Sistemas de Información para la Gestión

# UNIDAD 5
# Tema: FIRMA DIGITAL

## Unidad 5: SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

**Seguridad en los Sistemas de Información: Seguridad, Privacidad e Integralidad**: Objetivos de la seguridad en la información Análisis de Riesgos de los sistemas de información. **Tecnologías y herramientas para proteger los recursos de información.** Medidas de controles generales, de aplicación, y en comunicaciones. **Firma Digital**. **Plan de Contingencia de los sistemas de información.** Plan de reanudación de negocios Medidas de recuperación. **Aspecto económico de las medidas de seguridad.** Estructura de control: Costos Beneficios.

## Unidad 5: SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

Objetivos específicos:

- Conocer las herramientas y tecnologías para salvaguardar los recursos de información y áreas de TI para el aseguramiento de la disponibilidad la información sistemas

## Unidad 5: SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

Bibliografía Básica:


- Sistemas de información gerencial / Laudon, Kenneth C. (2012) Sistemas de información gerencial [texto impreso] / Laudon, Kenneth C.; Laudon, Jane P.. - 12a. ed.. - México: Pearson Educación, 2012. ISBN 978-607-32-0949-6. Nota de contenido: Cap. 8. Seguridad en los sistemas de información

## Unidad 5: SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

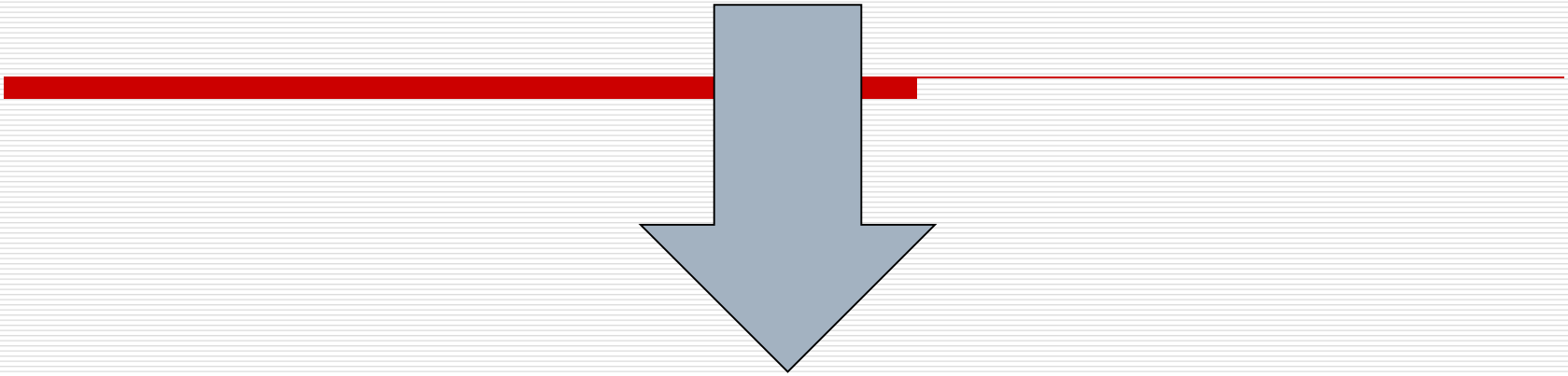
Bibliografía Básica:


- Sistemas de información para la gestión empresaria / Lardent, Alberto R. (2001) Sistemas de información para la gestión empresaria : procedimientos, seguridad y auditoría [texto impreso] / Lardent, Alberto R.. - Buenos Aires : Pearson Educación, 2001. . ISBN 987-9460-51-0. Nota de contenido: II: Seguridad y auditoría informática : 19. Seguridad informática 22. Controles de accesos lógicos y físicos - 23. Seguridad en los sistemas de base de datos - 24. Seguridad de redes y sistemas distribuidos  29. Recuperación de desastres. Continuidad de operaciones.

# Plan de clase

- Introducción
- Firma digital: Concepto. Valor Legal.
- Ventajas.
- Funcionamiento.
- Claves privadas y claves públicas
- Certificados Digitales: Contenido
- Firma Digital Token y Cloud
- Infraestructura de Firma Digital
- Aplicaciones
- Firma Digital Blockchain
- Conclusiones

# RETOS QUE PLANTEA EL ENTORNO



**El negocio, la Tecnología de la Información y Comunicaciones, la gestión de almacenes de datos y el entorno complejo traen aparejada la necesidad de alimentar buenas prácticas de gestión y administrar riesgos.**

# INTRODUCCION

Necesidad de que los instrumentos electrónicos cumplan los siguientes requerimientos:

- Certeza de quién es el emisor y quién es el receptor,

- Demostración de la existencia de la voluntad jurídica,

- Prueba fehaciente de la misma.

# FIRMA DIGITAL

## PUNTOS CRITICOS EN LA ACEPTABILIDAD Y VALIDEZ DE DOCUMENTOS ELECTRONICOS

1. CREDIBILIDAD.
2. FUGACIDAD.
3. IDENTIFICACION Y AUTENTICACION DE LAS PARTES.
4. IDENTIFICACION DEL DOCUMENTO.
5. INADECUACION DEL ORDEN JURIDICO.

# FIRMA DIGITAL

Conceptos:

**Firma**: “El trazo peculiar mediante el cual el sujeto consigna habitualmente su nombre y apellido, a fin de hacer constar las manifestaciones de voluntad”
(Diccionario Abeledo Perrot, citado por Lardent)

“La firma es el nombre escrito de una manera particular, conforme el modo habitual seguido por una persona en actos sometidos al cumplimento de formalidades”
(Revista Jurisprudencia Argentina, citado por Lardent)

# FIRMA DIGITAL

Conceptos:

**Documento tradicional** = papel + mecanismo de impresión + firma

**Documento electrónico** = no hay elemento físico. El documento y el medio de almacenamiento están integrados.

**Digitalizar** = convertir algo en números (dígitos)

# MARCO NORMATIVO

El marco normativo de la República Argentina en materia de Firma Digital está constituido por la Ley Nº 25.506, el Decreto Nº 2628/02 y su modificaciones, y un conjunto de normas complementarias que fijan o modifican competencias y establecen procedimientos.

# QUE ES FIRMA DIGITAL?

**Documento Digital**: representación digital de actos o hechos con independencia del soporte (art. 6, ley 25.506)

**Firma Electrónica**: conjunto de datos electrónicos ligados de manera lógica a otros datos electrónicos utilizados por el signatario como medio de identificación (art. 5) que carezca de algunos de los requisitos legales para ser considerada firma digital (art. 9 , ley 25.506)

# QUE ES FIRMA DIGITAL?

## Firma Digital

Herramienta Tecnológica garantiza

**autoría e integridad**

documentos digitales

# QUE ES FIRMA DIGITAL?

**Propuesta de tecnología informática**.

**Objetivo**: cumplir con la finalidad que tradicionalmente cumplía la firma ológrafa (manuscrita), pero adaptada al ciberespacio (redes)

**Partes:**

1. Método que haga imposible alterar la firma.
2. Verificación que la firma pertenece al firmante.

# QUE ES FIRMA DIGITAL?

## Características

- Equivalente digital a la firma manuscrita.
- NO ES LA IMAGEN ESCANEADA de la firma manuscrita.
- Es la encripción (criptografía) con la llave privada del hash (huella) de un documento.
- Existe una diferente para cada documento.

# QUE ES FIRMA DIGITAL?

| DIFERENCIA ENTRE FIRMA | |
|---|---|
| **Firma Analógica** | **Firma Digital** |
| Intrínsecamente seguras.<br><br>Garantizan la autenticidad de origen.<br><br>Garantizan la Integridad.<br><br>Únicas.<br><br>Difíciles de falsificar.<br><br>El secreto está en el carácter grafológico. | Las firmas deben ser generadas sólo por el firmante.<br><br>Computacionalmente seguras.<br><br>Verificables: Por los receptores y por los jueces.<br><br>El firmante no puede negar su propia firma.<br><br>Fáciles de generar.<br><br>Diferentes para cada documento.<br><br>El secreto está en la clave. |

# QUE ES FIRMA DIGITAL?

Resumiendo…

Una firma digital es un conjunto de datos asociados a un mensaje que permite asegurar la **identidad** del firmante y la **integridad** del mensaje.

La firma digital no implica que el mensaje esté encriptado, es decir, que este no pueda ser leído por otras personas; al igual que cuando se firma un documento holográficamente este sí puede ser visualizado por otras personas.

# QUE ES FIRMA DIGITAL?

Resumiendo…

es un instrumento idóneo para agilizar el sistema de transacciones electronicas y para dar confianza

se puede aplicar tanto a un correo electrónico como a un documento (texto, multimedia, etc.)

# QUE VALOR LEGAL TIENE LA FIRMA DIGITAL?

**existe una presunción "iuris tantum" a su favor**

Por ejemplo:

***Si un documento firmado digitalmente*** es verificado correctamente, se presume ***salvo prueba en contrario*** que proviene del suscriptor del certificado asociado y que no fue modificado

# QUE VALOR LEGAL TIENE LA FIRMA DIGITAL?

Por ejemplo:

En cambio, la ***firma electrónica***, en caso de ser desconocida la firma corresponde a quien la invoca acreditar su validez.

# VALIDEZ FIRMA DIGITAL SEGÚN LEY 25.506

## Requisitos Validez Firma Digital (Art. 9)

a) Creada durante vigencia certificado digital válido del firmante;

b) Ser Verificada en forma debida;

c) Certificado emitido o reconocido por certificador licenciado.

# VALIDEZ FIRMA DIGITAL SEGÚN CCCN – LEY 26.994

## CCCN Sec. 3ª-Forma y prueba acto jurídico

**ARTÍCULO 288. Firma.** La firma prueba autoría declaración de voluntad expresada en el texto[…]. Debe consistir en el nombre del firmante o en un signo.
En instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho **si se utiliza una firma digital**, que asegure indubitablemente autoría e integridad del instrumento.

# VENTAJAS FIRMA DIGITAL

- Brinda seguridad en el intercambio de información crítica.
- Reemplaza a la documentación en papel por su equivalente en formato digital.
- Reduce costos generales y mejora la calidad de servicio.
- Mayor velocidad de procesamiento.
- Las empresas podrán extender plataformas de comercio electrónico con mayor seguridad, garantizando el mismo marco jurídico que proporciona la firma hológrafa.

# COMO FUNCIONA FIRMA DIGITAL?

Clave Pública B

Mensaje Encriptado con Clave Privada A Clave Pública B

Mensaje Encriptado

Mensaje Encriptado con Clave Privada A Clave Pública B

Clave Privada B

Mensaje Encriptado con Clave Privada A

Clave Pública A

Mensaje

Mensaje Encriptado con Clave Privada A

Clave Privada A

Mensaje

Usuario A

Canal inseguro (internet)

Usuario B

# COMO FUNCIONA?

**El firmante Usuario A:**

**Genera mediante una función matemática una huella digital del mensaje.**

**Esta huella digital se encripta con la clave privada del firmante.**

**El resultado es lo que se denomina firma digital la cual se enviará adjunta al mensaje original y/o documento adjunto.**

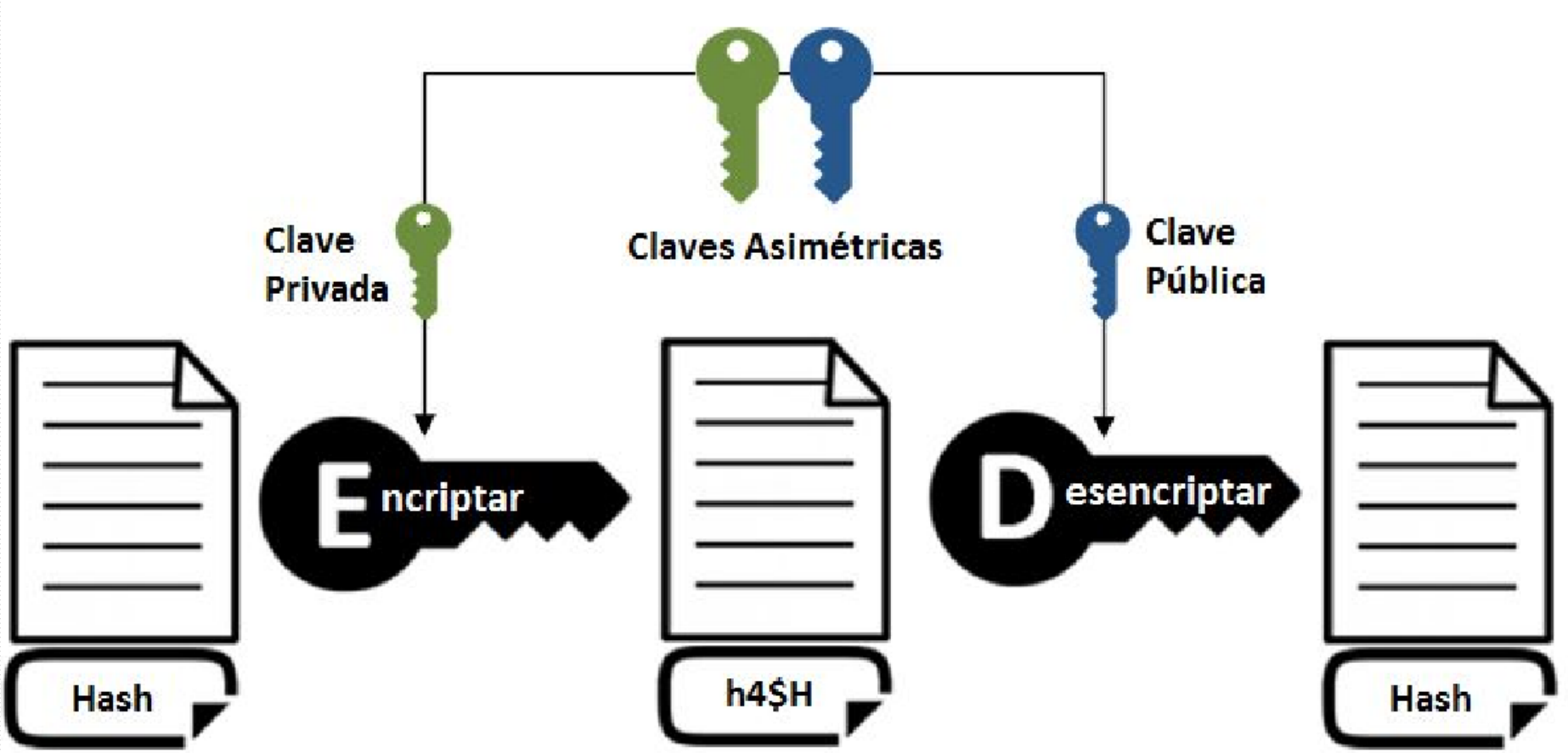
# COMO FUNCIONA?

**El Usuario B receptor del mensaje:**

**Genera huella digital del mensaje recibido, luego desencripta firma digital del mensaje utilizando clave pública del firmante, obtiene huella digital del mensaje original;**

**Si ambas huellas digitales coinciden, significa que el mensaje no fue alterado y que el firmante es quien dice serlo**

# COMO FUNCIONA?



# COMO FUNCIONA?

## Encriptar versus Desencriptar

**Encriptar:**

Texto Plano + Clave de **En**criptado


**Desencriptar:**

Texto Cifrado + Clave de **Des**encriptado

# COMO FUNCIONA?

## CRIPTOSISTEMA ASIMETRICO

Algoritmo que utiliza un par de claves, una clave privada para firmar digitalmente y su correspondiente clave pública para verificar dicha firma digital

## ENCRIPTACION

Transformación un documento legible (texto plano) en uno ilegible (texto cifrado) de acuerdo a una fórmula matemática (algoritmo) y de la utilización de una palabra clave o simplemente la “clave”

## DESENCRIPTACION

Transformación de un texto cifrado en un texto plano utilizando el algoritmo y la clave de encriptación. Proceso inverso a la Encriptación

# CLAVE PUBLICA Y CLAVE PRIVADA

## CLAVE CRIPTOGRÁFICA PRIVADA

En un criptosistema asimétrico es aquella clave que se utiliza para **firmar digitalmente**

## CLAVE CRIPTOGRÁFICA PÚBLICA

En un criptosistema asimétrico es aquella clave que se utiliza para **verificar** una **firma digital**

# CIFRADO FIRMA DIGITAL

**CIFRADO DE CLAVE PRIVADA:** Las claves de cifrado y descifrado son las mismas

Ejemplos: DES (Data Encryption Estándar), Triple DES

**CIFRADO DE CLAVE PUBLICA:** Las claves de cifrado y descifrado son diferentes no derivándose una de otra, por lo cual puede hacerse pública la clave de cifrado mientras se mantenga en secreto la clave de descifrado.

Ejemplo: RSA (Rivest, Shamir, Adlerman)

# FIRMA DIGITAL TOKEN

**Llaves por puerto USB - Dos tipos :**

**•Almacenan clave Privada generada en PC.**

**• Generan la Clave Privada directamente y la almacenan.**

**Lectores de Tarjetas**

**• Almacenan clave Privada generada en PC.**

**• Generan la Clave Privada directamente y la almacenan.**


**Grabación en Mini CD**

# FIRMA DIGITAL CLOUD

## FIRMA EN CLOUD O FIRMA REMOTA

**solución tecnológica segura y confiable que permite firmar digitalmente documentos electrónicos *sin token***

# INFRAESTRUCTURA PKI

**PKI significa Public Key Infraestructure o Infraestructura de Clave Pública**

**Sistema de hardware, software, personal, normas y procedimientos que proveen garantías de seguridad para los documentos, transacciones y comunicaciones electrónicas por internet.**

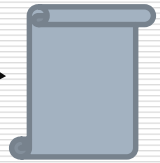
# ACTORES PKI

Autoridad de aplicación (Jefatura de Gabinete de Ministros -Secretaria Gob. De Modernización)

Ente licenciante
Autor. Certificante Raíz
(Secretaría de Gobierno de Modernización)

Ciberespacio

Certificador licenciado



Certificado Digital

Titular CD (PH/PJ)

# INFRAESTRUCTURA PKI

## Autoridad de Aplicación

**Es el órgano del estado facultado por ley a regular normas y procedimientos técnicos para la administración del documento digital**

## Ente Licenciante

**Órgano técnico, administrativo encargado de otorgar licencias a los certificadores y de supervisar su actividad**

# INFRAESTRUCTURA PKI

## Certificador Licenciado

**Toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia otorgada por el ente licenciante**

# INFRAESTRUCTURA PKI

## Certificado digital

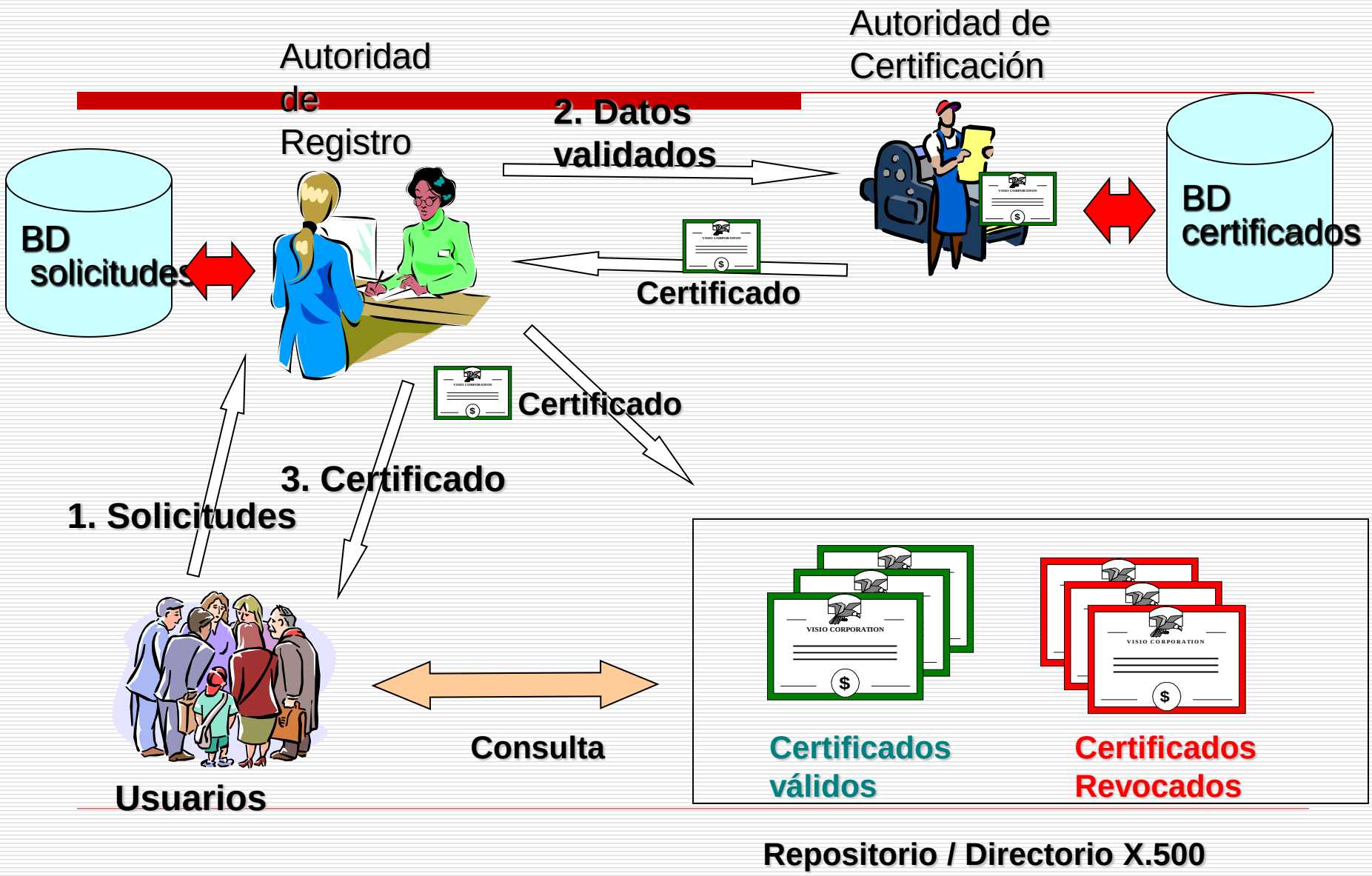
**Documento electrónico firmado digitalmente por certificador que relaciona una entidad con una clave pública**

**(DNI digital)**

## Suscriptor o Titular de certificado digital

**Persona a cuyo nombre se emite un certificado y posee una clave privada que se corresponde con la clave pública contenida en el certificado digital**

# PKI SOLICITUD CERTIFICADO DIGITAL

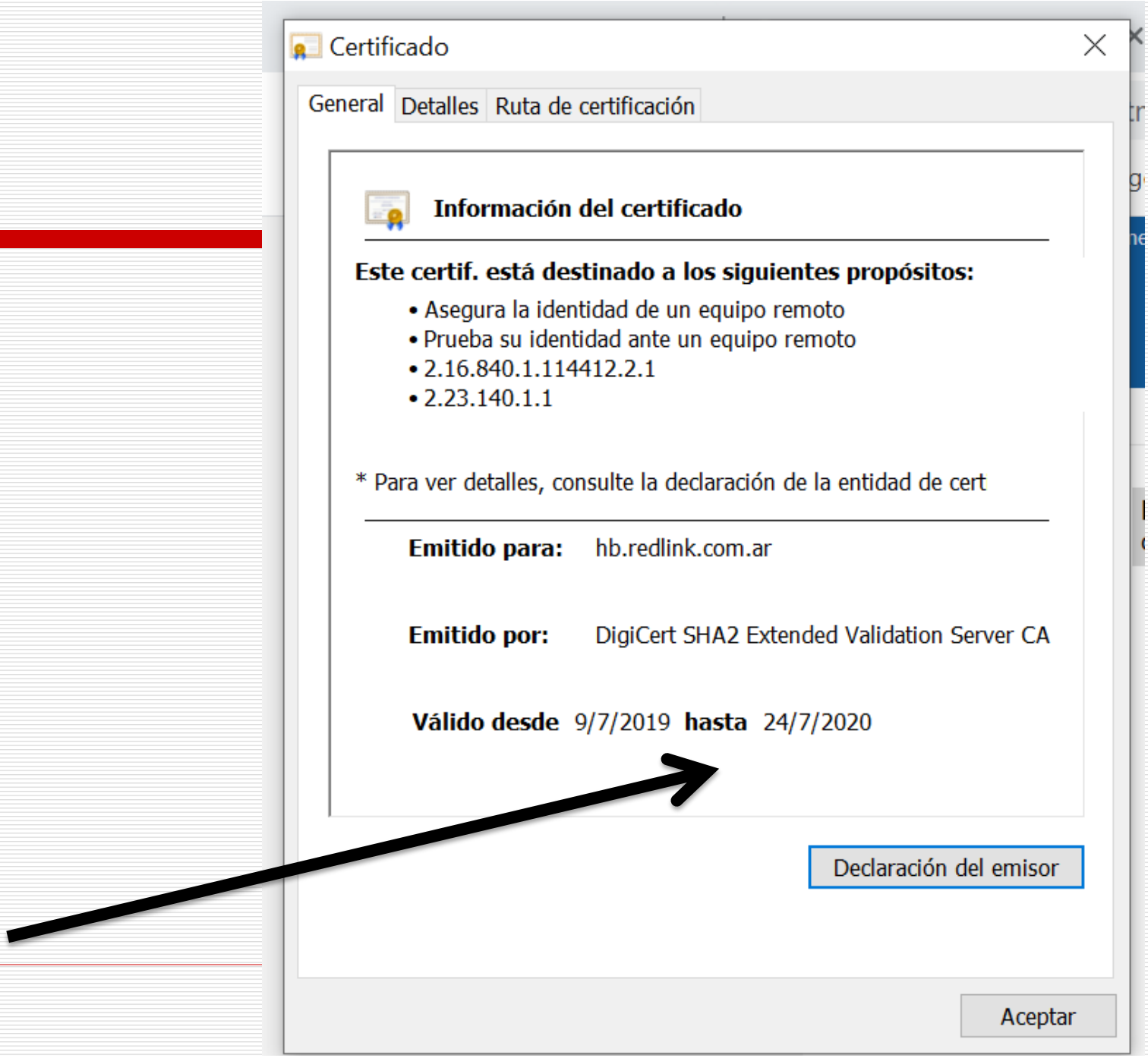


# QUE CONTIENE UN CERTIFICADO DIGITAL?

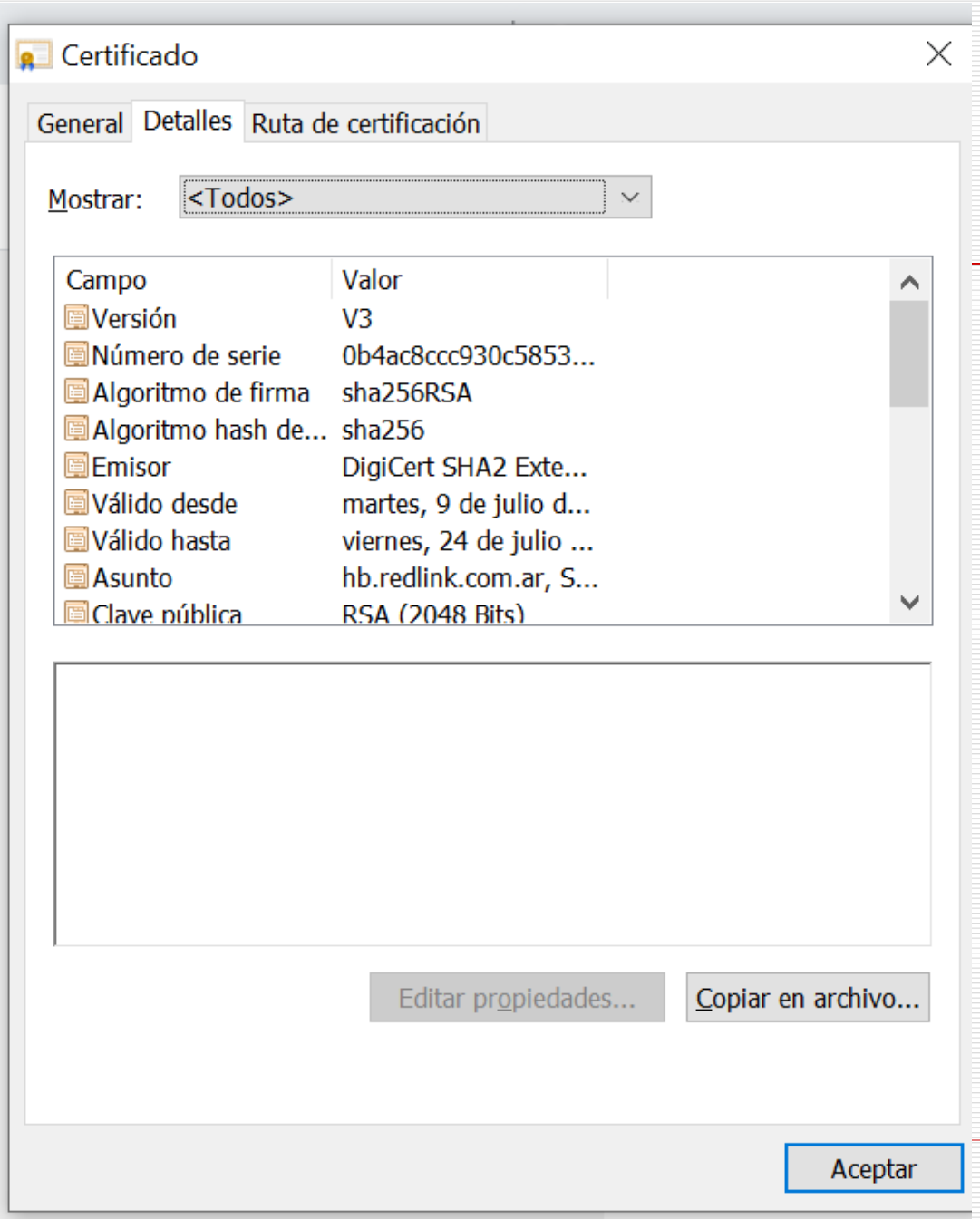
**Un certificado de clave pública contiene los siguientes campos:**

| |
|---|
| VERSIÓN |
| Nro. DE SERIE |
| IDENTIFICADOR DE ALGORITMO |
| AUTORIDAD DE CERTIFICACIÓN |
| PERÍODO DE VALIDEZ |
| USUARIO |
| CLAVE PÚBLICA DE USUARIO |
| FIRMA |

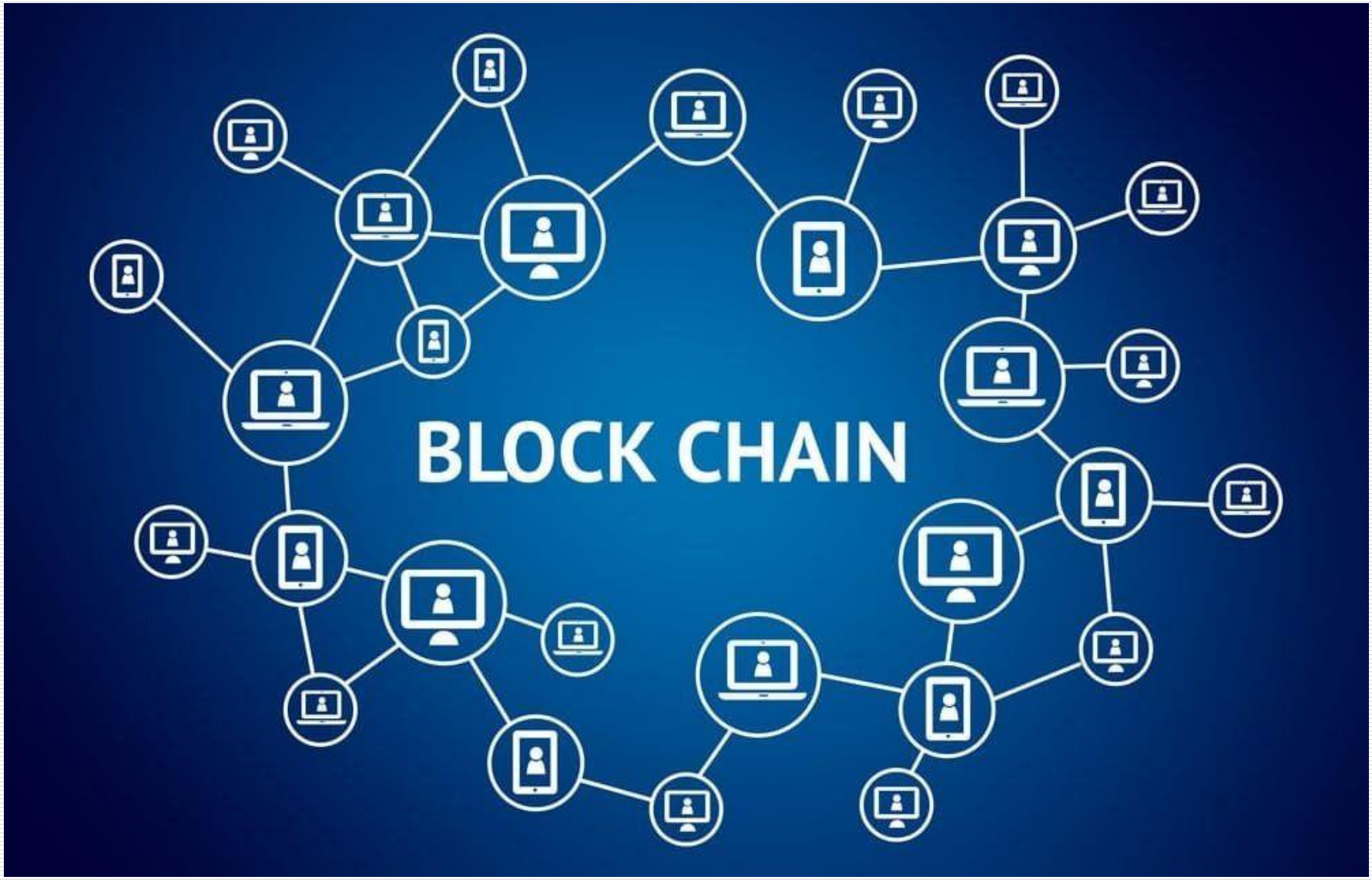
# CERTIFICADO DIGITAL - EJEMPLO



# CERTIFICADO DIGITAL - EJEMPLO



# FIRMA DIGITAL - BLOCKCHAIN



# FIRMA DIGITAL - BLOCKCHAIN

## ¿QUÉ ES UNA CADENA DE BLOQUES O BLOCKCHAIN?

Es cambio de paradigma.

Para muchos, es el método más seguro para crear, modificar, compartir y almacenar información.

## DEFINICION

Tecnología símil contabilidad pública entre pares que se mantiene mediante una red distribuida de PC y que no requiere ninguna autoridad central ni terceras partes que actúen como intermediarios.

# FIRMA DIGITAL - BLOCKCHAIN

## Criptoeconomía

- ✓ Nueva forma de desarrollar mecanismos económicos aplicando técnicas criptográficas y herramientas tecnológicas.

- ✓ Combina teorías económica y tecnológicas: redes, ciencias de computación, etc., que permiten crear nuevas herramientas tecnológicas basadas en BLOCKCHAIN.

# FIRMA DIGITAL - BLOCKCHAIN

## Criptoeconomía

Técnica Criptográfica: **protege documentos y datos confidenciales** que circulan en redes o internet mediante utilización de códigos o cifras

Herramientas Tecnológicas: Firma digital. Protocolo SSL (Secure Socket Layer). VPN (Virtual Private Network)

# FIRMA DIGITAL - BLOCKCHAIN

**Presenta tres componentes fundamentales:**

1) **Transacción**
2) **Registro de transacciones**
3) **Sistema que verifica y almacena la transacción**

Los bloques se generan a través de software de código abierto y registran la información sobre cuándo y en qué secuencia ha tenido lugar la transacción.

Este "bloque" almacena cronológicamente información de todas las transacciones.

# FIRMA DIGITAL - BLOCKCHAIN

**La tecnología Blockchain es la unión de:**

- ✓ **La tecnología peer to peer o P2P (una red de ordenadores conectados que facilita transacciones entre usuarios)**
- ✓ **La criptografía de clave pública que permite la creación de Internet del Valor**

# FIRMA DIGITAL - BLOCKCHAIN

## ¿Como funciona?

# APLICACIONES FIRMA DIGITAL

Firma en documento electrónico o transacción electrónica destinados al ámbito:

- ✓Comercial
- ✓Laboral
- ✓Impositivo
- ✓Financiero y bancario
- ✓Salud
- ✓Seguros
- ✓Profesional
- ✓Societario
- ✓Administración pública
- ✓Entre otros

# APLICACIONES – RECIBO SUELDO DIGITAL

**Resolución MTEySS Nº 1455/11 y N° 1361/2012**

Establecen requisitos mínimos solicitud recibo sueldo digital ante Secretaria de Trabajo:

- ✓ **El empleado y el empleador deben utilizar firma digital**

- ✓ **Indicar protocolos y estándares tecnológicos usados para garantizar la seguridad, autenticidad, autoría, integridad e inalterabilidad de recibos emitidos bajo la nueva modalidad**


# FIRMA DIGITAL
## Acordadas Corte de Justicia de Salta N° 10.940/12 y 11.918/15

- ✓ Acceso rápido a la información
- ✓ Ahorro de tiempo en el envío de notas y datos que tendrán garantía de integridad y autenticidad evitando la tradicional vía postal o la comunicación telefónica (notificación electrónica entre juzgados y tribunales y las partes de los actos de comunicación)

# FIRMA DIGITAL - EJEMPLOS

## Caso de Firma digital: Caja de Valores SA – Entidades Financieras

**Sistema de comunicaciones seguras (SCS) del Sistema Bursátil Argentino**

**Características del SCS:**

**algoritmo de clave simétrica 3DES (Triple Data Encryption Standard) con cambio automático de clave**

**algoritmo RSA (Rivers, Shamir y Adleman) para manejo de claves asimétricas**

**Tamaño de claves RSA no menor a 1024 bits**

**Método de certificación y firma digital aplicando el algoritmo RSA y la función de hash MD5**

# Conclusiones

**Gran desafío**

- ✓ **Proyectar aspectos de la vida papel transformándose a partir del uso de la firma digital.**
- ✓ **Haciendo mas confiable el comercio y el intercambio de información**

# Fin de la presentación

# Muchas Gracias!!