proxy, IPXd y SMAPd
#
# Descripcion :  Arranca ipxd y habilita las interfases de red con direcciones IPX.
#          Arranca los proxys para http telnet y ftp como demonios.
#
# nombre de procesos : ipxd
#
# Ultima modificacion TUE May 16th, 2K
#
# gmendoza@galois.dgae.unam.mx


case "$1" in
     start)


# == == == == == = PROXYS == == == == == == == == =
echo -n 'Starting proxy http-gw: '
/usr/fw/bin/http-gw -daemon http-gw
echo "http-gw"
echo -n 'Starting proxy ftp-gw: '
/usr/fw/bin/ftp-gw -daemon ftp
echo "ftp-gw"
echo -n 'Starting proxy tn-gw:'
/usr/fw/bin/tn-gw -daemon telnet
echo "tn-gw"


# == == == == == == = IPX == == == == == == == == == =
# Ultima modificacion 29 mayo 2000
# Ultima modificacion 18 Julio 2000
echo -n "Starting IPX-router: "
/usr/sbin/ipxd
```

```
echo "ipxd"
echo -n "Configuring IPX Interfaces: "
/sbin/ipx_interface add -p eth1 802.3 781
/sbin/ipx_interface add  eth0 802.3 780
echo "eth0 eth1"
echo " levantado ipx"
     ;;

    status)
 cp /dev/null /tmp/proxys
  ps x | grep http-gw | grep -v grep | cut -d'?' -f1 >> /tmp/proxys
  ps x | grep   tn-gw | grep -v grep | cut -d'?' -f1 >> /tmp/proxys
  ps x | grep  ftp-gw | grep -v grep | cut -d'?' -f1 >> /tmp/proxys

 if [ -s /tmp/proxys ];then
  echo "Proxies http-gw ftp-gw tn-gw up!"
 else
  echo "Proxies http-gw ftp-gw tn-gw down!"
 fi
       ;;

    stop)
echo -n "Closing proxy services: "
 cp /dev/null /tmp/proxys
  ps x | grep http-gw | grep -v grep | cut -d'?' -f1 >> /tmp/proxys
  ps x | grep   tn-gw | grep -v grep | cut -d'?' -f1 >> /tmp/proxys
  ps x | grep  ftp-gw | grep -v grep | cut -d'?' -f1 >> /tmp/proxys

 for i in `cat /tmp/proxys`;
  do
   kill -9 $i;
  done
 killall ipxd
```

| | | | |
|---|---|---|---|
| | echo "http-gw ftp-gw tn-gw ipxd"<br>;;<br><br>*)<br>echo "Usage: $0 {start\|status\|stop}"<br>exit 1<br>esac<br><br>exit 0<br><br>6.8 Hacer las siguientes ligas en etc/rc.d/rc3.d<br><br>ln-s ../init.d/network2 s15network2<br>ln-s ../init.d/proxies s35proxies<br>ln-s ../init.d/plugs-webserver s35plugs-webserver<br>ln-s ../init.d/plugs-bases s35plugs-bases | | |
| ELABORÓ | FECHA<br>17 – MAYO - 2002 | APROBÓ | FECHA<br>4 – JULIO - 2002 |

| **PROCEDIMIENTO: PARA REALIZAR PRUEBAS** | | | |
|---|---|---|---|
| **INTERVENCIÓN** | **ACTIVIDAD** | | |
| ADMINSITRADOR DE UNIX | 7.1 Estar seguro de haber inhabilitado el envío Ip<br><br>Inhabilitar el envío IP requiere que se configure un Kernel nuevo<br><br>- Este punto se refiere a hacer varios tipos de pruebas para verificar que el firewall está funcionando correctamente.<br>- Hacer conexiones ssh, ftp, tn y http a diferentes direcciones y viceversa desde dentro de la red protegida. | | |
| ELABORÓ | FECHA<br>17 – MAYO - 2002 | APROBÓ | FECHA<br>4– JUNIO - 2002 |

### 4.2. Procedimiento para instalar herramientas de seguridad al S.O. Solaris

## Objetivo

Para mantener el sistema seguro se debe de utilizar herramientas de seguridad con el objetivo de ayudar al administrador ya sea alertándolo o realizando por sí mismo las acciones necesarias.

## Normas de Operación

1.- La instalación de las herramientas la debe hacer una persona designada por el administrador.

2.- Se deben instalar en el momento que se instala el S.O.

3.- Las herramientas a instalar son:

- OpenSSH
- TCPWrappers
- PortSentry

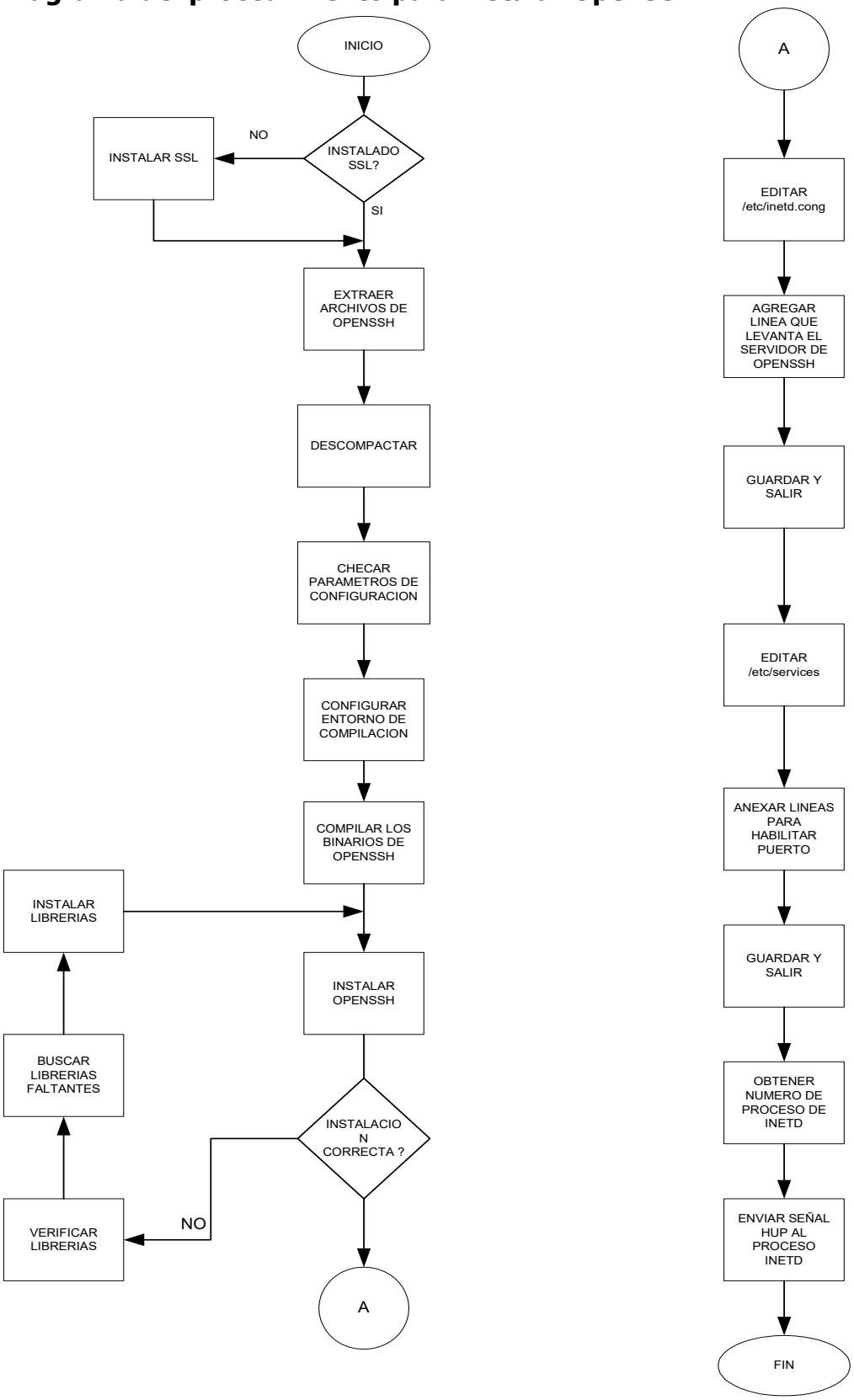
4.- En el procedimiento de instalación de cada una de ellas se divide en:

- Descompactar
- Instalar
- Configurar

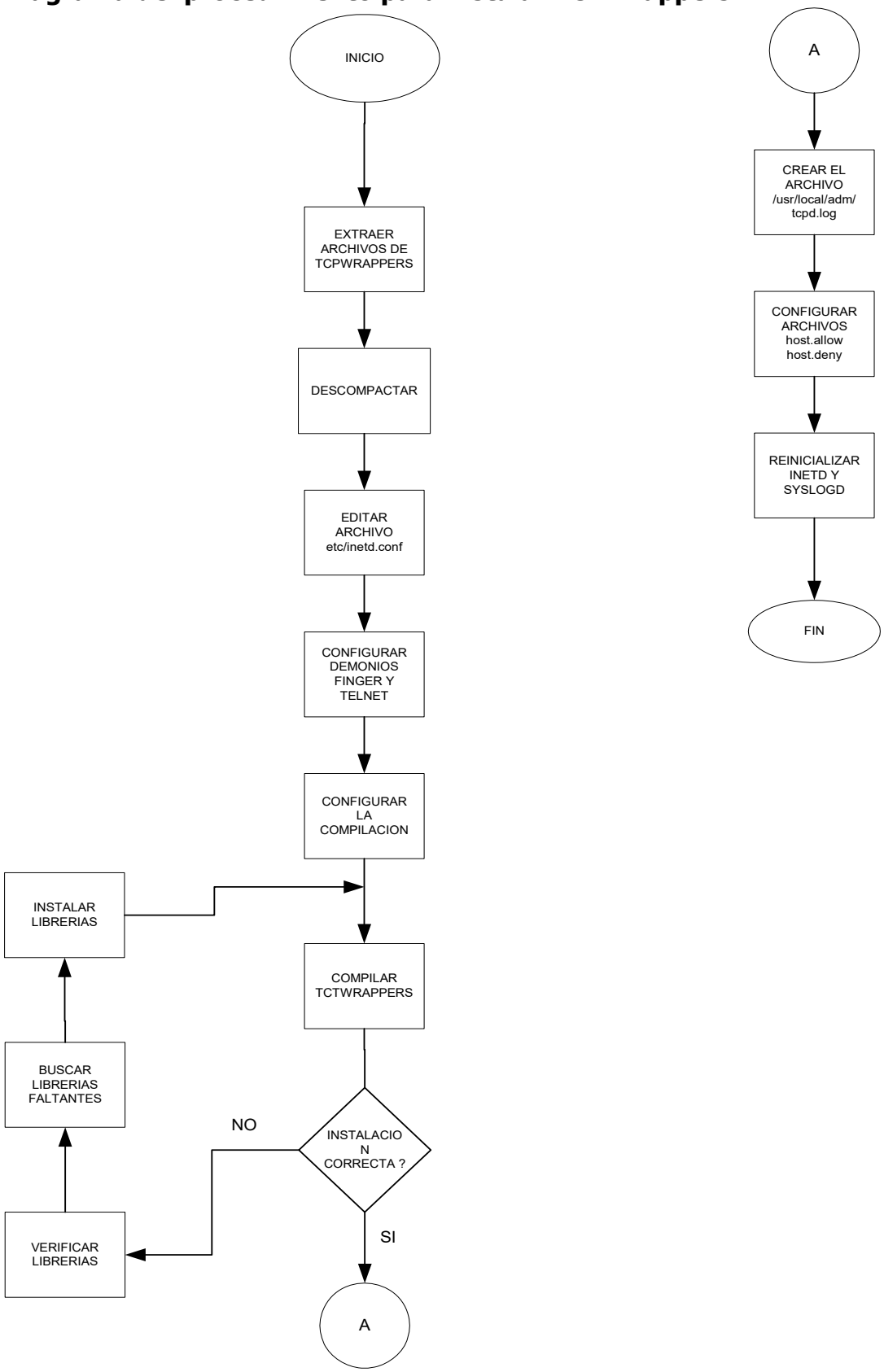
5.- Cada que salga una nueva versión o algún parche se debe actualizar cada una de las herramientas antes mencionadas.

6.- Los archivos de log generados por cada una de las herramientas instaladas se debe de analizar por lo menos una vez a la semana o antes si se presenta alguna contingencia.

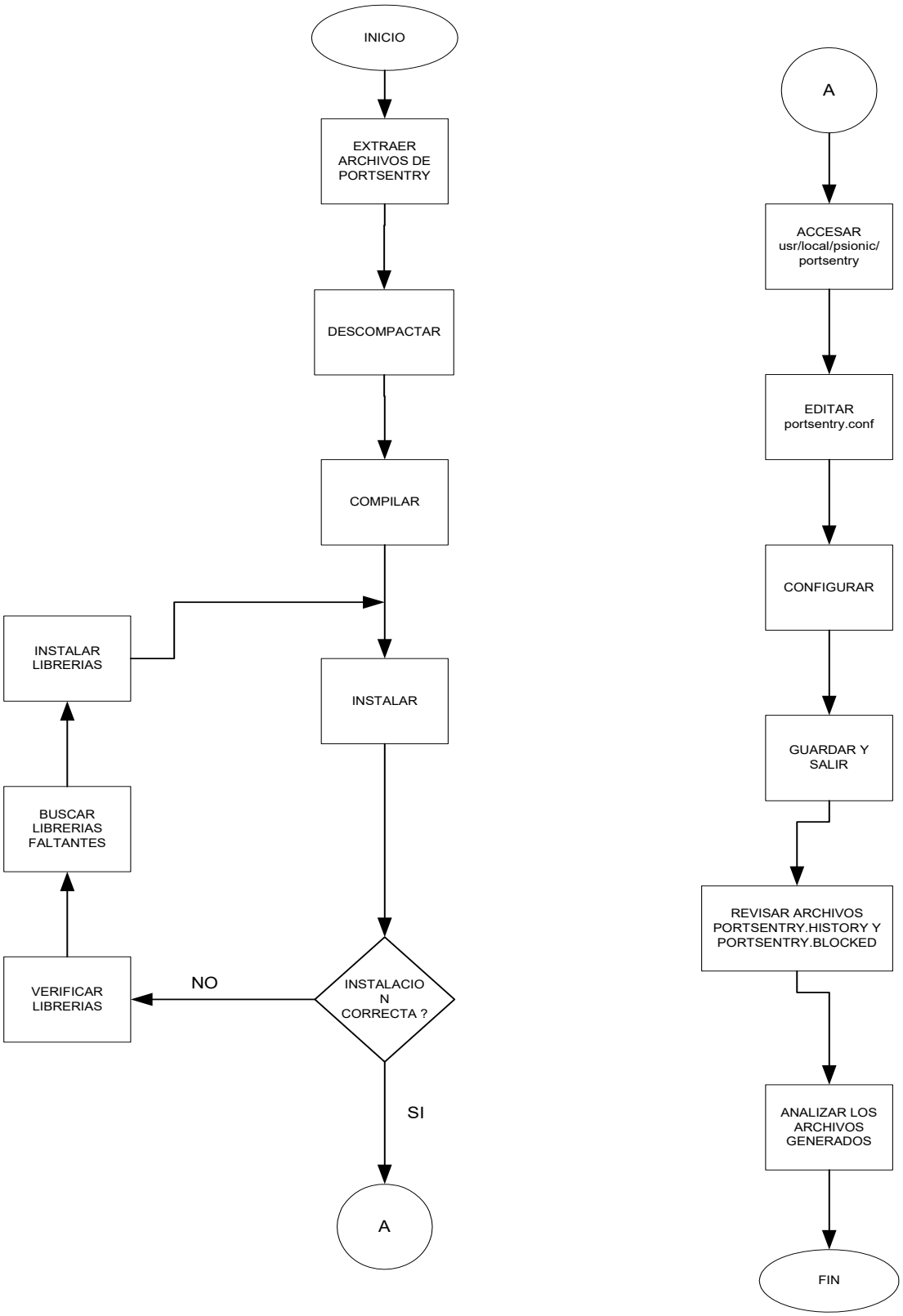
## Diagrama del procedimiento para instalar OpenSSH



## Diagrama del procedimiento para instalar TCPWrappers



## Diagrama del procedimiento para instalar PortSentry



## 4.3 Procedimiento de manejo de respaldo de B.D.

### Objetivo

Respaldar la B.D. para que en caso de que se presente alguna contingencia, el sistema en el menor tiempo posible vuelva a estar disponible e integro.

### Normas de Operación

1.- EL respaldo de la B.D. solo lo puede hacer el administrador de dicha B.D. o persona designada por dicho administrador bajo la autorización de la Subdirección.

2.- El manejo de respaldo de B.D. se divide en dos partes:

- Respaldo y recuperación de logs.
- Respaldo y recuperación de datos.

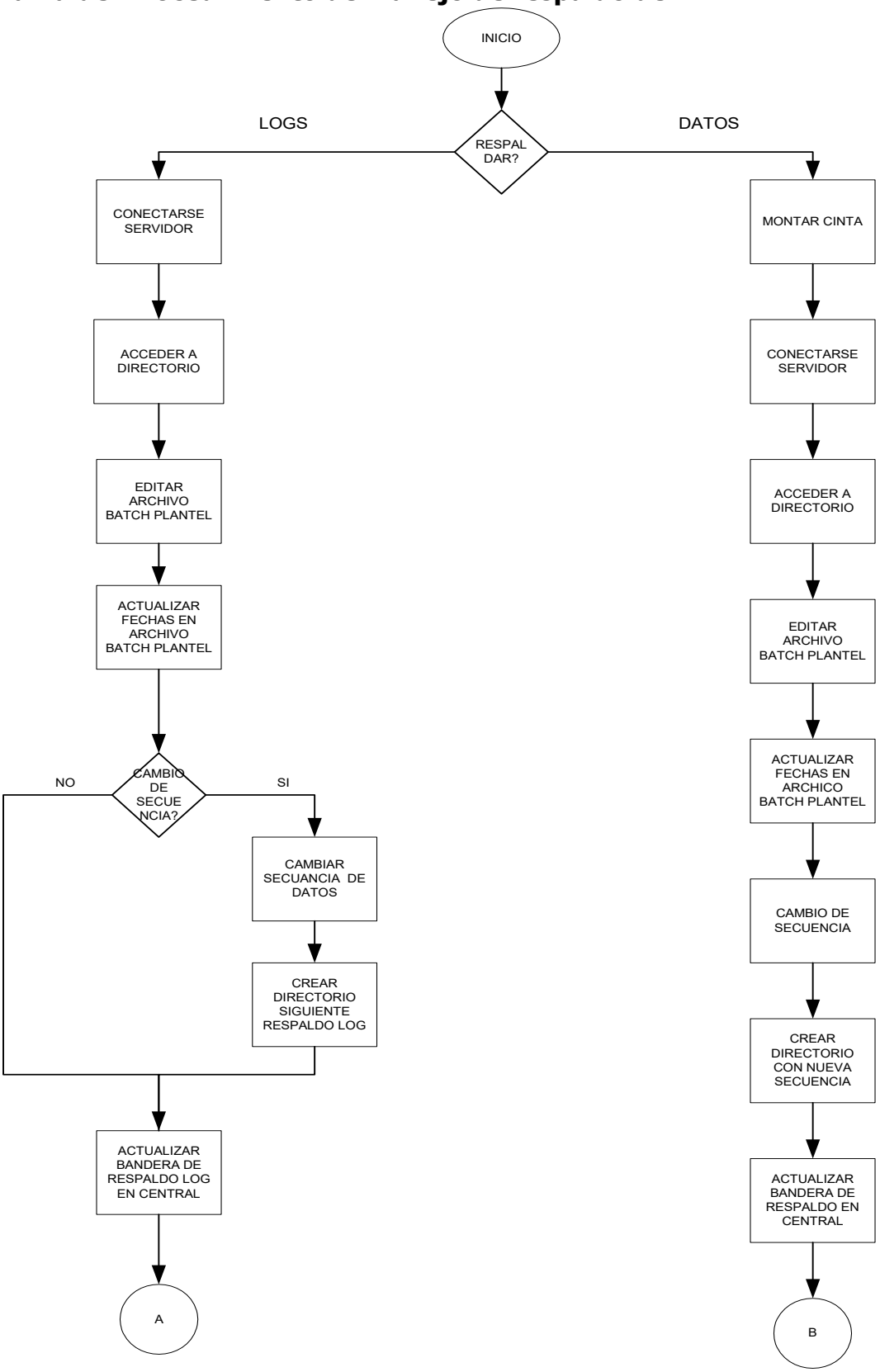
3.- En el procedimiento de manejo de respaldo de B.D. se realizaran:

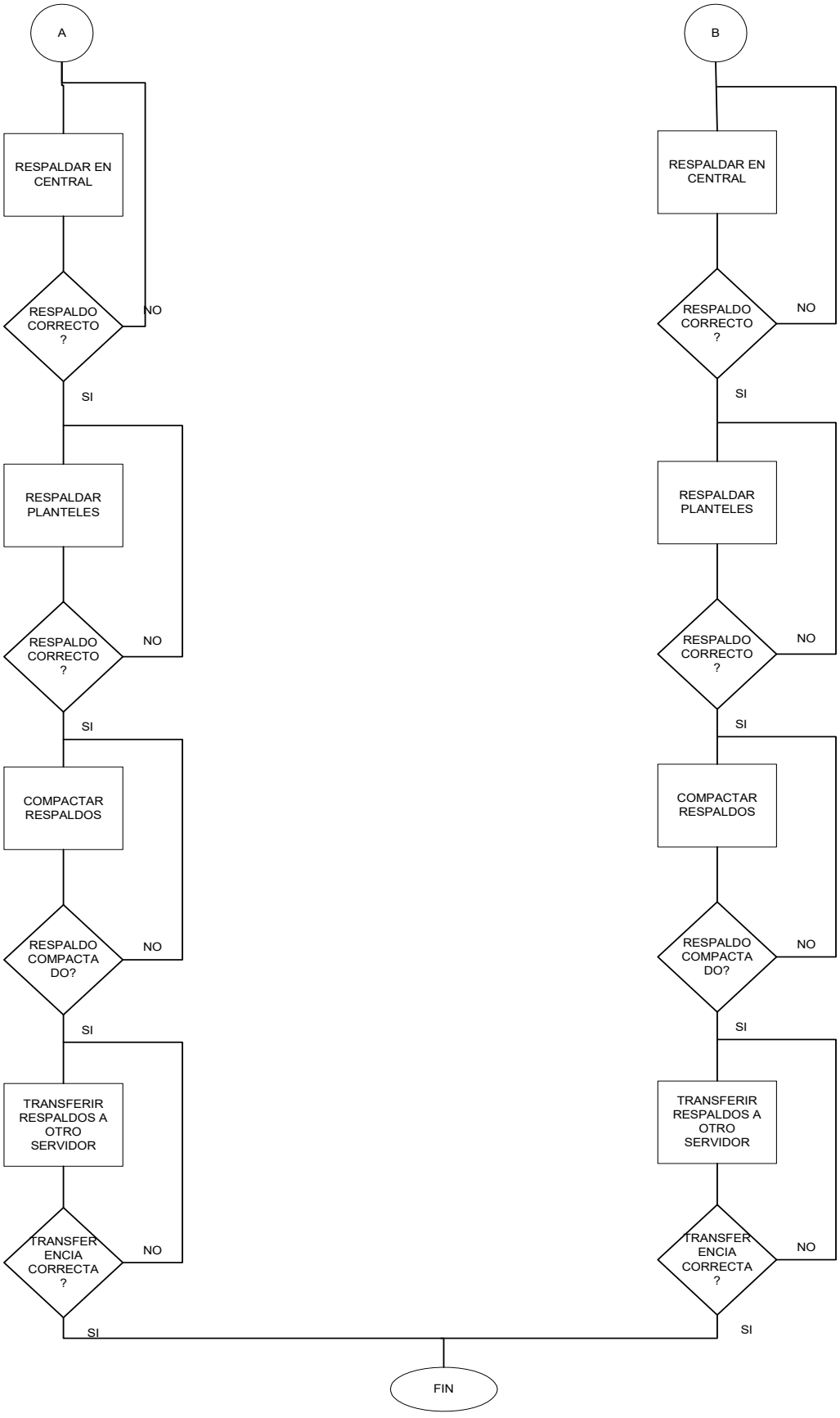
- Respaldo y recuperación de datos se realizará una vez al mes o cuando halla más movimientos de los previstos.
- Respaldo y recuperación de logs se realizará diariamente.

4.- Para hacer los respaldos de logs se tienen que llevar a cabo:

- Actualización de Scripts.
- Ejecución de Scripts.
- Compactación de archivos de respaldo.
- Transferencia de archivos compactados.

## Digrama del Procedimiento de manejo de respaldo de B.D.




A
RESPALDAR EN CENTRAL
RESPALDO CORRECTO ?
NO
SI
RESPALDAR PLANTELES
RESPALDO CORRECTO ?
NO
SI
COMPACTAR RESPALDOS
RESPALDO COMPACTADO?
NO
SI
TRANSFERIR RESPALDOS A OTRO SERVIDOR
TRANSFERENCIA CORRECTA ?
NO
SI
B
RESPALDAR EN CENTRAL
RESPALDO CORRECTO ?
NO
SI
RESPALDAR PLANTELES
RESPALDO CORRECTO ?
NO
SI
COMPACTAR RESPALDOS
RESPALDO COMPACTADO?
NO
SI
TRANSFERIR RESPALDOS A OTRO SERVIDOR
TRANSFERENCIA CORRECTA ?
NO
SI
FIN

### 4.4 Procedimiento para rastrear actividades sospechosas en S.O.

## Objetivo

Este procedimiento tiene como objetivo el poder rastrear alguna actividad que se considere como sospechosa dentro del S.O., para que en dado caso y dependiendo que tan grave se halla afectado al sistema se tome una decisión de que hacer.

### Normas de Operación

1.- El rastreo de actividades sospechosas se hará por lo menos cada dos meses o antes, si alguna de las herramientas utilizadas para seguridad nos indicaran la presencia de un intruso o que se sospechara de alguna actividad no deseada en el sistema.

2.- El rastreo se llevará a cabo por la persona designada por el administrador.

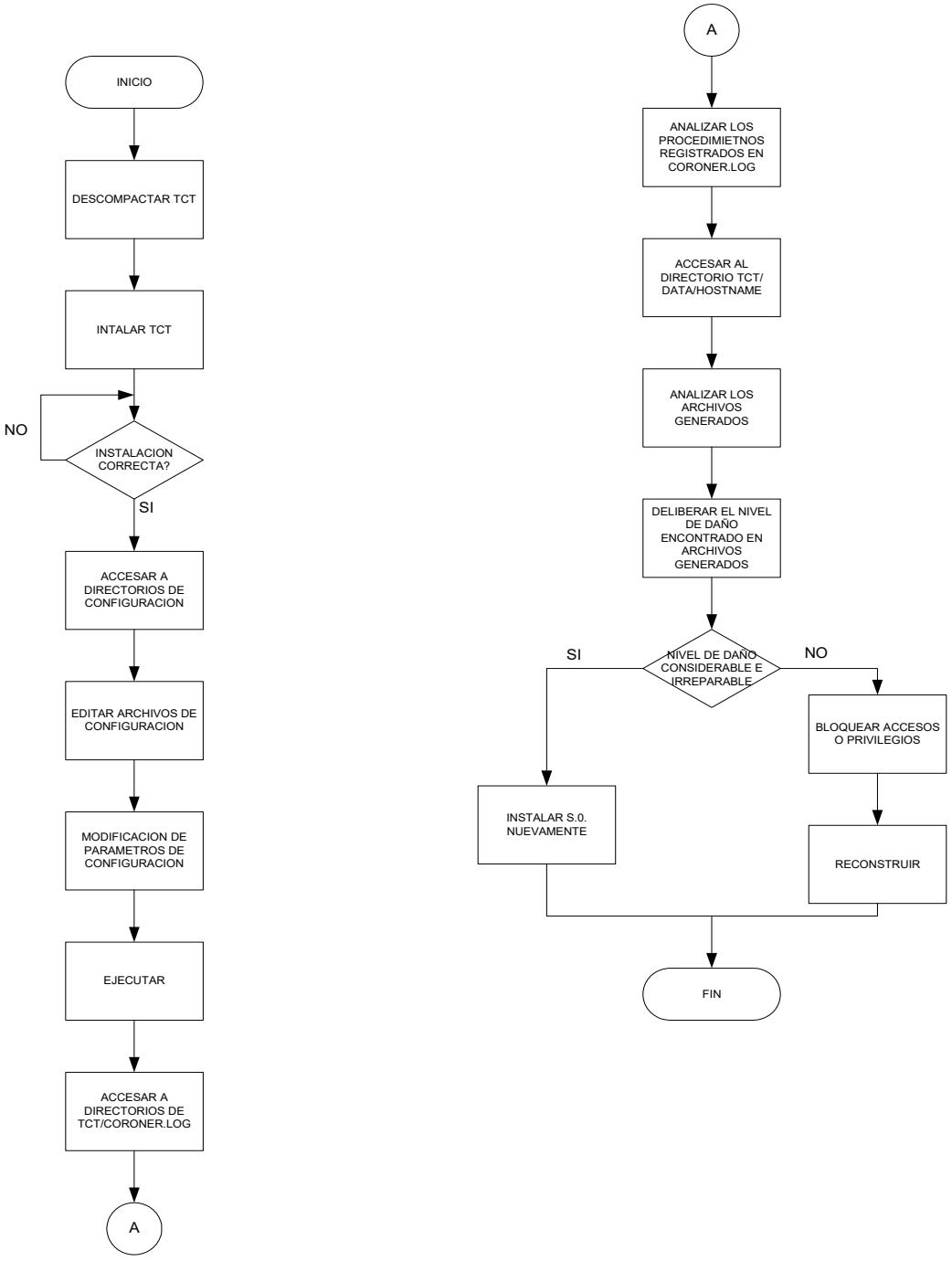
3.- Este rastreo se llevará a cabo con la herramienta TCT (The Coroner´s ToolKit).

4.- El rastreo de actividades sospechosas se divide en:

- Instalación de TCT.
- Configuración de TCT.
- Ejecución de TCT.
- Análisis de los archivos arrojados por TCT.

5.- La herramienta TCT tiene que ser actualizada cada que se lleve a cabo el procedimiento.

## DIAGRAMA DE PROCEDIMIENTO PARA RASTREAR ACTIVIDADES SOSPECHOSAS



## 5. Herramientas de seguridad

Una herramienta de seguridad es un programa diseñado para ayudar al administrador ya sea alertándolo o realizando por sí mismo las acciones necesarias a mantener su sistema seguro.

### Clasificación de herramienta de seguridad

- Orientadas a host: Trabajan exclusivamente con la información disponible dentro del host (configuración, bitácoras, etc.)
- Orientadas a red: Trabajan exclusivamente con la información proveniente de la red (barridos de puertos, conexiones no autorizadas, etc.)

Es importante destacar que toda herramienta de seguridad útil para el administrador es también útil para un atacante, y toda herramienta de seguridad disponible para un administrador debemos asumir que está también disponible para un atacante.

A continuación explicaremos brevemente las características de algunas de las herramientas de seguridad informática que se utilizan en la Red SIAE.

### 5.1 Auditoria de Sybase.

### Función

Registra la actividad del sistema relacionada con la seguridad en una lista de auditoría que puede utilizarse para detectar la penetración del sistema y el mal uso de los recursos del mismo.

### Sistema de auditoría

El sistema de auditoría se compone de la base de datos *sybsecurity* y de un conjunto de procedimientos almacenados que permiten definir selectivamente las opciones de auditoría que se necesitan.

Es posible realizar la auditoría de lo siguiente:

- Dentro de un servidor, es posible auditar los logins y logouts de sesión, los arranques del servidor, las conexiones RPC realizadas desde otros servidores, los errores y la ejecución de comandos que requieren roles especiales.
- A nivel de base de datos, se puede auditar el uso de los comandos **grant** , **revoke** , **truncate table** y **drop** dentro de una base de datos, el uso de los

comandos **drop** y **use** en una base de datos y las referencias a una base de datos específica desde dentro de otra base de datos.
- A nivel de usuario, es posible auditar los intentos de un usuario específico de tener acceso a tablas y vistas, y también se puede auditar el texto de los comandos enviados al servidor por un usuario.
- A nivel de objeto, se puede realizar una auditoría de los accesos a tablas y vistas especificadas y de la ejecución de procedimientos almacenados y disparadores.

**Base de datos sybsecurity**

La base de datos *sybsecurity* se compone de:

- La tabla *sysaudits* , registra la actividad de auditoria activada.
- La tabla *sysauditoptions* , que contiene una fila para cada opción de auditoría global.
- Las demás tablas del sistema predeterminadas, que se derivan de la base de datos *model* .

Consulte el *Suplemento de Referencia de SQL Server* para obtener una descripción de cada tabla del sistema.

**Instalación del sistema de auditoria**

El sistema de auditoria y la base de datos sybsecurity pueden instalarse en cualquier momento de manera manual, aplicando los siguientes pasos.

- Crear la B.D. sybsecurity.
- Ejecutar el procedimiento almacenado install security.
- Configurar la auditoria que se desea.
- Habilitar la auditoria.

**Definición de las opciones de auditoría**

Los oficiales de seguridad del sistema pueden determinar el tipo de auditoría que se va a realizar en el sistema. Las opciones de auditoría se administran usando los siguientes procedimientos del sistema:

**Tabla 5-1: Procedimientos del sistema usados para administrar las opciones de auditoría**

| Procedimiento del sistema | Descripción |
|---|---|
| **sp_auditoption** | Habilita e inhabilita la auditoría de todo el sistema y las opciones de auditoría globales |

**Tabla 5-1: Procedimientos del sistema usados para administrar las opciones de auditoría**

| Procedimiento del sistema | Descripción |
|---|---|
| **sp_auditdatabase** | Establece la auditoría de tipos diferentes de eventos dentro de una base de datos, o de referencias a objetos de dicha base de datos desde otra base de datos |
| **sp_auditobject** | Establece la auditoría selectiva de accesos a tablas y vistas |
| **sp_auditsproc** | Audita la ejecución de procedimientos almacenados y disparadores |
| **sp_auditsproc** | Audits the execution of stored procedures and triggers, and the set of labels with which a trusted stored procedure or trigger is invoked.invoked |
| **sp_auditlogin** | Audita los intentos de un usuario de tener acceso a tablas y vistas, o el texto de los comandos que el usuario ejecuta |
| **sp_addauditrecord** | Permite que los usuarios introduzcan registros (comentarios) de auditoría definidos por el usuario en la lista de auditoría |

### Cola de auditoría

Cuando se produce un evento auditado, un registro de auditoría va primero a la cola de auditoría, donde espera hasta que puede añadirse a la lista de auditoría. El tamaño de la cola se puede configurar con la opción **audit queue size** de **sp_configure**. El tamaño de dicha cola se establece según las necesidades del usuario. Consulte la *Guía de Administración de Seguridad* para obtener información sobre cómo configurar el tamaño de la cola de auditoría y los efectos de los distintos tamaños de cola.

### Lista de auditoría

La lista de auditoría se encuentra en la tabla *sybsecurity. sysaudits* . Es una tabla especial donde las únicas operaciones permitidas son **select** y **truncate table**, las cuales sólo pueden ser realizadas por oficiales de seguridad del sistema. Las columnas de *sysaudits* se describen en el *Suplemento de Referencia de SQL Server.* Los procedimientos para archivar la lista de auditoría se explican en la *Guía de Administración del Sistema*.

### Permisos

Sólo los oficiales de seguridad del sistema pueden habilitar la auditoría y ejecutar los procedimientos del sistema que definen las opciones de auditoría. La excepción es **sp_addauditrecord** , que puede ser ejecutado por cualquier usuario al que se le haya concedido el permiso para ejecutarlo.

## 5.2 Firewall

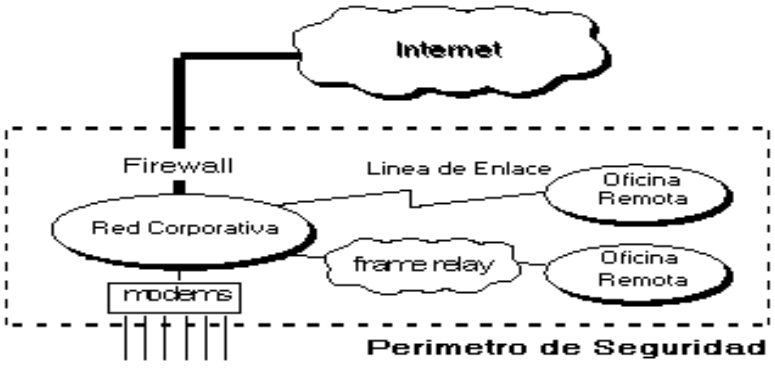
Un Firewall es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce la política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet).

Puede consistir en distintos dispositivos, tendientes a los siguientes objetivos:

1. Todo el tráfico desde dentro hacia fuera, y viceversa, debe pasar a través de él.

2. Sólo el tráfico autorizado, definido por la política local de seguridad, es permitido.

Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cual de los servicios de red pueden ser accesados dentro de esta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración, desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.




**Tipos de firewalls.**

- El servidor remoto o proxy. Un servidor proxy, es una aplicación que media en el tráfico que se produce entre una red protegida e Internet. Los proxies se utilizan a menudo, como sustitos de routers controladores de tráfico, para prevenir el tráfico que pasa directamente entre las redes. Muchos proxies contienen logines auxiliares y soportan la autentificación de usuarios. Un proxy debe entender el protocolo de la aplicación que está siendo usada,

aunque también pueden implementar protocolos específicos de seguridad (por ejemplo: un proxy FTP puede ser configurado para permitir FTP entrante y bloquear FTP saliente). Los servidores proxy, son aplicaciones específicas. Un conjunto muy conocido de servidores proxy son los **TIS** (Internet Firewall Toolkit "FWTK"), que incluyen proxies para Telnet, rlogin, FTP, X-Windows, http/Web, y NNTP/Usenet news.

- Las monitoras de rutas, que conectan dos o más computadoras juntas para hacer una red, son el tipo más básico de firewall. Su conexión del Internet se une a la monitora y usted tiene acceso al Internet a través de su red interna. Dos o más computadoras pueden compartir la conexión del Internet y ser protegidas por la firewall, que está construida en la monitora, al mismo tiempo.
- Firewall de red de alto nivel de seguridad. Estas firewalls comparan las configuraciones de bits de los paquetes de datos que son enviados a través de la red a los paquetes de datos que se enumeran como "confiables" o seguros. Estas firewalls se utilizan para ayudar a detener los ataques de DOS (negación del servicio). También utilizan filtro del paquete dinámico para controlar automáticamente el flujo de datos a través de los puertos, para reducir al mínimo el número de puertos abiertos en cualquier momento dado para ayudar a detener que hackers consigan tener acceso a la red.
- La aplicación o programa de firewall es probablemente el tipo más común. Es un programa que funciona en su computadora y que permite que los datos pasen a través de él, si usted ha configurado el programa para permitirlo. Usted selecciona simplemente cuál de sus aplicaciones, como buscadores de Internet, cliente del email, mIRC, etc. usted quiere que la "firewall" le permita tener acceso al Internet. Estas firewalls se diseñan principalmente para proteger solamente a la computadora en que está funcionando el programa.

## 5.3 OpenSSH

### ¿Qué es Secure Shell?

**Secure Shell** (ssh) es un programa que permite realizar conexiones entre máquinas a través de una red abierta de forma segura, así como ejecutar programas en una máquina remota y copiar archivos de una máquina a otra. Tal y como se explica en el RFC de Secure Shell:

"SSH(Secure Shell) es un programa para conectarse a otros equipos a través de una red, para ejecutar comandos en una máquina remota y para mover archivos de una máquina a otra. Proporciona una exhaustiva autenticación y comunicaciones seguras en redes no seguras"

Ssh provee autenticación y comunicación segura sobre un canal inseguro y nace como un reemplazo a los comandos **telnet, ftp, rlogin, rsh, y rcp**, los cuales proporcionan gran flexibilidad en la administración de una red, pero sin embargo, presenta grandes riesgos en la seguridad de un sistema. Adicionalmente, **ssh** provee seguridad para conexiones de servicios **X Windows** y envío seguro de conexiones arbitrarias TCP.

Secure Shell admite varios algoritmos de cifrado entre los cuales se incluyen:

- Blowfish
- 3DES
- IDEA
- RSA

La ventaja más significativa de ssh es que no modifica mucho las rutinas. En todos los aspectos, iniciar una sesión de ssh es tan sencillo como( y similar a) iniciar una sesión de telnet. Tanto el intercambio de llaves, la autenticación, así como el posterior cifrado de sesiones son transparentes para los usuarios.

### ¿De que Previene Secure Shell?

Debido a la promiscuidad de la interfaz ethernet, se genera una problemática sobre los siguientes servicios de red usados en la actualidad, tales como:

- telnet
- ftp
- http
- rsh
- rlogin
- rexec

Ello nos representa un problema importante, ya que, incluso en un entorno de red cerrado, debe existir como mínimo un medio seguro para poder desplazar archivos, hacer copia de archivos, establecer permisos, ejecutar archivos, scrips, etc, a través de medios seguros.

Por ello para evitar que determinadas personas capturen el trafico diario de la red, es conveniente instalar el Secure Shell(SSH).

Entre los ataques más comunes que nos previenen Secure Shell están:

- Sniffering(Captura de trafico)
- IP Spoofing
- MACpoofing
- DNS Spoofing
- Telnet Hickjacking
- ARP Spoofing
- ARP Spoofing
- IP Routing Spoofing
- ICMP Spoofing

**Protocolos de Secure Shell**

Existen actualmente dos protocolos desarrollados sobre ssh:

- **SSH1**: La última versión de **ssh cliente/servidor para Unix** que soporta este protocolo es la **1.2.31**, esta puede ser utilizada libremente para propósitos no comerciales y es ampliamente usada en ambientes académicos.
- **SSH2**: Provee licencias más estrictas que **SSH1** ya que es de carácter comercial. La ultima versión de ssh **cliente/servidor para Unix** con este protocolo es la **2.4.0** y puede ser utilizada libremente respetando la licencia expresa.

Actualmente existe un proyecto llamado **OpenSSH**, el cual fue desarrollado inicialmente dentro del proyecto **OpenBSD**.

**OpenSSH** es una versión libre de los protocolos **SSH/SecSH** bajo licencia BSD y es totalmente compatible con los protocolos **SSH1** y **SSH2**. La ultima versión de **OpenSSH cliente/servidor** para Unix es la 3.2.3. (Liberada el 11 de febrero del 2003).

Debido a que OpenSSH rompe la barrera de los protocolos que ha causado confusión entre diversos sectores, esta herramienta esta siendo muy usada en la

comunidad, tal es el caso de distribuciones como Linux RedHat 7.0 que ya la incluyen dentro de su sistema operativo.

Sin embargo OpenSSH ha demostrado en los últimos meses cierta inestabilidad, por lo que sí se instala dicha versión es altamente recomendable estar actualizando periódicamente el OpenSSH y estar al pendiente de vulnerabilidades presentadas.

Desafortunadamente los protocolos de **Secure Shell** (SSH1 y SSH2) no son compatibles uno con otro, por lo tanto, sí deseamos que exista compatibilidad debemos de instalar primero **Secure Shell protocolo SSH1** y posteriormente **Secure Shell protocolo SSH2**.

Otra opción para mantener la compatibilidad con los dos protocolos sin problema alguno es instalar **OpenSSH**.

## 5.4 SUDO

Sudo te permite definir grupos de hosts, grupos de comandos, y grupos de usuarios, haciendo la administración más sencilla, a largo plazo porque delega tareas del superusuario de Unix con sudo.

### *Introducción*

- ***sudo*** (***su***peruser ***do***)es un programa diseñado para permitir a un administrador de sistemas Unix el brindar privilegios de *superusuario* a sus usuarios y llevar una bitácora de la actividad de *root*.

- La filosofía básica de ***sudo*** es brindar los menos privilegios posibles, pero al mismo tiempo permitir que los usuarios lleven a cabo su trabajo.

- La filosofía de ***sudo*** se originó en SUNY-Buffalo (Universidad Estatal de Nueva York en Buffalo) a principios de los 80.

- En 1996 ***sudo*** fue comprado por *Todd C. Miller* a través de su firma consultora ***Courtesan Consulting***. Todd tenía ya varios años manteniendo sudo por su cuenta, labor que hasta la fecha desempeña.

### *¿Cómo trabaja?*

- Configurar *sudo*

  ***$ man sudoers***
  ***# /usr/local/sbin/visudo***

- *Ejecutar* sudo

  ***$ /usr/local/bin/sudo –u usuario comando***
  ***¿Cómo trabaja?***

- ***visudo*** permite editar el archivo ***/etc/sudoers***, bloquea este archivo para evitar ediciones simultáneas, realiza un chequeo básico de la integridad de este archivo y verifica errores de sintáxis en el mismo.

- ***sudoers*** es un archivo de texto que mediante reglas establece *qué* usuario(s) puede(n) ejecutar *qué* comando(s) en *qué* máquina(s) como *qué* usuario(s). Básicamente contiene variables (*aliases*) y especificaciones de usuarios (que especifican *quién* puede correr *qué*).

- ***sudo*** es básicamente un programa que permite a un usuario autorizado ejecutar un comando con los privilegios de *root* o de otros usuarios.

### *Características*

- ***sudo*** es distribuido con una licencia estilo BSD ("utilice este software bajo su propio riesgo").

- ***sudo*** ha sido probado en las siguientes plataformas: Solaris, HP-UX, IRIX, NEXTSTEP, AIX, OpenBSD, FreeBSD, Linux, NetBSD, Unicos, OSF y otras.

- La gramática del archivo ***/etc/sudoers*** puede ser descrita en ***EBNF*** (*Extended Backus-Naur Form*), que es una forma exacta y concisa de describir la gramática de un lenguaje.

- La última versión de ***sudo*** es la 1.6.7 P5, liberada el 8 de mayo del 2003.

### *Ventajas*

- ***sudo*** evita dar a conocer la contraseña (*password*) de *roo*t de una máquina a varios administradores de sistema operativo.

- ***sudo*** evita establecer permisos de SUID o SGID a gran cantidad de programas.

- ***sudo*** permite registrar en un *log* las actividades de los usuarios para propósitos de auditoria.

### *Requerimientos*

- Un sistema Unix System V ó BSD

- Compilador CC ó GCC

- Utilería *make*

- Tiempo y paciencia ☺

## 5.5 TCP-Wrapers.

El tcp-wrappers es un software de domino público desarrollado por Wietse Venema (Universidad de Eindhoven, Holanda). Su función principal es: proteger a los sistemas de conexiones no deseadas a determinados servicios de red, permitiendo a su vez ejecutar determinados comandos ante determinadas acciones de forma automática.

Es una herramienta que permite *monitorear* y *filtrar* diversos servicios de red en un sistema Unix, tales como telnet, ftp, ssh, rsh, rlogin, talk, y finger.

Una vez instalado, se pueden controlar los accesos mediante el uso de reglas y dejar una traza de todos los intentos de conexión tanto admitidos como rechazados (por servicios, e indicando la máquina que hace el intento de conexión), incrementando la Seguridad de un Sistema Unix.

### *Introducción*

- Las redes de computadoras nos brindan posibilidades nunca antes imaginadas, pero al mismo tiempo abren muchos *huecos de seguridad* en los sistemas conectados a ellas.

- ***TCP-Wrappers*** es una herramienta que permite *incrementar* la seguridad de un sistema Unix, pero su implantación es sólo una pequeña parte de las acciones que deben ser tomadas para realmente *asegurar* un sistema Unix.

- Herramienta creada para rastrear los ataques de un *cracker* alemán contra una máquina de la Universidad de Eindhoven, en Holanda.

- Es una herramienta de seguridad *libre*.

- Está basada en el concepto de *wrapper.*

### *¿Cómo trabaja?*

- Casi todas las aplicaciones del protocolo TCP-IP utilizan el modelo *cliente-servidor*.

- Cuando un usuario ejecuta el comando *ftp* en la máquina origen (cliente), quién atiende la petición es el *servidor de ftp* de la maquina destino (servidor).

### *Características*

- Control de acceso para restringir qué sistemas pueden conectarse a que servicios de red.

- Facilidad de detección del nombre de usuario cliente en base al nombre de la máquina remota (RFC 931).

- Protección adicional contra ataques de *ip address spoofing* y *host address spoofing*.

### *Limitantes*

- *TCP-Wrappers* no trabaja con servicios RPC sobre TCP (rpc/tcp en */etc/inetd.conf*). Ej. Servicios *RPC.*

- *TCP-Wrappers* sólo "verá" la petición que inició un demonio UDP y rpc/udp (demonios con la opción *wait* en */etc/inetd.conf*). Ej. Servicios *talk* y *tftp*

### *Requerimientos*

- Un sistema Unix System V ó BSD

- Compilador CC ó GCC

- Utilería *make*

- Demonios de red controlados por el "superdemonio" *inetd*

- Disponibilidad de un demonio *syslogd* y una biblioteca de *syslog*

- El deseo de asegurar un poco más el sistema Unix ☺

## 5.6 PortSentry

Portsentry es un programa que se usa para el barrido de puertos. Su misión es sentarse y escuchar a los puertos que le indiquemos que deben permanecer siempre inactivos. En caso de llegar una conexión a uno de ellos puede marcarlo en la bitácora del sistema, bloquear toda la comunicación con la dirección identificada como agresora, o correr un comando externo.

### Introducción

- Psionic portsentry es parte de las herramientas del proyecto Abacus (al lado de portsentry, tienen logcheck y hostsentry).
- Es un IDS (Sistema de detección de intrusión) dedicado a la detección de barridos de puertos y a la defensa activa.
- Funciona con muchos sabores de Unix incluso Mac OS X.
- La característica principal de un IDS es de informar al administrador sistema sobre intentos de intrusión.
- Portsentry va más lejos, puesto que es capaz de reaccionar a un ataque.

### ¿Cómo trabaja?

- Descompactar y extraer los archivos de Portsentry

  ***$ gunzip portsentry-2.0b1.tar.gz***
  ***$ tar xvf portsentry-2.0b1.tar***

- Compilar el sistema

  ***make <sistema>***

- Para instalar nos convertimos en root y le damos

  ***make install***

- Portsentry quedará instalado en el directorio /usr/local/psionic/portsentry listo para ser configurado.

- La configuración de Portsentry se hace en el archivo

  /usr/local/psionic/portsentry/portsentry.conf

- Portsentry tiene varios modos de operación. El más común y sencillo es el modo clásico, y el más poderoso (aunque no disponible en todos los sistemas) es el modo avanzado.

  **Modo clásico**

  En este modo, le especificamos a Portsentry que escuche determinados puertos TCP y UDP, especificados con las opciones UDP_PORTS y TCP_PORTS por los cuales no estamos dando ningún servicio y son poco solicitados. Por ejemplo, puede que nuestro servidor no esté dando servicio de red SMB (Samba, red tipo Microsoft). Sin embargo, es común que las computadoras windows manden mensajes broadcast buscando a un sistema en específico, con lo que podríamos recibir una gran cantidad de alertas en falso. Vienen varios puertos predefinidos en el archivo de configuración, y son buenos como recomendación inicial.

  **Modo stealth**

  En este modo Portsentry abre sockets crudos, lo que le permite detectar una mayor cantidad de barridos y ataques: Ataques de conexión normal, SYN/half-open, FIN, NULL y XMAS. Este modo es un tanto experimental, por lo cual no funcionará en todos los sistemas.

  **Modo avanzado**

  Este modo es también considerado hasta cierto punto perteneciente a la categoría stealth. En éste modo, Portsentry no abre ningún puerto, sino que le pide al kernel que le notifique si llega alguna petición a algún puerto menor al especificado en las opciones ADVANCED_PORTS_TCP y ADVANCED_PORTS_UDP. Claro, tendremos que excluir algunos puertos que sean particularmente ruidosos --como el ejemplo que comentábamos en la sección anterior de la red SMB-- y para ello tenemos las opciones ADVANCED_EXCLUDE_TCP y

ADVANCED_EXCLUDE_UDP. El modo avanzado es mucho más sensible que el modo clásico, dado que escucha a muchos más puertos, por lo que puede efectivamente causar una negación de servicio si no es configurado con cuidado.

**¿En qué sistemas funciona?**

Portsentry es un programa muy portátil, y podremos utilizarlo para virtualmente cualquier sistema operativo Unix. En el sitio FTP de Psionic hay un archivo llamado portsentry.COMPAT, donde detalla que los sistemas operativos compatibles con Portsentry son:

- Linux 1.x/2.x
- BSDI 2.x/3.x
- OpenBSD 2.x
- FreeBSD 3.x
- HPUX 10.20
- Solaris 2.6+
- AIX
- SCO
- Digital Unix
- NetBSD

**Ventajas**

- Portsentry puede aprovechar los filtrajes de paquetes tales como ipfwadm, ipchains o iptables según el kernel Linux que tienen.
- La característica más importante de portsentry, es probablemente "auto-bloqueo".
- Puede crear logs. Si son de la categoría de sysadmin quienes no lean los logs, pueden usar logcheck al lado de portsentry.
- Manda un correo para informarles de una tentativa de intrusión.
- Puede escribir el "target host" en el fichero /etc/hosts.deny, para beneficiar de TCPWrappers.
- El host local puede cambiar la ruta del tráfico de la red hacia un host muerte.
- El host local puede "echar" los paquetes via la herramienta local de filtraje de paquete.

## 5.6 Tcpdump.

Es un software de dominio público que imprime las cabeceras de los paquetes que pasan por una interfaz de red. Este programa es posible ejecutarlo en modo promiscuo con lo que tendremos las cabeceras de los paquetes que viajan por la red.

## Introducción

- El programa tcpdump, fue escrito por Van Jacobson, Craig Leres, y Steven McCanne, y ampliado por Andrew Tridgell.
- Tcpdump (y su port a Windows, Windump) son programas cuya utilidad principal es analizar el tráfico que circula por la red.
- Se apoya en la librería de captura pcap, la cual presenta una interfaz uniforme.
- Esconde las peculiaridades de cada sistema operativo a la hora de capturar tramas de red.
- Es necesario conocimientos básicos del protocolo TCP/IP.

## Características

- Más que un sniffer, tcpdump es una herramienta de depuración y análisis de problemas de red. Suele estar disponible en todas las distribuciones Linux.
- Tiene una potente capacidad de filtrado, pero presta poca atención a los datos que las aplicaciones transmiten. Esto es, es poco útil para los crackers.
- Por defecto imprime por la salida estándar las cabeceras de los paquetes.
- Se pueden hacer filtrados por dirección (origen y destino), puerto (rango, menor que, mayor que, etc.), protocolo, dirección física, comparaciones con cualquier byte del paquete. Es posible construir búsquedas complejas combinando primitivas mediante conectores lógicos (and, or, !).
- El manual en línea es la mejor fuente de información sobre la sintaxis.

## Uso básico

- Lo primero que debemos averiguar cuando estamos usando el tcpdump, es las interfaces que queremos escuchar. Por defecto cuando se ejecuta sin parámetros, en los Linux se pone a escuchar en la eth0.
- Para averiguar la interfaces en cualquier Unix recurrimos al comando ***ifconfig -a*** el cual nos da una lista de las interfaces que tenemos, así como sus parametros de configuración.

- Cuando estamos leyendo la red, puede que no nos interese que el tcpdump intente resolver los nombres de las maquinas (pueden que no estén dadas de alta en el DNS, por motivos de seguridad, etc), para ello disponemos de la opción **-n**.
- Para establecer la longitud de los datos que captura tcpdump usamos **-s len**, donde len es la longitud que nos interesa.
- Por defecto el tcpdump sólo captura los primeros 68 bytes, lo cual es útil si lo único que se quiere son las cabaceras IP, TCP o UDP, pero que en caso de estar especificando protocolos como el NFS truncan los datos. En ese caso podemos ajustar la longitud de la captura a la MTU del medio que estamos usando con esta opción. Por ejemplo para capturar toda la trama ethernet podemos usar *-s 1500*.
- En función de la cantidad de información que queramos a la hora de que el tcpdump nos interprete, podemos usar *-v,-vv,-vvv*, aumentando el grado de información con cada una de las opciones.
- Si queremos imprimir el contenido del paquete, podemos usar la opción *-x*.
- Si ademas queremos que nos imprima en ASCII el contenido de los paquetes podemos usar **-X**.
- La longitud que imprime viene determinada por la opción **-s** o los 68 bytes que usa captura por defecto.
- Podemos trabajar offline con el tcpdump.
- Si queremos grabar nuestra captura para posteriormente leerla y analizarla usamos la opción **-w file** donde *file* es el nombre del fichero donde queremos grabar la captura de datos.
- Posteriormente podemos leer y analizar offline con **-r file**. Además este tipo de ficheros de captura lo pueden leer otros analizadores como por ejemplo **Ethereal**.

## Ventajas

- Permite monitorear tráfico de red a tiempo real.
- Están disponibles una variedad de formatos de salida
- Puede filtrar la salida para buscar sólo un tipo particular de tráfico.
- Permite examinar todas las conversaciones entre el cliente y el servidor, incluyendo mensajes de broadcast SMB y NMB.
- Sus capacidades de detección de errores están principalmente a nivel de capa de red (OSI).
- Puede usar su salida para obtener una idea general que qué están intentando hacer el servidor y el cliente.

### 5.7 Snort

Dentro de la lista de programas de detección de intrusos (**IDS**) uno de los programas más populares es SNORT, no solo por que es ***gratuito*** sino porque además es bastante simple de configurar y es bastante sencillo de administrar.

## Introducción

- El autor es Marty Roesch.
- Sniffer para analizar tráfico que puede utilizarse como un IDS ligero.
- Capaz de realizar análisis de tráfico e ingreso de paquetes en la red IP en tiempo real.
- Puede realizar análisis de protocolo y búsquedas de contenido pudiendo ser utilizado para detectar distintos ataques y explorar como moderar shocks de overflow, prever scaneo de puertos, ataques de CGI, huellas de intento de intrusión al sistema operativo, y otras.
- Snort utiliza reglas flexibles en un lenguaje que describe el tráfico que debería ser admitido y cual no.
- Tiene además un sistema de alerta en tiempo real incorporando mecanismos de syslog, a un archivo especificado por un usuario, un socket UNIX, o un mensaje popup a los clientes windows utilizando Samba.
- Snort tiene tres usos principales:
    - Programa sniffer, como detector directo de paquetes como tcpdump.
    - Programa de análisis, como monitoreo de paquetes (útil para el análisis de tráfico de red).
    - Sistema detector de intrusos, como un potente sistema de detección de intrusión a la red, también tiene la capacidad de ejecutar acciones basadas en eventos de detección.

## Ventajas

- Es gratuito, simple de configurar y sencillo de administrar.
- Permiten una serie de expansiones tales como conexión a base de datos y otras mas.
- SNORT en sus comienzos no poseía soporte de interfaz grafica, por eso hoy en día sigue siendo posible utilizar la línea de comandos para ejecutar SNORT y sus opciones.
- Existen múltiples herramientas que permiten controlar el sistema desde Windows red que este monitoriza.
- Incorpora un sistema bastante sencillo para escribir nuestras reglas, de modo que podemos adaptarlo a nuestros requerimientos rescribiendo las reglas para los incidentes que deseamos monitorizar.

**Instalación**

- Si no se cuenta con la biblioteca libpcap (PCAP94), debemos instalarla, por lo tanto descompactamos y extraemos los archivos libcap.

  **$ gunzip libpcap.tar.Z**

  **$ tar xvf libpcap.tar**

- Compilación de libpcap. Debemos de ejecutar el script de configuración para posteriormente ser compilado.

  **$ ./configure**

  **$ make**

- Finalmente, ya con el binario construido, debemos de instalar la biblioteca en el sistema ejecutando los siguientes comandos como root

  **# make install**

  **# make install-incl**

  **# make install-man**

- Ahora descompactamos y extraemos Snort.

  **$ gunzip snort-1.9.0.tar.gz**

  **$ tar xvf sonrt-1.9.0.tar**

- Descompactamos y extraemos el parche de Snort y lo copiamos al directorio generado en el paso anterior.

  $ gunzip snort-1.9.0-patch2.tar.gz

  $ tar xvf snort-1.9.0-patch2.tar

  $ cp –r sonrt-1.9.0-patch2/* snort-1.8.2/.

- Ejecutamos el script de configuración de Snort.

  $ ./configure

- Finalmente, compilamos Snort y lo instalamos de la siguiente manera como root.

**$ make**

**# make install**

## Plataformas soportadas

- Unix
- Linux
- OpenBSD
- FreeBSD
- NetBSD
- Solaris
- SunOS 4.1.X

## 5.8 TCT (The Coroner´s ToolKit)

The Coroner's Toolkit es una colección de herramientas diseñadas para asistir al examen 'forense' de un equipo informático.

### Introducción

- Los creadores fueron Dan Farmer de EarthLink y Wietse Venema de IBM.
- Está diseñado, en principio, para sistemas Unix, pero también puede trabajar sobre otros sistemas.
- Las herramientas están orientadas a recoger o analizar datos forenses en un sistema.
- Permite la reconstrucción del pasado, determinando, tanto como sea posible lo que pasó en cierto instante dentro del sistema.

### Instalación

- Descompactar y extraer los archivos de TCT

```
$gunzip tct-1.11.tar.gz
$tar xvf tct-1.11.tar
```

- Una vez extraído el paquete TCT, debemos simplemente de ejecutar el comando "make". El archivo Makefile configurará adecuadamente las herramientas del TCT.

```
$ make
```

- Si todo ha salido bien ya se puede empezar a usar el toolkit.
- Debemos leer el archivo "README" que se encuentra en el directorio "doc" y el archivo "quick-start" para ver la forma de usar este toolkit. Todas las herramientas tienen páginas de manual en los subdirectorios apropiados o dentro del directorio "man" y "doc".

### Ventajas

- Esta colección de programas sirve para realizar una 'autopsia' sobre sistemas UNIX después de que han 'muerto' completamente.

- El funcionamiento de este software se basa principalmente en la recogida de grandes cantidades de datos para proceder a su análisis posterior. Algunos de sus componentes son la herramienta 'ladrón de tumbas' (que captura información), los programas para detectar archivos 'muertos' o 'vivos', así como 'lázaro', que restaura archivos borrados, y otra herramienta que restaura claves criptográficas desde un proceso activo o desde algún archivo.
- TCT puede obtenerse mediante descarga libre.
- Es útil para la recopilación de datos en base a los tiempos MAC.
- Realiza análisis en sistemas atacados.
- Permiten recuperar ficheros borrados siempre que no hayan sido sobrescritos.
- Calcula la integridad de los ficheros existentes en el equipo.
- Consulta que ficheros han sido accedidos desde una determinada fecha.
- Se compone de cuatro partes fundamentales:
    - Programa grave-robber.
    - Herramientas en C (ils, icat, Prat, file, etc…).
    - Los programas unrm y lazarus.
    - Programa mactime.

**Plataformas soportadas**

- Unix
- SunOS 4-5.*
- Linux 2.*
- FreeBSD 2-4.*
- OpenBSD 2.*
- BSD/OS 2-3.*

## CONCLUSIÓN

A lo largo de la presente tesis se pudo comprender que la seguridad en sistemas de cómputo es un conjunto de recursos destinados a lograr que los activos de una organización sean confidenciales, íntegros y disponibles en cualquier momento para todos sus usuarios, para lograrlo existe mecanismos de control tales como las políticas y procedimientos de seguridad.

Cuando la seguridad en un sistema informático fallan aun cuando existen redactadas e implementadas las políticas, es por debilidades naturales de dichas políticas tales como: pensar que la seguridad reduce la productividad y no le añade facilidad a la operación, que la seguridad informática es un comportamiento aprendido y frecuentemente no es intuitivo, por otra parte mientras más compleja es la política, más probabilidad tiene de fallar y por último las políticas frecuentemente son estáticas.

Para evitar en parte lo antes mencionado se recomienda que en cualquier sistema informático se cuente con un personal capacitado en seguridad informática (ISO), recibir la fuerza y el apoyo de los directivos, que las políticas sean constantemente revisadas, es decir, que no sean estáticas y que se cuente con un plan de auditoria tanto interno como externo ya que esto ayuda a que nuestro sistema sea más robusto en cuanto a seguridad informática se refiere.

Se espera que con este trabajo se halla resaltado la importancia de que la Seguridad debe ser vista como un elemento de vital importancia en el manejo de la información, también esperamos que las políticas sean claras, pues se tuvo el cuidado de que fueran breves, posibles de cumplir y cooperativas esto con el fin de que todo el personal entienda dichas políticas y a su vez resaltar la importancia de apegarse a las buenas prácticas de la seguridad informática.

Las ventajas de la elaboración de este trabajo es que nos va a ayudar a tomar decisiones, ya que contiene guías con respecto a los estándares de protección requeridos, nos va a permitir decidir que acciones llevar a cabo en circunstancias particulares, como en el caso de una violación de la seguridad, donde la Política indica lo que las personas con autoridad para la toma de decisiones deben hacer para minimizar el impacto de tal violación, cómo prevenir futuras violaciones de seguridad, y cómo identificar y sancionar a quiénes resulten responsables de dicha violación, hablara muy bien del profesionalismo de la subdirección y estaremos preparados en caso de una auditoria a la subdirección.

Estamos conscientes de que no existe un esquema de seguridad que cubra en su totalidad los posibles riesgos, sin embargo se debe estar preparado y dispuesto a reaccionar con rapidez ya que las amenazas y las vulnerabilidades están cambiando constantemente.

Disponer de una política de seguridad es importante, pero entendemos que hacer de la política de seguridad una parte del entorno de trabajo diario es esencial. La comunicación con los usuarios del sistema es la clave para hacer que esta política sea efectiva y se genere una "cultura de la seguridad".

La implantación de una política de seguridad informática en una empresa implica un gran desafío, pero sabemos además que es imprescindible, sobre todo si se tiene en cuenta que cada vez se produce un mayor número de ataques a los sistemas informáticos.

Otro aspecto muy importante que debemos tomar en cuenta son las herramientas de software que ayudan en el proceso de mejorar la seguridad, estas nos permite brindar mayores beneficios en cuanto a reparación de errores a nivel del software que se este utilizando, involucrando el debido "conocimiento", minimizando los riesgos, suministrando los controles en el manejo del bien mas preciado. Múltiples herramientas pueden ser utilizadas en las evaluaciones de seguridad.

Asimismo se puede afirmar que las expectativas personales también fueron cubiertas con éxito. Fue posible aprender nuevos conceptos, desarrollando un trabajo de investigación sobre temas vigentes y volcar toda la teoría asimilada a un caso práctico. Por último, espero con este trabajo generar en el lector una inquietud que incite a futuras investigaciones o proyectos que profundicen en el campo de la seguridad informática.

**ANEXO I**

# CUESTIONARIOS

Para el desarrollo del análisis de riesgos y vulnerabilidades fue necesario entrevistar a distintos usuarios del sistema y demás personas que interactúan con él. Se adjuntan los cuestionarios utilizados para la realización de éstas entrevistas.

## 1. Revelamiento inicial

### 1.2 Hardware

- Topología y protocolos de red
  - Protocolos
  - Conexión al exterior
- Características del servidor:
  - tipo o marca de servidor,
  - capacidad de procesamiento,
  - cantidad de memoria,
  - capacidad de disco,
  - placas de red,
  - dispositivos varios (CD's, cintas, scanner, switch, hub, etc.),
  - UPS o sistemas de alimentación alternativa del servidor,
  - servidor alternativo, espejo o de contingencia,
  - servidor de datos o de impresión,
- Impresoras y Gestión de impresión
- PC´s
  - Cantidad
  - Características particulares
  - Terminales o PC´s
  - Clones o de marcas
  - Características generales
- Web
  - Tipo de conexión
  - Permisos o acceso de las PC´s
  - Firewall y virus wall
  - Página dinámica o estática
  - Servidor propio o web hosting.
- Back up
  - Disco espejo
  - Tercerización
  - Dispositivos de back up (CD's, cintas magnéticas, HD, disquete, etc.)

### 1.2 Software

- Software del servidor
  - S.O.
  - Aplicaciones
  - Motor de bases de datos
- S.O. y software de las PC´s
- Aplicaciones bases en cada sector de la empresa (administración, ventas, cómputos, etc.)
- Gestión de virus.
- Detalle de aplicaciones propias, enlatadas
- Gestión de red física y lógica
- Licencias.

### 1.3 Usuarios

- Organigrama.
- Responsabilidades en área de informática
  - Responsables de Redes
  - Responsables de Bases de datos
  - Responsables de Aplicaciones
  - Responsables de Servicio técnico
- Tipo de perfiles de usuarios según sectores
  - Clasificación del perfil
  - Accesos del perfil a aplicaciones o datos.

## 2. Seguridad lógica

### 2.1 Identificación de ID's

### 2.1.1 Altas

• ¿Qué datos hay en el perfil del usuario cuando se hace un alta? ¿Se guardan los siguientes datos?

- ID de usuario,
- Nombre y apellido completo,
- Puesto de trabajo y departamento de la empresa,
- Jefe inmediato,
- Descripción de tareas,
- Consentimiento a que auditen sus actividades en el sistema, y de que conoce las normas de "buen uso" del sistema,
- Explicaciones breves y claras de cómo elegir su password
- Tipo de cuenta o grupo al que pertenece (empleado, gerente, etc.)
- Fecha de expiración de la cuenta
- Datos de los permisos de acceso y excepciones
- Restricciones horarias para el uso de recursos

• ¿Que otros datos del usuario son necesarios en el ID? ¿Que datos guardan en la planilla de personal?
• ¿El ID de usuario puede repetirse? ¿Y si una cuenta fue borrada o eliminada, puede utilizarse un ID ya usado y eliminado para un usuario nuevo?

### 2.1.2 Bajas

• ¿Cómo se relacionan con los de recursos humanos? ¿El departamento de recursos humanos se encarga de comunicar las modificaciones en el personal? ¿Qué se hace al respecto? ¿Cómo se actualiza la lista?
• ¿Cómo se administran los despidos (o desvinculación del personal)? ¿Se tiene en cuenta una política de despidos para evitar actos de vandalismo por posibles disgustos de los empleados desvinculados de la empresa?
• ¿Hay algún histórico de las cuentas que se dan de baja?
• ¿Se guardan los archivos y datos de las cuentas eliminadas? ¿Por cuánto tiempo? ¿Qué datos se guardan? ¿Con qué motivo?

### 2.1.3 Mantenimiento

• ¿Hay procedimientos para asignar los usuarios a un grupo de acuerdo a ciertas características?
• ¿Hay procedimientos para dar de alta, baja, modificar, suspender, etc. una cuenta de usuario?
• ¿Se hacen revisiones de las cuentas de usuarios? ¿Se revisan sus permisos?
• ¿Hay procedimientos para determinar los nuevos requerimientos relacionados con cambios en funciones del empleado? ¿Cómo se mantienen actualizadas las cuentas cuando esto pasa?
• ¿Se documentan las modificaciones que se hacen en las cuentas? ¿Se lleva un histórico de los cambios?

### 2.1.4 Permisos

• ¿Tienen una clasificación de los recursos (datos) en base a la sensibilidad? ¿O en base a los tipos (base de datos, archivos de configuración, datos personales, según el departamento de la organización.)? ¿Cómo se define la sensibilidad de los objetos?
• ¿Tienen distinción de los tipos de accesos que tiene cada usuario a cada recurso? (lectura, escritura, etc.)
• ¿Quién les asigna los permisos a los usuarios?

### 2.1.5 ID inactivas

- ¿Después de qué período de inactividad en que el usuario no realiza acciones en el sistema, se limpia la pantalla asociada al usuario, se desconecta el usuario inactivo o pide la password de nuevo?
- Antes de terminar con la sesión, ¿se avisa al usuario que se lo desconectará?
- Si en un determinado tiempo el usuario no responde, ¿entonces se termina la sesión?
- ¿Después de qué período de inactividad (de cuantos días) se pone una cuenta de usuario como inactiva, porque el usuario no se ha logeado? ¿Este proceso es automático (del sistema operativo) o lo realiza el administrador?

### 2.1.6 Acciones correlativas a usuarios

• ¿Los usuarios se identifican en forma única o existen usuarios genéricos que todas las personas usan? ¿Todos los usuarios tienen un perfil o pertenecen a algún grupo?
• ¿El sistema genera históricos o logs de las actividades de los usuarios en el sistema, para poder seguirles el rastro?
• ¿Tienen forma de asignar responsabilidades individualmente a cada usuario, identificándolo a través de su ID?

### 2.1.7 Grupos - Roles

• ¿Existen grupos de usuarios? ¿Cómo se forman los grupos? ¿Según el departamento de la dependencia donde trabajen, según el rol que desempeñen? ¿Por qué esa clasificación?
• ¿El acceso puede controlarse con el tipo de trabajo o la función (rol) del que pide acceso?
• ¿Los ID hacen referencia a una persona, o son anónimos? ¿Hacen referencia a un grupo?
• ¿Se eliminan los que vienen por default en el sistema operativo? (Cuentas Guest, por ejemplo)

### 2.1.8 Súper usuario

• ¿Qué tipos de perfil de administrador hay?
• ¿Cuántas personas y quiénes son administradores?
• ¿Desde qué terminal puede acceder un administrador?
• Además de la cuenta de administrador, ¿tienen otra cuenta para las funciones comunes?

### 2.1.9 Display

• ¿Qué datos se muestran cuando alguien intenta acceder al sistema? ¿Se muestran los siguientes datos?
- Nombre de usuario
- Password
- Grupo o entorno de red

- Estación de trabajo
- Fecha y hora

• ¿Qué datos se muestran cuando alguien logra acceder al sistema? ¿Se muestran los siguientes datos?
- Fecha y hora de la última conexión.
- Localización de la última conexión (Ej. número de terminal)
- Intentos fallidos de conexión de ese ID de usuario desde la última conexión lograda.

### 2.1.10 Varios

• ¿Utilizan el ID de usuario como un control de acceso a los recursos, o solo para ingreso al sistema?
• ¿Un usuario puede tener solo una sesión abierta, de alguna aplicación, de acuerdo a sus tareas o puede tener varias? ¿Depende de la cantidad de grupos a los que pertenezca?

## 2.2 Autenticación

### 2.2.1 Datos de autenticación

• ¿Cómo se protegen los datos de autenticación cuando están siendo ingresados por el usuario? ¿Qué se muestra en pantalla cuando se teclea el password? ¿Espacios, asteriscos, no se mueve el cursor?
• ¿Cómo se guardan los datos de autenticación en disco? ¿Encriptados? ¿Bajo password? ¿De que forma se los asegura?
• ¿Cómo se restringe el acceso a estos datos? ¿Hay un control de acceso más severo con estos datos? ¿Se los clasifica como confidenciales?
• ¿Quién tiene acceso a estos datos?
• ¿Cómo se transfieren los datos de autenticación desde la terminal que se logea hasta el servidor encargado de autenticar? ¿Encriptados, o solo en texto plano?

### 2.2.2 Alcance de la autenticación

• ¿Que alcances tienen las autenticaciones? ¿Es una autenticación para una aplicación en particular, para toda la red, o solo para la LAN, y otra para la WAN?

### 2.2.3 Límites de los intentos de acceso al sistema

• ¿Se bloquea el usuario después de varios intentos fallidos de autenticación o se inhabilita la cuenta o la terminal?
• ¿Después de cuantos intentos?
• ¿Que se hace después de la inhabilitación: se espera un tiempo y muestra nuevamente la pantalla de acceso o el administrador debe aprobar la operación de re-acceso?

### 2.2.4 Firmas digitales

• ¿Se usan firmas digitales para autenticar a los usuarios dentro de la organización, cuando mandan mensajes internos? ¿Y para mensajes externos?
• ¿Serían necesarias para algún documento?

### 2.2.5 Varias

• Interoperatividad: ¿De qué forma se "ponen de acuerdo" Windows y UNIX para la autenticación? ¿Es necesaria esa interoperatividad para algo? ¿Es necesaria alguna herramienta para esta comunicación?
• Separación de tareas: ¿Se manejan los controles de acceso de manera que una sola persona no tenga acceso a todo, en relación a una sola transacción?
¿Existe separación de tareas a través del control de acceso?
• Rotación de tareas: si existe rotación de tareas, ¿cómo es el mecanismo en el control de acceso para posibilitar esto? ¿Se modifican los permisos? ¿O tienen todos los permisos necesarios permanentemente?
• Vacaciones: ¿son obligatorias las vacaciones en la empresa? Si es así, ¿cómo se manejan con las passwords durante los períodos de vacaciones? ¿Qué ocurre con la cuenta del administrador en el período de vacaciones? ¿Puede ser modificada? ¿Cómo controlan que no sea modificada durante su ausencia?

## 2.3 Passwords

### 2.3.1 Generación

• ¿Las passwords son generadas con procesos automáticos (programas de generación de passwords) o son creadas por los usuarios? ¿Se usan estos programas en alguna máquina, por ejemplo en los servidores?
• ¿Qué características deben tener estas passwords?
- ¿Cuál es el conjunto de caracteres permitidos (alfa, numéricos y caracteres especiales)?
- ¿Cuál es el largo mínimo y máximo del password (seis a ocho, preferentemente nueve)?
- ¿La password se inicializa como expirada para obligar al cambio?
- ¿De qué forma se hace cumplir este requerimiento? ¿Se pone una fecha de expiración? ¿No se permite al usuario acceder al sistema ya que su password ha expirado?

• ¿Se chequean contra un diccionario on line para verificar que no sean palabras que existan?
• ¿Se permite que contengan el nombre de la empresa, o el nombre del usuario?
• ¿Dos cuentas pueden tener las mismas passwords?
• Si existe más de una cuenta de administrador, ¿algunas de estas (o todas) tienen los mismos passwords?
• ¿El password puede ser igual al ID del usuario?

### 2.3.2 Cambios

• ¿Qué procedimiento existe para el cambio de las passwords de los usuarios? ¿Se puede cambiar en cualquier momento?
• ¿Quién puede hacer los cambios? ¿El administrador? ¿Los usuarios a través de una opción en el menú? ¿Le tienen que avisar a alguien cuando cambian la contraseña? ¿Tiene que pedir autorización?
• ¿Qué procedimiento existe para comprobar que las passwords asignadas por default (por el administrador o por el sistema operativo) han sido cambiadas por el usuario?
• ¿Cuál es el procedimiento para manejo de password perdidas o reveladas? ¿Cómo se cambian? ¿Solo se cambia la password o se cambia también la cuenta y el nombre del usuario?
• ¿Con qué frecuencia es necesario cambiar la password antes que se vuelva obsoleta?

• Al modificar la password de una cuenta, ¿se puede repetir la misma password?
• ¿Se guarda una base de datos con las últimas password de los usuarios? ¿Cuántas passwords de cada usuario se guardan?

### 2.3.3 Entrenamiento a usuarios

• ¿Se entrena a los usuarios en la administración del password? ¿Se les enseña a:
- no usar passwords fáciles de descifrar?
- no divulgarlas?
- no guardarlas en lugares donde se puedan encontrar?
- entender que la administración de passwords es el principal método de seguridad del sistema?

## 2.4 Control de acceso lógico

• Modelos de control de acceso: ¿Siguen algún tipo de modelo o mecanismo estándar de control de acceso? ¿Sería factible y económico implementar uno?
• Aplicación: ¿para el control de acceso usan una aplicación? ¿Cómo se administra? ¿Qué características tiene? ¿Esta aplicación es:

- Propia del sistema operativo?
- De aplicación y programas propios o comprados?
- Con paquetes de seguridad agregados al sistema operativo?

### 2.4.1 Criterios de acceso

¿Qué criterio usan para el control de acceso? ¿Alguno de los siguientes?:

• Identidad (ID de usuario)
• Roles
• Localización: ¿existen controles de acuerdo a la localización de la información?
• Recursos: ¿se pide un password cada vez que alguien quiera entrar a una carpeta compartida del servidor de UNIX? ¿El password que los usuarios ingresan para la aplicación de la dependencia sirve para explorar el sistema y así poder ver las carpetas de los servidores? ¿Es necesario poner otro password además del login?

• Tiempo: ¿se limita el momento del día (o del año) en el que un usuario puede entrar al sistema? ¿Cómo? ¿Que días, horas? ¿Con qué aplicación?
• Limitaciones a los servicios: ¿Existen restricciones de servicio? ¿Cómo?
• Modos de acceso:

- ¿Si el acceso es desde módem existen distintas permisos que desde terminal?
- ¿Se toma en cuenta el número de teléfono al comunicarse vía módem?
- ¿Usan un sistema call-back?

• Transacción: ¿se permite hacer ciertas transacciones a unos usuarios que otros no pueden hacer? ¿Dependiendo de qué? ¿Del tipo de usuario y del grupo?
• Aplicación: ¿se restringe el acceso a ciertos programas a ciertos usuarios? ¿Cómo?

### 2.4.2 Mecanismos de control de acceso interno

¿Cuáles de estos mecanismos de control de acceso se usan?

• Passwords
• Listas de control de acceso (ACL)

- ¿Existe una ACL o matriz, o algo similar donde se especifiquen los usuarios y los accesos que tienen?
- ¿Qué sería más conveniente, una lista o una matriz? ¿Por qué?
- ¿Con qué aplicaciones se manejan? ¿Con alguna del sistema operativo, o con otro software?
- ¿Cómo se actualiza? ¿En forma manual o, si se modifica la lista de usuarios del sistema, se actualiza automáticamente la ACL? ¿Con qué frecuencia se revisa y actualiza?
- ¿Se usa encriptación para almacenarla? ¿Se protege de alguna manera? ¿Qué sería lo mejor y por qué para protegerla?

• Interfaces de usuarios restringidas

- ¿Se restringen las interfaces que ven los usuarios, (como el escritorio de windows) de manera que los usuarios solo vean lo que les está permitido?
- ¿Cómo se hacen las restricciones? ¿Con la vista de menús?
- ¿Los usuarios solo ven una determinada vista o ciertas tablas de las bases de datos?

• Encriptación: ¿se encriptan algunos datos? ¿Cuales?

- ¿Las ACL?
- ¿Los mensajes?
- ¿Las passwords y datos de las cuentas de usuarios?
- ¿Los datos de configuración?
- ¿Los datos críticos de la empresa?
- ¿Los datos que están siendo transmitidos (internamente en la Lan o externamente a través de Internet o el módem)?

• Protección de puertos: ¿usan dispositivos externos físicos para proteger el puerto de los intrusos (llaves de hardware, por ejemplo)?

### 2.4.3 Control de acceso externo

• Mecanismos de control de acceso externo:

- Gateways (puertas de seguridad) o firewalls seguros
- Acceso de personal contratado, consultores o mantenimiento
- Autenticación basada en host: ¿existe una autenticación que da acceso al sistema basándose en la identidad del host que pide el acceso, y no en la identidad del usuario que quiere entrar?

• ¿Existe acceso externo a los datos, desde Internet o desde el módem? ¿Quién tiene ese acceso?
• ¿Qué procedimientos se tienen en cuenta para mantener la integridad y la confiabilidad de los datos? ¿Se tienen en cuenta los siguientes?

- ¿Alguna forma de identificación o autenticación?
- ¿Control de acceso para limitar lo que se lee, ve, borra, modifica, etc.?
- ¿Firmas digitales?
- ¿Ponen las copias de seguridad de la información pública, en otro lado, no en la misma máquina?
- ¿Prohíben el acceso público a bases de datos "vivas" (live data base o bases de datos)?
- ¿Verifican que los programas y la información pública no tenga virus?
- ¿Passwords one-time?
- ¿Están separados los datos que se publican en Internet de los datos del interior de la empresa?

- ¿Son los mismos datos o están en PC's diferentes?
- ¿Usan alguna forma de acceso remoto para cambiar las configuraciones de un sistema?

## 2.5 Sistema de detección de intrusos

• ¿Ha habido intentos de intrusión? ¿Vale la pena implementar un sistema como estos?
• ¿Se usa algún software de IDS? ¿Son tolerantes al fallo? ¿Usan muchos recursos?
• ¿Se usan herramientas de monitorización de red para encontrar intrusos?
• ¿Se releen los logs de auditoria buscando pistas de IDS? ¿Se buscan algunas de las siguientes?

- Muchos intentos fallidos de autenticación,
- Tráfico excesivo de red,
- Muchas violaciones a permisos.

• Si hubiera una entrada de un intruso, ¿se documenta? ¿Que medidas se tomarían (o tomaron) para que no ocurra más?

## 2.6 Denial of Service

• ¿Se llevan a cabo algunas de las siguientes actividades?

- ¿Instalan ACL en los routers?
- ¿Quitan los servicios de red no necesarios o no utilizados, por ejemplo: ECHO, etc.?
- ¿Separan los datos críticos de los que no lo son, a través de lo que haya disponible, como por ejemplo: sistemas de cuotas (disk QUOTAS, o particiones, o volúmenes)?
- ¿Establecen valores base para la actividad normal, en cuanto a memoria, utilización de disco, de la CPU o tráfico de red?
- ¿Usan herramientas para detectar cambios en la configuración o en los archivos?
- ¿Usan configuraciones redundantes de red y tolerantes a fallos?

**3 Seguridad de las comunicaciones**

## 3.1 Configuración de red

### 3.1.1 Activos de la red

• ¿Cómo es la topología de la red? ¿Existe un inventario o gráfico topológico?
Debería incluir lo siguiente:

- switch
- routers
- hub's
- modem
- PC's
- conexiones de radio
- fibra óptica
- etc.
- ¿Cuantos dispositivos de esta lista hay y en que forma están ubicados y utilizados?
- ¿Qué filtros tiene cada uno de estos dispositivos?
- ¿Existe encriptación a nivel de hardware?

• ¿Por qué pusieron un switch en lugar de un router? ¿Por el costo? ¿Por el tamaño de la red?
• ¿Por qué implementaron un sistema radial? ¿Es demasiado inseguro? ¿No es muy caro?

### 3.1.2 Comunicaciones

• Con respecto al MODEM con el que se comunican con la dependencia:

- ¿Pasa por el firewall?
- ¿Los datos van encriptados?

• ¿Se realizan los controles de acceso adecuados a los servidores que se encuentran conectados a Internet?

### 3.1.3 Recursos compartidos

• ¿Se comparten los discos de las PC's en la red? ¿Por que?

- ¿Que carpetas comparten?
- ¿Se pueden ver las carpetas de los mails de mis compañeros?
- ¿Tienen contraseñas estas carpetas? ¿Quién pone las contraseñas: el dueño de la información o el administrador?

### 3.1.4 Configuración de puertos

• ¿Se deshabilitaron los puertos que no son necesarios? ¿Cuáles? ¿De qué protocolos o servicios? ¿Quién lo hizo?
• ¿Se prueban los puertos de la red? ¿Y el firewall? ¿Con qué herramientas?
• ¿Se ha hecho una prueba de auto hackeo?
• ¿Con qué herramientas se prueban o pueden probar los puertos? ¿Solo con el SQuid? ¿Por qué no usaron otro programa?

### 3.1.5 Testeo mensual de la red

• ¿Se hace algún chequeo periódico de la red y sus permisos?
• ¿Qué se controla?
• ¿Se documentan la ejecución y los resultados de estas pruebas?

### 3.1.6 Acceso remoto

• ¿Cómo se mantienen las máquinas con UNIX? ¿Vía acceso remoto? ¿Quién las mantiene?
• ¿Qué herramientas se usan? ¿Cómo funciona la herramienta?
• ¿Se debe cambiar la configuración del firewall para hacer este acceso remoto?
• ¿Qué servicios son necesarios para el mantenimiento (HTML, FTP, IP, DNS, TELNET)? ¿El firewall no tiene restricción en ese servicio, se le saca la restricción del servicio al firewall o solo habilito una dirección específica, la de la máquina desde donde se hace el mantenimiento?
• ¿Qué es lo que se mantiene con este sistema?

### 3.1.7 Medidas de fiabilidad

• ¿Existen medios alternativos de transmisión de datos en caso de que exista alguna contingencia con la red? ¿Que se haría si se cae un nodo? ¿Está prevista esa situación?
• ¿Existe una redundancia de acceso a Internet? (si no funciona ADSL tener un dial up configurado)

### 3.2.3 Espacio en disco

• ¿Cómo se administra la capacidad de disco?

- ¿Se asigna un espacio de disco a cada departamento?
- ¿Existen distintas cantidades asignadas a los usuarios de acuerdo a su perfil o grupo, o todos los usuarios tienen la misma cantidad de espacio en disco?

• ¿Que pasa si se llega al límite de espacio en disco asignado? ¿Ha pasado alguna vez? ¿Se le avisa al usuario correspondiente que limite el uso de su cuenta?
• ¿Cuando se ha llenado el servidor o antes, para poder hacer algo para vaciarlo?
• ¿Existe un límite para los mensajes de salida o de entrada?

### 3.2.6 Chat

• ¿Se permiten los servicios de chat?
• ¿Cuáles se usan? MSN, ICQ, Yahoo! ¿Chat? ¿Otros?
• ¿Se permite bajar archivos a través de estos programas?
• ¿Se usan programas de file sharing (Morfeus, Kazaa, Napster, Audio Galaxy, iMesh, eDonkye2000, etc.)?

### 3.2.7 Copia de seguridad

• ¿Se genera una copia de seguridad de los mensajes enviados y recibidos? ¿De todos? ¿Se guardan en el disco? ¿Se comprimen?
• ¿Se hacen back up de las carpetas del SendMail (como las dbx del Outlook Express)?

• ¿Se imprimen para su control o para que conste en algún archivo en papel?
• ¿Poseen un sistema propio de mail record definido o alguna herramienta automática de gestión de mails record?

### 3.2.8 Privacidad – Firma digital – Encriptación de mails

• ¿Prohíben el envío de archivos de la empresa u otros documentos confidenciales vía mail?
• ¿Se toman medidas de seguridad especiales cuando el mensaje de salida tiene datos confidenciales? ¿Se exige que vaya firmado, o encriptado? ¿Se exige que la dirección de destino sea conocida o confiable?
• ¿Se utiliza la firma digital en algún tipo de mensajes? ¿Qué tipo de firma se usa?
• ¿Se usa para mensajes externos e internos?
• ¿La clave privada de la firma digital es realmente privada, o la utilizan las secretarias (por ejemplo) para mandar mensajes en nombre de sus jefes? ¿Cómo se controla esto?
• ¿Utilizan la priorización de mail para la encriptación de los mismos?
• ¿Que sería importante proteger, en el caso de mensajes internos y externos?:

- ¿Integridad?
- ¿Confidencialidad?
- ¿No repudio?
- ¿Autenticación del remitente?

• ¿Se pide generalmente una confirmación de lectura en los mails salientes? ¿En todos, solo en los que tienen datos confidenciales, o cuando el usuario los configura?
• ¿Se encriptan los datos confidenciales que se guardan en disco (ejemplo: EFS?

- Encrypted File System - de Microsoft)?
- ¿Archivo con contraseñas?
- ¿Archivos de configuración?
- ¿Archivos top secret?
- ¿Qué otros datos se encriptan?

## 3.3 Virus - Antivirus

### 3.3.1 Herramientas

• ¿Cuáles de éstas medidas o herramientas poseen para evitar los virus?

- Paquetes de software antivirus
- Firewalls
- Sistemas de detección de intrusos
- Monitorización para evaluar el tráfico de red y detectar anomalías, como la acción de troyanos.
- Creación de un disco de rescate o de emergencia
- Procedimientos para cuando ocurra una infección con virus.
- Hardware de seguridad de red dedicado
- Back up de datos

• ¿Está habilitada alguna herramienta antivirus mientras se envían y reciben mails? ¿Cuál? ¿Por qué se usa esa?
• ¿Están seguros que detecta los virus y los elimina correctamente?
• ¿Han probado con otra herramienta?
• ¿Qué precio tiene el antivirus que compran? ¿Y las actualizaciones?
• ¿Hay un antivirus instalado en cada PC (incluyendo los servidores) o hay un solo antivirus en toda la red?
• ¿Que significa que el antivirus sea corporativo? ¿Uno para los servidores y otra versión para los clientes? ¿En qué se diferencian?

### 3.3.3 Actualización de antivirus

• ¿Cómo se actualizan las definiciones de virus? ¿Quién las baja de Internet? ¿Quién ejecuta las actualizaciones en la PC's? ¿Cómo se enteran de las nuevas actualizaciones de virus?
• ¿Cuánto tiempo lleva diseminar y actualizar el antivirus en toda la organización?
• ¿Se hacen chequeos ocasionales para ver si se han actualizado los antivirus?

## 3.4 DOCUMENTACIÓN – NORMAS

• ¿Qué documentación existe de la red?
- ¿Diagramas topológicos?
- ¿Procedimientos?
- ¿Manuales?
- ¿Certificados (Ej.: de calidad, etc.)?
- ¿Licencias de software?
- ¿Planes de contingencia, de seguridad, etc.?
- ¿Contratos (Ej.: responsabilidades y mecanismos de transmisión al establecer una comunicación con las fábricas)
- ¿Cambios realizados en la configuración de la red?
- ¿Qué mas?

• ¿Poseen cada uno de estos elementos de documentación de la empresa?:

- Manual de uso del software y de hardware usado (del software desarrollado y del comprado).
- Diagramas de red y documentación de la configuración de routers, switches y dispositivos de red.
- Procedimientos de emergencia (plan de contingencia)
- Plan de seguridad
- Manual de procesos estándares del Sistema Operativo (en especial de UNIX)
- Métodos para compartir datos entre sistemas (por ejemplo con las dependencias o entre las PC´s de la red)

• ¿Se han instalado correctamente todos los parches de seguridad disponibles del sistema operativo y de los programas usados? ¿Cómo se conoce de los parches? ¿Están suscriptos a un mailing list?
• ¿Hay alguna documentación donde se anote la configuración de las PC´s en la red? ¿Sus números IP, sus placas de red, etc.?

## 3.5 ATAQUES DE RED

• ¿Han tenido algún ataque en la red?
• ¿Que se ha hecho para arreglarlo?
• De los siguientes métodos contra los ataques más comunes, ¿qué está implementado?

- Denial of service:

- ¿Hay herramientas Anti DoS?
- ¿Limitan el tráfico de red?
- ¿Se hizo alguna simulación ocupando una gran cantidad de recursos de algún tipo?
- ¿Instalan los parches de seguridad del sistema operativo?
- ¿Implementan un sistema de cuotas (Disk Quotas)?
- ¿Utilizan alguna herramienta para detectar cambios en la información de configuración u otros archivos (como Tripwire)?

**-** Sniffing:

- ¿Las líneas de comunicación se segmentan tanto como sea práctico?
- ¿Los datos de firma al sistema y otros datos sensibles son transmitidos encriptados?
- ¿Las cuentas privilegiadas (como root) se logean usando passwords one time o shadow passwords, y autenticación fuerte?

- Spoofing:

- ¿Tienen alguna herramienta anti-spoofing?
- ¿Los routers son configurados para que rechacen los ataques de spoofing?
- ¿Solo los hosts apropiados son definidos como confiables en el Linux (como el /etc/hosts.equiv)? ¿Y este archivo tiene los permisos restringidos?
- Por más que el acceso externo esté prohibido, ¿se configura el control de acceso para denegar cualquier tráfico de la red externa que tiene una dirección fuente que debería estar en el interior de la red interna?

**-** Ataque a las passwords:

- ¿Donde se guardan las password del sistema operativo? ¿En el archivo /etc/passwd y /etc/group?
- ¿Se chequean regularmente las passwords para comprobar su consistencia los archivos que nombré arriba?

### 3.6 Flirewall

• ¿Qué firewall usan?
• ¿En que máquina (servidor) se encuentra el Firewall? ¿En una máquina dedicada? ¿En el servidor de Internet?

### 3.6.1 Tipos de firewall

• ¿Qué tipo de firewall hay?
- ¿Gateway de filtrado de paquetes (Packet Filtering Gateways)?
- ¿Gateway de aplicación?
- ¿Gateways híbridos o complejos?
- ¿Otro?

### 3.6.2 Política de configuración

• ¿En base a que criterios definieron las configuraciones del firewall?
• ¿Tienen una política definida en cuanto a la configuración del firewall?
• ¿Usan una política de acceso a servicios?
• ¿Usan una política de diseño y configuración del firewall? ¿Alguna de estas dos?:
- Postura de negación preestablecida: se especifica sólo lo que está permitido y se prohíbe todo lo demás:
  - ¿Se examinan los servicios que los usuarios necesitan?
  - ¿Se considera como afectarían la seguridad tales servicios y como se los puede proporcionar a los usuarios de manera segura?
  - ¿Se permiten sólo los servicios que se comprenden o se tiene experiencia, que se pueden proporcionar con seguridad y para los cuales existe una necesidad legitima?
- Postura de permiso preestablecido: se especifica sólo lo que está prohibido y se permite todo lo demás.

### 3.6.3 Características del firewall

• ¿Qué controles de acceso tiene el firewall? ¿Que servicios tiene habilitados y cuáles deshabilitados?
• ¿Soporta autenticación? ¿Con qué técnica? ¿Y passwords?
• ¿Que habilidades tiene para monitorizar la red? Incluye:

- ¿Intentos no autorizados de ingreso?
- ¿Genera logs?
- ¿Provee reportes? ¿O mails?
- ¿Tiene alarmas?

• ¿Es lo suficientemente rápido para que no demore a los usuarios en sus intentos por acceder a la red (cómo es su performance)?
• ¿Qué tan configurables son sus opciones?
• ¿Puede adaptarse a distintas configuraciones de red o de sistemas (es escalable)?
• ¿Es fácil de configurar?
• ¿Es fácil de usar?
• ¿Es fácil de mantener?
• ¿Tiene un buen servicio postventa?
• Si se cae el firewall, ¿que pasa? ¿Es una "falla segura"?
• ¿Se hizo alguna prueba de la configuración del firewall? ¿Trató de hacerse un intento de entrada sin autorización, por ejemplo?

## 3.7 Configuración de servicios y protocolos de red

• De todos estos servicios:

- ¿Cuáles se usan en la red?
- ¿Cómo están configurados?
- ¿Están habilitados o prohibidos?
- ¿Existen excepciones?
- ¿Poseen acceso de entrada y/o salida?
- ¿Que pasa con los otros puertos que quedan libres?

• ¿Se desactivan completamente los siguientes servicios o protocolos?

- RLOGIN, RSH, REXEC (Comandos "r" Remote), SU (SuperUser), NetStar, GOPHER, TFTP (Trivial File Transfer Protocol), Telnet, SYSTAT, FINGER, TALK, EXPN, VFRY.

• ¿Cómo se configuran los siguientes servicios o protocolos?

**-** POP (Post Office Protocol), MIME, HTTP, SMTP, FTP, Applets, Pruebas Cgi, Scripts Query, SHELL, NIS.

### 3.8 Herramientas para la administración de red y protocolos

• ¿Usan alguna de estas herramientas o protocolos para la seguridad de la red?

- Tcp-wrappers, Netlogv, Satan, AntiSniff, Cops, SafeSuite, Gabriel, Courtney, Tcplist, SSL (secure socket layer), SHTTP, SMIME, NOCOL (Network Operations Center On-Line).

• ¿Las herramientas que se usan tienen las siguientes funciones?

**-** ¿Pueden monitorear y filtrar peticiones entrantes a distintos servicios? ¿Cómo lo hacen? ¿Con qué aplicación?
**-** ¿Indican la hora, la máquina origen (el número de IP) y el puerto de esa conexión?
**-** ¿Pueden seguir una traza de todos los intentos de conexión tanto admitidos como rechazados?
**-** ¿Se monitorea la red buscando ciertos protocolos con actividad inusual? Se controlan los siguientes:

- Conexiones tftp,
- Acesos vía rsh (remote shell),
- Comandos en el puerto de sendmail como vrfy, expn, etc.
- Algunos comandos de rpc (remote procedure call) como el rpcinfo,
- Peticiones al demonio de mountd.

• ¿Se llevan estadísticas de uso de los protocolos?
• ¿Se puede utilizar para detectar cambios en los patrones de uso de la red, y todo aquello que nos puedan hacer sospechar que algo raro está pasando en la misma?
• ¿Se audita el tráfico IP?
• En la captura de paquetes IP, ¿se le puede especificar condiciones de filtrado como protocolos específicos, nombres de máquinas, etc.?
• ¿Tienen la posibilidad de filtrar paquetes Por hardware o por software?
• ¿Van creando una base de datos de todas las máquinas chequeadas y las va relacionando entre ellas (Satan es una herramienta que hace esto)?

• ¿Qué otra funcionalidad no nombramos que si tiene la herramienta usada? ¿Que función sería muy útil al trabajar en la red?
• ¿Se mantiene actualizado el software? ¿Se investiga para mantener actualizadas las herramientas? ¿Alguien está a cargo de esta actividad?
• ¿Se buscan herramientas nuevas que faciliten la tarea? ¿Consultan a algún Organismo (como el CERT)?

**4 – Seguridad de las aplicaciones**

## 4.1 Elección de sistema a usar

¿Se hicieron los siguientes cuestionarios al elegir los sistemas operativos y programas usados en la empresa? ¿Qué respuestas tenían?

- Para todo tipo de sistemas se debe tener en cuenta los siguientes requisitos:
  - Requerimientos funcionales: ¿qué funciones debe cumplir el sistema?
  - Entorno necesario: ¿Windows, Unix o Linux?
  - Requerimientos de compatibilidad: ¿se ajusta a estándares o a regulaciones internacionales, o a programas existentes en la dependencia?
  - Requerimientos de performance: respuestas por segundo, errores, etc.
  - Requerimientos de interoperatividad: ¿cómo se relaciona con los demás sistemas?
  - Fiabilidad: errores tolerables del sistema
  - Amigable: fácil de usar.
  - Precio y precio adicional de mantenimiento
  - Documentación y manuales propios del software

- Además hay que tener en cuenta los siguientes requisitos de seguridad

  - Identificación y autenticación,
  - Control de acceso,
  - Login,
  - Evaluación de protocolos,
  - Incorruptibilidad,
  - Fiabilidad,
  - Seguridad en la transmisión,
  - Back up de datos,
  - Encriptación,
  - Funciones para preservar la integridad de datos,
  - Requerimientos sobre privacidad de datos.

### 4.2 Control de datos y aplicaciones

• ¿Existe un control de cambios para los archivos del sistema o para las bases de datos de la empresa, como por ejemplo una base de datos, que se modifique cada vez que alguien haga una modificación sobre un archivo?
• ¿Existen restricciones de datos de salida, por ejemplo al portapapeles o a la impresora, y otros?
• ¿Cómo es el acceso a las librerías de programa (o a la carpeta "Archivos de programa")?
• ¿Se generan logs en cada transacción de manera de poder hacer un "undo"? ¿Estos registran los cambios en los datos críticos del sistema?
• ¿Se generan históricos de auditoria indicando qué procesos se corrigieron, quién los corrigió y qué cambios hizo (control de cambios – gestión de configuración)?
• ¿Los archivos de programa y los de trabajo se almacenen en directorios separados?

### *4.3 Control de datos en el desarrollo*

• ¿Se asegura la integridad, exactitud y validez de los datos de entrada y salida de las aplicaciones?
• ¿Las variables, parámetros y / o fórmulas de cálculo se incluyen en tablas o archivos separados de los programas, para facilitar su modificación?
• ¿Existe un proceso de control de cambios para el desarrollo? ¿Cómo se documentan estos cambios?
• ¿Controlan el contenido de los archivos de entrada? ¿Controlan que existan los archivos antes de ejecutar el programa?
• ¿Se hacen controles sobre la validez de los datos ingresados manualmente? (Controles de integridad de datos)
• ¿Se controla la consistencia de los datos de salida de las aplicaciones?
• ¿Las aplicaciones se operan a través de menús obligatorios o es a través de comandos del sistema? ¿Los operadores de estas aplicaciones pueden editar los datos reales del mismo (o sea las bases de datos)?

### 4.4 Seguridad de base de datos

• ¿Los archivos de la base de datos tienen control de acceso? ¿O solo se hacen controles en las aplicaciones?
• ¿Se controlan las siguientes ocurrencias?

- tiempo y duración de los usuarios en el sistema,
- número de conexiones a bases de datos,
- número de intentos fallidos de conexiones a bases de datos,
- ocurrencias de deadlock con la base de datos,
- estadísticas de entrada-salida para cada usuario,
- generación de nuevos objetos de bases de datos,
- modificación de datos.

• ¿Se hace algún chequeo regular de la seguridad de la base de datos? ¿Se documentan los chequeos incluyendo lo siguiente?

- ¿Se hacen y son efectivos los backups y los mecanismos de seguridad?
- ¿Hay algún usuario de la base de datos que no tenga asignado un password?
- ¿Hay algún usuario que no ha usado la base de datos por un período largo de tiempo?
- Además del administrador de datos, ¿quién tiene acceso a los archivos del software de base de datos, a los del sistema operativo y a las tablas del sistema ?
- ¿Quién puede ejecutar un editor SQL?
- ¿Quién tiene acceso de lectura – escritura a los archivos de programa?
- ¿Qué usuarios tienen los mismos permisos que el administrador?
- ¿La base de datos tiene suficientes recursos libres para trabajar?

• ¿Se borran físicamente los registros de las bases de datos cuando un usuario los elimina, o se marcan como "borrados"?

### 4.5 Control de aplicaciones

• ¿Todas las máquinas de la empresa tienen los mismos programas con las mismas versiones? ¿Existe un estándar de configuración de PC´s a seguir? ¿Usan alguna herramienta como el Norton Ghost para copiar la configuración de las PC's?
• ¿Existe un procedimiento para instalar las aplicaciones en las máquinas de los usuarios?
• ¿Quién los instala y administra?
• ¿Existen controles para realizar la instalación o la actualización de parches de las aplicaciones?
• ¿Cómo se documenta la instalación o actualización del software que se instala en las máquinas?
• ¿Existe algún procedimiento para encontrar programas que no deberían estar en las máquinas de los usuarios, ya sea por problemas de licencias o virus?
¿Existe un método a seguir? ¿Se usa algún producto para detectar estos programas? ¿Se hacen auditorias periódicas para verificar?
• ¿Cómo se controla a los usuarios y las aplicaciones que bajan de la web?
¿Cómo controlan que éstas tengan las licencias correspondientes (esto puede terminar en un problema para la empresa)? ¿Se borran las versiones de prueba (trial version) o demos cuando expiran?
• ¿Se permiten los registros on line de las aplicaciones?
• ¿Existen métodos para autorizar y registrar software?
• ¿Cómo manejan las actualizaciones del software?
• ¿Existe alguna forma de configurar las PC´s de manera que no se pueda instalar software nuevo sin autorización del administrador?

### 4.6 Mantenimiento de las aplicaciones

• ¿Cómo se etiquetan y almacenen los instaladores de los programas o los drivers? ¿Se almacenan en disco duro, en disquete, en CD, en cinta?
• ¿Existe algún tipo de mesa de reportes donde los usuarios con incidentes de seguridad pueden recibir ayuda o realizar un reporte?
• ¿Se controla el funcionamiento correcto de las aplicaciones? ¿Se hacen chequeos periódicos sobre el funcionamiento, la configuración, etc.? ¿Se generan alertas?
• ¿Cómo se administran las emergencias?
• ¿Si se hacen cambios de emergencia, cómo se documenta?

• ¿Se borran los archivos de las carpetas temporales, para que no se llenen los discos de basuras y provoquen la caída del sistema?
• ¿Se revisan periódicamente los sistemas para eliminar los programas o servicios innecesarios (como algunos servicios web, FTP, http)? ¿Se buscan vulnerabilidades nuevas durante estas revisiones?
• ¿Es automático el método de actualización de los Antivirus para que los mensajes internos en el interior y el exterior de la organización no propaguen virus? ¿Se programan los escaneos automáticos de virus una vez por semana? ¿Por qué no la actualiza la aplicación automáticamente con un schedule?
• ¿Existe alguna aplicación de gestión para tomar decisiones de alto nivel gerencial? ¿Esta obtiene datos automáticamente de las bases de datos?
• ¿Existe un undelete como la Papelera de Reciclaje de Norton? ¿En el servidor o en las PC´s?
• ¿Se hace un back up de la configuración de los sistemas antes de hacer algún cambio de manera de poder hacer un undo?
• ¿Los cambios complejos en los archivos de configuración se hacen primero (a modo de prueba) en una copia de los archivos o se hacen directamente en la configuración original?
• ¿Se registran o documentan los cambios hechos a una configuración?

### 4.7 Ciclo de vida

• ¿Qué aplicaciones se desarrollaron en la dependencia? ¿Una para cada área de la empresa?
• ¿Qué metodología estándar usan para el desarrollo de sistemas? ¿De qué fases consta? ¿Qué mecanismos de seguridad manejan durante estas fases?

### 4.7.1 Iniciación

• ¿Cómo se expresan las necesidades del sistema?

### 4.7.2 Desarrollo

• ¿Se hace un análisis de riesgos antes de empezar con el desarrollo?
• ¿En caso de que haya participación de terceros en el desarrollo (como en la web, o en UNIX) el código fuente queda en la empresa? ¿Dejan documentación? ¿Tienen alguna reglamentación para trabajar con terceros?

• ¿Usan métricas durante el desarrollo? ¿Les sirven? ¿Qué miden? ¿En qué las utilizan?
• ¿Se mantienen registros históricos de las modificaciones llevadas a cabo en los sistemas durante el desarrollo y el mantenimiento? ¿Qué se guarda?

- sistema que afecta,
- fecha de la modificación,
- persona que realizó el cambio,
- descripción global de la modificación,
- ¿Qué mas?

• ¿En qué momento se definen los requisitos de seguridad de un sistema? ¿Es durante el desarrollo?

### *4.7.3 Implementación*

• ¿En qué lenguajes se implementan los sistemas? ¿Reusan software?
• ¿Qué medidas de seguridad toman durante la implementación?

### *4.7.4 Prueba*

• ¿Cómo se hace la prueba de los sistemas?
• ¿Se generan planes de prueba?
• ¿Qué tipos de prueba se llevan a cabo? ¿De unidad? ¿De integración? ¿Por módulos? ¿Por sistema?
• ¿Se generan escenarios de prueba para el testeo?
• ¿Se documentan las pruebas y sus resultados? ¿Qué datos se guardan?
• ¿Cómo se realiza el control de cambios del sistema?

### 4.7.5 Instalación y mantenimiento

• ¿Qué metodología usan para el mantenimiento?

### 4.7.6 Documentación

• ¿Qué documentación generan de los desarrollos que hacen? ¿Se incluyen las siguientes cosas?

- Generalidades del sistema, incluyendo fecha de implementación y analista / programador responsable.
- Documentación del sistema, incluyendo sus objetivos, diagramas general y de funciones y diseños de registros.
- Documentación de los programas, incluyendo objetivos, diagrama de flujo y archivos de entrada y salida que utiliza.
- Manual de operación, que contenga el diagrama de flujo general de procesamiento donde se identifiquen los procesos que deben haber finalizado y las interfaces de entrada que se deben haber cubierto como paso previo a la ejecución de cada proceso, los procedimientos de supervisión, seguridad y control sobre los procesos y los pasos a seguir ante la ocurrencia de errores.
- Manual de usuario.
- Manual de características de seguridad.
- Descripción del hardware y software, políticas, estándares, procedimientos, backup, plan de contingencia, descripción del usuario y del operador del sistema.

## 5. Seguridad física

### 5.1 Control de acceso al centro de cómputo

• ¿Se hizo un análisis costo beneficio a la hora de implementar los controles? ¿Cómo se asesoraron?
• ¿Se restringe el acceso al centro de cómputo a la gente que no pertenece a esa área?
• ¿Existen algunos de los siguientes métodos? ¿Dónde?

- tarjetas de entradas,
- guardias de Seguridad,
- llaves Cifradas (Looked Door),
- circuito cerrado de televisión.

• ¿Cuál es la función de la doble puerta en la entrada?
• ¿Qué tipos de autenticación se utilizan en la empresa? Hay cuatro formas:

- con algo que el individuo sabe (password, PIN, etc.),
- algo que el individuo procesa (un token, una smart card, etc.),
- algo que el individuo es (controles biométricos),
- algo que sabe hacer (como los patrones de escritura).

• ¿Por qué no usan las otras? ¿Por el costo? ¿No vale la pena?
• ¿Solo dejan entrar a aquellos que lo necesiten? ¿Les hacen algún control de seguridad?

### 5.2 Control de acceso a equipos

¿Cómo se controlan los siguientes accesos?

• ¿La BIOS tiene habilitada una contraseña?
• ¿Las PC's tienen habilitados los dispositivos externos, como la disquetera o la lectora de CD? ¿Cómo se controlan estos dispositivos?
• ¿Cómo se controlan los virus en las disqueteras o CD's? ¿Qué otros peligros pueden tener?
• ¿Son dispositivos booteables (se permite desde el setup de la máquina el booteo con estos dispositivos)?
• ¿Ha habido robo de datos usando estos dispositivos?
• ¿Existen copiadoras de CD's en la empresa? ¿Quién tiene acceso a ellas? ¿En qué máquinas están?
• ¿Usan llave de bloqueo en las CPU´s?

• ¿Las CPU´s y dispositivos externos extraíbles están guardados con llave?
• ¿Existe algún control sobre los terceros que realizan el mantenimiento?
• ¿Existen entradas no autorizadas en las PC's, como puertos no usados y no deshabilitados?
• ¿Puede alguien enchufar e instalar una impresora u otro dispositivo (un zip o un disco removible) en alguna máquina?
• ¿Cómo se realiza el control sobre los dispositivos que se instalan en las PC´s? ¿Se hace una revisión periódica de los mismos? ¿Quién las hace? ¿Cada cuanto? ¿Qué buscan?
• ¿Se apagan los servidores en algún momento? ¿Es necesario que queden prendidos las 24 hs.?

### 5.3 Utilidades de soporte

¿Existen, se mantienen y revisan todos estos aparatos periódicamente en busca de fallas?

• Aire acondicionado (18º C a 20º C)
• Calefacción
• Humidificador en la biblioteca de cintas y centro de cómputos
• Luz de emergencia en el centro de cómputos
• Detectores de humo, agua y calor
• Instalación de alarmas:

- contra fuego,
- humo,
- calor,
- intrusos,
- agua,
- ¿Qué otras hay?

• Servidor de repuesto o redundante
• UPS (Uninterruptible power supply) ¿para mantener los servidores de red funcionando por cuántas horas? ¿Cuántos UPS? ¿En qué máquinas?
• Estabilizador de tensión: ¿cuántos? ¿En qué máquinas?
• Extinguidotes de incendio:

- ¿Son los adecuados?
- ¿Son manuales o automáticos (rociadores)?
- ¿Se corta la energía eléctrica cuando se activan estos rociadores?
- ¿Están en el lugar correcto? ¿En qué lugares? ¿Cómo eligieron el lugar?

- ¿Se revisan las posibles fallas eléctricas o posibles causas de incendio?
- ¿Qué pasa con las máquinas cuando cae la lluvia artificial? ¿Existen cubiertas plásticas para protección de agua?
- ¿Qué pasa con los extinguidotes de incendio en el centro de cómputos?

• ¿Hay una sola red eléctrica?
• ¿Hay un dispositivo que evite la sobrecarga de la red eléctrica?
• ¿Hay hardware especial de aislamiento y protección de dispositivos magnéticos?

## 5.4 Estructura del edificio

• ¿Se tuvo en cuenta la seguridad de los datos y equipos en el momento de hacer la estructura de los edificios? ¿O se hizo primero la red y luego el edificio?
• Centro de cómputos:
- ¿Está ubicado en pisos elevados (para prevenir inundaciones)?
- ¿Existe un piso o techo falso para pasar el cableado por debajo de él? ¿El área debajo del piso o del techo falso es fácilmente accesible?
- ¿Es lo suficientemente grande, anticipándose al crecimiento de la red y predispuesto a reinstalaciones?
- ¿La localización del centro de cómputos, tiene paredes externas o ventanas?
- ¿Está cera del (backbone) caño central de la red?
- ¿Esta permitido comer, fumar y beber dentro del centro de cómputos?
- ¿En el resto de los escritorios se puede?

• Cableado:

- ¿Usan cableado estructurado? ¿Quién lo instaló? ¿Tercerizaron la instalación?
- ¿Usaron alguna norma para hacer el cableado?
- ¿Se tuvo en cuenta el lugar de los canales de red, de manera que no sean afectados por desastres como inundación, cortes eléctricos, problemas de desagües o campos magnéticos?
- ¿Que tipo de cable usan para que no haya interferencias?
- ¿Qué medidas toman para las interferencias?
- ¿Cómo previenen los daños o cortes en los cables?
- ¿Cómo calcularon el ancho de banda de la red? ¿Es suficiente?

- ¿Bocas de red: son suficientes? ¿Hay de más? ¿Cómo protegen a las que sobran? ¿Están habilitadas o no? ¿Cómo las deshabilitan?

• ¿Se conoce por donde van las cañerías de manera que no interfieran con la red?
• ¿El local se sitúa encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas?
• ¿Esto causa molestias o interferencias?
• ¿Existe un interruptor de energía de emergencia en la puerta de salida?
• ¿Los muebles son de madera? ¿Son inflamables?

## 5.5 Interceptación física, visual y electromagnética

• ¿Puede haber emisiones electromagnéticas desde los monitores o desde los cables UTP, que se pueden interceptar o provocar ruidos?
• Emisiones visuales: ¿se evita que los monitores puedan verse a través de las ventanas?
• Emisiones de sonido (ruido): ¿se toma alguna medida para que no afecten el funcionamiento normal? ¿Hay ruidos que puedan causar problemas? ¿La ubicación de las antenas de radio interfiere con los datos de alguna manera? ¿No son necesarias las cortinas de aluminio para aislar de ruido a las señales? ¿Usan algún otro tipo de aislamiento en algún lado?

### 5.6 Emergencias

¿Cómo se procede en caso de una emergencia?

- Error físico de disco de un servidor,
- Error de memoria RAM,
- Error de tarjetas controladoras de disco,
- Incendio total o factores catastróficos,
- Durante y después de la situación de emergencia, ¿se controla el acceso al centro de cómputos?

### 5.7 Clasificación de datos y hardware

- ¿Existen procesos para rotular, manipular y dar de baja la computadora, sus periféricos y medios de almacenamiento removibles y no removibles? ¿Cómo son estos procesos? ¿Con qué se rotulan los dispositivos?
- ¿Tienen un inventario de recursos de hardware y software? ¿Existe documentación sobre los dispositivos instalados en cada máquina, su configuración, modificación, forma de mantenimiento, versión, etc.?

  - ¿Cómo se guarda? ¿Es una planilla?
  - ¿Dónde se almacena?
  - ¿Quién lo actualiza?
  - ¿Cada cuanto?

### 5.8 Backup

- ¿Con qué frecuencia hacen los backups?
- ¿Qué datos se almacenan? (datos y programas de aplicación y de sistemas, equipamiento, requerimientos de comunicaciones, documentación)

  - Software de base y su configuración:

    - ¿Se hacen discos de inicio de Windows?
    - ¿Hay imágenes Ghost de las máquinas?
    - ¿Se hacen backups de la configuración de red?

  - Software aplicativo,

- Parámetros de sistema,
- Logs e informes de auditorias,
- Datos,
- ¿Qué mas?
- Backups del Hardware.

• ¿Hay backup especiales (con datos distintos, o particulares)? ¿Cada qué período de tiempo se hacen? ¿Que datos guardan?
• ¿Qué tipo de back up hacen? (backups normales, backups incrementales, backups diferenciales) ¿En qué áreas o datos usan incrementales, en cuáles usan normales, etc.?
• ¿En qué medio se almacena? ¿Con qué dispositivo se hace?
• ¿Cómo es la rotación de los medios de backup? ¿En una semana, un mes?
• ¿Con qué aplicación se hacen? ¿Con algún tipo especial de aplicación de manejo de backup? ¿Es una del sistema operativo, del administrador de archivos u otra? ¿Utilizan archivos de tipo específicos o archivos .zip, por ejemplo?
• ¿Hay herramientas de back up automáticas, o sea que a través de una agenda hacen las copias?
• ¿Quién es el encargado o el responsable? ¿Los hace el administrador de sistemas?
• ¿Tienen formalizados los procedimientos de back up? ¿Existe un procedimiento escrito? ¿Si falta el responsable del backup, quién los hace?
• ¿Existen procedimientos escritos para recuperar archivos backupeados, o un Plan de backup?
• ¿Hacen pruebas periódicas de recuperación de backups?
• ¿Quién puede levantar los archivos de los usuarios, los backups de Mis Documentos, cualquier otro usuario?
• ¿Qué PC's o máquina es la que tiene mayor prioridad? ¿Cómo son las prioridades? ¿Según qué se determinó la prioridad de las máquinas: según un análisis de impacto, según la confidencialidad de la información?
• ¿Los backups se almacenan dentro y fuera del edificio? ¿Estos lugares son seguros?
• ¿Cómo se rotulan e identifican?
• ¿Hay documentación escrita sobre los backups hechos, sus modificaciones, fechas, etc.?
• ¿Se necesita algún dispositivo (llaves, tarjeta) para entrar al almacén de cintas?
• ¿Se crean discos de inicio de Windows?
• ¿Hay información afuera de la red interna de la empresa que sea valiosa? ¿El web host tiene datos importantes de usuarios? ¿Se hacen backups de estos datos? ¿Dentro de la empresa o por el web host?
• ¿Hay backups de las páginas web y de sus actualizaciones?

• ¿Existen procedimientos automáticos para que, en caso que un usuario cometa un error en la base de datos, ésta pueda volverse a su estado anterior? ¿Cómo se hace?

# 6 Administración de centros de cómputo

## 6.1 Centro de procesamiento de datos

• ¿Se realizan los siguientes chequeos en el sistema?

- Diariamente:

  - ¿Extraen un logístico sobre el volumen de correo transportado?
  - ¿Extraen un logístico sobre las conexiones de red levantadas?

- Semanalmente

  - ¿Extraen un logístico sobre los intentos de ingresos desde el exterior a la red interna?
  - ¿Extraen un logístico con las conexiones externas realizadas desde nuestra red?
  - ¿Obtienen un logístico sobre los downloads de archivos realizados y quién los realizó?
  - ¿Obtienen gráficos sobre tráfico en la red?
  - ¿Obtienen logísticos sobre conexiones realizadas en horarios no normales (desde dónde, a qué hora y con qué destino)?

- Mensualmente

  - ¿Realizan un seguimiento de todos los archivos logísticos a fin de detectar cambios en las estadísticas obtenidas (realizados en comparación con los archivos del mes anterior, por ejemplo)?
  - ¿Existe un programa que haga estas comparaciones? ¿Se usa? ¿Da buenos resultados?

• ¿Existen procedimientos para dar publicidad a las nuevas normas de seguridad?

- ¿Cómo harían el aviso de las políticas de seguridad?

  - ¿A través del mailing?

- ¿Con charlas o reuniones?
- ¿Exposición en transparencias?
- ¿Por una notificación expresa a cada empleado?

• ¿Cómo funciona el boletín mensual que les entregan a los usuarios? ¿Qué temas trata?
• ¿Se entrena a los usuarios y administradores? ¿Quién es el encargado? ¿Por qué?
• ¿Se tienen en cuenta los delitos no tecnológicos? (Ej: discutir temas privados de la organización en lugares no aptos, ingeniería social, etc.)
• ¿Existe algún tipo de mesa de reportes donde los usuarios con incidentes de seguridad pueden recibir ayuda o realizar un reporte? ¿Existe un tipo de feedback o buzón de sugerencia de cambios de los usuarios?
• ¿Existe un Plan de Sistemas formal?

- ¿Quién los hace?
- ¿En base a qué estudios definen las cosas por hacer?

• ¿Existe un Plan Estratégico de Sistemas? (plan a largo plazo de proyectos)
• ¿Existen políticas, normas, estándares y procedimientos que sirvan como base para la planificación, el control y la evaluación de las actividades del área de sistemas de información?
• ¿Existe una planificación y documentación escrita y actualizada de las actividades que se desarrollan normalmente en el centro de procesamiento de información? Deberá incluir como mínimo el detalle de:

- los procesos a realizar,
- los controles que se efectúan,
- los mecanismos de registros de problemas y hechos,
- los procedimientos sobre cancelaciones y re-procesos en cada un de las actividades,
- las relaciones con otras áreas,
- los mecanismos de distribución de la información.

• ¿Existe documentación detallada sobre el equipamiento informático? ¿Incluye los siguientes datos?

- distribución física de las instalaciones (identificación de PC´s y equipos, y puesto de trabajo),
- inventario de "hardware" y "software" de base,
- número de serie de hardware,
- número de licencia de software,
- inventario de insumos,
- diagramas topológicos de las redes,

- tipos de vínculos,
- ubicación de nodos,
- trabajos de mantenimiento y entrada del personal externo.

• ¿Se tienen en cuenta tanto al centro de procesamiento de datos principal como de los secundarios, redes departamentales, sucursales y al centro alternativo para contingencias?
• ¿Se actualiza la lista de activos?
• ¿Existe algún manual de seguridad, para el personal de seguridad o para los usuarios? Existe alguno de los siguientes documentos:

- Plan de contingencia,
- Plan de continuidad,
- Plan de seguridad,
- Manual de procedimientos del CPD,
- Trusted Facility Manual: detalla las funciones y privilegios de la seguridad. Contiene: configuración, administración y operación del sistema, guías para el buen uso de las características de protección del sistema, etc.
- Security Features User's guide: asiste a los usuarios del sistema, describe como usar las protecciones, las responsabilidades de la seguridad del sistema.

• ¿Es automático el método de actualización de los antivirus para que los mensajes internos en el interior y el exterior de la organización no propaguen virus? ¿Se programan los escaneos automáticos de virus? ¿Cada cuanto tiempo? ¿Porque no se actualiza la aplicación automáticamente con un schedule?
• ¿Cómo se etiquetan y almacenen los instaladores de los programas o los drivers? ¿Se almacenan en disco duro, en disquete, en CD, en cinta?
• ¿Se borran los archivos de las carpetas temporales, para que no se llenan los discos de basuras y provoquen la caída del sistema?
• Todas estas tareas ¿Son realmente útiles? ¿Se dan en la práctica?

### 6.2 Responsabilidad del equipo de seguridad

- ¿Cómo se administran las emergencias? ¿Si se hacen cambios de emergencia, cómo se documenta?
- ¿Quién es el encargado de la seguridad? ¿Y de una política de seguridad y su administración?
- ¿Quién se encarga de administrar la estructura de seguridad una vez implementada?
- ¿Existe un solo responsable del centro de cómputos?
- ¿Qué privilegios (o accesos) se le dan a las personas recién contratadas en el centro de cómputos?
- ¿Cuál es la diferencia de permisos entre los desarrolladores y los administradores?
- ¿Quién asigna los permisos a los distintos roles o grupos?
- ¿Quién es el encargado de informar a los ejecutivos de la empresa sobre la administración de seguridad, actividad de seguridad de la información, y riesgos? ¿Se realizan informes periódicos? ¿Son a pedido de alguien o a modo de auto evaluación?
- ¿Quién es el encargado de recomendar la separación de tareas y responsabilidades para las funciones?
- ¿Quién es responsable de asegurar que los sistemas de seguridad física están en su lugar?
- ¿Existe en los empleados y altos ejecutivos una conciencia sobre su importancia de la seguridad?
- Todas estas tareas ¿Son realmente útiles? ¿Se dan en la práctica?

# 7 Auditorias y revisiones

## 7.1 Auditorias generales

• ¿Se hacen auditorías en la empresa?
• ¿Qué objetos se auditan? Para cada clase de objetos, ¿qué accesos se auditarán?

- Archivos y directorios
- Claves del registro
- Servicios
- Objetos del kernel
- Impresoras

• ¿Qué actividades se monitorizan?

- Monitorización del sistema general
- Monitorización de reinicio de los sistemas
- Monitorización de colapsos (crashes) del sistema
- Monitorización de fallas de hardware
- Monitorización de procesos
- Monitorización de aplicaciones

• Gestión de red: ¿Para el monitoreo de la red se utilizan aplicaciones propias de UNIX, como:

- monitores de tráfico de red?
- monitores de rendimiento?
- monitores de control de cantidad de archivos abiertos?
- monitores de usuarios conectados al servidor?
- aplicación de monitoreo gráfico de la red?

• ¿Qué otra clase de eventos se auditarán?
• ¿Con qué tipo de herramientas se hace la monitorización?

- Escáner de puertos y vulnerabilidades
- Chequeadores del sistema de archivos
- Analizadores de logs de eventos
- Analizadores de registro
- Analizadores de listas de control de acceso (ACL)
- Sniffers de paquetes
- Herramientas para craquear passwords
- Escáner de seguridad integral (Overall security scanners)

• ¿Se hacen chequeos aleatorios para verificar el cumplimiento de los requerimientos y procedimientos de seguridad? ¿Sería útil?
• ¿Cuánto se monitoriza? (Monitorizar tiene un impacto directo en la performance del sistema) ¿Cómo hacen para que los recursos alcancen? ¿Cómo hacen con cada uno de los cuellos de botella?

- Carga de CPU
- Memoria disponible
- Performance del sistema de disco
- Ancho de anda de la red

• ¿Cuándo se eliminan los logs para evitar llenar el disco? ¿Tienen un tamaño máximo?
• ¿Qué pasa con la información que se obtiene de las auditorías? ¿Pasa algo de lo siguiente?

- Se solicita la información y se ve que:

  - No tiene y se necesita.
  - No se tiene y no se necesita.

- Se tiene la información pero:

  - No se usa.
  - Es incompleta.
  - No esta actualizada.
  - No es la adecuada.
  - Se usa, está actualizada, es la adecuada y está completa.

• ¿Las auditorías permiten rastrear las acciones de cada usuario?

- ¿Que se audita?
- ¿Se audita según las acciones, las maquinas o los usuarios?
- ¿Cada uno de estos activos en particular o depende de los sectores y/o máquinas y/o sensibilidad de la información?

• ¿Las auditorías soportan investigaciones luego de los hechos, con datos sobre cómo, cuando y por qué cesaron las operaciones normales?
• ¿Se reúne información de las auditorías para formar perfiles de los usuarios del sistema? ¿Observan, por ejemplo, patrones en los usuarios, como las terminales que utilizan, horas de acceso, y permisos que solicitan, para determinar qué acciones son inusuales y deben ser investigadas?

• ¿Se usan herramientas automáticas para revisar los registros de auditorías en tiempo real?
• ¿Debido a que no hay herramientas que generen warnings ni alarmas, se revisan los logs de auditorías periódicamente? ¿Qué se revisa?
• ¿La aplicación es en tiempo real?
• ¿La aplicación es del sistema operativo, es un programa desarrollado por ustedes o es un programa comprado?
• Se deberían utilizar chequeos aleatorios, con frecuencias más bajas, para hacer auditorias manuales y/o mensuales de este tipo.
• ¿Se generan históricos de auditoria indicando qué procesos se corrigieron, quién los corrigió y qué cambios hizo (control de cambios – gestión de configuración)?
• ¿Se investiga la actividad sospechosa? ¿Se toman acciones?
• ¿Se documentan la ejecución y los resultados de estas pruebas?

## 7.2 Logs

• ¿Está controlado el acceso a los logs on line de auditoria?
• ¿Cómo se identifica qué tipo de logs son generados? ¿Se almacenan en diferentes carpetas los que son generados por diferentes programas?
• ¿Los logs se almacenan externamente a la empresa? ¿Los almacenamientos externos de logs de auditorías se retienen por un período de tiempo? ¿Está controlado el acceso a estos logs, también?
• ¿Hay demasiada información guardada? ¿Los archivos largos de logs hacen más difícil encontrar irregularidades?
• Los logs de los eventos deberían contener los siguientes campos:

- Fecha y hora
- Tipo (severidad del evento)
- Fuente (el componente que disparó o acceso el evento)
- Categoría (subgrupo de eventos de seguridad)
- ID del evento (número único que identifica el evento)
- Usuario (nombre del usuario relacionado con el evento, si hay)
- Computadora (máquina donde se acceso el evento)
- Descripción (datos como mensajes de error, asociados con el evento)
- Datos (datos binarios asociados con el evento)

• Análisis de los logs de auditoria:

- ¿Qué datos son los más importantes o los más leídos?
- ¿Cuánto tiempo lleva hacer los análisis?

- ¿Es necesario mejorar los análisis? ¿De que forma, cuál es la falla?

• ¿Porque no se analizan los logs, aunque sea los que posean alguna conducta irregular?

- ¿Es totalmente necesario un sistema automático de monitorización y análisis de logs que emita alarmas ante determinados eventos?
- ¿Porque esto no se da en la realidad?
- ¿Es mucho trabajo?
- ¿No vale la pena?
- ¿No hay gente que se dedique a esto?

### 7.3 Línea de base

• ¿Se hace una línea de base de la performance de los servidores y de la red? ¿Qué medidas se toman?
• ¿Qué datos se recogen para hacer la línea?
• ¿A qué intervalo de tiempo se toman estos datos? ¿Con qué frecuencia se tomarán las líneas base?
• ¿Se hacen nuevamente las líneas de base si se modifica alguna configuración en el sistema?
• ¿Cuándo se actualizan las líneas de base?
• ¿Cómo se guardan? ¿Dónde? ¿En qué formato?

### 7.4 Responsabilidades de los encargados de seguridad

• ¿Quién administra, desarrolla e implementa los procedimientos de auditoría y revisión? ¿Quién conduce la auditoría?
• ¿Quién selecciona los eventos de seguridad a ser auditados?
• ¿Quién administra la documentación sobre los resultados?
• ¿Quién se encarga de monitorizar y reaccionar a los avisos (warnings) y reportes?
• ¿Quién hace chequeos aleatorios para verificar el cumplimiento de los requerimientos y procedimientos de seguridad?
• ¿Quién se encarga de reunir datos de las auditorías para formar perfiles de los usuarios del sistema?
• ¿Quién revisa los reportes de auditorías buscando anomalías?
• ¿Hay separación de tareas entre los que administran el control de acceso y los que hacen las auditorías, o son las mismas personas?

- ¿Quién se encarga de buscar nuevas herramientas que faciliten la auditoría?

## 7.5 Auditoria del servidor

• CPU del servidor usado

- ¿Qué trabajos usan más CPU?
- ¿Quién usa más CPU?
- ¿En qué momento se usa más el CPU?
- ¿Cuánto tiempo el CPU permanece usada en un 100%?

• Memoria del servidor usada

- ¿Qué trabajos usan más memoria?
- ¿Quién usa más memoria?
- ¿En qué momento se usa más la memoria?
- ¿Cuánto tiempo la memoria permanece usada en un 100%?

• Datos del servidor usados

- ¿Qué datos son los que consumen más tráfico, memoria o CPU?
- ¿Qué datos se usan más?
- ¿Qué datos se modifican más?
- ¿Quién entra a cada dato?

• Aplicaciones del servidor usadas

- ¿Qué aplicaciones consumen más recursos?
- ¿Qué aplicaciones se usan más?
- ¿Qué aplicaciones se cuelgan más veces?

## 7.6 Auditoria de control de acceso

• ¿Se generan logs de auditoria del control de acceso?
• ¿Cuándo se almacenan, ante qué eventos? ¿Se almacenen cuando ocurre alguno de estos eventos?

- Login exitoso
- Login fallido
- Procedimientos de cambios de passwords satisfactorio
- Procedimientos de cambios de passwords fallido
- Lockeo de un usuario
- Modificación en bases de datos

- Utilización de herramientas del sistema
- Modificación de ciertos datos (como datos de configuración, datos críticos, datos de otros usuarios)
- Acceso a Internet
- Alertas de virus

• ¿Dónde se almacenan?
• ¿Quién tiene acceso a los logs?
• ¿Por cuanto tiempo permanecen guardados?
• ¿Se borran cuando expira ese tiempo o se genera una estadística comprimida de los mismos y de guarda un análisis de ellos solamente?
• ¿Qué datos se almacenan en los logs? ¿Se almacenan los siguientes datos?

- Para todos los eventos:

  - Fecha y hora del evento
  - Tipo de evento (Ej. Login, modificación de datos, etc.)
  - ID de usuario
  - Origen del evento (Ej. Terminal Nº 9)

- Acceso a Internet:

  - Páginas visitadas
  - Cookies guardadas
  - Archivos descargados
  - Servicios utilizados
  - Aplicaciones utilizadas

- Modificación de ciertos datos

  - Datos modificados
  - Valor anterior

    - ¿por cuanto tiempo se guarda el valor anterior de los datos?
    - ¿Se hace alguna comprobación antes de efectuar el cambio definitivo?
    - ¿Que se hace si se modifica algún valor de la configuración del sistema?

- Login fallido

  - Motivo del fallo

- Procedimientos de cambios de passwords

    - Password anterior
    - Password nueva fallida
    - Aplicación usada
    - Motivo del fallo

- Lockeo de un usuario

    - Motivo del lockeo del usuario
    - Aplicación que realiza el lockeo.

- Modificación en bases de datos

    - Datos modificados
    - Valor anterior
    - Aplicación usada

- Utilización de herramientas del sistema

    - Herramienta usada
    - Rastreo de acciones del usuario con esa herramienta
    - Modificaciones realizadas.

• ¿Las estadísticas que genera son buenas? ¿Faltan datos por analizar que son importantes para la administración del control de acceso?
• Prestar especial atención con los logs que fueron generados con el ID de Administrador, ¿hay irregularidades en estos logs? ¿Se han controlado alguna vez?

## 7.7 Auditoria de redes

### 7.7.1 Correo

• ¿La herramienta de administración de correo genera logs de auditoria?
• ¿Qué contienen?
• ¿Quién los administra?
• ¿Cada cuanto se leen?
• ¿Se generan avisos cuando:

- Se está por llenar el espacio asignado para el correo?
- Hay muchos mensajes de la misma dirección fuente?
- Hay muchos mensajes para la misma dirección destino?
- Hay muchos mensajes con el mismo encabezado, o cuerpo, o archivo adjunto?
- Hay posibles virus?
- Hay SPAM?
- Se baja la performance del correo?
- Hay algún problema para enviar o recibir los mensajes?
- Hay muchos mensajes entrantes o salientes, más de lo normal?
- Cuándo más?

### 7.7.2 Mantenimiento – Monitoreo – Auditorias

- ¿Usan herramientas de monitorización de red?
- ¿Se hace algún chequeo periódico de la red y sus permisos?
- ¿Qué datos se pueden ver?

  - Datos

    - ¿Programas que se ejecutan en las PC's y servidores?
    - ¿Qué prioridades tienen los trabajos?
    - ¿Qué prioridades tienen los usuarios?
    - ¿Con qué reglas de trabajos se están corriendo?
    - ¿El estado de cada trabajo (en cola, ejecutándose, esperando una respuesta del operador, etc.)?
    - ¿Desde dónde se ejecuta el programa (usuario, ID, terminal)?
    - ¿Porcentaje de CPU y memoria (recursos) usado por programa? ¿Y por terminal? ¿Y por usuario?
    - ¿Colas de impresión de cada usuario? ¿De cada impresora? ¿De cada terminal?
    - ¿Trabajos programados por cada usuario? ¿Por cada terminal?
    - ¿Dispositivos conectados a la red? ¿El estado de los a dispositivos?
    - ¿Dispositivos con problemas?
    - ¿Qué usuario está asignado (o usando) cada dispositivo? ¿Qué trabajo lo está ocupando?
    - ¿Se monitorean los puertos de la red? ¿Se puede ver si hay intentos de intrusión?
    - Alertas de virus

- Tipo y nombre del virus
- Archivo infectado (nombre, ubicación etc.)
- Antivirus usado
- Acciones llevadas a cabo
- Resultado de las acciones (satisfactorio o no)

- Estadísticas de red:

- ¿En qué parte de la línea el tráfico es más intenso?
- ¿Quién de las terminales usa más tráfico de red?
- ¿Gráfico del uso de la red por terminal?
- ¿Se discrimina el tráfico ocupado por mail, datos, aplicaciones, mensajes, Internet, etc.?
- ¿Cuantos intentos de intrusos hubo?
- ¿Cuantos intentos de otros ataques?
- Etc.
- Internet

  - ¿Páginas más visitadas por usuario?
  - ¿Tiempo promedio de estadía en Internet?
  - ¿Recursos usados por Internet?

- Mail
  - ¿Cantidad de datos que se mueven diariamente vía mail?
  - ¿Mensualmente?
  - ¿Anualmente?
  - ¿Cantidad de mail enviados y recibidos por usuario?
  - ¿Por departamento?
  - ¿En toda la empresa?
  - ¿Controles para saber si un usuario en particular excede el promedio de mail diarios?
  - ¿Mensajes infectados, salientes y entrantes?
  - ¿Se usan estadísticas para controlar el mail bombing?
- Virus

  -¿Cantidad de mails infectados en un determinado tiempo?
  - ¿Direcciones fuentes qué más mails infectados envía?
  - ¿Cantidad de archivos infectados por extensión? (Ej. Los archivos de Word se infectan más que los de Excel).

- Alarmas – Avisos

  - ¿Se generan avisos ante virus?

- ¿Se generan avisos ante intrusos?
- ¿Se generan avisos ante poco espacio en disco de servidores o de PC's?
- ¿Se generan avisos ante poca disponibilidad de CPU o de memoria en los servidores?
- ¿Cuándo más?

• ¿Quién se encarga de procesar y/o monitorear los datos generados por la herramienta?
• ¿Cómo se actúa en consecuencia? ¿Existe algún procedimiento específico?
• ¿Qué datos parecen faltar al monitor de red que serían útiles para la administración de la red?

# 8 Plan de contingencias

## 8.1 Planes de contingencia

• ¿Existe un plan de contingencias? ¿Cómo es? ¿Es formal? ¿Quién lo desarrolló?
• ¿Ha habido alguna contingencia que justifique el desarrollo del plan?
• ¿Se desarrolló un previo análisis de riesgo antes de realizar el plan de contingencias?
• ¿El plan de contingencias se desarrolló solo en base al área de cómputos, se tuvieron en cuenta otras áreas de la dependencia? ¿Cuáles? ¿Por qué esas áreas?
• ¿El plan de contingencias incluye un Plan de recuperación de desastres?
• ¿El plan de contingencias incluye un Plan de reducción de riesgos?
• ¿Se definen las responsabilidades y funciones de las personas en el plan de contingencias?
• ¿Existe entrenamiento para los responsables del plan de contingencias? ¿Y para los usuarios?
• ¿Poseen las acciones defensivas en caso de violación interna o externa? (Ej. desconectar los servidores, cerrar los accesos, rastrear al intruso, etc.),
• ¿Hay algún tipo de mecanismo de reportes o historial, para el manejo de incidentes?
• ¿Documentan el plan de contingencias? ¿Contiene todos estos datos?:

- Objetivo del plan.
- Modo de ejecución.
- Tiempo de duración.
- Costes estimados.
- Recursos necesarios.
- Evento a partir del cual se pondrá en marcha el plan.
- Personas encargadas de llevar a cabo el plan y sus respectivas responsabilidades.

• ¿Existe alguna copia del plan de contingencia fuera de la empresa? ¿Está protegida en caja de seguridad? ¿Cada cuanto se actualiza?
• ¿Se hacen pruebas del plan? ¿Con qué frecuencia? ¿Anualmente?
• ¿Se mantiene actualizado de acuerdo a nuevos puestos y funciones, o amenazas?

### 8.2 CPD alternativo

• ¿Se mantiene un centro de procesamiento alternativo? ¿Qué características tiene, en comparación con el CPD principal?
• ¿Es propio o contratan un tercero que facilite el CPD? En el segundo caso, ¿cómo es el contrato para este servicio?
• ¿Cómo se aseguran que este centro tenga las mismas condiciones de seguridad y calidad que las instalaciones del CPD principal?
• ¿Existe la posibilidad de poner el CDP alternativo en otra sucursal o en otro lado? ¿Por qué?
• ¿Si llega a haber un problema, en cuanto tiempo puede estar en óptimo funcionamiento este CPD alternativo?

### 8.3 Plan de recuperación de desastres

• ¿Cuánto cuesta un plan de recuperación de desastres? ¿Tiene relación con la información a recuperar? ¿O a cualquier costo se salva la información crítica?
• ¿En el caso de que haya un plan, cada miembro del equipo tiene una responsabilidad asignada? ¿O la responsabilidad es del Departamento de Sistemas?
• ¿Se dividen las acciones correctivas en equipos de trabajo? ¿Cómo forman esos equipos? ¿Dependen del desastre ocurrido?
• ¿Luego del desastre existe un equipo de evaluación para corregir y documentar los errores cometidos en tal circunstancia, para luego generar un plan de contingencia de mayor efectividad y eficiencia?

#### 8.3.1 Antes del desastre

• Identificación de las funciones críticas.

**-** ¿Cuáles serían los datos críticos a proteger en la organización, en el momento de un desastre? (Agregar lista de datos).
**-** ¿Cuáles serían los elementos de hardware y de software críticos a proteger en la organización, en el momento de un desastre? (Agregar lista de elementos).
**-** ¿Cómo se ordenarían según la importancia?

• Constitución del grupo de desarrollo del plan.

**-** ¿Quién sería le responsable del plan de emergencias, de su implementación y puesta en práctica? ¿El Jefe de Sistemas?
**-** En cada área que cubrirá el plan debe haber un líder del plan de contingencia. ¿Quién sugiere, el Jefe de cada área? ¿Alguien de más bajo rango? ¿Por qué?

• Sistemas de información:

**-** ¿Existe un responsable de la información, en cada área de la empresa? ¿Conocen sus responsabilidades? ¿Los responsables que figuran en la documentación, son los que ejercen realmente el papel de responsables de la información? ¿Qué funciones tiene que cumplir?
**-** ¿Están identificados todos los sistemas de información y sus características (como si fuera un inventario de los sistemas)?
**-** ¿Qué datos se almacenan de los sistemas? Se sugiere almacenar:

- Nombre
- Lenguaje
- Departamento de la empresa que genera la información (dueño del sistema)
- Departamentos de la empresa que usan la información
- Volumen de archivos con los que trabaja
- Volumen de transacciones diarias, semanales y mensuales que maneja el sistema
- Equipamiento necesario para un manejo óptimo del Sistema
- La(s) fecha(s) en las que la información es necesitada con carácter de urgencia.
- El nivel de importancia estratégica que tiene la información de este Sistema para la Institución (medido en horas o días que la Institución puede funcionar adecuadamente, sin disponer de la información del Sistema).
- Equipamiento mínimo necesario para que el Sistema pueda seguir funcionando (considerar su utilización en tres turnos de trabajo, para que el equipamiento sea el mínimo posible).
- Actividades a realizar para volver a contar con el Sistema de Información (actividades de restauración).

**-** ¿Se puede dar un orden de importancia a los sistemas de la lista de arriba?

• Equipos de cómputos:

**-** ¿Se mantiene un inventario de los equipos de cómputos? Se debería incluir:

- Hardware: procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, cableado de la red, servidores de terminal, routers, bridges.
- Software: programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicaciones.
- Datos (principales archivos que contienen los equipos): durante la ejecución, almacenados en línea, archivados fuera de línea, backup, bases de datos, dueño designado de la información.
- Configuración de los equipos (y sus archivos de configuración).
- Ubicación de los equipos y de los datos.
- Nivel de uso Institucional de los equipos.
- Etc.

**-** ¿Existen pólizas de seguros para los equipos en el caso de siniestros? ¿Cómo son estos seguros?

**-** ¿Las PC's o equipos se categorizan según su importancia (señalización o etiquetado de los Computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación.)?

**-** ¿Existe una relación de las PC's requeridas como mínimo para cada Sistema permanente de la Institución? ¿Está actualizada siempre?

• Backup:

**-** ¿Existen procedimientos para realizar back up?

**-** ¿Están incluidos en el plan de contingencia?

• Definición de los niveles mínimos de servicio.

**-** ¿Cuáles son las contingencias o problemas que pueden ocurrir? (agregar lista de las posibles contingencias)

- ¿Cuáles serían los peores problemas a los que se puede ver sometida la empresa? ¿Cuáles serian las peores contingencias?
- ¿Cuáles serían las más probables?
- ¿Cuáles son las que ocurren más a menudo?
- ¿Cuales son las que no ocurren nunca?

**-** ¿Se pueden nombrar algunas funciones o servicios que funcionen como los niveles críticos de servicio para cada una de las contingencias nombradas arriba? ¿Qué opinión tiene el jefe de cada área en cuanto a los niveles críticos de su área? Un ejemplo puede ser: el que no se caiga el servidor de aplicaciones, o el router, o la conexión de radio.
**-** ¿Qué recursos se necesitan para que funcione este servicio?
- ¿Cuales son las prioridades de procesamiento que tendrán estas funciones o servicios críticos en caso de una emergencia?

• Evaluación de la relación coste / beneficio de cada alternativa.

- ¿Qué costo tendría cada uno de los niveles críticos de servicio que se determinaron arriba? Contar los costos de implementación, de mantenimiento, de entrenamiento de usuarios, y de restauración en caso de una emergencia.

• Entrenamiento:

**-** ¿Entrenan al personal de alguna manera ante un siniestro?
- ¿Simulan siniestros para entrenar al personal?

### 8.3.2 Durante el desastre

• ¿Poseen un plan de emergencia (consiste de las acciones a llevar a cabo durante el siniestro)?
• ¿Se tienen en cuenta los distintos escenarios posibles? Ej.: durante el día, la noche.
• ¿Se incluyen los siguientes puntos?:

**-** ¿Vías de salida?
**-** ¿Plan de evacuación del personal?
**-** ¿Plan de puesta a buen recaudo de los activos?
**-** ¿Ubicación y señalización de los elementos contra el siniestro?

• ¿Existen funciones (encargado de retirar los equipos, encargado de las cintas, etc.) y equipos con funciones claramente definidas a ejecutar durante el siniestro?

### 8.3.3 Después del desastre

Después de ocurrido el Siniestro o Desastre es necesario realizar las actividades que se detallan, las cuales deben estar especificadas en el Plan de Acción.

• Evaluación de Daños: ¿se realizan las siguientes actividades después de que ha ocurrido algún desastre?

- ¿Evalúan la magnitud del daño que se ha producido?
- ¿Que sistemas se están afectando?
- ¿Que equipos han quedado no operativos?
- ¿Cuales se pueden recuperar?
- ¿En cuanto tiempo?
- ¿Qué más se evalúa o debería evaluarse, según sus experiencias?

• Ejecución de Actividades.

- ¿Se determina un coordinador que se encargará de las operaciones necesarias para que el sistema funcione correctamente, después de la emergencia?
- Para cada tipo de emergencia, de las enumeradas arriba, ¿qué acciones se deben tomar para que el sistema vuelva a su funcionamiento normal?

• Evaluación de Resultados.

- ¿Se evalúan los desempeños de las personas, y del Plan, luego de ocurrido el desastre?
- ¿Se genera una lista de recomendaciones para minimizar los riesgos?

• Retroalimentación del Plan de Acción.

- ¿Se evalúa el desempeño del personal durante el desastre?
- ¿Se tiene en cuenta la información que se obtiene luego de una emergencia para retroalimentar el Plan?

  - ¿Se reordena la lista de personal afectado en tareas de emergencia, con esta experiencia obtenida?
  - ¿Se modifican las prioridades? ¿Qué elemento tenía demasiada prioridad?
  - ¿Qué actividades faltaron incluir en el plan de emergencia?
  - ¿Qué se mejoraría?

- ¿Cuál hubiera sido el costo de no haber tenido el plan de contingencias? ¿Qué se hubiera perdido?

# Glosario

**ACCESO:** es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal, desde donde pueden ser vistos, modificados o eliminados.
**ACTIVE X:** es un lenguaje de programación apoyado en controles OLE, Visual Basic y librerías del entorno Windows (OCX) de Microsoft. Active X permite que interactúenaplicaciones Windows con el World Wide Web (Internet).
**ADSL**: (Asymmetric Digital Suscribe Line - Línea de Usuario Digital Asimétrica). Usa la infraestructura telefónica actual para proveer servicios de transmisión de datos en alta velocidad.
**AMENAZA:** cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal o equipo informático, o causar la difusión no autorizada de información confiada a una computadora. Ejemplo: fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.
**ANTIVIRUS:** son todos aquellos programas que permiten analizar memoria, archivos y unidades de disco en busca de virus. Una vez que el antivirus ha detectado alguno de ellos, informa al usuario procediendo inmediatamente y de forma automática a desinfectar los ficheros, directorios, o discos que hayan sido víctimas del virus.
**ARCHIVO DE PROCESO POR LOTES (.BAT o BATCH):** los ficheros de proceso por lotes o ficheros Batch se caracterizan por tener extensión BAT. Son ficheros de texto que contienen comandos, uno por cada línea escrita. Cuando se ejecuta este tipo de ficheros, cada una de las líneas en él escritas se va ejecutando de forma secuencial.
**ARCHIVO, DOCUMENTO:** estos términos tienen el mismo significado y hacen referencia a la información que se encuentra en un soporte de almacenamiento informático. Es el trabajo real que realiza cada usuario (textos, imágenes, bases de datos, hojas de cálculo, etc.). Cada uno de ellos se caracteriza por tener un nombre identificativo. El nombre puede estar seguido de un punto y una extensión, compuesta por tres caracteres que identifican el tipo de fichero del que se trata. Algunas extensiones comunes son: EXE y COM (ficheros ejecutables, programas), TXT y DOC (ficheros de texto), etc.
**ATAQUE:** término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.
**ATAQUE ACTIVO:** acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal. Ejemplo: borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.

**ATAQUE PASIVO**: intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la intercepción de una red. Todo esto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene.

**AUDITORÍA:** llevar a cabo una inspección y examen independiente de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y procedimientos operativos, y para recomendar cualquier cambio que se estime necesario.

**AUTENTICIDAD:** capacidad de determinar si una lista de personas han establecido su reconocimiento y/o compromiso sobre el contenido del documento electrónico.

**BASES DE DATOS:** Es un conjunto de datos interrelacionados y un conjunto de programas para accesarlos. Una recopilación de datos estructurados y organizados de una manera disciplinada para que el acceso a la información de interés sea rápido.

**BIOS:** es la abreviatura de Basic Input / Output System e identifica al software o conjunto de programas que arrancan el ordenador (antes de encontrarse un disco de sistema) cuando se pulsa el botón de encendido. La BIOS es un programa que se no se encuentra en la memoria RAM (Random Access Memory – memoria de acceso aleatorio) pues al apagar el ordenador se borraría, sino en la memoria principal o ROM (Read Only Memory -Memoria de Sólo Lectura), cuyo almacenamiento es permanente.

**CARPETA:** se trata de divisiones (no físicas sino lógicas) en cualquier tipo de disco donde son almacenamos determinados ficheros. Forman parte de una manera de organizar la información del disco, guardando los documentos como si de una carpeta clasificadora se tratase.

**CHAT:** se trata de conversaciones escritas en Internet. Mediante una conexión a la red y un programa especial, es posible conversar (mediante texto escrito) con un conjunto ilimitado de personas, al mismo tiempo

**COBOL:** (Common Organization Business Oriented Language) lenguaje de programación creado en la década del 60.

**CONFIDENCIALIDAD:** capacidad de mantener datos inaccesibles a todos, excepto a una lista determinada de personas.

**COOKIE:** procedimiento ejecutado por el servidor que consiste en guardar información acerca del cliente para su posterior recuperación En la práctica la información es proporcionada desde el visualizador al servidor del Word Wide Web vía una forma o un método interactivo que puede ser recuperado nuevamente cuando se accede al servidor en el futuro. Es utilizado por ejemplo para el registro a un servicio.

**CPD**: centro de procesamiento de datos, centro de cómputos.

**CRIPTOGRAFÍA:** (encriptación) es la rama de las matemáticas aplicadas que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlas a su forma original.

**DATOS:** los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), video (secuencia de tramas), etc.

**DEPARTAMENTO DE CÓMPUTO:** es la entidad encargada del buen uso de las tecnologías de la computación, organización y optimización de los recursos computacionales de la institución. Es la entidad encargada de desarrollar el plan estratégico que favorezca la prestación de servicios eficientes, eficaces y de utilidad en la transmisión de datos para apoyar efectivamente los requerimientos del usuario. Es la entidad encargada de ofrecer sistemas de información administrativa integral permitiendo en forma oportuna satisfacer necesidades de información, como apoyo en el desarrollo de las actividades propias del centro.

**DOMINIO:** conjunto de computadoras que comparten una característica común, como el estar en el mismo país, en la misma organización o en el mismo departamento. Cada dominio es administrado un servidor de dominios.

**DOS (MS/DOS):** estas siglas significan Disk Operating System (DOS). Se refieren al sistema operativo (S.O.) anterior a Windows que, en su momento, creó la empresa Microsoft.

**EQUIPO DE CÓMPUTO:** dispositivo con la capacidad de aceptar y procesar información en base a programas establecidos o instrucciones previas, teniendo la oportunidad de conectarse a una red de equipos o computadoras para compartir datos y recursos, entregando resultados mediante despliegues visuales, impresos o audibles.

**EQUIPO DE TELECOMUNICACIONES:** todo dispositivo capaz de transmitir y/o recibir señales digitales o analógicas para comunicación de voz, datos y video, ya sea individualmente o de forma conjunta.

**FILTRO DE PAQUETES:** programa que intercepta paquetes de datos, los lee y rechaza los que no estén en un formato predefinido.

**FINGER:** programa que muestra información acerca de un usuario específico, o acerca de todos los usuarios, conectados a un sistema remoto. Habitualmente se muestra el nombre y apellido, hora de la última conexión, tiempo de conexión sin actividad y terminal. Puede también mostrar archivos de planificación y de proyecto del usuario.

**FIREWALL:** es un sistema diseñado para evitar accesos no autorizados desde o hacia una red privada. Los Firewalls pueden estar implementados en hardware o software, o una combinación de ambos. Los firewalls son frecuentemente utilizados para evitar el acceso no autorizado de usuarios de Internet a redes privadas conectadas a la misma, especialmente intranets. Todos los mensajes que dejan o

entran a la red pasan a través del firewall, el cual examina cada mensaje y bloquea aquellos que no cumplan con determinado criterio de seguridad.

**FIRMA DIGITAL:** valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

**FTP:** (File Transfer Protocol) protocolo parte de la arquitectura TCP/IP utilizado para la transferencia de archivos.

**GUSANO:** es programa similar a un virus que se diferencia de éste en su forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos solamente realizan copias de ellos mismos.

**HACKER:** persona que tiene un conocimiento profundo acerca del funcionamiento de redes y que puede advertir los errores y fallas de seguridad del mismo. Al igual que un cracker busca acceder por diversas vías a los sistemas informáticos pero con fines de protagonismo.

**HOST:** (sistema central) computador que permite a los usuarios comunicarse con otros sistemas centrales de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, Telnet y FTP.

**HTML:** lenguaje de marcado de hipertexto, (Hyper-Text Markup Language) es el lenguaje con que se escriben los documentos en el World Wide Web (Internet).

**HTTP:** Protocolo de Transferencia de Hipertextos (Hyper-Text Transfer Protocol). Es el protocolo usado por el Word Wide Web para transmitir páginas HTML.

**HUB:** Un punto común de conexión de dispositivos en una red. Los hubs son usados comúnmente para conectar segmentos de una LAN. Un hub contiene múltiples puertos. Cuando un paquete llega al puerto, es copiado a los otros puertos, de esta manera los otros segmentos de la LAN pueden ver todos los paquetes. Un hub pasivo simplemente sirve de conductor de datos entre los diferentes puertos. Los llamados hubs inteligentes incluyen servicios adicionales como permitir a un administrador monitorear el tráfico y configurar cada puerto del hub. Estos hubs se conocen generalmente como hubs administrables (manageable hubs). Un tercer tipo de hub, llamado switching hub, lee la dirección de destino en cada paquete y lo envía al puerto correcto.

**IDENTIFICACIÓN:** un subtipo de autenticación, verifica que el emisor de un mensaje sea realmente quien dice ser.

**INCIDENTE:** cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido

**INFECCIÓN:** es la acción que realiza un virus al introducirse, empleando cualquier método, en nuestro ordenador (o en dispositivos de almacenamiento) para poder realizar sus acciones dañinas.

**INTEGRIDAD:** se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software

de la base de datos, por fallas de programas, del sistema, hardware o errores humanos. El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

**INTRANET:** una red privada dentro de una compañía u organización que utiliza el mismo software que se encuentra en Internet, pero que es solo para uso interno.

**IP ADDRESS:** (Dirección IP) dirección de 32 bits definida por el Protocolo Internet en STD 5, RFC 791. Se representa usualmente mediante notación decimal separada por puntos.

**ISP**: (Internet Service Provider – Proveedor de servicios de Internet) Empresa que presta servicios de conexión a Internet.

**LOCAL AREA NETWORK:** (LAN) (Red de Área Local) red de datos para dar servicio a un área geográfica pequeña, un edificio por ejemplo, por lo cual mejorar los protocolos de señal de la red para llegar a velocidades de transmisión de hasta 100 Mbps (100 millones de bits por segundo).

**MACRO / VIRUS DE MACRO:** una macro es una secuencia de operaciones o instrucciones que definimos para que un programa (por ejemplo, Word, Excel, o Access) realice de forma automática y secuencial. Estas son "microprogramas" que pueden ser infectados por los virus. Los documentos de texto, las bases de datos o las hojas de cálculo no son programas y por ello no deberían ser infectados por ningún virus. No obstante, en cada uno de los ficheros creados con este tipo de aplicaciones se pueden definir macros y éstas sí son susceptibles de ser infectadas. Los virus de macro son aquellos que infectan exclusivamente documentos, hojas de cálculo o bases de datos que tienen macros definidas.

**MAN:** Metropolitan Area Network. Red de Área Metropolitana.

**MENSAJE DE DATOS:** la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama o el telefax.

**NAT:** (Network Address Translation) las direcciones NAT son utilizadas comúnmente
cuando se requiere conectividad de una LAN a Internet pero solo se tiene acceso a una sola
dirección IP de Internet.

**NAVEGADOR:** (browser): término aplicado normalmente a programas usados para conectarse al servicio WWW.

**POP:** (Protocolo de Oficina de Correos - Post Office Protocol) programa cliente que se comunica con el servidor, identifica la presencia de nuevos mensajes, solicita información de los mismos y utiliza al servidor como oficina despachadora de correo electrónico cuando el usuario envía una carta.

**PRIVACIDAD:** se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos será difundidas o transmitida a otros.

**PROGRAMAS (FICHEROS .EXE y .COM):** los ficheros, documentos o archivos se componen de un nombre (cuyo número de caracteres antiguamente se limitaba a

8) y una extensión que puede no existir o contener, hasta tres caracteres como máximo. Esta extensión especifica el tipo de fichero. Si es EXE o COM, el fichero será un programa ejecutable. De esta forma si hacemos doble clic sobre él o escribimos su nombre, se realizarán determinadas acciones.

**PROTOCOLO:** descripción formal de formatos de mensaje y de reglas que dos computadores deben seguir para intercambiar dichos mensajes**.**

**PROXY:** una substitución de direcciones, usado para limitar la información de direcciones disponibles externamente**.**

**REDIRECCIONAR:** esta acción permite aplicar un nuevo destino. En el caso de los virus, se puede hablar de éste término cuando un virus es capaz (por ejemplo) de hacer que el sistema en lugar de acceder a una dirección en la que debería encontrar determinados componentes, es obligado por el virus a saltar o acceder a otra dirección diferente.

**ROUTER:** (direccionador) dispositivo que distribuye tráfico entre redes. La decisión sobre a dónde enviar se realiza en base a información de nivel de red y tablas de direccionamiento.

**SATAN:** (Security Analysis Tool for Auditing Networks). Herramienta de Análisis de Seguridad para la Auditoria de Redes. Conjunto de programas para la detección de problemas relacionados con la seguridad.

**SCRIPT:** archivos con su extensión SCR que sirven para determinar los parámetros ("condiciones") con los que se deben ejecutar unos determinados programas. Permiten iniciar un programa con unas pautas fijadas de antemano.

**SEGURIDAD:** se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados. En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos. El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos.

**SENDMAIL**: aplicación de administración de correo electrónico propia del sistema operativo Linux.

**SHTTP:** (secure HTTP - HTTP seguro). Protocolo HTTP mejorado con funciones de seguridad con clave simétrica.

**SISTEMA OPERATIVO (S.O.):** existen dos términos muy utilizados en informática. Estos son los conceptos de hardware y software. El primero de ellos se refiere a todo lo que es físico y tangible en el ordenador, como unidades de disco, tarjetas gráficas, microprocesador, memoria, etc. Por otro lado está el software que se define como el conjunto de programas (o información) con la que puede trabajar el hardware (ficheros, directorios, programas ejecutables, bases de datos, controladores, etc.). El sistema operativo pertenece al software y más concretamente es el conjunto de programas (y ficheros o archivos de otro tipo) que

permite que se pueda utilizar el hardware. Se puede tener el mejor ordenador del mundo (el mejor hardware), pero si éste no tiene instalado un sistema operativo, no funcionará (ni siquiera se podrá encender). Algunos ejemplos de sistemas operativos son: MS/DOS, UNIX, OS/2, Windows 95/98/2000/NT, etc.

**SMTP:** (Simple Mail Transfer Protocol - Protocolo de Transferencia Simple de correo). Es el protocolo usado para transportar el correo a través de Internet.

**SPAM**: Envío masivo, indiscriminado y no solicitado de publicidad a través de correo electrónico.

**SSL:** (Secure Sockets Layer - Capa de Socket Segura). Protocolo que ofrece funciones de seguridad a nivel de la capa de transporte para TCP.

**TCP:** (Transmission Control Protocol - Protocolo de control de Transmisión). Uno de los protocolos más usados en Internet. Es un protocolo de capa de transporte.

**TELNET:** Telnet es el protocolo estándar de Internet para realizar un servicio de conexión desde un terminal remoto.

**TEXTO PLANO:** (Plain Text) se llama así al documento antes de ser encriptado.

**TROJAN HORSE:** (Caballo de Troya) programa informático que lleva en su interior la lógica necesaria para que el creador del programa pueda acceder al interior del sistema que lo procesa.

**URL:** (Localizador Uniforme de recursos - Uniform Resource Locator). Sistema de direccionamiento estándar para archivos y funciones de Internet, especialmente en el Word Wide Web. El URL esta conformado por el servicio (p. e. http://) más el nombre de la computadora (p. e. www.sfp.gov.ar ) más el directorio y el archivo referido.

**WAN:** Wide Area Network. Red de Area Extensa.

**WEBMIN**: es una aplicación con interface gráfica para la administración de sistemas Unix.

**WWW:** World Wide Web. Estrictamente la Web es la parte de Internet a la que accedemos a través del protocolo HTTP y en consecuencia gracias a browsers normalmente gráficos como Netscape o Internet Explorer.

**Bibliografía**

1. Mario Gerardo Piattini Velthius, Emilio del Peso Navarro. 1998. **Auditoría Informática: un enfoque práctico**. Alfa-Omega - Ra-ma.
2. José Antonio Echenique. 1996. **Auditoría en Informática**. Mc Graw Hill.
3. Humberto David Rosales Herrera. **Determinación de riesgos en los centros de cómputos**. 1996. Editorial Trillas.
4. David Pitts, Hill Ball. **Red Hat Linux Unleashed. The comprehensive solution**. 1998. Sams Publishing.
5. BCRA (Banco Central de la República Argentina). "**Anexo a la Comunicación "A" 2659** – Requisitos operativos mínimos del área de sistemas de información (SI) – Tecnología Informática". 1998.
www.bcra.gov.ar
6. BCRA (Banco Central de la República Argentina). "**Anexo a la Comunicación "C" 30275** – Requisitos operativos mínimos del área de sistemas de información (SI) – Tecnología Informática- Fe de erratas".
2001. www.bcra.gov.ar
7. BCRA (Banco Central de la República Argentina). "**Anexo a la Comunicación "A" 3198** – Texto ordenado actualizado de las Normas sobre Requisitos operativos mínimos del área de sistemas de información (SI) – Tecnología Informática". 2001. www.bcra.gov.ar
8. Cobit (Control Objectives for Information Technology) "**Audit Guidelines**" 3ra. Edición. 2000.
9. Cobit (Control Objectives for Information Technology) "**Control Objectives**" 3ra. Edición. 2000.
10. ISO (International Standard Organization). "**Estándar de Seguridad ISO 17799**"
11. ISO (International Standard Organization). "The Common Criteria for Information Technology Security Evaluation" v2.1
12. DoD (Department of Defense) Rainbow Series Library. "**Trusted Network Interpretation of the TCSEC - Red Book**". 1987.
13. DoD (Department of Defense) Rainbow Series Library. "**Password Management Guideline – Green Book**". 1985.
14. SIGEN (Sindicatura General de la Nación). "**Normas generales control interno**". Resolución SIGEN N° 107/98. 1998.
15. AGN (Auditoría General de la Nación). "**Normas de auditoria externa de la Auditoria General de la Nación**". 1993.
16. ISACA (Information Systems Audit and Control Association). "**Planning the IS Audit**". 1998.
17. ISACA (Information Systems Audit and Control Association). "**Normas generales para la auditoría de los sistemas de información**". 1997.
18. NIST (National Institute of Standards and Technology - U.S. Department of Commerce).

19. NIST (National Institute of Standards and Technology - U.S. Department of Commerce). "**Generally Accepted Principles and Practices for Securing Information Technology Systems**". Marianne Swanson y Barbara Guttman, 1996.
20. NIST (National Institute of Standards and Technology - U.S. Department of Commerce). "**Guide for Developing Security Plans for Information Technology Systems**" Marianne Swanson, 1998.
21. NIST (National Institute of Standards and Technology - U.S. Department of Commerce). "**Security Self- Assessment Guide for Information Technology Systems**" Marianne Swanson, 2001.
22. NIST (National Institute of Standards and Technology - U.S. Department of Commerce). "**Automated Tools for Testing Computer System Vulnerability**" W. Timothy Polk, 1992.
23. Cisco Systems. "**Cisco SAFE: A Security Blueprint for Enterprise Networks**". Sean Convery y Bernie Trudel. 2000.
24. Cisco Systems. "**Beginner's guide to network security**". 2001
25. CERT (Computer Emergency Response Team) "**Tutorial de seguridad**".
26. "**IT Baseline Protection Manual - Standard security safeguards**". Bundesanzeiger – Verlag, Alemania. 2001.
27. Hal Tipton, Micki Krause. "**Handbook of Information Security Management**". Consulting Editors, 1998.
28. "**Internet Security Professional Reference, Second Edition**". New Riders Publishing. 1997.
29. Gonzalo Alvarez Marañón. "**Manual onLine de Criptografía y Seguridad**". Consejo Superior de Investigaciones Científicas (CSIC), Madrid, España. 1997.
30. Tomas Olovsson. "**A Structured Approach to Computer Security**". Department of Computer Engineering, Chalmers University of Technology (Gothenburg – SWEDEN). Technical Report No 122, 1992.
31. Peter Vincent Herzog. "**Open-source security testing methodology manual**", Idea Hamster, GNU,
2001.
32. "**Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network**" Macmillan Computer Publishing. 1998.
33. Steven Shaffler y Alan Simon. "**Network Security**". AP Professional, 1994.
34. Jorge Tomás Curras. "**Transacciones comerciales en Internet**". Columbus Internet Marketing & Consulting. Madrid. www.columbus-digital.com
35. "**SET Software Compliance Testing**". SET Secure Electronic Transaction LLC. www.setco.org
36. "**Seguridad en Internet**". Microsoft. www.microsoft.com
37. Ministerio de Economía de la Nación www.mecon.ar
38. Tim Dierks. "**SSL as a protocol security solution**". Consensus Development Corp. www.consensus.com
42. Portales relativos a seguridad informática:
- xwww.insecure.org

- http://securityfocus.com
- www.hispasec.com
- http://secinf.net
- www.securityportal.com.ar
- www.itsec.gov.uk
- www.privacyexchange.org
- www.seguridadunam.com
- www.unamcert.com