Introducción a la Seguridad de la Información

Víctor Bravo, Pedro Buitrago[1]

[1]Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres
Nodo Mérida

CENDITEL, 2013

Licencia de Uso

Agenda

1. **Definición de Seguridad de la Información**
   - Activos de la Información
   - Principios de Seguridad de la Información
   - Niveles de Seguridad
2. **La amenaza**
   - Ciclo de la seguridad de la Información
   - La Confianza
3. **La firma electrónica**

Reto para el nuevo paradigma tecnológico (Seguridad)

Lograr la **aceptación cultural** de nuevos conceptos como la **firma electrónica**, del tal manera que la tecnología mejore la **relación humana** y no la empobrezca. Este objetivo implica la identificación de algunos mitos.

"Todo pasado fue mejor" ..."La tecnología anterior es mejor"

"El futuro tecnológico es predecible"

- Es una tarea extremadamente díficil
- Historia puede servir
- Quizás la mejor herramienta es la "imaginación"
- Mejor los escritores que los tecnólogos

Algunas frases célebres ...

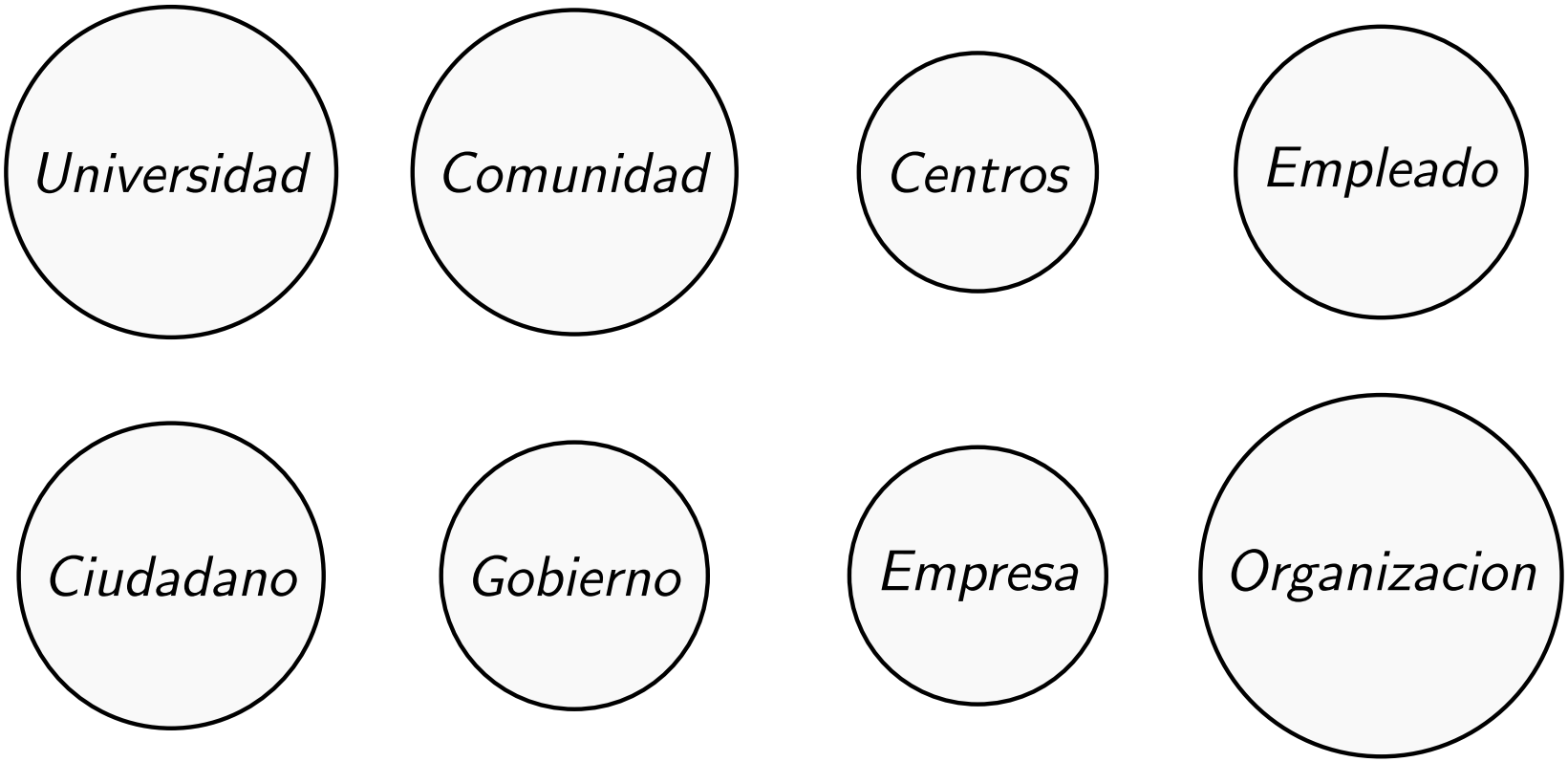
- **1876:** "El teléfono debería ser usado únicamente para informar a la gente de la llegada de telegramas"
  Alexander G. Bell (supuesto inventor del teléfono)
- **1943:** "Pienso que el mercado mundial de ordenadores puede ser de cinco unidades"
  Thomas Watson, Presidente de IBM
- **1981:** "640 Kb son suficientes para cualquiera"
  Bill Gates (Hablando de memoria RAM, hoy una computadora de hogar tiene 1.000.000Kb)

La sociedad de la Información

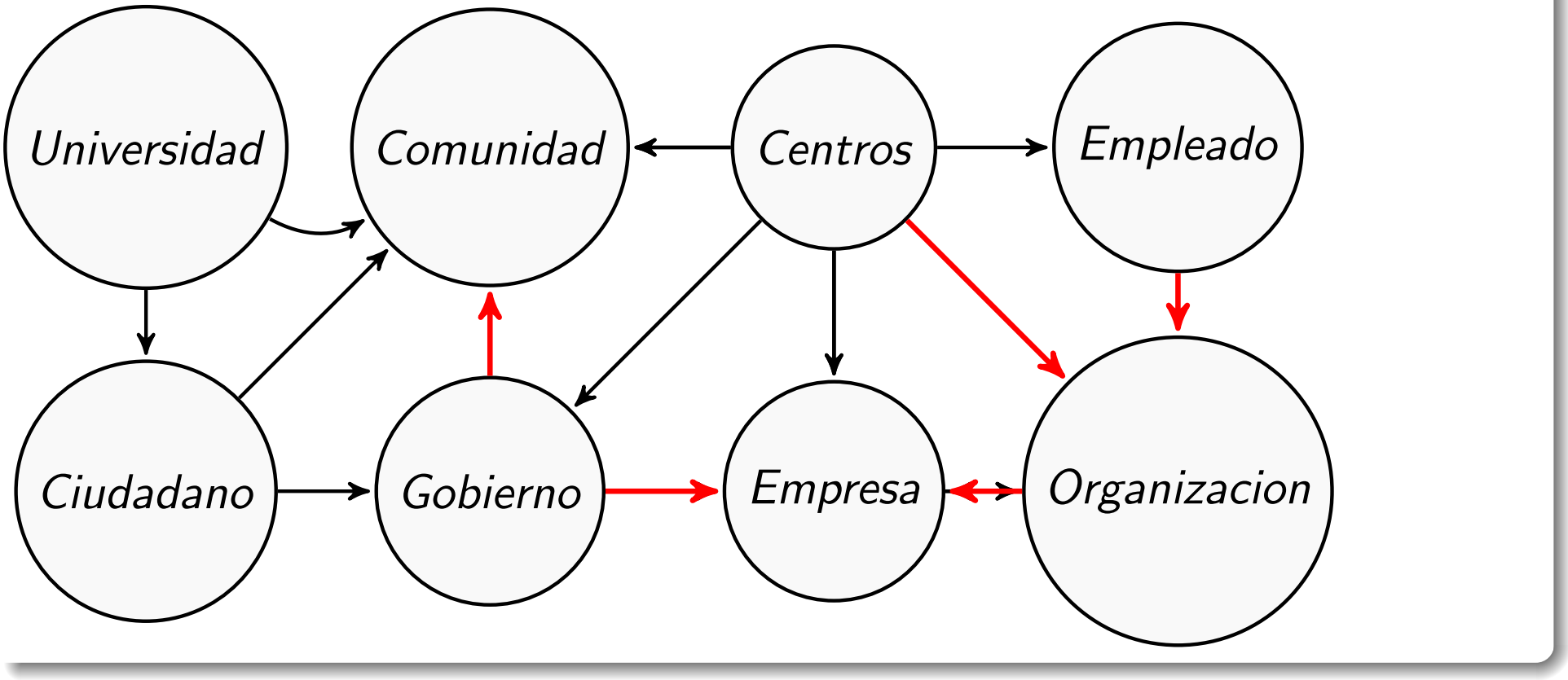
Hitos

- Imprenta (J. Gutenberg, 1448)
- Teléfono (A. Meucci, 1854 Polémica con G. Bell)
- Computador Digital (ENIAC, 1945)
- Internet (CERT Web, 1991)
- Redes Inalámbricas (CERT Web, 1991)

La Sociedad de la Información



La Sociedad de la Información



Activos de Información

Todo lo que se puede "digitalizar" (entender como cadenas de 0 y 1)

- **Documentos de texto:** Cartas, Memorandum, Balances, Contratos, Calificaciones, Planes
- **Sonido:** canciones, conferencias, grabaciones
- **Video:** televisión, conciertos, juegos, reuniones, tiempo real
- **Valores biológicos:** pulso, tensión, imagenología, etc.
- **Valores procesos físicos/químicos:** temperatura, presión, velocidad, densidad

Activos de Información

¿Qué puedo hacer con mis activos?

- Leerlos
- Escribirlos: Iniciarlos o Modificarlos
- Trasformarlos: base para otros activos
- Eliminarlos ¿Iguál que un objeto físico?
- Enviarlos, Trasladarlos ¿Iguál que un objeto físico?
- **Asegurarlos** ¿Iguál que un objeto físico?

Ejercicio

Objetivo: Identificar los retos actuales de la firma electrónica para lograr su masificación y aceptación cultural en Venezuela

¿Cómo aseguro mis activos de información?

Aplico tres principios

- Confidencialidad
- Integridad
- Disponibilidad

Confidencialidad

Se refiere a que se debe mantener inaccesible a todos los usuarios que no estén autorizados a los datos e información, cuando se requiera

Integridad

Se refiere a la protección que debe tener la información, datos, sistemas y otros activos informáticos contra cambios o alteraciones en su estructura o contenido ya sean intencionales o causales por usuarios no autorizados

Disponibilidad

Se refiere a la capacidad que tenga el sistema para mantener los datos e información el mayor tiempo y desde la mayor cantidad de lugares posibles la información accesible a los usuarios autorizados

Ejercicio 2 CID

1. Evaluar los sistemas que se listan abajo para hallar sus valores de Confidencialidad, Integridad y Disponibilidad:
   - Teléfono célular personal
   - Sistema de Correo Electrónico
   - Sitio Web de su Organización

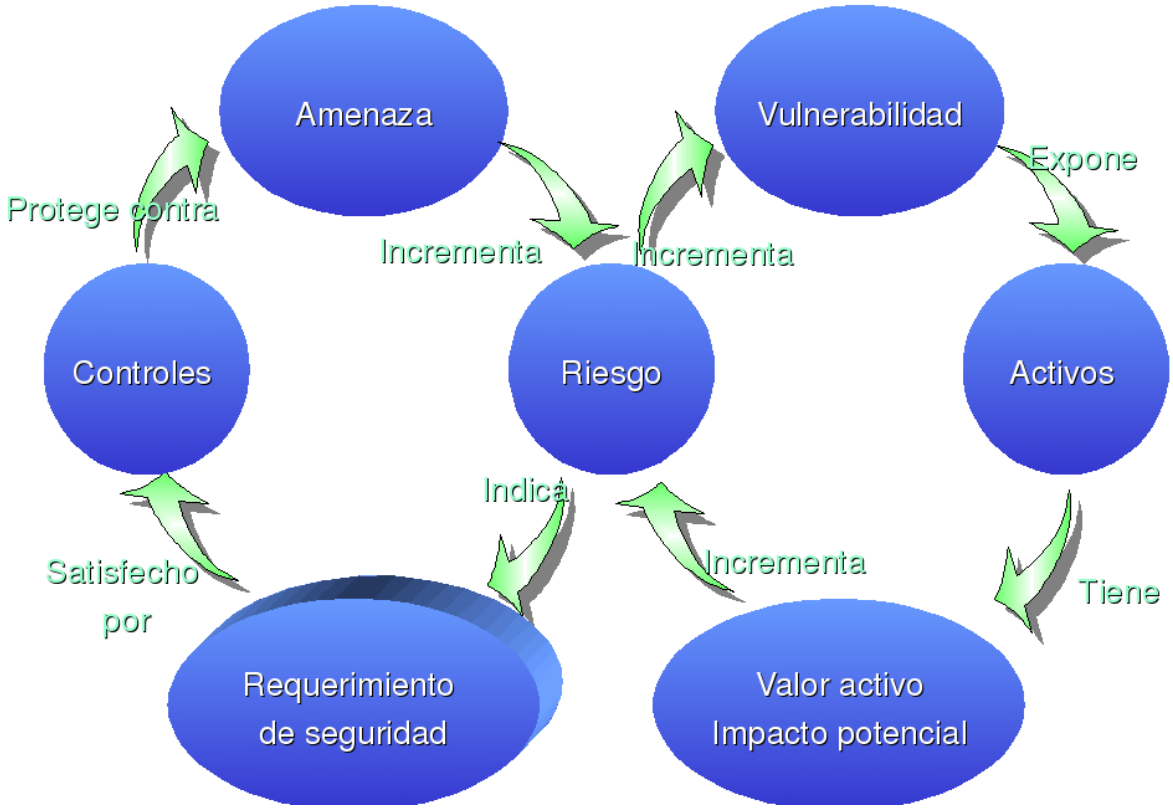
Niveles de Seguridad

¿Cómo saber si es el usuario autorizado?

1. Algo que tu sabes →
2. Algo que tu tienes →
3. Algo que tu eres →
4. y ... Algo que sabes como se hace ¿?

La amenaza: ¿Porqué nos preocupa la seguridad?

Existe un ciclo para mantener asegurados los activos



La amenaza: la multiplicación de los hackers

Personas o organizaciones transgresoras de la Ley.

- Interés Económico
- Interés Político
- Interés Personal (Ataque Interno)
- Interés de Entretenimiento
- Otros Intereses

La amenaza: la multiplicación de los hackers

Cuáles son los medios para ser hackers

1. Internet
2. Acceso a aplicaciones de hackeo
3. Libros, Revistas, Folletos
4. Ingenería Social (Ataques Internos)
5. Técnicas de Inteligencia Artificial
6. No se está familiarizado con este tipo de Delito

Algunos nombres de la amenaza

- Crackers
- Hackers
- Lammers
- Robots
- Spammers
- ...

La amenaza: ¿Porqué nos preocupa la seguridad?

Pero, ¿Es real la amenaza?

La Confianza

No es el que me digas mentiras sino el que ya no crea en tí es lo que me ha hecho estremecer.

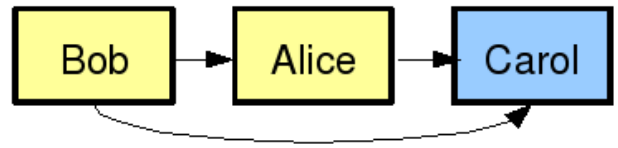
La Confianza: Dos modelos esenciales

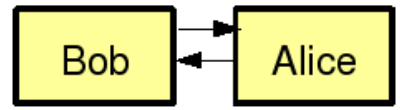
- Basado en pares
- Basado en un tercero

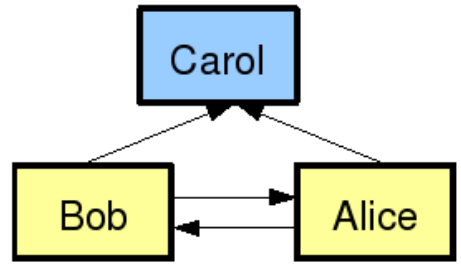
Modelo Basado En pares

Reciprocidad:
Bob confía en Carol, porque Carol confía en Bob

Reciprocidad



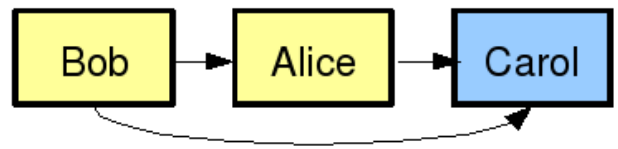


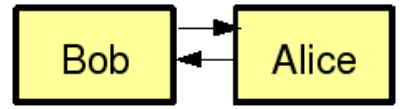


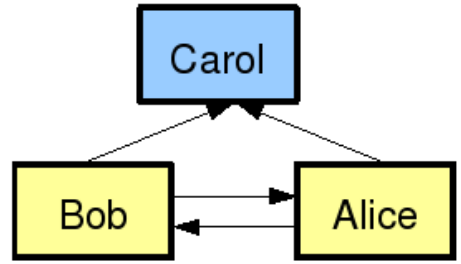
Modelo Basado En pares

Transitividad: Bob confía en Carol, porque Alice confía en Carol y Bob confía en Alice

Transitividad

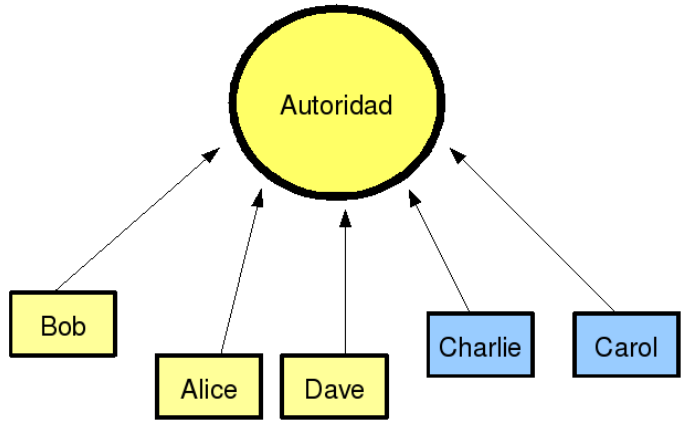






La Confianza: Modelo Basado En un tercero (Autoridad)

- Se establece un protocolo más o menos complejo (conjunto de reglas a seguir)
- Existe una autoridad o infraestructura de autoridades (muy segura)
- Más utilizado en comercio electrónico, banca, aseguramiento de servidores



Firma Manuscrita

Rasgos positivos

Elementos biométricos

Longeva

Lápiz y papel

Culturalmente aceptada

Rasgos negativos

Principio de buena fe

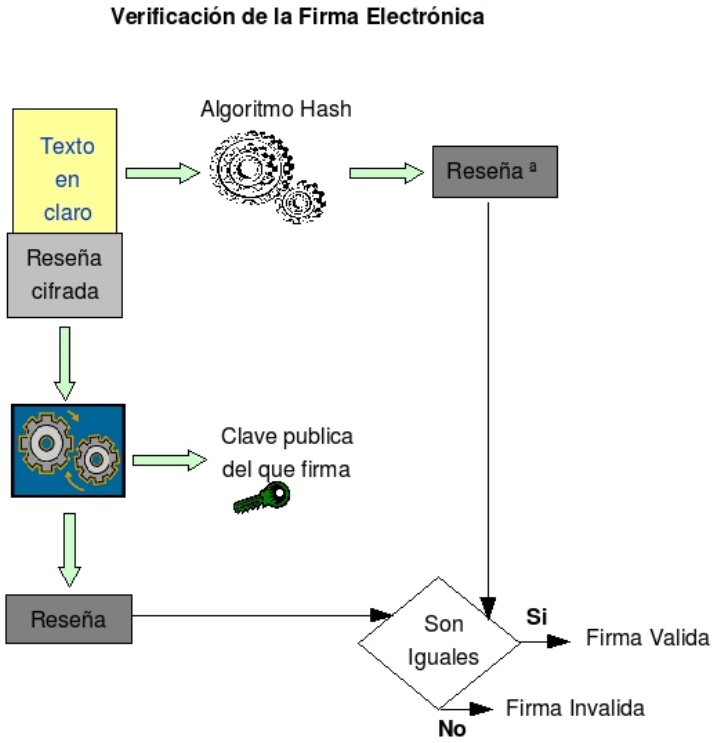
No integrada a sistemas informáticos

Desconocimiento "a priori" de la identidad del firmante

Acto de firma es presencial

No hay un tercero de confianza

reseña Protocolo criptrográfico : hash + cifrado asimétrico.



- PKCS #7 (RFC 2315)
- S/MIME (RFC 3875)
- XMLSig (RFC 3275)
- CADES, XADES (RFC 5126, W3C Note 20 February 2003)
- PADES, PDF/A (ISO 32000)

- Motores criptrográficos (OpenSSL, CrytoAPI)
- Navegadores, Clientes de correo
- Adobe®Reader®, MS Office®
- Xyzmo
- @Firma
- iText
- BDoc*

- Basada en PKI
- Metáfora de la **firma**
- Remota
- Tarjetas Inteligentes
- Formato
- Ergonómica y acceso ubicuo
- Otros (Longeva, por lote, sellado de tiempo, cofirma, firma en cascada)

Preguntas, Dudas y Comentarios

≪ Si un hombre se imagina una cosa, otro la tornará en realidad.≫

Julio Verne

Ejercicio 3 Niveles de Seguridad

1. Evaluar el siguiente tipo de sistema para hallar el nivel de seguridad adecuado, detalle el uso de dispositivos, mecanismo para asegurarlos: enumere las posibles amenazas y el modelo de confianza que podría aplicar para mantener el sistema seguro
   - Sistema de Información en una competición de Programación/Certificación