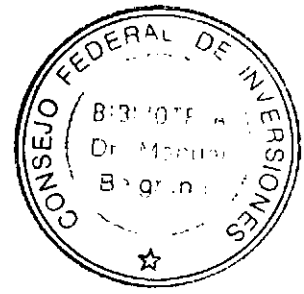
GOBIERNO DE MENDOZA

SECRETARÍA ADMINISTRATIVA LEGAL Y TÉCNICA

UNIDAD DE REFORMA DEL ESTADO

2º informe parcial



CONSEJO FEDERAL DE INVERSIONES

CONSULTOR: LIC. PABLO GUILLERMO LIOY

Fecha de impresión 29/11/2004 10:59

ÍNDICE

I. Introducción

Se presentan a continuación, como 2º informe parcial, las actividades y tareas desarrolladas en el marco de planificación del proyecto de Firma Digital Mendoza.

Actividad	Estado
2. Implementación de experiencia piloto en la DGE:	Concluida
•Identificación de la necesidad: se recopila y analiza información sobre el problema, se entrevista a los posibles usuarios y se precisa la necesidad de aplicación de tecnología de firma digital	Concluida
•Análisis del sistema: se releva el circuito actual, y se define el alcance de la experiencia piloto	Concluida
•Diseño de la implementación: se elabora el diseño conceptual de la experiencia piloto	Concluida
•Desarrollo e implementación: se lleva a la práctica la experiencia piloto real. Se emiten los certificados de firma digital, se realizan las configuraciones, instalación de protocolos, ajustes y desarrollos necesarios en el equipamiento informático	Concluida
•Prueba del Sistema: se elabora y se pone en práctica un Plan de Pruebas	Concluida

•Puesta en Marcha de la implementación: el sistema existente se reemplaza por el nuevo mejorado y se capacita a los usuarios	Concluida
•Evaluación de la experiencia: se definen métricas de evaluación que a futuro permitirán evaluar el éxito de la implementación	Concluida

2º informe parcial: la culminación de la actividad 2 se presentará a los cuatro meses de iniciadas las tareas.

II. Implementación de Experiencia Piloto en la DGE:

A partir de nuestra estrategia de difusión del proyecto y a través de las herramientas de interacción con la demanda local incluidas en nuestra página Web, estamos comenzando a dar respuestas a las necesidades de implementación de tecnología de firma digital en el ámbito de los procesos del sistema de planta funcional de recursos humanos de la DGE (Dirección General de Escuelas)

A. Identificación de la necesidad:

A través de las entrevistas con los responsables del circuito administrativo en cuestión se plantea el problema a solucionar desde el del tipo de información que se manipula.

Información: datos referidos a antigüedad del personal de la DGE

Partiendo de la base que la información es un recurso que, como el resto de los activos, tiene valor y por consiguiente debe ser debidamente protegida surge la necesidad de valorarla según su sensibilidad y criticidad.

Para clasificar este Activo de Información, utilizaremos los criterios ya definidos en los siguientes niveles:

1 – SIN CLASIFICAR	Información de dominio público que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de la dependencia o no.

2-RESERVADA-USO INTERNO	Información que puede ser conocida y utilizada por todos los empleados y algunos colaboradores externos autorizados, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la dependencia.
3 - RESERVADA - CONFIDENCIAL	Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas, materiales o de imagen.
4 - RESERVADA - SECRETA	Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección, y cuya divulgación o uso no autorizados podría ocasionar graves pérdidas materiales o de imagen.

Consideramos a este tipo de información Reservada y Confidencial ya que representa un componente esencial en el proceso de liquidación de sueldos al personal y su manipulación negligente podría provocar:

- daños a los titulares con las consiguientes acciones legales en perjuicio de la dependencia.
- Liquidaciones "infladas" con la consiguiente pérdida de dinero para el Estado.

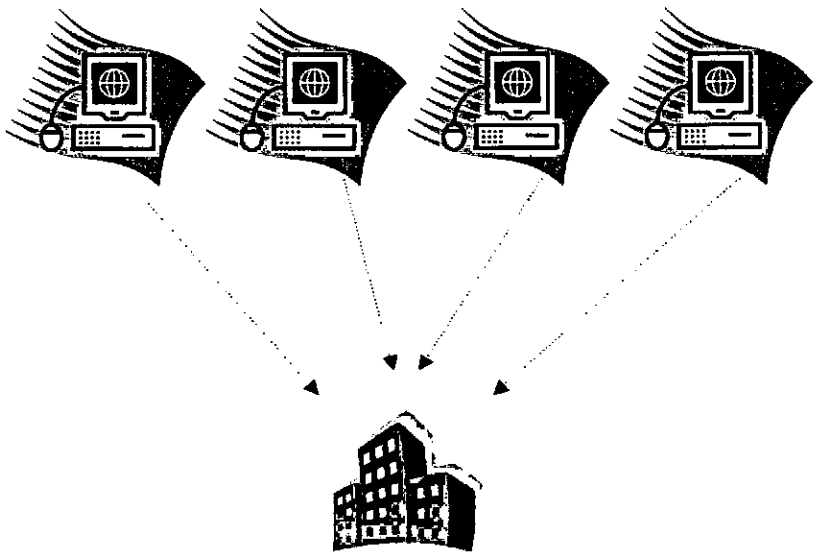
Por otro lado, debemos tener en cuenta la naturaleza descentralizada del circuito ya que la información viaja desde delegaciones administrativas repartidas por el territorio de la provincia hacia la Administración central situada en la capital de Mendoza:

- Delegación Este.
  Comprende: San Martín, Junín, Rivadavia, Santa Rosa y La Paz

- Delegación Centro Sur.
  Comprende: Tupungato, Tunuyán y San Carlos

- Delegación Sur-Oeste:
  Comprende: General Alvear y Malargüe

- Delegación Sur
  Comprende: San Rafael



Por ello nuestro objetivo es:

Proteger la información de antigüedad del personal de la DGE y la tecnología utilizada para su transmisión, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información manipulada en el circuito.

En este caso la información adopta muchas formas, tanto en los sistemas como fuera de ellos. Puede ser:

- Almacenada, en los sistemas o en medios portátiles.
- Transmitida, a través de redes o entre sistemas.
- Impresa o escrita, en papel.

Entonces, la ***transmisión segura de datos sensibles*** para liquidación de sueldos en el sistema de planta funcional de recursos humanos de la DGE, ***parece ser el problema a resolver.***

Analizamos el problema a través de nuestra estrategia de identificación de procedimientos y precisamos detalladamente la necesidad de aplicación de tecnología de firma digital en este circuito:

Estrategia para la Identificación de Procedimientos Aptos

Casi cualquier tipo de transacciones electrónicas puede requerir los niveles de seguridad que provee la tecnología de firma digital, sin embargo es importante hacer una adecuada elección del alcance y los ámbitos de aplicación de los servicios de criptografía asimétrica para lograr ahorros y no incurrir en sobrecostos de implementación:

Guías de aplicación

- Privacidad, integridad y autenticación de la información: la administración pública quiere utilizar Internet como un canal de comunicaciones entre sus ministerios o dependencias, o entre ella y sus administrados en la prestación de los servicios públicos. Tales comunicaciones pueden estar en variedad de formas tales como correo electrónico, normativa interna, documentos, trámites, declaraciones juradas y, es muy frecuente que contengan información confidencial y con propiedad intelectual. Lograr que tales comunicaciones no se encuentren expuestas a falsificaciones o adulteraciones es una cuestión de alta prioridad.
- Ahorros y reducción de tiempos en el trabajo de oficina: la administración pública debe procesar documentos firmados y luego archivarlos por un período de tiempo extendido para satisfacer las disposiciones legales. Con la finalidad de reducir los costos de almacenamiento, soporte, procesamiento y archivo del trabajo de oficina resulta deseable reemplazar los documentos firmados en forma hológrafa con documentos firmados digitalmente.

Tales guías resultan aplicables para el caso ya que consideramos a la transmisión de la información de antigüedad de Recursos Humanos de la DGE como una transacción que reviste importancia desde el carácter sensible de la información en cuestión y por el alto volumen en papel firmado en forma hológrafa que se maneja.

Criterios de selección de circuitos administrativos

- Trámites con alta frecuencia de repetición a cargo de la misma oficina, ente o persona: en este caso las delegaciones administrativas deben remitir con una periodicidad deseable no mayor a 15 días la actualización de información de antigüedad a la Administración Central.

- Circuitos que requieren autenticación de las partes involucradas: resulta muy importante poder identificar al responsable o jefe de la delegación que transmite o firma la información de antigüedad, asegurando unívocamente que es quién dice ser y no otra persona.

- Circuitos administrativos que enlazan importantes distancias geográficas: sin duda este criterio se torna muy importante para el circuito en cuestión, ya que algunas delegaciones se encuentran muy alejadas de la Administración Central.

- Circuitos administrativos de transferencia de información sensible: como lo es la información relativa a la antigüedad del personal de la DGE

- Circuitos basados en gran cantidad de papeleo: si tenemos en cuenta la cantidad de personal, del cual se procesa información con en las delegaciones administrativas de la DGE, alrededor de 1700 docentes, apreciamos el gran volumen de información en papel que se maneja.

Criterios de selección de transacciones aptas para ser firmadas digitalmente

- Aquellas que requieren efectiva autenticación de personas o entes involucrados en la transacción: en este caso se requiere la efectiva autenticación de las personas involucradas en las transmisión de la información, el emisor (las delegaciones) y el receptor (la Administración Central)

- Aquellas que autorizan subsidios o prestaciones sociales de ayuda o liquidaciones: en este caso la información de antigüedad en cuestión es insumo directo del proceso de liquidación de sueldos.

Criterios de selección de transacciones aptas para ser encriptadas

- Aquellas que contengan información estrictamente confidencial: de acuerdo con la clasificación de la información que ya realizamos resulta necesario disponer de los medios tecnológicos de cifrado de información en este circuito.

Tales pautas fundamentan la necesidad de la aplicación de tecnologías de firma digital y son el marco conceptual a tener en cuenta a la hora de analizar y definir particularmente la aplicación de cara a los potenciales beneficios y ahorros que puede producir.

B. Análisis del sistema:

Presentamos a continuación el relevamiento del circuito administrativo actual de transferencia de información de Antigüedad desde las Delegaciones Administrativas hacia la Administración Central.

Descripción del Procedimiento:

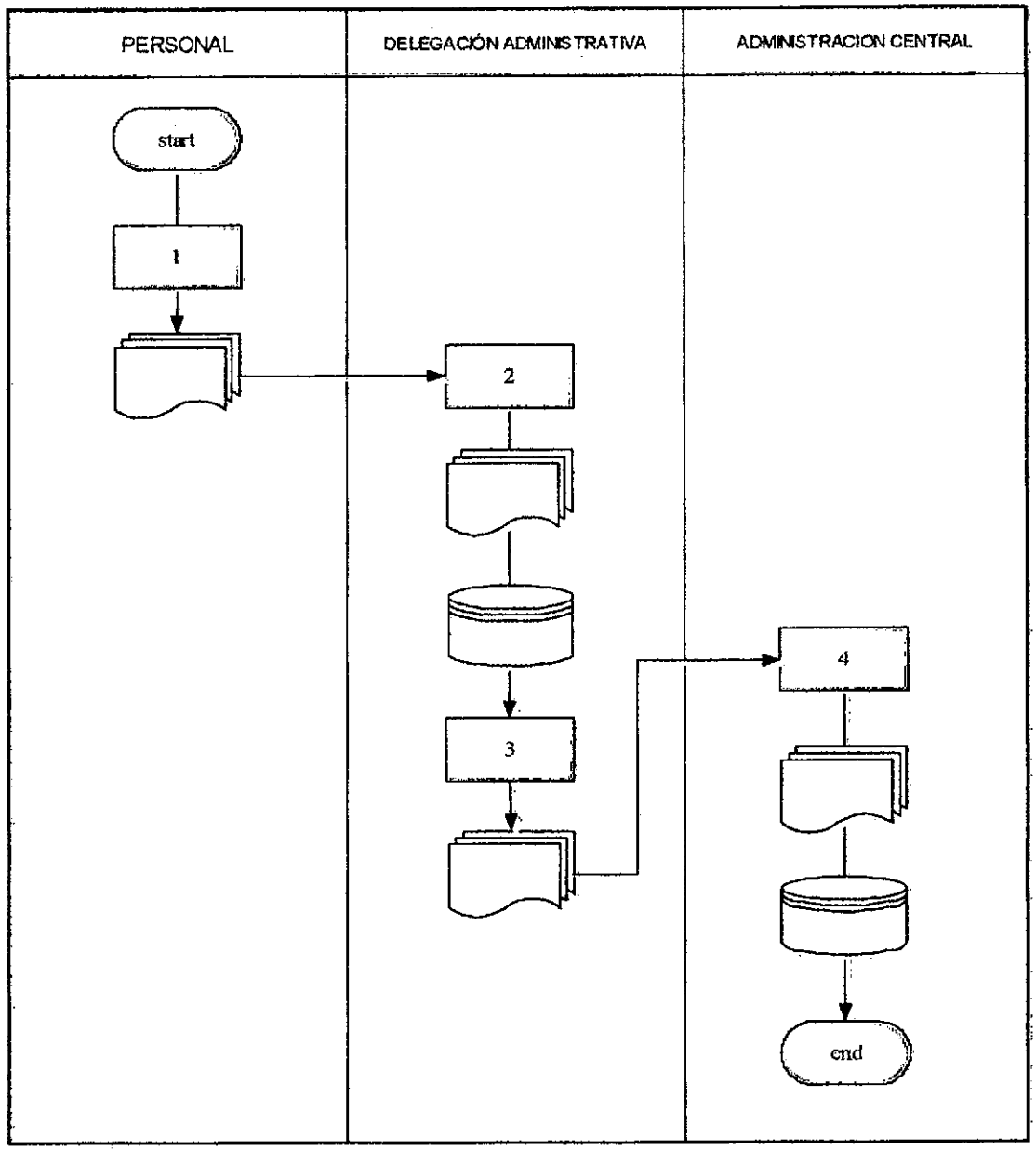
1. ***Personal:*** se presenta ante el Responsable de la Delegación Administrativa con la información actualizada de su antigüedad (antecedentes), acreditada por los establecimientos educativos en los que ha prestado servicio.

2. ***Delegación Administrativa:*** el responsable de la Delegación recibe la información de antigüedad acompañada de la documentación que la acredita, y toma nota de las fechas "desde y hasta" de cada caso se carga en el sistema de recursos humanos y se determina la antigüedad total, ésta se anota en un Parte de Antigüedad.

3. ***Delegación Administrativa:*** el responsable de la Delegación firma y envía todos los Martes por Bolsa de OCA los partes de Antigüedad a la Administración Central.

4. ***Administración Central:*** el responsable recibe los partes de Antigüedad y carga en el Sistema Informático de Recursos Humanos que calcula el monto de liquidación por antigüedad.

Diagrama del Procedimiento



El procedimiento actual, como se puede ver, presenta inconsistencias entre su completa informatización y el soporte papel. Estas inconsistencias vienen dadas fundamentalmente por la necesidad de estampar una firma hológrafa del responsable de la delegación en los partes de antigüedad, a su vez, la necesidad real de esta firma radica en la criticidad de la información que se transmite.

Con la aplicación de tecnologías de firma digital en estos procedimientos podríamos:

- Lograr celeridad y seguridad en la transmisión de datos
- Eliminar la duplicidad del trabajo de carga de información
- Cumplir con las exigencias de calidad de la información a transmitir: oportunidad, integridad, autoría y confidencialidad.
- Generar ahorros de traslado
- Asegurar la identidad tanto del emisor como del receptor de la información

C. Diseño de la implementación:

De acuerdo con la identificación de la necesidad básica y el relevamiento del circuito actual hemos elaborado el diseño conceptual de la experiencia a través de tres alternativas

Procedimiento de transmisión de información del sistema de Recursos Humanos de la DGE

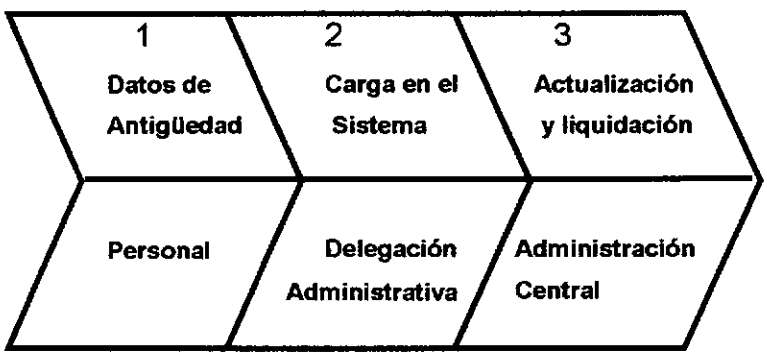
El presente procedimiento describe el conjunto de pasos a realizar por el personal de las Delegaciones Administrativas y la Administración Central de la DGE en la transmisión de información referente a antigüedad del personal para alimentar el sistema de Recursos Humanos.

El circuito se puede esquematizar en las siguientes etapas:

Secuencia Sintética del Proceso

(Arrow chart)

Etapas



Principal sector interviniente

Objetivo:

A través de la redacción de este procedimiento se busca formalizar las tareas que lo conforman y fortalecer el diseño administrativo con la implementación de la tecnología de firma digital en el mismo. Además, se busca asegurar garantías de integridad de la información transmitida y de autenticación de los responsables involucrados.

Alcance:

Este procedimiento es de aplicación en las Delegaciones Administrativas:

- Delegación Este.
  Comprende: San Martín, Junín, Rivadavia, Santa Rosa y La Paz
  Domicilio: 9 de Julio y Paso de Los Andes - San Martín

- Delegación Centro Sur:
  Comprende: Tupungato, Tunuyán y San Carlos
  Domicilio: San Martín y Dalmau – Tunuyán

- Delegación Sur-Oeste:
  Comprende: General Alvear y Malargüe
  Domicilio: Italia 295 - General Alvear

- Delegación Sur
  Comprende: San Rafael
  Domicilio: Cmte. Salas y Alsina

y la Administración Central de la Dirección General de Escuelas de la provincia de Mendoza situada en La Casa de Gobierno Peltier 351 Ala Este.

Definición de Roles

Para el cumplimiento de sus funciones en este procedimiento se definen los siguientes roles:

- Delegación Este.
  Responsable: a designar

- Delegación Centro Sur:
  Responsable: Cont. Ana Lo Giudice
  DNI. No.: 16109518

- Delegación Sur-Oeste:
  Responsable: Prof. Myrna Osorio
  DNI. No.: 18534255

- Delegación Sur
  Responsable: Cont. Elizabeth Masi
  DNI. No.: 16459689

- Administración Central
  Responsable: Marcela Vargas

Descripción del Procedimiento (alternativa I):

1. ***Personal:*** se presenta ante el Responsable de la Delegación Administrativa con la información actualizada de su antigüedad (antecedentes), acreditada por los establecimientos educativos en los que ha prestado servicio.

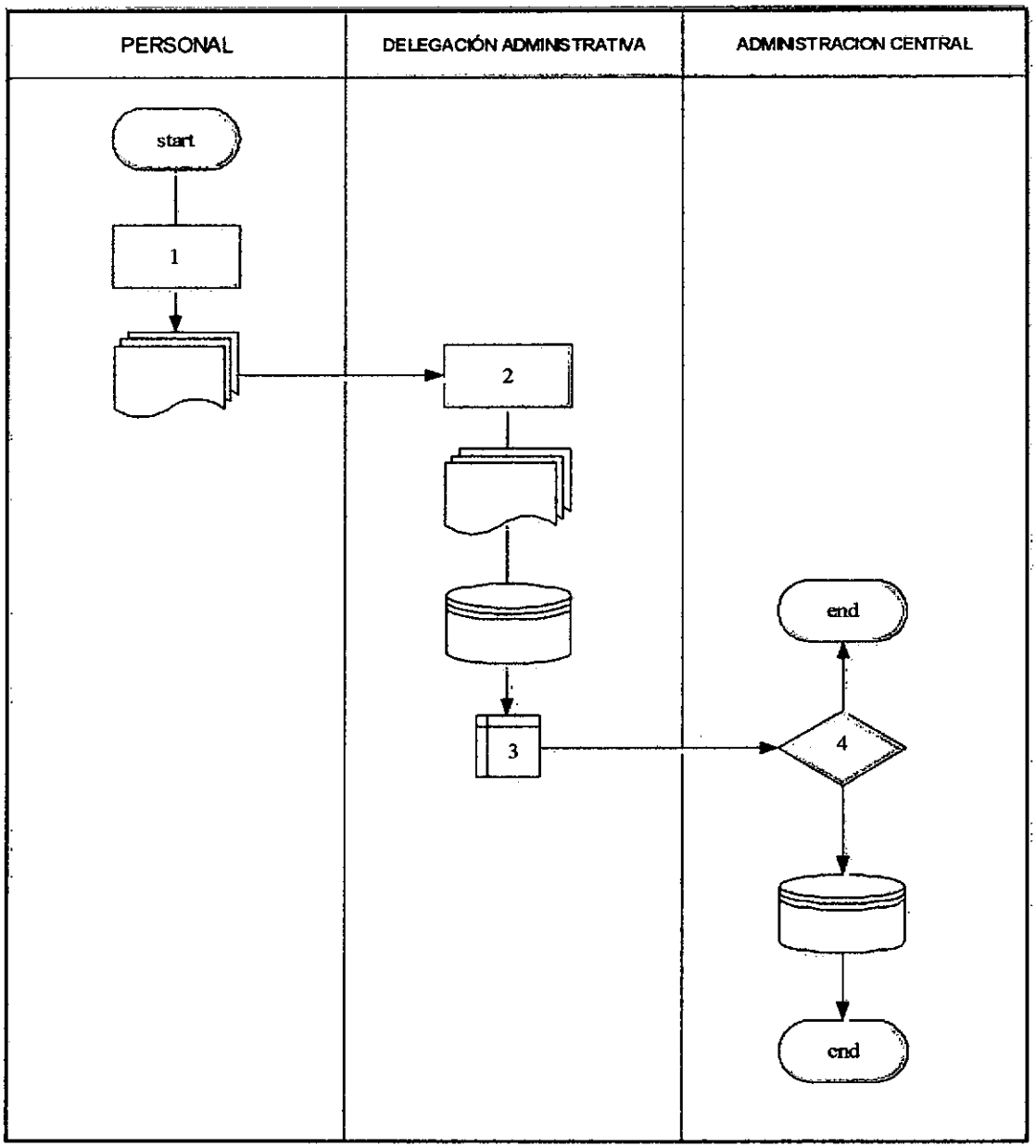
2. ***Delegación Administrativa:*** el responsable de la Delegación recibe la información de antigüedad acompañada de la documentación que la

acredita, y la carga en el Sistema Informático de Recursos Humanos de la DGE.

3. ***Delegación Administrativa:*** el responsable de la Delegación con una periodicidad no superior a los 15 días, variable en función del volumen de información recibido, emite a través del Sistema Informático de Recursos Humanos las tablas digitales de datos correspondientes a los movimientos realizados. Posteriormente se conecta a un Sitio Seguro, hosteado en la Administración Central, que le pedirá que se autentique a través de un certificado digital a su nombre.

4. ***Administración Central:*** Luego, si la autenticación es correcta, el sitio le permitirá subir los archivos de actualización de antigüedad y firmarlos digitalmente. Automáticamente, si todo es correcto, el sistema se actualiza y calcula el monto de liquidación por antigüedad. Posteriormente el responsable de la Administración Central controla el proceso y realiza actividades de mantenimiento tanto del Sistema Informático de Recursos Humanos como de su interfaz Web para transmisión segura de datos desde la Delegaciones Administrativas.

Diagrama del Procedimiento



Flowchart Alternativa I

Descripción del Procedimiento (alternativa II):

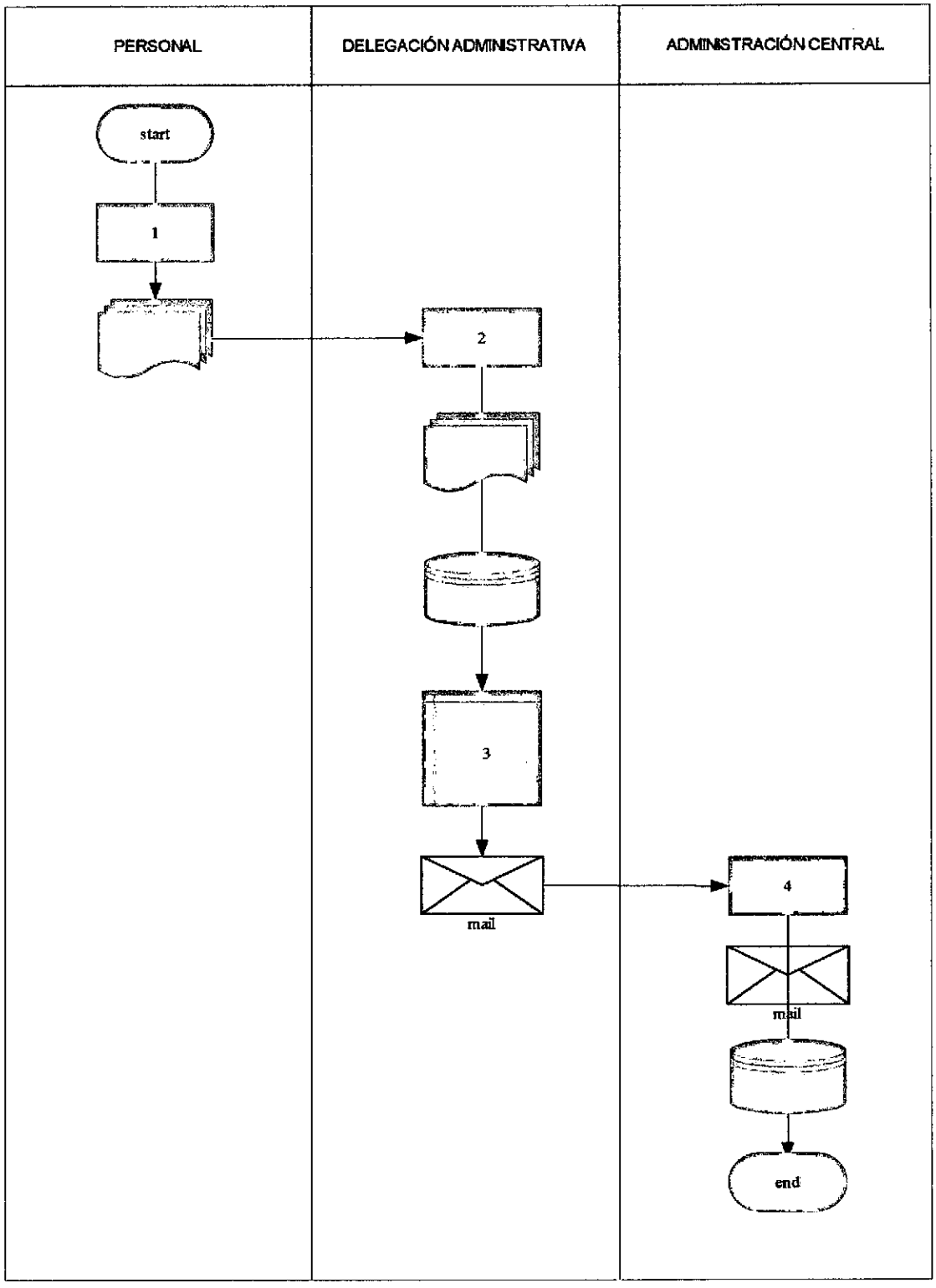
1. ***Personal:*** se presenta ante el Responsable de la Delegación Administrativa con la información actualizada de su antigüedad (antecedentes), acreditada por los establecimientos educativos en los que ha prestado servicio.

2. ***Delegación Administrativa:*** el responsable de la Delegación recibe la información de antigüedad acompañada de la documentación que la acredita, y la carga en el Sistema Informático de Recursos Humanos de la DGE.

3. ***Delegación Administrativa:*** el responsable de la Delegación con una periodicidad no superior a los 15 días, variable en función del volumen de información recibido, emite a través del Sistema Informático de Recursos Humanos las tablas digitales de datos correspondientes a los movimientos realizados. Posteriormente, firma los archivos digitales y los cifra haciendo uso de su certificado digital. Finalmente los envía a la Administración Central por Correo electrónico.

4. ***Administración Central:*** el responsable recibe los archivos firmados y cifrados vía correo electrónico, actualiza el Sistema y calcula el monto de liquidación por antigüedad.

Diagrama del Procedimiento



Flowchart Alternativa II

Descripción del Procedimiento (alternativa III):

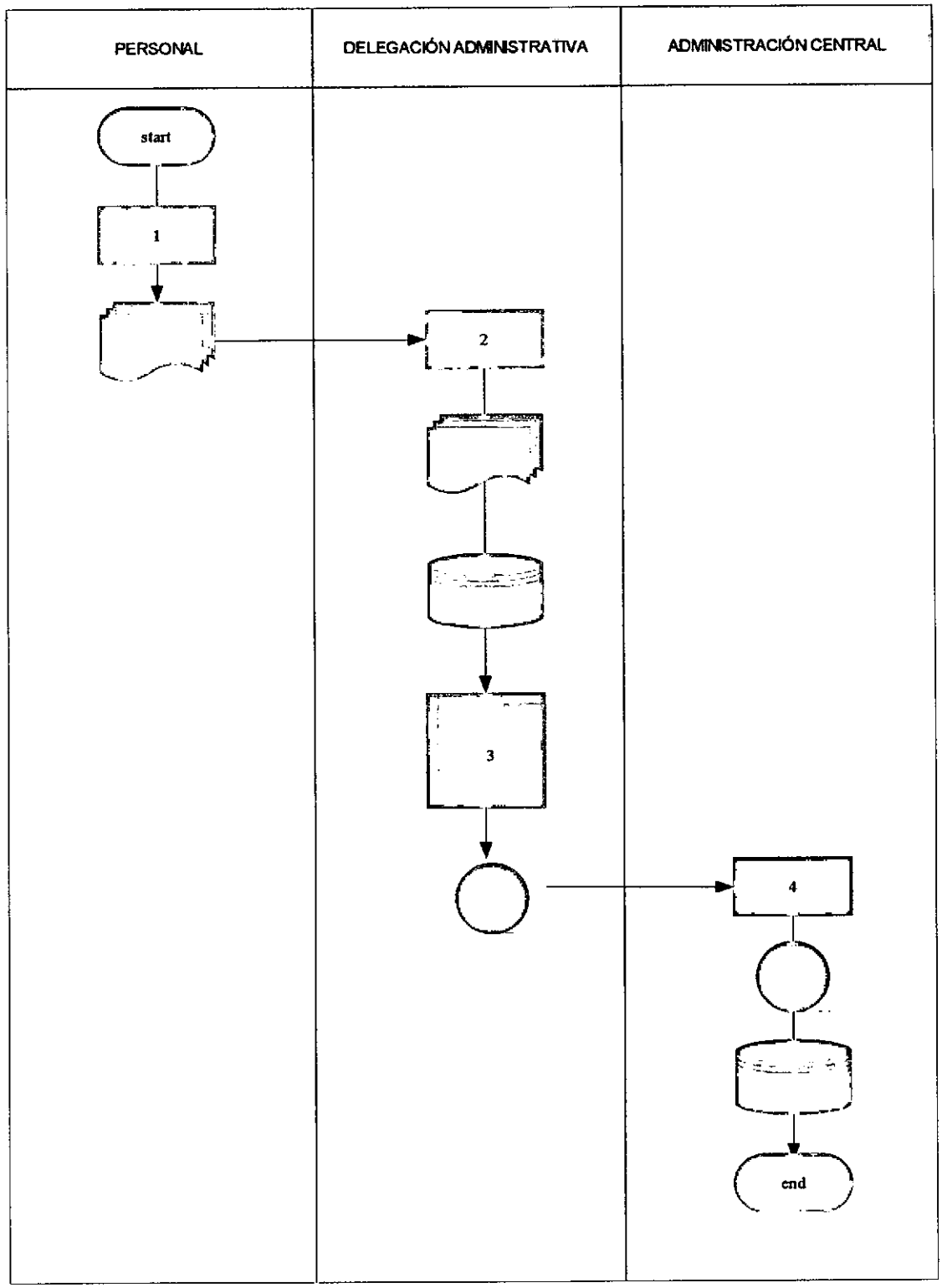
1. ***Personal:*** se presenta ante el Responsable de la Delegación Administrativa con la información actualizada de su antigüedad (antecedentes), acreditada por los establecimientos educativos en los que ha prestado servicio.

2. ***Delegación Administrativa:*** el responsable de la Delegación recibe la información de antigüedad acompañada de la documentación que la acredita, y la carga en el Sistema Informático de Recursos Humanos de la DGE.

3. ***Delegación Administrativa:*** el responsable de la Delegación con una periodicidad no superior a los 15 días, variable en función del volumen de información recibido, emite a través del Sistema Informático de Recursos Humanos las tablas digitales de datos correspondientes a los movimientos realizados. Posteriormente, firma los archivos digitales y los cifra haciendo uso de su certificado digital. Finalmente los graba en un dispositivo magnético externo y envía a la Administración Central por Bolsa.

4. ***Administración Central:*** el responsable recibe los dispositivos magnéticos, extrae los archivos firmados y cifrados, actualiza el Sistema y calcula el monto de liquidación por antigüedad.

Diagrama del Procedimiento



Flowchart Alternativa III

D. Desarrollo e implementación:

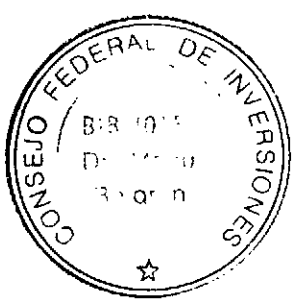
En la etapa de análisis y diseño evaluamos distintas alternativas de desarrollo e implementación del circuito de gestión y transferencia de información relativa a la liquidación de antigüedad docente desde las Delegaciones Administrativas hasta la Administración Central de la DGE.

Considerando la ***Alternativa I*** como curso de acción óptimo se emprendió el desarrollo de las aplicaciones informáticas pertinentes en cooperación con el equipo técnico de la Dirección de Tecnologías de la Información de la DGE.

Las tareas de desarrollo realizadas tuvieron como objetivo disponer de una solución tecnológica que con el uso de la firma digital permita:

- Prescindir totalmente del soporte impreso de información relativa a altas, modificaciones y reclamos relativos a la liquidación de antigüedad docente en todo el ámbito provincial y para todos los niveles educativos.
- Descentralizar el proceso de carga, gestión y consulta de información relativa a liquidación de antigüedad docente, aprovechando la existencia de Delegaciones Administrativas descentralizadas y los beneficios que las nuevas tecnologías aportan para el acceso y traspaso de datos, sin perder garantías en cuanto a integridad de la información y la responsabilidad por su administración.
- Contar con un mecanismo de transferencia de archivos informáticos (documentos de texto, bases de datos, planillas de cálculo, etc.), firmados digitalmente; de forma de promover la descentralización incremental de información sensible para la gestión escolar.

En este sentido se trabajó en el desarrollo de las siguientes aplicaciones informáticas.



TED Tool de extracción de actualizaciones en bases de datos locales

TFD Aplicación de firma digital

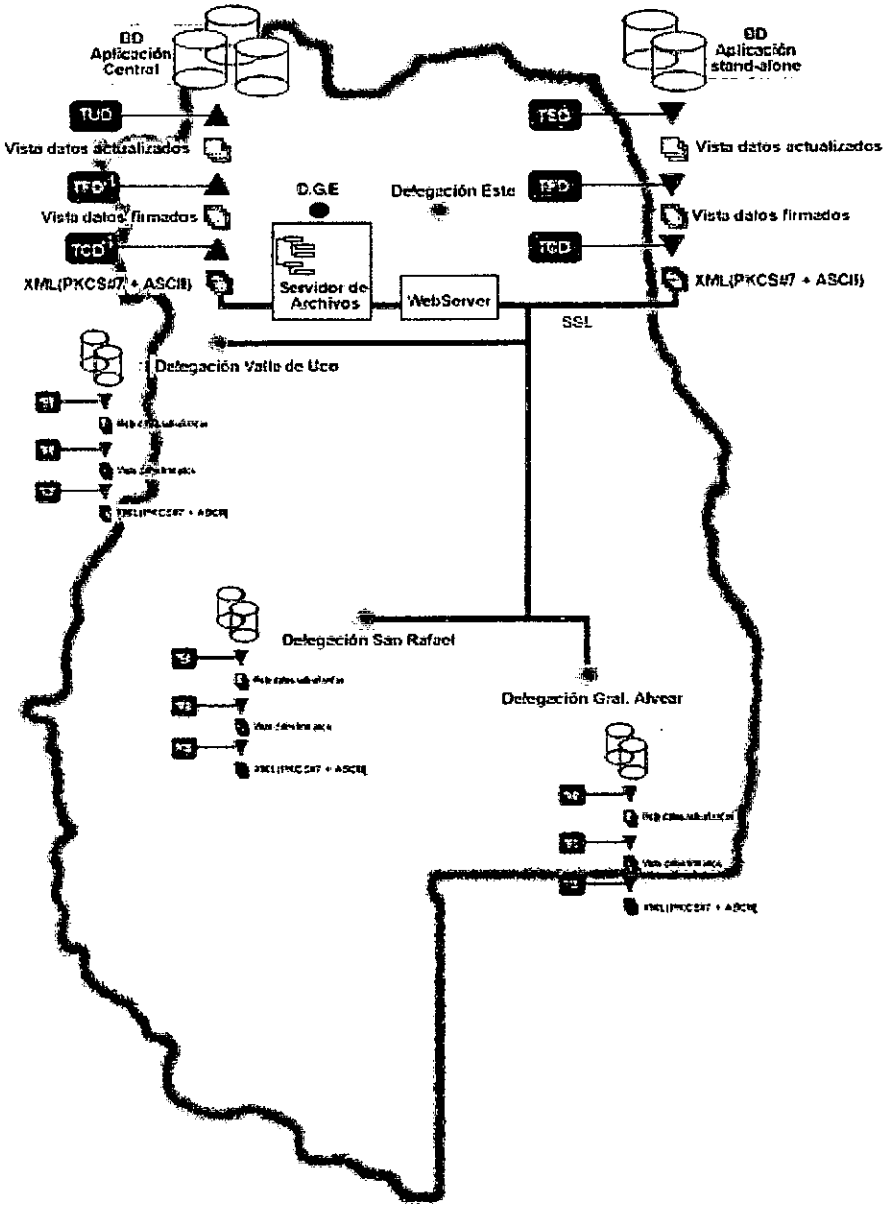
TCD Aplicación de encapsulamiento de datos criptográficos

TCD^{-1} Aplicación de extracción de firma y certificados

TFD^{-1} Aplicación de verificación de firma

TUD Tool de update de actualizaciones a la base de datos central

Estas aplicaciones, que constituyen la columna vertebral de la solución tecnológica, se incorporan al siguiente modelo operativo del circuito digital.



Se documenta a continuación la descripción de cada uno de los módulos. Seguidamente se explica como se integran en una solución tecnológica adecuada para el circuito operativo.

TED – Tool de Extracción de Datos

Las Delegaciones Administrativas en las que se descentraliza la gestión escolar tienen instalada las aplicaciones del Sistema de Gestión de RR.HH. y una copia local de la Base de Datos del Sistema con la información de su zona necesaria para operar.

TED es el módulo de software encargado de extraer de la Base Local de cada delegación una vista con los datos de antigüedad docente actualizados con posterioridad a la fecha de última remisión de datos.

TED extrae un archivo de texto plano ASCII con el extracto de información y lo almacena en un directorio local dispuesto a tal fin.

Según lo establece el procedimiento dispuesto el archivo se denominará de acuerdo al siguiente formato.

ant + ddmmaa + CodigoDelegación

Donde ***ant*** es un prefijo que indica que la información refiere al circuito de liquidación de antigüedad docente, ***ddmmaa*** representa la fecha en que se realiza la extracción de la vista de datos y ***CodigoDelegación*** es un número de dos dígitos que identifica la Delegación Administrativa a la que pertenecen los datos.

El directorio establecido por procedimiento debe respetar la estructura:

Esta metodología de formato, denominación y estructura de archivos se establece con fines de normalizar el procedimiento previendo que en un futuro se aplique a la transferencia de otra información de gestión descentralizada tal como novedades de sueldo, alta de servicios, notas, etc.

TFD – Aplicación de Firma de Datos

TFD es el módulo de software encargado de firmar digitalmente el archivo ASCII con el extracto de información generado por TED.

Con el objetivo de garantizar interoperabilidad con los principales manejadores de firma y encripción de archivos, TFD utiliza los algoritmos estándar de hash y firma digital Md5/RSA.

La firma se construye de la siguiente forma: el módulo de software aplica el algoritmo de hash sobre el archivo de texto (algoritmo matemático unidireccional, es decir, lo encriptado no se puede desencriptar), obteniendo un extracto de longitud fija, y absolutamente específico para ese mensaje. Un mínimo cambio en el mensaje produciría un digesto completamente diferente, y por tanto no correspondería con el que originalmente firmó el responsable de ejecutar el proceso. El algoritmo hash utilizado para esta función es MD5. Eventualmente TFD está preparado para aplicar el algoritmo de hash SHA-1, otro de los estándares más aplicados. El extracto conseguido, cuya longitud oscila entre 128 y 160 bits (según el algoritmo utilizado), se somete a continuación a cifrado mediante la clave privada del responsable. Este es un procedimiento de encriptación asimétrica que se logra mediante la aplicación del algoritmo RSA. En nuestro contexto aplicamos claves RSA de 1024 bits. De esta forma obtenemos un extracto final cifrado con la clave privada del responsable de la Delegación.

Es importante observar que TFD está implementado en un applet java que opera localmente en la máquina del firmante. Es una condición sumamente importante que todo el proceso de firma se concrete de forma standalone y bajo completo control del firmante. TFD garantiza este requerimiento.

***TCD* - Aplicación de encapsulamiento de datos criptográficos**

La firma y el digesto firmado (hash md5 o sha-1 del archivo ASCII firmado) se encapsulan en un objeto PKCS#7 junto al certificado X.509 del firmante y el certificado de Autoridad Certificante de la ONTI.

El estándar PKCS#7 define la sintaxis general para mensajes que incluyen información criptográfica como firmas digitales y datos cifrados. Un objeto PKCS#7 encapsula la información codificándola en formato BER.

La ventaja de utilizar el estándar PKCS#7 para encapsular los datos firmados es que este formato puede ser interpretado por la mayoría de las herramientas comerciales de criptografía de clave pública. Mantener interoperabilidad con los principales manejadores de firma y encripción de archivos es fundamental para que eventualmente la firma pueda ser verificada por herramientas estándares e independientes.

El objeto PKCS#7 con el digesto firmado y los certificados X.509 correspondientes, codificados en BASE64, se incluyen junto al archivo ASCII en blanco en un único archivo basado en un lenguaje de etiquetas XML. Este archivo actúa como contenedor de los datos y de la firma correspondiente y es el archivo digital que se transmite desde las Delegaciones Administrativas hasta la Administración Central.

TCD^{-1} Aplicación de extracción de firma y certificados

Este módulo tiene la capacidad de extraer del archivo XML contenedor, el objeto PKCS#7 y la tabla ASCII en claro.

De igual forma extrae la firma MD5/RSA, el certificado X.509 del firmante y su cadena de certificación desde el objeto PKCS#7 y entrega todos los componentes al módulo de Verificación de Firma.

TFD-1 Aplicación de verificación de firma

La función de verificación de firma es la encargada de comprobar la autenticidad y validez de la firma digital. Para ello, el módulo trabaja sobre los componentes de información proporcionados por TCD-1: el archivo ASCII con la información en claro, su firma digital y el certificado de clave pública del firmante. En primer lugar, descifra la firma digital utilizando la clave pública extraída del certificado en cuestión y obtiene el valor de hash que calculó TFD al momento de aplicar la firma. Por otra parte utiliza el mismo algoritmo

de hash (MD5) que utilizó TFD y lo aplica al archivo de texto ASCII recibido; de esta forma obtiene otro valor de hash. Si ambos números de hash coinciden entonces se puede garantizar la integridad de la información contenida en el archivo ASCII. Si no coinciden el archivo ASCII ha sido alterado y TFD^{-1} informará inmediatamente esta situación al usuario mediante un mensaje de advertencia.

En el mismo procedimiento se valida la autoría de la firma ya que para poder obtener el número de hash calculado por el firmante (TFD) es necesario descifrar la firma digital con la clave pública que se corresponde con la única clave privada capaz de producir esa firma. Por lo tanto el propietario de esa clave pública, que es quien figura en el certificado recibido, es la única persona capaz de haber producido esa firma.

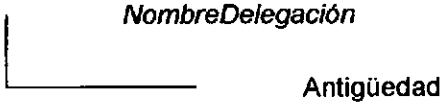
Al momento de ejecutar el procedimiento de verificación de firma, TFD^{-1} emite una llamada al servidor de la Autoridad Certificante de la ONTI para cotejar contra la última CRL (Certificate Revocation List) emitida, la validez del Certificado de Clave pública que avala la identidad del firmante.

TUD Tool de update de actualizaciones a la base de datos central

La Dirección de Tecnologías de la Información de la DGE. centraliza toda la información vinculada a la gestión escolar de la provincia. En los servidores de esta administración central se encuentran instaladas las aplicaciones del Sistema de Gestión de RR.HH. y la Base de Datos Maestra del Sistema. Esta base integra la información recibida desde todas las Delegaciones Administrativas.

TUD es el módulo de software encargado de incorporar a la Base de Datos central la información de antigüedad docente, contenida en el archivo ASCII, previamente validado, que se recibe desde cada una de las Delegaciones Administrativas.

Según lo establece el procedimiento dispuesto, TUD recorre la estructura de directorios.



Y de esta estructura recupera el archivo ASCII cuya estructura de nombre coincide con el formato ***ant + ddmmaa + CodigoDelegación.***

Solución Tecnológica Integral

Los módulos anteriores se han implementado como la capa de aplicación de un desarrollo Web que constituye la solución tecnológica adoptada como alternativa. Como puede verse en el modelo, los usuarios en las delegaciones acceden a una internase Web con tecnología de sitio seguro SSL instalada en los servidores de la Administración Central y desde allí ejecutan la actualización a la base de datos central. Para el usuario son transparentes los detalles de operación de cada uno de los módulos. Es la aplicación quien se encarga de concatenar las llamadas sucesivas de módulos y pasar la información generada por cada módulo al siguiente. El usuario solo deberá indicar que va a realizar una actualización, revisar el extracto de información que se propone firmar y realizar el procedimiento de firma digital de esa información. A partir de allí operarán los módulos de encapsulamiento y transferencia de la información firmada hasta el servidor de archivos de la Administración Central. En este punto un usuario autorizado es quien valida la firma de los archivos recibidos e impacta las actualizaciones sobre la base de datos central.

En el servidor de archivos quedarán copias digitales de los archivos recibidos desde las delegaciones con fines de comprobación posterior. Además los logs del sistema y bases de datos, registran accesos desde los

clientes, transacciones realizadas, conexiones a la CRL, y otra información de control necesaria para garantizar la seguridad y trazabilidad de las operaciones realizadas.

Los módulos, planteados en esta primera versión como Java Beans y applets basados en la Plataforma de Seguridad Java que se acceden desde una internase Web, podrían eventualmente trabajarse como plugins del sistema de RR.HH. desarrollado por DGE. o montarse sobre una aplicación independiente y portable. Esta portabilidad de los módulos que constituyen la capa de aplicación, garantiza la escalabilidad e interoperabilidad del sistema y su futura adaptación a los requerimientos del proceso de descentralización de la gestión escolar.

E. Prueba del Sistema:

Documentamos a continuación el ***Conjunto de Pruebas*** que se realizaron sobre las aplicaciones informáticas desarrolladas. Estas pruebas se realizaron previo a comenzar las instancias de capacitación e implementación, de forma tal de detectar a priori posibles fallas a nivel de interfase, integridad de datos, control de acceso o aplicación de estándares. Cabe aclarar que las pruebas instrumentadas tenían como principal objetivo garantizar un adecuado grado de ***tolerancia a fallas*** del sistema, tanto en los aspectos vinculados a la plataforma de hardware y software, como a las fallas que pueden producirse por errores humanos en su operación.

De acuerdo a su orientación, dividimos las pruebas en tres tipos:

a. Pruebas operativas del sistema

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
Control de acceso de usuarios	Validar los esquemas de control de acceso a nivel de usuarios, de forma de garantizar que sólo ingresen	▪ Intento de acceso al sitio seguro por canal http no seguro. ▪ Emisión de Certificados Digitales de prueba. ▪ Inclusión de Certificados de prueba en el reposi-	Se comprobó el correcto funcionamiento de los esquemas de control de acceso con autenticación de cliente en el sitio seguro.

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
	al sitio seguro usuarios autorizados de las delegaciones administrativas o de la Administración Central.	torio de Certificados del sitio seguro. ▪ Intentos de ingreso con Certificados válidos. ▪ Intentos de acceso con Certificados no válidos. ▪ Comprobación de access-logs.	
Manejo de sesiones y logs de transacciones	Comprobar la correcta apertura, mantenimiento y cierre de las sesiones iniciadas en los browsers clientes. Verificar la correcta registración en logs de transacciones de sesiones iniciadas y su duración, con fines	▪ Apertura de múltiples sesiones desde un mismo cliente. ▪ Cierre de sesiones desde una ventana de browser, manteniendo otras conexiones abiertas. ▪ Apertura de sesiones desde distintos clientes, con el mismo usuario. ▪ Apertura de sesiones y cierre de aplicaciones sin cerrar sesión. ▪ Seguimientos y comprobación de logs man-	Se comprobó el correcto funcionamiento de los esquemas de mantenimiento de sesiones. El sistema maneja adecuadamente la apertura de múltiples sesiones y el cierre de conexiones abiertas.

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
	de seguimiento y auditoría.	tenidos por el Application Server y por logs de transacciones del motor de base de datos.	
Prueba de extracción de datos TED	Medir la tasa de fallas en intentos de generación de vistas sobre las tablas de bases locales. Medir porcentaje de extracciones correctas e incorrectas frente a distintos parámetros de volumen de datos extraídos.	▪ Prueba de volumen. ▪ Introducción explícita de errores en los parámetros de extracción.	No se detectaron fallas en el funcionamiento del módulo. Frente a fallas forzadas del módulo o los parámetros de conexión se comprobó el correcto disparo, captura y manejo de excepciones por parte de la aplicación.
Prueba de firma de datos TFD	Medir la tasa de fallas de usuarios en	▪ Firma de múltiples archivos con distintas extensiones, formatos y	No se detectaron fallas en el funcionamiento del módulo.

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
	intentos de generación de firma sobre archivos en distintos formatos.	atributos de acceso. ▪ Intentos de Firma con certificados válidos y no válidos	Frente a fallas forzadas del módulo o los certificados se comprobó el correcto disparo, captura y manejo de excepciones por parte de la aplicación.
Manejo de excepciones	Garantizar el correcto manejo de errores en el sistema.	▪ Introducción explícita de fallas y errores en puntos de control de código y en esquemas operativos de la plataforma, para generar excepciones SQL, excepciones en peticiones al Application Server y excepciones en la construcción de objetos.	La corrida de pruebas se ejecutó con resultados exitosos.
Mensajes de error y advertencia.	Comprobar la claridad y pertinencia de	▪ Establecimiento de puntos de control sobre el código de manejo de excepciones.	Se comprobó la pertinencia en la aparición de mensajes de error y adver-

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
	los mensajes de error y/o advertencia	▪ Revisión sobre la sintaxis de mensajes. ▪ Corridas de pruebas con conjuntos de datos erróneos para forzar la aparición de mensajes. ▪ Ejecución de pruebas aleatorias, para testear el correcto manejo de errores y su identificación mediante mensajes.	tencia. Se corrigieron errores de redacción sobre los textos de mensajes para favorecer su correcta interpretación.
Prueba de menús	Comprobar la correcta vinculación de procesos y selección de menús	▪ Comprobación puntual de cada acceso, mensajes de guía y titulaciones. ▪ Navegación programada de la aplicación por rutas de menús alternativos.	La prueba fue exitosa en todos sus aspectos.
Prueba de verificación de firma TFD^{-1}	Garantizar el buen funcionamiento de la aplicación de verifi-	▪ Prueba sobre múltiples archivos firmados, en distintos formatos, con distintos algoritmos de firma y con distintos cer-	No se detectaron fallas en el funcionamiento del módulo. El módulo de verificación informó

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
	cación de firma.	tificados. ▪ Prueba de verificación sin conectividad a la CRL. ▪ Prueba de verificación de firma con certificados vencidos. ▪ Prueba de verificación de firma con certificados revocados. ▪ Prueba de verificación de firma sobre objetos PKCS#7 que no incluyen la cadena de certificación.	correctamente de todas las situaciones en las que una firma, el certificado del firmante o la integridad del documento pudiera estar comprometida.

b. **Pruebas sobre estándares criptográficos**

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
Testear adaptabilidad del software al estándar X509 v3 y PKIX (RFC3280)	Evaluar características básicas de adaptación a distintas configuraciones de certificados X.509	▪ Se configuraron distintos perfiles de Certificados y se emitieron certificados bajo estos perfiles y en distintos formatos. ▪ Se importaron los certificados emitidos en aplicaciones browsers IE y Netscape y en la máquina virtual java JRE1.5. ▪ Se emitieron distintas versiones de CRL. ▪ Se accedió a través de funciones criptográficas a la información de los campos de los certificados emitidos, de acuerdo a la estructura propuesta por el estándar X509 v3.	Los módulos operan adecuadamente con los certificados X.509 que se ajustan a las recomendaciones de la RFC3280 y a las recomendaciones de la ONTI.

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
Verificación con herramientas independientes.	Garantizar la compatibilidad de las firmas generadas y encapsuladas en objetos PKCS#7 con otras herramientas de verificación.	• Se aplicaron tres softwares de apertura y verificación de PKCS#7 independientes sobre los objetos generados por la aplicación.	Las firmas pudieron ser verificadas correctamente con las herramientas externas.
Comprobación de certificados contra puntos de acceso a la CRL.	Garantizar la correcta conexión a puntos de distribución de la CRL y la comprobación del certificado del firmante contra la CRL.	• Se verificó a partir del seguimiento de conexiones establecidas mediante un firewall, las llamadas de CRL realizadas en cada procedimiento de verificación de firma. • Se registraron las descargas de actualización de CRL.	La validación de Certificados contra la CRL actualizada se concretó en todos los casos correctamente.
Comprobación de algoritmos de firma md5withRSAEncryption y Sha1RSA contemplados	Evaluar la generación de firma y su verificación con los algoritmos estándar más aplicados.	• Se firmaron 5 archivos ASCII con firma MD5/RSA • Se firmaron 5 archivos ASCII con firma SHA1/RSA	La aplicación soporta correctamente la generación y verificación de firma con ambos algoritmos. Por defecto se usarán firmas MD5/RSA,

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
en la RFC3279.		• Se encapsularon las firmas, digesto y certificados en objetos PKCS#7. • Se verificaron las firmas con TFD^{-1} • Se verificaron las firmas con herramientas independientes.	ya que los certificados emitidos por la ONTI adoptan este algoritmo de firma.

c. Pruebas de compresión y transferencia de datos

<table>
<tr><th>Descripción de la Prueba</th><th>Objetivo de la Prueba</th><th>Ejecución de la Prueba</th><th>Resultados/Conclusiones</th></tr>
<tr><td>Índices de compresión de la información cifrada y firmada.</td><td>Evaluar los tamaños medios de archivos a transferir por el canal SSL.</td><td>Se firmaron y cifraron archivos en distintos formatos con tamaños que oscilaban entre 40Kb y 252Kb. Se cifró con algoritmo RSA.</td><td>
<table>
<tr><th>Formato</th><th>Tamaño RSA en Kb.</th><th>Tamaño Original en Kb.</th></tr>
<tr><td>.doc</td><td>13</td><td>40</td></tr>
<tr><td>.xls</td><td>22</td><td>69</td></tr>
<tr><td>.rtf</td><td>21</td><td>101</td></tr>
<tr><td>.dbf</td><td>28</td><td>252</td></tr>
</table>
</td></tr>
<tr><td>Firma y cifrado de archivos grandes</td><td>Evaluar restricciones de tamaño ante tablas eventualmente muy grandes</td><td>Se firmaron y cifraron archivos .avi y .dbf de gran tamaño.</td><td>
<table>
<tr><th></th><th>Tamaño</th><th>Satisfactorio</th></tr>
<tr><td>.avi</td><td>290 Mb</td><td>SI</td></tr>
<tr><td>.dbf</td><td>5 Mb</td><td>SI</td></tr>
</table>
</td></tr>
</table>

Pasos de ejecución de Pruebas

Se realizaron las pruebas siguiendo los siguientes pasos para su ejecución:

Paso 1: Se prepararon tres máquinas con las siguientes configuraciones de prueba

1. JRE 1.5 con librería BouncyCastle para Windows 98/ME, Sistema de RR.HH. stand-alone y Browser IE 5.0 .
2. JRE 1.5 con librería BouncyCastle para Windows XP/2000, Sistema de RR.HH. stand-alone. Browser IE 5.0 y Netscape 4.0
3. Web Server, Application Server y Servidor de Archivos funcionando sobre un servidor central de DGE con plataforma Linux/Apache/Tomcat.

Paso 2: Se confeccionó una planilla de documentación de pruebas, para conducir la ejecución de las validaciones previstas

Paso 3: Se seleccionó un conjunto de archivos con diversos formatos y características especiales para someterlos a las pruebas diseñadas. Se diseñaron el conjunto de datos de prueba y se generaron los certificados de prueba tanto para usuarios finales como de servidor.

Paso 4: Se ejecutaron las pruebas previstas y se documentaron los resultados en la planilla diseñada para tal fin.

F. Puesta en marcha de la implementación

Concretada la etapa de pruebas se emprendió la implementación efectiva de la aplicación en las distintas Delegaciones Administrativas y en la Administración Central.

Para ello se visitaron las cuatro delegaciones y se trabajó con los responsables de cada Delegación Administrativa y un representante de la Dirección de Tecnologías de la Información de la DGE. Se fijaron pautas en cuanto a responsabilidades asumidas, procedimientos de trabajo y controles.

Veamos las principales características del proceso de implementación:

Objetivo: El período de implementación y capacitación tuvo como objetivo iniciar el funcionamiento del nuevo circuito de gestión de información vinculada a antigüedad docente en el ámbito de la DGE.

Alcance: La implementación inicial aspira a la puesta en marcha de la dinámica del circuito, logrando el mejor impacto posible sobre las personas y procesos involucrados.

En esta instancia se realizaron las siguientes actividades:

1. Definiciones finales sobre la metodología de implementación y puesta en marcha

Por los alcances legales de los certificados de firma digital involucrados en el proceso y por ser una experiencia preliminar, se decidió en esta instancia, adoptar una metodología de implementación en ***paralelo*** al circuito actual, mantenimiento en primera instancia las copias en papel que circulan según el procedimiento descrito. Esta forma de implementación, permitirá además medir el impacto de la introducción del nuevo circuito en comparación con las prácticas habituales.

2. Asignación de recursos y responsables

Se designaron 2 empleados de cada delegación, el responsable de la delegación y un suplente para ser capacitados y colaborar con la implementación del circuito.

Estas personas se desempeñaron durante la etapa de implementación, con el soporte permanente del equipo de desarrollo de firma digital y bajo el control del responsable designado por la Administración Central.

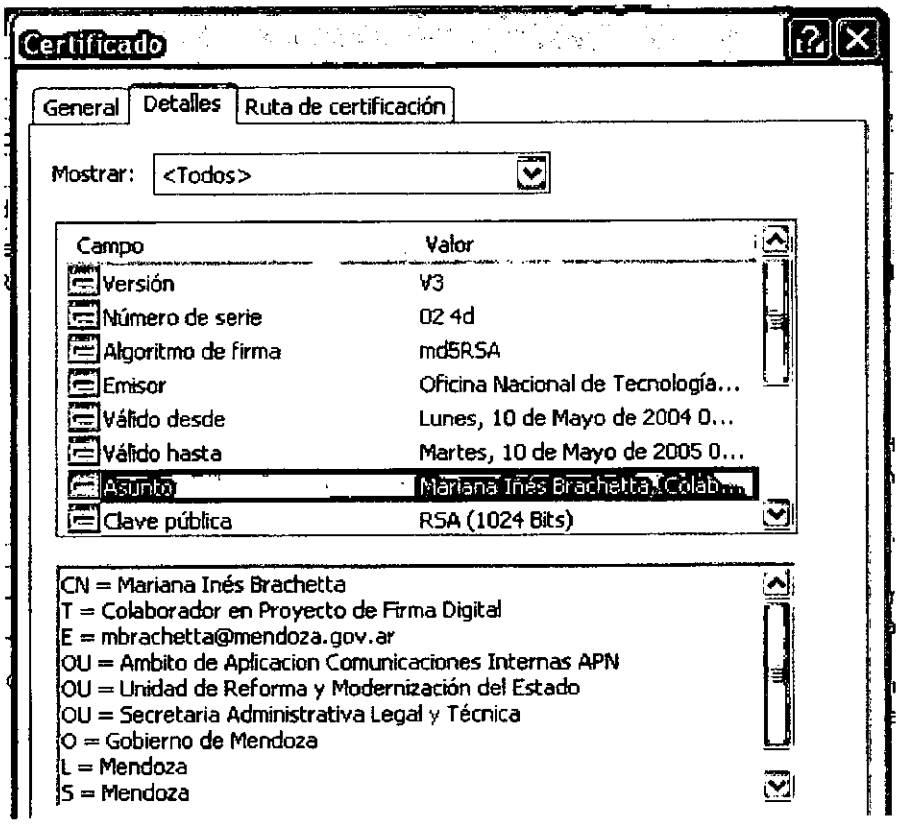
Para la implementación del circuito se dispone en cada Delegación de los siguientes recursos.

- 1 PC con sistema operativo Windows 98.
- 1 conexión dial-up o ADSL a Internet.
- Sistema de RR.HH. de la DGE. instalado en forma stand-alone
- Certificados Digitales.
- Disco de backup.

Este equipamiento no requirió inversión alguna debido a que constituyen recursos de los que disponían previamente las delegaciones.

3. Provisión de Certificados de firma digital a responsables

A través de la Autoridad de Registro de la ONTI, constituida en la Unidad de Reforma y Modernización del Estado, se proveyó de Certificados Digitales con capacidades de firma digital a los responsables de la carga y administración del sistema de RR.HH. de DGE (1 responsable en cada Delegación Administrativa). También se proveyó un certificado al responsable de la Administración Central con firma autorizada (Jefe de Sistemas de la Dirección de Tecnologías de la Información). En esta primera etapa se emitieron 5 certificados digitales a tal efecto. Se emitió también el certificad SSL para el sitio seguro. Se adjunta a continuación una imagen del Certificado de Administrador de Sitio.



4. *Capacitación de responsables*

Se realizó un adiestramiento intensivo de los responsables en una jornada de 4 hs. realizada en la Administración Central, tanto en los aspectos operativos del sistema, como en la toma de conciencia sobre la mejora de procesos y principios básicos introducidos por el circuito digital.

5. Puesta en marcha del circuito

Una vez capacitados los responsables se inició el proceso de remisión de información firmada sobre actualizaciones a las tablas de antigüedad del Sistema de RR.HH. de la DGE. El esfuerzo en esta etapa, de acuerdo al objetivo de implementación planteado, no radicó en el volumen de información

descentralizada, sino en la puesta en marcha y ajuste de la dinámica de sistemas, de forma tal de garantizar la continuidad e independencia de su ciclo de vida en el tiempo.

6. Soporte continuo y retroalimentación al sistema

Las etapas de capacitación y puesta en marcha, constituyen en toda implementación oportunidades de prueba funcional del sistema. De estas etapas, se obtiene en general retroalimentación para los diseñadores y desarrolladores, en función de la experiencia que aportan los actores involucrados en su operación y uso.

En nuestro caso particular, la interacción permanente de los expertos del proyecto de firma digital con los responsables del desarrollo del Sistema de RR.HH. de la DGE y los responsable designados en cada Delegación Administrativa, aportó a: vencer la resistencia al cambio, cubrir dudas operativas que surgieron durante la etapa de operación inicial y fundamentalmente a identificar necesarios ajustes sobre el desarrollo de las herramientas informáticas el circuito operativo.

G. Evaluación de la experiencia:

Se definen métricas de evaluación que a futuro permitirán evaluar el éxito de la implementación.

Indicadores críticos

La siguiente tabla define los indicadores generales utilizados para medir el rendimiento de la experiencia con enfoque en los procesos de las aplicaciones específicas.

Experiencia DGE (Mediciones realizadas al 26/11/04)	
Indicadores Cualitativos	**Métricas y Resultados**
Satisfacción de los usuarios: # Quejas y Reclamos	No se han registrado quejas por el sistema de Sitio Seguro
Marco legal: Documentación de la experiencia	Procedimiento de transmisión de información del sistema de Recursos Humanos de la DGE
Alcance: Participación de los sectores relacionados	Delegación Este: San Martín, Junín, Rivadavia, Santa Rosa y La Paz Delegación Centro Sur: Tupungato, Tunuyán y San Carlos Delegación Sur-Oeste: General Alvear y Malargüe Delegación Sur: San Rafael

Indicadores Cuantitativos	Métricas y Resultados
Eficiencia:	
% de certificados emitidos correctamente	100 % (4 personales y 1 de servidor)
# de fallas del sistema	0 (No se produjeron fallas)
# de interrupciones del servicio	1 (corte de luz 2 horas)
Asistencia:	
# de actores capacitados	10 (diez) Responsables y suplentes
# de asistencias otorgadas	15 (quince) Acciones de asistencia técnica
% de asistencias exitosas	100%
Uso del Sistema:	
% de utilización de servicios	100% de accesos con certificado
# de comunicaciones seguras establecidas	8
% información transferida con éxito	100% (no se reportan fallas)
Acciones correctivas detectadas	**Acciones correctivas implementadas**
No se han detectado hasta la fecha	Ninguna

Calificación ponderada final

Implementación exitosa de la experiencia piloto