

CAPÍTULO 3

Tesis "Seguridad Informática: Sus
Implicancias e Implementación".
Copyright Cristian F. Borghello 2001
webmaster@cfbsoft.com.ar
www.cfbsoft.com.ar



“Miro a mi alrededor veo que la tecnología ha sobrepasado nuestra humanidad, espero que algún día nuestra humanidad sobrepase la tecnología.”

Albert Einstein

SEGURIDAD LÓGICA

Luego de ver como nuestro sistema puede verse afectado por la falta de Seguridad Física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputos no será sobre los medios físicos sino contra información por él almacenada y procesada.

Así, la Seguridad Física, sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la **información**, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la Seguridad Lógica.

Es decir que la **Seguridad Lógica** consiste en la “aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.”

Existe un viejo dicho en la seguridad informática que dicta que “todo lo que no está permitido debe estar prohibido” y esto es lo que debe asegurar la Seguridad Lógica.

Los objetivos que se plantean serán:

1. Restringir el acceso a los programas y archivos.
2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
3. Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
5. Que la información recibida sea la misma que ha sido transmitida.
6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
7. Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Tesis "Seguridad Informática: Sus Implicancias e Implementación". □ Copyright Cristian F. Borghello 2001 □ webmaster@cfbsoft.com.ar □ www.cfbsoft.com.ar □
--

3.1 CONTROLES DE ACCESO

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso. Al respecto, el National Institute for Standards and Technology (NIST)¹ ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad en cualquier sistema:

3.1.1 IDENTIFICACIÓN Y AUTENTIFICACIÓN

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

¹ <http://www.nist.gov>

Se denomina **Identificación** al momento en que el usuario se da a conocer en el sistema; y **Autenticación** a la verificación que realiza el sistema sobre esta identificación.

Al igual que se consideró para la seguridad física, y basada en ella, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

1. Algo que solamente el individuo conoce: por ejemplo una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, etc.
2. Algo que la persona **posee**: por ejemplo una tarjeta magnética.
3. Algo que el individuo **es** y que lo identifica unívocamente: por ejemplo las huellas digitales o la voz.
4. Algo que el individuo es capaz de **hacer**: por ejemplo los patrones de escritura.

Para cada una de estas técnicas vale lo mencionado en el caso de la seguridad física en cuanto a sus ventajas y desventajas. Se destaca que en los dos primeros casos enunciados, es frecuente que las claves sean olvidadas o que las tarjetas o dispositivos se pierdan, mientras que por otro lado, los controles de autenticación biométricos serían los más apropiados y fáciles de administrar, resultando ser también, los más costosos por lo dificultosos de su implementación eficiente.

Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de allí, a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. Esto se denomina "single log-in" o sincronización de passwords.

Una de las posibles técnicas para implementar esta única identificación de usuarios sería la utilización de un servidor de autenticaciones sobre el cual los usuarios se identifican, y que se encarga luego de autenticar al usuario sobre los restantes equipos a los que éste pueda acceder. Este servidor de autenticaciones no debe ser necesariamente un equipo independiente y puede tener sus funciones distribuidas tanto geográfica como lógicamente, de acuerdo con los requerimientos de carga de tareas.

La Seguridad Informática se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos. Esta administración abarca:

1. Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios. Es necesario considerar que la solicitud de habilitación de un permiso de acceso para un usuario determinado, debe provenir de su superior y, de acuerdo con sus requerimientos específicos de acceso, debe generarse el perfil en el sistema de seguridad, en el sistema operativo o en la aplicación según corresponda.
2. Además, la identificación de los usuarios debe definirse de acuerdo con una norma homogénea para toda la organización.
3. Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos. Las mismas deben encararse desde el punto de vista del sistema operativo, y aplicación por aplicación, pudiendo ser llevadas a cabo por personal de auditoría o por la gerencia propietaria del sistema; siempre sobre la base de que cada usuario disponga del mínimo permiso que requiera de acuerdo con sus funciones.

4. Las revisiones deben orientarse a verificar la adecuación de los permisos de acceso de cada individuo de acuerdo con sus necesidades operativas, la actividad de las cuentas de usuarios o la autorización de cada habilitación de acceso. Para esto, deben analizarse las cuentas en busca de períodos de inactividad o cualquier otro aspecto anormal que permita una redefinición de la necesidad de acceso.
5. Detección de actividades no autorizadas. Además de realizar auditorias o efectuar el seguimiento de los registros de transacciones (pistas), existen otras medidas que ayudan a detectar la ocurrencia de actividades no autorizadas. Algunas de ellas se basan en evitar la dependencia hacia personas determinadas, estableciendo la obligatoriedad de tomar vacaciones o efectuando rotaciones periódicas a las funciones asignadas a cada una.
6. Nuevas consideraciones relacionadas con cambios en la asignación de funciones del empleado. Para implementar la rotación de funciones, o en caso de reasignar funciones por ausencias temporales de algunos empleados, es necesario considerar la importancia de mantener actualizados los permisos de acceso.
7. Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización, llevadas a cabo en forma amistosa o no. Los despidos del personal de sistemas presentan altos riesgos ya que en general se trata de empleados con capacidad para modificar aplicaciones o la configuración del sistema, dejando "bombas lógicas" o destruyendo sistemas o recursos informáticos. No obstante, el personal de otras áreas usuarias de los sistemas también puede causar daños, por ejemplo, introduciendo información errónea a las aplicaciones intencionalmente.

Para evitar estas situaciones, es recomendable anular los permisos de acceso a las personas que se desvincularán de la organización, lo antes posible. En caso de despido, el permiso de acceso debería anularse previamente a la notificación de la persona sobre la situación.

3.1.2 ROLES

Tesis "Seguridad Informática: Sus
Implicancias e Implementación". □
Copyright Cristian F. Borghello 2001 □
webmaster@cfbsoft.com.ar □
www.cfbsoft.com.ar □

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso. Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, etc. En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

3.1.3 TRANSACCIONES

También pueden implementarse controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada.

3.1.4 LIMITACIONES A LOS SERVICIOS

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema. Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un

determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.

3.1.5 MODALIDAD DE ACCESO

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser:

- **Lectura:** el usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.
- **Escritura:** este tipo de acceso permite agregar datos, modificar o borrar información.
- **Ejecución:** este acceso otorga al usuario el privilegio de ejecutar programas.
- **Borrado:** permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.
- Todas las anteriores.

Además existen otras modalidades de acceso especiales, que generalmente se incluyen en los sistemas de aplicación:

- **Creación:** permite al usuario crear nuevos archivos, registros o campos.
- **Búsqueda:** permite listar los archivos de un directorio determinado.

3.1.5 UBICACIÓN Y HORARIO

Tesis "Seguridad Informática: Sus
Implicancias e Implementación".
Copyright Cristian F. Borghello 2001
webmaster@cfbsoft.com.ar
www.cfbsoft.com.ar

El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas. En cuanto a los horarios, este tipo de controles permite limitar el acceso de los usuarios a determinadas horas de día o a determinados días de la semana. De esta forma se mantiene un control más restringido de los usuarios y zonas de ingreso.

Se debe mencionar que estos dos tipos de controles siempre deben ir acompañados de alguno de los controles anteriormente mencionados.

3.1.6 CONTROL DE ACCESO INTERNO

3.1.6.1 PALABRAS CLAVES (PASSWORDS)

Generalmente se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones. Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo. Sin embargo cuando el usuario se ve en la necesidad de utilizar varias palabras clave para acceder a diversos sistemas encuentra difícil recordarlas y probablemente las escriba o elija palabras fácilmente deducibles, con lo que se ve disminuida la utilidad de esta técnica.

Se podrá, por años, seguir creando sistemas altamente seguros, pero en última instancia cada uno de ellos se romperá por este eslabón: la elección de passwords débiles.

Es mi deseo que después de la lectura del presente quede la idea útil de usar passwords seguras ya que aquí radican entre el 90% y 99% de los problemas de seguridad planteados.

- **Sincronización de passwords:** consiste en permitir que un usuario acceda con la misma password a diferentes sistemas interrelacionados y, su actualización automática en todos ellos en caso de ser modificada. Podría pensarse que esta es una característica negativa para la seguridad de un sistema, ya que una vez descubierta la clave de un usuario, se podría tener acceso a los múltiples sistemas a los que tiene acceso dicho usuario. Sin embargo, estudios hechos muestran que las personas normalmente suelen manejar una sola password para todos los sitios a los que tengan acceso, y que si se los fuerza a elegir diferentes passwords tienden a guardarlas escritas para no olvidarlas, lo cual significa un riesgo aún mayor. Para implementar la sincronización de passwords entre sistemas es necesario que todos ellos tengan un alto nivel de seguridad.
- **Caducidad y control:** este mecanismo controla cuándo pueden y/o deben cambiar sus passwords los usuarios. Se define el período mínimo que debe pasar para que los usuarios puedan cambiar sus passwords, y un período máximo que puede transcurrir para que éstas caduquen.

3.1.6.2 ENCRIPCIÓN

Tesis "Seguridad Informática: Sus
Implicancias e Implementación".
Copyright Cristian F. Borghello 2001
webmaster@cfbsoft.com.ar
www.cfbsoft.com.ar

La información encriptada solamente puede ser descryptada por quienes posean la clave apropiada. La encriptación puede proveer de una potente medida de control de acceso. Este tema será abordado con profundidad en el Capítulo sobre Protección del presente.

3.1.6.3 LISTAS DE CONTROL DE ACCESOS

Se refiere a un registro donde se encuentran los nombres de los usuarios que obtuvieron el permiso de acceso a un determinado recurso del sistema, así como la modalidad de acceso permitido. Este tipo de listas varían considerablemente en su capacidad y flexibilidad.

3.1.6.4 LÍMITES SOBRE LA INTERFASE DE USUARIO

Estos límites, generalmente, son utilizados en conjunto con las listas de control de accesos y restringen a los usuarios a funciones específicas. Básicamente pueden ser de tres tipos: menús, vistas sobre la base de datos y límites físicos sobre la interfase de usuario. Por ejemplo los cajeros automáticos donde el usuario sólo puede ejecutar ciertas funciones presionando teclas específicas.

3.1.6.5 ETIQUETAS DE SEGURIDAD

Consiste en designaciones otorgadas a los recursos (como por ejemplo un archivo) que pueden utilizarse para varios propósitos como control de accesos, especificación de medidas de protección, etc. Estas etiquetas no son modificables.

3.1.7 CONTROL DE ACCESO EXTERNO

3.1.7.1 DISPOSITIVOS DE CONTROL DE PUERTOS

Estos dispositivos autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem.

3.1.7.2 FIREWALLS O PUERTAS DE SEGURIDAD

Permiten bloquear o filtrar el acceso entre dos redes, usualmente una privada y otra externa (por ejemplo Internet). Los firewalls permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de la organización. Este tema será abordado con posterioridad.

3.1.7.3 ACCESO DE PERSONAL CONTRATADO O CONSULTORES

Debido a que este tipo de personal en general presta servicios temporarios, debe ponerse especial consideración en la política y administración de sus perfiles de acceso.

3.1.7.4 ACCESOS PÚBLICOS

Para los sistemas de información consultados por el público en general, o los utilizados para distribuir o recibir información computarizada (mediante, por ejemplo, la distribución y recepción de formularios en soporte magnético, o la consulta y recepción de información a través del correo electrónico) deben tenerse en cuenta medidas especiales de seguridad, ya que se incrementa el riesgo y se dificulta su administración.

Debe considerarse para estos casos de sistemas públicos, que un ataque externo o interno puede acarrear un impacto negativo en la imagen de la organización.

3.1.8 ADMINISTRACIÓN

Tesis "Seguridad Informática: Sus
Implicancias e Implementación".
Copyright Cristian F. Borghello 2001
webmaster@cfbsoft.com.ar
www.cfbsoft.com.ar

Una vez establecidos los controles de acceso sobre los sistemas y la aplicación, es necesario realizar una eficiente administración de estas medidas de seguridad lógica, lo que involucra la implementación, seguimientos, pruebas y modificaciones sobre los accesos de los usuarios de los sistemas.

La política de seguridad que se desarrolle respecto a la seguridad lógica debe guiar a las decisiones referidas a la determinación de los controles de accesos y especificando las consideraciones necesarias para el establecimiento de perfiles de usuarios.

La definición de los permisos de acceso requiere determinar cual será el nivel de seguridad necesario sobre los datos, por lo que es imprescindible clasificar la información, determinando el riesgo que produciría una eventual exposición de la misma a usuarios no autorizados.

Así los diversos niveles de la información requerirán diferentes medidas y niveles de seguridad.

Para empezar la implementación, es conveniente comenzar definiendo las medidas de seguridad sobre la información más sensible o las aplicaciones más críticas, y avanzar de acuerdo a un orden de prioridad descendiente, establecido alrededor de las aplicaciones.

Una vez clasificados los datos, deberán establecerse las medidas de seguridad para cada uno de los niveles.

Un programa específico para la administración de los usuarios informáticos desarrollado sobre la base de las consideraciones expuestas, puede constituir un compromiso vacío, si no existe una conciencia de la seguridad organizacional por parte de todos los empleados. Esta conciencia de la seguridad puede alcanzarse mediante el ejemplo del personal directivo en el cumplimiento de las políticas y el establecimiento de compromisos firmados por el personal, donde se especifique la responsabilidad de cada uno.

Pero además de este compromiso debe existir una concientización por parte de la administración hacia el personal en donde se remarque la importancia de la información y las consecuencias posibles de su pérdida o apropiación de la misma por agentes extraños a la organización.

3.1.8.1 ADMINISTRACIÓN DEL PERSONAL Y USUARIOS

3.1.8.1.1 Organización del Personal

Este proceso lleva generalmente cuatro pasos:

1. Definición de puestos: debe contemplarse la máxima separación de funciones posibles y el otorgamiento del mínimo permiso de acceso requerido por cada puesto para la ejecución de las tareas asignadas.
2. Determinación de la sensibilidad del puesto: para esto es necesario determinar si la función requiere permisos riesgosos que le permitan alterar procesos, perpetrar fraudes o visualizar información confidencial.
3. Elección de la persona para cada puesto: requiere considerar los requerimientos de experiencia y conocimientos técnicos necesarios para cada puesto. Asimismo, para los puestos definidos como críticos puede requerirse una verificación de los antecedentes personales
4. Entrenamiento inicial y continuo del empleado: cuando la persona seleccionada ingresa a la organización, además de sus responsabilidades individuales para la ejecución de las tareas que se asignen, deben comunicárseles las políticas

Tesis "Seguridad Informática: Sus
Implicancias e Implementación".
Copyright Cristian F. Borghello 2001
webmaster@cfbsoft.com.ar
www.cfbsoft.com.ar

organizacionales, haciendo hincapié en la política de seguridad. El individuo debe conocer las disposiciones organizacionales, su responsabilidad en cuanto a la seguridad informática y lo que se espera de él.

Esta capacitación debe orientarse a incrementar la conciencia de la necesidad de proteger los recursos informáticos y a entrenar a los usuarios en la utilización de los sistemas y equipos para que ellos puedan llevar a cabo sus funciones en forma segura, minimizando la ocurrencia de errores (principal riesgo relativo a la tecnología informática).

Sólo cuando los usuarios están capacitados y tienen una conciencia formada respecto de la seguridad pueden asumir su responsabilidad individual. Para esto, el ejemplo de la gerencia constituye la base fundamental para que el entrenamiento sea efectivo: el personal debe sentir que la seguridad es un elemento prioritario dentro de la organización.

3.2 NIVELES DE SEGURIDAD INFORMÁTICA

El estándar de niveles de seguridad mas utilizado internacionalmente es el TCSEC Orange Book², desarrollado en 1983 de acuerdo a las normas de seguridad en computadoras del Departamento de Defensa de los Estados Unidos.

Los niveles describen diferentes tipos de seguridad del Sistema Operativo y se enumeran desde el mínimo grado de seguridad al máximo.

Estos niveles han sido la base de desarrollo de estándares europeos (ITSEC/ITSEM) y luego internacionales (ISO/IEC).

Cabe aclarar que cada nivel requiere todos los niveles definidos anteriormente: así el subnivel B2 abarca los subniveles B1, C2, C1 y el D.

3.2.1 NIVEL D

Tesis "Seguridad Informática: Sus <input type="checkbox"/>
Implicancias e Implementación". <input type="checkbox"/>
Copyright Cristian F. Borghello 2001 <input type="checkbox"/>
webmaster@cfbsoft.com.ar <input type="checkbox"/>
www.cfbsoft.com.ar <input type="checkbox"/>

Este nivel contiene sólo una división y está reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad. Sin sistemas no confiables, no hay protección para el hardware, el sistema operativo es inestable y no hay autenticación con respecto a los usuarios y sus derechos en el acceso a la información. Los sistemas operativos que responden a este nivel son MS-DOS y System 7.0 de Macintosh.

3.2.2 NIVEL C1: PROTECCIÓN DISCRECIONAL

Se requiere identificación de usuarios que permite el acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso.

Muchas de las tareas cotidianas de administración del sistema sólo pueden ser realizadas por este "super usuario"; quien tiene gran responsabilidad en la seguridad del

² Orange Book. Department Of Defense. Library N° S225, 711. EEUU. 1985. <http://www.doe.gov>

mismo. Con la actual descentralización de los sistemas de cómputos, no es raro que en una organización encontremos dos o tres personas cumpliendo este rol. Esto es un problema, pues no hay forma de distinguir entre los cambios que hizo cada usuario.

A continuación se enumeran los requerimientos mínimos que debe cumplir la clase C1:

- Acceso de control discrecional: distinción entre usuarios y recursos. Se podrán definir grupos de usuarios (con los mismos privilegios) y grupos de objetos (archivos, directorios, disco) sobre los cuales podrán actuar usuarios o grupos de ellos.
- Identificación y Autenticación: se requiere que un usuario se identifique antes de comenzar a ejecutar acciones sobre el sistema. El dato de un usuario no podrá ser accedido por un usuario sin autorización o identificación.

3.2.3 NIVEL C2: PROTECCIÓN DE ACCESO CONTROLADO

Este subnivel fue diseñado para solucionar las debilidades del C1. Cuenta con características adicionales que crean un ambiente de acceso controlado. Se debe llevar una auditoria de accesos e intentos fallidos de acceso a objetos. Tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización.

Requiere que se audite el sistema. Esta auditoría es utilizada para llevar registros de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios. La auditoría requiere de autenticación adicional para estar seguros de que la persona que ejecuta el comando es quien dice ser. Su mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos.

Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de administración del sistema sin necesidad de ser administradores. Permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.

3.2.4 NIVEL B1: SEGURIDAD ETIQUETADA

Tesis "Seguridad Informática: Sus <input type="checkbox"/>
Implicancias e Implementación". <input type="checkbox"/>
Copyright Cristian F. Borghello 2001 <input type="checkbox"/>
webmaster@cfbsoft.com.ar <input type="checkbox"/>
www.cfbsoft.com.ar <input type="checkbox"/>

Este subnivel, es el primero de los tres con que cuenta el nivel B. Soporta seguridad multinivel, como la secreta y ultrasecreta. Se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio. A cada objeto del sistema (usuario, dato, etc.) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, etc.) y con unas categorías (contabilidad, nóminas, ventas, etc.).

Cada usuario que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa. Es decir que cada usuario tiene sus objetos asociados. También se establecen controles para limitar la propagación de derecho de accesos a los distintos objetos.

3.2.5 NIVEL B2: PROTECCIÓN ESTRUCTURADA

Requiere que se etiquete cada objeto de nivel superior por ser padre de un objeto inferior. La Protección Estructurada es la primera que empieza a referirse al problema de un objeto a un nivel mas elevado de seguridad en comunicación con otro objeto a un nivel inferior. Así, un disco rígido será etiquetado por almacenar archivos que son accedidos por distintos usuarios.

El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas; y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.

3.2.6 NIVEL B3: DOMINIOS DE SEGURIDAD

Refuerza a los dominios con la instalación de hardware: por ejemplo el hardware de administración de memoria se usa para proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos de diferentes dominios de seguridad. Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido

Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y testeos ante posibles violaciones. Este nivel requiere que la terminal del usuario se conecte al sistema por medio de una conexión segura.

Además, cada usuario tiene asignado los lugares y objetos a los que puede acceder.

3.2.7 NIVEL A: PROTECCIÓN VERIFICADA

Tesis "Seguridad Informática: Sus
Implicancias e Implementación".
Copyright Cristian F. Borghello 2001
webmaster@cfbsoft.com.ar
www.cfbsoft.com.ar

Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema.

Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. El software y el hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento.

SEGURIDAD LÓGICA	1
3.1 CONTROLES DE ACCESO	2
3.1.1 IDENTIFICACIÓN Y AUTENTIFICACIÓN	2
3.1.2 ROLES.....	4
3.1.3 TRANSACCIONES.....	4
3.1.4 LIMITACIONES A LOS SERVICIOS.....	4
3.1.5 MODALIDAD DE ACCESO	5
3.1.5 UBICACIÓN Y HORARIO	5
3.1.6 CONTROL DE ACCESO INTERNO	5
3.1.6.1 Palabras Claves (Passwords).....	5
3.1.6.2 Encriptación	6
3.1.6.3 Listas de Control de Accesos.....	6
3.1.6.4 Límites sobre la Interfase de Usuario	6
3.1.6.5 Etiquetas de Seguridad.....	7
3.1.7 CONTROL DE ACCESO EXTERNO.....	7
3.1.7.1 Dispositivos de Control de Puertos	7
3.1.7.2 Firewalls o Puertas de Seguridad	7
3.1.7.3 Acceso de Personal Contratado o Consultores	7
3.1.7.4 Accesos Públicos	7
3.1.8 ADMINISTRACIÓN	7
3.1.8.1 Administración del Personal y Usuarios.....	8
3.2 NIVELES DE SEGURIDAD INFORMÁTICA.....	9
3.2.1 NIVEL D.....	9
3.2.2 NIVEL C1: PROTECCIÓN DISCRECIONAL.....	9
3.2.3 NIVEL C2: PROTECCIÓN DE ACCESO CONTROLADO	10
3.2.4 NIVEL B1: SEGURIDAD ETIQUETADA	10
3.2.5 NIVEL B2: PROTECCIÓN ESTRUCTURADA.....	11
3.2.6 NIVEL B3: DOMINIOS DE SEGURIDAD.....	11
3.2.7 NIVEL A: PROTECCIÓN VERIFICADA.....	11