SIEMENS

Soluciones de Seguridad para la Universidad

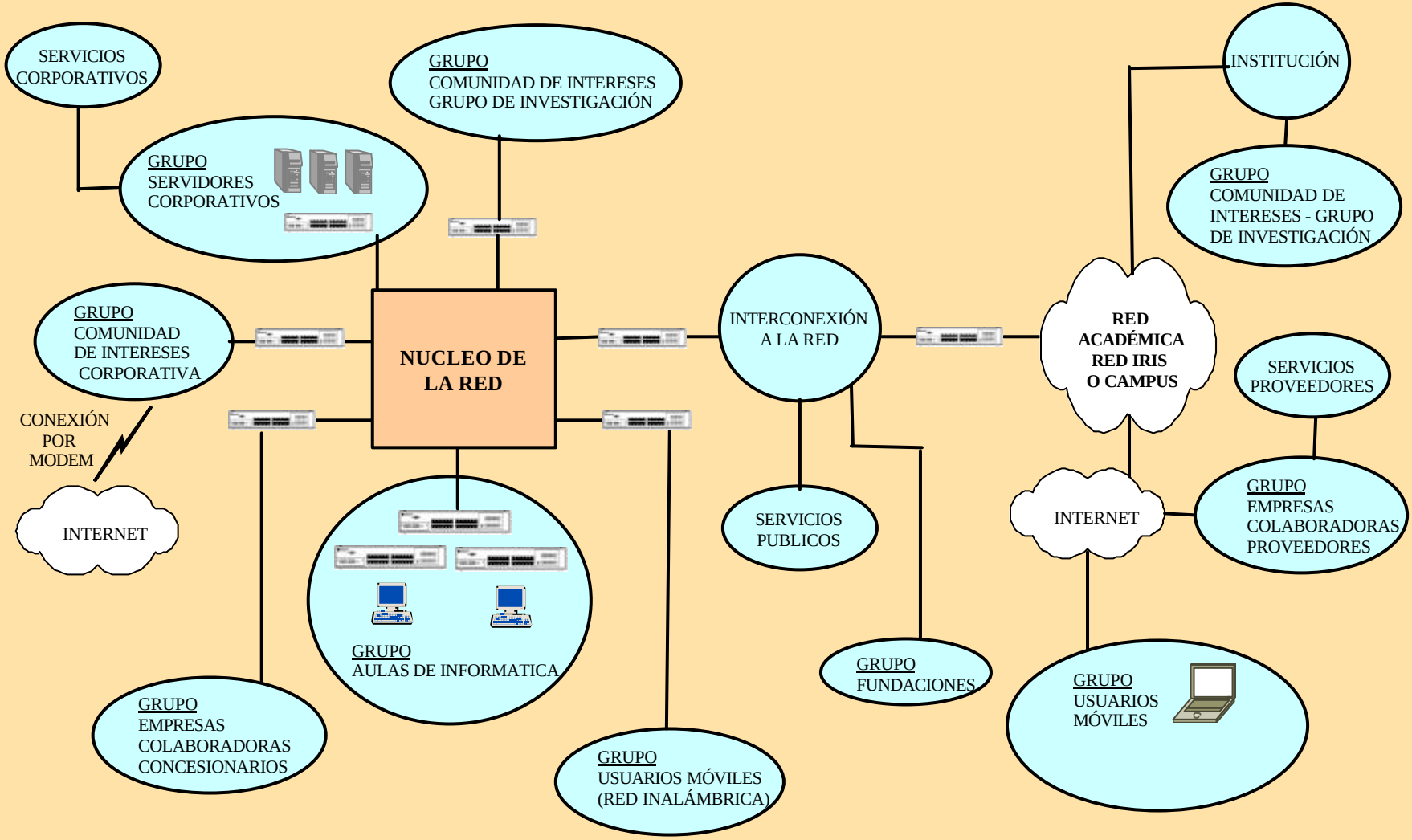
Carolina de Oro
carolina.oro@siemens.com

Siemens Information and Communication Networks
Trusted Networks Applications
www.siemens.es/seguridad

Situación de partida

SIEMENS

http://www.siemens.es/seguridad



Agenda

SIEMENS

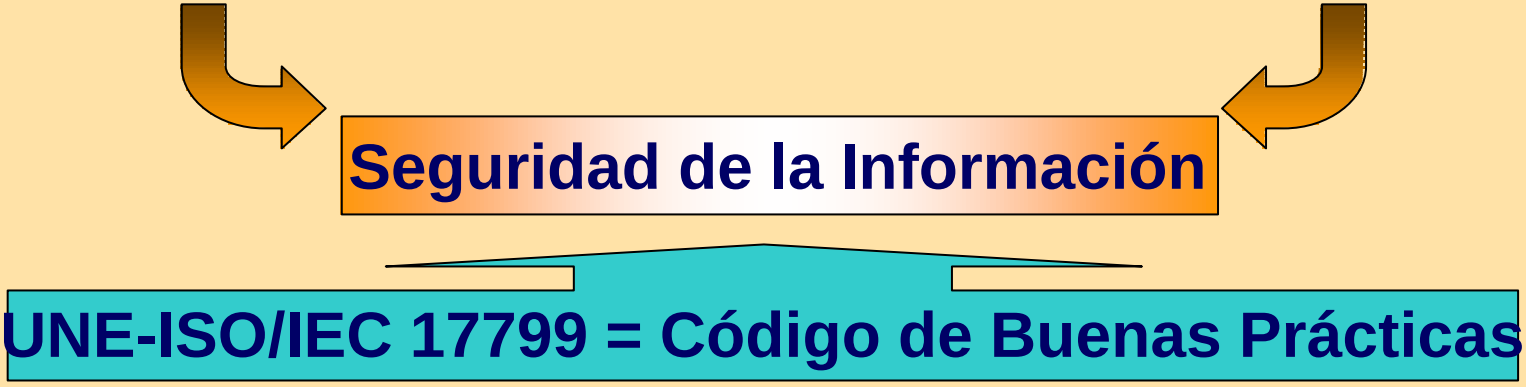
- Introducción
- Requerimientos generales:
  - Núcleo
  - Servicios
- Requerimientos de usuario:
  - Colaboradores
  - Investigadores
  - Alumnos
  - Moviles
  - Inalámbricos
- Requerimientos de adminstrador
  - Gestión de la seguridad

Seguridad de la Información

SIEMENS

- Declaración de principios:

  "La información es un activo que, como otros activos importantes del negocio, tiene valor para la Organización y requiere en consecuencia una protección adecuada."



¿Por qué la seguridad de la información es necesaria?

Requisitos de Seguridad

SIEMENS

Política de Seguridad

SIEMENS

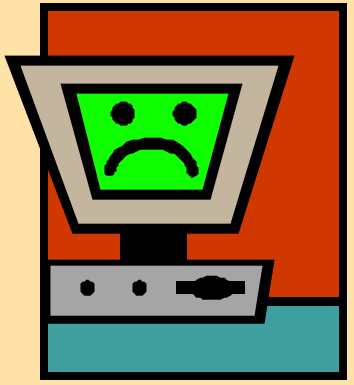
http://www.siemens.es/seguridad

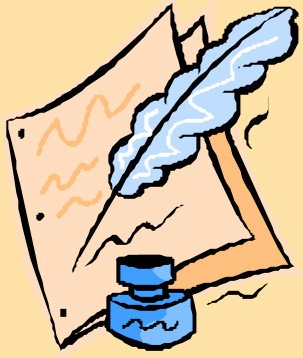
- Algunas premisas:
  - Una declaración del soporte de la dirección
  - Explicaciones breves sobre políticas, principios, practicas y cumplimiento de seguridad
  - Una definición general de las responsabilidades
  - debe ser revisado periódicamente

Análisis del Riesgo

SIEMENS

¿Conoce la universidad la importancia y valor de la información que maneja su organización?





Confidencialidad

Disponibilidad

Integridad

http://www.siemens.es/seguridad

Legalidad

SIEMENS

http://www.siemens.es/seguridad

UNE-ISO/IEC 17799 (12.1.1)

LSSICE
34/2002

Firma Electrónica
L 14/1999

Código Penal
L.O. 1.995

Leyes

Códigos

Directivas

LOPD
L.O.15/1999

PATENTES DE INVENCIÓN
Y MODELOS DE UTILIDAD.
Ley 11/1986

MARCAS
Ley 17/2001

Agenda

SIEMENS

- Introducción
- Requerimientos generales:
  - Servicios
  - Núcleo de Red
- Requerimientos de usuario:
  - Colaboradores
  - Investigadores
  - Alumnos
  - Móviles
  - Inalámbricos
- Requerimientos de adminstrador
  - Gestión de la seguridad

http://www.siemens.es/seguridad

Requisitos generales

SIEMENS

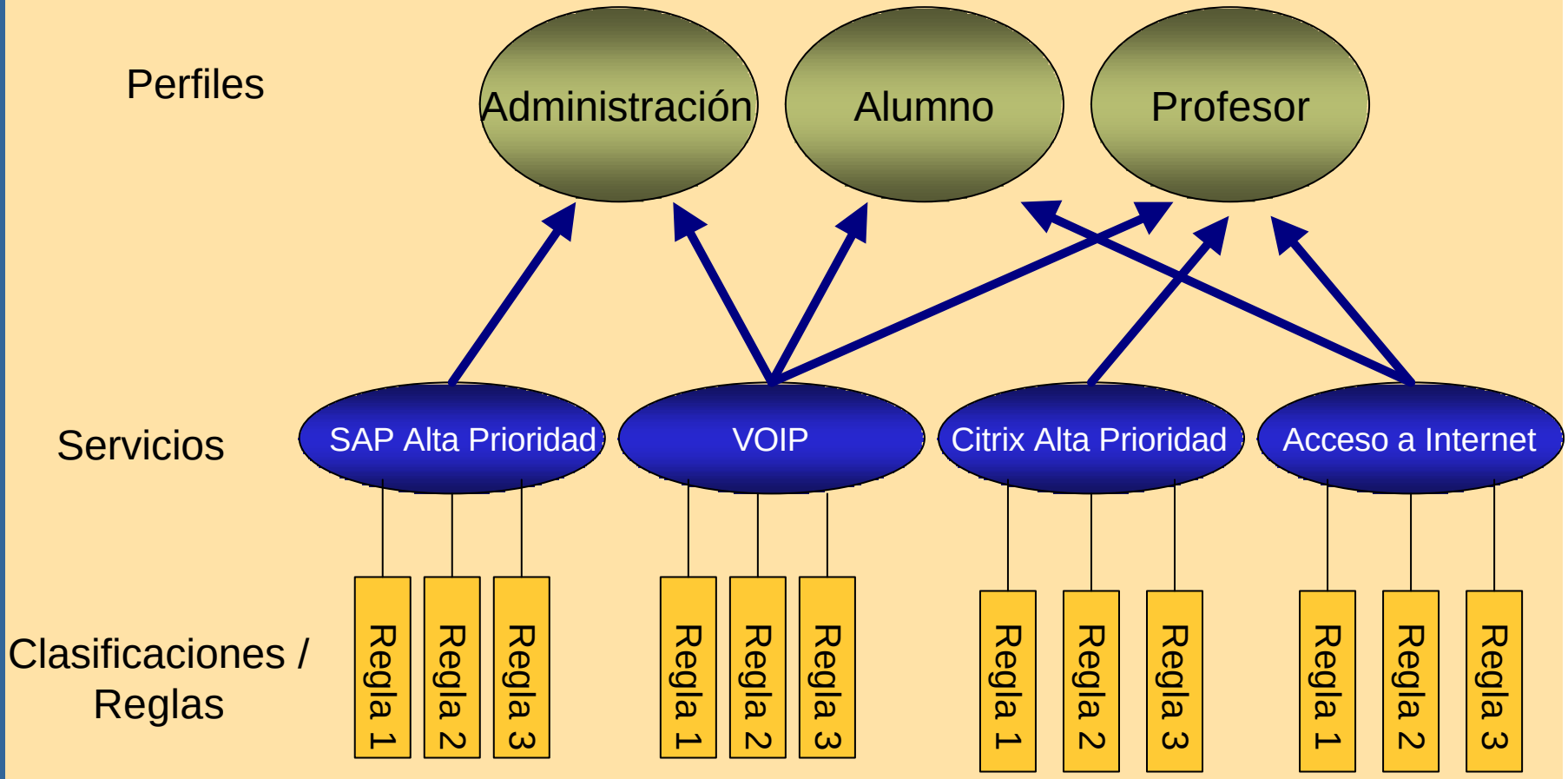
- Servicios:
  - VoIP
  - Grids
  - Multimedia
  - Videoconferencia IP

- Núcleo de red:
  - Altas capacidades a velocidad de cable
  - Asegurar calidad de servicio y seguridad:
    - distinguir usuarios y servicios
  - Capacidad de gestión y control
  - Alta disponibilidad de recursos de red

Escenario

SIEMENS

http://www.siemens.es/seguridad



Esquema de redes personalizadas

SIEMENS

http://www.siemens.es/seguridad

Login Web-based o EAP

802.1X

Decodificación de perfles y Aplicación de Clasificacíones

Adaptación entre perfiles y Directorios

NUCLEO DE LA RED

Autenticación Radius

Servidor RADIUS

Sistema de Directorios

Creación y distribución de Perfiles

La combinación de Autenticación, Servicios en el Punto de Entrada

Agenda

SIEMENS

- Introducción
- Requerimientos generales:
  - Servicios
  - Núcleo de Red
- Requerimientos de usuario:
  - Colaboradores
  - Investigadores
  - Alumnos
  - Móviles
  - Inalámbricos
- Requerimientos de adminstrador
  - Gestión de la seguridad

http://www.siemens.es/seguridad

Usuarios Corporativos

SIEMENS

http://www.siemens.es/seguridad

Principios Objetivos

- Facilidad de uso
- Libertad y apertura
- Procesos establecidos
- Utilización de modems

Análisis de riesgo

- Expedientes críticos

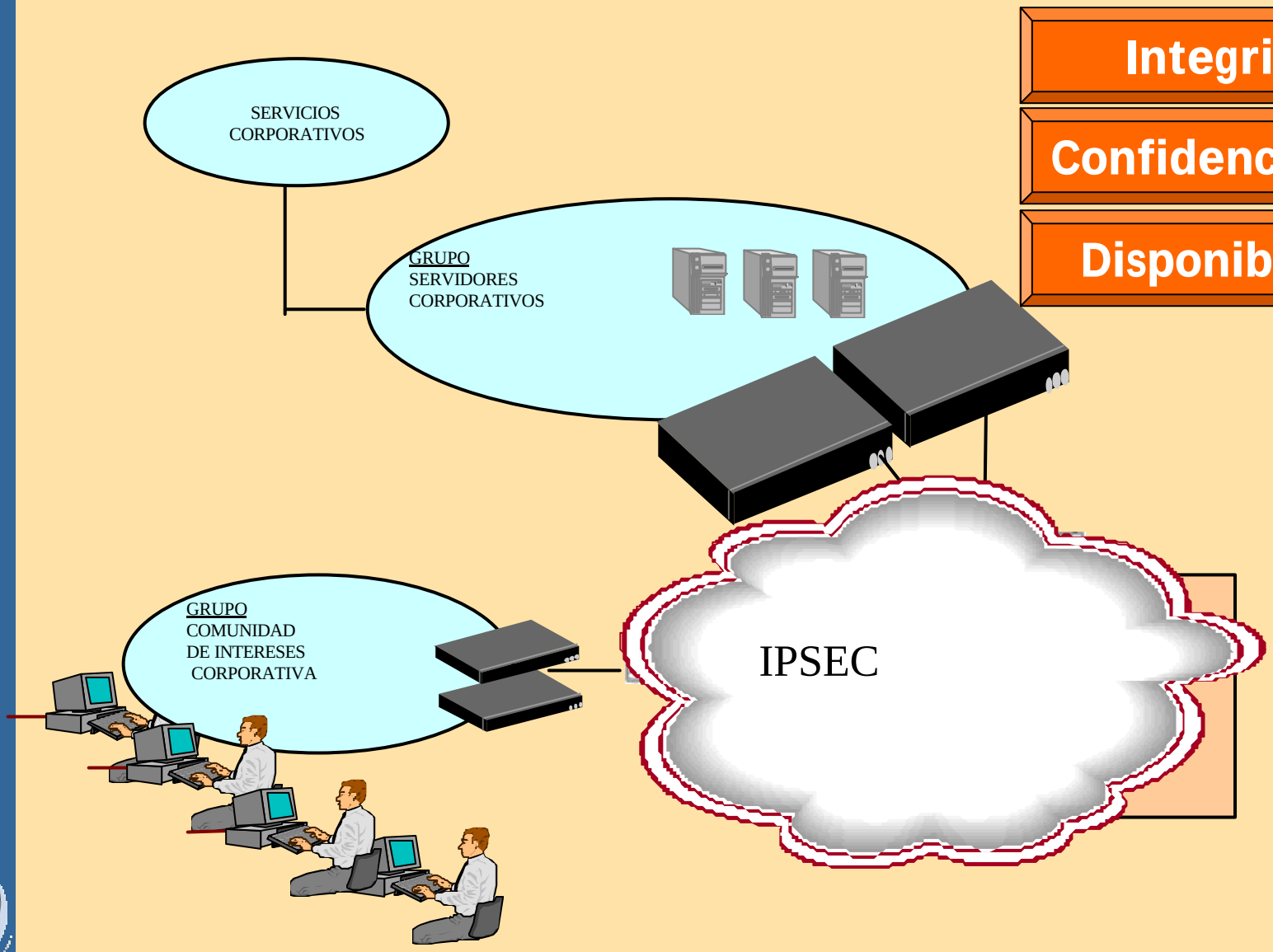
Contractual Legal

- LOPD nivel alto
- Cumplimiento de plazos

- **Confidencialidad**
- **Integridad**
- **Disponibilidad**
- **Identificación**

Corporativos: Cifrado

SIEMENS



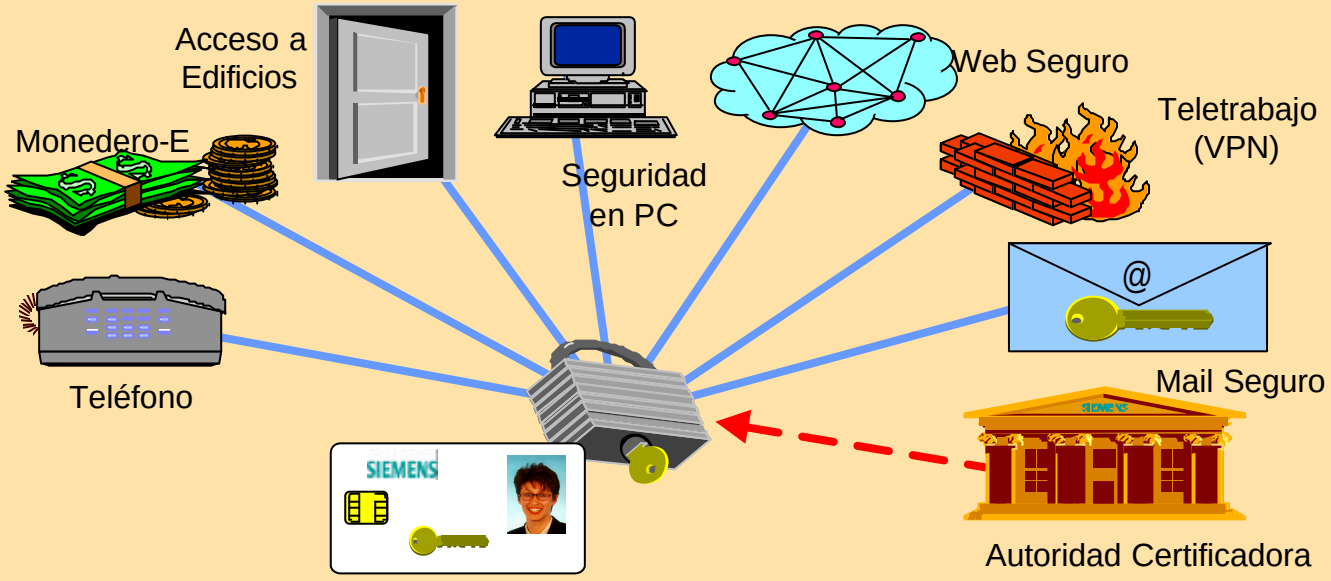
Integridad

Confidencialidad

Disponibilidad

Corporativos: Tarjeta multiaplicación

SIEMENS



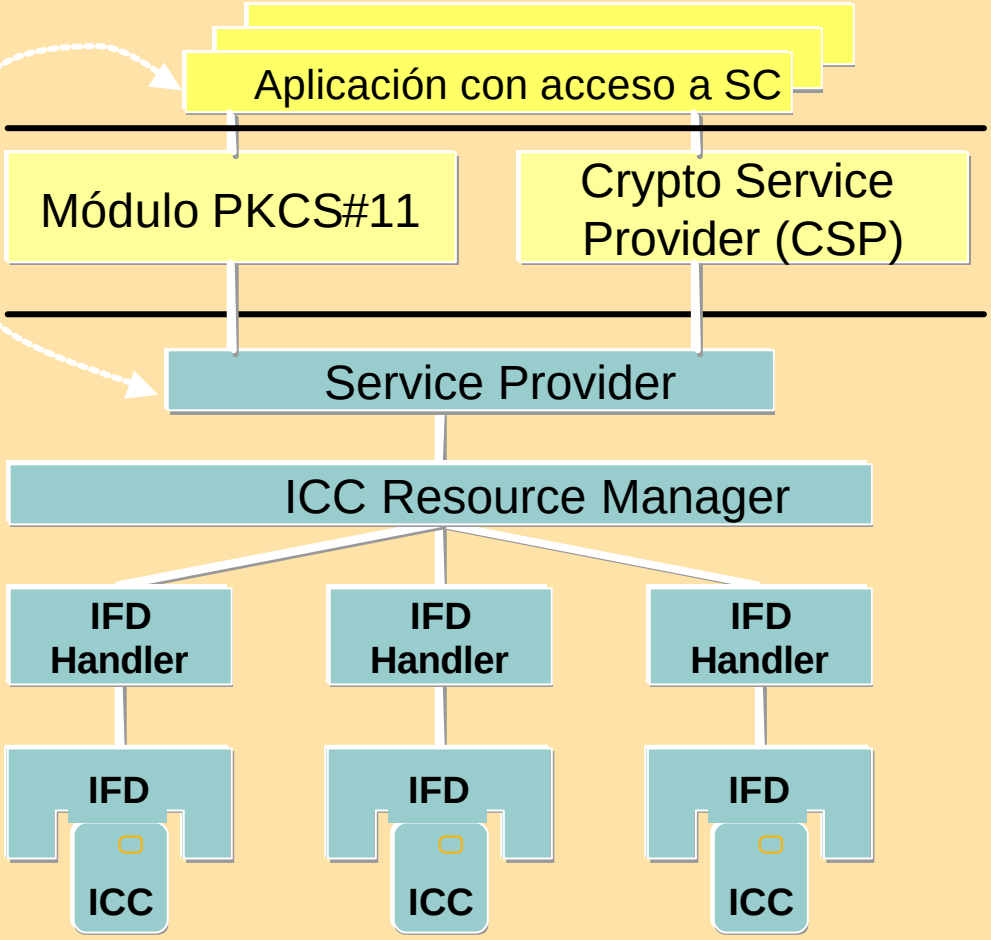
No repudio | **Identificación** | **Autorización**

Autenticación

http://www.siemens.es/seguridad

Corporativos: Tarjeta multiaplicación

SIEMENS



Crypto-interface a la aplicación

Opciones: PKCS#11 o CSP (Microsoft).Solo tarjetas con cripto-coprocesador.

Interface PC/SC

Provisto por el fabricante de la tarjeta/SO

Parte del sistema operativo (NT, UNIX, ...)

Provisto por el fabricante del lector

Lector Smart card (**I**nter**f**ace **D**evice)

Smart card (**I**ntegrated **C**ircuit **C**ard). Con Sistema Operativo específico

Corporativos: PKI y Firma Digital

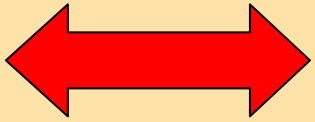
SIEMENS

Usuarios Corporativos: Modems

SIEMENS

Política de universidad: Anulación del uso de modems.

Excepción a esta regla será tratada como privilegios



Firewall personal

Gestión centralizada de firewalls personales

Grupos de investigación

SIEMENS

http://www.siemens.es/seguridad

Principios Objetivos

Facilidad de uso

Libertad y apertura

Necesidad colaboración total

Velocidad en el acceso

Usuarios menos controlados

Análisis de riesgo

Información tecnológica avanzada

Contractual Legal

LOPD nivel medio

Propiedad intelectual

Patentes de investigación

Confidencialidad

Integridad

Disponibilidad

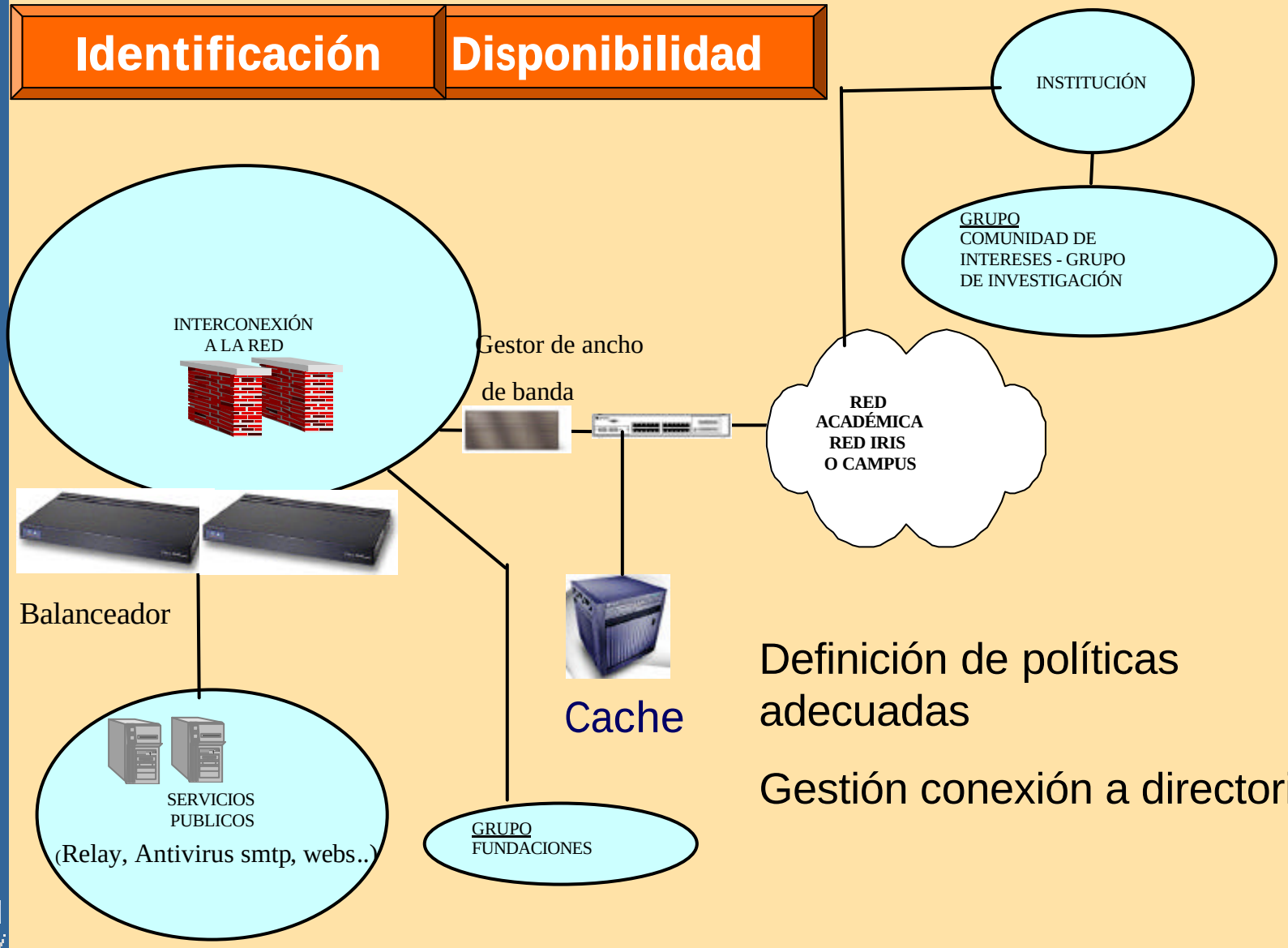
Identificación

Investigación: Firewall conexión red IRIS

SIEMENS

http://www.siemens.es/seguridad

Identificación | **Disponibilidad**



Definición de políticas adecuadas

Gestión conexión a directorio

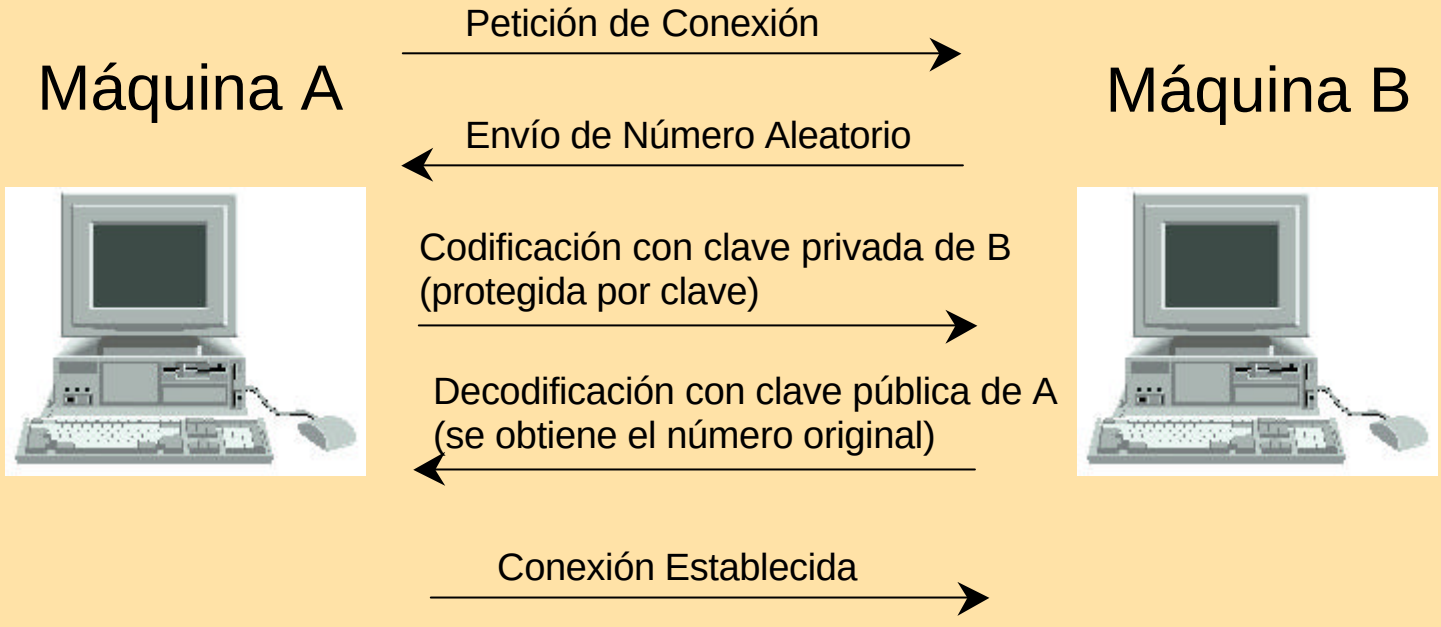
Investigadores: SSH

SIEMENS

Confidencialidad

SSH es un protocolo diseñado para establecer comunicaciones seguras en redes inseguras, sustituyendo a los métodos tradicionales de comunicación como telnet, rlogin, rsh,...

Está basado en un sistema de Claves Pública / Privada



Aulas de informática

SIEMENS

http://www.siemens.es/seguridad

Principios Objetivos

Libertad y apertura

Usuarios no controlados

Servicios docentes

Análisis de riesgo

Altas amenazas

Información menos sensible

Contractual Legal

LOPD nivel bajo

Confidencialidad

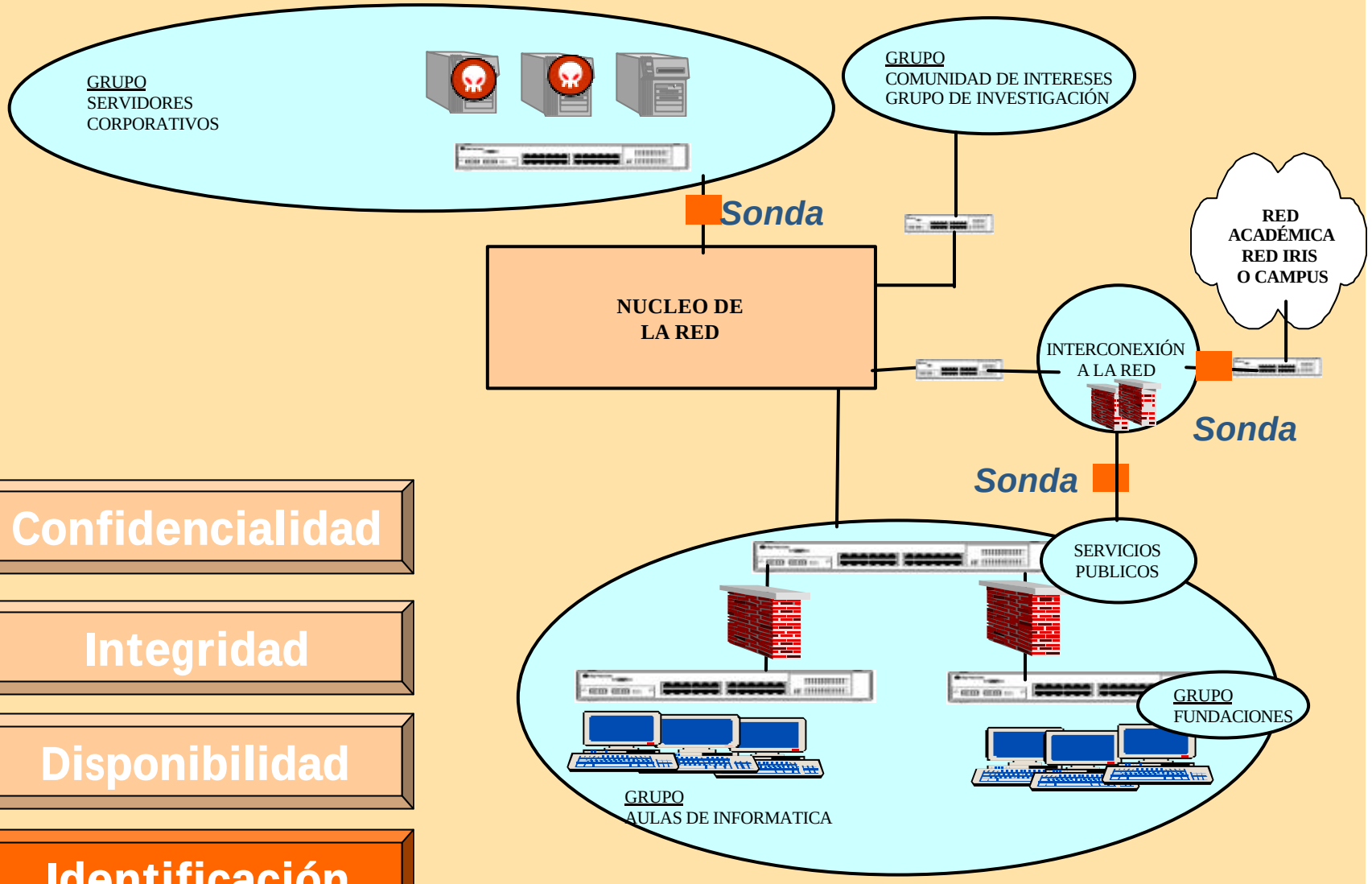
Integridad

Disponibilidad

Identificación

Aulas de informática: Firewalls,IDS

SIEMENS



- Confidencialidad
- Integridad
- Disponibilidad
- Identificación

http://www.siemens.es/seguridad

Usuarios móviles

SIEMENS

http://www.siemens.es/seguridad

Principios Objetivos

Todo tipo de usuarios con las características anteriores

Análisis de riesgo

Altas amenzas

Altas vulnerabilidades

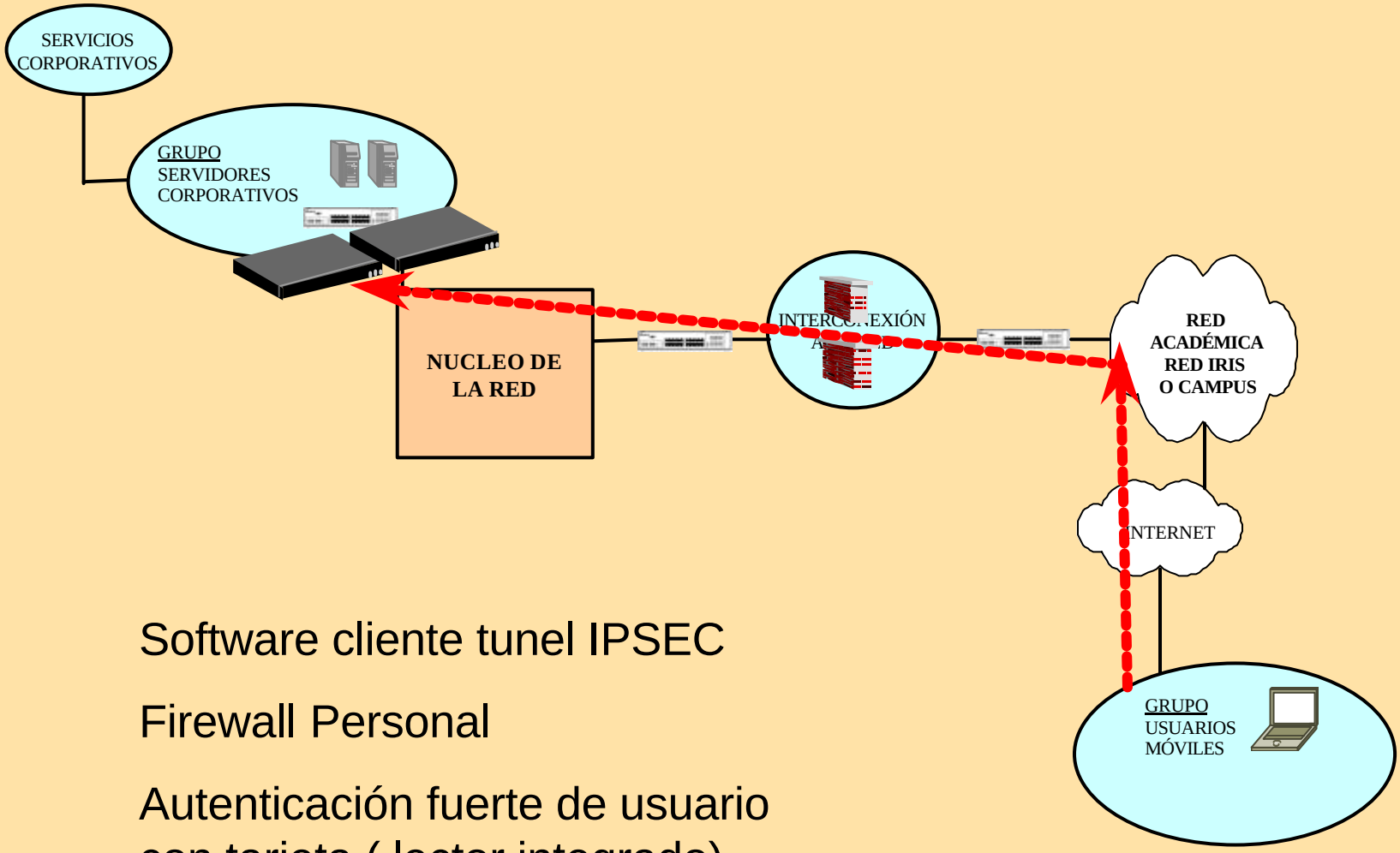
Contractual Legal

Todos los niveles de LOPD

- **Confidencialidad**
- **Integridad**
- **Disponibilidad**
- **Identificación**

Usuarios móviles - colaboradores

SIEMENS



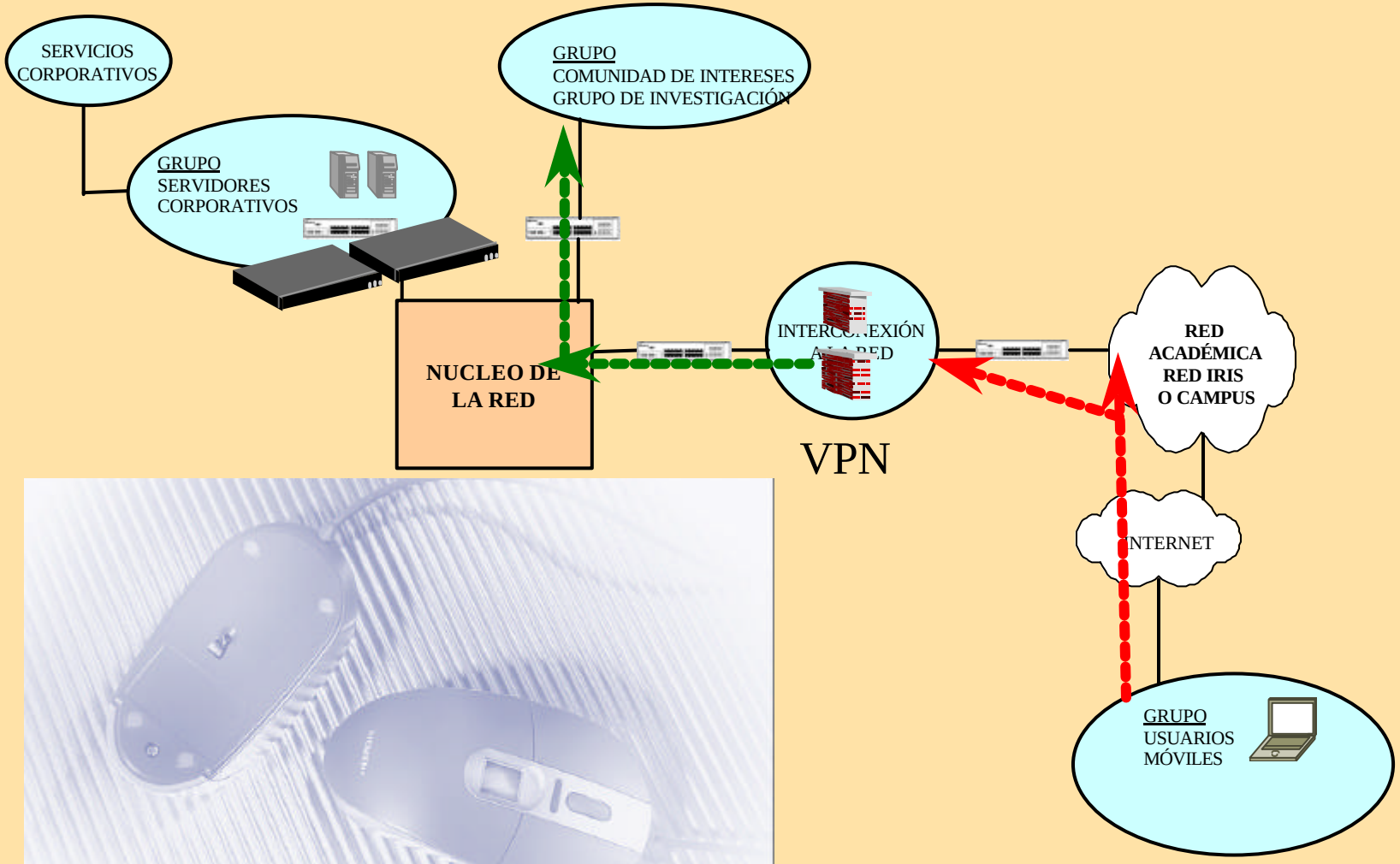
Software cliente tunel IPSEC

Firewall Personal

Autenticación fuerte de usuario con tarjeta (lector integrado)

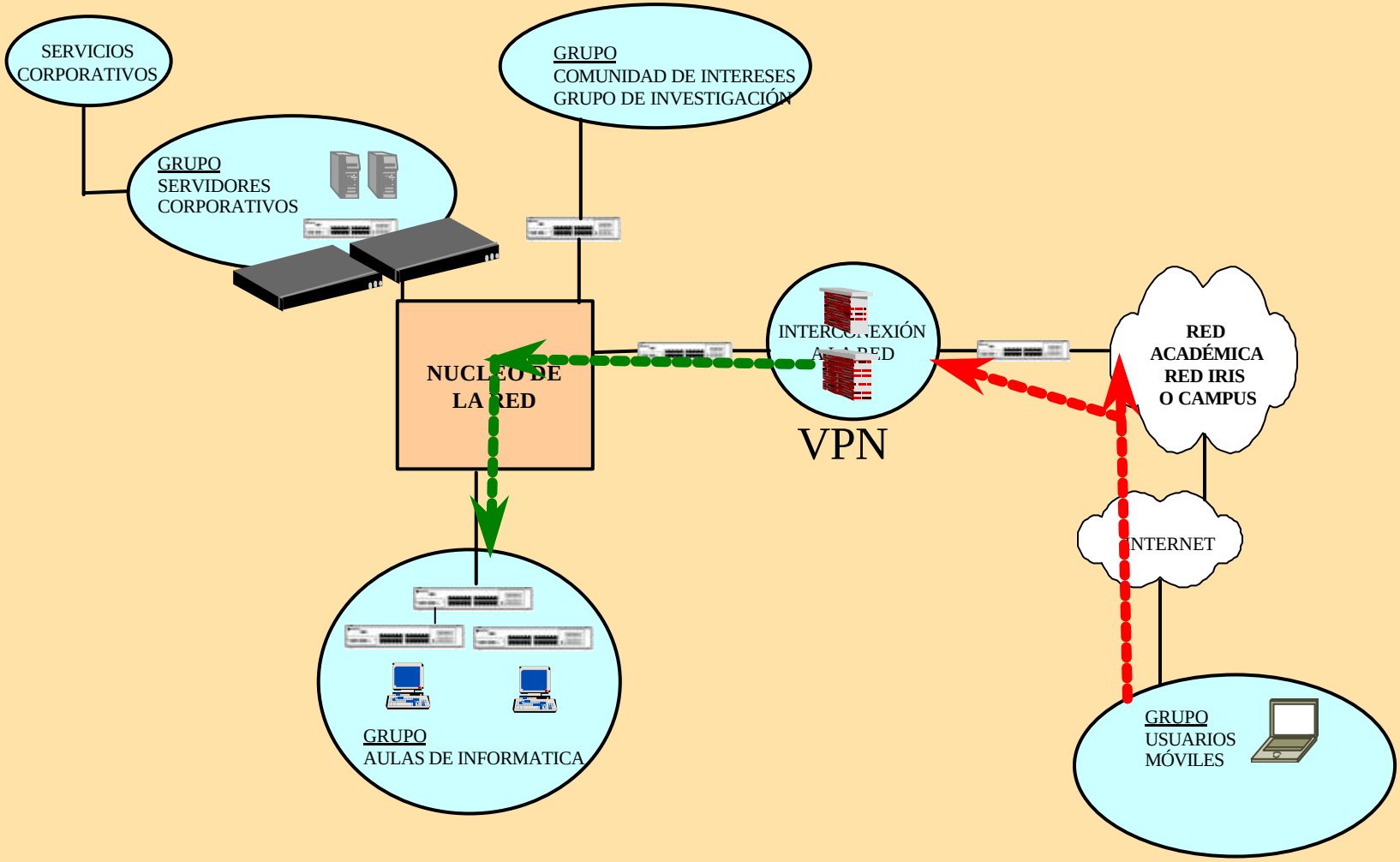
Usuarios móviles- Investigadores

SIEMENS



Usuarios móviles- Alumnos

SIEMENS



Autenticación con usuario y password

http://www.siemens.es/seguridad

Redes inalámbricas

SIEMENS

http://www.siemens.es/seguridad

Principios Objetivos

Profesores y alumnos

Análisis de riesgo

Altas amenzas

Altas vulnerabilidades

Contractual Legal

LOPD nivel medio

Propiedad intelectual

- **Confidencialidad**
- **Integridad**
- **Disponibilidad**
- **Identificación**

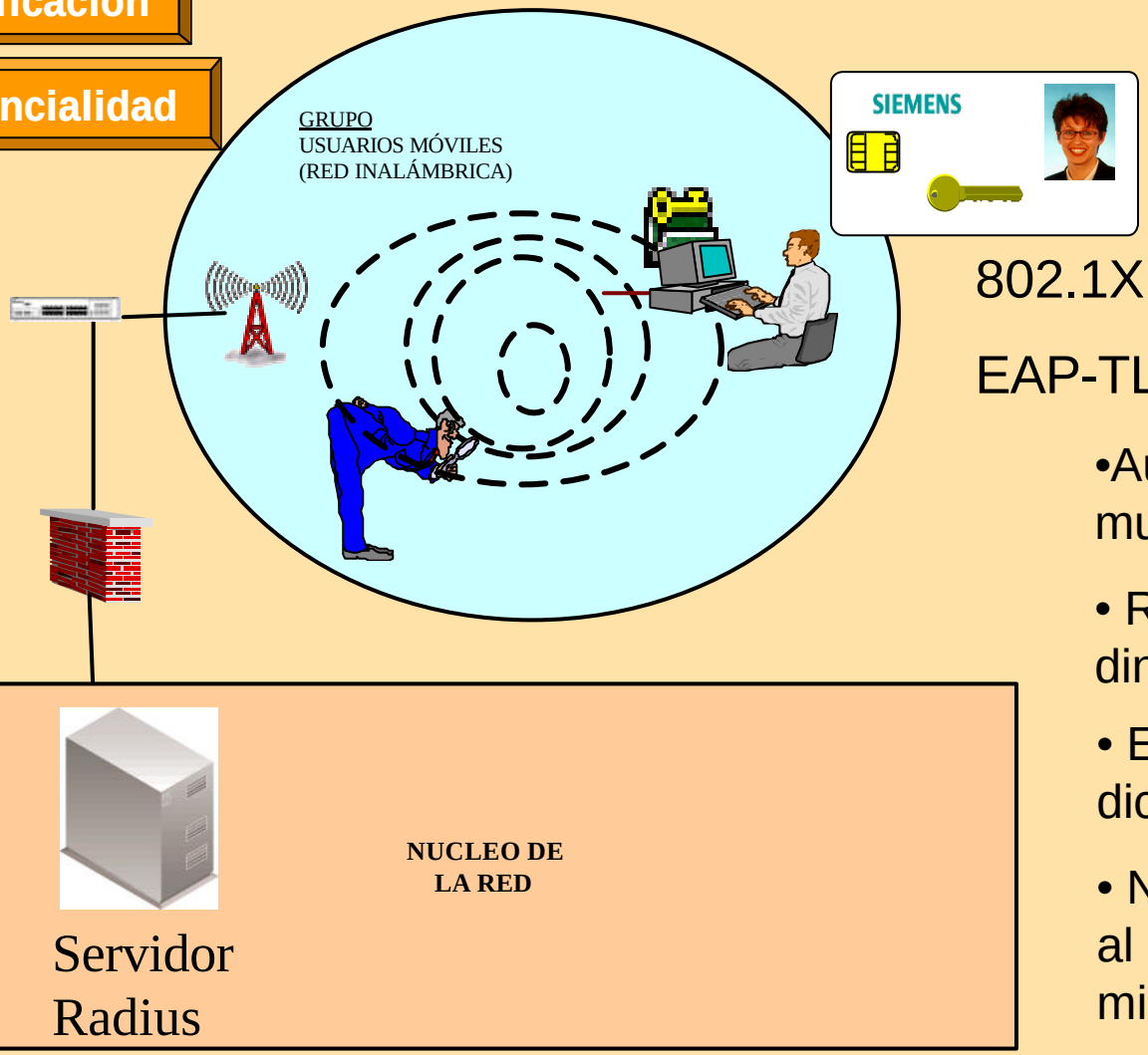
Redes inalámbricas

SIEMENS

http://www.siemens.es/seguridad

Identificación

Confidencialidad



802.1X

EAP-TLS:

- Autenticación mutua
- Rekeying dinámico
- Evita ataques de diccionario
- No es susceptible al “man in the middle”

Agenda

- Introducción
- Requerimientos generales:
  - Servicios
  - Núcleo de Red
- Requerimientos de usuario:
  - Colaboradores
  - Investigadores
  - Alumnos
  - Móviles
  - Inalámbricos
- Requerimientos de adminstrador
  - Gestión de la seguridad

Organización de seguridad

SIEMENS

http://www.siemens.es/seguridad

UNE-ISO/IEC 17799 (4.1)

Infraestructura de la Seguridad de la Información

Objetivo: **Gestionar la seguridad de la información dentro de la Organización.**

- 4.1.1 Comité de Seguridad de la Información.
- 4.1.2 Coordinación de la Seguridad de la Información.
- 4.1.3 Asignación de responsabilidades sobre Seguridad de la Información.
- 4.1.5 Asesoramiento de especialistas en seguridad de la información.
- 4.1.6 Cooperación entre organizaciones

Formación

SIEMENS

UNE-ISO/IEC 17799 (6.2)

Capacitación de usuarios

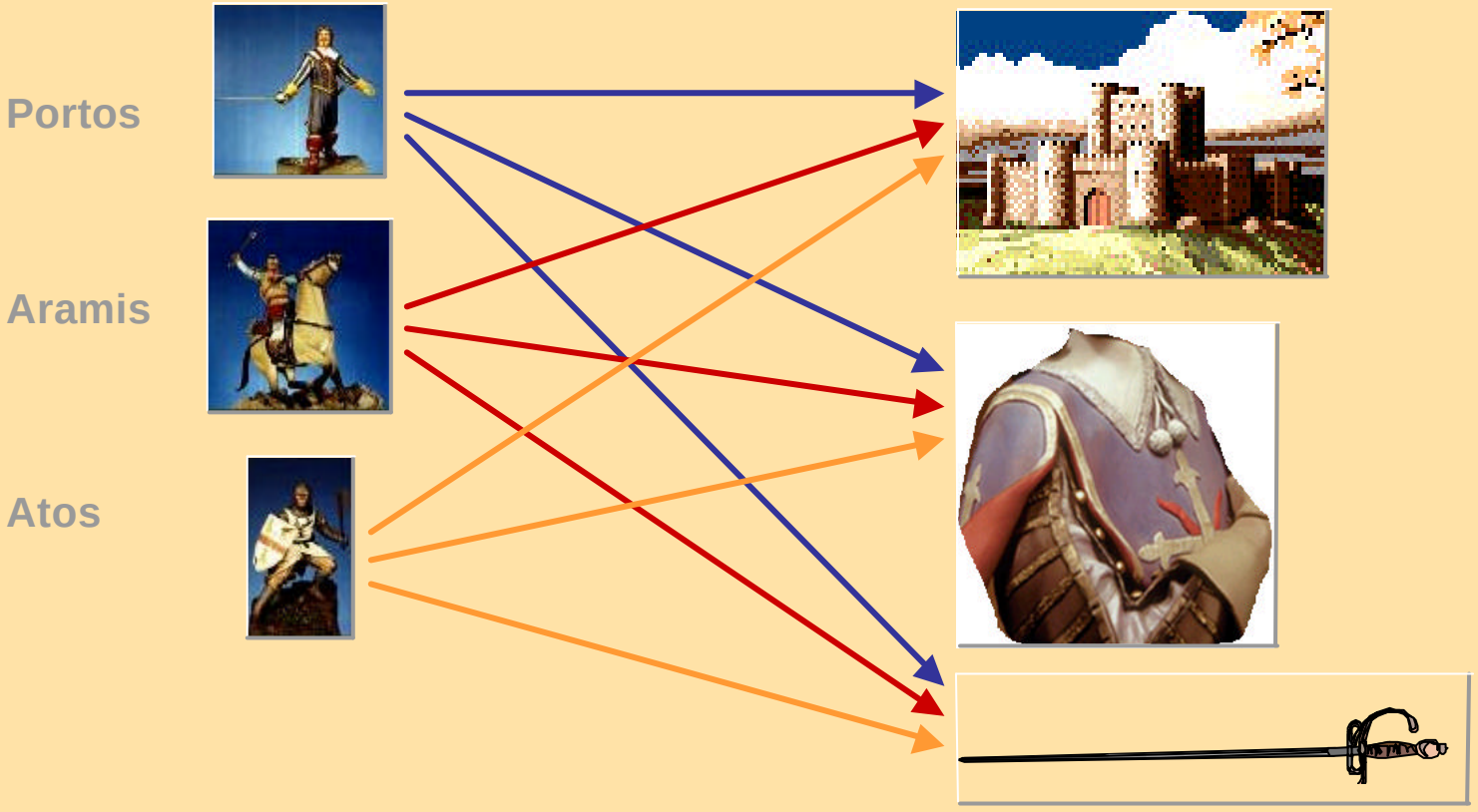
Objetivo: **Asegurar que los usuarios son conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que están preparados para sostener la Política de seguridad de la Organización en el curso normal de su trabajo.**

- 6.2.1 Educación y capacitación en seguridad de la información

- Herramientas para difundir la políticas de seguridad

Gestión de usuarios

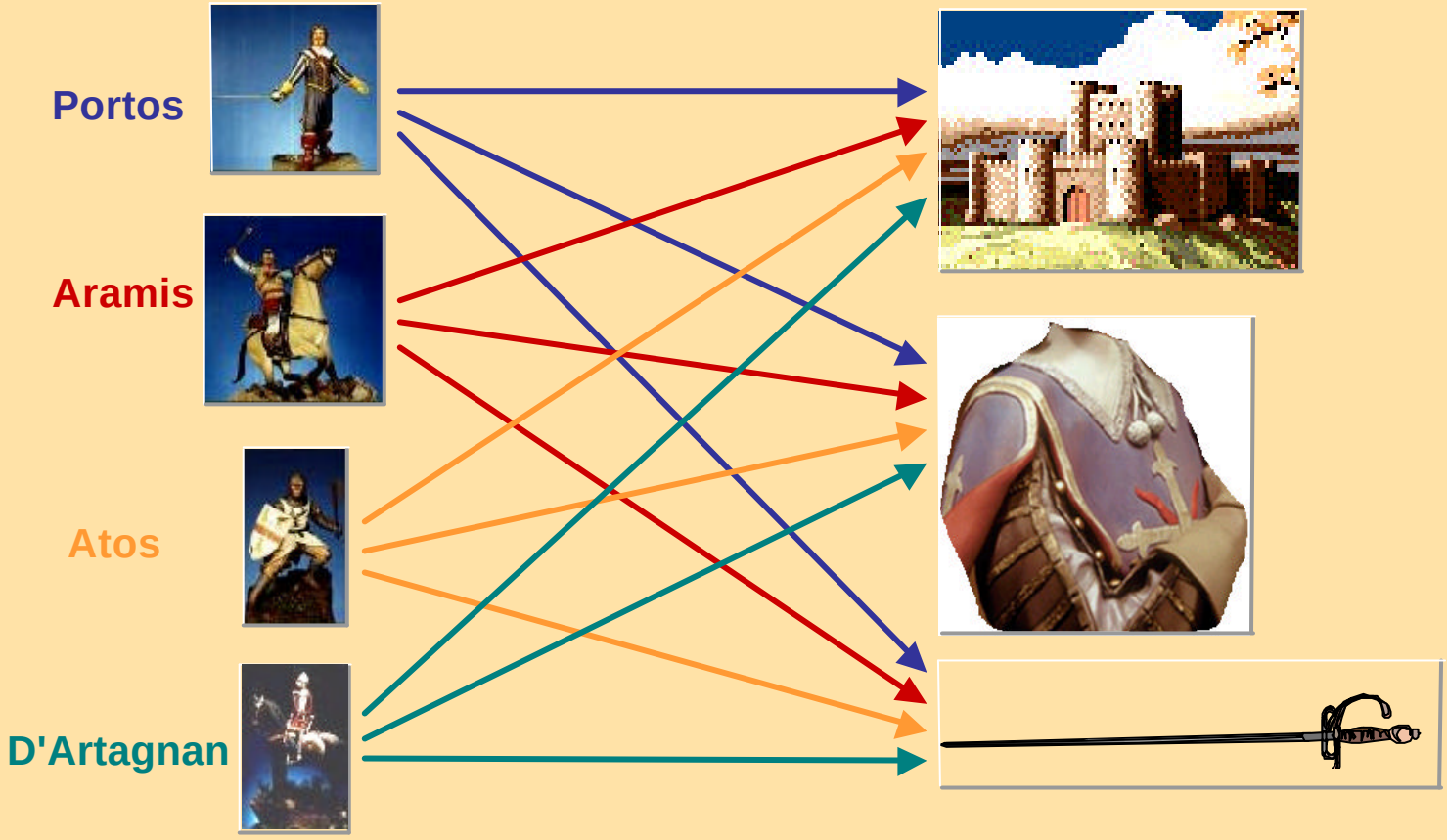
SIEMENS



Quelle: Don Bowen, The Burton Group

Gestión de usuarios

SIEMENS

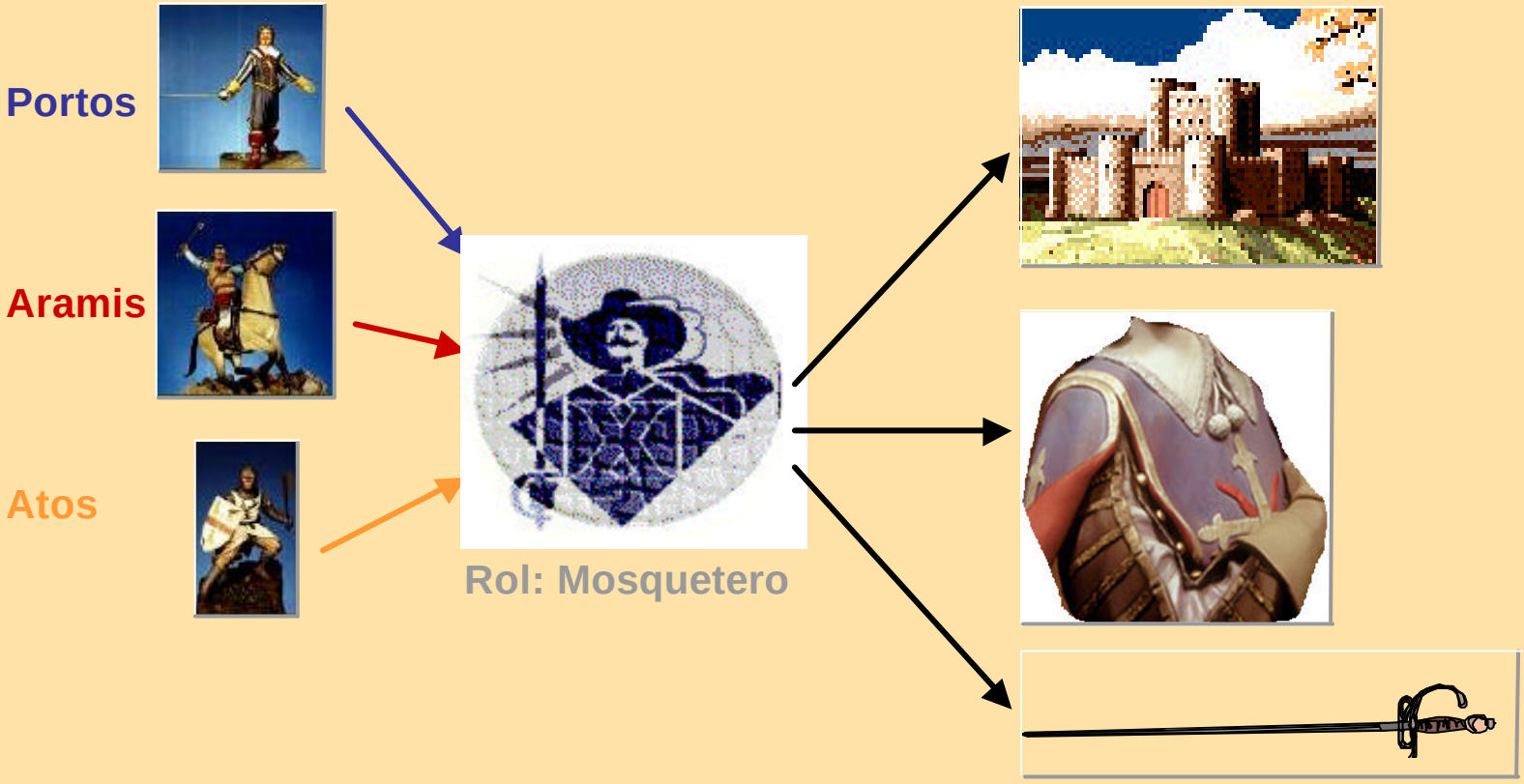


Quelle: Don Bowen, The Burton Group

Usuarios x permisos = 12 parámetros a manejar

Control de acceso basado en roles

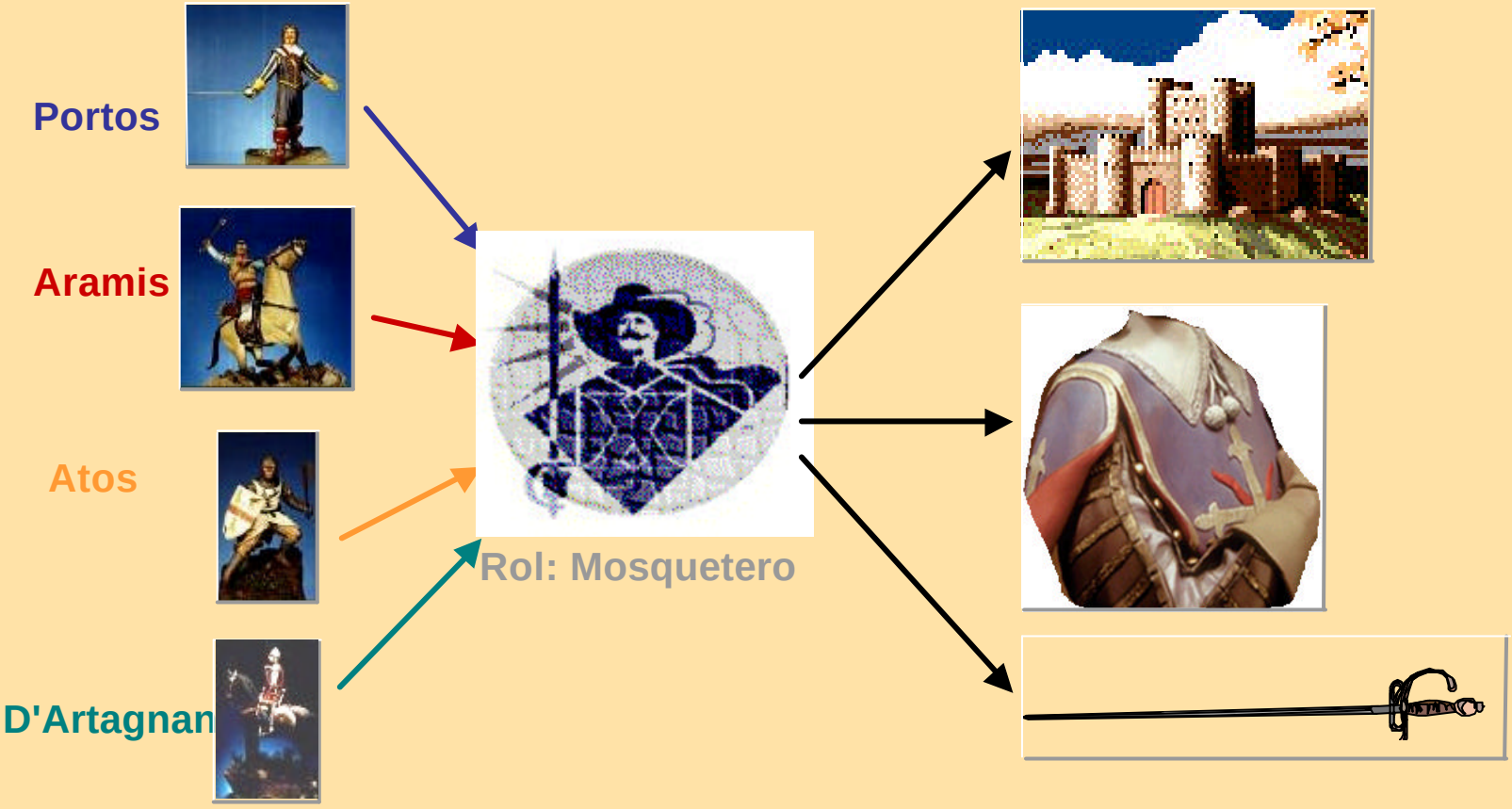
SIEMENS



Quelle: Don Bowen, The Burton Group

Control de acceso basado en roles

SIEMENS



Usuarios x permisos = 7 parámetros a manejar

Quelle: Don Bowen, The Burton Group

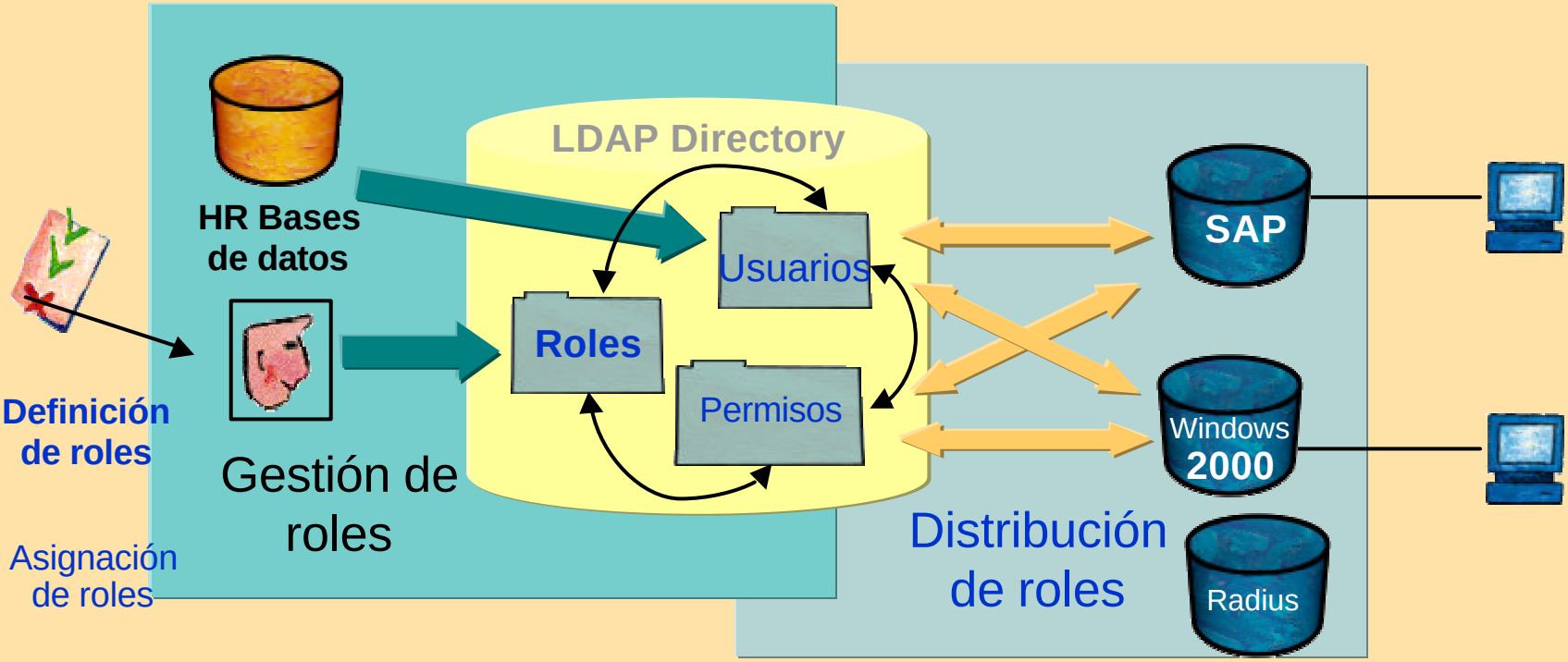
Control de acceso basado en roles

SIEMENS

http://www.siemens.es/seguridad

UNE-ISO/IEC 17799 (9.6) **Control de acceso a las aplicaciones**

Objetivo: **Evitar el acceso no autorizado a la información contenida en los sistemas.**



- Identidad totalmente integrada y gestión de acceso para todos los escenarios

Revisión

SIEMENS

- Mejora continua. Verificación:
  - Ejecución de procedimientos de monitorización:
    - detectar, lo antes posible, fallos, debilidades, responsabilidades incumplidas o inadecuadas,..
    - revisar registros de las operaciones controladas
  - Revisión técnica de las medidas de seguridad en cuanto a su implementación, operación y efectividad.
  - Evaluación de los indicadores de Seguridad

Análisis de vulnerabilidades

SIEMENS

- Objetivo: Detectar riesgos de vandalismo, espionaje, robo, etc. en los Sistemas de Información de la Empresa
- Método:
  - Test de penetración: Intentos de acceso a la red coorporativa desde el exterior
  - Test de vulnerabilidades interno: Chequeando de manera específica: servidores, bases de datos, routers, PCs
  - Se exploran todo tipo de vulnerabilidades.

El reto de la gestión de seguridad

SIEMENS

Arquitectura distribuida.

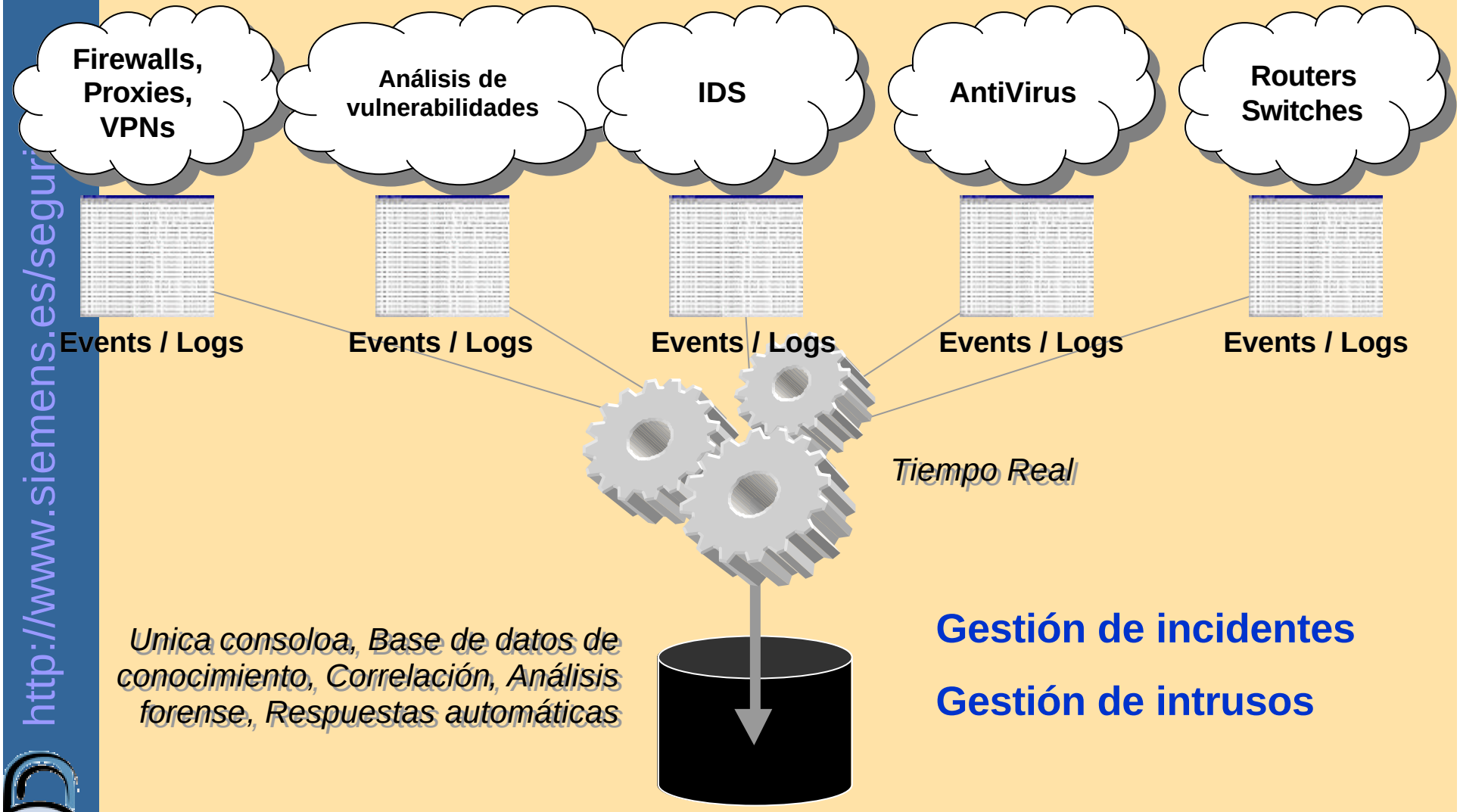
Crecimiento número de eventos

Capacidad humana

http://www.siemens.es/seguridad

Gestión de la seguridad

SIEMENS



Gestión de incidentes

Gestión de intrusos

http://www.siemens.es/seguri

- Log Manager
- Host-Intrusion Detector
- Firewall Monitor
- IDS Monitor
- Antivirus Monitor

SIEMENS

Configuration G

⊕Log Manager

⊖Host Intrusion Detector

- View intrusion alerts
- Create a filtered, real-time view of alerts
- Learn to set-up real-time alerts and alert notifications based on a specific event
- Learn to set-up automatic responses to security threats
- View built-in expert security knowledge
- Add real-time protection to additional servers or workstations

⊕Firewall Monitor

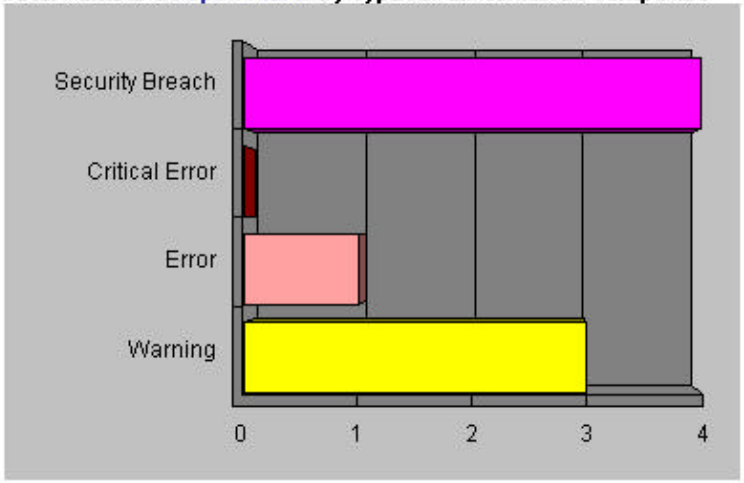
⊕Antivirus Monitor

⊕IDS Monitor

Number of Monitored Computers:	3
Average Alert Latency:	14703 s
Average Security Breach Reaction Time:	69736 s
Number of New Events Today:	5

Security-at-a-Glance

Total Number of Open Alerts by Type for all Monitored Computers



Computer Security Overview

Number of computers with at least one alert of each type.

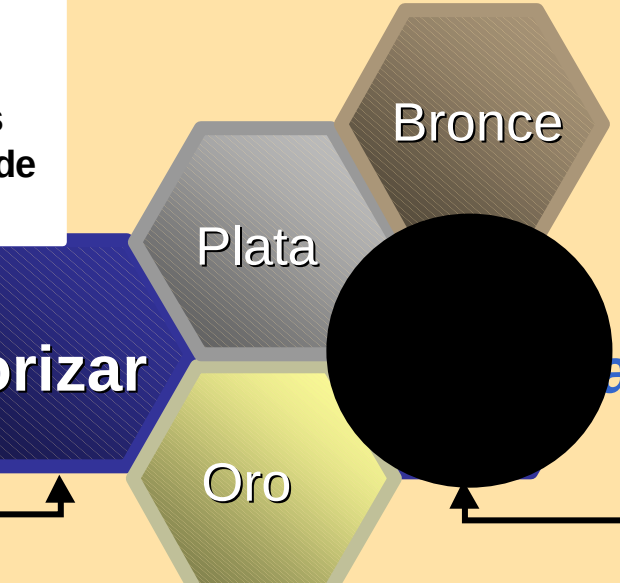
Security Breaches:	0	computers
Critical errors:	0	computers
Errors:	0	computers
Warnings:	0	computers

Desarrollo y mantenimiento

SIEMENS

http://www.siemens.es/seguridad

7x24 monitorización de sistemas, identificación de anomalías y alertas según los acuerdos de servicio.



Mantenimiento continuado de sistemas y provisión de actualizaciones de software
El clinete retiene todo el control sobre la configuración de sistemas y su uso.

Un servicio totalmente proactivo identificando y gestionando incidentes de seguridad.

UNE-ISO/IEC 17799 (8)

SIEMENS

Su **socio tecnológico** en Seguridad:

- Fortaleza de un integrador mundial
- Múltiples Referencias de Seguridad
- Expertos en las últimas tecnologías

Carolina.oro@siemens.com