XX SEMINARIO “DUQUE DE AHUMADA”
“SEGURIDAD Y NUEVAS TECNOLOGÍAS”
7 de Mayo de 2008

Seguridad en las Tecnologías de la Información

dsa-research.org

Ignacio Martín Llorente
Distributed Systems Architecture Research Group
Universidad Complutense de Madrid

Universidad Complutense Madrid

La Suma de Todos
Comunidad de Madrid
www.madrid.org

MINISTERIO DE EDUCACION Y CIENCIA

1. **Introducción a la Seguridad en Tecnologías de la Información**
   - ¿Qué es Seguridad de la Información?
   - Causas comunes de fallos
   - Resultado para la empresa
   - Terminología
2. **Visión Tecnológica**
   - Tipos de tecnologías
   - Inconvenientes
3. **Visión Estratégica**
   - Modelo de Gestión de Seguridad de la Información NO Dirigido por la Tecnología sino orientado a Procesos de Negocio
   - Herramienta de Toma de Decisiones sobre Seguridad de la Información

1.1. ¿Qué es Seguridad en Tecnologías de la Información?

Protección de información (**datos**) de daño intencionado o accidental

- Seguridad de acceso a sistema y ficheros
- Realización de copias de seguridad

Miscellaneous stats about computer data loss:

- 32% of data loss is caused by human error
- 31% of PC users have lost all of their PC files to events beyond their control
- 25% of lost data is due to the failure of a portable drive
- 44% of data loss caused by mechanical failures
- 15% or more of laptops are stolen or suffer hard drive failures
- 1 in 5 computers suffer a fatal hard drive crash during their lifetime
- The overall average failure rate of disk and tape drives is 100% - all drives eventually fail

1.1. ¿Qué es Seguridad en Tecnologías de la Información?

Protección de servicio de daño intencionado o accidental

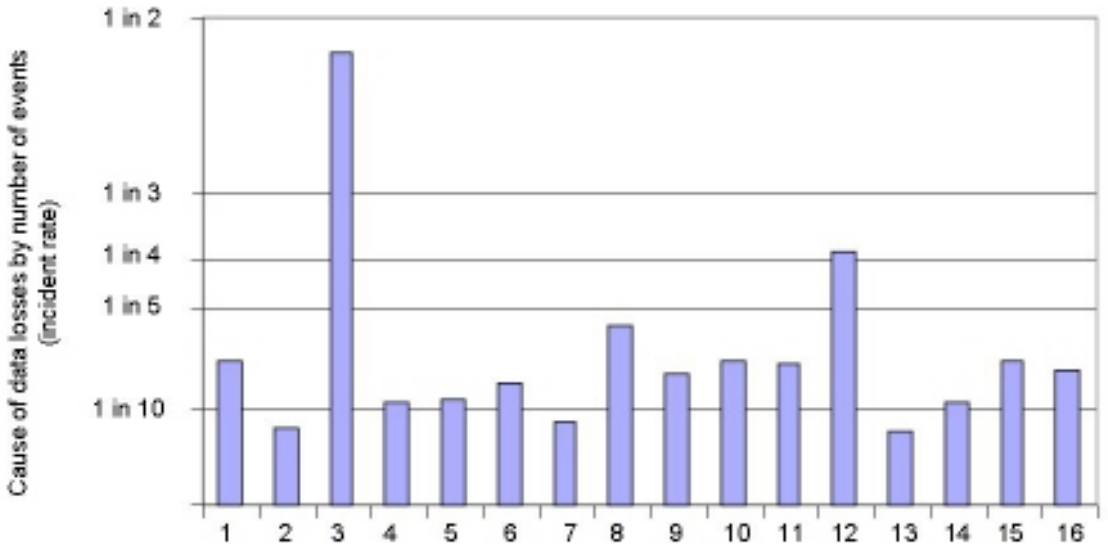
- Cualquier desviación del comportamiento esperado para un sistema se puede considerar como un fallo de seguridad

2001 Cost of Downtime Survey:

- 46% said each hour of downtime would cost their companies up to $50k
- 28% said each hour would cost between $51K and $250K
- 18% said each hour would cost between $251K and $1 million
- 8% said it would cost their companies more than $1 million per hourmillion per

1.2. Causas Comunes de los Fallos de Seguridad

> *"In one form or another, **human error is the overwhelming cause of sensitive data loss**, responsible for 75 percent of all occurrences. User error is directly responsible for one in every two cases (50 percent) while violations of policy - intended, accidental and inadvertent - is responsible for one in every four cases (25 percent). Malicious activity in the form of Internet-based threats, attacks and hacks is responsible for one in every five occurrences."*



1: Lost or stolen laptops
2: Improperly disposed of computer equipment
3: User errors
4: Improperly transferred backup media
5: Inappropriate access to IT resources
6: Insufficient controls in business procedures
7: Insufficient controls on IT procedures
8: Internet threats, attacks and hacks
9: Employee manipulation and malfeasance
10: Accidental damage to computing equipment
11: Inappropriate usage of IT resources
12: Violation of policies
13: Unauthorized access to IT resources
14: Insufficient auditing, monitoring and reporting
15: IT vulnerabilities
16: Insufficient IT controls

N: 201

Source: ITPolicyCompliancecom, 2007

La mayor parte de los daños no son intencionados

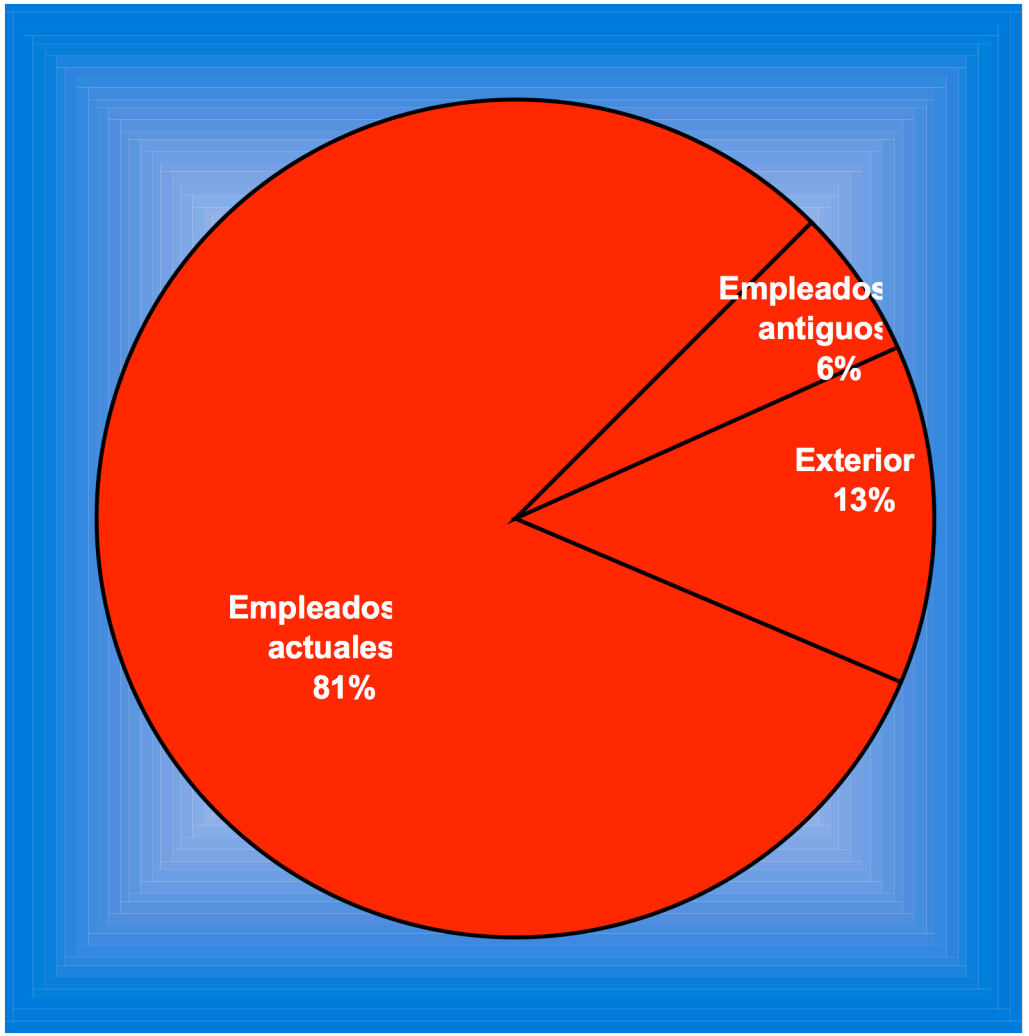
La componente crítica de la seguridad es el usuario

- Se debe invertir tiempo y dinero en formación adecuada para los usuarios y administradores
- Se deben desarrollar políticas y procedimientos que regulen el uso de los sistemas

EU Report:

- Hardware malfunction accounts for 44 percent of all data loss
- Human Error accounts for 32 percent of all data loss
- Software Corruption Accounts for 14 percent of all data loss
- Computer Viruses Account for 7 percent of all data loss
- Natural Disasters Account for 3 percent of all data loss

1.2. Causas Comunes de los Fallos de Seguridad



Data Processing Management Association, 1992

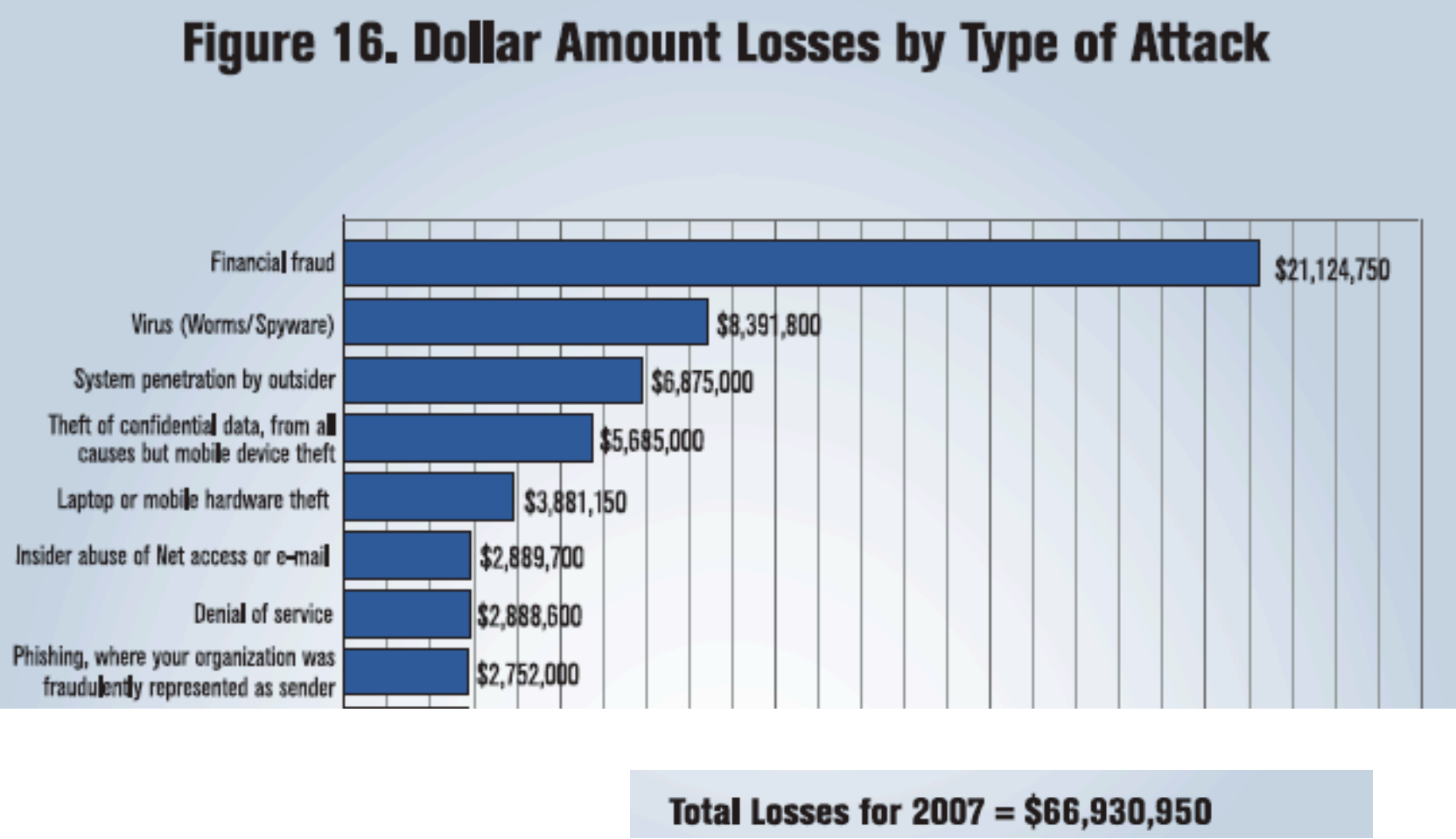
La mayor parte de los daños son causados por empleados descontentos

No debemos olvidarnos de la seguridad interna

- La mayoría de las empresas solo se preocupan de la seguridad del perímetro

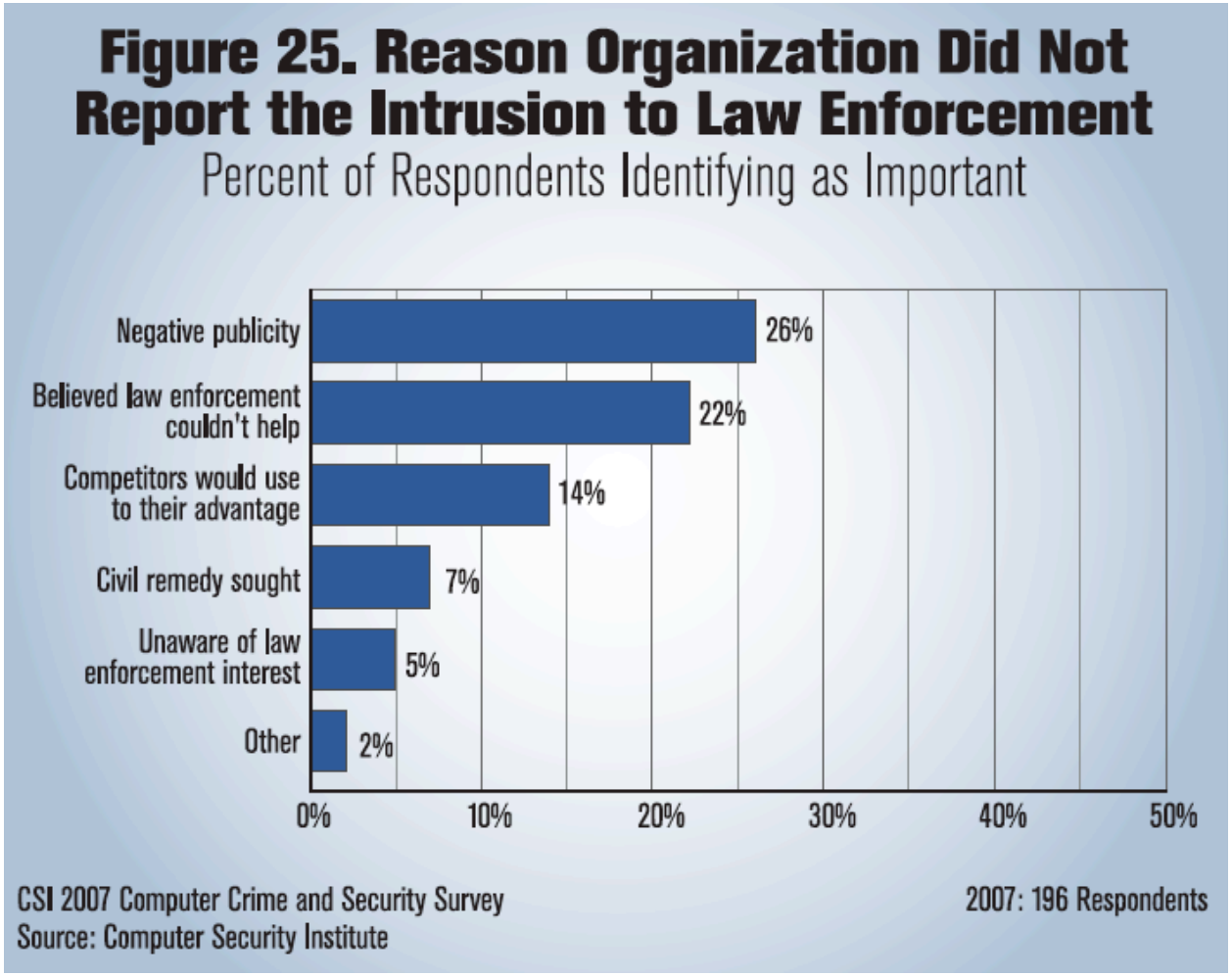
1.3. ¿Cuál es el Resultado para la Empresa?

- Pérdida económica



1.3. ¿Cuál es el Resultado para la Empresa?

- Pérdida de confianza de los clientes
- Pérdida del valor fundamental => **cierre**
- ...



Autenticación

- Habilidad para demostrar:
  - Algo que conozco: Una contraseña, un pin o una frase clave
  - Algo que tengo: Una tarjeta de códigos
  - Algo sobre mi: huella dactilar o escáner de retina
- La respuesta a la pregunta, *¿cómo me aseguro de que eres quien dices ser?* forma parte de la política de seguridad.

Autorización

- La autorización se consigue por medio de control de acceso y confidencialidad que proporciona:
  - Concesión o denegación de permisos de acceso a datos
  - Restricciones en el acceso a los datos
  - Control de quién tiene acceso a qué y cuando
  - Una seguridad de que los secretos permanecen no relevados

1.4. Terminología

Contabilidad

¿Cómo contabilizo las acciones realizadas por los usuarios autorizados?

- Registro de acceso y uso de un recurso

Disponibilidad

¿Cómo me aseguro que los servicios mínimos están siempre operativos?

- Una buena política debería asegurar disponibilidad de **sistema y servicio** incluyendo:
  - Control de aire acondicionado e inundaciones
  - Acceso físico de seguridad a cables de red y equipos

Confidencialidad

¿Cómo puedo asegurarme de que nadie puede leer mis datos?

- Encriptación

Integridad

¿Cómo puedo asegurarme de que nadie haya modificado mis datos?
(mails)

- Resúmenes de mensaje (*message digest*)
  - Un mensaje largo se representa por su resumen de 126 bits que se firma con la clave secreta del emisor dando lugar a la firma digital.

- También se utiliza para descubrir suplantaciones de software (MD5 en sunsolve o PGP en otros sitios de distribución software)

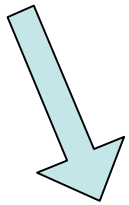
No Repudio

¿Cómo puedo asegurarme de que nadie niegue su participación previa?

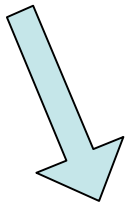
- Debe garantizarse que ninguno de las personas involucradas en la transacción puedan negar posteriormente el hecho de haber participado en la misma

2.1. Tipos de Problemas de Seguridad

- Catástrofe natural
- Ataque físico accediendo al sistema o a la red
- **Ataque informático**



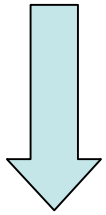
- Fallo no intencionado
- Fallo intencionado por usuario interno
- **Fallo intencionado por intruso**



- Los *hacker* tienen mucha información (internet) pero afortunadamente el 90% carece de conocimiento informáticos
- Suelen seguir siempre las mismas pautas
- Los intrusos no suelen ser expertos y suelen buscar las vulnerabilidades más evidentes (**Top20 Security Risks**)

Protección del exterior

- Evitar que el intruso se haga con una cuenta normal



Protección interior

- Evitar que un usuario se haga con la cuenta de supervisor o que acceda a información confidencial

Daños que puede causar un usuario normal

- Denegación de servicio
  - Monitorización y gestión de los recursos del sistema
- Leer/modificar/destruir información crítica o confidencial
  - Permisos básicos y avanzados ACL
  - Herramientas de auditoria de sistemas de ficheros: *ASET*, *COPS*, *Tiger* y *TripWire*
- Abrir una sesión de root por medio de inclusión de troyanos, ejecución de *Crackers* o *exploits* (*buffer overflow* de órdenes SUID)
  - Monitorización y búsquedas en el sistema de ficheros
  - Ejecución de *Crackers*
  - Instalación de parches

Daños que puede causar como superusuario

- Destruir el sistema
  - Superusuarios reducidos
  - Copias de seguridad
- Incluir trampas en el sistema
  - Conocimiento perfecto del sistema y análisis de fallos
- Utilizar herramientas tipo *sniffer*
  - Transmisión encriptada de la información por medio de VPN: *SKIP*, ...
  - Uso de shells seguros: *ssh*, *openssh*, ...
  - NFS seguro
- Ataque a puertos TCP de otro sistema
- Acceder a información confidencial
  - Criptografía

El objetivo es hacerse con una cuenta

- Ataques por la red por medio de sniffers
  - Herramientas para realizar el ataque: *snoop*, *solsniff*, *sniffit*, *ethereal*, ...
  - Herramientas para defenderse: *SKIP*, *ssh, cpm, PGP, MD5, ...*

- Ataque a los puertos TCP para averiguar UNIX y servicios => exploit
  - Herramientas para realizar el ataque: *SATAN*, *SAINT*, *ISS*, *tcpdump*, ...
  - Herramientas para defenderse:
    - Eliminar servicios no necesarios
    - Instalar últimos parches
    - Estudiar servicios más vulnerables
    - Contraseñas robustas a ataques de *Crackers*
    - Herramientas de control de red como *TCP_Wrapper, firewalls*, ...
    - Herramientas de detección de ataques: *Syn*, *Klaxon*, *Courtney*, *Tocsin*, *Gabriel*, *logcheck, logsurf, scanlogd, syn,* ...
    - Mecanismos de autenticación: *DES* y *Kerberos*

- Denegación de servicio por red

2.5. Seguridad Física

A pesar de que nos centraremos en seguridad del sistema no debemos descuidar la seguridad física:

- **Acceso a la red para monitorizar la información o interrumpir su funcionamiento**
  - Cables

    Permite anular el funcionamiento del sistema
  - Dispositivos físicos

    Routers, gateways, hubs, impresoras de red avanzadas, ... permiten conexión por la red para su configuración donde los superusurios podrían desvelar su contraseña
- **Entorno del sistema**
  - Debe estar cerrado (se podría apagar la máquina, arrancar con CDROM, ...)

2.6. Inconvenientes de la Seguridad

- **Costoso en tiempo y dinero**
  - El análisis de riesgos evaluará que este coste es menor que el consumido en caso de ataque

- **Disminuye la eficiencia global de los sistemas**
  - Mecanismos de autenticación, encriptación, procedimientos para los usuarios, ...

- **Consume recursos**
  - Disco, procesador, ancho de banda en red, ...

dsa-research.org

Bagle.B, tercer virus más virulento de la historia, según expertos

Un hacker controló la página web del Banco Central

El peligro del us[illegible]As

DESORIENTACIÓN

La s[illegible]ción a sus problemas de seguridad

Gestión integrada de riesgos

Confusión del ejecutivo

- Nuevos ataques
- Nuevas tecnologías de seguridad

La seguridad no es un problema tecnológico

- La seguridad es una cuestión estratégica, no es cuestión de resolver los problemas de seguridad actuales de forma defensiva o reactiva
- Aunque renovemos continuamente las tecnologías con presupuestos millonarios, sin un planteamiento estratégico siempre iremos detrás de los nuevos ataques

Lo importante es la seguridad de la información y de los procesos de negocio

- Es un error pensar en seguridad de los computadores o la red

La Seguridad Aumenta cuando Disminuimos el Riesgo

- No existe la seguridad absoluta
- El nivel óptimo de seguridad es un compromiso
- Cada empresa tiene un grado de seguridad óptimo

Importancia de la Seguridad de la Información

- Garantiza el correcto funcionamiento de la actividad empresarial
- Es una obligación legal (normativas LOPD y LSSI)
- Puede actuar de factor diferenciador (certificación ISO/IEC 17799:2000)
- Protege ante posibles fallos humanos
- Evita que usuarios internos puedan atacar sistemas externos (con la responsabilidad legal que ello conlleva)
- Previene la entrada de intrusos en los sistemas
- Impide que usuarios descontentos puedan causar daños importantes que lleguen a alterar o incluso a detener las actividades de la empresa

La Seguridad Puede Llegar a Transformar el Sector

La Seguridad Puede Proporcionar Nuevas Oportunidades de Negocio

3.3. ¿Para Qué Empresas es Importante la Seguridad?

Negocios que se Basen su Ventaja Competitiva en:

- Manejo seguro y fiable de información
- Compartición segura y fiable de información (alianzas)

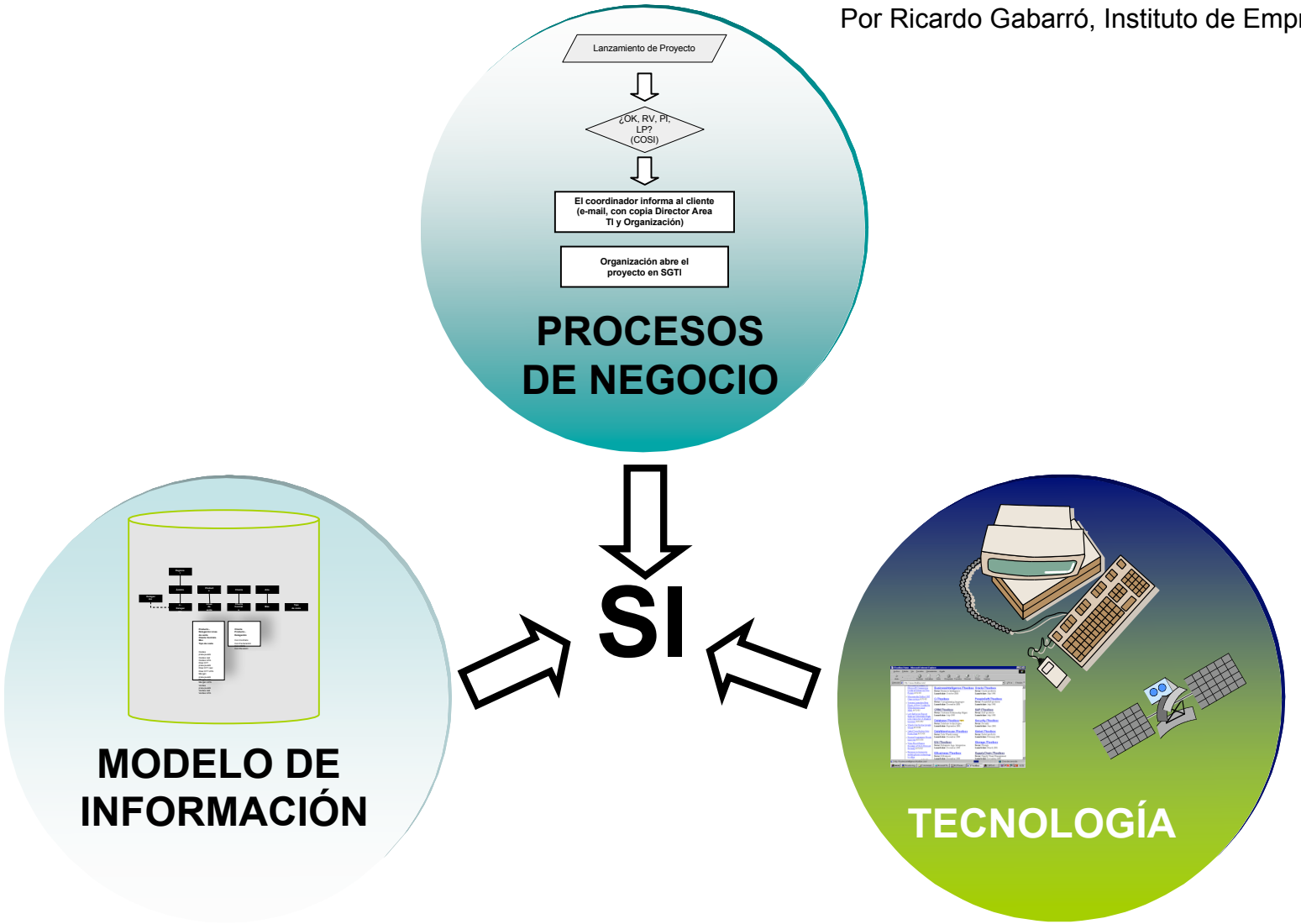
Donde Información Significa:

- Diseños
- Datos de clientes
- Patentes
- Contratos
- Cuentas bancarias
- …

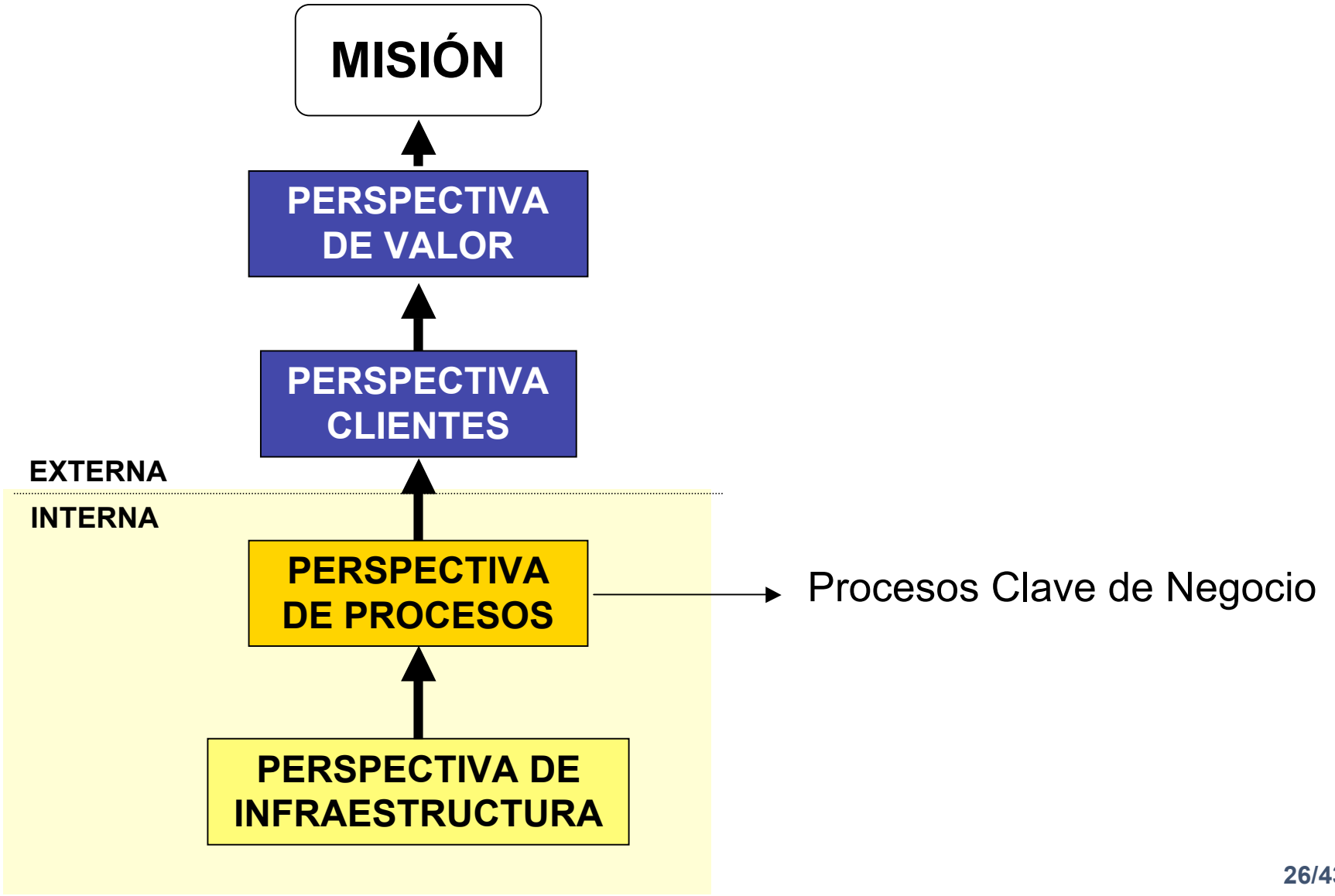
No Necesariamente Empresas de Internet

3.4. Sistemas de Información

Por Ricardo Gabarró, Instituto de Empresa, 2003



Procesos Asociados a los Activos de Información en CMI



Aspectos a Recordar

- El proceso de seguridad no protege computadores sino **información** y **procesos de negocio**
- La implantación de tecnologías de seguridad debe ser un modo de implantar unas políticas de seguridad

Diseño de un Modelo de Seguridad Orientado a Procesos

1. Identificar **Parámetros de Seguridad** para los procesos de negocio y activos de información
2. Desarrollar el **Diseño del Sistema de Seguridad** de acuerdo a los parámetros de seguridad y según las limitaciones existentes y desarrollar las **Políticas y Procedimientos de Seguridad**
3. Implantar la **Tecnología** que fuerce el cumplimiento del Diseño y las Políticas y Procedimientos y un posterior **Análisis de Riesgos**
   - Identificar **Amenazas y Vulnerabilidades**
   - Implantar **Tecnología**

¿Qué Pretendemos Defender y Cuál es su Prioridad?

- Origen del diseño del sistema de seguridad

Tipos de Activos de Información

- Documentos electrónicos con contratos, patentes, fórmulas…
- Bases de datos de clientes, competidores…
- Códigos fuente y ejecutables propietarios, con licencia…

Esta Información Puede ser Propia o de Otras Empresas

Definición de la Granularidad

- **Autorización**:
  - ¿Hay usuarios con permiso para manipular una parte que no pueda manipular otra? => dividir
  - ¿Hay usuarios con permiso para manipular un activo que tienen permiso para manipular otro => Fusionar

Tiene Siempre Asignado un Proceso o Conjunto de Procesos

- En ocasiones son diferentes aplicaciones las que gestionan diferentes procesos

Tabla de Activos

Nombre	Nombre que identifica al activo
Valor	Valor cualitativo del activo • De 1 a 5 en función de la pérdida para la compañía que supondría perderlo o un competidor accediera o modificara el activo considerando pérdida económica puntual y potencial por pérdida de oportunidad o prestigio
Procesos	Referencia a descripción de procesos asociados
Agentes	Personas, grupos, empresas, equipos implicados…
Propietario	Departamento propietario responsable

Los 5 Parámetros de Seguridad

- **Confidencialidad**: Mantener secreta la información sensible
- **Identificación y autenticación**: Verificar la identidad de los agentes implicados (personas, empresas o equipos)
- **Autorización:** Privilegios de cada agente (personas, empresas o equipos)
- **Auditoria** (contabilidad): Registro de acciones de los agentes
- **Integridad**: Seguridad de que la información es veraz

3.8. Parámetros de Seguridad: Confidencialidad

Secreto en el Almacenamiento y Transferencia de la Información

- Cuentas de clientes
- Tarjetas de crédito de clientes
- Negociaciones de contratos

Situaciones Frecuentes

- Acceso del superusuario
- Robo de portátiles
- Sniffers en la red
- Último mecanismo de defensa ante ataques

Tecnología

- Encriptación simétrica y asimétrica, sus vulnerabilidades son la mala gestión de las claves, el uso de algoritmos de encriptación poco robustos y programas mal desarrollados

Tabla de Activos

Confidencialidad	¿Se debe mantener encriptada la información?

3.8. Parámetros de Seguridad: Identificación y Autenticación

¿Cómo Indico Quien Soy y lo Demuestro?

- Algo semejante al DNI pero en formato electrónico
- La base de la autorización y la contabilidad
- Extensible a equipos o servicios (web)

Debemos Distinguir entre la Creación de la Identidad y su Autenticación

- ¿Cuál el nivel de verificación de la identidad de una persona?
- ¿Cómo esta persona podrá demostrar que es quién dice ser?

Tecnologías

- **Algo que conocemos**: Usuario y contraseñas o PINs => Importancia de la selección robusta para evitar *cracking*
- **Algo que tenemos**: Certificados digital y clave privada en smartcard (doble nivel ya que necesito la tarjeta y además la contraseña) con entidad de certificación, tarjetas de contraseñas de una sola vez
- **Algo que somos**: Usuario y retina o huella dactilar

Tabla de Activos

Autenticación	Nivel de identificación y autenticación deseable

3.8. Parámetros de Seguridad: Autorización

Una Vez Identificado Qué Acciones Puedo Realizar

- Quién debe tener acceso a la información
- Que tipo de acceso a información de cada agente en el proceso

Problemas Potenciales

- Trabajador que acceda/manipule información sin permiso
- Atacante que entra en el sistema

Tipos de Políticas de Acceso

- Según funciones (departamentos)
- Basado en roles con definición de roles y asignación de roles a usuarios

Tecnologías

- Permisos de ficheros y directorio
- Conexiones de red por medio de hosts de confianza
- Control de acceso a sistemas NFS

Tabla de Activos

Autorización	Privilegios de acceso de cada agente

3.8. Parámetros de Seguridad: Contabilidad

Registrar las Acciones de los Agentes

- Es importante llevar la cuenta de las acciones de los usuarios
- Asegurarse que los usuarios no exceden sus privilegios

Requisitos

- Identificación única de los usuarios
- Capacidad de auditar los eventos
- Un modo de proteger los registros individuales y el global

Tecnologías

- Usuarios
- *Logging* de aplicaciones
- Contabilidad de procesos
- *Basic Security Module*

Tabla de Activos

Contabilidad	Nivel de contabilidad requerido

3.8. Parámetros de Seguridad: Integridad

Conocer Qué es Real en el Mundo Digital

- E-mails
- Documentos
- Software
- Contratos

Es Fundamental Conocer en Qué Información Puedo Confiar

- Quién envío la información
- La información recibida es exactamente la misma que la enviada

Tecnologías

- Firmas digitales basada en MD5

Tabla de Activos

Integridad	Nivel de integridad requerido

3.8. Parámetros de Seguridad: Disponibilidad

Incluye los siguientes factores

- Ventana horaria
- Importancia y frecuencia de las copias de seguridad
- Importancia de la alta disponibilidad

Tecnologías

- Limitación de franjas horarias
- Alta disponibilidad
- Recuperación por medio de copias de seguridad

Tabla de Activos

Disponibilidad	Nivel de disponibilidad

3.8. Diseño, Políticas y Procedimientos

Limitaciones

- **Presupuesto**
- **Tecnología** actual (aplicaciones)
- **Productividad** en el trabajo

Debemos Describir el Diseño Final y Práctico de la Solución

- Junto con el Responsable de Sistemas de Información

Políticas y Procedimientos

- Quedan por escrito las decisiones

Tabla de Activos

Políticas y Procedimientos	Referencia a documento de diseño

3.8. Tecnologías

Tecnologías para la Implantación del Diseño

- Además, debe resolver otras **vulnerabilidades** por medio de un análisis de riesgos e implantar las **medidas de detección de intrusos necesarias**

Tabla de Activos

Tecnologías	Tecnologías de implantación

Nos Quedan por Resolver Riesgos

- Ataque físico
- Accidentes y catástrofes naturales
- Atacantes del interior y exterior aprovechando
  - Diseño demasiado simplificado
  - Fallo en la implantación del sistema de seguridad
  - Vulnerabilidad de algún servicio
  - Fallos de algún servicio

Tabla de Riesgos

Nombre	Nombre que identifica al activo
Valor	Valor cualitativo del activo (1 a 5)
Propietario	Departamento propietario
Amenaza	Pongámonos en el peor de los casos
Nivel de la Amenaza	Desde 1 (irrelevante) a 5 (destrucción total)
Vulnerabilidades	Modos de que tenga lugar la amenaza
Probabilidad de la Vulnerabilidad	Desde 1 (baja) a 5 (alta)
Controles	Referencia a cláusula de políticas y procedimientos que se aplican para reducir la amenaza o la vulnerabilidad o el valor del activo

Un **Riesgo** es la combinación de una **Amenaza** aprovechando alguna **Vulnerabilidad** que pueda dañar algún activo

Concienciar a los Gestores

- Motivación orientada al coste de perder la información que manejan, a cumplir las regulaciones del gobierno
- **La Seguridad es una Decisión de Negocio**, no una cuestión tecnológica

Consejos Generales

- Los empleados son nuestros aliados
- La formación es más importante que la tecnología
- No es responsabilidad únicamente del Departamento de Sistemas de Información

Equipo de Trabajo

- Experto de seguridad externo que aporte un punto de vista imparcial
  - Analiza la información y propone alternativas
- Responsable del programa
  - Desarrollo y seguimiento de tareas y presupuestos, enlace formal…
- Administrador
  - Recoger información de activos e implantación de las medidas, ayudado de un equipo de soporte

Comisión de Seguridad

- Ejecutivo sponsor
- Responsable de estrategia
- Gestores de negocio

Planificación

- Pasos Preliminares
- Recogida y Análisis de Información
- Implantación del Sistema de Seguridad
- Proceso Continuo de Seguridad

1. **Introducción a la Seguridad en Tecnologías de la Información**
   - ¿Qué es Seguridad de la Información?
   - Causas comunes de fallos
   - Resultado para la empresa
   - Terminología
2. **Visión Tecnológica**
   - Tipos de tecnologías
   - Inconvenientes
3. **Visión Estratégica**
   - Modelo de Gestión de Seguridad de la Información NO Dirigido por la Tecnología sino orientado a Procesos de Negocio
   - Herramienta de Toma de Decisiones sobre Seguridad de la Información