Gestión de la Seguridad Informática

Dr. Félix Oscar Fernández Peña

ffernandez1@utmachala.edu.ec

Presentación del Profesor

Félix Oscar Fernández Peña.

- Ing. Informático, 1999.
- MSc. Telemática, 2001.
- Dr. Ciencias Técnicas (Informática) 2008.

Estudiante

- Nombres y Apellidos.
- Experiencia en redes de computadoras / administración / seguridad informática.
- Expectativas con la asignatura.

Actualidad

- Adopción rápida y masiva de tecnologías informáticas y de telecomunicaciones.
- Limitaciones en las herramientas legales.
- Volumen creciente de vulnerabilidades.
- Conocimientos limitados sobre seguridad.

Objetivo General

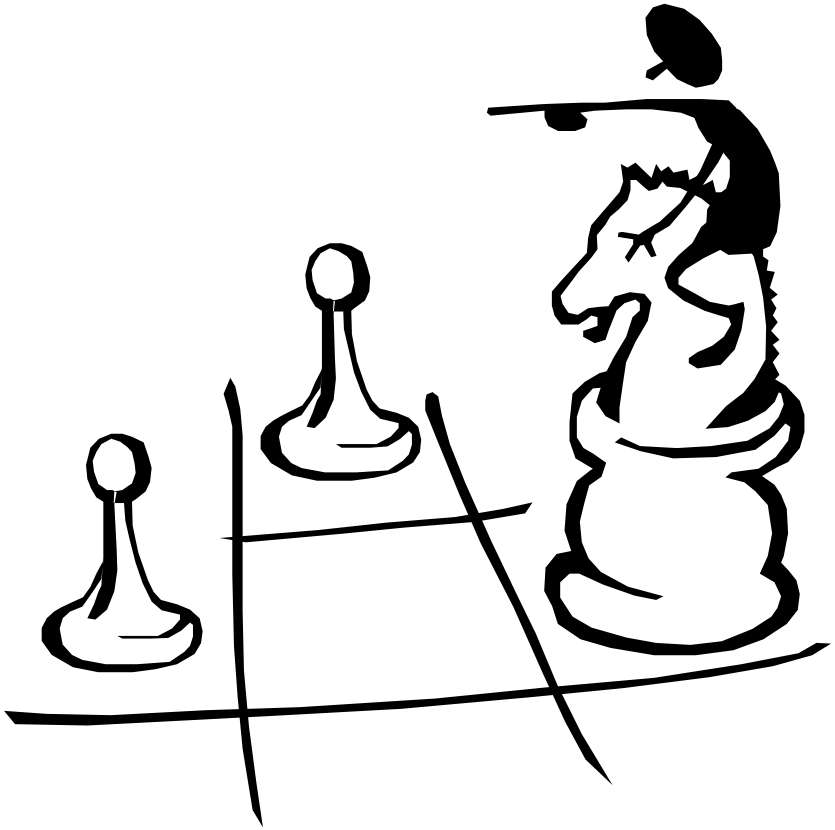
Adquirir competencias relacionadas con la gestión de la seguridad del software.

Temas de la Asignatura

1. Pilares de la seguridad del software.
2. Desarrollo seguro del software.
3. Auditoría de la seguridad del software.
4. Ingeniería social.

Sistema de Evaluación

Parámetro de Evaluación	Porcentaje
Participación en clases.	15
Presentación de trabajos en grupo.	15
Actividades de laboratorio (informe a través de Plataforma).	20
Trabajo autónomo	10
Exámenes (evaluación con reactivos en Plataforma).	40



TEMA 1. PILARES DE LA SEGURIDAD DEL SOFTWARE

Seguridad Computacional

"Un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza". Dr. Jorge Ramió Aguirre, Universidad Politécnica de Madrid.

"La protección de sistemas, datos y servicios contra amenazas accidentales y deliberadas que pudieran resultar en una pérdida de confidencialidad, integridad y disponibilidad".

Robert English, e-Security, OSIPTEL.

Redes de Computadoras

- Investigación universitaria.
- Correo electrónico.
- Compartir recursos (impresoras, …).
- Transacciones bancarias.
- Compras.
- Declaraciones de impuestos.

Seguridad de las Redes: Problema potencial de grandes proporciones.

Operación en la red

- La mayoría de los servicios descansan en el modelo cliente-servidor.
- Las mejores soluciones de gestión empresarial son débiles desde la perspectiva de la seguridad.
- Elevar los niveles de seguridad deriva en un complejo sistema de permisos y accesos en los sistemas.

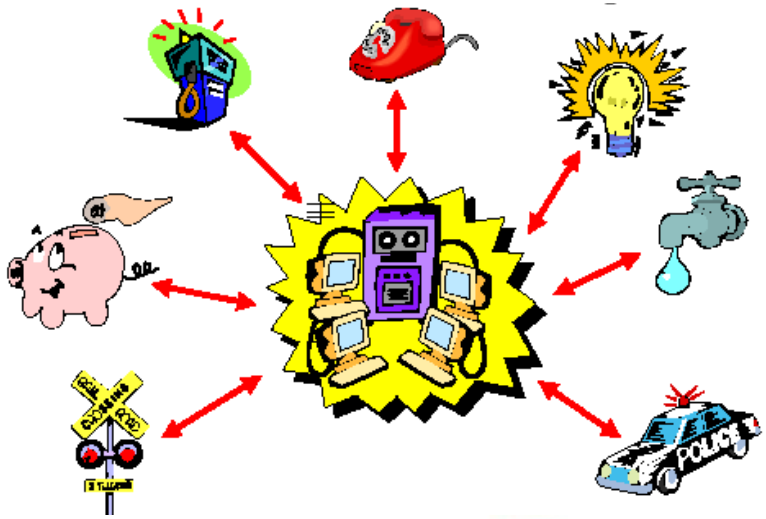
Situación en EE.UU

Más del 85% de las empresas están utilizando tecnologías de Firewalls, IDS, Certificados Digitales y Anti-virus.

Los virus informáticos, el phishing y el robo de identidad son la problemática más común.

El 78% declaró a Internet como el punto de ataque más frecuente.

Actualidad



Convergencia IP

Dispositivos de Hoy y del Mañana

"We haven't seen many smart phone attacks yet, because it's still much easier to break into a desktop," Maiffret said. "But that's going to shift because smart phones are becoming increasingly like a wallet, with applications that support banking right on the device. More sensitive data will be on the phone, making it much more worthwhile for attackers."

Compounding the problem is that smart phone makers are repeating the old mistakes made by computer manufacturers more than a decade ago. Specifically, in the rush to bring new technology to market, developers are overlooking security. The secure development lifecycle you've heard about doesn't apply to smart phones -- yet.

Marc Maiffret, eEye CTO . **December 07, 2010**

“Delincuentes” más comunes

- Estudiante.
- Hacker.
- Representante de ventas.
- Hombre de negocios.
- Ex empleado.
- Contador.
- Corredor de bolsa.
- Timador.
- Espía.
- Terrorista.

Tanenbaum. “Redes de Computadoras”. 3a edic. Cap. 7. p. 578.

Tipos de Ataque

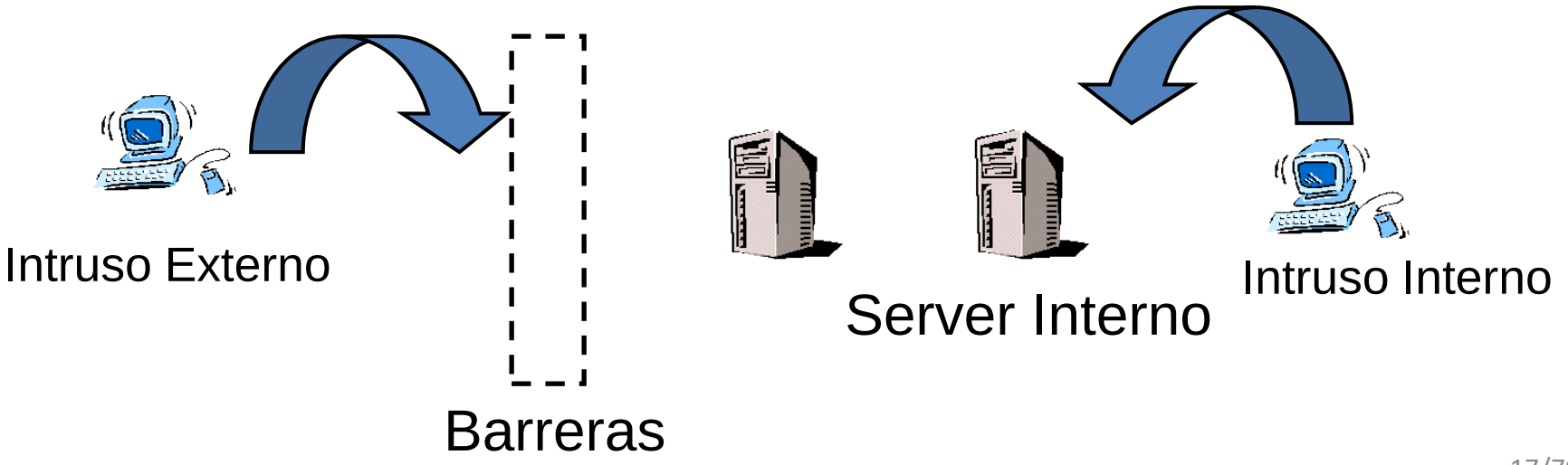
- Ataque pasivo: quien escucha en el canal de comunicación.

- Ataque activo: quien modifica los mensajes legítimos por un interés particular.

Tipos de Ataque

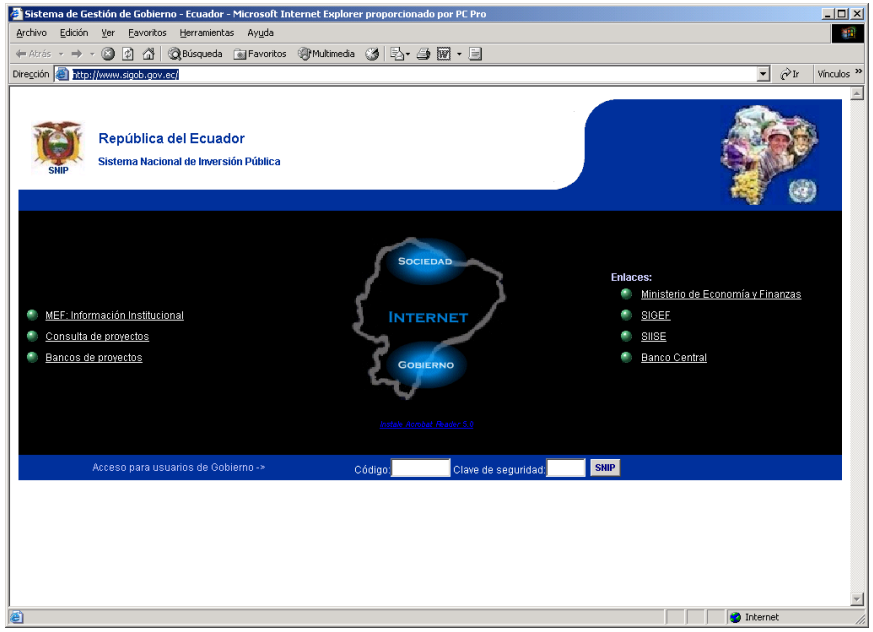
- Ataque interno.

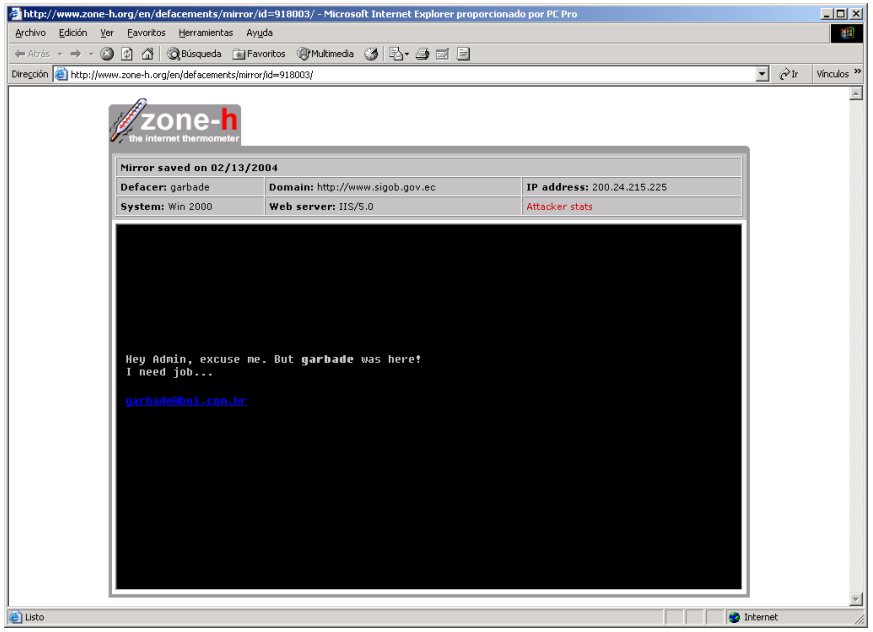
- Ataque externo.



Sitios Hackeados (1/2)

www.sigob.gov.ec

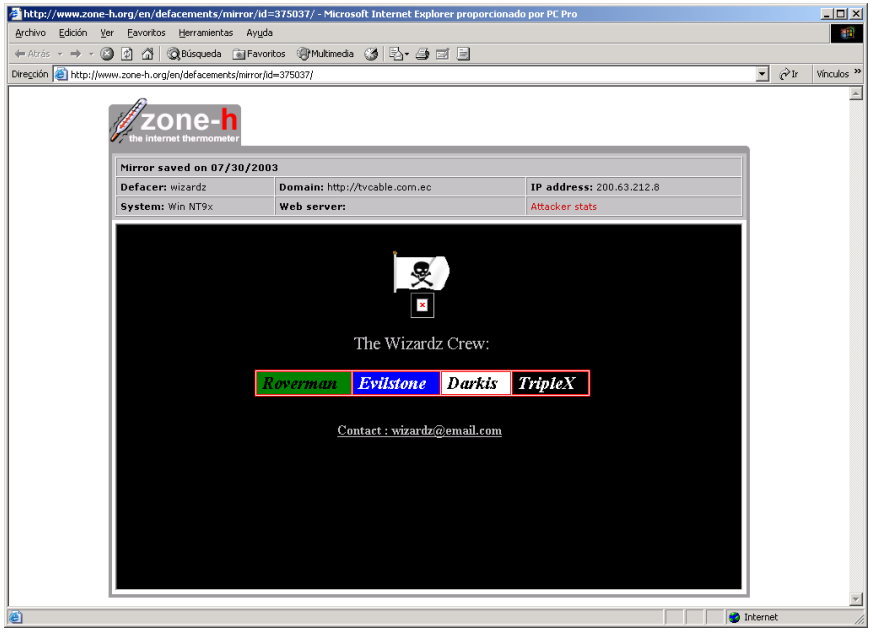




13 de Febrero de 2004

Sitios Hackeados (2/2)

www.tvcable.com.ec



4 de Agosto de 2003

Factor Humano

- Factor determinante.
- Las personas dejan el tema de la seguridad a los expertos.
- En no pocas entidades no se realiza salvas de la información, no se actualizan los antivirus, no se posee un plan para enfrentar las contingencias….
- Existen importantes carencias de instrucción en el tema.

Aspectos Legales

- Cheque electrónico y su copia son idénticos.
- Marco legal para la operación de una empresa virtual.
- Marco legal para la “delincuencia digital” en Internet.

Áreas del Problema

- Autenticidad: ¿con quién se está hablando?
- Confidencialidad: mantener la información accesible solo a usuarios autorizados.
- Control de integridad: validación de contenido.
- No repudio: certificación de origen.

Situaciones Prácticas

- El usuario A se autentica en un servidor ftp y tiene acceso a información del usuario B del sistema.
- El usuario A envía un mensaje X al usuario B y el usuario C intercepta el mensaje y hace llegar al usuario B un mensaje X'.
- El usuario A accede a información del usuario B sin que el sistema le requiera autenticarse.
- El usuario A envía mensaje cifrado con el certificado digital del usuario B.

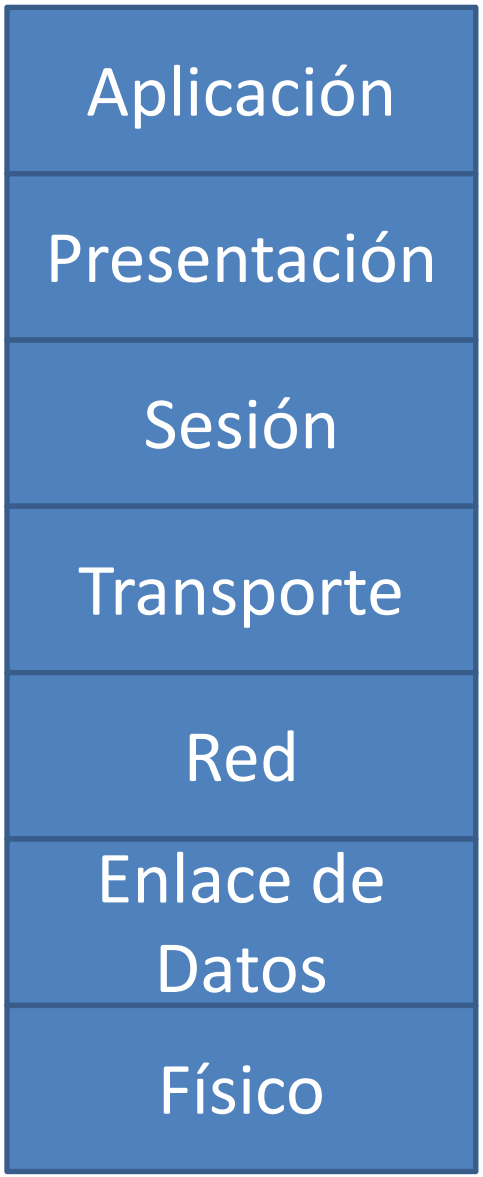
Modelo de Seguridad

7498-2, Jul. 1988 describe el modelo de referencia OSI.

Presenta en su parte 2 una Arquitectura de seguridad ("Information Processing Systems. OSI Reference model- Part 2: Security Architecture". ISO/IEC IS 7498-2, Jul. 1988).

Objetivo: proteger las comunicaciones de los usuarios en las redes.

Modelo de Seguridad



- Validación de autenticidad /No repudio / Cifrado.
- Cifrado de conexión.
- Muros de Seguridad.
- Cifrado de datagramas.
- Protección contra la intervención de las líneas.

Políticas de Seguridad

- Define qué es valioso y cómo protegerlo.
- Indica qué está y que no está permitido.
- Diferentes enfoques en su formulación.
  - General, que cubra la mayor cantidad de posibilidades.
  - Una por cada grupo de recursos a proteger (correo, información personal, etc.)
  - Sencilla pero enriquecida con estándares y líneas directrices.
  - Administrativas, control de acceso y flujo de información.

Definición de Políticas

- Plan de Seguridad Informática.
- Códigos de Ética.
- Plan de Contingencia.

Establece los **principios organizativos y funcionales** de la actividad de Seguridad Informática en un órgano, organismo o entidad, a partir de las **políticas y conjunto de medidas** aprobadas sobre la base de los resultados obtenidos en el **análisis de riesgo** previamente realizado.

Establece las medidas para **restablecer y dar continuidad** a los procesos informáticos ante una **eventualidad o desastre**.

Elementos de Seguridad

- Detección y prevención de intrusos.
- Filtrado de paquetes.
- Cifrado (Firma digital, Certificación digital, Cifrado de información).
- Salvas o respaldos de información.
- Mecanismos de actualización o parches de sistemas.
- Antivirus.
- Trabajo Forense.
- Diagnósticos de Seguridad.
- Análisis estadístico de eventos.
- Sistemas proxy o intermediarios.

Áreas del Problema

- Confidencialidad: mantener la información accesible solo a usuarios autorizados.

Cifrado

- Autenticidad: ¿con quién se está hablando?

Autenticación

Certificado Digital

- No repudio: certificación de origen.

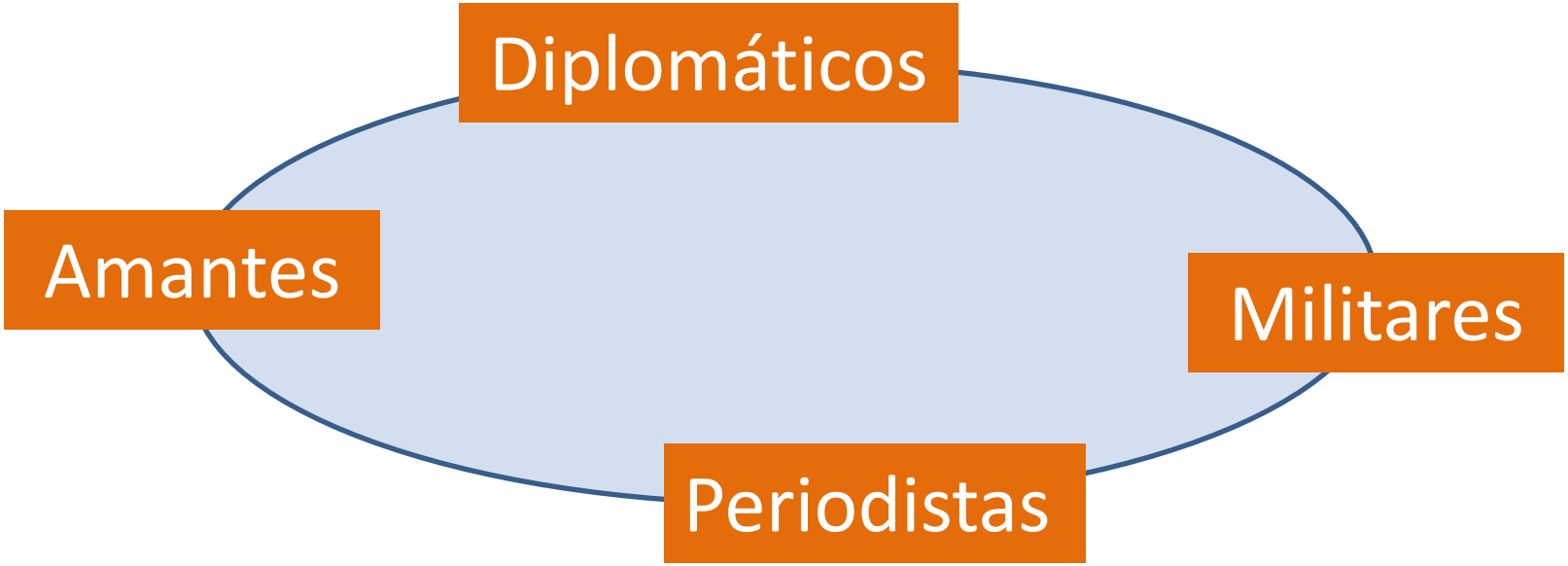
Firma Digital

- Control de integridad: validación de contenido.

Funciones Hash.

Aplicaciones en Red Actuales

- Plataformas de autenticación.
- Uso de tokens de seguridad.
- Aplicaciones n-capas.
- Posibilidad de suplantación de identidad por un robot.



CRIPTOGRAFÍA

Cifrado

Disciplina que estudia los principios, métodos y medios de ocultar la información contenida en un mensaje.

<u>Según la RAE:</u>

el arte de escribir con clave secreta o de modo enigmático.

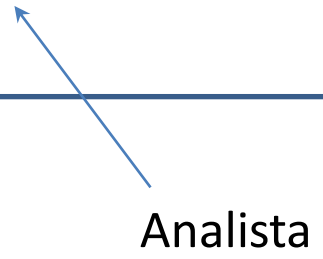
Rama inicial de las Matemáticas, y en la actualidad también de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar, y por tanto proteger, un mensaje o archivo por medio de un algoritmo, usando una o más claves.

Jorge Ramió Aguirre. Universidad Politécnica de Madrid.

Criptología

Criptoanálisis: arte de descifrar.

Criptología = Cifrado + Criptoanálisis.



Tanenbaum. “Redes de Computadoras”. 3ª edición, pp. 581.

No todo es lo que parece…

¿Cuántos estudiantes se necesitan en un grupo antes de que la probabilidad de tener dos personas con el mismo cumpleaños exceda ½?

Cant. parejas = $\frac{n(n-1)}{2}$

Para n=20 → Cant. parejas = 190, P= $190*\frac{1}{365}>0.5$

Aspectos Legales

- En Francia, la criptografía no gubernamental es prohibida, a no ser que el gobierno tenga las claves empleadas.

- Phil Zimmermann, autor de PGP fue acusado de exportación de material de guerra.

Tanenbaum. “Redes de Computadoras”. 3ª edición, pp. 621.

Conclusiones

- Importancia de la seguridad en el ciclo de desarrollo del software.
- La seguridad está integrada en el modelo OSI del estándar ISO 7498.
- Los ataques de criptoanalistas pueden ser pasivos o activos.
- Las políticas de seguridad incluyen la definición de un plan de seguridad informática, códigos de ética y plan de contingencia.

Orientaciones de Trabajo Autónomo

- Caracterizar la situación de la seguridad informática y marco legal de esta en:
  - Tecnología ubicua.
  - Computación en la nube.
  - Redes sociales.
  - Sistemas de información.