PLAN de FORMACIÓN 2008

énformate

Comunidad de Madrid

PLAN DE FORMACIÓN 2008

DIRECCIÓN GENERAL DE PROMOCIÓN DEPORTIVA

COMUNIDAD DE MADRID

# Curso de Gestión de la Seguridad de usuarios de servicios deportivos

**TEMA:** Aplicación de las nuevas tecnologías de la información y la comunicación

**PONENTE:** Javier Portillo García

# AMENAZAS:

- Robo físico. Sustracción de los ordenadores de los discos duros de los mismos o de los soportes de las copias de respaldo.
- Robo "lógico". Se trata de la técnica, cada vez más extendida, de conseguir acceso remoto al ordenador donde se encuentran los datos, y copiarlos en el sistema del ladrón, que puede estar incluso en otra parte del mundo.
- Acceso a las comunicaciones. Muchas veces es posible interceptar una comunicación de datos de forma que el atacante "escucha" lo que se está transmitiendo, y puede acceder por tanto a esa información.

# NECESIDADES:

- Necesidad de identificar a las personas que acceden a un determinado recinto.
- Necesidad de identificar claramente las personas que acceden al ordenador.
- Necesidad de proteger el ordenador frente a amenazas del exterior.
- Necesidad de proteger las comunicaciones frente a interceptaciones o escuchas indeseadas.

# TECNOLOGÍAS:

- Tecnologías biométricas. Se basan en reconocer a una persona por una característica de su cuerpo: huellas dactilares, iris, voz, etc.
- Tecnologías de tarjetas inteligentes. identificación por radiofrecuencia (RFID). Se basa en la posibilidad de transmitir información de forma inalámbrica entre un lector y una etiqueta. Como veremos posteriormente, esto posibilita usos muy interesantes en el ámbito de la seguridad.
- Tecnologías de cifrado en comunicaciones. Que se utilizan para que la información que se transmite por una red informática (interna o externa a una empresa) no sea reconocible por un posible intruso que escuche las transmisiones o las intercepte.
- Tecnologías de seguridad informática. En este caso se refiere a la utilización de programas de seguridad como antivirus, firewalls, gestores de contraseñas, programas de auditoría de seguridad, programas de cifrado y ocultación de archivos, etc. Sin olvidar la realización periódica de las copias de respaldo y seguridad.

# BIOMETRÍA:

La tecnología de los sistemas de identificación biométrica utiliza características fisiológicas que son estables en los individuos. Estas características no se limitan sólo a las huellas dactilares. Existen sistemas basados en reconocimiento de la forma de la mano, de la voz, del iris, de la retina, de la firma, etc.

Dos tipos fundamentales:

- Los *sistemas de reconocimiento*, cuyo objetivo es distinguir la identidad de un individuo particular de la de los demás usuarios del sistema.

- En los *sistemas de verificación*, el individuo declara su identidad y el objetivo es averiguar si es quien dice ser.

# BIOMETRÍA:

En términos generales, los sistemas de identificación de usuario se basan fundamentalmente en tres tipos de elementos, denominados los tres pilares de la autentificación:

- Algo que el usuario *sabe*: una contraseña.
- Algo que el usuario *posee*: una llave, una tarjeta.
- Algo que el usuario *es*: una característica corporal del mismo.

# BIOMETRÍA:

Para que una característica biométrica resulte de utilidad debe cumplir algunas propiedades esenciales:

- Debe permanecer constante con el tiempo en un mismo individuo.
- Debe ser distinta para individuos distintos.
- Debe ser accesible y sencilla de obtener, y la verificación debe realizarse con rapidez. Por ejemplo, una muestra de ADN es perfectamente característica de los individuos, y cumple las dos condiciones anteriores, pero evidentemente la extracción de muestras de ADN y su posterior análisis no cumplen esta tercera condición.

# BIOMETRÍA:

Las características corporales que utilizan los sistemas de identificación biométrica son principalmente:

- Huellas dactilares.
- Patrón de las venas de la retina.
- Patrón del iris.
- Venas del dorso de la mano.
- Geometría de la mano.
- Rostro.
- Análisis de gestos.
- Patrón de voz.
- Firma manuscrita.

# BIOMETRÍA:

**Clasificación de los sistemas biométricos atendiendo al grado de participación de los usuarios que los utilizan:**

- ***Sistemas pasivos***. **Estos sistemas no necesitan que los usuarios participen activamente en la medida. De hecho, el usuario ni siquiera tiene que saber que está siendo sometido a reconocimiento biométrico. Como ejemplos tenemos el análisis del patrón de voz, del rostro o de los gestos.**

- ***Sistemas activos***. **En estos sistemas el usuario debe participar activamente en la medida. Por tanto, éstos son conscientes de que están siendo analizados biométricamente. El análisis de huellas dactilares, del iris, de la forma de la mano o del patrón de venas de la retina son ejemplos de este segundo tipo.**

# BIOMETRÍA:

De forma general, los sistemas de identificación biométrica están compuestos de tres partes:

- *Sistema de captura*. Adquiere las características (imágenes o sonidos) a analizar.
- *Sistema de proceso*. Analiza las imágenes o sonidos y extrae una serie de características, generalmente numéricas, que serán los patrones característicos de cada individuo.
- *Sistema de clasificación*. Compara las características extraídas por el sistema de proceso con las almacenadas en la base de datos del sistema. Si la comparación es positiva (las características extraídas y las almacenadas se parecen suficientemente), se autoriza el acceso.

# BIOMETRÍA:

**Errores que se pueden cometer:**

- ***Falso rechazo***. **Se produce cuando el sistema rechaza a un usuario autorizado. Se cuantifica mediante la probabilidad (o tanto por ciento) de falsos rechazos. Es un error molesto para los usuarios legítimos, pero no crítico para la seguridad. Sin embargo, es importante desde el punto de vista de la aceptación que el sistema tendrá en los usuarios. Si un usuario legítimo se ve rechazado muchas veces, su confianza en el sistema disminuirá y sus quejas sobre el mismo aumentarán.**
- ***Falsa aceptación***. **Se produce cuando el sistema acepta a un usuario no autorizado, y le facilita el acceso. Se cuantifica mediante la probabilidad (o tanto por ciento) de falsas aceptaciones. Es un error crítico tanto para la aceptación del sistema como para la seguridad. Debe minimizarse en la medida de lo posible.**

# BIOMETRÍA:

**“Buen” sistema:**

- **Que proporcione buenos resultados de identificación, es decir una baja tasa de falsos rechazos y falsas aceptaciones.**

- **Que sea aceptado por los usuarios que lo van a utilizar, es decir, que sea sencillo de utilizar y poco invasivo.**

# BIOMETRÍA:

**Aspectos clave:**

- ***Facilidad de uso***. **Es claro que si la tecnología en la que se basa el sistema de análisis biométrico no es fácil de utilizar, los usuarios lo rechazarán y el sistema fracasará. Esto implica, entre otras cosas, que el sistema sea ergonómico, que la tasa de falsos rechazos sea moderada y que el software y su interfaz con el usuario sea usable.**
- ***Posibilidades de despliegue***. **Lógicamente, el sistema debe requerir una instalación que sea abordable, lo que implica tener en cuenta factores como el tamaño de los dispositivos de adquisición de datos biométricos y de los dispositivos procesadores, la influencia de las condiciones ambientales (ventilación, humedad, temperatura, etc.) y los requisitos de infraestructura (alimentación, conectividad a red, etc…).**
- ***Coste***. **Obviamente, se trata de un factor fundamental. Hay que tener en cuenta los costes propios del dispositivo, los costes de instalación y despliegue, y los costes de mantenimiento y de las actualizaciones de hardware y software.**
- ***Aceptación de los usuarios***. **Ningún dispositivo de análisis biométrico pasará operativo más de un tiempo breve si no es aceptado por los usuarios que deben ser analizados. Es fundamental por tanto que el sistema sea fácil de utilizar (aspecto de facilidad de uso comentado anteriormente) y que además el proceso de toma de datos sea lo menos invasivo y molesto posible, y también todo lo breve posible.**

# BIOMETRÍA:

**Huella dactilar:**

- El funcionamiento básico de un sistema de identificación de huellas dactilares es el siguiente: el usuario pone su dedo sobre un sensor, que captura una imagen de la huella. De dicha imagen se buscan y extraen las características, que son de dos tipos, patrones y minucias.
- Los patrones hacen referencia a la posición de las líneas y valles, y pueden ser percibidos a simple vista por el ojo humano, mientras que las minucias se refieren a la aparición de singularidades en las líneas, como puntos de bifurcación, cercado, unión, terminación, etc., y son más difíciles de ver y de localizar Dos dedos diferentes nunca pueden poseer más de ocho minucias iguales, y cada uno tiene más de 30 ó 40 minucias.

# BIOMETRÍA:

**Huella dactilar:**

- **Los detalles relativos a las líneas (curvatura, separación, etc.), así como la posición absoluta y relativa de las minucias extraídas, son procesados mediante algoritmos que permiten componer un índice numérico correspondiente a cada huella.**

- **Este índice numérico de la huella se guarda en la base de datos del programa, en una tarjeta o en otro tipo de soporte.**

- **Es imposible reconstruir la huella a partir del índice registrado en el fichero ya que no se guarda la propia imagen de la huella, sino que la información guardada es información numérica (los patrones extraídos).**

# BIOMETRÍA:

**Huella dactilar:**

**Tipos de falsificación:**

- ***Falsificación de dedo.***

- ***Ataque al canal de comunicaciones.*** **Si el sistema de análisis de huellas necesita comunicarse vía red con una base de datos remota, esa comunicación puede ser interceptada y alterada.**

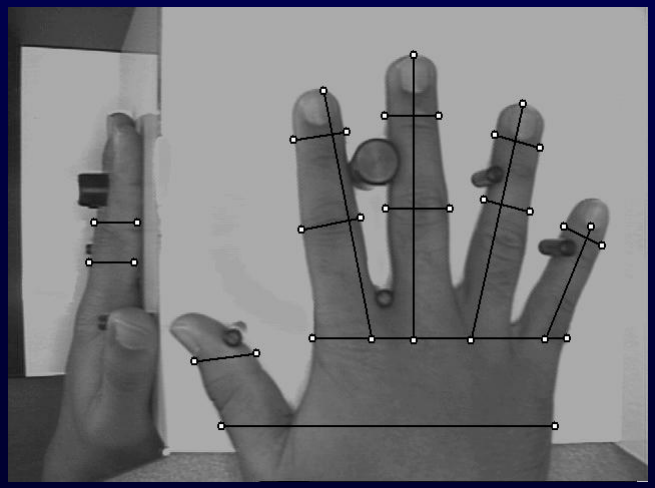
- ***Alteración de la base de datos.*** **Por último, si la base de datos con las huellas dactilares resulta comprometida, pueden sustituirse los patrones verdaderos por patrones falsos, correspondientes a personas no autorizadas que serían reconocidas positivamente.**

# BIOMETRÍA:

**Forma de la mano:**

**Estos sistemas obtienen una imagen del perfil de la mano completa, de dos dedos o de un solo dedo.**

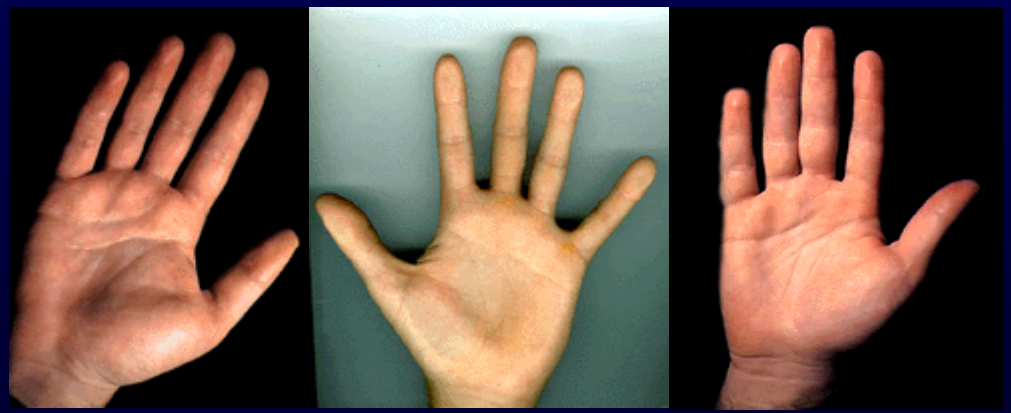
**Una vez tomadas las imágenes, se extraen una serie de características de la mano y los dedos, como pueden ser longitudes, anchuras, alturas, posiciones relativas de dedos, articulaciones, disposición de venas, etc. Los sistemas empleados hoy en día toman unas 90 mediciones. Esas características se transforman en una serie de patrones numéricos, que luego se comparan con los patrones previamente almacenados.**



# BIOMETRÍA:

**Forma de la mano:**

**Debido a que la forma de la mano se puede ir alterando con el paso del tiempo, con el aumento o la disminución de peso o con la presencia de heridas, cicatrices, etc., una característica importante que deben poseer estos sistemas es la capacidad de aprendizaje, alterando los patrones con los pequeños cambios que se pueden producir en la forma de la mano en intervalos de tiempo cortos, pero que acumulativamente no denieguen el paso a un usuario aunque en un periodo de tiempo largo.**



# BIOMETRÍA:

**Reconocimiento del iris:**

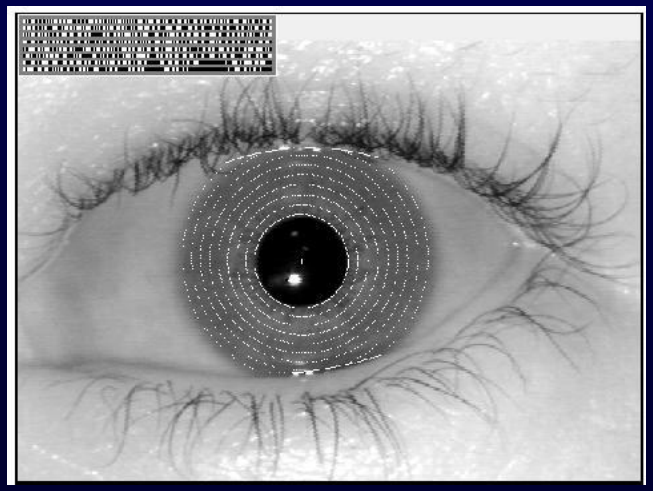
**El iris es la franja de tejido coloreado que rodea nuestra pupila. Se encuentra situado entre la córnea y el humor acuoso. Aunque lo que más resalta es su color, un estudio cercano del mismo muestra un conjunto de rasgos característicos, como estrías, anillos, surcos, texturas, etc. En el iris hay más de 400 características distintivas, o grados de libertad, que pueden ser cuantificadas y usadas para identificar a un individuo. En la práctica, se usan aproximadamente 260 de estas características.**

# BIOMETRÍA:

**Reconocimiento del iris:**

**Inicialmente, una cámara de reconocimiento de iris toma una fotografía del mismo. El sistema adquiere una imagen del iris y transforma las características anteriormente mencionadas en patrones numéricos, denominados *iriscodes*, que se contrastan con los previamente almacenados.**

**Las cámaras cumplen los estándares internacionales de iluminación segura, y utilizan un método de iluminación de longitud de onda cercana al infrarrojo que es escasamente visible y muy seguro.**



# BIOMETRÍA:

**Reconocimiento del iris:**

**Los ataques a esta tecnología pueden ser los siguientes:**

- ***Suplantación del iris*. En algún caso se ha conseguido engañar al sistema de identificación imprimiendo una imagen digital de alta resolución del iris. Esta imagen se coloca delante del verdadero iris. En todo caso, los sistemas actuales realizan una comprobación de infrarrojo, con lo que el iris que se les presenta debe ser de una persona real, lo que dificulta considerablemente este tipo de ataque.**

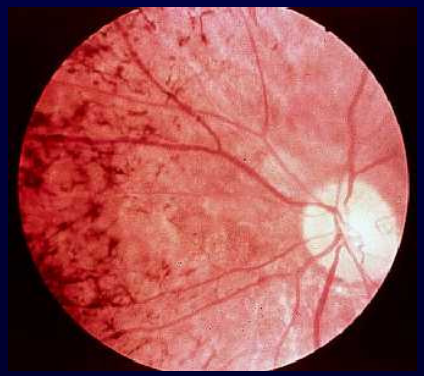
- ***Ataque a las comunicaciones*. Ya comentado anteriormente.**

- ***Ataque a la base de datos de patrones*. También comentado anteriormente.**

# BIOMETRÍA:

**Patrón de venas de la retina:**

- En esta técnica se examina el fondo del ojo y se detectan los patrones de venas que se extienden por la retina. Son también característicos y estables en cada individuo, y permiten diferenciar unos individuos de otros.
- En los sistemas biométricos basados en patrones de vasos de la retina, el usuario mira a través de unos binoculares, realiza algunos ajustes, mira a un punto determinado y por último pulsa un botón. El sistema toma una imagen de la retina, detectando la estructura de vasos sanguíneos de la retina y transformándola en una serie de características numéricas para compararlas con las almacenadas. El barrido de la retina se realiza mediante un haz infrarrojo de baja intensidad que se proyecta a través de la parte de atrás del ojo en la retina.



# BIOMETRÍA:

**Reconocimiento de voz:**

**En esta tecnología se adquiere la voz del usuario utilizando un micrófono, y seguidamente se analiza mediante un ordenador. Se buscan principalmente patrones de intensidad y frecuencia.**

**Tipos:**

- **De *texto fijo*, en los que el entrenamiento y el reconocimiento se basan en una sola palabra o frase.**
- **De *vocabulario fijo*. En este caso el entrenamiento y el reconocimiento se basan en conjunto limitado de palabras o frases. En la fase de entrenamiento, el usuario repite al sistema todas las palabras del conjunto. En la fase de reconocimiento, el sistema propone al usuario un subconjunto aleatorio de las palabras o frases para que las repita, y el sistema las compara con sus patrones almacenados.**
- **De *vocabulario flexible*. En este tipo de sistemas el usuario puede utilizar para su reconocimiento un conjunto de palabras elegidas por el, pertenecientes a un vocabulario preestablecido.**
- **De *texto independiente*, que no están atados a vocabularios fijos, ni a entrenamiento con palabras fijas. Este tipo de sistemas ofrece una tasa de errores mayor, siendo más recomendables para objetivos de seguridad los tres anteriores.**

# BIOMETRÍA:

**Reconocimiento de voz:**

**Los ataques a esta tecnología pueden ser los siguientes:**

- ***Sustitución de la voz*. Se trata de utilizar la voz grabada de un usuario autorizado para engañar al sistema. Lógicamente, este tipo de ataque es más sencillo de realizar en los sistemas de texto fijo puesto que al ser el texto limitado, se hace más susceptible a la falsificación. En los otros sistemas, al disponer de un vocabulario mas amplio o donde el sistema puede elegir para solicitar al usuario, el éxito de este tipo de ataques es más difícil.**

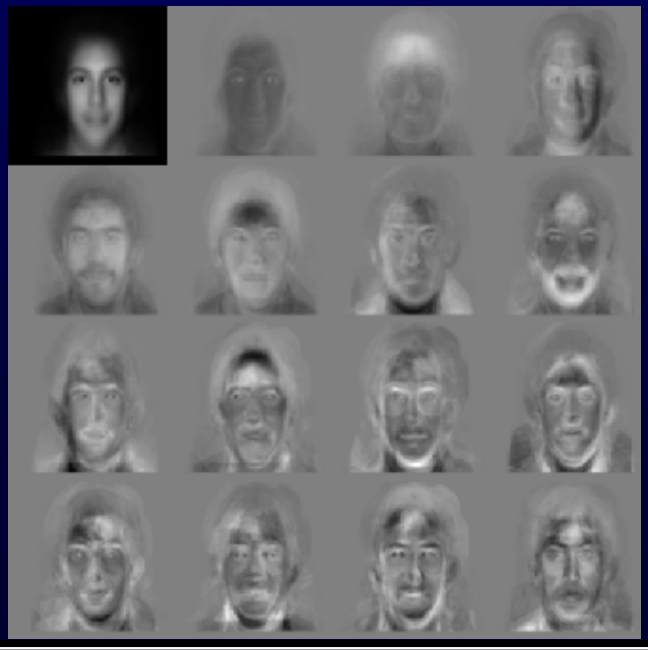
- ***Ataque a las comunicaciones*. Ya comentado anteriormente.**

- ***Ataque a la base de datos de patrones*. También comentado anteriormente.**

# BIOMETRÍA:

**Reconocimiento facial:**

**Se trata de un sistema de desarrollo relativamente reciente. Se toma una imagen de la cara de una persona (a veces se pueden tomar varias, de frente y de perfil), y se analizan las imágenes para extraer determinados parámetros, como forma general de la cara, curvaturas, situación absoluta y relativa de ojos, nariz y boca, marcas notables, etc. Esos parámetros se comparan con los almacenados en una base de fotografías o imágenes de usuarios autorizados.**



# BIOMETRÍA:

**Reconocimiento facial:**

**Este tipo de sistemas de análisis biométrico también puede ser comprometido. Las formas más habituales son:**

- ***Suplantación de la cara*. Puede hacerse tomando fotos o video de una persona autorizada y (tras un procesado de imagen si procede) utilizando la imagen como suplantación.**

- ***Ataque al sistema de comunicaciones*. Ya comentado anteriormente.**

- ***Ataque a la base de datos*. También comentado anteriormente.**

# BIOMETRÍA:

**Consideraciones importantes:**

- **Probabilidad de fallos (falsos rechazos y falsas aceptaciones). Ya hemos hablado de cifras al considerar las tecnologías anteriormente expuestas.**
- **Estabilidad, o robustez del sistema a cambios (normales) en la característica biométrica que mide. Nos referimos, por ejemplo, a cambios en el timbre de voz por un catarro, o a cambios en las características de las manos o de la cara debidas a heridas, aumento o disminución de peso, etc.**
- **Comodidad y facilidad de uso del sistema por parte de los usuarios.**
- **Invasividad, aspecto ya comentado anteriormente.**
- **Aceptación de los usuarios de que sus datos biométricos no serán accesibles por terceros.**
- **Posibilidad de engañar al sistema, obteniendo autorización mediante la sustitución de una identidad verdadera, es decir, suplantando una característica biométrica.**

# BIOMETRÍA:

**Comparativa de tecnologías:**

| | Huellas Dactilares | Mano | Iris | Retina | Cara | Voz |
|---|---|---|---|---|---|---|
| **Fiabilidad** | +++ | +++ | ++++ | ++++ | +++ | +++ |
| **Estabilidad** | +++ | ++ | +++ | +++ | ++ | ++ |
| **Comodidad** | +++ | +++ | ++ | + | +++ | +++ |
| **Aceptación** | ++ | +++ | ++ | ++ | ++ | +++ |
| **Seguridad** | +++ | +++ | ++++ | ++++ | +++ | ++ |

# TARJETAS INTELIGENTES: RFID

- RFID (Identificación por Radiofrecuencia) es un método de almacenamiento y recuperación de datos de forma remota, basado en el empleo de etiquetas o "tags" en las que reside la información.
- RFID se basa en un concepto similar al del sistema de código de barras; la principal diferencia entre ambos reside en que el segundo utilizan señales ópticas para transmitir los datos entre la etiqueta y el lector y RFID, en cambio, emplea señales de radiofrecuencia (en diferentes bandas dependiendo del tipo de sistema, tradicionalmente 125KHz, 13,56MHz, 433-860-960MHz y 2,45GHz).

# TARJETAS INTELIGENTES: RFID

- *Número de patentes sobre RFID:*

| *Año* | *Número de patentes relativas a RFID* |
|---|---|
| *2006 (Enero-Marzo)* | 225 |
| *2005* | 1250 |
| *2004* | 665 |
| *2003* | 408 |
| *2002* | 320 |
| *2001* | 210 |
| *2000* | 115 |
| *1999* | 51 |
| *1998* | 30 |
| *1997* | 12 |

# TARJETAS INTELIGENTES: RFID

- El uso tradicional ha sido en aplicaciones de logística, trazabilidad, control de inventarios, etc…
- Sin embargo, la posibilidad de escribir, almacenar (desde 1 bit a decenas de KB) y leer información de forma remota y la localización espacial del tag abren la puerta a nuevas aplicaciones, como las de seguridad.

# TARJETAS INTELIGENTES: RFID

Un sistema básico RFID está compuesto por:

- Una etiqueta (tag) RFID, en su versión más simple formada por un chip y una antena, con la capacidad de ser programada con información. Se trata de un dispositivo con memoria (de tamaño variable, desde una pegatina a un paquete de tabaco), que puede ser adherido o incorporado a un producto, animal o persona.

- Un sistema formado por un lector y una antena que interroga a la etiqueta de RFID. El sistema induce un campo electromagnético mediante el cual los datos son recibidos o transmitidos a las etiquetas RFID.

# TARJETAS INTELIGENTES: RFID

La distinción principal de las etiquetas se hace en función de su fuente de alimentación. Las etiquetas pueden ser *activas* o *pasivas:*

- Las **etiquetas RFID pasivas** reflejan la señal de radiofrecuencia transmitida hacia ellas desde un transceptor y añaden información modulando la señal reflejada. Trabajan a corta distancia ( 1 m.).

- Las **etiquetas RFID activas** disponen de alimentación propia que permite recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID, a gran distancia (decenas de metros).

# TARJETAS INTELIGENTES: RFID

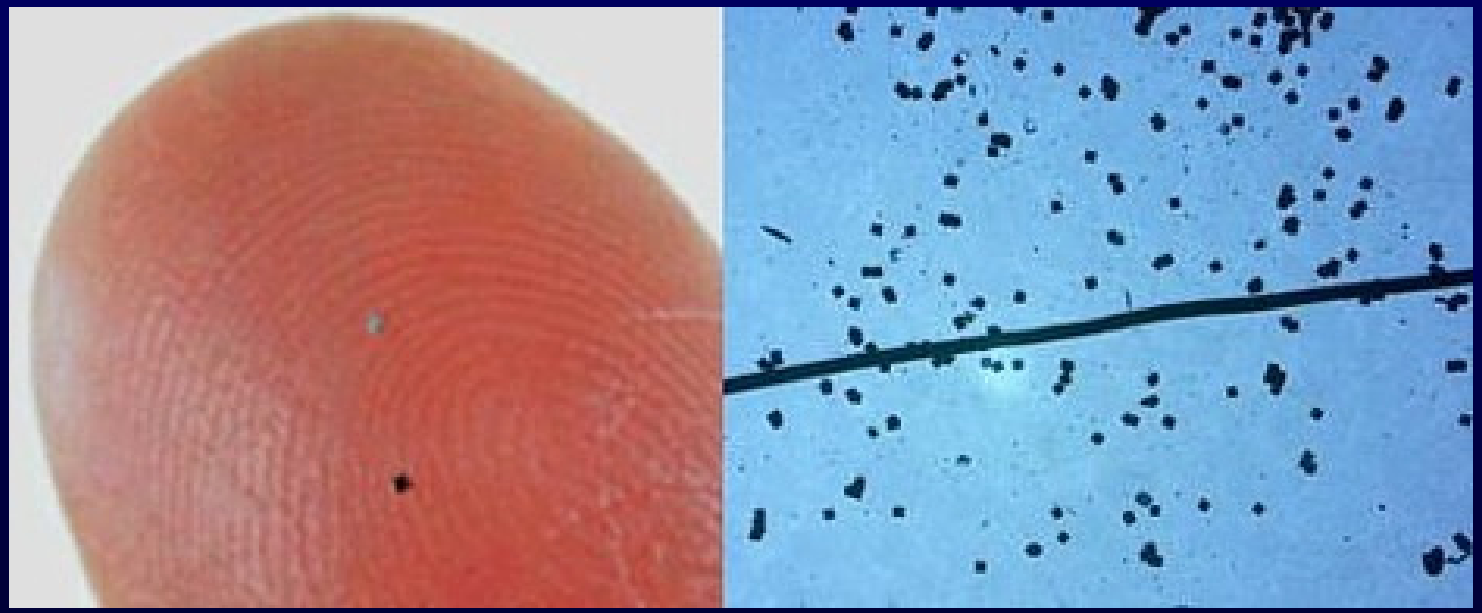

# TARJETAS INTELIGENTES: RFID

La distinción principal de las etiquetas se hace en función de su fuente de alimentación. Las etiquetas pueden ser *activas* o *pasivas:*

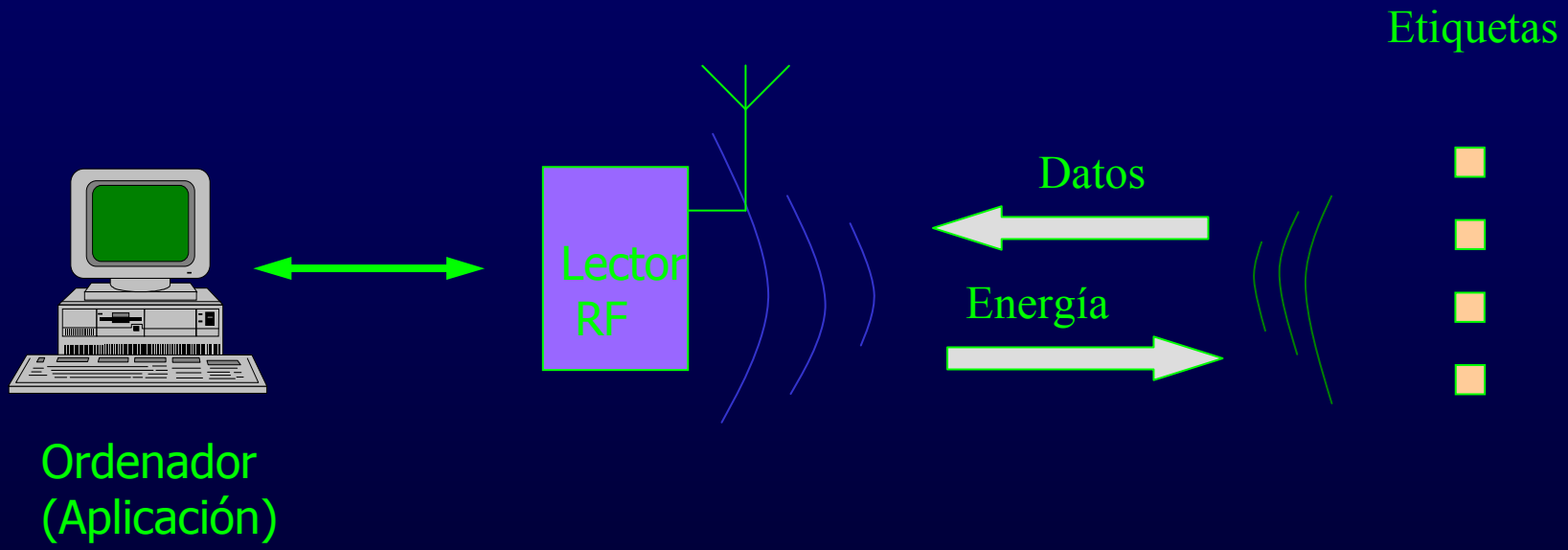
- Las **etiquetas RFID pasivas** reflejan la señal de radiofrecuencia transmitida hacia ellas desde un transceptor y añaden información modulando la señal reflejada. Trabajan a corta distancia ( 1 m.).

- Las **etiquetas RFID activas** disponen de alimentación propia que permite recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID, a gran distancia (decenas de metros).

# TARJETAS INTELIGENTES: RFID



# TARJETAS INTELIGENTES: RFID



# TARJETAS INTELIGENTES: RFID

- Posibilidad de añadir información (reprogramación).
- Alta capacidad de almacenamiento de información.
- Reutilización y durabilidad.
- Mecanismo anticolisión para realizar múltiples lecturas.
- Robustez y seguridad (puede proteger la información, codificarla).
- Capacidad de lectura sin necesidad de tener línea de vista.

# SEGURIDAD INFORMÁTICA

**Podemos catalogar los problemas de seguridad como:**

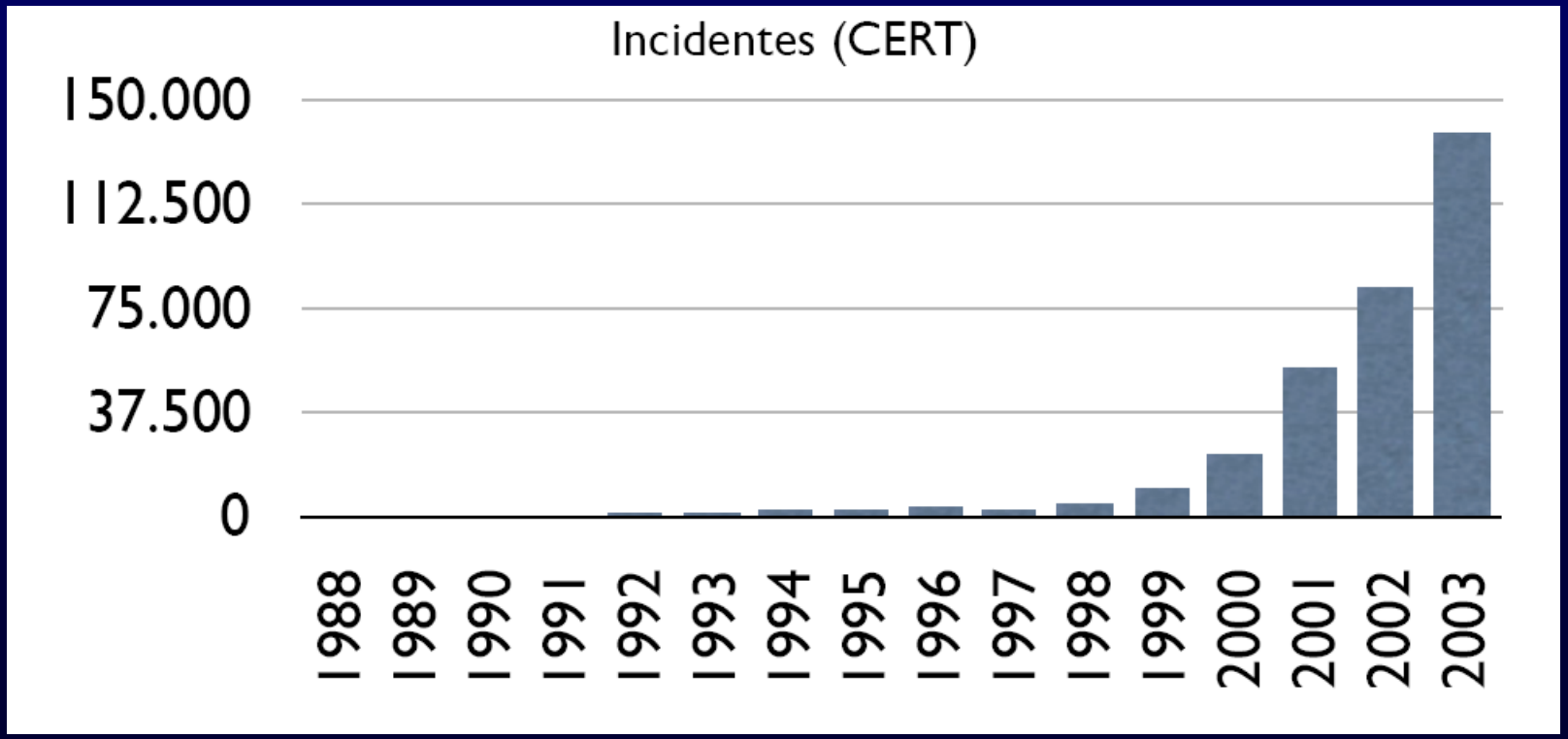
- **Aquellos que comprometen la integridad o la privacidad de los datos almacenados.**
- **Aquellos que permiten acceso a recursos supuestamente no permitidos.**
- **Aquellos que impiden el acceso a recursos a usuarios legítimos.**
- **Aquellos que permiten hacer un mal uso de los recursos informáticos.**

# SEGURIDAD INFORMÁTICA

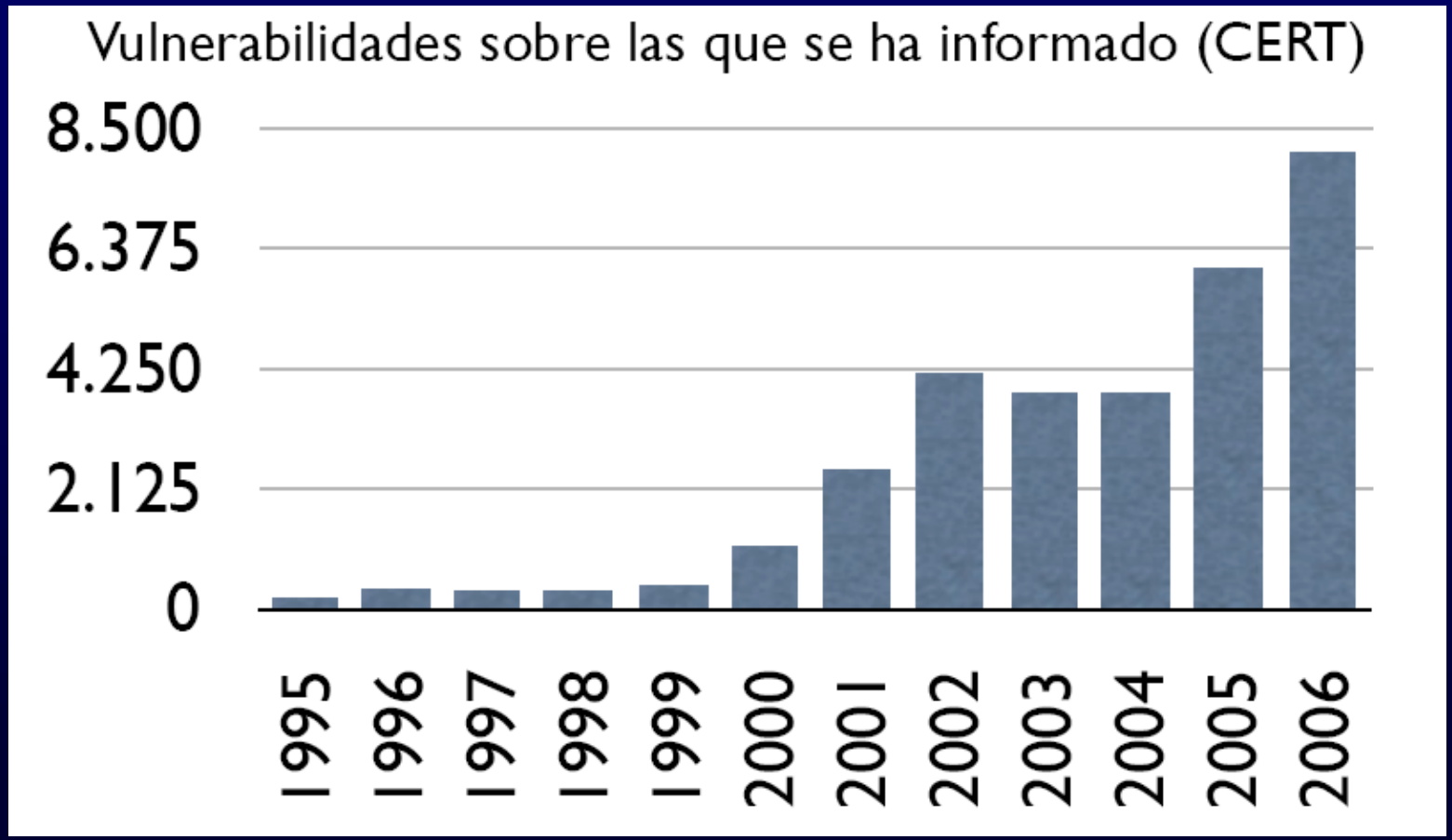
Hoy en día existen numerosas amenazas a un sistema informático, y a los datos almacenados en el mismo. Por ejemplo:

- Virus informáticos, Troyanos, Gusanos.
- Páginas web “hostiles”.
- “Spyware”.
- Entradas en sistemas ajenos.
- Robo de datos bancarios.
- Cambio de páginas Web.
- Ataques DoS a nivel mundial.

# SEGURIDAD INFORMÁTICA



# SEGURIDAD INFORMÁTICA



# SEGURIDAD INFORMÁTICA

¿Cuáles pueden ser las razones de la inseguridad de un ordenador? Algunas de ellas pueden ser:

- Instalaciones "por defecto" no pensadas para la seguridad.
- Facilitar al máximo todo al usuario, automatización. Seguridad vs. Comodidad.
- Complejidad de los sistemas, interacciones no previstas.
- Sistemas "distribuidos"
- Desconocimiento en temas de seguridad por parte de los programadores y responsables de archivos informáticos.
- Renuncia por parte de los usuarios a aprender cómo funcionan las cosas.
- Credibilidad y buena voluntad del usuario.
- Falta de concienciación.

# SEGURIDAD INFORMÁTICA

Una vez se ha encontrado y explotado un problema de seguridad en un ordenador, las consecuencias pueden ser múltiples. Por ejemplo:

- Denegación de servicio.
- Eliminación de evidencias.
- Ejecución no permitida.
- Acceso a datos ajenos.
- Modificación de datos ajenos.
- Ejecución arbitraria.
- Control total.

# SEGURIDAD INFORMÁTICA

Y ello trae como consecuencia una serie de problemas para los usuarios y responsables de los archivos informáticos:

- Pérdida de tiempo, sistemas más lentos.
- Pérdida de trabajo (datos).
- Pérdidas económicas (robos).
- Coste de protección y reparación.
- Deterioro de sistemas vitales.

# SEGURIDAD INFORMÁTICA

**Métodos de ataque. Se pueden distinguir:**

- **Métodos basados en ingeniería social.**
- **Métodos que necesitan la cooperación (inconsciente) del usuario: virus y troyanos.**
- **Métodos que necesitan al interacción con el usuario: Phishing.**
- **Métodos autónomos.**

# SEGURIDAD INFORMÁTICA

Las principales medidas de seguridad que conviene conocer son:

A nivel de usuario.

- Conocimiento del sistema.
- Verificación de integridad (hay programas, y recursos en Internet)
- Protocolos cifrados.
- Revisión de registros (”logs”).
- Paranoia. Evitar ejecución de código externo.
- Utilizar aplicaciones “seguras”.
- Tener instalados todos los parches de seguridad (Windows Update…)
- Utilizar contraseñas seguras.
- Utilizar para trabajar cuentas sin privilegios especiales.
- Eliminar servicios que no se utilicen
- Utilizar antivirus y el cortafuegos, configurarlos adecuadamente y activar la opción de actualizaciones automáticas de los mismos.

# SEGURIDAD INFORMÁTICA

**A nivel de administración**

- **Políticas de seguridad.**
- **Diseño estricto de la red y los servicios.**
- **Barreras de acceso.**
- **Copias de seguridad, recuperación ante desastres,**
- **Configuración correcta de la red.**
- **Cifrado de las comunicaciones.**
- **Protocolos seguros de autentificación.**
- **Medidas preventivas.**
- **Trampas (”Honeypots”)**
- **Departamento legal. Registros. LSSI.**

# SEGURIDAD INFORMÁTICA

Un informe de seguridad realizado por Panda Software (www.pandasoftware.es) sobre protección antivirus en pymes arroja resultados cuanto menos preocupantes; basta con observar las siguientes cifras:

- Sólo el 32,09% de las empresas tienen instalado y actualizado un antivirus.
- El 33,39% no dispone de antivirus, o no tiene correctamente actualizado el que utiliza.
- El 28,52% ni siquiera saben si están protegidos, o si lo están correctamente.

# ATAQUES INFORMÁTICOS

**Algunos tipos de ataques:**

1. **Ataques de Monitorización. El objetivo de estos ataques es estudiar el sistema objetivo, y las potenciales víctimas en busca de debilidades, vulnerabilidades o puntos abiertos de acceso.**
2. **Ataques de Autentificación. El objetivo de estos ataques es conseguir el acceso al sistema objetivo mediante tácticas de engaño. Puede realizarse consiguiendo una clave de acceso válida (mediante un ataque de monitorización realizado con éxito), o bien interponiéndose en una sesión ya establecida y suplantando a uno de los actores.**
3. **Ataques de denegación de servicio (DoS). Este tipo de ataque busca inutilizar el funcionamiento de un programa o servicio, o impedir que los usuarios puedan utilizarlos.**
4. **Ataques de modificación. Lo que distingue a estos ataques es que la entidad atacante puede causar daños en el sistema, modificando o borrando información de los sistemas víctima. Puede considerarse uno de los objetivos finales de un ataque, tras los correspondientes ataques de monitorización y autentificación.**

# LOS VIRUS

**Tipos**

- **Virus de archivo**

**Infectan archivos ejecutables y se activan con la ejecución de éstos. Pueden "dormir", y activarse ante un evento temporal (bomba de tiempo) o ante la realización de una acción específica por parte de un usuario u otro programa.**

- **Virus de sector de arranque**

**Reside en el sector de arranque de los disquetes, y se cargan en memoria al arrancar el sistema desde disquete.**

- **Virus residentes**

**Residen en memoria, infectando todos los archivos sensibles empleados por el usuario.**

- **Virus polimórficos**

**Las copias de sí mismos no son idénticas, lo que dificulta su detección e identificación.**

# LOS VIRUS

- Virus de macro

Infectan las macros de ejecución automática en programas como Word, Excel, etc…

- Virus de correo electrónico

Se propagan por los mensajes de correo electrónico, y usan diversas técnicas (doble extensión, ingeniería social,…) para lograr que el usuario ejecute el código malicioso de los archivos adjuntos. A veces, para que actúen, basta con visualizar el mensaje. Suelen reenviarse además a las direcciones presentes en la libreta de direcciones de la víctima, para lo que algunos disponen incluso de su propio motor de correo SMTP.

- Caballos de Troya o troyanos

Se trata de programas que, además de su función habitual, realizan funciones no conocidas por el usuario, como por ejemplo, facilitar el acceso y control del sistema por parte de un intruso.

# LOS VIRUS

- **Gusanos**

**Son programas que, aprovechando la infraestructura de Internet, consiguen propagarse de forma exponencial. A su gran facilidad de difusión hay que añadir la sencillez de programación, lo que les hace potencialmente muy perniciosos, especialmente cuando incluyen código dañino.**

- **Amenazas combinadas**

**Se trata de programas que aúnan las características de virus, troyanos y gusanos, multiplicando así su capacidad de difusión y daño. Este tipo de amenaza es la tendencia a la que se mueven los creadores de códigos maliciosos.**

# SOLUCIONES

- **Programas antivirus**
  - **Son programas capaces de impedir la entrada de un virus en nuestro sistema, así como de detectar y eliminar los virus ya existentes en el mismo. Los programas antivirus contienen, entre otras cosas, extensas bases de datos con las denominadas "firmas" de los virus, que son secuencias de código características de cada virus.**

- **Programas cortafuegos**

  **Son sistemas hardware o software que se insertan entre nuestra red o sistema y otra red considerada como no segura. Monitorizan e interpretan todo el tráfico entrante y saliente permitiendo sólo las comunicaciones autorizadas.**

# SOLUCIONES

- Los Sistemas de Detección de Intrusos permiten detectar los ataques a los sistemas, y proporcionar detalles sobre los mismos. Proporcionan tres funciones fundamentales:

  - Monitorización: Actúan como un "sniffer", vigilando continuamente las actividades de la red.
  - Detección: Mediante patrones de comportamiento configurables detectan posibles actividades sospechosas.
  - Acción: Actuaciones que se realizan al detectar un patrón de actividad sospechoso. Pueden variar desde un simple aviso al administrador hasta la expulsión del un usuario del sistema.

# SOLUCIONES

- **Contraseñas seguras**

**Resultados de un estudio que aplicó ataques basados en diccionario a 13794 cuentas, con un diccionario de 62727 palabras: Klein, David V, "Foiling the Cracker: A Survey of and Improvement to Password Security".**

| Tiempo | Número de contraseñas descubiertas |
|---|---|
| 15 minutos | 368 (2,66%) |
| 1 semana | 3000 (21,74%) |
| 1 año | 3340 (24,22%) |

| | Número de posibles caracteres del alfabeto | | | |
|---|---|---|---|---|
| **Longitud (caracteres)** | **26** | **36** | **52** | **96** |
| **6** | 51 minutos | 6 horas | 2,3 días | 3 meses |
| **7** | 22,3 horas | 9 días | 4 meses | 24 años |
| **8** | 24 días | 10,5 meses | 17 años | 2288 años |
| **9** | 21 meses | 336 años | 890 años | 219601 años |
| **10** | 45 años | 1160 años | 45840 años | 21081705 años |

# LAS CONTRASEÑAS

**Algunas reglas para contraseñas seguras:**

1. **No utilizar nunca palabras ni secuencias de números relacionados con los datos personales (nombre, DNI, teléfono, etc.).**
2. **Mezclar mayúsculas, minúsculas, números y caracteres no alfanuméricos.**
3. **Usar contraseñas largas, como mínimo de 8 caracteres.**
4. **No utilizar palabras que puedan estar en diccionarios.**
5. **Utilizar, por ejemplo, acrónimos de frases, es decir, componer una frase que sea fácil de recordar y concatenar las primeras letras de las palabras que la componen.**
6. **No apuntar nunca por escrito una contraseña, ni revelársela a nadie.**
7. **Contestar siempre que no a los programas que piden almacenar una contraseña para usos posteriores.**
8. **Cambiar la contraseña regularmente.**

# SOLUCIONES

- La Criptografía consiste en la utilización de sistemas para transformar un mensaje inteligible en uno ininteligible.
- Uso de Protocolos Seguros. Son conocidos los problemas de seguridad de servicios como Telnet, FTP, etc., entre otras cosas por el envío “en claro” de las contraseñas que pueden ser monitorizadas por un “sniffer”. Los protocolos seguros ofrecen alternativas de seguridad en los diversos niveles de la estructura de transmisión de datos.

# SOLUCIONES

- El uso de Herramientas de Auditoría no debe faltar en la implementación de ningún sistema de seguridad. Estas herramientas permiten identificar vulnerabilidades y proponer medidas de corrección. En la auditoría de un sistema informático deben contemplarse tareas como:

  - Descripción de los sistemas físicos, redes y protocolos.
  - Análisis de aplicaciones y servicios.
  - Análisis de vulnerabilidades.
  - Registro de actividades de usuarios y del sistema.

# LA POLÍTICA DE SEGURIDAD

- La política de seguridad informática establece los procedimientos y acciones que se deben realizar en una organización para la salvaguarde de sus sistemas informáticos y de la información almacenada en los mismos.
- Puntos comunes de acción:
  - Evaluación de riesgos.
  - Evaluación de amenazas.
  - Mecanismos de seguridad física.
  - Control de accesos.
  - Mecanismos de seguridad lógica.
  - Planes de contingencia.
  - Directivas de uso de aplicaciones y servicios.
  - Grupos de usuarios y privilegios.
  - Política de copias de seguridad.
  - Auditoría informática.

# EL FUTURO DE LAS AMENAZAS

- Las amenazas combinadas son códigos que combinan las características de virus, troyanos y gusanos para propagarse e infectar servidores y ordenadores, aprovechando vulnerabilidades de diversas aplicaciones.

- Los gusanos del futuro: supergusanos y gusanos durmientes. En palabras de George Bakos, experto en seguridad en Institute for Security Technology Studies de Hanover: "Los gusanos híbridos serán el estándar del futuro. Atacarán múltiples vulnerabilidades en múltiples plataformas. Por otra parte, los gusanos durmientes accederán a los sistemas para permanecer "dormidos" e indetectables. En un determinado momento, y respondiendo por ejemplo a pautas de ataque sincronizado, los gusanos pueden activarse simultáneamente.

- Una nueva amenaza se cierne sobre los usuarios de dispositivos móviles: los virus de PDA y de teléfono móvil.

# GRACIAS POR LA ATENCIÓN PRESTADA

**Javier Portillo García**

**javierp@grpss.ssr.upm.es**