Universidad F.A.S.T.A.

Facultad de Ciencias Económicas

Tesis de Graduación

Tema:

"Aplicación de la Biometría"

Autor: **Lucila María Verde**

Carrera: **Contador Público Nacional**

Cátedra: **Seminario de Graduación**

Tutor: **C.P.N. Cecilia Beatriz Mendez**

Asesoramiento metodológico:

Dra. Cipriano Laura

Lic. Ramirez Amelia

Departamento de Metodología de la Investigación

Mar del Plata, Febrero de 2003

JUSTIFICACION DEL TRABAJO

A nadie escapa la enorme influencia que ha alcanzado la informática en la vida diaria de las personas y organizaciones. Las transacciones comerciales, la comunicación, los procesos industriales, las investigaciones, la seguridad, etc, son todos aspectos que dependen cada día mas de un adecuado desarrollo de la tecnología informática.

El reconocimiento de la necesidad de seguridad es una conclusión natural de la creencia de que la información es un recurso organizacional fundamental.

El desarrollo de la sociedad de la información, con el aumento incesante de las comunicaciones, conlleva a la necesidad de asegurar la identidad de los usuarios en los accesos a los datos informatizados. La importancia y valor de estos datos manejados, motiva a los impostores a superar los sistemas de seguridad existentes, lo que obliga a los usuarios a instalar nuevos sistemas cada vez más potentes y fiables.

A través del presente trabajo, se pretende analizar la biometría como una solución para superar los fraudes ocasionados en la verificación de la identidad de un individuo en el acceso a la información.

Este tema cobra una importancia fundamental, dado que en los últimos años se ha manifestado una creciente cantidad de incidentes de seguridad. Se estima que solamente en el año 2000, el costo mundial de estos incidentes fue de 16.000 millones de euros.

Además, resulta interesante tratar un tema que resulta tan actual y que continuamente se pone sobre el tapete, pero del cual en realidad se conoce muy poco.

Diseño de la Investigación

Tema:

Aplicación de la biometría

Problema:

Biometría. Posible solución a la vulnerabilidad de la seguridad lógica actual en el acceso a la información a través de claves de identificación.

Objetivo general:

Determinar si la biometría puede ser una solución a la vulnerabilidad que presenta hoy en día la seguridad lógica en el acceso a la información a través de claves de identificación.

Objetivos Específicos:

- Analizar y comprender el concepto de seguridad lógica dentro del concepto general de seguridad informática.

- Conocer las debilidades que posee la seguridad lógica en la actualidad en el acceso a la información a través de claves de identificación.

- Determinar las consecuencias que puede generar la vulnerabilidad de la seguridad lógica en el acceso a la información.

- Explicar el concepto y funcionamiento de la biometría.

- Analizar las características y el funcionamiento de las claves de identificación.

- Demostrar los beneficios del uso de los sistemas biométricos.

Hipótesis:

La biometría es una solución a las debilidades que posee en la actualidad la seguridad lógica en el acceso a la información a través de claves de identificación.

Variables:

- Soluciones biométricas
- Debilidades de la seguridad lógica en el acceso a la información a través de claves de identificación.

Indicadores:

- Dispositivos biométricos
- Claves de acceso o passwords
- Ataques informáticos

Tipo de investigación

- S/ su profundidad: Descriptiva y explicativa
- S/ el tiempo: Sincrónica
- S/ la fuente: Primaria y secundaria
- S/ el objetivo: Básica
- S/ el enfoque: Micro

Fuentes de información

- Entrevistas a personas vinculadas al tema
- Fuentes secundarias de información como libros, investigaciones científicas, revistas especializadas y publicaciones.
- Búsquedas realizadas en internet

Esquema de trabajo

A. MARCO TEÓRICO

A.1. Concepto y evolución del término seguridad

La "Seguridad es una necesidad básica. Estando interesada en la prevención de la vida y las posesiones, es tan antigua como ella".

Los primeros conceptos de seguridad se evidencian en los inicios de la escritura con los Sumerios (3000 A.C.) o el Hammurabi (2000 A.C.). También la Biblia, Homero, Cicerón, Cesat han sido autores de obras en donde aparecen ciertos rasgos de la seguridad en la guerra y el gobierno.

Se sabe que los primitivos, para evitar amenazas, reaccionaban con los mismos métodos defensivos de los animales: luchando o huyendo, para eliminar o evitar la causa. Así la pugna por la vida se convertía en una parte esencial y los conceptos de alertar, detectar, evitar, alarmar y reaccionar ya eran manejados por ellos.

Como todo concepto, la Seguridad se ha desarrollado y ha seguido una evolución dentro de las organizaciones sociales. La sociedad se conformó en familias, y esto se convirtió en un elemento limitante para huir. Se tuvieron que concebir nuevas estrategias de intimidación y disuasión para convencer al atacante que las pérdidas eran inaceptables contra las posibles ganancias.

La primera evidencia de una cultura y organización en seguridad "madura" aparece en los documentos de la Res Pública (estado) de Roma Imperial y Republicana.

El próximo paso de la Seguridad fue la especialización. Así nace la Seguridad Externa (aquella que se preocupa por la amenaza de entes externos hacia la organización); y la Seguridad Interna (aquella preocupada por las amenazas de la organización con la organización misma).

Desde el siglo XVIII, los descubrimientos científicos y el conocimiento resultante de la imprenta han contribuido a la cultura de la seguridad. Los principios de probabilidad, predicción y reducción de fallos y pérdidas han traído nueva luz a los sistemas de seguridad.

La Seguridad moderna se originó con la Revolución Industrial para combatir los delitos y movimientos laborales, tan comunes en aquella época. Finalmente, un teórico y pionero del Management, Henry Fayol en 1919 identificó la Seguridad como una de las funciones empresariales, luego de la técnica, comercial, financiera, contable y directiva.

Al definir el objeto de la Seguridad, Fayol dice "...salvaguardar propiedades y personas contra el robo, fuego, contrarrestar huelgas y felonías, y de forma amplia todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio."

Las medidas de seguridad a las que se refiere Fayol, se restringían exclusivamente a lo físico de la instalación, ya que el mayor activo era justamente ese: los equipos. Con la aparición de los "cerebros electrónicos", esta mentalidad se mantuvo ya que el pensamiento de esa época era: ¿quién sería capaz de entender estos complicados aparatos como para poner en peligro la integridad de los datos por ellos utilizados?

Hoy, desde el punto de vista técnico, la Seguridad está en manos de la dirección de las organizaciones y, en última instancia, en cada uno de nosotros y en nuestro grado de concientización respecto de la importancia de la información y el conocimiento en este nuevo milenio.

Es en este proceso en el que se aprecia que no se ha añadido ningún nuevo concepto a los ya conocidos en la antigüedad: los actuales sólo son perfeccionamientos de aquellos: llaves, cerraduras, cajas fuerte, puertas blindadas, trampas, vigilancia, etc.

Para conceptualizar el término Seguridad podemos hablar de tres figuras:

1) El poseedor del valor: **Protector**
2) Un aspirante a poseedor: **Competidor –Agresor**
3) Un elemento a proteger: **Valor**

Luego, podemos definir la Seguridad como: La interrelación dinámica (competencia) entre el agresor y el protector para obtener (o conservar) el valor tratado. De esta manera la Seguridad es un problema de antagonismo y competencia, ya que si no existe un competidor-amenaza el problema no es de seguridad.

A.2. Seguridad Informática

La seguridad informática es un elemento al que se le da relativa importancia entre las actividades comerciales. Sólo es tenida realmente en cuenta cuando nos hemos visto perjudicados por hechos accidentales o intencionales, y luego de producida la pérdida consecuente. Cuando ocurre un

desastre, recuperar la información es una de las principales prioridades para las empresas. Sin computadoras, teléfonos, fax y correo electrónico, las organizaciones no pueden operar.

Como primer paso para pretender conceptualizar la Seguridad Informática, debemos conocer las características de lo que se pretende proteger: **la información**.

Así, definimos Dato como la unidad mínima con la que se compone cierta información.

La Información "es una segregación de datos que tiene un significado específico más allá de cada uno de éstos", y tendrá un sentido particular según cómo y quién la procese. En otras palabras, la información es un conjunto de datos debidamente organizados que nos agregan conocimientos.

Establecer el valor de la información resulta bastante dificultoso, pues constituye un recurso que en muchos casos no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos y la documentación.

Existe información que debe o puede ser pública, puede ser visualizada por cualquier persona (por ejemplo el índice de analfabetismo de un país); y aquella que debe ser privada: sólo puede ser visualizada por un grupo selecto de personas que trabaja con ella (por ejemplo antecedentes médicos). En esta última, debemos maximizar nuestros esfuerzos para preservarla de ese modo, reconociendo las siguientes características en la Información:

1. Es crítica: es indispensable para garantizar la continuidad operativa.
2. Es valiosa: es un activo con valor en sí misma.
3. Es sensitiva: debe ser conocida por las personas que la procesan y sólo por ellas.

La **Integridad de la Información** es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles. Una falla de integridad puede estar dada por anomalías en hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

La **Disponibilidad u Operatividad de la Información** es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Es decir, la recepción por parte de quienes hayan de ser sus destinatarios

autorizados, así como la posibilidad de acceso por quienes estén autorizados y cuando la necesiten.

La **Confidencialidad de la Información** es la necesidad de que la misma sólo sea conocida por personas autorizadas. De algún modo es un concepto relacionado con la **privacidad**, como derecho de las personas a determinar qué datos suyos pueden ser conocidos, por parte de quiénes y durante cuánto tiempo. En casos de falta de confidencialidad, la Información puede provocar daños severos a su dueño (por ejemplo: conocer los antecedentes médicos de una persona) o volverse obsoleta (por ejemplo: los planes de desarrollo de un producto que se filtran a una empresa competidora).

El **Control sobre la Información** permite asegurar que sólo los usuarios autorizados pueden decidir cuándo y cómo permitir el acceso a la misma.

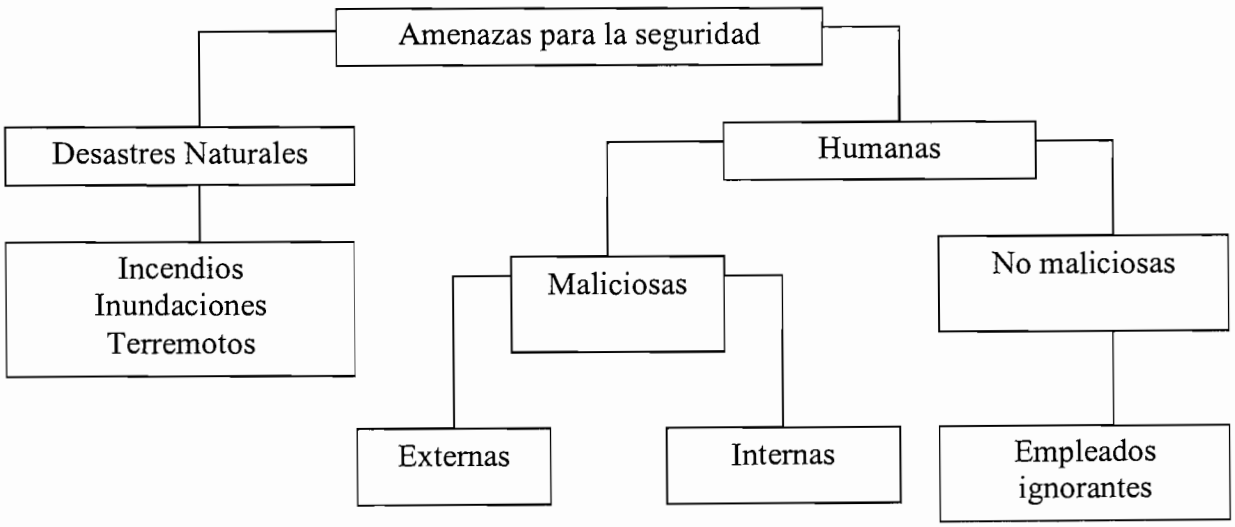
La **Autenticidad** permite definir que la Información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información validando la misma, para evitar suplantación de identidades.

La Seguridad Informática indicará el índice en que un sistema informático está libre de todo peligro, daño o riesgo. Esta característica es muy difícil de conseguir en un 100% por lo que sólo se habla de Fiabilidad y se la define como "...la probabilidad de que un sistema se comporte tal y como se espera de él"[1], y se habla de sistema fiable en vez de sistema seguro.

Luego para garantizar que un sistema sea Fiable, se deberán garantizar las características ya mencionadas. Se deberá conocer "qué es lo que queremos proteger", "de quién lo queremos proteger", "cómo se puede lograr esto técnicamente", para luego concluir con la formulación de estrategias adecuadas de seguridad tendientes a la disminución de los riesgos (se define riesgo como la proximidad o posibilidad de daño sobre un bien).

Las amenazas que atentan contra la Seguridad Informática pueden resumirse en el siguiente gráfico:

[1] HUERTA, Antonio Villalón. "**Seguridad en Unix y Redes**". Versión 1.2 Digital – Open Publication License v.10. 2 de Octubre de 2000.en: http://www.kriptopolis.com



Cabe definir amenaza, en el entorno informático, como cualquier elemento que comprometa al sistema.

B. INTRODUCCION

B.1. Seguridad física y Seguridad lógica

A los fines de este trabajo, se definen dos componentes de la Seguridad Informática que resulta necesario conocer: Seguridad Física y Seguridad Lógica, ya que para muchas personas la seguridad, aplicada a la información se asocia sólo con aspectos parciales, generalmente relacionados con la disponibilidad y la seguridad física, pero soslayan otros aspectos más relacionados con la integridad y con la confidencialidad de la información, y con la seguridad lógica más que con la física.

Seguridad Física

La seguridad física se refiere a la seguridad de las instalaciones de computación, su equipo y software por medios físicos. Consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro de cómputos.

Las principales amenazas que se prevén en la seguridad física son:

- Desastres naturales, incendios accidentales, tormentas e inundaciones.
- Amenazas ocasionadas por el hombre.
- Disturbios, sabotajes internos y externos deliberados.

Los **incendios** son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas. El fuego es una de las principales amenazas contra la seguridad, es considerado el enemigo número uno de las computadoras ya que puede destruir fácilmente los equipos, archivos de información y programas. Los centros de cómputos deben estar provistos de equipos para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.

En relación a las condiciones climatológicas, normalmente se reciben por anticipado los avisos de **tormentas, tempestades, tifones y catástrofes**

sísmicas similares. La comprobación de los informes climatológicos permite que se tomen precauciones adicionales, tales como retirada de objetos móviles, provisión de calor, iluminación o combustible.

Trabajar con computadoras implica trabajar con **electricidad**. Por lo tanto ésta es una de las principales áreas a considerar en la seguridad física. Además es una problemática que abarca desde el usuario hogareño hasta la gran empresa. En la medida que los sistemas se vuelven más complicados, se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones adecuadas.

El **control de acceso** no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.

En cuanto a las **acciones hostiles**, hay que tener en cuenta que las computadoras son posesiones valiosas de las empresas y están expuestas, de la misma manera que lo están las piezas de stock o incluso el dinero. Por su parte, el software, es una propiedad muy fácilmente sustraíble y las cintas y discos son fácilmente copiados sin dejar ningún rastro.

Además es frecuente que los operadores utilicen la computadora de la empresa para realizar trabajos privados o para otras organizaciones y, de esta manera robar tiempo de máquina.

Seguridad Lógica

Es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputos no será sobre los medios físicos sino contra la información por él almacenada y procesada, ya que ésta es el activo más importante que se posee. 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 a hacerlo.

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

El National Institute for Standars and Technology (NIST) ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad lógica en cualquier sistema:

1) Identificación y autenticación

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.

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.

En todos los sistemas multiusuario, cada usuario posee un identificador (ID) que define quién es y que lo identifica unívocamente en el sistema diferenciándolo del resto. Usualmente este identificador es un código o nombre de usuario.

Una vez identificado el usuario, es necesario que éste demuestre de algún modo que es quien dice ser. Existen cuatro técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

a) *Algo que solamente el individuo conoce*: este es el método más común de autentificación, y consiste en asociar al identificativo de usuario una palabra de paso, una clave secreta de acceso o password, un número de identificación personal o pin. La autentificación se basa en que sólo el usuario identificado conoce la contraseña asociada, por lo tanto esta palabra demuestra que el usuario es quien dice ser.

b) *Algo que la persona posee:* En este caso el usuario tiene algún objeto que demuestra su identidad. El objeto utilizado para autentificar puede ser una llave, una placa, una tarjeta magnética o cualquier otro dispositivo hardware que permita el acceso.

c) *Algo que el individuo es:* Este método se basa en autentificar al usuario mediante alguna característica física que lo identifica unívocamente. Entre las más usuales se encuentran las huellas digitales, el iris o la voz.

d) *Algo que el individuo es capaz de hacer*: Este método se basa en aptitudes o hábitos del usuario, por ejemplo los patrones de escritura.

2) Roles

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso. Algunos ejemplo de roles serían los siguientes: programador, gerente, administrador de sistemas, etc.

3) Transacciones

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

4) Limitaciones a los servicios

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización 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 software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.

5) Modalidad de acceso

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

a) Lectura: el usuario puede únicamente leer o visualizar la información pero no puede alterarla.

b) Escritura: este tipo de acceso permite agregar datos, modificar o borrar información.

c) Ejecución: este acceso otorga al usuario el privilegio de ejecutar programas.

d) Borrado: permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos).

6) Ubicación y horario

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

B.2. Seguridad y protección

Se debe hacer una distinción entre seguridad y protección. El problema de la seguridad consiste en lograr que los recursos de un sistema sean, bajo toda circunstancia, utilizados para los fines previstos. Para eso se utilizan mecanismos de protección. Es importante destacar que la protección absoluta contra el uso malicioso de los sistemas es imposible, y que se debe lograr que esa protección no obstaculice el uso del sistema por parte de los usuarios autorizados.

Demasiada seguridad podría ser contraproducente si es muy engorrosa para los usuarios, pues estos tenderían a eludir los procedimientos para facilitarse la vida. Los mecanismos de protección deben ser simples y construidos en las capas más básicas del sistema, y adicionalmente deben ser psicológicamente aceptados por los usuarios.

Seleccionar las medidas de seguridad a implementar requiere considerar el equilibrio entre los intereses referidos a la seguridad, los requerimientos operacionales y la "amigabilidad" para el usuario.

Para ilustrar lo antedicho imaginemos una computadora "extremadamente" segura:

- Instalada a 20 metros bajo tierra en un recinto de hormigón.
- Aislada informáticamente de otras computadoras.
- Aislada eléctricamente y alimentada por un sistema autónomo.

Ahora imaginemos la utilidad de "esta super segura computadora": tendiente a nula.

Con esto se refleja que la Seguridad y la Utilidad de una computadora son inversamente proporcionales; es decir que al incrementar la seguridad en un sistema informático, su operatividad desciende y viceversa.

$$\text{Operatividad} = \frac{1}{\text{Seguridad}}$$

Como se observa en el gráfico N°1 esta función se vuelve exponencial al acercarse al 100% de seguridad. Los costos se disparan por los complejos estudios que deberán realizar para mantener este grado de seguridad.

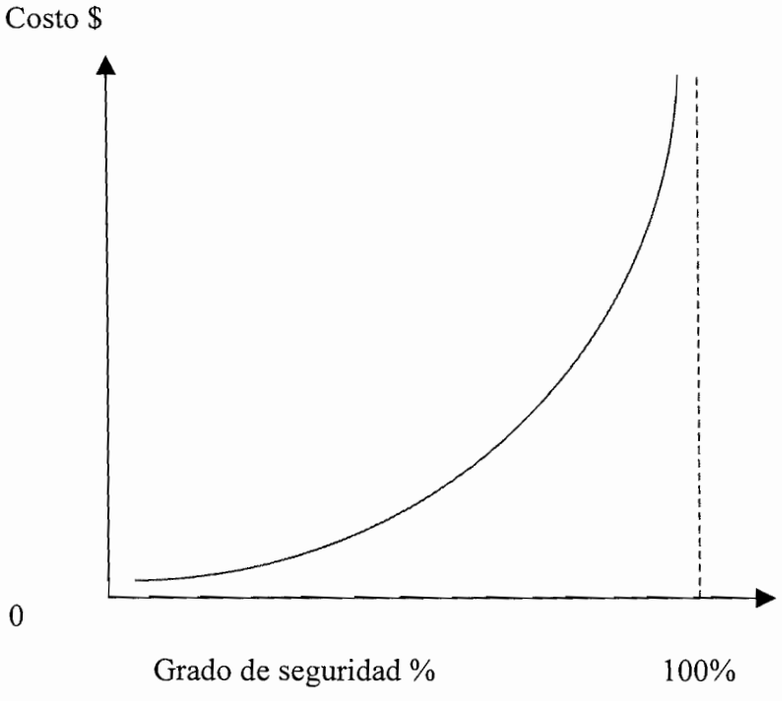


Gráfico 1: Relación Operatividad–Seguridad. Fuente: ALDEGANI, Gustavo Miguel. Seguridad Informática. MP Ediciones. 1°Edición. Argentina. 1997. Pág. 26

El amplio desarrollo de las nuevas tecnologías informáticas está ofreciendo un nuevo campo de acción a conductas antisociales y delictivas

manifestadas en formas antes imposibles de imaginar. La mayoría del mundo informático desconoce la magnitud del problema con el que se enfrenta y, generalmente no se invierte en el capital humano y económico necesarios para prevenir el daño y/o pérdida de la información que, en última instancia es el conocimiento con el que se cuenta.

A pesar de los numerosos ataques e infecciones sufridos por todo tipo de organizaciones e instituciones, éstas aún no se toman la seguridad en serio. Por desgracia, aún son muchas las empresas que no actualizan regularmente sus antivirus, y que no tienen ningún sistema de protección instalado. Y si lo tienen, en muchos casos está tan anticuado que resulta completamente inefectivo ante la creciente sofisticación de los hackers, cada vez más hábiles para penetrar en los sistemas.

Para las empresas, implementar una política de seguridad efectiva, protección adecuada y siempre actualizada debe ser algo básico. Hoy en día, la mayoría de las comunicaciones, datos y recursos, descansan en sistemas informáticos, ya sea en aplicaciones de software como en bases de datos. Por ello, cualquier vulnerabilidad puede costar muy cara: pérdida de datos, robo de información confidencial, pérdida de horas y dinero en soluciones tardías y, por supuesto mala imagen de cara al público y a las demás empresas.

Para conseguir una protección adecuada de sistemas y redes informáticas es necesario implementar soluciones tecnológicas.

C. MÉTODOS PARA LA RECOPILACION DE LA INFORMACIÓN

Las fuentes de información a las que se han recurrido para recolectar los datos que han permitido la elaboración de este trabajo fueron:

a) Entrevistas a personas vinculadas al tema.

b) Búsquedas realizadas en internet.

c) Fuentes secundarias de información como investigaciones científicas, libros y revistas especializadas.

C.1. Entrevistas a personas vinculadas al tema

La selección de las personas a entrevistar se hizo siguiendo las siguientes pautas:

- *Objetividad*: Debían ser personas que tuviesen un punto de vista objetivo y desinteresado sobre el tema.
- *Experiencia:* A su vez, debían ser personas que tuvieran conocimiento acerca de la biometría y la seguridad informática, por estar vinculadas de alguna manera a esta problemática.

Los seleccionados por cumplir los parámetros establecidos fueron:

- Leonardo Tadei
- Federico Cuñado
- Beny Blom
- Nancy Medina
- Sandra Caielli
- Carlos Rossi
- Luciano Tornini
- Paola Ragon

El detalle de las entrevistas efectuadas se encuentra en el Anexo Documental. A continuación incorporé un modelo con la estructura de las entrevistas formuladas a las personas antes mencionadas.

Modelo de entrevista

Ocupación: _____

1) **¿Qué importancia tiene para usted la protección de la información guardada en la memoria de su PC?**
   a) ___ Poca o ninguna
   b) ___ Alguna importancia
   c) ___ Mucha importancia

2) **a) ¿Considera seguro y confiable el sistema actual de identificación de usuarios a través de claves de acceso o passwords? Fundamente**
   b) ¿Conoce usted otros sistemas de Identificación de usuarios?

3) **¿En su opinión cuáles son las principales causas de la vulnerabilidad del acceso a la información mediante claves?**

4) **¿Considera que la utilización de dispositivos biométricos puede ser una alternativa que logre solucionar la falta de seguridad del sistema de claves de identificación? Fundamente.**

5) **¿Qué beneficios traería para el usuario el uso de la biometría?**

6) **¿Considera que los usuarios, tanto de ordenadores personales como de los sistemas multiusuarios, aceptarían sin problema el uso de algún dispositivo biométrico para poder acceder a su PC o workstation?**

7) **¿Cuál de los siguientes dispositivos le parece más conveniente para su utilización, y por qué?**
   ___ **Huella dactilar**
   ___ **Reconocimiento del Iris**
   ___ **Reconocimiento de la Retina**
   ___ **Geometría de la mano**
   ___ **Verificación de firmas**
   ___ **Reconocimiento de la voz**

8) ¿Desea usted formular algún comentario en relación a los temas objeto de la entrevista que no le hayan sido consultados?

C.2. Búsquedas realizadas en Internet

Las búsquedas en Internet fueron motivadas por la actualidad del tema objeto de este trabajo y la constante incorporación de novedades en este medio de información. La forma más rápida y segura de obtener datos y experiencias es Internet.

Los principales sitios utilizados para recabar información fueron:

- http://www.kripotopolis.com: **K**riptopolis.
- http://www.nextvision.com: Nextvision Seguridad
- http://www.cybsec.com: CybSec S.A.
- http://www.iec.csic.es/criptonomicon.com: Criptomicon
- http://www.nai.com: Network Associates

C.3. Fuentes secundarias de información como investigaciones científicas, libros y revsitas especializadas

La bibliografía utilizada se detalla como corresponde en una sección especialmente destinada a tal fin.

D. ASPECTOS TEÓRICOS

D. 1. Claves de acceso o de identificación

Para poder acceder a un sistema informático, el sistema operativo procede a identificar y autentificar al usuario, con el fin de comprobar si se trata de un usuario autorizado a acceder a los recursos del mismo.

Este proceso tiene mayor sentido en los ordenadores o sistemas multiusuario, de ahí que no se utilice en la mayoría de los ordenadores personales. Sin embargo, si se quiere proteger la información almacenada en un ordenador personal, aún siendo el único usuario del mismo, es conveniente establecer algún mecanismo de identificación y autentificación.

Como se indicó con anterioridad, el mecanismo más ampliamente usado para identificar y autentificar a los usuarios se basa en el uso de claves de identificación o password. Es fácil de entender y fácil de implementar.

Consiste en asociar una contraseña única en forma de una palabra (con o sin sentido) a cada identificador de usuario:

- En primer lugar se pide el identificador o nombre de usuario:

login: xxx

- Una vez introducido éste, sin realizar ningún tipo de comprobación sobre el mismo, se le pide al usuario que introduzca su contraseña:

password: xxx

Tras introducir la contraseña, el sistema comprueba la validez de la misma. Si la contraseña corresponde con el nombre de usuario, se permite el acceso. Si por el contrario la contraseña no se corresponde, se permite al usuario reintentar su introducción un número limitado de veces. Si después de estos reintentos el usuario no ha conseguido introducir su contraseña correctamente, el sistema bloquea el proceso.

Debido a la importancia de mantener el secreto de las contraseñas, el sistema no las almacena directamente, sino que mantiene una copia cifrada de las mismas.

Existen diversos métodos para la obtención de una contraseña en una máquina. Básicamente se pueden señalar los siguientes:

- Elegida por el usuario sin ninguna comprobación posterior.
- Generada aleatoriamente por el ordenador y escogida por el usuario.

- Asignada por el administrador del sistema.
- Elegida por el usuario y comprobada por el administrador del sistema o por algún software específico para hacerla encuadrar dentro de ciertas restricciones.

D. 1. 1. Elección y gestión de contraseñas

Tal y como se afirmó a lo largo de este trabajo, las contraseñas son la primera y principal línea de defensa contra los intrusos. Para proteger al sistema y a los datos que contiene es necesario elegir contraseñas adecuadas y protegerlas cuidadosamente.

Si se seleccionara una contraseña en forma aleatoria de 8 caracteres alfanuméricos, el número de posibles combinaciones a comprobar para descubrirla será de 2.8 billones. Incluso comprobando un millón de contraseñas por segundo se tardaría una media de 45 años en adivinarla. El problema radica en que no se seleccionan las contraseñas en forma aleatoria por que sería muy difícil de recordar por los usuarios y por lo tanto los mismos tenderían a escribirlas o modificarlas por otras más simples de memorizar.

Lo que realmente sucede es que los usuarios seleccionan como contraseñas:

- Su nombre de usuario o una variación mínima del mismo.
- Su nombre, apellido o alguna fecha significativa.
- Parte de su teléfono, DNI, matrícula del auto, o algún otro dato personal o familiar.
- Palabras comunes y con sentido.
- Nombres de personas conocidas o personajes de ficción.
- Nombres de lugares.

De esta manera, las contraseñas resultan fáciles de recordar, aunque también es muy común que para no olvidarlas las anotan en lugares cercanos a la estación de trabajo o las comenten con algún compañero.

Algunas normas o ideas que sugieren los expertos en el tema de seguridad informática, para la elección de claves son las siguientes:

- Optar por claves de acceso de por lo menos 8 caracteres, ya que es una longitud mínima respetable.
- No utilizar contraseñas que sean palabras comunes o nombres.

- No utilizar claves completamente numéricas con algún significado, por ejemplo números en orden ascendente o descendente, o repetidos.
- Elegir una contraseña que mezcle caracteres numéricos y alfabéticos (alfanuméricos).
- Tener contraseñas diferentes en máquinas diferentes.
- Combinar palabras cortas con algún número o carácter de puntuación, por ejemplo: soy2_yo2.
- Elegir una frase y utilizar las primeras letras de cada palabra, por ejemplo: "lo que el viento se llevó", la clave sería lqevsl.
- Elegir una palabra sin sentido, aunque pronunciable, por ejemplo tachunda71.

Adicionalmente, hay normas de protección que colaboran con la gestión de claves entre las cuales podemos nombrar: que el sistema pidiera a cada usuario el cambio de clave cada 30 días y chequeara que no se utilicen claves viejas o ya usadas; que toda cuenta de usuario fuera bloqueada después de tres intentos de ingreso consecutivos fallidos; que cualquier sesión que aparezca inactiva por más de diez minutos, el sistema exija el reingreso del password para continuar.

En función de lo analizado, se puede resumir el problema de la elección de las contraseñas en el siguiente dilema:

"Cuanto más fácil de recordar es una contraseña, más fácil es de adivinar, mientras que cuanto más difícil es de descubrir, más difícil es de recordar."

La vulnerabilidad de un sistema está dada en gran parte por la fortaleza de sus claves de acceso. La debilidad en la elección de las contraseñas o claves de acceso por parte de los usuarios hace que toda la fortaleza del sistema de seguridad se caiga.

D. 2. Amenazas y ataques al sistema de información

La Seguridad Informática tiene como objetivo el mantener la Confidencialidad, la Integridad y la Disponibilidad de los sistemas de

información los cuales se ven amenazados por un número importante de Riesgos que debemos conocer.

El Riesgo es la probabilidad de que una amenaza se materialice sobre una Vulnerabilidad del Sistema de Información, causando un impacto al afectar negativamente a alguna de las propiedades de la información que la Seguridad Informática trata de mantener.

Debemos distinguir tres términos para comenzar a analizar este tema: acceso, uso y autorización; ya que el uso de alguno de estos conceptos implica un uso desapropiado de los otros. Por ejemplo:

- Cuando un *usuario* tiene *acceso autorizado*, implica que *tiene autorizado el uso* de un recurso.
- Cuando un *atacante* tiene *acceso desautorizado* está haciendo *uso desautorizado* del sistema.
- Pero, cuando un *atacante* hace *uso desautorizado* de un sistema, esto implica que el *acceso fue autorizado* (simulación de usuario).

Luego un ataque será un intento de acceso o uso desautorizado de un recurso, sea este intento satisfactorio o no. Un incidente envuelve un conjunto de ataques que pueden ser distinguidos de otro grupo por las características del mismo (grado, similitud, técnicas utilizadas, tiempos, etc.).

D.2.1. Potenciales atacantes

Los personajes que pueden ser potenciales atacantes del sistema son: el mundo under y el personal perteneciente a la organización.

a) Mundo Under:

Dentro del mundo under podemos definir varios personajes de características diferentes:

Hackers

Es el más conocido de estos personajes y se lo puede definir como una persona que está siempre en una continua búsqueda de conocimientos en todo lo relacionado con sistemas informáticos, sus mecanismos de seguridad, las vulnerabilidades de los mismos, la forma de aprovechar estas vulnerabilidades y los mecanismos para protegerse de aquellos que saben hacerlo.

Vive para aprender y todo para él es un reto; no existen barreras y lucha por la difusión libre de información, distribución de software sin costo y la globalización de la comunicación.

Hay varias teorías acerca del origen de la palabra hacker. Una historia relata que los primeros ordenadores grandes y defectuosos, se bloqueaban continuamente y fallaban. Los que los manejaban se devanaban los sesos creando rutas para aumentar la velocidad y cosas parecidas. Estas cosas se denominaban hacks y a los que las hacían se los llamaba hackers. Otra denominación se le hacía a aquel experto en cualquier campo que disfrutaba modificando el orden de funcionamiento del aparato, de esta forma siempre superaba las limitaciones y esto le producía una alta satisfacción. A estas personas también las llamaban hackers.

El concepto de hacker, generalmente es confundido erróneamente con los mitos que existen acerca de este tema:

- Un hacker es pirata. Esto no es así ya que los piratas comercian con la información que obtienen, entre otras cosas, y un verdadero kacker sólo obtiene esa información para su uso personal.

- Un hacker es el que entra en los sistemas ajenos y se dedica a destruir la información almacenada en ellos. El error consiste en que el que destruye información y sistemas ajenos, no es el hacker sino el cracker.

Crackers

Los crackers son hackers cuyas intenciones van más allá de la investigación. Es una persona que tiene fines maliciosos o de venganza, quiere demostrar sus habilidades pero de manera equivocada o simplemente personas que hacen daño sólo por diversión.

Tiene dos definiciones, según se hable de Seguridad Informática o de crackeo de programas:

- En el caso de seguridad informática, el cracker es aquel que permanentemente intenta violar la seguridad de los sistemas informáticos, con fines justificados o no.

- En el caso de crackeo de programas la definición es la de creador de cracks, (lo que significa literalmente romper), que son programitas destinados

a la desprotección de programas comerciales para que puedan ser usados sin límites.

Phreakers

El phreaking es la actividad por medio de la cual algunas personas con ciertos conocimientos y herramientas de hardware y software, pueden engañar a las compañías telefónicas para que éstas no cobren las llamadas que se hacen.

La realidad indica que los phreakers son crackers de las redes de comunicación. Personas con amplios conocimientos en telefonía (generalmente mayores que el de los propios empleados de las compañías).

Lus gurús

Son considerados los maestros y los encargados de formar a los futuros hackers. Generalmente no están activos pero son identificados y reconocidos por la importancia de sus hackeos, de los cuales sólo enseña las técnicas básicas.

Los lamers o script-kidders

Prueban todos los programas que llegan a sus manos. Generalmente son los responsables de soltar virus o bombas lógicas en la red sólo con el fin de molestar y que otros se enteren que usa tal o cual programa.

El Samurai

Son lo más parecido a una amenaza pura. Sabe lo que busca, donde encontrarlo y cómo lograrlo. Hace su trabajo por encargo y a cambio de dinero. Estos personajes, a diferencia de los anteriores, no tienen conciencia de comunidad y no forman parte de los clanes reconocidos de hackers. Se basan en el principio de que cualquiera puede ser atacado y saboteado, sólo basta que alguien lo desee y tenga dinero para pagarlo.

Piratas informáticos

Este personaje (generalmente confundido con el hacker) es el realmente peligroso desde el punto de vista del copyright, ya que copia soportes

audiovisuales (discos compactos, DVD, cassettes, etc.) y los vende ilegalmente.

b) Personal (Insiders).

Julio César Ardita (director de Cybsec S.A. Security Sistem) plantea que "de los robos, sabotajes o accidentes relacionados con los sistemas informáticos, el 70% son causados por el propio personal de la organización propietaria de dichos sistemas. Siendo de ese porcentaje:

- 15% efectuados por deshonestidad,
- 15% efectuados por descuidos
- 70% efectuados por errores."

Esto es realmente preocupante, ya que, una persona que trabaje con el administrador, el programador o el encargado de una máquina conoce perfectamente el sistema, sus puntos débiles y fuertes; de manera que un ataque realizado por esa persona podrá ser más directo, difícil de detectar y más efectivo que el de un atacante externo.

D.2.2. Tipos de ataques

En los primeros tiempos, los ataques involucraban poca sofisticación técnica. Los Insiders (operadores, programadores, data entrys) utilizaban sus permisos para alterar archivos o registros. Los Outsiders ingresaban a la red simplemente averiguando una password válida. A través de los años se han desarrollado formas cada vez más sofisticadas de ataque, siendo la mayoría de ellos perpetrados por hackers y otros personajes similares.

Solamente se expondrán los ataques cuya finalidad es la obtención de claves de acceso o passwords.

D.2.2.1. Ingeniería Social

Es la manipulación de las personas para convencerlas de que ejecuten acciones o actos que normalmente no realizan con la finalidad de que revele todo lo necesario para superar las barreras de seguridad. Si el atacante tiene la experiencia suficiente, puede engañar fácilmente a un usuario (que desconoce muchas veces las mínimas medidas de seguridad) en beneficio propio. Esta

técnica es una de las más usadas y efectivas a la hora de averiguar nombres de usuarios y passwords.

Por ejemplo, suele llamarse a un usuario haciéndose pasar por el administrador del sistema y requerirle la password con alguna excusa convincente. O bien, podría enviarse un mail (falsificando la dirección origen a nombre del administrador) pidiendo al usuario que modifique su password a una palabra que el atacante suministra.

D.2.2.2. Ingeniería social inversa (ISI)

Consiste en la generación por parte de los intrusos, de una situación inversa a la originada en Ingeniería Social.

En este caso el intruso publicita de alguna manera que es capaz de brindar ayuda a los usuarios, y estos lo llaman ante un imprevisto. El intruso aprovechará esta oportunidad para pedir información necesaria para solucionar el problema del usuario y el suyo propio (la forma de acceso al sistema).

La ISI es más difícil de llevar a cabo y por lo general se aplica cuando los usuarios están alertados acerca de las técnicas de Ingeniería Social. Puede usarse en algunas situaciones específicas y después de mucha preparación e investigación por parte del intruso:

1) Generación de una falla en el funcionamiento normal del sistema. Generalmente esta falla es fácil de solucionar pero puede ser difícil de encontrar por los usuarios inexpertos. Requiere que el intruso tenga un mínimo contacto con el sistema.
2) Comunicación a los usuarios de que la solución es brindada por el intruso. (publicidad)
3) Provisión de ayuda por parte del intruso encubierto como servicio técnico.

D.2.2.3. Trashing (Cartoneo)

Generalmente un usuario anota su login y password en un papelito, cuando lo recuerda, lo arroja a la basura. Este procedimiento por más inocente que parezca es el que puede aprovechar un atacante para hacerse de una llave para entrar al sistema.

El trashing puede ser físico (como el caso descripto) o lógico, como analizar buffers de impresoras y memoria.

El trashing físico suele ser común en organizaciones que no disponen de alta confidencialidad, como colegios y universidades.

D.2.2.4. Shoulder surfing

Consiste en espiar físicamente a los usuarios para obtener el login y su password correspondiente. El surfing explota el error de los usuarios de dejar su login y password anotadas cerca de la computadora. Cualquier intruso puede pasar por allí, buscar y memorizarlos para su posterior uso.

Otra técnica relacionada con el surfing es aquella mediante la cual se ve, por encima del hombro, al usuario cuando teclea su nombre y password.

D.2.2.5 Señuelos (Decoy)

Los Decoy son programas diseñados en la misma interface que otro original. En ellos se imita la solicitud de un logeo y el usuario desprevenido lo hace. Luego, el programa guardará esta información y dejará paso a las actividades normales del sistema. La información recopilada será utilizada por el atacante para futuras "visitas".

D.2.2.6. Cracker de passwords u obtención de claves de acceso

Cuando un intruso entra en un sistema, lo considera propiedad de él, y tratará de mantenerse en el sistema la mayor cantidad de tiempo posible. Para realizar esto, el intruso se vale de varias herramientas, una de las más usadas y principales es el cracker de passwords, que traducido al castellano sería "reventador de claves de acceso".

Una vez que el intruso ha logrado conseguir el archivo de claves, pone a funcionar el cracker con ese archivo. Este cracker, es un programa que se dedica a comparar las claves encriptadas contra un diccionario.

Debido a la debilidad en las contraseñas elegidas por muchos usuarios es que existe este método de cracker, actualmente muy extendido, para atacarlas. También es llamado "ataque mediante diccionario" debido a la forma en que el mismo opera.

Los diccionarios son archivos con millones de palabras, las cuales pueden ser posibles passwords de los usuarios. Con este programa se consigue una copia del fichero en que se almacenan las passwords cifradas. Luego, este programa es el encargado de probar cada una de las palabras encriptando cada una de ellas, mediante el algoritmo utilizado por el sistema atacado, y compara la palabra encriptada contra el archivo de passwords del sistema atacado (previamente obtenido). Si alguna de ellas coincide, el atacante acaba de descubrir una de las claves de acceso al sistema.

En la siguiente tabla podemos observar el tiempo de búsqueda de una clave de acuerdo a su longitud y tipo de caracteres utilizados. La velocidad de búsqueda se supone en 100.000 passwords por segundo, aunque este número suele ser mucho mayor dependiendo del programa utilizado.

Cantidad De caracteres	Letras minúsculas	Letras y dígitos	Mayúsculas y minúsculas	Todos los caracteres
6	51 minutos	6 horas	2,3 días	3 meses
7	22,3 hora	9 días	4 meses	24 años
8	24 días	10,5 meses	17 años	2288 años
9	21 meses	32,6 años	896 años	219601 años
10	45 años	1160 años	45840 años	21081705 años

Tabla que indica cantidad de claves generadas según el número de caracteres empleado. Fuente: http://www.cfbsoft.com.ar

Aquí puede observarse la importancia de la utilización de passwords con al menos 8 caracteres de longitud y combinando todos los tipos de caracteres disponibles.

La importancia y efectividad de este tipo de ataque puede constatarse citando parte del artículo "Foiling the Cracker: A survoy of, and Improvement to, Password Security" de Daniel V. Klein.

En este artículo el autor muestra los resultados obtenidos al aplicar el ataque mediante diccionario sobre un total de 13.794 cuentas. Para ello utilizó un diccionario con un total de 62.727 palabras, además de distintas combinaciones, permutaciones y variaciones del resto de los campos contenidos en el fichero */etc/passwords*. Usando este tipo de ataque durante un

año el autor llegó a descubrir 3.340 de las contraseñas, es decir, un 24.2 % del total. Más aún, en los primeros 15 minutos descubrió 368 y en la primer semana 3.000. En máquinas con 50 cuentas o más el ataque consiguió descubrir el primer password en una media de 2 minutos, y entre 5 y 15 passwords el primer día.

La siguiente tabla muestra cuales fueron los tipos de contraseñas descubiertos, y que porcentaje representaron del total:

Passwords descubiertas sobre un total de 13797 cuentas						
Tipo de contraseña	Tamaño del diccion.	Duplicados eliminados	Tamaño de búsqueda	Número de coinciden.	% sobre el total	Coste/ Beneficio*
Nombre de usuario	130 #	-	130	368	2,7%	2831
Secuencia de caracteres	866	0	866	22	0,2%	0.025
Números	450	23	427	9	0,1%	0,021
Chino	398	6	392	56	0,4%	0,143
Lugares	665	37	628	82	0.6%	0,131
Nombres comunes	2268	29	2239	548	4,0%	0,245
Nombres de mujeres	4955	675	4280	161	1,2%	0,038
Nombres de hombres	3901	1035	2866	140	1,0%	0,049
Nombres no comunes	5559	604	4955	130	0,9%	0,026
Mitos y leyendas	1357	111	1246	66	0,5%	0,053
Shakespeare	650	177	473	11	0,1%	0,023
Términos deportivos	247	9	238	32	0,02%	0,134
Ciencia ficción	772	81	691	59	0,4%	0,085
Películas y actores	118	19	99	12	0,1%	0,0121
Dibujos animados	133	41	92	9	0,01%	0,098
Gente famosa	509	219	290	55	0,4%	0,190
Frases	998	65	933	253	1,8%	0,271
Alias	160	127	33	9	0,1%	0,273
Biología	59	1	58	1	0,0%	0,017
/usr/dict/words	24474	4791	19683	1027	7,4%	0,052
Nombres de	12983	3965	9018	132	1%	0,015

máquinas						
Memotécnicos	14	0	14	2	0,0%	0,143
Biblia	13062	5537	7525	83	0,6%	0,011
Palabras varias	8146	4934	3212	54	0,4%	0,017
Palabras yiddish	69	13	56	0	0,0%	0,00
Asteroides	3459	1052	2407	19	0,1%	0,008
Total	86280	23553	62727	3340	24,2%	0,053

Por cada nombre de usuario (login) se han probado 130 permutaciones y variaciones.

* Número de coincidencias dividido por el tamaño de búsqueda. Cuantas más palabras es necesario testear para conseguir una coincidencia, menor es el ratio costo/beneficio.

Los resultados de este artículo muestran claramente la enorme debilidad del sistema de contraseñas sin ninguna medida adicional de selección y administración de contraseñas.

Si nos diéramos cuenta que un intruso ha logrado entrar al sistema, tendríamos que cambiar todas las claves de acceso para que el intruso no pueda ingresar más a nuestro sistema; lo que nos tomaría mucha pérdida de tiempo, el sistema se debería mantener abajo por unas horas, mientras se cambian las claves de acceso, y esto acarrearía numerosos problemas de índole personal con los usuarios del sistema, ya que deberían volver a cambiar sus claves de acceso.

Cuando un intruso ha ingresado al sistema, y posee el archivo de claves de acceso, la única forma de asegurarnos que no volverá a entrar, es cambiando todas las contraseñas de acceso al sistema, ya que si dejamos alguna sin cambiar, esa puede ser la futura puerta de acceso del intruso.

D. 3. Biometría

Identificación, vigilancia, control no son conceptos del mundo moderno, sino que caminan de la mano de la historia del hombre. Ya en el antiguo Egipto se llevaban registros de población que facilitaban el control fiscal o militar y son bien conocidos también los censos Israelitas, que datan del siglo XV A.C. y que permitían, entre otras cosas, la identificación de los componentes de las tribus nómades para su posterior reagrupamiento. Desde entonces hasta hoy la identificación personal se ha basado tradicionalmente en la posesión de llaves,

tarjetas, claves de palabras o números. Sin embargo, el ser humano posee características que lo hacen único: las huellas dactilares, la voz, el iris, el rostro, el ADN.

Si hace un tiempo atrás se le hubiera propuesto a una empresa o a un individuo implementar un sistema digital de reconocimiento biométrico, hubiéramos obtenido una pregunta como respuesta: ¿qué es biométrico?

El concepto biometría proviene de las palabras:

BIO: vida

METRÍA: medida

Por lo tanto con ello se infiere que todo equipo biométrico mide e identifica alguna característica propia de la persona. La Biometría es una tecnología que permite la identificación de personas a partir de rasgos o características físicas particulares.

Todos los seres humanos tenemos características morfológicas únicas que nos diferencian. La forma de la cara, la geometría de partes de nuestro cuerpo como las manos, nuestros ojos, la huella digital son algunos de los rasgos que nos distinguen del resto de las personas.

Actualmente el 99% de todos los sistemas de acceso instalados trabajan por "suposición". Simplemente asumen que si la persona posee la llave, tarjeta o sabe la contraseña, es el usuario legítimo. El mercado de controles de acceso se abrió con la proliferación de los sistemas, pero ninguno de ellos se ha revelado eficaz contra el fraude, ya que todos utilizan un medio externo como pueden ser las tarjetas de identificación, llaves, claves...

Es frecuente olvidar una clave de acceso. Para evitar olvidos, se suele anotar esta clave en agendas o cuadernos, perdiendo así toda confidencialidad. Es frecuente también perder una tarjeta de identificación o una llave.

Existen varios métodos para verificar la identidad de un individuo, sin embargo, la biometría se considera como el método más apropiado, ya que ciertos rasgos de una persona son inherentes a ella y sólo a ella. La biometría permite una autentificación segura, al contrario que el empleo de contraseñas o tarjetas, ya que estos últimos pueden ser robados o utilizados por personas no autorizadas.

Las necesidades de autentificación y seguridad, unidas a las ya mencionadas anteriormente en materia de seguridad de accesos físicos, han determinado un interés creciente por los sistemas electrónicos de identificación y autentificación. Su denominador común es la necesidad de que sean medios simples, prácticos y fiables, para verificar la identidad de una persona.

Este sistema evita:

- la duplicación
- el robo
- el olvido
- la pérdida

	COPIA	ROBO	OLVIDO	PÉRDIDA
LLAVE	X	X	X	X
TARJETA	-	X	X	X
CLAVE	X	-	X	-
HUELLA	-	-	-	-

Para que una característica biométrica sea efectiva en el reconocimiento de personas, debería cumplir con las siguientes propiedades:

Universalidad: Todos los miembros de la base de usuarios deben poseer esta característica biométrica. Por supuesto que no se puede controlar el acceso mediante la voz, si entre los usuarios existen personas mudas.

Singularidad: La característica biométrica debe ser diferente para cada una de las personas que forman la base de usuarios, de forma que no existan dos individuos con las mismas características.

Invarianza: La característica biométrica debe ser invariante a las condiciones en las que se capturó. Por ejemplo, en el reconocimiento de caras debe ser invariante a los diferentes peinados, etc.

Resistencia: La característica biométrica debería ser resistente a contramedidas fraudulentas, como grabaciones magnetofónicas de la voz, resistente a lentes de contacto en el caso de reconocimiento del iris, etc.

D.3.1. Identificación y verificación

Existen dos grandes grupos de aplicaciones dentro del reconocimiento de personas:

Identificación

Consiste en determinar la identidad de la persona que accede al sistema de reconocimiento. Para ello, a partir de la característica biométrica de entrada que se desea utilizar, se realizará un test consistente en comparar los datos de entrada con el modelo de todas las personas que integran la base de datos. A partir de la comparación entre los datos de entrada y los datos almacenados en memoria durante el proceso de captación de los datos, se decidirá la identidad de la persona que accede al sistema.

Verificación

En este caso el individuo de entrada suministra su identidad, y el sistema deberá comprobar los datos de entrada con los almacenados en memoria de esa misma persona, para comprobar si es quien dice ser.

Dado que en los sistemas que requieren el reconocimiento de personas, normalmente el conjunto de posibles usuarios es muy elevado, los sistemas que se utilizan suelen ser del tipo verificación, usándose el mecanismo de identificación para sistemas de pocos usuarios.

D.3.2. Descripción del funcionamiento de los sistemas biométricos

Los sistemas biométricos se componen de un hardware y un software; el primero captura la característica concreta del individuo y el segundo interpreta la información y determina su aceptabilidad o rechazo, todo en función de los datos que han sido almacenados por medio de un registro inicial de la característica biométrica que mida el dispositivo en cuestión.

El mecanismo biométrico consta de tres partes: un mecanismo de captura, un mecanismo de procesamiento y un medio de almacenamiento.

El primer paso en el sistema biométrico es llamado enrolamiento, en el que la característica biométrica (llamada "ejemplo" a los fines de la descripción del proceso) es capturada por el mecanismo de captura. Este "ejemplo" es luego pasado a un mecanismo de procesamiento como una computadora, que extrae características únicas del ejemplo para crear una plantilla: una

representación matemática del ejemplo que toma mucho menos espacio que el ejemplo original. Esta plantilla es luego almacenada en el disco duro de la computadora.

Cuando un usuario previamente enrolado decide tener acceso a través del sistema, deberá presentar su biometría al mecanismo de captura una vez más. El sistema de procesamiento hará luego, una de estas dos acciones dependiendo de la aplicación:

- Si el sistema de procesamiento estuviera comparando el ejemplo biométrico actual con una sola plantilla almacenada, el sistema estaría efectuando una verificación uno a uno.
- Si en cambio, el sistema estuviera comparando el ejemplo biométrico con una base de datos de muchas plantillas almacenadas previamente, muchas de las cuales no son del propio usuario, el sistema estaría ejecutando la identificación buscando a través de cada plantilla, verificando si alguna coincide. Este método es conocido como la búsqueda uno a varios.

Si en cualquiera de estas dos situaciones planteadas la comparación coincide, se garantiza el acceso; caso contrario el sistema lo niega.

Es importante destacar que la identificación biométrica se basa en un principio de umbral. Esto significa que es casi imposible capturar la biometría de la misma forma cada vez que se usa para el acceso; por lo tanto el sistema no puede esperar un 100% de coincidencia.

D.3.2.1. Precisión del sistema

En las aplicaciones de verificación el resultado es una decisión binaria "si" o "no" que permite o deniega el acceso al sistema. El funcionamiento puede resumirse en los siguientes pasos:

- El usuario suministra su identidad (mediante un login), así como la característica biométrica que desea medirse.
- El sistema realiza a parametrización de la característica biométrica de entrada.

- Se compara la información parametrizada con el modelo correspondiente a la persona cuya identidad se ha suministrado. Este modelo se ha obtenido en el proceso de enrolamiento.
- El resultado de la comparación es una medida de distancia entre ambas informaciones, y se compara con un umbral prefijado para dicho usuario. Si la distancia es menor al umbral, se acepta al usuario. Si es mayor, se deniega el acceso.

El sistema de verificación puede valorarse en función de las tasas de falsa aceptación y falso rechazo:

Tasa de falsa Aceptación (TFA): Representa el porcentaje de personas no autorizadas, erróneamente aceptadas por el sistema.

Tasa de falso Rechazo (TFR): Representa el porcentaje de personas autorizadas, a las cuales se les deniega el acceso erróneamente.

Se trata de características contrapuestas, puesto que mejorar (reducir) la tasa de falsa aceptación supone hacer que el sistema sea más restrictivo y, por lo tanto, se empeora (aumenta) la tasa de falso rechazo, y viceversa.

Uno de los aspectos clave es la determinación del umbral de distancia, puesto que condiciona los valores de dichas tasas. En algunas aplicaciones interesa que una de las dos tasas sea baja a costa de elevar la otra. Generalmente, se ajustan los umbrales para conseguir que ambas tasas sean idénticas. Cuando la Tasa de falsa aceptación es igual a la tasa de falso rechazo, se habla de Equal Error Rate (EER) o tasa de errores idénticos.

La elección del umbral se realiza a partir de un procedimiento de prueba y error. Un posible ejemplo es el siguiente:

- Para cada uno de los usuarios se prueban varios umbrales posibles, entre el valor mínimo de distancia y el máximo.

- Para cada uno de los umbrales de test se calculan las correspondientes tasas TFA yTFR.

- Se escoge como umbral aquel que consigue TFA = TFR.

D.3.3. Tipos de dispositivos biométricos

El reconocimiento biométrico de personas consiste en medir, almacenar y comparar características personales únicas. En cuanto a que partes del

cuerpo son las más adecuadas para su utilización biométrica, aunque en principio cualquiera sería susceptible de ser usada, para su elección se atiende a criterios prácticos concretos. Lo ideal es que se trate de una característica física robusta, es decir, no sujeta a grandes cambios; que sea lo más distintiva posible en relación con el resto de la población, que sea una zona accesible y disponible y, por supuesto aceptable por el usuario que en ocasiones, puede llegar a percibir algunos dispositivos biométricos como intrusivos.

Las características personales se pueden dividir en dos grandes grupos:

De comportamiento: Se basan en hábitos que la persona ha aprendido a lo largo del tiempo, como su forma de firmar, la manera de teclear un ordenador, etc.

Características fisiológicas: Se basan en medidas de características únicas de cada persona, tales como las huellas dactilares, forma y tamaño de la mano, el iris, etc.

De esta división de las características personales, surgen los distintos dispositivos biométricos: los que miden el comportamiento y los que miden una característica fisiológica. Entre los primeros se encuentran el análisis de la dinámica de la firma; los segundos incluyen la huella dactilar, la geometría de la mano y la exploración del iris o la retina. El reconocimiento de la voz, es un parámetro biométrico basado en ambos análisis, por un lado el fisiológico que determina la zona vocal; y por otro el de comportamiento del lenguaje y las palabras usadas. Evidentemente, aquellos dispositivos que se basan en el comportamiento requieren de la cooperación del usuario, mientras que se puede identificar fisiológicamente a cualquiera sin su cooperación e incluso sin su conocimiento, como en el caso de la imagen captada por una videocámara.

D.3.3.1.Huella dactilar

Está basado en el principio de que no existen dos huellas dactilares iguales. Se ha estimado bajo un análisis exhaustivo, que la posibilidad de que dos personas tengan las mismas huellas dactilares (incluyendo los gemelos), es menor a uno entre un billón. Cada huella digital posee pequeños arcos, ángulos, bucles, remolinos, etc. (llamados minucias); características que junto a la posición relativa de cada una de ellas es lo analizado para establecer la identificación de una persona. Está aceptado que dos personas no tienen más

de ocho minucias iguales, y cada persona posee más de 30 minucias, lo que hace al método sumamente confiable.

Su funcionamiento se basa en tomar una imagen de la huella y por medio de algoritmos reducir dicha imagen a una representación matemática de la huella, llamada comúnmente "template".

Este template patrón (también llamado original) se acumula en la memoria interna del equipo, junto con un número de identificación o PIN (Personal Identification Number, la cual es única e irrepetible) a fin de tener asociada la huella del individuo.

Luego, cada vez que la persona necesite identificarse, debe digitar su Pin y a continuación colocar su dedo en el lector. El equipo captura la nueva imagen de la huella y a continuación la compara con el template original que figura en su memoria. Si coincide, permite el acceso. En caso de no coincidir, muestra un mensaje rechazando la identidad.

D.3.3.2. Reconocimiento de Retina o de Iris

El reconocimiento de la retina se basa en examinar los patrones de los vasos sanguíneos en la parte posterior del ojo. Consiste en dirigir un haz infrarrojo de baja intensidad a través de la pupila, hacia la parte posterior del ojo; de manera que la delicada retina es barrida por una luz y acoplador óptico. Pero requiere que la persona mire dentro de un receptáculo y enfoque su mirada hacia un punto. Esto es un inconveniente si la persona usa anteojos o lentes de contacto, y además es un sistema poco aceptado por el usuario, dada la desconfianza que suscita la exploración del ojo a poca distancia.

La barrida de Iris, a diferencia de la retina, analiza la superficie del ojo, lo cual permite tomar la imagen del ojo a mayor distancia que el método anterior (a unos 30 cm del ojo). El iris es un componente de la anatomía realmente estable e inalterable que permite identificar a un individuo de una forma tan precisa como la huella dactilar, y además no puede ser falsificado con ningún tipo de lente.

El procedimiento de este sistema tiene dos fases. En la primera se efectúa el escaneo del iris del ojo del usuario, y esa información, luego de ser codificada (template) se almacena en un archivo en la memoria del equipo. En la segunda fase, el usuario debe mirar una cámara que vuelve a capturar la

imagen de su iris: el sistema fotografía el ojo y transforma la imagen en dígitos. Una vez convertida en un código, esa información es contrastada con los datos almacenados en el archivo, confirmando o no la identidad del usuario, y permitiendo o denegando el acceso. Una identificación positiva puede lograrse en menos de 3 (tres) segundos, con búsqueda en una base de datos con más de 4000 (cuatro mil) registros.

El barrido de iris es biológicamente aséptico y físicamente no invasivo, ya que no realiza los reconocimientos mediante radiaciones láser ni infrarrojas ni ninguna otra tecnología que pudiera afectar la visión. Sólo usa una cámara convencional y no requiere contacto físico entre el equipo y la persona a identificar; no hay problema en los registros de personas que utilicen anteojos o lentes de contacto.

D.3.3.3. Geometría de la mano

Los equipos biométricos por geometría de la mano, se basan en capturar información de las medidas de la mano del individuo mediante el uso de un escáner tridimensional, para luego contrastarla con los intentos posteriores a fin de verificar si se trata de la misma persona.

Como en todos los sistemas biométricos, el individuo debe enrolarse previamente en el equipo a fin de obtener el patrón original, se mide la longitud, grosor y altura de la mano y de los dedos. De esta manera se obtiene información a la cual el sistema le aplica un algoritmo de proceso que origina un "template", el cual se almacena en la memoria del equipo asociado a un pin único para cada template y normalmente a elección del usuario. Cuando el individuo se presenta ante la terminal, digita su pin en el teclado para identificarse y a continuación el equipo lo invita a colocar la mano en el lector, toma un nuevo registro de la misma, le aplica el algoritmo de proceso y el resultado se chequea con el template que tiene guardado en memoria asociado al pin que ingresó. El resultado de esta comparación determina la identificación positiva o negativa de la persona.

Entre los posibles problemas que se plantean con este dispositivo cabe destacar, la posibilidad de errores en el reconocimiento ante casos de pérdidas o aumentos considerable de peso, así como la de transmitir gérmenes a través del sensor, dado que existe contacto físico.

D.3.3.4. Verificación de firmas

En este caso lo que se considera es lo que el usuario es capaz de hacer. Es posiblemente el método más aceptado socialmente. Si se utilizan las características dinámicas de la forma de escribir, es posible conseguir altos grados de precisión, ya que es posible medir variables adicionales al mero resultado final, como por ejemplo la velocidad, presión y dirección de los trazados. Para ello es necesario disponer de una tarjeta digitalizadora y un lápiz especial.

Entre los inconvenientes que puede plantear este dispositivo, cabe destacar la existencia de una gran variabilidad en la manera de firmar de las personas, y los expertos en imitar firmas. La clave para conseguir buenos resultados está en diferenciar aquellas partes de la firma que son habituales de las que varían cada vez que se firma.

D.3.3.5. Verificación por voz

La dicción de una frase es grabada y en el acceso se compara la voz (entonación, diptongos, agudeza, etc.)

Este sistema es muy sensible a los factores externos como el ruido, el estado de ánimo y enfermedades de la persona, el envejecimiento, etc. Por lo tanto no tiene mucha aplicación en la actualidad.

E. ANALISIS DE DATOS Y EXPOSICIÓN DE RESULTADOS

E.1. Datos y estadísticas

- Fuente http://www.ey.com

Según los datos obtenidos en Marzo de 2001 por la consultora Ernst & Young sobre 273 empresas de distintos sectores de actividad y países:

- El 40% de las empresas estudiadas consideran como un problema grave la seguridad informática.
- El "gasto" en seguridad informática oscila entre el 4% y el 10% del gasto total informático-
- El 83% de las empresas reconoce no haber emprendido nunca acciones legales después de un ataque.
- El 72% se muestra reacia a admitir que sus sistemas han sido saboteados.
- El 79% cree que existen mayores probabilidades de sufrir un ataque informático procedente del exterior, lo cual es un error.
- El 66% consideran a la Seguridad y Privacidad de la información el impedimento principal para el crecimiento del e-comerse (comercio electrónico).
- El 80% manifestó no haber experimentado un ataque por intrusión durante el año anterior; pero sólo el 33% indicó su capacidad para la detección de dichos ataques.
- Sólo el 39% hace uso de software estándar de seguridad y el 20% de ese total hace uso avanzado de estas herramientas.

- Fuente Monografía: Seguridad en un sistema de información, elaborada por Jose Alfredo Jimenez.

Entre los hechos criminales más famosos de los Estados Unidos están:

- El caso del Banco Wells Fargo donde se evidenció que la protección de archivos era inadecuada, cuyo error costo USD 21.3 millones.
- El caso de la NASA donde dos alemanes ingresaron en archivos confidenciales.
- El caso de un muchacho de 15 años que entrando en al computadora de la Universidad de Berkeley en California destruyó gran cantidad de archivos.

- También se puede mencionar el caso de un estudiante de una escuela que ingresó a una red canadiense con un procedimiento de admirable sencillez, otorgándose una identificación como un usuario de alta prioridad, y tomó el control de una embotelladora en Canadá.

Estos hechos, entre otros muestran claramente que los componentes del sistema de información no presentaban un adecuado nivel de seguridad. Ya que se logró penetrar en el sistema de información.

- Fuente Claxion Digital S.L.

En el año 2000, el costo mundial de los incidentes de seguridad fue de 16.000 millones de euros, mientras que el gasto en tecnologías y servicios de seguridad no llegó a los 9.300 millones de euros.

Esta enorme diferencia es la que ha permitido que se den casos tan sonados como el de Citibank, en que le hacker ruso Vladimir Levin penetró en sus sistemas para robarles 10 millones de dólares: o los virus y deformaciones sufridos por Microsoft debido a que ni siquiera tenía en funcionamiento el software de protección fabricado por la misma empresa. Otro caso conocido es el ataque de negación de servicios que dejó a Yahoo y Amazon, entre otros portales líderes, fuera de servicio durante todo un día.

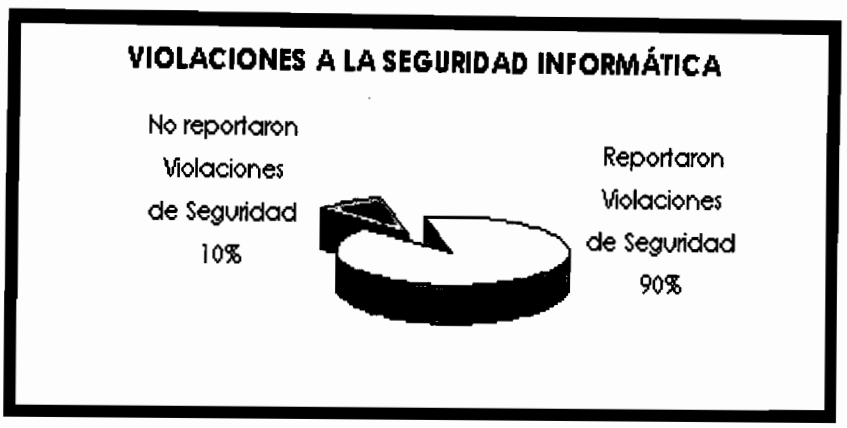
Estos ataques, aunque son de los más impactantes y conocidos, no son casos aislados. Desde hace cinco años existe, en los Estados Unidos, una institución que realiza un estudio anual sobre la Seguridad Informática y los crímenes cometidos a través de las computadoras. Esta entidad es el CSI (Computer Security Institute) y el quinto estudio anual (año 2000) denominado "Estudio de Seguridad y delitos informáticos" fue realizado a un total de 273 instituciones, principalmente grandes corporaciones y agencias del gobierno. Los resultados de dicho estudio arrojan los siguientes datos:

1)Violaciones a la seguridad Informática

Respuestas	**PORCENTAJE (%)**
No reportaron Violaciones de Seguridad	10%
Reportaron Violaciones de Seguridad	90%

El 90% de los encuestados descubrió violaciones a la seguridad de las computadoras dentro de los últimos 12 meses.

El 70% reportaron una variedad de serias violaciones de seguridad en las computadoras, y que las más comunes de estas violaciones son los virus de computadoras, robo de computadoras portátiles o abuso por parte de los empleados – por ejemplo, robo de información, fraude financiero, penetración del sistema por intrusos y sabotaje de datos o redes.

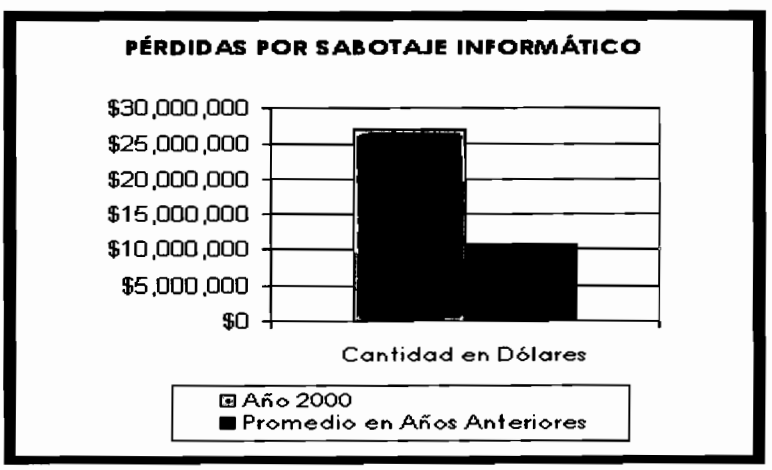


2) Perdidas financieras

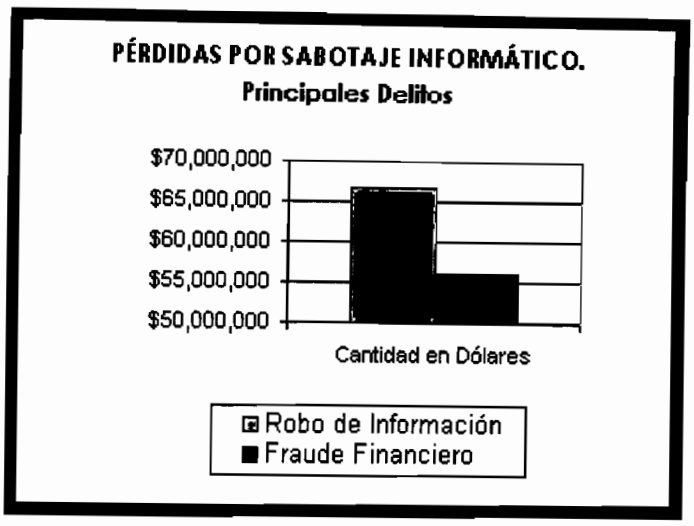
El 74% reconocieron pérdidas financieras debido a las violaciones de las computadoras.

Estas pérdidas en el año 2000 ascendieron a UDS 265.589.940, mientras que el promedio de los últimos tres años era de UDS 120.240.180.

Sesenta y un (61) encuestados cuantificaron pérdidas debido al sabotaje de datos o redes para un total de UDS 27.148.000. Las pérdidas financieras totales debido al sabotaje durante los años anteriores combinados ascendieron a sólo 10.848.850.

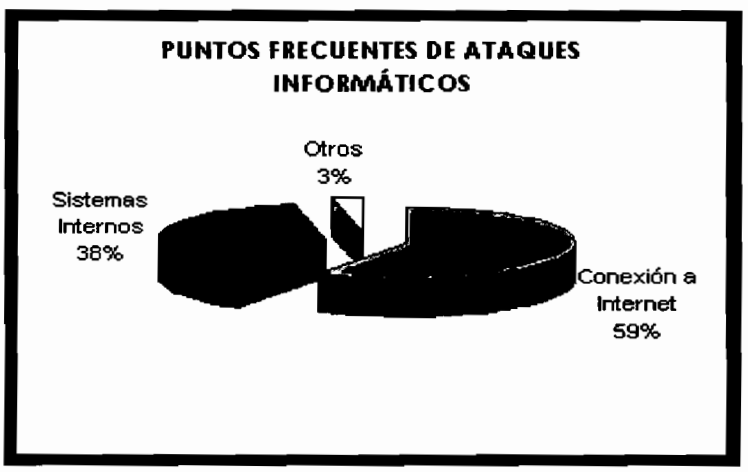


Como en los años anteriores, las pérdidas financieras más serias, ocurrieron a través de robo de información: 66 encuestados reportaron UDS 66.708.000, y el fraude financiero: 53 encuestados informaron UDS 55.996.000.



3) Accesos no autorizados

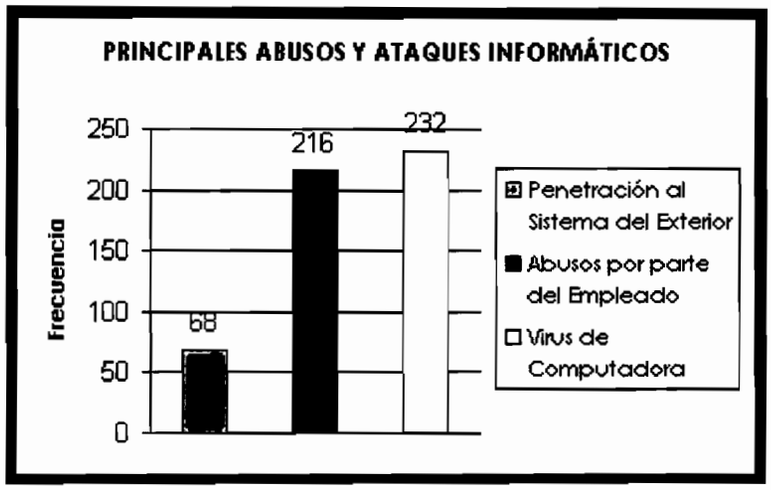
El 71% de los encuestados descubrieron acceso desautorizado por personas dentro de la empresa. Pero por tercer año consecutivo, la mayoría de encuestados (59%) mencionó su conexión de internet como un punto frecuente de ataque, los que citaron sus sistemas interiores como un punto frecuente de ataque fue un 38%.



Basado en contestaciones de 643 practicantes de seguridad en corporaciones americanas, agencias gubernamentales, instituciones financieras, instituciones médicas y universidades, los hallazgos del "Estudio de seguridad y delitos informáticos 2000" confirman que la amenaza del crimen por computadoras y otras violaciones de seguridad de información continúan constantes y que el fraude financiero está en ascenso.

Los encuestados detectaron una amplia gama de ataques y abusos. Aquí están algunos otros ejemplos:

- 25% de encuestados descubrieron penetración al sistema desde el exterior.
- 79% descubrieron el abuso del empleado por acceso de Internet (por ejemplo: transmitiendo pornografía o pirateo de software, o uso inapropiado de sistemas de correo electrónico.
- 85% descubrieron virus de computadoras



Las tendencias que el estudio de CSI ha resaltado por años son alarmantes. Los "cyber crímenes" y otros delitos de seguridad de información se han extendido y diversificado.Nueve de cada diez empresas afirmaron haber sufrido violaciones de seguridad y el 70% fueron víctimas de ataques de virus, o "abuso del sistema" por parte de empleados. Entre estos ataques tan comunes se hallan el robo de información confidencial, fraude financiero, penetración de terceros en el sistema, ataques de negación de servicio y sabotaje de datos o redes.

Además un 74% de los encuestados aseguraron haber sufrido pérdidas financieras debido a tener seguridad insuficiente, sobretodo en lo referente a robo de información confidencial y fraude financiero.

Es importante destacar que, aunque normalmente cuando se habla de "ciber delincuencia" se hace referencia a ataques desde el exterior, lo cierto es que la mayor parte de los ataques provienen del interior de la empresa (un 60% de los casos), normalmente causados por empleados descontentos.

El director del CSI, Patrice Rapalus, ha asegurado que el "90% de los encuestados han sufrido ataques, que pueden resultar en un serio peligro. Resulta evidente que las empresas tiene que tomar medidas del estilo implantar sofisticados programas y tecnologías, desarrollar y hacer cumplir una serie de prácticas y normas de seguridad y, muy importante, la formación de los empleados"

Aunque en nuestro país cada vez son más las empresas e instituciones que están implantando sofisticadas medidas de seguridad para la protección de sus sistemas, redes y bases de datos, lo cierto es que aún hay un gran número de organizaciones que parecen ignorar los riesgos que la falta de seguridad puede provocar. La seguridad no se refiere sólo a evitar la infección de nuevos virus, sino que es un tema que se está haciendo cada vez más complejo debido a la creciente cantidad de información que circula a través de nuestras redes y ordenadores y que se almacena en ellos.

El problema es que muchas organizaciones todavía creen que un ataque es algo que "a mí no me va a pasar" cuando lo más probable es que ya hayan sufrido ataques y ni siquiera lo hayan notado.

E. 2. Análisis de los resultados obtenidos de las entrevistas efectuadas

De las entrevistas efectuadas a las personas seleccionadas se pueden desprender los siguientes análisis:

E.2.1. Importancia de la protección de la información guardada en la memoria de la PC.

Un 100% de los entrevistados manifestó que es de mucha importancia la protección de la información guardada en la memoria de sus PC.

E.2.2. Seguridad y confiabilidad del sistema actual de identificación de usuarios a través de claves de acceso o passwords

De los ocho entrevistados, seis coincidieron en que la seguridad y confiabilidad del sistema de identificación de usuarios a través de claves de acceso o passwords es baja o media.

Ellos fundamentan sus respuestas básicamente en que las claves de acceso son fáciles de descubrir, debido a la obviedad en la elección de las mismas o en la existencia de programas que permiten fácilmente crackear estas claves.

Dos de los entrevistados, no coincidieron en esta opinión sino que manifestaron que el sistema de identificación de usuarios mediante claves sí es seguro. La vulnerabilidad de este sistema radica en las claves utilizadas, por lo tanto el sistema no es seguro o inseguro en sí mismo, sino que debe analizarse el mecanismo y la política de claves y de cambio de claves.

E.2.3. Principales causas de vulnerabilidad del acceso a la información mediante claves

De las respuestas dadas por los entrevistados sobre este tema, se puede efectuar un resumen acerca de la opinión de los mismos sobre las principales causas de la vulnerabilidad del acceso a la información mediante claves. El detalle de las mismas es:

- claves obvias o simples: claves fáciles de descubrir por tratarse de datos personales o de familiares.
- Contraseñas cortas o de pocos caracteres
- Guardar las claves en lugares no adecuados (bajo el teclado, o lugares de fácil acceso) o comentarlas con otras personas.
- Existencia de programas destinados a descifrar las claves de acceso.
- Mala criptografía al guardar las contraseñas.
- Falta de seguridad en los repositores de las claves.

E.2.4. Uso de dispositivos biométricos

Acerca de este tema se efectuaron varias preguntas distintas.

La primera de ellas se centró en la opinión de los entrevistados acerca de la posibilidad de que el uso de algún dispositivo biométrico logre solucionar la falta de seguridad de los sistemas de claves de identificación.

De los ocho entrevistados,

- Siete opinaron que la biometría puede ser una alternativa para solucionar los problemas de seguridad de las claves, debido a que reemplaza la necesidad del uso de claves y que es un sistema más difícil de violar.
- Uno opinó que puede complementarlo.
- Uno opinó que el sistema biométrico puede resolver el problema de cultura del usuario en el uso de claves obvias pero no resuelve el problema de raíz ya que a largo plazo éste sistema biométrico también se vuelve inseguro debido a que no cumple con el requisito de rotación de claves.

La segunda de las preguntas estuvo enfocada a averiguar cuáles serían los beneficios que traería para el usuario el uso de la biometría. En este punto todos los entrevistados coincidieron en que los principales beneficios son el no tener que recordar claves de acceso o contraseñas y lograr mayor seguridad.

Acerca del dispositivo más conveniente para su utilización, las respuestas se basaron en dos de ellos: La huella dactilar y el reconocimiento de la voz.

Las razones para la elección de la huella dactilar fueron:

- dispositivo menos costoso
- tecnología mejor desarrollada, segura y económica
- dispositivo pequeño y fácil de instalar en cualquier clase de terminal o PC.
- comodidad y practicidad para el usuario
- fácil aceptación por parte del usuario

Las razones para la elección del reconocimiento de la voz fueron:

- más natural y menos invasivo para el usuario.
- comodidad en su uso.

Por último se les preguntó su opinión sobre la posibilidad de que, tanto los usuarios de ordenadores personales como de los sistemas multiusuarios, acepten sin problemas el uso de algún dispositivo biométrico para poder acceder a su PC o workstation.

Las respuestas de todos los entrevistados fueron similares. Opinan que si bien en principio todo cambio genera cierta resistencia, mientras el uso del dispositivo biométrico no resulte invasivo o incómodo para los usuarios, los mismos lo aceptarían con facilidad.

Dos de los entrevistados ampliaron su respuesta efectuando una aclaración: en el caso de los usuarios de ordenadores personales, si bien están expuestos a los riesgos de un ataque informático, el uso "casero" que le dan a sus PC no les justificaría la implementación de un dispositivo biométrico.

F. Glosario de terminología técnica

ADMINISTRADOR:

Persona que se encarga de todas las tareas de mantenimiento de un sistema informático. Tiene acceso total y sin restricciones al mismo.

ANTIVIRUS:

Programa que encargado de evitar que cualquier tipo de virus ingrese al sistema, se ejecute y se reproduzca. Par realizar esta labor, existen muchos programas, que comprueban los archivos para encontrar el código de virus en su interior.

ATAQUE:

Intento de traspasar las medidas de seguridad de un sistema.

BIOMETRIA:

Conjunto de técnicas que se basan en una característica biológica única (como por ejemplo las huellas digitales, la cara, la voz o los rasgos oculares, entre otros) para identificar y autentificar a un usuario.

BOMBA LÓGICA:

Programa ilegítimo contenido dentro de un sistema y que ante un hecho o una fecha prevista "explota" causando daños al sistema que lo contiene u a otro. Raramente tiene la capacidad de reproducción.

CABALLO DE TROYA:

Programa aparentemente útil el cual contiene código adicional escondido, desarrollado para obtener algún tipo de información o causar algún daño.

CLAVE, CONTRASEÑA (PASSWORD)

Palabra o frase que permite acceder a un sistema, encriptar un dato, determinar privilegios de usuarios, etc.

CONTROL DE ACCESO:

Control administrativo utilizado para restringir de modo selectivo el acceso a recursos específicos, incluyendo ficheros, directorios, redes, servidores, impresoras y otros dispositivos.

CRACKER:

Persona que quita la protección a programas con sistemas anticopia. Hacker maligno, que se dedica a destruir información.

CRIPTOGRAFIA:

Ciencia que consiste en transformar un mensaje inteligible en otro que no lo es, mediante la utilización de claves, que sólo el emisor y receptor conocen.

FIREWALL:

Barrera de protección. Es un procedimiento de seguridad que coloca un sistema de computación programado especialmente entre una red segura y una red insegura. Un sistema o combinación de sistemas que fija los límites entre dos o más redes y restringe la entrada y salida de información.

GUSANO:

Programa ilegítimo que es capaz de reproducirse a sí mismo infinitas veces hasta colapsar el sistema, en el que se está ejecutando, por falta de recursos.

HACKER:

Persona que disfruta explorando los detalles de los ordenadores y como estirar sus capacidades. A menudo se interpreta como malicioso e inquisitivo que intenta descubrir información hurgando a su alrededor.

LOGIN:

Nombre de acceso de un usuario a una red o sistema multiusuario. Este término se le puede aplicar tanto al nombre de su cuenta como al hecho de ingresar a un sistema de este tipo. El usuario debe usar el nombre, así como su contraseña, para tener acceso al sistema.

SERVER (Servidor):

Máquina que ofrece servicios a otras dentro de una red. También llamada Host.

SOFTWARE:

Programas de sistemas, utilerías o aplicaciones expresadas en un lenguaje de máquina.

USERNAME:

Nombre único que identifica a un usuario, y es utilizado como medio de identificación ante un sistema.

VIRUS:

Programa de actuar subrepticio (oculto o a escondidas) para el usuario; cuyo código incluye información suficiente y necesaria para que, utilizando los mecanismos de ejecución que le ofrecen otros programas, puedan reproducirse y ser susceptibles de mutar; resultando de dicho proceso la modificación, alteración y/o daño de los programas, información y/o hardware afectados.

VULNERABILIDAD:

Impureza del hardware o software deja a un sistema informático expuesto a potenciales ataques. Debilidad en los procedimientos de los sistemas automatizados de seguridad, controles administrativos, disposición física, controles internos, etc. Que puede ser explotada por una amenaza de ganar acceso no autorizado a información o alterar un proceso crítico.

G. Conclusiones finales

Luego de la investigación realizada sobre la biometría y su utilización como una posible solución a las vulnerabilidades que posee en la actualidad la seguridad lógica en el acceso a la información a través de claves de identificación, se ha arribado a las siguientes conclusiones.

"La seguridad informática por el propio peso de la realidad se ha convertido en un tema cotidiano en los niveles de dirección tanto de empresas e instituciones, como en los propios niveles de dirección de las áreas de sistemas y de auditoría"[2].

Las empresas y organismos necesitan mantener políticas de seguridad adecuadas para restringir el acceso a los usuarios. Esta seguridad se vuelve realmente importante cuando se trata de proteger información valiosa. Tradicionalmente los métodos de identificación, confían en un identificador externo para validar a sus usuarios: generalmente una clave o contraseña.

A lo largo de este trabajo, se han demostrado las debilidades del uso del sistema de identificación de usuarios a través de claves de acceso o contraseñas. Estas debilidades están basadas principalmente en los siguientes puntos:

- La elección por parte de los usuarios de claves obvias o simples, es decir claves fáciles de recordar pero por lo general vinculadas a información pública del usuario como por ejemplo, datos personales; palabras comunes y con sentido; nombres de lugares; etc.
- La longitud de las claves elegidas.
- El manejo inadecuado de las claves, es decir, usualmente los usuarios las anotan en lugares cercanos a la estación de trabajo o en agendas personales, o las comentan con conocidos o compañeros.
- El constante crecimiento de posibles atacantes a los sistemas de información, como son los crackers o el mismo personal interno de la organización; esto unido al desarrollo y sofisticación de las acciones y programas destinados a la obtención de claves de acceso o contraseñas.

[2] Juan Sabalain, **"Mitos y realidades en Seguridad Informática"**, en: http://www.cybsec.com

Con el uso de un sistema biométrico, la identificación de los usuarios se vuelve más confiable, evitando el uso de contraseñas o claves de acceso que luego pueden ser violadas por personas no autorizadas. La identificación y autenticación biométricas explota el hecho de que ciertas características biológicas de un individuo son singulares e inalterables y son además, imposibles de perder, transferir u olvidar. Esto brinda mayor seguridad a los usuarios.

Cada tecnología biométrica (huella dactilar, rostro, voz, etc) tiene sus propias características y variedades, sin embargo el proceso de captura, el almacenamiento y la comparación de tales características y variedades es universalmente similar.

Existen diversidad de dispositivos biométricos, y la elección de alguno de ellos en función de las características personales de los usuarios y de la aceptación por parte de estos últimos, es un aspecto en donde se ha encontrado cierta dificultad para la utilización de sistemas biométricos. La dificultad radica principalmente en dos puntos:

- Se debe seleccionar alguna parte del cuerpo que no esté sujeta a grandes cambios (gordura, envejecimiento, etc.), que sea una zona accesible y disponible y que sea lo más distintiva posible en relación al resto de la población. Frente a esto, la elección debe tener en cuenta que todos los posibles usuarios del sistema posean dicha característica.
- La utilización del dispositivo biométrico debe ser lo más cómoda y sencilla posible para el usuario, tratando de evitar de esta manera la resistencia que podría generar en el usuario sentir el uso del mismo como invasivo de su persona. Asimismo, también deben tenerse en cuenta factores como la cultura en seguridad que posean los usuarios, la concientización de la importancia de los datos; y en caso de que sea necesario efectuar capacitación al respecto.

Durante el recorrido de esta investigación, se han aportado gran cantidad de datos y por lo expuesto anteriormente podemos concluir que: *la biometría es una solución a las debilidades que posee en la actualidad la seguridad lógica en el acceso a la información a través de claves de identificación,* quedando validada la hipótesis planteada originalmente.

H. Bibliografía consultada

LIBROS

- ALDEGANI, GUSTAVO MIGUEL. **"Seguridad Informática".** MP Ediciones, Primera Edición, Uruguay, 1997.
- FAÚNDEZ ZANUY, MARCOS. **"Tratamiento digital de voz e imagen y aplicación a la multimedia"**. Editorial Marcombo S.A., España, 2000.
- FERNANDEZ, CARLOS M. **"Seguridad en sistemas informáticos"**. Ediciones Diaz de Santos S.A., España, 1988.
- KENDALL Y KENDALL. **"Análisis y diseño de sistemas".** Editorial Prentice Hall Hispanoamericana, Tercera Edición, México, 1997.
- KLANDER LARS. **"A prueba de Hackers"**. Editorial Anaya Multimedia, EE.UU., 1998.
- LEVIN, RICARDO. **"Virus informáticos".** Editorial Mc Graw Hill, España, 1992.
- NOMBELLA, JUAN JOSE. **"Seguridad Informática"**. Editorial Paraninfo, España, 1996.
- SOLER DE ARESPACOCHAGA, JOSE ANTONIO. **"Manual de Seguridad Informática"**. España, 1998.

REVISTAS, PUBLICACIONES Y SITIOS DE INTERNET

- ARDITA, JULIO. **"Elección de claves de acceso (Passwords)"**, Argentina, 1996. http://www.cybsec.com.ar
- ABIE – Asociación de Biometría Informática Española. http://www.abie.com
- Artículo: **"Las víctimas de las modernas piraterías"** en Revista Compumagazine., MP Ediciones, Argentina, Octubre 1990.
- Artículo: **"La sociedad ante la piratería"** en Revista Compumagazine, MP Ediciones, Argentina, Septiembre 1993.
- Artículo: **"Hacking"** en Revista Compumagazine, MP Ediciones, Argentina, Año X-N°109. Argentina, 1997.
- Artículo: **"Seguridad y protección: Situación actual"** en Claxion Digital, Febrero 2001. http://www. Claxiondigital.com.ar

- Artículo: **"Seguridad y protección de la información"**, BADIA CONTELLAS, JOSE MANUEL Y COLTELL SIMON OSCAR, , 3 er. Curso Ingeniería Técnica en Informática de Gestión, España, 1997/1998.
- Artículo: **"Tecnología biométrica"**, LOZANO MARTIN., 2001. http://securynet.com
- Artículo: **"Recomendaciones de Seguridad. Definición de una política de Seguridad"**, POYATO, CHELO. COLL, FRANCISCO. MORENO, DAVID. España, 15 de Diciembre de 2000. http://www.rediris.es/cert
- Artículo: **"Novedades en Biometría y Tecnología Grid"** en http://www.cibernauta.com
- Artículo: **"Seguridad Biométrica"**, Barcelona, Diciembre 2001. http://www.eurologic.es/noticias
- Artículo: **"¿Qué es biometría?"** en . http://www.hormini.com
- Artículo: **"Sistema de Identificación mediante huella digital"**, Luque José y Barrios Alejandro. En revista Tecnia, Vol. 8 N°3, páginas 11-17. Publicada por la Universidad Nacional de Ingeniería, Lima, Perú, 1999.
- Artículo: **"Mitos y realidades en Seguridad Informática"**, Sabalain Juan, en: http://www.cybsec.com
- Biometría. AST, Presentación de la Seguridad Biométrica. http://www.ast.com
- CALVO, RAFAEL FERNANDEZ. Glosario básico inglés- español para usuarios de internet. 1994-2000. http://www.ati.es/novatica
- International Biometric Group. Biometric Technology Offerings. http://www.biometricstore.com
- HUERTA ANTONIO, **"Seguridad en Unix y Redes"**. Versión 1.2 Digital – Open Publication License V10.2., Octubre 2000. http://kripotopolis.com/
- LUCENA LÓPEZ, MANUEL JOSE. **"Criptografía y Seguridad en Computadoras"**. Dpto. de Informática Universidad de Jaén. Edición Virtual, España, 1999, http://www.kripopolis.com/
- Revista Byte. Propiedad intelectual. MP Ediciones, Argentina, Mayo 1997.
- Revista Virus Report N° 6, 7, 9, 13, 15, 16. Ediciones Ubik. Hackers y virus, Argentina, 1996.

- Revista Electrónica d-zone. N°37– 31/07/2000. http://www.dzone.com

I. ANEXOS

Entrevista N°1

Nombre: Beny Blom

Ocupación: Propietario empresa de Informática

1) ¿Qué importancia tiene para usted la protección de la información guardada en la memoria de su PC?

a) ___ Poca o ninguna
b) ___ Alguna importancia
c) _X_ Mucha importancia

2) a) ¿Considera seguro y confiable el sistema actual de identificación de usuarios a través de claves de acceso o passwords? Fundamente.

Tiene un nivel de seguridad baja/media, según su estructura. Los passwords compuestos solamente por números o letras son comparativamente fáciles de crackear. Combinaciones alfanuméricas con signos # o &, junto con combinaciones de mayúsculas y minúsculas aumentan la seguridad notablemente.

b) ¿Conoce usted otros sistemas de identificación de usuarios?

Los sistemas biométricos, solos o en combinación con tarjetas inteligentes son interesantes tecnologías, si bien son en ciertos sentidos más costosas, también aumenta la seguridad considerablemente.

3) ¿En su opinión cuáles son las principales causas de vulnerabilidad del acceso a la información mediante claves?

En principio dos factores:

1. Claves simples, fáciles de descubrir (nombres de familiares, DNI, etc.)
2. Tener las claves guardadas en lugares NO adecuados (escritos bajo el teclado, en un archivo no encriptado, etc.)

4) ¿Considera que la utilización de dispositivos biométricos puede ser una alternativa que logre solucionar la falta de seguridad de los sistemas de claves de identificación? Fundamente.

Sin dudas.

5) ¿Qué beneficios traería para el usuario el uso de la biometría?

Seguridad personal, que ninguna persona pueda acceder a un sistema en nombre del usuario.

6) ¿Considera que los usuarios, tanto de ordenadores personales como de los sistemas multiusuarios, aceptarían sin problemas el uso de algún dispositivo biométrico para poder acceder a su PC o workstation?

Hoy existen una gran cantidad de dispositivos biométricos que cumplen con esta función.

7) ¿Cuál de los siguientes dispositivos le parece más conveniente para su utilización y por qué?

_X_ Huella dactilar
___ Reconocimiento del Iris
___ Reconocimiento de la retina
___ Geometría de la mano
___ Verificación de firmas
_X_ Reconocimiento de la voz

Huella dactilar, por ser la tecnología mejor desarrollada, segura y económica en este momento.

Reconocimiento de la voz, por ser interesante si se usan sistemas automatizados con acceso a base de datos restringidos vía sistemas telefónicos.

8) ¿Desea usted formular algún comentario en relación a los temas objeto de la entrevista que no le hayan sido consultados?

No por el momento.

Entrevista N° 2

Nombre: Leonardo Tadei

Ocupación: Director Ejecutivo de Empresa de Seguridad Informática

1) **¿Qué importancia tiene para usted la protección de la información guardada en la memoria de su PC?**

   a) ___ Poca o ninguna

   b) ___ Alguna importancia

   c) _X_ Mucha importancia

2) **a) ¿Considera seguro y confiable el sistema actual de identificación de usuarios a través de claves de acceso o passwords? Fundamente.**

Si, lo es. Las vulnerabilidades de estos sistemas son debido a la forma en que se encriptan las contraseñas, y a la complejidad de la contraseña utilizada. Es decir que si la clave usada es la fecha de nacimiento de la persona, la seguridad disminuye por ser la clave información pública.

Combinando un buen método de criptografía con una contraseña robusta y cambiada periódicamente, la seguridad de este sistema es muy buena.

El método de usuario/contraseña no es seguro o inseguro en sí mismo. Debe analizarse la implementación del mecanismo y la política de claves y de cambio de claves.

b) ¿Conoce usted otros sistemas de identificación de usuarios?

Si, varios.

3) **¿En su opinión cuáles son las principales causas de vulnerabilidad del acceso a la información mediante claves?**

En orden son: claves obvias, contraseñas cortas, mala criptografía al guardar claves, falta de seguridad en los repositorios de claves, usar criptografía simétrica e inseguridad en el medio de transmisión.

4) ¿Considera que la utilización de dispositivos biométricos puede ser una alternativa que logre solucionar la falta de seguridad de los sistemas de claves de identificación? Fundamente.

Tu pregunta asume que hay un problema de seguridad en el sistema de claves de identificación, lo cual no comparto plenamente. En un sistema de seguridad bien diseñado y bien usado por el usuario, el método usuario/contraseña es excelente.

Un sistema biométrico puede resolver el problema de cultura del usuario en usar claves obvias, pero no cumple con el requisito de rotación de claves, haciendo el mecanismo inseguro a largo plazo por vulnerabilidad en el repositorio de claves, ni implica que la transmisión de las medidas biométricas sea segura, ni que el repositorio sea seguro, etc.

Por ejemplo, un sistema biométrico que transmita el escaneo por un canal inseguro para validar contra el repositorio, es tan inseguro como un sistema usuario/contraseña que transmita los datos en forma insegura.

Los problemas de seguridad estarán más en la implementación que en la tecnología.

5) ¿Qué beneficios traería para el usuario el uso de la biometría?

Bien implementado, trae el beneficio de no tener que recordar la contraseña.

6) ¿Considera que los usuarios, tanto de ordenadores personales como de los sistemas multiusuarios, aceptarían sin problemas el uso de algún dispositivo biométrico para poder acceder a su PC o workstation?

Esto dependerá del método para tomar la medida biométrica. Si el método es un sensor dactilar, será fácil de usar y por ende aceptado. Si el método es incómodo o agresivo, será en general resistido.

También influirán factores como la cultura en seguridad de los usuarios, la concientización de la importancia de los datos, etc.

7) ¿Cuál de los siguientes dispositivos le parece más conveniente para su utilización y por qué?

___ Huella dactilar

___ Reconocimiento del Iris

___ Reconocimiento de la retina

___ Geometría de la mano

___ Verificación de firmas

_X_ Reconocimiento de la voz

Por ser el más natural y el menos invasivo. Si la implementación consiste en decir "Hola computadora" como mecanismo para iniciar una sesión, la comodidad sería la mayor posible.

8) ¿Desea usted formular algún comentario en relación a los temas objeto de la entrevista que no le hayan sido consultados?

Si. No tiene sentido hablar de seguridad en computadoras si se usa como plataforma un sistema operativo que no tiene seguridad en su diseño.

Entrevista N° 3

Nombre: Carlos Rossi

Ocupación: Director empresa de Diseño de Software

1) **¿Qué importancia tiene para usted la protección de la información guardada en la memoria de su PC?**

   a) ___ Poca o ninguna

   b) ___ Alguna importancia

   c) _X_ Mucha importancia

2) **a) ¿Considera seguro y confiable el sistema actual de identificación de usuarios a través de claves de acceso o passwords? Fundamente.**

No es del todo confiable, su seguridad depende en gran medida de las claves de acceso que se utilicen y de la discreción del usuario para el manejo de dichas claves.

b) ¿Conoce usted otros sistemas de identificación de usuarios?

Sí, varios.

3) **¿En su opinión cuáles son las principales causas de vulnerabilidad del acceso a la información mediante claves?**

Creo que principalmente la inseguridad de las claves se basa en que el usuario elige claves fáciles de recordar o, en el caso de que elija otras más complejas las anota en lugares inapropiados (agendas, teclado, etc.) por temor a olvidarse de la misma.

4) **¿Considera que la utilización de dispositivos biométricos puede ser una alternativa que logre solucionar la falta de seguridad de los sistemas de claves de identificación? Fundamente.**

Sí. Son sistemas más difíciles de violar.

5) **¿Qué beneficios traería para el usuario el uso de la biometría?**

No tener que recordar la contraseña o inventar contraseñas nuevas en forma periódica (en caso de que el sistema de claves utilizado exija su cambio periódicamente).

6) **¿Considera que los usuarios, tanto de ordenadores personales como de los sistemas multiusuarios, aceptarían sin problemas el uso de algún dispositivo biométrico para poder acceder a su PC o workstation?**

Considero que sí, actualmente existen dispositivos biométricos que no resultan agresivos para el usuario, por lo que lo aceptarían con facilidad.

7) **¿Cuál de los siguientes dispositivos le parece más conveniente para su utilización y por qué?**

_X_ Huella dactilar
___ Reconocimiento del Iris
___ Reconocimiento de la retina
___ Geometría de la mano
___ Verificación de firmas
___ Reconocimiento de la voz

Utilizando un buen dispositivo de escaneo de la huella dactilar, me parece el dispositivo más práctico para el usuario y el que generaría menos resistencia su implementación.

8) **¿Desea usted formular algún comentario en relación a los temas objeto de la entrevista que no le hayan sido consultados?**

No.

Entrevista N° 4

Nombre: Federico Cuñado

Ocupación: Contador Público Nacional y Docente de la cátedra de Informática de la Universidad FASTA

1) **¿Qué importancia tiene para usted la protección de la información guardada en la memoria de su PC?**

   a) ___ Poca o ninguna
   b) ___ Alguna importancia
   c) _X_ Mucha importancia

2) **a) ¿Considera seguro y confiable el sistema actual de identificación de usuarios a través de claves de acceso o passwords? Fundamente.**

No. Por que la clave de acceso se puede conocer, ya sea por que es obvia, o por que es muy difícil y se encuentra escrita.

b) ¿Conoce usted otros sistemas de identificación de usuarios?

Si.

3) **¿En su opinión cuáles son las principales causas de vulnerabilidad del acceso a la información mediante claves?**

El que se utilizan datos personales en las mismas y es de fácil identificación.

4) **¿Considera que la utilización de dispositivos biométricos puede ser una alternativa que logre solucionar la falta de seguridad de los sistemas de claves de identificación? Fundamente.**

Creo que pueden complementarla, son más difíciles de violar.

5) **¿Qué beneficios traería para el usuario el uso de la biometría?**

Más seguridad.

6) **¿Considera que los usuarios, tanto de ordenadores personales como de los sistemas multiusuarios, aceptarían sin problemas el uso de**

algún dispositivo biométrico para poder acceder a su PC o workstation?

En ordenadores personales no creo que pueda aceptarse fácilmente, en sistemas multiusuarios si.

7) ¿Cuál de los siguientes dispositivos le parece más conveniente para su utilización y por qué?

_X_ Huella dactilar
___ Reconocimiento del Iris
___ Reconocimiento de la retina
___ Geometría de la mano
___ Verificación de firmas
___ Reconocimiento de la voz

Es el dispositivo menos costoso.

8) ¿Desea usted formular algún comentario en relación a los temas objeto de la entrevista que no le hayan sido consultados?

No.

Entrevista N° 5

Nombre: Nancy Medina
Ocupación: Licenciada en sistemas

1) **¿Qué importancia tiene para usted la protección de la información guardada en la memoria de su PC?**
   a) ___ Poca o ninguna
   b) ___ Alguna importancia
   c) _X_ Mucha importancia

2) **a) ¿Considera seguro y confiable el sistema actual de identificación de usuarios a través de claves de acceso o passwords? Fundamente.**

Creo que el sistema de claves es seguro en la medida en que las claves utilizadas no sean obvias, esto significa utilizar claves de acceso con combinaciones alfanuméricas y de una cantidad de caracteres no menor de 6. Igualmente el usuario tendría que seleccionar contraseñas que no sean públicas, como por ejemplo nombres de familiares o apodos, fechas de nacimiento, DNI, etc., así como también modificarlas periódicamente.

b) ¿Conoce usted otros sistemas de identificación de usuarios?

Sí. Varios.

3) **¿En su opinión cuáles son las principales causas de vulnerabilidad del acceso a la información mediante claves?**

La elección por parte de los usuarios, de claves de acceso fáciles de conocer. También se suma a esta situación la gran cantidad de programas existentes para crackear las claves.

4) **¿Considera que la utilización de dispositivos biométricos puede ser una alternativa que logre solucionar la falta de seguridad de los sistemas de claves de identificación? Fundamente.**

Es una buena opción para liberar al usuario de la necesidad de inventar contraseñas complicadas y de recordar las mismas, así como también creo que

los dispositivos biométricos generan mayor seguridad que el sistema de claves de acceso.

5) ¿Qué beneficios traería para el usuario el uso de la biometría?

Creo que el beneficio más notorio para el usuario, es que ninguna otra persona pueda acceder a su información.

6) ¿Considera que los usuarios, tanto de ordenadores personales como de los sistemas multiusuarios, aceptarían sin problemas el uso de algún dispositivo biométrico para poder acceder a su PC o workstation?

Creo que sí.

7) ¿Cuál de los siguientes dispositivos le parece más conveniente para su utilización y por qué?

___ Huella dactilar
___ Reconocimiento del Iris
___ Reconocimiento de la retina
___ Geometría de la mano
___ Verificación de firmas
_x_ Reconocimiento de la voz

Por que es el dispositivo que da más comodidad al usuario.

8) ¿Desea usted formular algún comentario en relación a los temas objeto de la entrevista que no le hayan sido consultados?

No.

Entrevista N° 6

Nombre: Sandra Caielli

Ocupación: Ingeniera electrónica - Jefe centro de cómputos

1) **¿Qué importancia tiene para usted la protección de la información guardada en la memoria de su PC?**

   a) ___ Poca o ninguna

   b) ___ Alguna importancia

   c) _X_ Mucha importancia

2) **a) ¿Considera seguro y confiable el sistema actual de identificación de usuarios a través de claves de acceso o passwords? Fundamente.**

No del todo, depende sobre que operativo trabaje y el nivel de seguridad que requieran los datos.

b) ¿Conoce usted otros sistemas de identificación de usuarios?

Sí.

3) **¿En su opinión cuáles son las principales causas de vulnerabilidad del acceso a la información mediante claves?**

Como los usuarios no tienen en cuenta la seguridad de los datos, les pasan sus claves a otros o las anotan en lugares fácilmente accesibles, o se fijan en el teclado cuáles son las teclas que se están usando para un acceso determinado, otra causa son los programas que existen para descifrar claves.

4) **¿Considera que la utilización de dispositivos biométricos puede ser una alternativa que logre solucionar la falta de seguridad de los sistemas de claves de identificación? Fundamente.**

Sí, por supuesto. Ya que es bastante más difícil para el común de los usuarios de PC violar este tipo de sistemas.

5) **¿Qué beneficios traería para el usuario el uso de la biometría?**

La seguridad, básicamente.

6) ¿Considera que los usuarios, tanto de ordenadores personales como de los sistemas multiusuarios, aceptarían sin problemas el uso de algún dispositivo biométrico para poder acceder a su PC o workstation?

Siempre existe algún tipo de resistencia cuando se coloca algo nuevo y que implica de alguna forma un compromiso mayor, pero si se demuestra la eficacia e imposibilidad de violar la seguridad supongo que no existe mayor inconveniente.

7) ¿Cuál de los siguientes dispositivos le parece más conveniente para su utilización y por qué?

_x_ Huella dactilar
___ Reconocimiento del Iris
___ Reconocimiento de la retina
___ Geometría de la mano
___ Verificación de firmas
___ Reconocimiento de la voz

Por que el dispositivo es pequeño y fácil de instalar en cualquier tipo de terminal o PC.

8) ¿Desea usted formular algún comentario en relación a los temas objeto de la entrevista que no le hayan sido consultados?

No.

Entrevista N° 7

Nombre: Luciano Tornini
Ocupación: Analista de sistemas

1) **¿Qué importancia tiene para usted la protección de la información guardada en la memoria de su PC?**
   a) ___ Poca o ninguna
   b) ___ Alguna importancia
   c) _X_ Mucha importancia

2) **a) ¿Considera seguro y confiable el sistema actual de identificación de usuarios a través de claves de acceso o passwords? Fundamente.**

La seguridad del sistema de claves es bajo, no por que sea malo el sistema en sí, sino por que los usuarios eligen contraseñas fáciles de descubrir.

b) ¿Conoce usted otros sistemas de identificación de usuarios?

Sí.

3) **¿En su opinión cuáles son las principales causas de vulnerabilidad del acceso a la información mediante claves?**

Claves obvias, de poca longitud (es decir con pocos caracteres), sistemas que no piden al usuario el cambio de claves en forma periódica.

4) **¿Considera que la utilización de dispositivos biométricos puede ser una alternativa que logre solucionar la falta de seguridad de los sistemas de claves de identificación? Fundamente.**

Sin lugar a dudas. Primero por que el usuario no tiene que recordar claves o tomar los recaudos de no escribirlas en lugares de fácil acceso; y segundo por que son sistemas más difíciles de violar.

5) **¿Qué beneficios traería para el usuario el uso de la biometría?**

Ante todo, no tener que recordar contraseñas.

6) ¿Considera que los usuarios, tanto de ordenadores personales como de los sistemas multiusuarios, aceptarían sin problemas el uso de algún dispositivo biométrico para poder acceder a su PC o workstation?

Mientras se trate de algún dispositivo que no resulte invasivo, considero que no habría inconvenientes.

7) ¿Cuál de los siguientes dispositivos le parece más conveniente para su utilización y por qué?

_X_ Huella dactilar
___ Reconocimiento del Iris
___ Reconocimiento de la retina
___ Geometría de la mano
___ Verificación de firmas
___ Reconocimiento de la voz

Me parece que es el dispositivo que puede dar la posibilidad de que el usuario lo acepte sin sentirse incómodo y además es de fácil instalación en cualquier puerto de entrada.

8) ¿Desea usted formular algún comentario en relación a los temas objeto de la entrevista que no le hayan sido consultados?

No.

Entrevista N° 8

Nombre: Paola Ragon
Ocupación: Ingeniera Informática

1) **¿Qué importancia tiene para usted la protección de la información guardada en la memoria de su PC?**
   a) ___ Poca o ninguna
   b) ___ Alguna importancia
   c) _X_ Mucha importancia

2) **a) ¿Considera seguro y confiable el sistema actual de identificación de usuarios a través de claves de acceso o passwords? Fundamente.**

No totalmente, ya que las claves que los sistemas permiten utilizar muchas veces son demasiado cortas o sin combinaciones de caracteres de distinto tipo, es decir con símbolos o mayúsculas y minúsculas, etc. Lo que genera que el usuario seleccione claves que le resultan familiares por ser nombres o sobrenombres de familiares, fechas importantes, etc.

b) ¿Conoce usted otros sistemas de identificación de usuarios?

Sí. Varios.

3) **¿En su opinión cuáles son las principales causas de vulnerabilidad del acceso a la información mediante claves?**

Como dije antes, creo que la principal es la selección de las claves de acceso. Adicionalmente, existen en la actualidad gran cantidad de programas destinados a descubrir dichas claves.

4) **¿Considera que la utilización de dispositivos biométricos puede ser una alternativa que logre solucionar la falta de seguridad de los sistemas de claves de identificación? Fundamente.**

Creo que si, ya que reemplazaría el uso de contraseñas y es más difícil de violar.

5) ¿Qué beneficios traería para el usuario el uso de la biometría?

Mayor seguridad.

6) ¿Considera que los usuarios, tanto de ordenadores personales como de los sistemas multiusuarios, aceptarían sin problemas el uso de algún dispositivo biométrico para poder acceder a su PC o workstation?

Creo que los usuarios de ordenadores personales no verían mayor utilidad en el uso de este tipo de dispositivos, no por que no estén expuestos a la posibilidad de que algún extraño ingrese en sus PC, sino por que quizás el uso que le dan a sus máquinas es más "casero". En el caso de los sistemas multiusuarios no tendrían problemas.

7) ¿Cuál de los siguientes dispositivos le parece más conveniente para su utilización y por qué?

___ Huella dactilar
___ Reconocimiento del Iris
___ Reconocimiento de la retina
___ Geometría de la mano
___ Verificación de firmas
_x_ Reconocimiento de la voz

Considero que este dispositivo es muy bueno ya que permite comenzar a operar en la PC sólo con pronunciar una frase, y que de esa manera el usuario se sienta seguro de que la PC lo reconoció como auténtico usuario.

8) ¿Desea usted formular algún comentario en relación a los temas objeto de la entrevista que no le hayan sido consultados?

No.