FIRMA DIGITAL

PARA LA SIMPLIFICACIÓN ADMINISTRATIVA

Sylvain Lesage, Jefe de Unidad Innovación y Desarrollo, ADSIB

Presentación el 08/04/2015 en UTEPSA, Santa Cruz

ADSIB

- Agencia para el Desarrollo de la Sociedad de la Información en Bolivia
- depende de la Vicepresidencia del Estado Plurinacional

En su parte técnica, provee los siguientes servicios:

- Nombres de dominio **nic.bo**
- Entidad Certificadora Pública para la **firma digital**
- Consultoría en desarrollo informático, redes y servidores

SYLVAIN LESAGE

- Jefe de la Unidad Innovación y Desarrollo
- Tel: 2200730 - int 1008
- mail: slesage@adsib.gob.bo

PLAN

1. La firma digital en Bolivia
2. SIESU y tramites en papel
3. Propuesta de simplificación con firma digital

1. LA FIRMA DIGITAL EN BOLIVIA

¿QUÉ ES LA FIRMA DIGITAL?

Es un número calculado por criptografía a partir del contenido del archivo digital. Por ejemplo:

```
iQIcBAEBCAAGBQJU6UamAAoJEMZwSKNoagIrEv8QAIqXg9ET85CNSpGMBvVDbcP/
EN6l5SX0K9IqHpV1L+VTHnL9AoKPzpRa8u7OzxxkPy/JxiJKA1mSkE7uyksy6V19
...
1y+fBFlGTT51AG/PFK2rMAhxb67wnpCkz9z2U1EivcgOLkLQwn9TljdqTxXVnBAa
YmWADd/rdAetDksMgyOi
```

- equivalente de la firma manual, para documentos digitales
- **no se ve**: un documento impreso no lleva la firma digital
- la firma digital solo tiene una existencia en el *mundo digital*

¿QUÉ ES LA FIRMA DIGITAL?

La firma digital asegura:

- la autenticidad
- el no-repudio
- la integridad

¿QUÉ PODEMOS FIRMAR?

Todo archivo o documento digital puede ser firmado:

- PDF, DOC, ODT
- correo electrónico
- foto, vídeo
- software
- protocolos de intercambio / API

A NIVEL TÉCNICO

La firma digital necesita un *par de claves* criptográficos: la clave privada y la clave pública.

La clave privada realiza la firma digital, a partir de un "hash" del documento digital.

La firma digital se distribuye con la clave pública, que permite verificar la firma.

SEGURIDAD

La firma digital implica algunas precauciones:

- secreto absoluto del signatario sobre su clave privada:
  - se recomienda el uso de un token USB
- conservación de los documentos firmados, que solo existen en el mundo digital:
  - facilidad de replicación múltiple
  - *pero* alto riesgo de perdida

INFRAESTRUCTURA DE CLAVE PÚBLICA

Para asegurar la identidad del posesor de una clave pública y de las firmas digitales correspondientes, la Infraestructura de Clave Pública provee un mecanismo de tercer de confianza.

La entidad certificadora verifica cuidadosamente la identidad del posesor de una clave pública, y emite un **certificado digital** que asocia de manera infalsificable la clave pública y la identidad del signatario. Quién confía en la entidad certificadora confía en todas las firmas digitales realizadas con este certificado digital.

INFRAESTRUCTURA DE CLAVE PÚBLICA

Una Infraestructura de Clave Pública tiene una organización jerárquica, con:

- una entidad certificadora raíz, con certificado auto-firmado
- una o varias entidades certificadoras de segundo nivel
- (opcional) una o varias entidades certificadoras de tercer nivel, cuarto nivel...
- (opcional) una o varias autoridades de registro
- los signatarios, que adquieren los certificados

INFRAESTRUCTURA DE CLAVE PÚBLICA DEL ESTADO PLURINACIONAL DE BOLIVIA

La Infraestructura de Clave Pública del Estado Plurinacional de Bolivia tiene una organización jerárquica, con:

- una entidad certificadora raíz: **ATT**
- una entidad certificadora pública: **ADSIB**, y quizás otras entidades certificadoras de segundo nivel privadas
- **ninguna** entidad certificadora de tercer nivel, cuarto nivel...
- quizás una o varias autoridades de registro: ¿SEGIP?, ¿Aduana nacional?, ¿Banco Unión?
- los signatarios

INFRAESTRUCTURA DE CLAVE PÚBLICA DEL ESTADO PLURINACIONAL DE BOLIVIA

La norma establece tres tipos de certificados:

- persona natural
- persona jurídica - para los responsables de las Universidades Privadas
- cargo público - para el Director de Educación Superior

Todos los tipos de certificados son compatibles y permiten firmar digitalmente.

NORMA Y PLAZOS

La firma digital, a través de la Infraestructura de Clave Pública del Estado Plurinacional de Bolivia, tiene **valor legal** según la Ley 164 de agosto de 2011.

La implementación esta en curso. La ATT esta revisando la solicitud de habilitación de la ADSIB como Entidad Certificadora Pública.

Fecha de inicio de servicio de la Entidad Certificadora Pública: estimada a la mitad del año 2015

2. SIESU Y TRAMITES EN PAPEL

SIESU

El SIESU (**http://siesu.minedu.gob.bo/**) es el sistema de habilitación a examen de grado del Viceministerio de Educación Superior para las universidades privadas.

Permite agilizar el tramite, pero que todavía queda una gran cantidad de papel y mucho trabajo manual de revisión.

LISTA DE DOCUMENTOS DE LA CARPETA DE CADA ESTUDIANTE

La carpeta de un estudiante contiene:

- 1 - certificado de nacimiento original
- 2 - cédula de identidad simple fotocopia
- 3 - Titulo de bachiller legalizado por la dirección departamental de educación
- 4 - Resolución Ministerial de autorización y funcionamiento de la Universidad y carrera por esta Cartera de Estado simple fotocopia

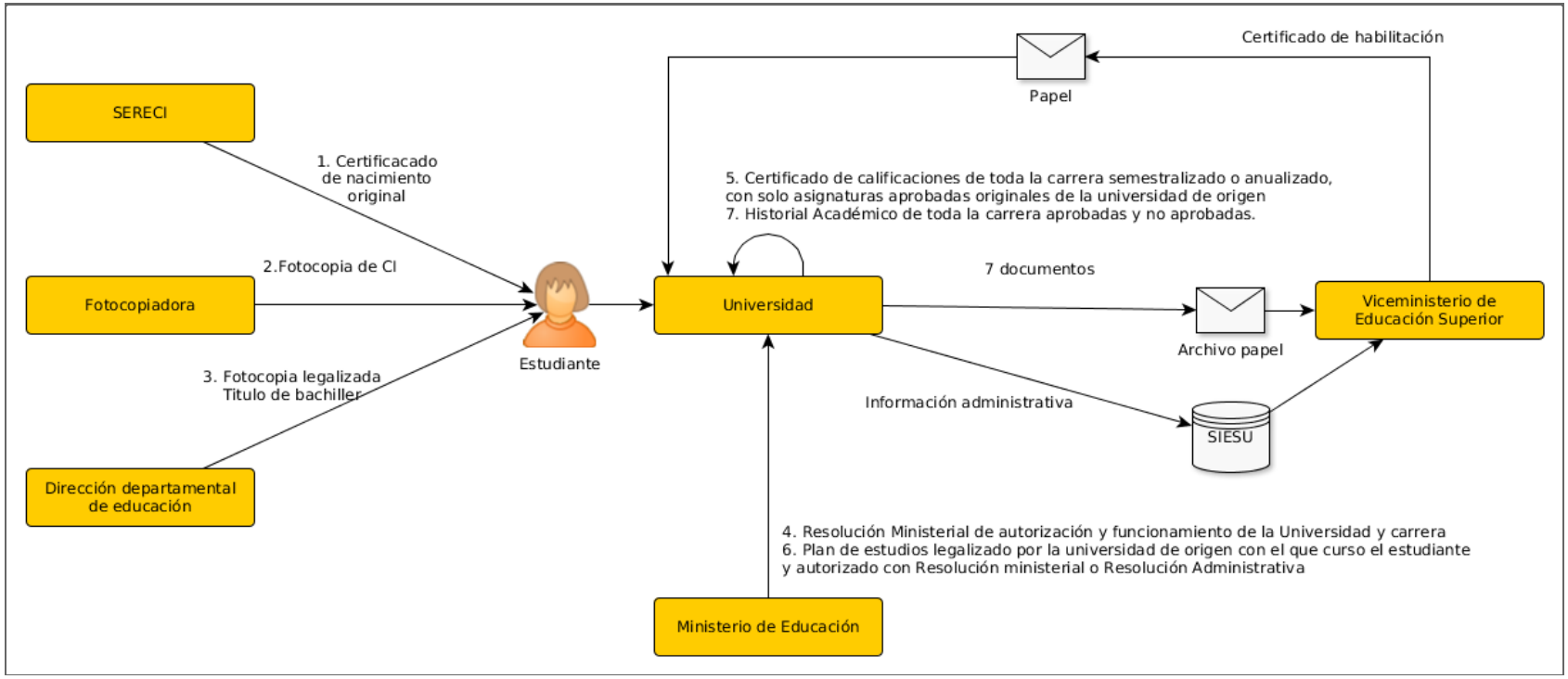
LISTA DE DOCUMENTOS DE LA CARPETA DE CADA ESTUDIANTE

La carpeta de un estudiante contiene:

- 5 - Certificado de calificaciones de toda la carrera semestralizado o anualizado, con solo asignaturas aprobadas originales de la universidad de origen
- 6 - Plan de estudios legalizado por la universidad de origen con el que curso el estudiante y autorizado con Resolución ministerial o Resolución Administrativa
- 7 - Historial Académico de toda la carrera aprobadas y no aprobadas.

Si el estudiante ha cambiado de universidad, se requieren 6 documentos adicionales.

TRAMITE ACTUAL PARA HABILITACIÓN A EXAMEN DE GRADO



USO DEL SIESU POR LAS UNIVERSIDADES

Una universidad utiliza el sistema de la siguiente forma:

1. llena el formulario de un estudiante
2. imprime la carta de solicitud de habilitación (firmada físicamente por el rector o delegado), la lista de formularios, y el formulario de solicitud para cada estudiante (firmado por el rector y los dos responsables de llenado y habilitación de la universidad)
3. envía físicamente la carpeta de cada estudiante, con la carta, el formulario y el respaldo

USO DEL SIESU POR EL VICEMINISTERIO DE EDUCACIÓN SUPERIOR

El Viceministerio utiliza el sistema de la siguiente forma:

1. verifica cada solicitud de habilitación: observado o validado
2. imprime la carta de habilitación, para firma del director de educación superior (4 ejemplares)
3. manda la carta de habilitación a la universidad

PROBLEMAS IDENTIFICADOS

- el estudiante debe realizar varios tramites
- todos los documentos están entregados en papel (solo una parte de la información administrativa esta manejada por el SIESU)
- se realiza mucho trabajo de verificación de manera manual
- el Viceministerio pide resoluciones emitidas por el mismo Ministerio

3. PROPUESTA DE SIMPLIFICACIÓN CON FIRMA DIGITAL

PROPUESTA PARA CADA PROBLEMA

Problema: el estudiante debe realizar varios tramites

Propuesta: ningún tramite realizado por el estudiante, gracias a una mejor sistematización de los documentos y una mejor interconexión entre sistemas

PROPUESTA PARA CADA PROBLEMA

Problema: todos los documentos están entregados en papel

Propuesta: remplazar los documentos papel por:

- **un sistema**:
  - CI: desde la API del SEGIP
  - Resolución ministerial, Plan de estudios, Certificado de calificaciones: desde nuevos sistemas del Ministerio
- **un documento digital firmado digitalmente**: formulario de solicitud de habilitación, generado por el SIESU
- **desaparición**: certificado de nacimiento se vuelve innecesario si SEGIP certifica la CI

PROPUESTA PARA CADA PROBLEMA

Problema: se realiza mucho trabajo de verificación de manera manual

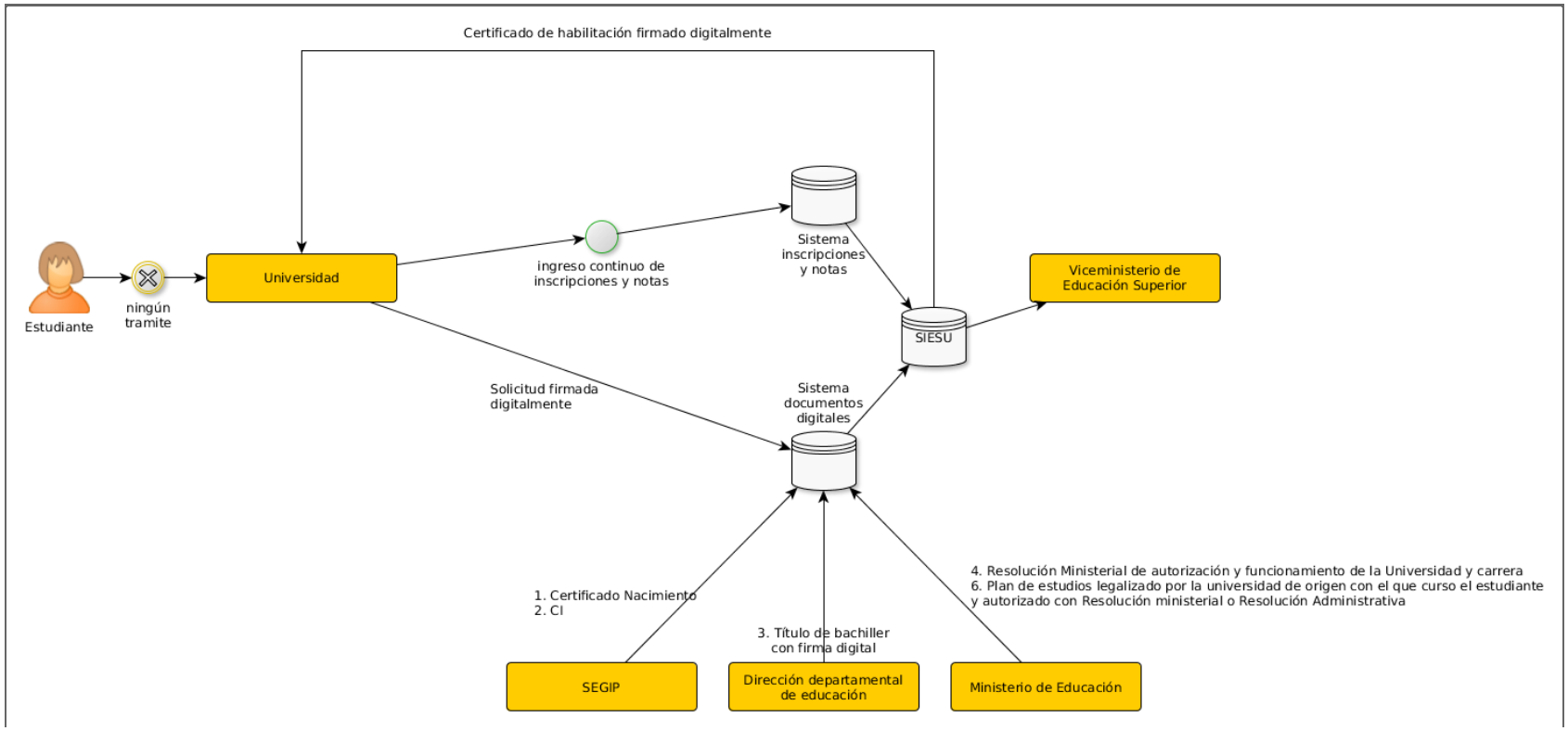
Propuesta: verificación automática cruzando los datos de varios sistemas. La verificación manual se limitaría a los casos complicados u observados.

PROPUESTA PARA CADA PROBLEMA

Problema: el Viceministerio pide resoluciones emitidas por el mismo Ministerio

Propuesta: elaboración de un sistema de publicación de todas las resoluciones ministeriales, y interconexión con el SIESU

TRAMITE CON LA SOLUCIÓN PROPUESTA



DETALLE: SISTEMA DE REGISTRO DE NOTAS

Implementar un sistema de registro de todas las notas de los estudiantes.

Permite remplazar los requisitos 5. (certificado de calificaciones) y 7. (historial académico) por un simple archivo firmado digitalmente. Este archivo puede ser importado en el sistema SIESU y procesado automáticamente para verificar las notas y aprobaciones.

DETALLE: SISTEMA DE MATERIAS

El requisito 6. (plan de estudio) puede ser remplazado por un sistema de materias.

En este sistema las universidades llenan todo el detalle de sus materias. El plan de estudio se genera automáticamente a partir de este sistema, se puede firma digitalmente por el responsable de la universidad, y mandar e incorporar al SIESU automáticamente.

DETALLE: SISTEMA DE RESOLUCIONES MINISTERIALES

El requisito 4. (Resolución Ministerial de autorización y funcionamiento de la Universidad y carrera) puede ser remplazado por un sistema de gestión documental de las resoluciones emitidas por el Ministerio.

DETALLE: API DEL SEGIP

Los requisitos 1. (certificado de nacimiento) y 2. (cédula de identidad) pueden ser remplazados por una consulta al servicio web del SEGIP.

DETALLE: SISTEMA DE TÍTULOS

El requisito 3. (Título de bachiller legalizado por la dirección departamental de educación) es quizás más complicado de sistematizar.

Sin embargo, se puede elaborar un sistema de títulos que registre todos los nuevos títulos de bachiller. De esta forma, en el transcurso de los años, el requisito 3. será remplazado para la mayoría de los estudiantes por un acceso directo al sistema de títulos.

DETALLE: DOCUMENTOS DIGITALES MIXTOS

Para todos los nuevos sistemas, se propone elaborar documentos mixtos en formato PDF:

- parte visible que se puede imprimir - para auditoría por ejemplo
- parte invisible con datos codificados - para importación y procesamiento automático por los sistemas

DETALLE: DOCUMENTOS DIGITALES MIXTOS

Por ejemplo, para el certificado de calificaciones:

- la parte visible presenta una tabla de calificaciones
- la parte invisible incorpora los mismos datos en formato CSV o JSON
- la parte invisible puede incorporar también la firma digital

FIN