GOBIERNO DE MENDOZA
SECRETARÍA ADMINISTRATIVA LEGAL Y TÉCNICA
UNIDAD DE REFORMA DEL ESTADO

firma Digital

Informe Final

CONSEJO FEDERAL DE INVERSIONES
CONSULTOR: LIC. PABLO GUILLERMO LIOY

Fecha de impresión 28/03/2005 11:07

Mendoza, 29 de marzo del 2005

SR SECRETARIO GENERAL DEL
CONSEJO FEDERAL DE INVERSIONES
ING. JUAN JOSE CIÁCERA

Me dirijo a Ud. a efectos de presentar el Informe Final correspondiente a las tareas ejecutadas en el marco del Proyecto de ***"Firma Digital"***

Detalle de Tareas
Se presentan las actividades y tareas desarrolladas en el marco de planificación del proyecto de Firma Digital Mendoza.

1. ***Extensión de la Experiencia Piloto de Repositorio de Normas Legales con Firma Digital:***
    - Soporte continuo: se respondió a los requerimientos de soporte de los usuarios y operadores del sistema.
    - Seguridad y backup: se planificó y desarrolló procedimientos y mecanismos de seguridad preventiva y correctiva a nivel físico y lógico sobre los datos contenidos en el repositorio.
    - Mantenimiento del ciclo de vida del sistema: se garantizó la dinámica, flexibilidad y escalabilidad del sistema a través de la retroalimentación y actualización permanente.
    - Carga de datos históricos: se desarrolló y aplicó un procedimiento de carga masiva de documentos para incorporar al repositorio el volumen de datos necesarios para satisfacer necesidades de consulta e integración de datos.
2. ***Implementación de experiencia piloto en la DGE:***
    - Identificación de la necesidad: se recopiló y analizó información sobre el problema, se entrevistó a los posibles usuarios y se precisó la necesidad de aplicación de tecnología de firma digital
    - Análisis del sistema: se relevó el circuito actual, y se definió el alcance de la experiencia piloto

- Diseño de la implementación: se elaboró el diseño conceptual de la experiencia piloto.
- Desarrollo e implementación: se llevó a la práctica la experiencia piloto real. Se emitieron los certificados de firma digital, se realizaron las configuraciones, instalación de protocolos, ajustes y desarrollos necesarios en el equipamiento informático
- Prueba del Sistema: se elaboró y se puso en práctica un Plan de Pruebas
- Puesta en Marcha de la implementación: el sistema existente se reemplazó por el nuevo mejorado y se capacitó a los usuarios.
- Evaluación de la experiencia: se definieron métricas de evaluación que a futuro permitirán evaluar el éxito de la implementación

3. ***Implementación de experiencia piloto en la Penitenciaría Provincial:***

- Identificación de la necesidad: se recopiló y analizó información sobre el problema, se entrevistó a los posibles usuarios y se precisó la necesidad de aplicación de tecnología de firma digital
- Análisis del sistema: se relevó el circuito actual, y se definió el alcance de la experiencia piloto
- Diseño de la implementación: se elaboró el diseño conceptual de la experiencia piloto.
- Desarrollo e implementación: se llevó a la práctica la experiencia piloto real. Se emitieron los certificados de firma digital, se realizaron las configuraciones, instalación de protocolos, ajustes y desarrollos necesarios en el equipamiento informático
- Prueba del Sistema: se elaboró y se puso en práctica un Plan de Pruebas
- Puesta en Marcha de la implementación: el sistema existente se reemplazó por el nuevo mejorado y se capacitó a los usuarios.
- Evaluación de la experiencia: se definieron métricas de evaluación que a futuro permitirán evaluar el éxito de la implementación

4. ***Participación en el proceso de Reglamentación de la Ley 7234:***

- Reuniones con el equipo legal de la Gobernación: se realizaron reuniones con el objeto de aclarar los alcances del proyecto de firma digital, las tendencias nacionales y el estado actual de la materia.

- Participación en la redacción del decreto reglamentario: se brindó asesoramiento desde los conocimientos específicos y Know How adquirido en materia de Firma Digital por parte del equipo del proyecto.

5. ***Investigación de nuevas tecnologías de firma digital:***

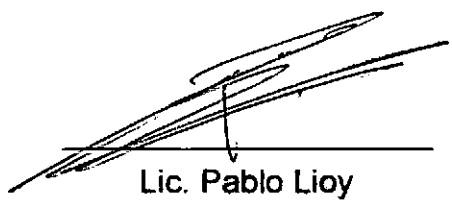
   - Investigación de tecnología de time stamping: se recopiló y analizó información sobre la tecnología que permite la prestación de servicios seguros de registro de hora y se presentaron las principales conclusiones

6. ***Identificación de nuevas implementaciones***

   - Identificación de Procedimientos aptos: se realizaron sondeos de nuevos ámbitos de implementación de firma digital, a través de la aplicación de nuestra estrategia de identificación de procedimientos aptos y el estudio analítico de circuitos administrativos en la Administración Pública Provincial.
   - Formulación de nuevas propuestas de implementación: se realizaron reuniones con los principales responsables y usuarios de los procesos identificados en el punto anterior para generar nuevas propuestas de implementaciones y experiencias con tecnología de Firma Digital.

Los nuevos contenidos correspondientes a lo planificado para el informe final corresponden a la las actividades 4,5 y 6, se presentan a los ocho meses de iniciadas las tareas.

De esta manera se cumple con las actividades propuestas para el proyecto y con las líneas de acción planteadas:



Lic. Pablo Lioy

ÍNDICE

I. Resumen de contenidos 3
II. Extensión de la Experiencia Piloto de Repositorio de Normas Legales con Firma Digital: 8
A. Soporte continuo: 8
1. Programa de capacitación 9
2. Documentación de consulta y ayuda en línea 10
3. Mesa de ayuda – Help Desk 10
4. Soporte in situ – Asistencia Desk-side 11
B. Seguridad y backup: 11
Política de Seguridad 12
C. Mantenimiento del ciclo de vida del sistema: 23
D. Carga de datos históricos: 29
Etapa 1 Digitalización de Resoluciones 29
Etapa 2 Firma de Resoluciones Digitalizadas 31
Etapa 3 Carga de información en base de datos 31
III. Implementación de Experiencia Piloto en la DGE: 33
A. Identificación de la necesidad: 33
B. Análisis del sistema: 39
C. Diseño de la implementación: 41
D. Desarrollo e implementación: 50
E. Prueba del Sistema: 58
F. Puesta en marcha de la implementación 68
G. Evaluación de la experiencia: 71
IV. Implementación de Experiencia de Sitio Seguro en la Penitenciaría Provincial: 73
A. Identificación de la necesidad: 73
B. Análisis del sistema: 77
C. Diseño de la implementación: 78
D. Desarrollo e implementación: 84
E. Prueba del Sistema: 91
F. Puesta en marcha de la implementación 92
G. Evaluación de la experiencia: 94
V. Participación en el proceso de reglamentación de la Ley 96
VI. Investigación de nuevas tecnologías de firma digital 97
VII. Identificación de nuevas implementaciones 117

I. Resumen de contenidos

Se presentan a continuación, a modo de Informe Final, las actividades y tareas desarrolladas en el marco de planificación del proyecto de Firma Digital Mendoza.

Los contenidos ya presentados en informes anteriores se presentan resumidos y sintetizados por importancia, para obtener una versión más detallada de los temas por favor remitirse a los informes precedentes.

El resumen de las actividades realizadas es el siguiente:

1. ***Extensión de la Experiencia Piloto de Repositorio de Normas Legales con Firma Digital:***
    - Soporte continuo: se respondió a los requerimientos de soporte de los usuarios y operadores del sistema.
    - Seguridad y backup: se planificó y desarrolló procedimientos y mecanismos de seguridad preventiva y correctiva a nivel físico y lógico sobre los datos contenidos en el repositorio.
    - Mantenimiento del ciclo de vida del sistema: se garantizó la dinámica, flexibilidad y escalabilidad del sistema a través de la retroalimentación y actualización permanente.
    - Carga de datos históricos: se desarrolló y aplicó un procedimiento de carga masiva de documentos para incorporar al repositorio el volumen de datos necesarios para satisfacer necesidades de consulta e integración de datos.
2. ***Implementación de experiencia piloto en la DGE:***
    - Identificación de la necesidad: se recopiló y analizó información sobre el problema, se entrevistó a los posibles usuarios y se precisó la necesidad de aplicación de tecnología de firma digital
    - Análisis del sistema: se relevó el circuito actual, y se definió el alcance de la experiencia piloto
    - Diseño de la implementación: se elaboró el diseño conceptual de la experiencia piloto.

- Desarrollo e implementación: se llevó a la práctica la experiencia piloto real. Se emitieron los certificados de firma digital, se realizaron las configuraciones, instalación de protocolos, ajustes y desarrollos necesarios en el equipamiento informático
- Prueba del Sistema: se elaboró y se puso en práctica un Plan de Pruebas
- Puesta en Marcha de la implementación: el sistema existente se reemplazó por el nuevo mejorado y se capacitó a los usuarios.
- Evaluación de la experiencia: se definieron métricas de evaluación que a futuro permitirán evaluar el éxito de la implementación

3. ***Implementación de experiencia piloto en la Penitenciaría Provincial:***

- Identificación de la necesidad: se recopiló y analizó información sobre el problema, se entrevistó a los posibles usuarios y se precisó la necesidad de aplicación de tecnología de firma digital
- Análisis del sistema: se relevó el circuito actual, y se definió el alcance de la experiencia piloto
- Diseño de la implementación: se elaboró el diseño conceptual de la experiencia piloto.
- Desarrollo e implementación: se llevó a la práctica la experiencia piloto real. Se emitieron los certificados de firma digital, se realizaron las configuraciones, instalación de protocolos, ajustes y desarrollos necesarios en el equipamiento informático
- Prueba del Sistema: se elaboró y se puso en práctica un Plan de Pruebas

- Puesta en Marcha de la implementación: el sistema existente se reemplazó por el nuevo mejorado y se capacitó a los usuarios.
- Evaluación de la experiencia: se definieron métricas de evaluación que a futuro permitirán evaluar el éxito de la implementación

4. ***Participación en el proceso de Reglamentación de la Ley 7234:***

- Reuniones con el equipo legal de la Gobernación: se realizaron reuniones con el objeto de aclarar los alcances del proyecto de firma digital, las tendencias nacionales y el estado actual de la materia.
- Participación en la redacción del decreto reglamentario: se brindó asesoramiento desde los conocimientos específicos y Know How adquirido en materia de Firma Digital por parte del equipo del proyecto.

5. ***Investigación de nuevas tecnologías de firma digital:***

- Investigación de tecnología de time stamping: se recopiló y analizó información sobre la tecnología que permite la prestación de servicios seguros de registro de hora y se presentaron las principales conclusiones

6. ***Identificación de nuevas implementaciones***

- Identificación de Procedimientos aptos: se realizaron sondeos de nuevos ámbitos de implementación de firma digital, a través de la aplicación de nuestra estrategia de identificación de procedimientos aptos y el estudio analítico de circuitos administrativos en la Administración Pública Provincial.
- Formulación de nuevas propuestas de implementación: se realizaron reuniones con los principales responsables y usuarios de los procesos identificados en el punto anterior para generar

nuevas propuestas de implementaciones y experiencias con tecnología de Firma Digital.

Los nuevos contenidos correspondientes a lo planificado para el informe final corresponden a la las actividades 4,5 y 6, se presentan a los ocho meses de iniciadas las tareas.

De esta manera se cumple con las actividades propuestas para el proyecto y con las líneas de acción planteadas:

LÍNEA DE IMPLEMENTACIÓN DE EXPERIENCIAS

Actividades:

Extensión de la Experiencia Piloto de Repositorio de Normas Legales con Firma Digital: luego de la puesta en marcha inicial en paralelo de la experiencia, que le da un punto de partida a la dinámica del sistema (planificada para el proyecto precedente), se produce ahora, una revisión general del sistema y del circuito de implementación. Al inicio del presente proyecto, procedemos a documentar este proceso de retroalimentación y soporte continuo que se da con los usuarios del sistema, reportando incidentes, desarrollando acciones correctivas y plasmando el proceso implementación total de la experiencia a través del volumen de resoluciones cargadas en el repositorio.

Implementación de sitio seguro en la Penitenciaría Provincial: de acuerdo con la propuesta de aplicación plasmada en el Informe Final del proyecto de Firma Digital precedente, implementaremos sitio seguro con autenticación de clientes en el sistema de mesa de entrada de la intranet de la Penitenciaría Provincial de Mendoza.

Implementación de correo seguro en comunicaciones internas: de acuerdo con la propuesta de aplicación plasmada en el Informe Final del proyecto de Firma Digital precedente, implementaremos Correo

Electrónico Seguro en el ámbito de los procesos de comunicación interna y transferencia de datos del sistema de planta funcional de recursos humanos de la Dirección General de Escuelas.

LÍNEA DE INVESTIGACIÓN Y DESARROLLO

Actividades

Investigación renuevas tecnologías de firma digital: siguiendo la línea de investigación de nuestro proyecto, proponemos el estudio analítico de nuevos tipos de aplicaciones disponibles con tecnología de firma digital que nos permitan brindar nuevos y mejores servicios en el marco del proyecto

LÍNEA DE FORTALECIMIENTO Y CRECIMIENTO DE PROYECTO

Actividades

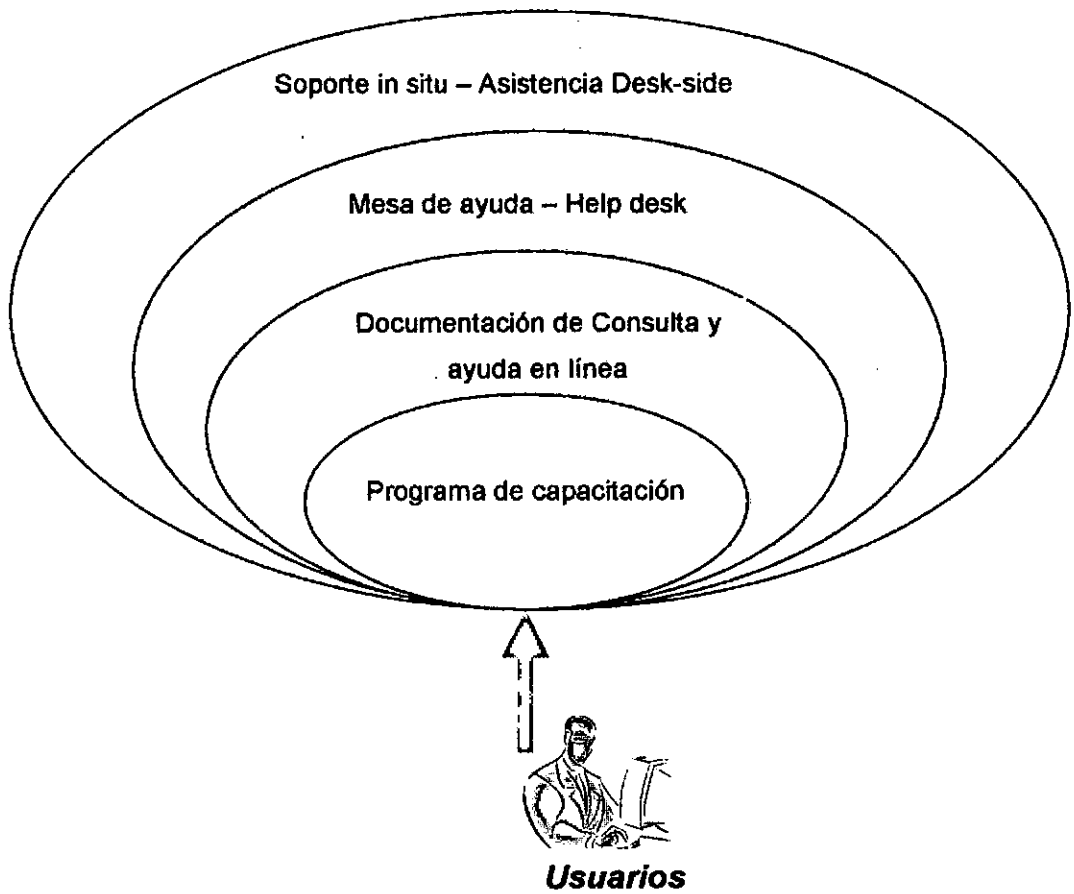
Participación en el proceso de Reglamentación del la Ley 7234: la inminente aprobación de la Ley de Adhesión provincial a la Ley nacional de firma digital, elaborada a instancias de nuestro equipo de firma digital, determina la obligación del PE provincial de reglamentar dicha Ley. Por ello, resulta necesario trabajar estrechamente con las oficinas legales de la Gobernación asesorando desde los conocimientos específicos y experiencia técnica del equipo en materia de firma digital.

Identificación de nuevas implementaciones: de manera de asegurar el cumplimiento de los objetivos que el proyecto de Firma digital propone para la Administración Pública Provincial, continuaremos trabajando para precisar nuevos ámbitos y circuitos de implementación de experiencias a la luz de nuestra estrategia de Identificación de Procedimientos aptos.

II. Extensión de la Experiencia Piloto de Repositorio de Normas Legales con Firma Digital:

A. Soporte continuo:

Una vez iniciada la dinámica del sistema, con la carga inicial de datos, se diseño y puso en marcha un esquema de soporte continuo a usuarios finales y usuarios administradores del sistema que básicamente incluye los siguientes servicios integrados:



Como lo muestra el esquema, los servicios propuestos han sido estructurados de forma incremental, de manera que un usuario acceda a un determinado nivel de atención y soporte, cuando no haya encontrado solu-

ción en el nivel precedente. Por otra parte, cada nivel de orden superior es incluyente con respecto a los servicios de los niveles inferiores.

Este modelo se sustenta en la concepción de favorecer la autonomía de los usuarios en el uso del repositorio, en la medida que ello sea factible.

En este sentido, conviene aclarar que si bien la envergadura actual del sistema no implica una carga excesiva de requerimientos de asistencia y soporte, es bueno adoptar una estrategia de soporte consistente con grandes volúmenes de usuarios, previendo el crecimiento futuro que se pretende para el repositorio.

Veamos en detalle cada una de las dimensiones de soporte continuo propuestas.

1. Programa de capacitación

Como se informó precedentemente la capacitación de los empleados y funcionarios involucrados en el circuito se abordó desde dos dimensiones igualmente importantes. Por un lado la capacitación operativa en el uso de las herramientas informáticas y los cambios en los procesos habituales de gestión, firma y consulta de normas legales. Por otro, la formación acerca de los alcances tecnológicos y legales de la firma digital; y la concientización sobre las ventajas comparativas que la introducción de esta tecnología tiene sobre la gestión. En ambas dimensiones se entendió que la capacitación constituía una herramienta fundamental para garantizar el éxito del la aplicación y que debía ser utilizada para generar confianza, difundir y provocar entusiasmo contagioso entre todos los actores involucrados en el circuito.

El programa de capacitación abordó los siguientes temas:

- Modelo lógico y funcional del repositorio.
- Estructura conceptual del sitio web: zonas pública y segura.
- Aplicación y alcances de la firma digital y certificados digitales al digesto.
- Obtención de Certificados digitales.
- Seguridad SSL en el sistema y autenticación de clientes.

- Parametrización inicial.
- Administración del módulo temas.
- Administración del módulo vínculos.
- Administración de los módulo autoridades y cargos.
- Administración del módulo de normas.
- Carga y firma de documentos digitales.
- Consultas al sistema en zona segura.
- Consultas al sistema en zona pública.

2. Documentación de consulta y ayuda en línea

En esta instancia, se diseño un ***Manual del Usuario Administrador*** destinado a brindar asistencia y guía en la operación del sistema, a todos los agentes involucrados en la gestión de información y carga de documentos al repositorio.

Complementariamente el sistema cuenta con ayuda en línea tanto en la ***zona pública*** como en la ***zona segura*** del repositorio, que orienta a los usuarios en sus consultas. La ayuda en línea está construida sobre la base de documentos html, con imágenes y ejemplos ilustrativos, permitiendo una navegación hipertextual por los distintos ítems de contenido.

3. Mesa de ayuda – Help Desk

A través de un interno telefónico y un e-mail de contacto publicado en el digesto digital, se fijó un punto único de contacto, con el fin de instrumentar un help desk centralizado para todas las necesidades de soporte de usuarios finales y de usuarios administradores.

El objetivo de este help desk es proveer una rápida solución a problemas y dudas puntuales que no han sido contempladas en la ayuda escrita, reportar errores en el sistema y canalizar inquietudes o requerimientos de los grupos de usuarios. Es también un deseo que a través de esta mesa de ayuda se identifiquen puntos a ser tenidos en cuenta en el mantenimiento preventivo del sistema.

4. Soporte in situ – Asistencia Desk-side

En aquellos casos que así se requiera, se brindará un servicio de soporte in-situ o desk-side. Este servicio sólo deberá proveerse en caso de problemas graves que el usuario no puede resolver por los canales de soporte descriptos anteriormente.

Hasta el momento no se han registrado peticiones de este tipo de asistencia, ya que al contar el sistema con una interfase web total, no se producen los típicos problemas de configuración e instalación de software stand-alone o módulos cliente que requieren la presencia de técnicos en las máquinas cliente. Bajo nuestro esquema de diseño y desarrollo, la mayor parte de los problemas pueden resolverse de manera centralizada, mediante una buena administración del sistema.

B. Seguridad y backup:

La seguridad de la información se entiende como la preservación de las siguientes características:

- **Confidencialidad**: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad**: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad**: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deberán considerarse los conceptos de:

- **Legalidad**: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la dependencia.
- **Confiabilidad de la Información**: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación, se realizan las siguientes definiciones:

- **Información**: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
- **Sistema de Información**: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
- **Tecnología de la Información**: Se refiere al hardware y software operados por la dependencia o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Política de Seguridad

1. Generalidades

La información es un recurso que, como el resto de los activos, tiene valor y por consiguiente debe ser debidamente protegida.

Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos.

Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional.

Para esto, se debe asegurar un compromiso manifiesto del las máximas Autoridades y de los titulares de Unidades Organizativas para la difusión, consolidación y cumplimiento de la presente Política.

2. Objetivo

Proteger los recursos de información y la tecnología utilizada para su procesamiento, 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 Digesto Digital de Resoluciones.

3. Alcance

Esta Política se aplica a los recursos y a la totalidad de los procesos vinculados con la carga, firma y publicación de resoluciones firmadas digitalmente de la secretaría administrativa legal y técnica.

4. Usuarios del sistema

Usuario final: es cualquier empleado público con acceso a la Intranet del Gobierno de Mendoza, que desee consultar normas legales en nuestro Digesto Digital.

Usuario-administrador: es el encargado de cargar y actualizar los documentos digitales y las fichas de información que permiten su organización y acceso. Para cumplir con su función, este usuario-operador contará con un Certificado Digital que acredite su identidad ante el sistema y podrá con esta identidad realizar las operaciones de altas, bajas y modificaciones que no son permitidas a usuarios comunes.

Firma autorizada: son los funcionarios con firma digital autorizada sobre las normas cargadas al digesto digital. En la presente versión del sistema estos usuarios no tienen permisos especiales de operación sobre el sistema y son tratados como usuarios comunes a los fines de consultas al repositorio. La firma digital sobre los documentos se realiza en un ambiente externo al sistema. Las normas firmadas son cargadas a posteriori al sistema por los usuarios-operadores

Administrador de TI: este perfil refiere al encargado de administración y mantenimiento de la plataforma de hardware y software sobre la que funciona el sistema. Sus funciones son administrar el servidor

web, la base de datos y las aplicaciones informáticas y garantizar el buen funcionamiento y seguridad del sistema y de los datos y documentos almacenados.

Responsabilidad

La Política de Seguridad de Información es de aplicación obligatoria para todos los usuarios definidos en el punto anterior, cualquiera sea su situación de revista, el área a la cual se encuentre afectado y cualquiera sea el nivel de las tareas que desempeñe.

Los usuarios de la información y de los sistemas utilizados para su procesamiento para firma digital de resoluciones son responsables de:

a) Acceder solamente a aquellos datos y recursos respecto a los cuales cuentan con la autorización respectiva.
b) Utilizar esos recursos según las funciones que le fueron asignadas y con los fines para los que dispone de autorización.
c) Mantener la confidencialidad de la información del Organismo y la privacidad de la información de terceros.
d) Cumplir todos los procedimientos y controles previstos para la utilización de los sistemas y demás recursos de la tecnología de la información.
e) Cumplir y observar el cumplimiento por parte del resto del personal de los controles y medidas de seguridad orientadas a la protección física y lógica de los recursos.
f) Notificar ante la Unidad de Reforma y Modernización del Estado las violaciones y riesgos que detecten relacionados con la seguridad de la información y de los recursos.

5. Clasificación y Control de Activos

Las clasificaciones y los controles de protección de la información deben considerar las necesidades respecto a la distribución (uso compartido) y/o las restricciones de la información, y su incidencia en las actividades de la dependencia.

En general, la clasificación asignada a la información es una forma sencilla de señalar cómo ha de ser tratada y protegida.

Se deben rotular según su valor y grado de sensibilidad para el Organismo tanto la información como las salidas de los sistemas que administran datos clasificados. Asimismo, resulta conveniente rotular la información según su grado de criticidad, por ejemplo en términos de integridad y disponibilidad.

Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos deben tenerse en cuenta, puesto que la clasificación por exceso puede traducirse en gastos adicionales innecesarios para la dependencia.

La responsabilidad por la definición de la clasificación de un ítem de información, por ejemplo un documento, registro de datos, archivo de datos o disquete, y por la revisión periódica de dicha clasificación, debe ser asignada al responsable de la información.

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.

Bajo el punto de vista de Seguridad, las medidas de protección deben ser aplicadas a todas y cada una de las formas relacionadas con los sistemas de información de la dependencia.

Objetivo

Garantizar que los recursos de información reciban un apropiado nivel de protección.

Clasificar la información para señalar la necesidad, prioridad y grado de protección requerido, definiendo niveles de protección y comunicando la necesidad de medidas de tratamiento especial.

Alcance

Se aplica a toda la información relacionada con la redacción y firma digital de resoluciones administrada en la dependencia, cualquiera sea el soporte en que se encuentre.

Responsabilidad

Los propietarios de los sistemas y datos, es decir los Responsables de Activos de Información, son los encargados de clasificar la información de su propiedad de acuerdo con el grado de sensibilidad y criticidad de la misma, y de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.

Clasificación

Para clasificar un Activo de Información, se utilizarán los criterios 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.

En adelante, se hablará de Información Clasificada refiriéndose exclusivamente a la descrita en los niveles 3 y 4 precedentes.

Sólo el Responsable de un Activo de Información puede asignar o cambiar el nivel de clasificación, cumpliendo con los siguientes requisitos previos:

- Asignarle una fecha de efectividad.
- Comunicárselo al depositario del recurso.
- Realizar los cambios necesarios para que los Usuarios conozcan la nueva clasificación.

Rotulado de la Información

La información clasificada que aparezca en los terminales o estaciones de trabajo de usuario, tiene que reflejar su nivel de clasificación, como mínimo, en la pantalla inicial y siempre que sea posible, en todas y cada una de las pantallas o estar permanentemente en la cabecera de pantalla.

Cada medio de almacenamiento removible (cintas, CDs, cartuchos, disquetes, etc.), que contenga información clasificada, tiene que ser etiquetado con el nivel más alto de clasificación de la información que contenga. Los medios de almacenamiento no removibles no necesitan ser marcados con etiquetas de clasificación. La Información transmitida por medio de redes de comunicaciones (correo electrónico, teléfono, fax, etc.) debe ser rotulada de acuerdo con el nivel más alto de clasificación de la información que contenga.

Protección de la Información Clasificada

La principal regla de protección es que la información clasificada sea conocida o utilizada sólo por personas autorizadas y siempre con motivo del ejercicio de sus funciones.

Guardar información clasificada en cualquier sistema o medio de almacenamiento supone:

- Tener los medios físicos y lógicos adecuados para protegerla.
- No permitir su acceso público.
- Limitar el acceso a esta información.

Protección de Información Impresa

La información clasificada debe permanecer, en todo momento, lejos del alcance de empleados y personas que no tengan necesidad de conocerla.

La Información Clasificada, debe guardarse bajo llave permanentemente, y durante su uso debe evitarse que puedan tener acceso personas no autorizadas.

El empleo de cualquier dispositivo para generar salidas impresas que contengan Información Clasificada debe limitarse a aquellos que cumplan con las siguientes condiciones:

- Estén situados en áreas de acceso limitado o restringido.
- Tengan algún tipo de control de borrado de listados.
- Sean de uso exclusivo del usuario (impresora personal).

Si ninguna de las opciones anteriores está disponible, se puede imprimir en cualquier otro dispositivo siempre que los listados sean esperados por el usuario y recogidos inmediatamente por el mismo.

En cualquier caso, la creación de salidas impresas de información clasificada estará siempre bajo la responsabilidad y el control del usuario que genera la impresión.

Divulgación de la Información Clasificada

La información clasificada se debe divulgar únicamente sobre la base de la necesidad de conocerla por motivos de trabajo y tiene que ser autorizada formalmente, caso a caso, por el Responsable de dicha información.

El copiado y distribución de información clasificada debe contar previamente con la aprobación explícita del Responsable de dicha información, quien puede reservarse el derecho de aprobar personalmente cada caso, pudiendo añadir la leyenda **"Prohibida la Reproducción"** o bien numerar las copias aprobadas, para su control.

Para una correcta divulgación, la información clasificada no podrá ser transmitida a través de medios de comunicación inseguros, a menos que se encuentre cifrada.

Transporte de la Información Clasificada

Siempre que la información clasificada sea transportada dentro del ámbito de la dependencia, bastará con ponerla en un sobre o contenedor cerrado y marcarlo con la clasificación más alta del contenido.

Siempre que la información clasificada sea enviada a través de redes de comunicaciones, propias o ajenas debe utilizarse un método de cifrado seguro. Para ello se utilizará en orden de preferencia:

- Método de Cifrado Asimétrico (por ejemplo Certificado Digital)
- Método de Cifrado Simétrico, que incluya la protección de la clave de cifrado mediante el uso de Cifrado Asimétrico.
- Otro método de Cifrado Simétrico.

En este último caso, se enviará la información cifrada y por otra vía la clave correspondiente.

Fuera del ámbito de la dependencia, el personal evitará el transporte de información clasificada. Si esto no fuera posible, deberá conservar la información en su poder, no debiendo dejarla desatendida y, siempre que sea posible, manteniéndola cifrada.

6. Resguardo de la Información

El Administrador de TI dispondrá la realización periódica de copias de resguardo de la información y el software esenciales para la dependencia. Para esto se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y el software critico de la dependencia. Los sistemas de resguardo deberán probarse periódicamente.

Se definen procedimientos para el resguardo de la información, que deberán considerar los siguientes puntos:

a) Almacenar en una ubicación remota un nivel mínimo de información de resguardo, junto con registros exactos y completos de las copias de resguardo y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Se deberán retener al menos tres generaciones o ciclos de información de resguardo para la información y el software esenciales para la dependencia.
b) Asignar a la información de resguardo un nivel de protección física y ambiental según los estándares aplicados en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.
c) Probar periódicamente los medios de resguardo.
d) Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

7. Uso de Contraseñas

Los usuarios deben cumplir las siguientes directivas:

a) Mantener las contraseñas en secreto.
b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
c) Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el Administrador de TI, que:
    1. sean fáciles de recordar.

2. no estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
3. no tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.

d) Cambiar las contraseñas cada vez que el sistema operativo de red se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
e) Cambiar las contraseñas provisorias en el primer inicio de sesión ("log on").
f) Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquéllas almacenadas en una tecla de función o macro.

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se notificará a los mismos que pueden utilizar una única contraseña para todos los servicios que brinden un nivel razonable de protección de las contraseñas almacenadas.

8. Administración de Claves

Protección de Claves Criptográficas

Se implementará un sistema de administración de claves criptográficas para respaldar su uso por parte de la dependencia de los dos tipos de técnicas criptográficas, los cuales son:

a) Técnicas de clave secreta, cuando dos o más actores comparten la misma clave y esta se utiliza tanto para cifrar información como para descifrarla.
b) Técnicas de clave publica, cuando cada usuario tiene un par de claves: una clave pública (que puede ser revelada a cualquier persona) utilizada para cifrar y una clave privada (que debe mantenerse en secreto) utilizada para descifrar.

Todas las claves serán protegidas contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada.

Se proveerá de protección adecuada al equipamiento utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.

9. Utilización de Controles Criptográficos.

Se establece que:

a) Se utilizarán controles criptográficos en las siguientes ocasiones:
   1) Para la protección de claves.
   2) Para la transmisión de información clasificada, fuera del ámbito de la dependencia.
   3) Para el resguardo de información.

b) Se desarrollarán procedimientos respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado.

c) Se utilizarán los siguientes algoritmos de cifrado y tamaños de clave:

Utilizar Para	Algoritmo	Longitud de Clave
Para certificados utilizados en servicios relacionados a la firma digital (certificación de hora digital, almacenamiento seguro de documentos electrónicos, etc.)	RSA	2048 bits
	DSA	2048 bits
	ECDSA	210 bits
Para certificados de Certificador o de información de estado de certificados	RSA	2048 bits

	DSA	2048 bits
	ECDSA	210 bits
Para certificados de usuario (personas físicas o jurídicas)	RSA	1024 bits
	DSA	1024 bits
	ECDSA	190 bits

Cifrado

El Administrador de TI se identificará el nivel requerido de protección tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar.

Firma Digital

Se tomarán recaudos para proteger la confidencialidad de las claves privadas.

Asimismo, es importante proteger la integridad de la clave pública. Esta protección se provee mediante el uso de un certificado de clave pública.

Al utilizar firmas digitales, se considerará la legislación pertinente (Ley 25.506, el Decreto Nº 2628/02, la ley provincial 7234 de adhesión y el conjunto de normas complementarias que fijan o modifican competencias y establecen procedimientos) que describa las condiciones bajo las cuales una firma digital es legalmente vinculante.

C. Mantenimiento del ciclo de vida del sistema:

Si bien el desarrollo del Repositorio de Normas Legales se concibió en sus orígenes como una experiencia piloto de aplicación de firma digital en el ámbito de la Secretaría Administrativa, Legal y Técnica; siempre se consideró posible su aplicación gradual a escala global en la Administración Pública de Mendoza, puesto que sería en este contexto amplio donde la aplicación generaría su mayor impacto.

Producir aplicaciones en las cuales el usuario pueda aprovechar el potencial del paradigma de la navegación de sitios *web*, mientras ejecuta transacciones sobre bases de información, es una tarea que requiere de un profundo conocimiento de los requerimientos y un cuidadoso esfuerzo de diseño. Si se agrega al modelo la introducción de la tecnología de firma digital, encontramos en un escenario complejo, sobre el que no existen metodologías de análisis, diseño, desarrollo, implantación y mantenimiento específicas.

No obstante esta carencia, se procuró desde un principio trabajar sujetos a un esquema metodológico, previendo el futuro crecimiento del sistema. Este esquema se fue construyendo en cada etapa, tomando recomendaciones, modelos y buenas prácticas de análisis y diseño de sistemas; y de desarrollo de aplicaciones web, e integrándolas adecuadamente de forma de promover el cumplimiento de las siguientes condiciones necesarias para un desarrollo sostenible y escalable:

- Reusabilidad
    - Modularidad
    - Cohesión de los módulos
    - Modelo en capas
- Robustez
    - Consistencia de datos, integridad referencial
    - Seguridad
    - Tolerancia a fallos
- Presentación adecuada
    - Usabilidad, accesibilidad, navegabilidad
    - Presentación visual

- Documentación
    - "Web Application Extension for UML"
- Eficiencia
    - Tiempo medio de respuesta
    - Red
        - Ancho de Banda
        - Latencia (Keep-alive)
        - Utilización de la red
        - Utilización de la capacidad de procesamiento de servidores
        - Utilización de la capacidad de almacenamiento secundario

De acuerdo al escenario planteado, se decidió adoptar un modelo de ***desarrollo evolutivo*** para el sistema, proponiendo su crecimiento y perfeccionamiento gradual a partir de la retroalimentación y actualización permanente. En este sentido, la tarea de mantenimiento resulta un aspecto fundamental.

El desarrollo evolutivo de sistemas propone a los analistas definir un subconjunto de requerimientos conocidos (incremental), sabiendo que muchos nuevos requerimientos pueden aparecer cuando el sistema sea desplegado. Sobre este conjunto preliminar de requerimientos, se desarrolla el sistema, los usuarios lo usan, y proveen retroalimentación a los desarrolladores. Basada en esta retroalimentación, la especificación de requerimientos es actualizada, y una nueva versión del producto es desarrollada y desplegada. El proceso se repite indefinidamente.

El desarrollo de software en forma evolutiva requiere un especial cuidado en la manipulación de documentos, programas, datos de test, etc. des-

arrollados para distintas versiones del software. Cada paso debe ser registrado, la documentación debe ser recuperada con facilidad, los cambios deben ser efectuados de una manera controlada.

Para garantizar estas condiciones de mantenimiento, se propuso la división en capas en tiempo de diseño y desarrollo del repositorio y su estructuración como aplicación web de administración centralizada.

Las etapas de capacitación y puesta en marcha, constituyeron en la etapa de implementación oportunidades de prueba funcional del sistema. De estas etapas, se obtuvo retroalimentación importante, en función de la experiencia que aportaron los actores involucrados en la operación y uso del repositorio. En nuestro caso particular, la interacción permanente de los expertos del proyecto de firma digital con los responsables designados para la tarea, aportó a: la selección de los parámetros iniciales, cubrir dudas operativas que surgieron durante la etapa de carga inicial y fundamentalmente a identificar necesarios ajustes sobre el desarrollo de la herramienta informática y el circuito operativo.

Con todos estos elementos y bajo el enfoque de diseño evolutivo propuesto, diseñamos en esta etapa, la siguiente metodología de mantenimiento para el repositorio con el fin de garantizar la dinámica, flexibilidad y escalabilidad del sistema a través de la retroalimentación y actualización permanente.

Metodología de Mantenimiento y Escalabilidad para el Repositorio de Normas Legales con firma digital. (MME)

Descripción general de la MME

El objetivo de esta metodología es introducir y documentar cambios y actualizaciones en el repositorio de normas legales con firma digital, a partir de las peticiones de mantenimiento que los usuarios realizan con motivo de un problema detectado en el sistema, o por la necesidad de una mejora del mismo.

En este proceso se realiza el registro de las peticiones de mantenimiento recibidas, con el fin de llevar el control de las mismas y de proporcionar, si fuera necesario, datos estadísticos de peticiones recibidas o atendidas en un determinado período, módulos que se han visto afectados por los cambios y el tiempo empleado en la resolución de dichos cambios. Se propone, por lo tanto, llevar un catálogo de peticiones de mantenimiento, en el que se registre una serie de datos que nos permitan disponer de la información antes mencionada.

En el momento en el que se registra la petición, se procede a diagnosticar de qué tipo de mantenimiento se trata. Atendiendo a los fines, se establecen los siguientes tipos de mantenimiento:

Correctivo: son aquellos cambios precisos para corregir errores del software del repositorio.

Evolutivo: son las incorporaciones, modificaciones y eliminaciones necesarias en el software para cubrir la expansión o cambio en las necesidades de los usuarios.

Adaptativo: son las modificaciones que afectan a los entornos en los que el sistema opera, por ejemplo, cambios de configuración del hardware, software de base, gestores de base de datos, conectividad, etc.

Perfectivo: son las acciones llevadas a cabo para mejorar la calidad interna del sistema en cualquiera de sus aspectos: reestructuración del código, definición más clara del sistema y optimización del rendimiento y eficiencia.

Una vez registrada la petición e identificado el tipo de mantenimiento y su origen, se verifica y reproduce el problema, o se estudia la viabilidad del cambio propuesto por el usuario. Si la modificación es inapropiada o inviable, la petición puede ser denegada dando las justificaciones del caso. En este caso, se notifica al usuario y acaba el proceso. Si los cambios son viables, se estudia el alcance de la modificación y se analizan las alternativas de solución identificando la más adecuada. El plazo y urgencia de la solución a la petición se establece de acuerdo con el estudio anterior.

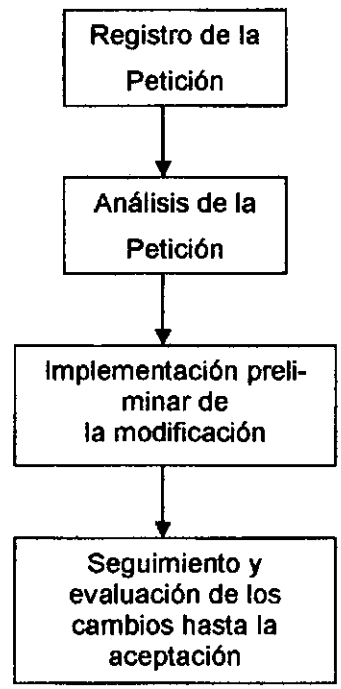
La definición de la solución incluye el estudio del impacto de la solución propuesta para la petición en los módulos afectados. Mediante el análisis de dicho estudio, la persona encargada del Proceso de Mantenimiento valora el esfuerzo y costo necesario para la implementación de la modificación.

Las tareas de desarrollo que sea necesario realizar son determinadas en función de los componentes del sistema afectados por la modificación. Estas tareas pertenecen a actividades de los procesos Análisis, Diseño, Construcción e Implantación.

Por último, y antes de la aceptación del usuario, es preciso establecer un plan de pruebas de regresión que asegure la integridad del sistema en su conjunto.

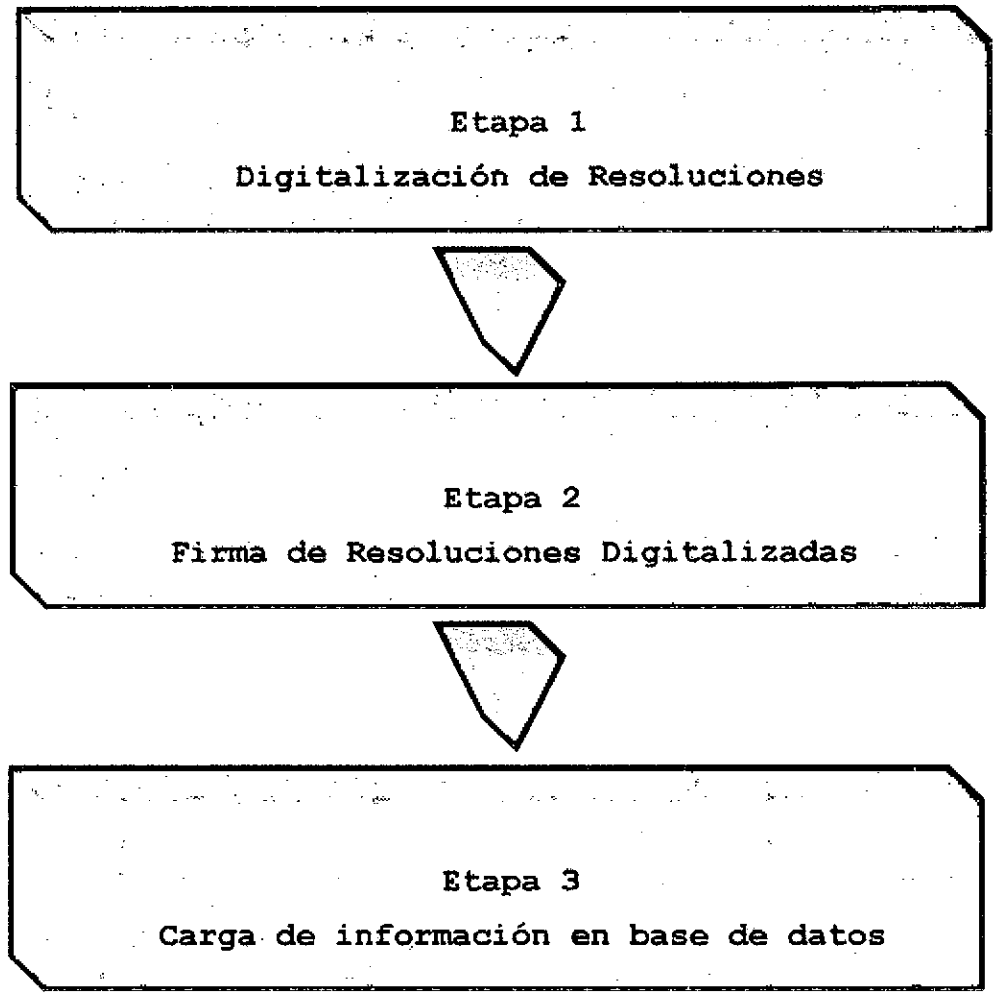
La mejor forma de mantener el costo de mantenimiento bajo control es una gestión del Proceso de Mantenimiento efectiva y comprometida. Por lo tanto, es necesario registrar de forma disciplinada los cambios realizados en el repositorio y en su documentación.

En síntesis, la estructura propuesta para el proceso de mantenimiento involucra las siguientes actividades:



D. Carga de datos históricos:

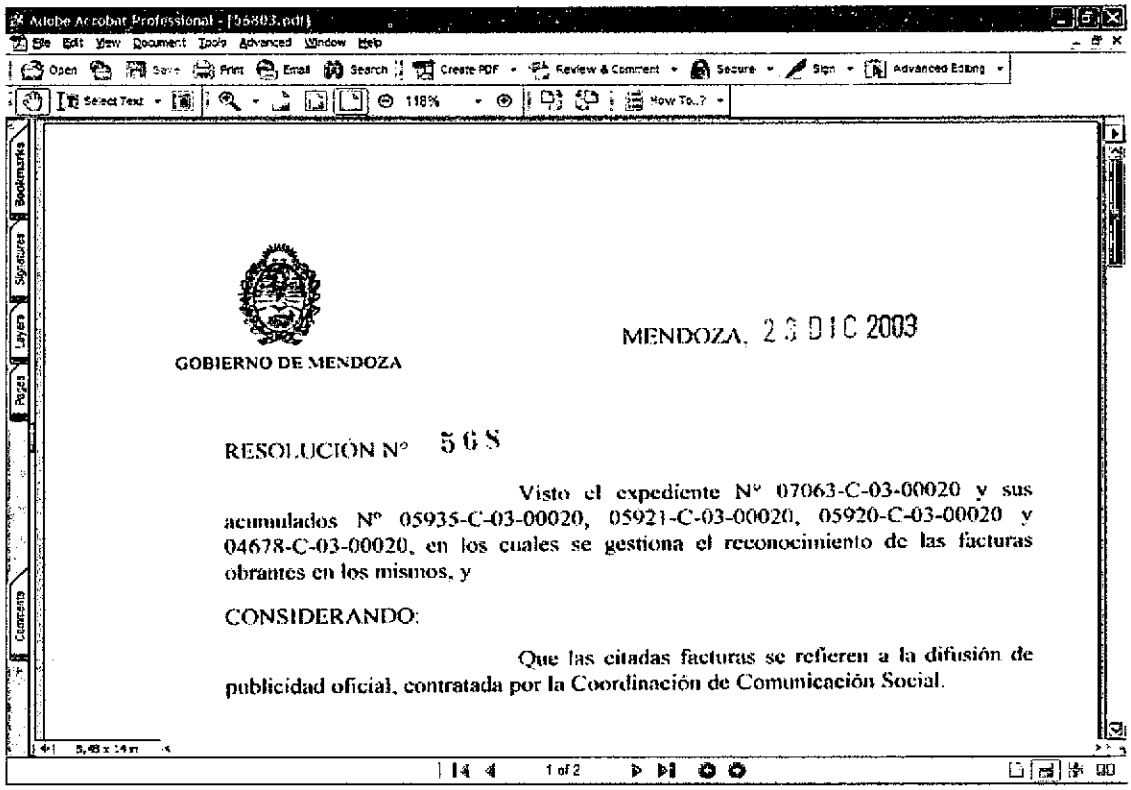
De manera de satisfacer necesidades de consulta al repositorio de resoluciones y de lograr la integración efectiva de datos a través de referencias cruzadas entre resoluciones, se puso en marcha un procedimiento de digitalización masiva de documentos para incorporar al repositorio digital. Dicho procedimiento se realiza en tres etapas:



Etapa 1 Digitalización de Resoluciones

En la primer etapa de la carga de documentos históricos, se procedió a digitalizar los documentos impresos correspondientes a las resoluciones firmadas en papel por el actual Secretario Administrativo Legal y Técnico el

Sr. Claudio Romano. Dichas resoluciones corresponden al año 2002, 2003 y parte del 2004. Cabe señalar que desde la fecha de implementación de nuestro repositorio digital, ya no será necesario continuar con la digitalización ya que nuestro sistema de repositorio digital prevé la carga en tiempo real de las resoluciones en documentos digitales para su inmediata firma digital por parte de los funcionarios responsables. La digitalización de los datos históricos, como ya mencionamos, responde a razones de consulta e integración de la información manipulada que, según nuestro análisis, quedan satisfechas con la incorporación al repositorio digital de los períodos anteriormente descriptos.



GOBIERNO DE MENDOZA

MENDOZA, 23 DIC 2003

RESOLUCIÓN N° 568

Visto el expediente N° 07063-C-03-00020 y sus acumulados N° 05935-C-03-00020, 05921-C-03-00020, 05920-C-03-00020 y 04678-C-03-00020, en los cuales se gestiona el reconocimiento de las facturas obrantes en los mismos, y

CONSIDERANDO:

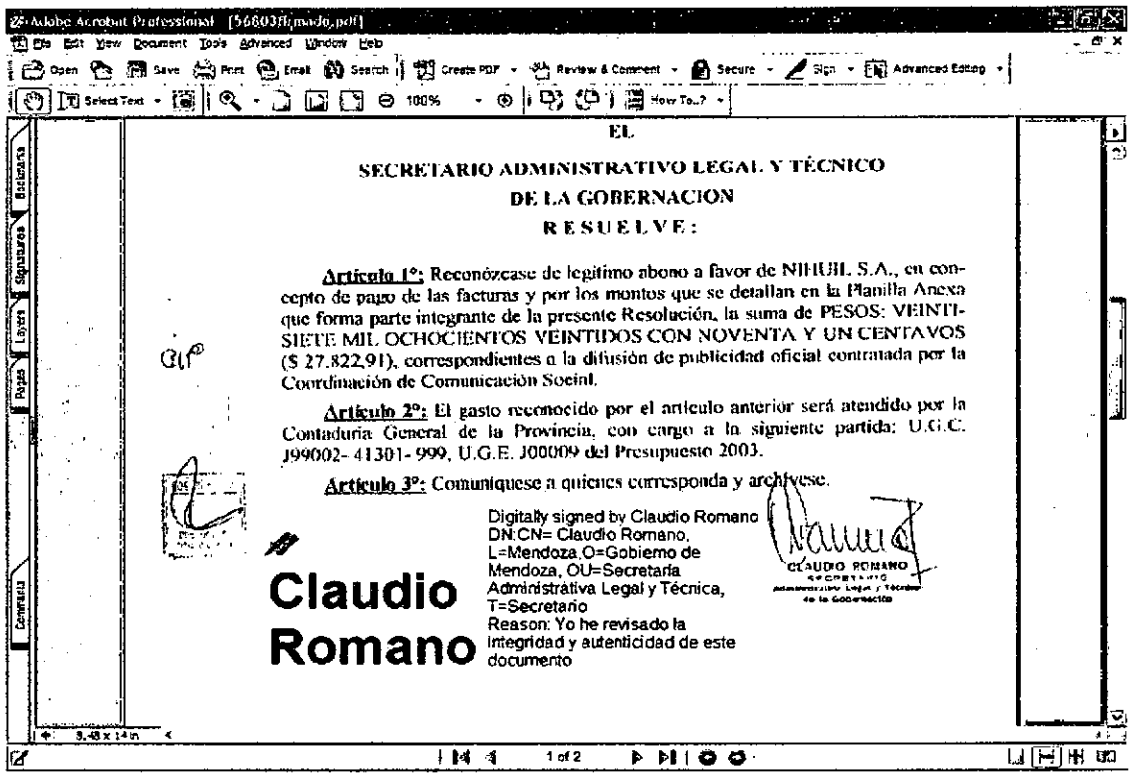
Que las citadas facturas se refieren a la difusión de publicidad oficial, contratada por la Coordinación de Comunicación Social.

Documento histórico digitalizado

Aunque el desarrollo no condiciona en principio el formato de los documentos digitales que puede almacenar el repositorio, se utilizan documentos en formato .pdf, dado que este formato constituye un estándar para la publicación de documentos en Internet.

Etapa 2 Firma de Resoluciones Digitalizadas

La segunda etapa del proceso incorpora a los documentos digitalizados la propia firma digital de los funcionarios responsables. Esto es, una vez digitalizadas las resoluciones impresas en papel, el archivo digital generado pasa a la firma digital del Director de Administración el Sr. Adelmo Pesce y luego al Secretario Administrativo Legal y Técnico el Sr. Claudio Romano para luego ser archivado en nuestro repositorio digital de resoluciones con firma digital. Tal evento es posible gracias a que los funcionarios actuales son los mismos que firmaron en forma hológrafa, en su momento, los textos de las resoluciones.



EL

SECRETARIO ADMINISTRATIVO LEGAL Y TÉCNICO

DE LA GOBERNACION

R E S U E L V E :

Artículo 1°: Reconózcase de legítimo abono a favor de NIHUIL S.A., en concepto de pago de las facturas y por los montos que se detallan en la Planilla Anexa que forma parte integrante de la presente Resolución, la suma de PESOS: VEINTISIETE MIL OCHOCIENTOS VEINTIDOS CON NOVENTA Y UN CENTAVOS ($ 27.822,91), correspondientes a la difusión de publicidad oficial contratada por la Coordinación de Comunicación Social.

Artículo 2°: El gasto reconocido por el artículo anterior será atendido por la Contaduría General de la Provincia, con cargo a la siguiente partida: U.G.C. J99002- 41301- 999, U.G.E. J00009 del Presupuesto 2003.

Artículo 3°: Comuníquese a quienes corresponda y archívese.

Digitally signed by Claudio Romano
DN:CN= Claudio Romano, L=Mendoza,O=Gobierno de Mendoza, OU=Secretaria Administrativa Legal y Técnica, T=Secretario
Reason: Yo he revisado la integridad y autenticidad de este documento

Claudio Romano

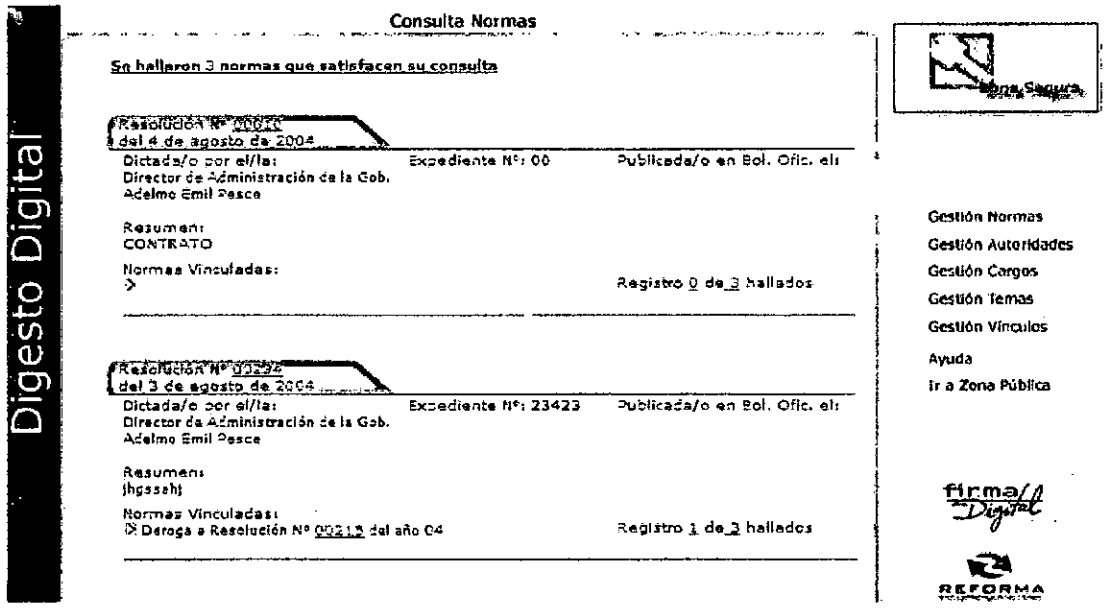
CLAUDIO ROMANO

Documento histórico digitalizado y firmado digitalmente

Etapa 3 Carga de información en base de datos

En la tercera etapa, el *Usuario-administrador* es el encargado de cargar y actualizar las fichas de información que permiten la organización y acceso a los documentos digitales (Resoluciones firmadas digitalmente). Para

ello debe generar previamente los listados de Autoridades, Cargos y Temas. Este usuario cuenta con un Certificado Digital que acredita su identidad ante el sistema y lo habilita para realizar las operaciones de altas, bajas y modificaciones que no son permitidas a usuarios comunes.



Fichas de información para consulta y búsqueda de resoluciones

III. 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:

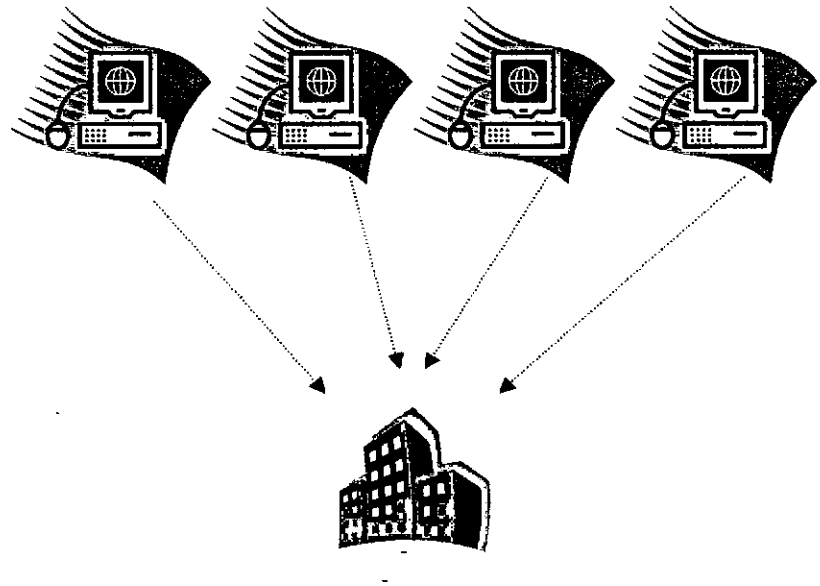
- Delegación Este.

  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 docu-

mentos 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.

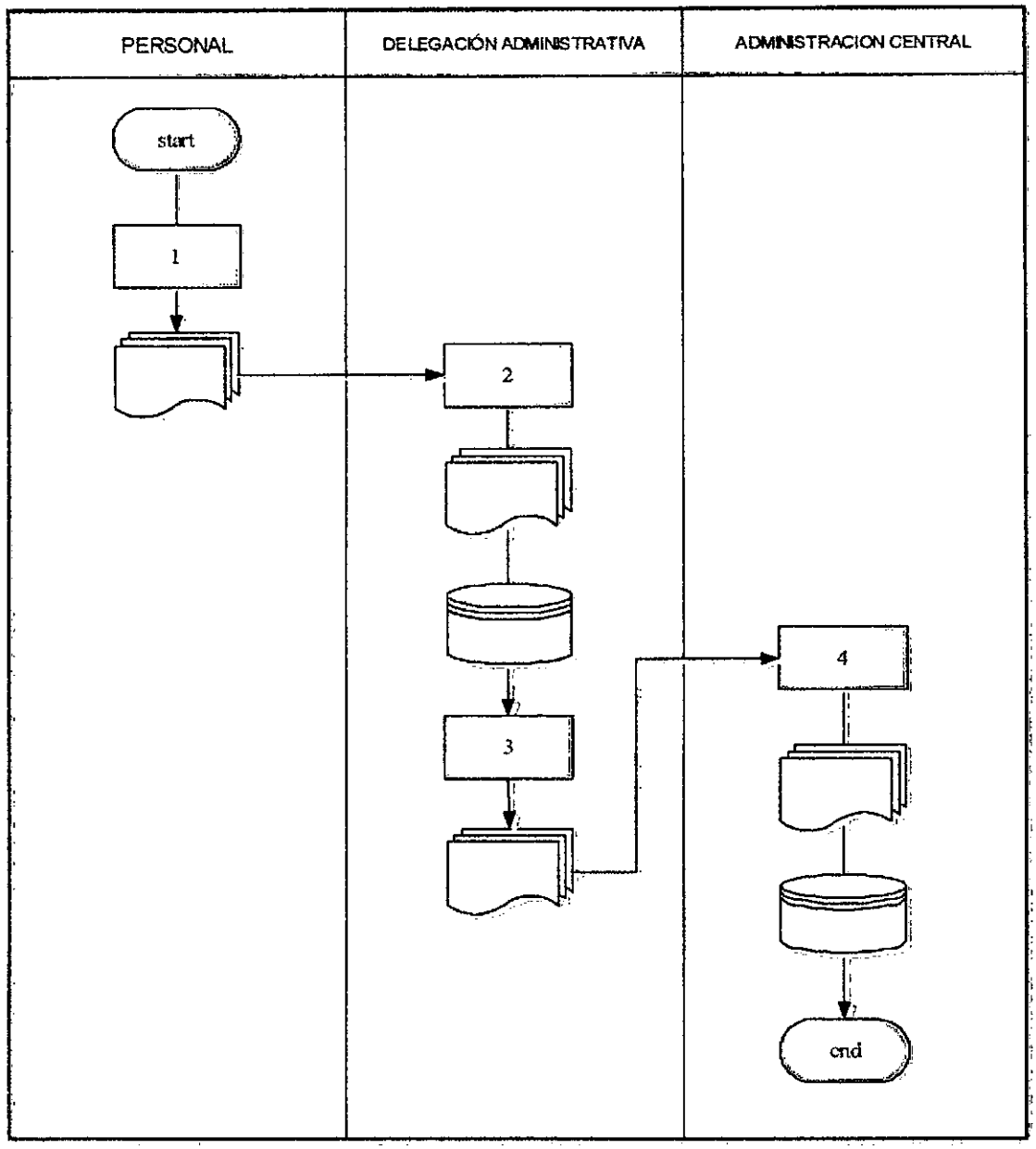
B. Análisis del sistema:

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

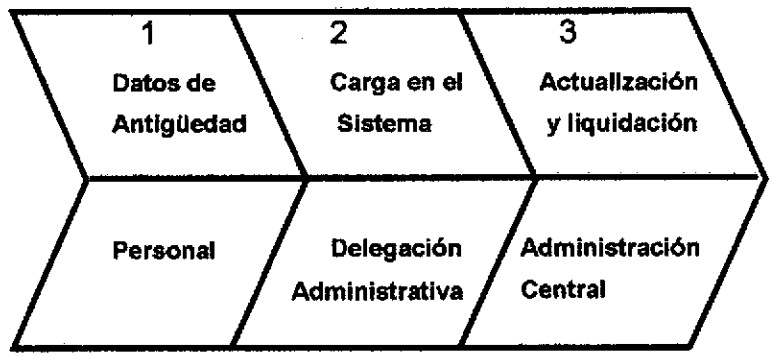
El presente procedimiento describe el conjunto de pasos a realizar por el personal de las Delegaciones Administrativas y la Administración Central de la DGE en la transmisión de información referente a antigüedad del personal para alimentar el sistema de Recursos Humanos.

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

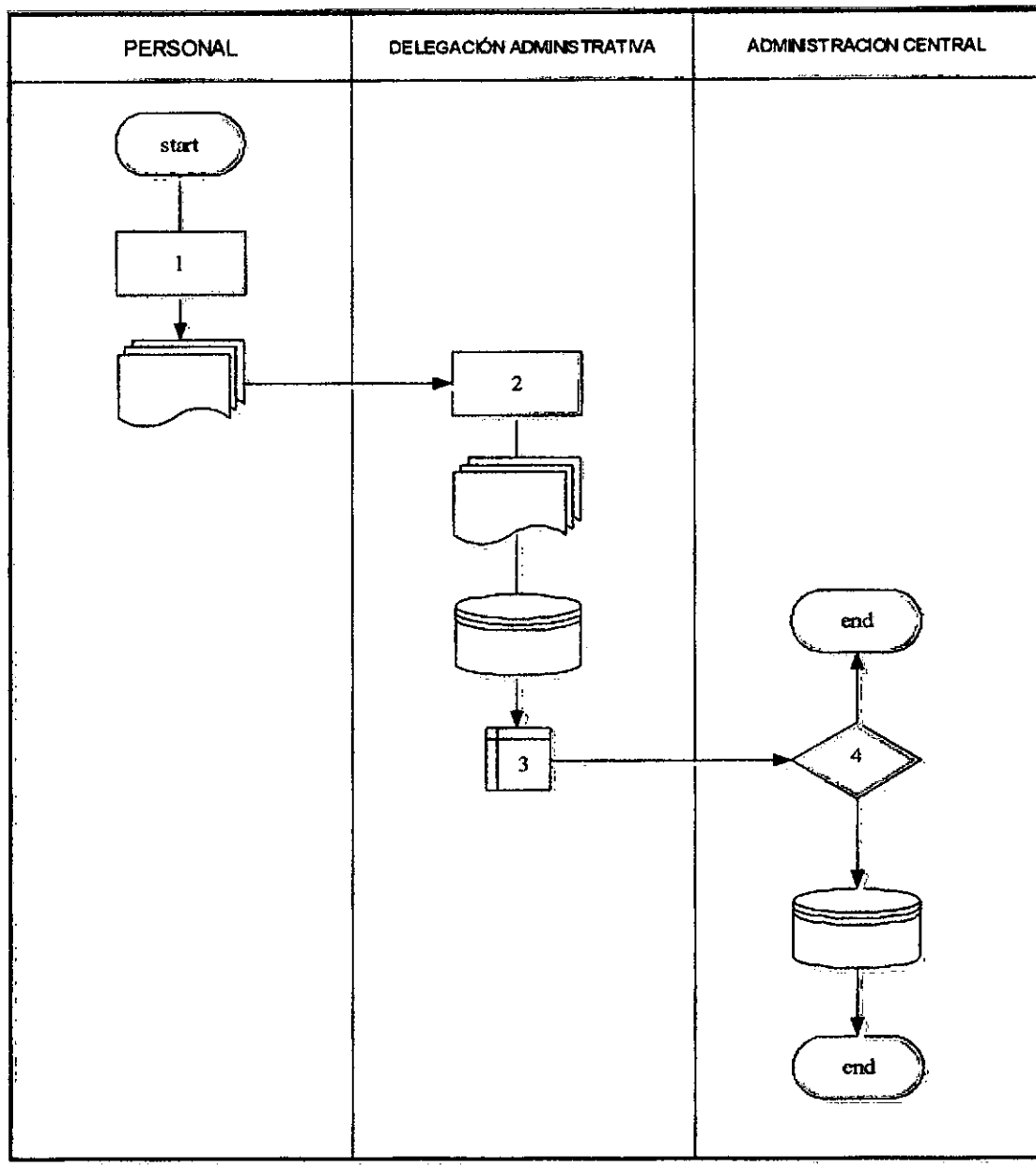
Descripción del Procedimiento (alternativa I):

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 movimien-

tos 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

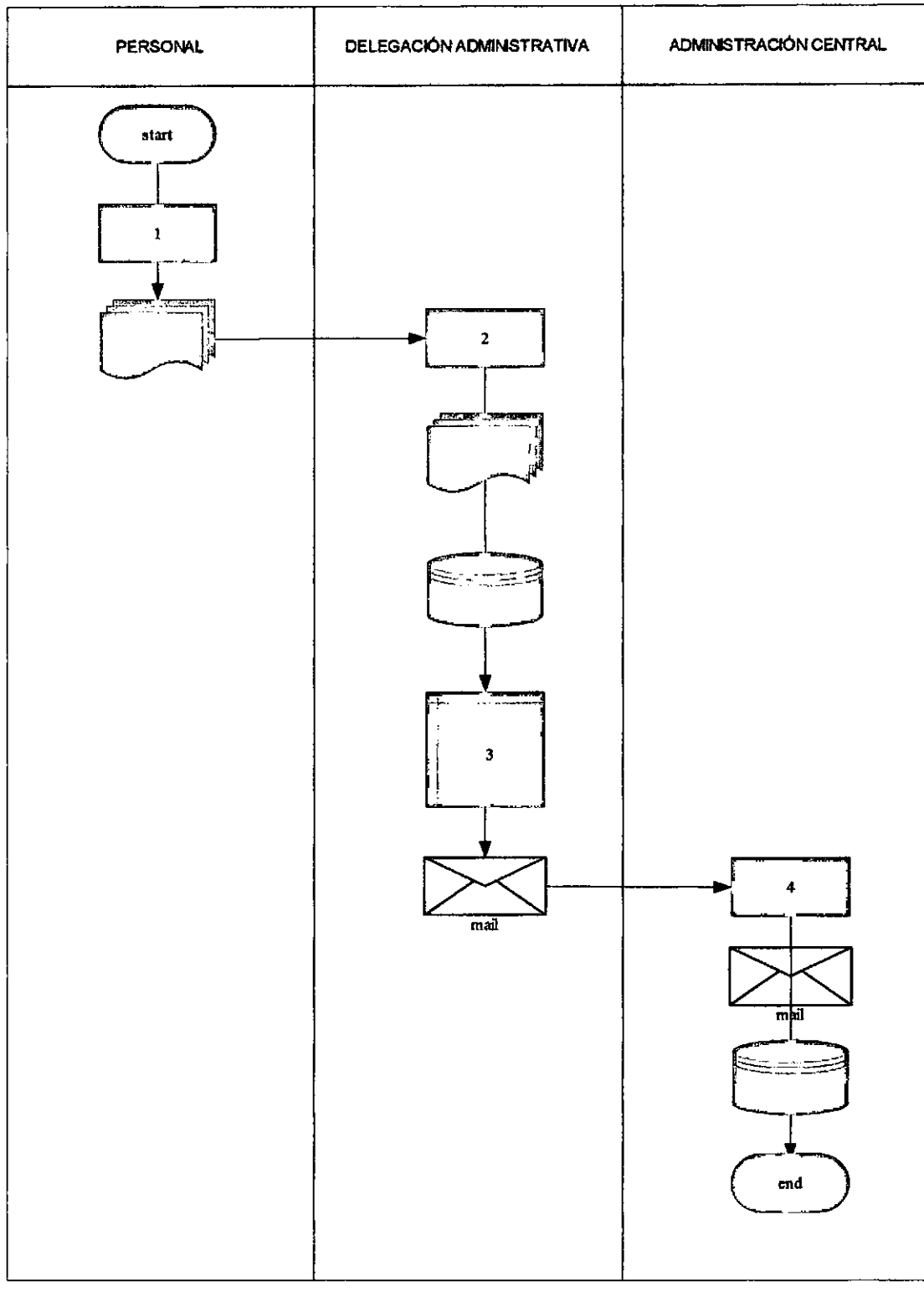


Flowchart Alternativa I

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

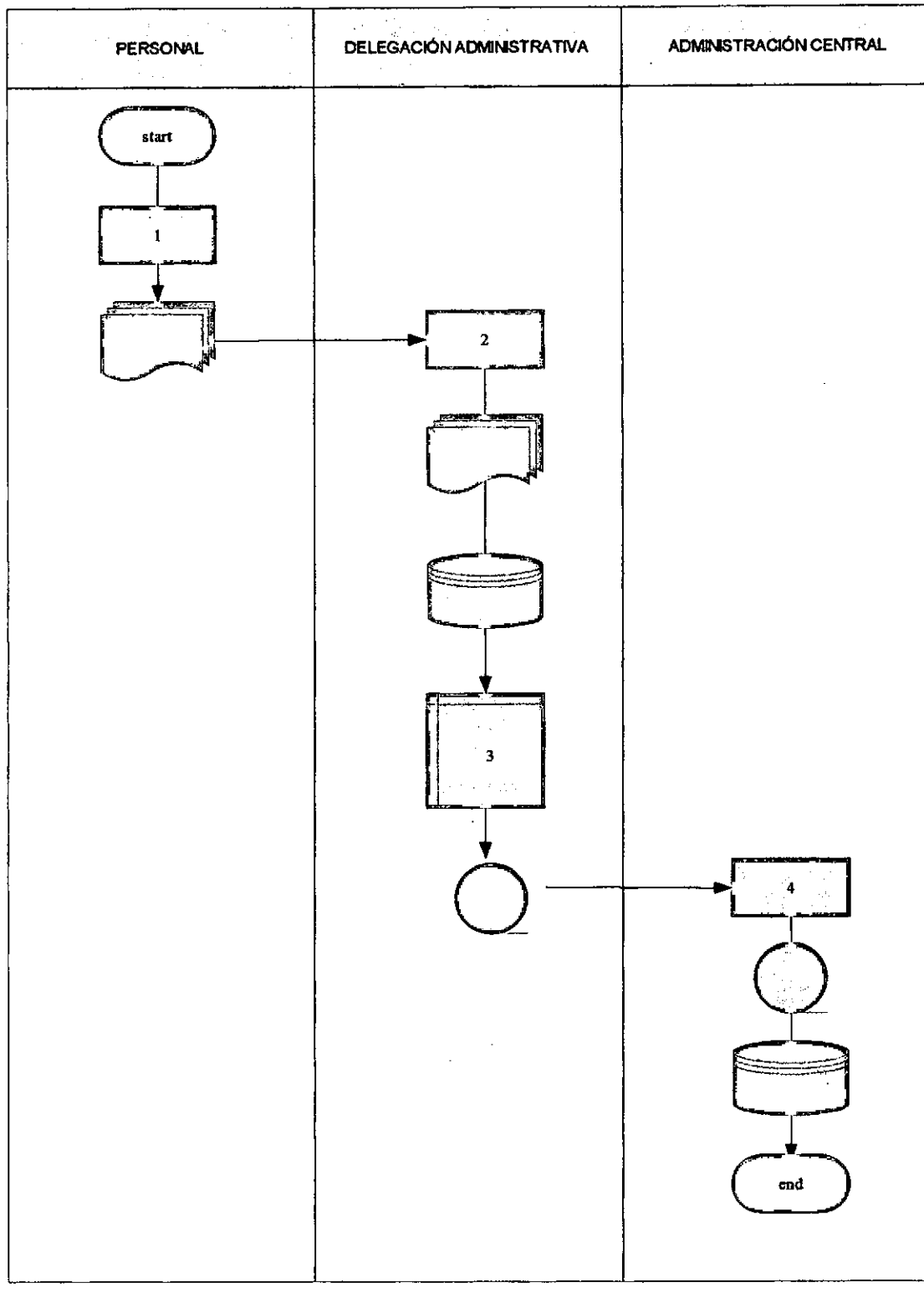


Flowchart Alternativa II

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

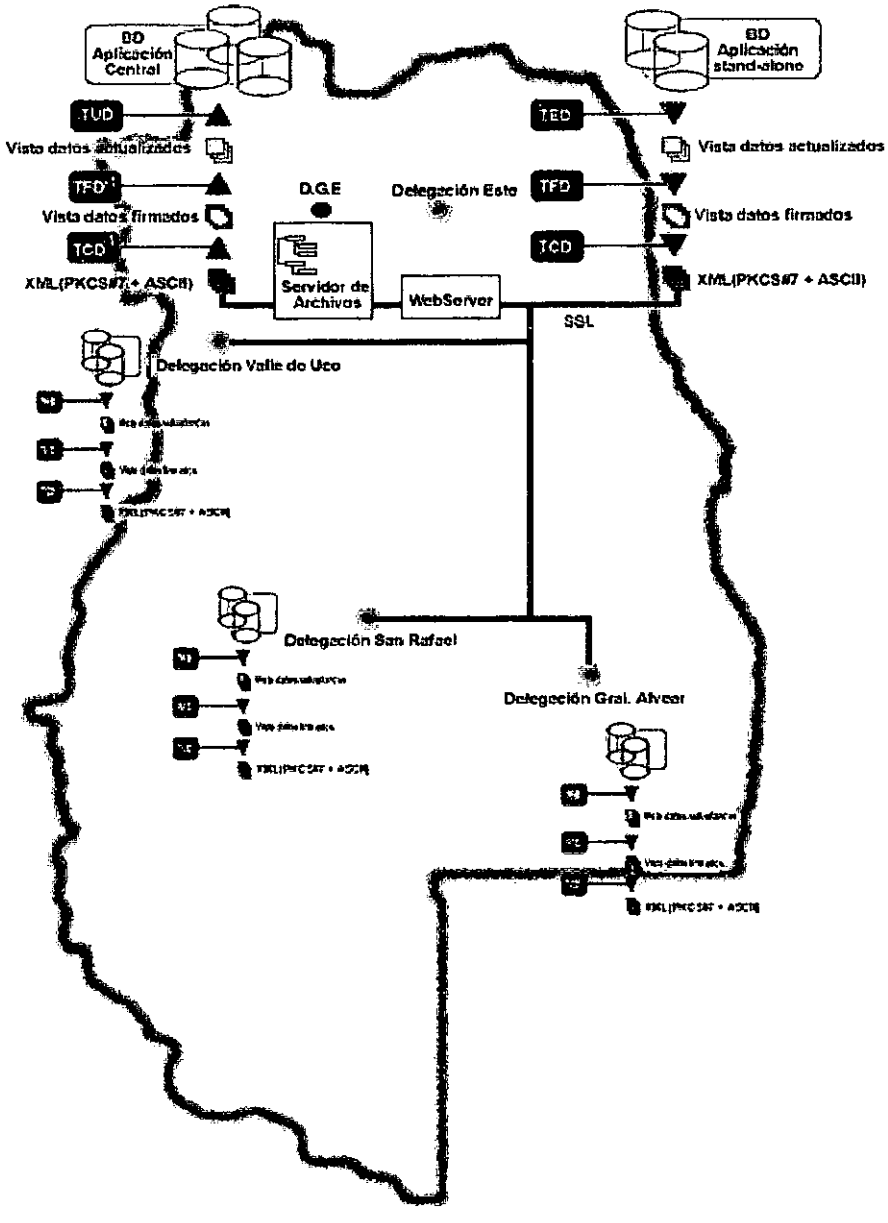
TCD Aplicación de encapsulamiento de datos criptográficos

***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 coinci-

den 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.

NombreDelegación

Antigüedad

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 sis-

tema 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 al sitio seguro usua-	▪ Intento de acceso al sitio seguro por canal http no seguro. ▪ Emisión de Certificados Digitales de prueba. ▪ Inclusión de Certificados de prueba en el repositorio de Certificados del sitio seguro. ▪ Intentos de ingreso con Certificados válidos.	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
	rios autorizados de las delegaciones administrativas o de la Administración Central.	▪ 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 de seguimiento y au-	▪ 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 mantenidos por el Application Server y por logs de transacciones del motor de base de datos.	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
	ditoría.		
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 intentos de generación de firma sobre	▪ Firma de múltiples archivos con distintas extensiones, formatos y atributos de acceso. ▪ Intentos de Firma con certificados válidos y no válidos	No se detectaron fallas en el funcionamiento del módulo. Frente a fallas forzadas del módulo o los certificados se com-

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
	archivos en distintos formatos.		probó 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 los mensajes de error y/o advertencia	▪ Establecimiento de puntos de control sobre el código de manejo de excepciones. ▪ 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	Se comprobó la pertinencia en la aparición de mensajes de error y advertencia. Se corrigieron errores de redacción sobre los textos de mensajes para favorecer su co-

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
		errores y su identificación mediante mensajes.	rrecta 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 verificación de firma.	▪ Prueba sobre múltiples archivos firmados, en distintos formatos, con distintos algoritmos de firma y con distintos certificados. ▪ 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.	No se detectaron fallas en el funcionamiento del módulo. El módulo de verificación informó 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, ya

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.	que los certificados emitidos por la ONTI adoptan este algoritmo de firma.

c. Pruebas de compresión y transferencia de datos

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
Índices de compresión de la información cifrada y firmada.	Evaluar los tamaños medios de archivos a transferir por el canal SSL.	Se firmaron y cifraron archivos en distintos formatos con tamaños que oscilaban entre 40Kb y 252Kb. Se cifró	

Formato	Tamaño RSA en Kb.	Tamaño Original en Kb.
.doc	13	40
.xls	22	69
.rtf	21	101

		con algoritmo RSA.	.dbf	28	252
Firma y cifrado de archivos grandes	Evaluar restricciones de tamaño ante tablas eventualmente muy grandes	Se firmaron y cifraron archivos .avi y .dbf de gran tamaño.		**Tamaño**	**Satisfactorio**
			.avi	290 Mb	SI
			.dbf	5 Mb	SI

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.

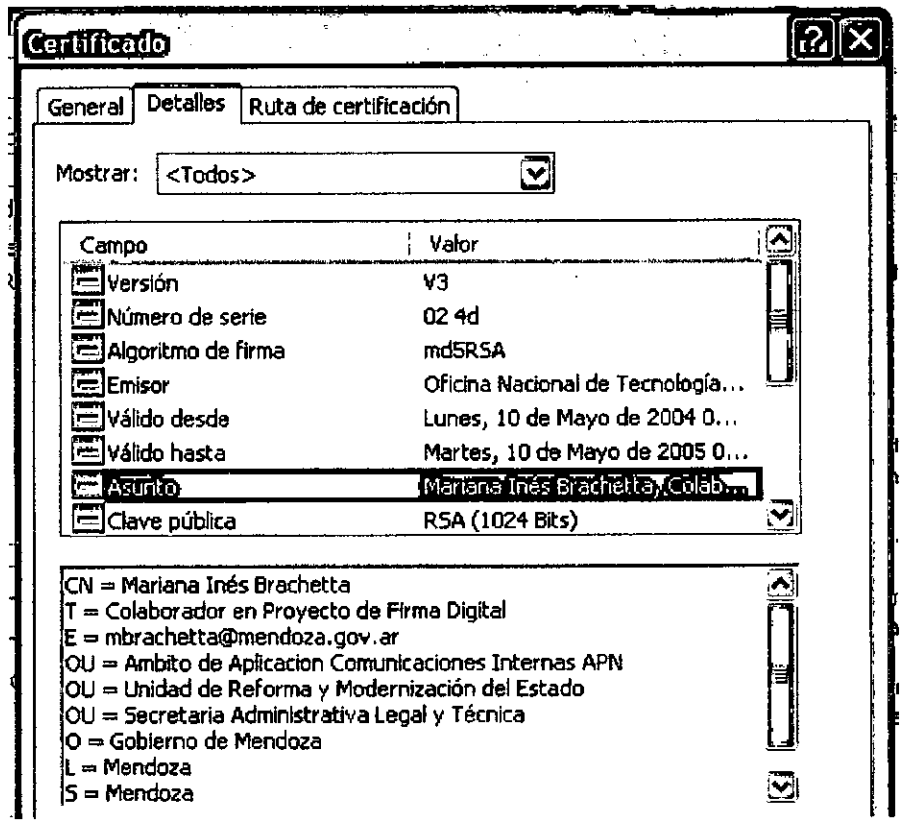
Para la implementación del circuito se dispone en cada Delegación de los siguientes recursos.

- 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

IV. Implementación de Experiencia de Sitio Seguro en la Penitenciaría Provincial:

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, continuamos dando respuestas a las necesidades de implementación de tecnología de firma digital, esta vez, en el ámbito de los sistemas de intranet en la Penitenciaría Provincial.

Hablamos de un "Sitio Seguro" cuando nos referimos a un lugar virtual confiable en Internet, perteneciente a una empresa u organización que lo mantiene en línea por medio de un servidor de www (World Wide Web).

Cuando una persona se conecta a un sitio seguro, el servidor presenta un certificado emitido y firmado por la Entidad Emisora de Certificados.

Los programas habitualmente utilizados para navegar por Internet (Browser o Navegador) deben estar configurados para aceptar certificados, que garantizan la confiabilidad del sitio, los que son emitidos por la Entidad Emisora de Certificados. Además, existe la posibilidad de ir más allá y asegurar la identidad de los usuarios del sistema utilizando la misma tecnología de certificación digital, es decir, garantizando al servidor que la persona que accede es aquella a la cual este le ha dado privilegios de acceso y si así lo establecen previamente podría ingresar la base de datos y agregar o modificar información sensible con total seguridad de que la única persona que pudo hacerlo es la titular del certificado digital.

A. Identificación de la necesidad:

El desafío planteado, en este apartado es determinar claramente cuáles son las necesidades de seguridad que el sistema demanda y cuáles son los fundamentos de la aplicación de tecnologías de clave pública en la Intranet de la Penitenciaría de Mendoza.

Tales conclusiones deberán surgir de la consideración del tipo de información que se está consultando y/o transfiriendo al sitio y la valoración de las posibles acciones que se puedan realizar en pos de quebrar la seguridad

que éste método sugiere en función de la evolución del poder computacional disponible.

Tipo de información que se maneja

La Intranet de la Penitenciaría Cuenta con un Sitio web por el cual se presenta y manipula información sobre:

- Antecedentes de los internos
- Situación Judicial de los internos
- Beneficios otorgados a los internos
- Actuaciones Disciplinarias
- Informes de Asistentes Sociales y Psicológicos
- Jornales de los internos
- Fondos de reserva (contaduría)

Tal información a su vez, se somete a eventos tales como:

- Alta , modificación y eliminación de contenidos on-line
- Consulta de contenidos desde todas las áreas del establecimiento , Poder Judicial , Ministerio de Seguridad y Justicia , Investigaciones , Policia, etc.
- Generación de números de pieza relacionadas con internos o personal.
- Consulta y carga en las bases de datos desde Internet.

Los indicadores más significativos son:

- Aproximadamente 300 antecedentes diarios son consultados mediante la web
- Se realizan 30 beneficios diarios
- Se confeccionan 100 boletas de audiencias a tribunales diarias

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 estos Activos 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 representan información sensible sobre los internos y su falsa manipulación o manipulación negligente podría provocar daños como:

- Daños y perjuicios a los titulares con las consiguientes acciones legales contra la dependencia.

- Otorgamiento de beneficios, jornales o cualquier otro tipo de valoración a los internos basados en antecedentes fraguados, no reales o tapados.

Entonces, la constitución de un SITIO SEGURO consiste en la seguridad en la comunicación a través de redes, especialmente Internet, consistente en prevenir, impedir, detectar y corregir violaciones a la seguridad durante la transmisión de información, más que en la seguridad en los ordenadores, que abarca la seguridad de sistemas operativos y bases de datos. Consideraremos la información esencialmente en forma digital y la protección se asegurará mayormente mediante medios lógicos, más que físicos.

Los mecanismos básicos pueden agruparse de varias formas para proporcionar los servicios previamente mencionados. Conviene resaltar que los mecanismos poseen tres componentes principales:

- Una información secreta, como claves y contraseñas, conocidas por las entidades autorizadas.
- Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado, hash (desmenuce de un mensaje compilado) y generación de números aleatorios.
- Un conjunto de procedimientos, que definen cómo se usarán los algoritmos, quién envía qué a quién y cuándo.

Asimismo es importante notar que los sistemas de seguridad requieren una gestión de seguridad. La gestión comprende dos campos bien amplios:

- Seguridad en la generación, localización y distribución de la información secreta, de modo que sólo pueda ser accedida por aquellas entidades autorizadas.
- La política de los servicios y mecanismos de seguridad para detectar infracciones de seguridad y emprender acciones correctivas.

Conclusiones/Identificación de la necesidad

Nuestro, entonces, es: ***Proteger, a través de un sitio seguro, la información contenida en la Intranet de la Penitenciaría de Mendoza 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 Sitio web.***

B. Análisis del sistema:

Cuando usamos un típico sistema de intranet, en el que mantenemos un sitio para brindar servicios y/o simplemente información dentro de una institución, como el usado actualmente por la Penitenciaría, tenemos (como usuarios), un débil nivel de identificación del sitio al cual accedemos, es decir, dadas las condiciones y variables del entorno puede resultar adecuado o no aumentar ese nivel de seguridad. Por ahora, lo que resulta un hecho es que el método utilizado actualmente no garantiza:

- ***Identificación unívoca***: el usuario no sabe que está ingresando a su sitio o a una réplica.
- ***Confidencialidad***: la información puede ser interceptada.
- ***Integridad:*** los datos pueden llegar incompletos y con posibilidad de error.
- ***No repudio:*** la información no es digitalmente firmada probando así que fue enviado por cierta persona evitando el rechazo de la misma.

Mejoras puntuales:

La implementación de sitio seguro en la intranet de la Penitenciaría persigue la efectiva consecución de las siguientes mejoras en la seguridad:

- **Protección de los sistemas de transferencia o transporte.** En este caso debemos garantizar, en el diseño del sistema la transferencia segura de la información de forma transparente al usuario final. Ejemplos de este tipo de planteamientos serían el establecimiento de un

nivel de transporte seguro, de un servicio de transmisión de datos seguro.

- **Gestión de claves:** Éste es un tópico de capital importancia, al que se aplica el uso de la criptografía y debe estar resuelto antes de que el usuario esté en condiciones de enviar un solo bit seguro. En el caso de las claves secretas el problema mayor consiste en mantener su privacidad durante su distribución, en caso de que sea inevitable su envío de un punto a otro. En el caso de clave pública, los problemas tienen que ver con la garantía de que pertenecen a su titular y la confianza en su vigencia (que no haya caducado o sido revocada).
- ***Identificación unívoca del servidor***: desde el sitio de la intranet necesitamos asegurarle a los usuarios que está ingresando al sitio de la penitenciaría y no a una réplica.
- ***Confidencialidad***: resulta de vital importancia garantizar que la información que se le carga al sistema llegue a la base de datos de una manera segura, evitando bajo todo punto de vista la interceptabilidad de la información
- ***Integridad:*** evitar la posibilidad de que los datos pueden llegar incompletos y con posibilidad de error.

C. Diseño de la implementación:

De acuerdo con la identificación de la necesidad básica y el relevamiento general de la situación actual hemos elaborado el diseño conceptual de la experiencia.

Un sitio seguro conlleva la emisión de **un certificado** (también conocido como certificado de clave-publica o identificador digital) es un documento electrónico, emitido por una Autoridad Certificadora, que **identifica de forma segura al poseedor del mismo** evitando la suplantación de identidad por terceros, es este caso del propio sitio web.

¿Cómo funciona?

•Client Hello : El "saludo de cliente" tiene por objetivo informar al servidor qué algoritmos de criptografía puede utilizar y solicitar una verificación de la identidad del servidor. El cliente envía el conjunto de algoritmos de criptografía y compresión que soporta y un número aleatorio. El propósito del número aleatorio es para que en caso de que el servidor no posea un certificado para comprobar su identidad, aún se pueda establecer una comunicación segura utilizando un conjunto distinto de algoritmos. Dentro de los protocolos de criptografía hay un protocolo de intercambio de llave que define cómo cliente y servidor van a intercambiar la información, los algoritmos de llave secreta que definen que métodos pueden utilizar y un algoritmo de hash de una sola vía. Hasta ahora no se ha intercambiado información secreta, solo una lista de opciones.

•Server Hello: El servidor responde enviando su identificador digital el cual incluye su llave pública, el conjunto de algoritmos criptográficos y de compresión y otro número aleatorio. La decisión de qué algoritmos serán utilizados está basada en el más fuerte que tanto cliente como servidor soporten. En algunas situaciones el servidor también puede solicitar al cliente que se identifique solicitando un identificador digital.

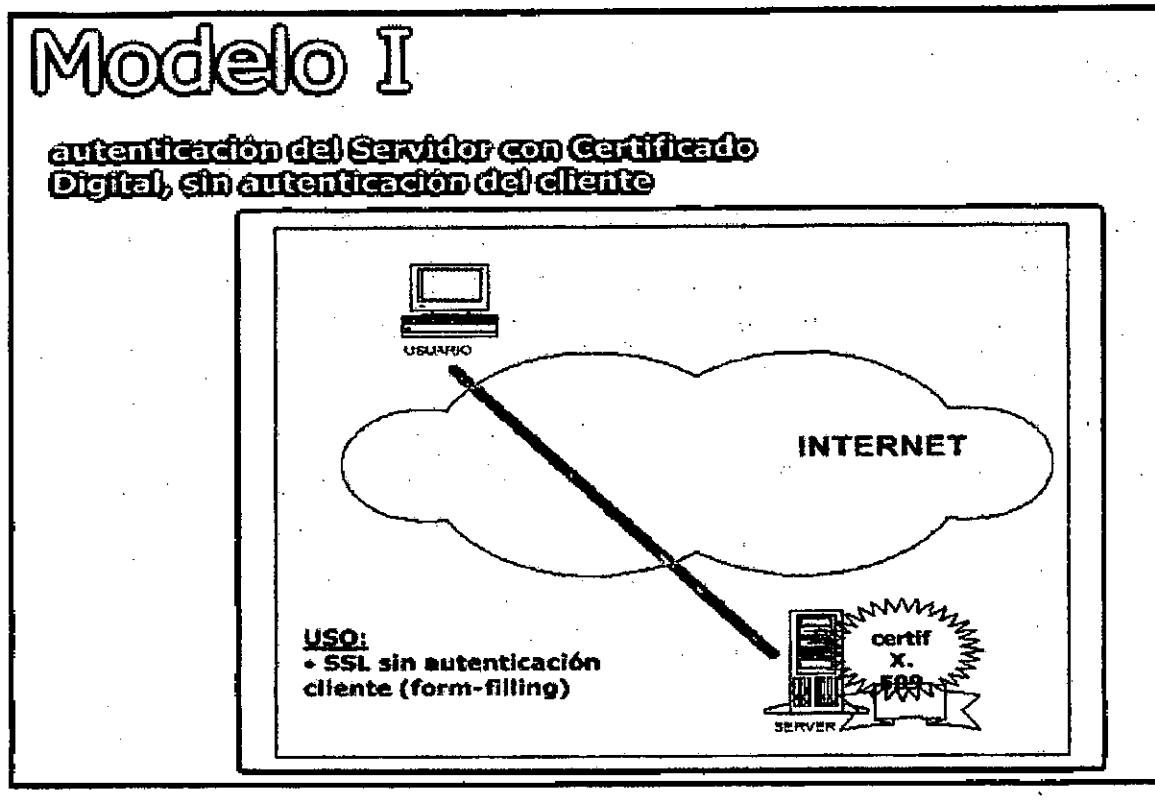
•Aprobación del Cliente: El cliente verifica la validez del identificador digital o certificado enviado por el servidor. Esto se lleva a cabo desencriptando el certificado utilizando la llave pública del emisor y determinando si este proviene de una entidad certificadora de confianza. Después se hace una serie de verificaciones sobre el certificado, tales como fecha, URL del servidor, etc. Una vez se ha verificado la autenticidad de la identidad del servidor. El cliente genera una llave aleatoria y la encripta utilizando la llave pública del servidor y el algoritmo criptográfico y de compresión seleccionado anteriormente. Esta llave se le envía al servidor y en caso de que el handshake tenga éxito será utilizada en el envío de futuros mensajes durante la sesión.

•Verificación: En este punto ambas partes conocen la llave secreta, el cliente por que la generó y el servidor por que le fue enviada utilizando su llave pública, siendo la única forma posible de desencriptarla utilizando la llave privada del servidor. Se hace una última verificación para comprobar si la información transmitida hasta el momento no ha sido alterada. Ambas partes se envían una copia de las anteriores transacciones encriptada con la llave secreta. Si ambas partes confirman la validez de las transacciones, el handshake se completa, de otra forma se reinicia el proceso.

Ahora ambas partes están listas para intercambiar información de manera segura utilizando la llave secreta acordada y los algoritmos criptográficos y de compresión.

Modelos

Concretamente existen dos modelos para mejorar la seguridad del sistema a través de la implementación de Sitio Seguro:



En el primer modelo la aplicación de ésta tecnología proporciona:

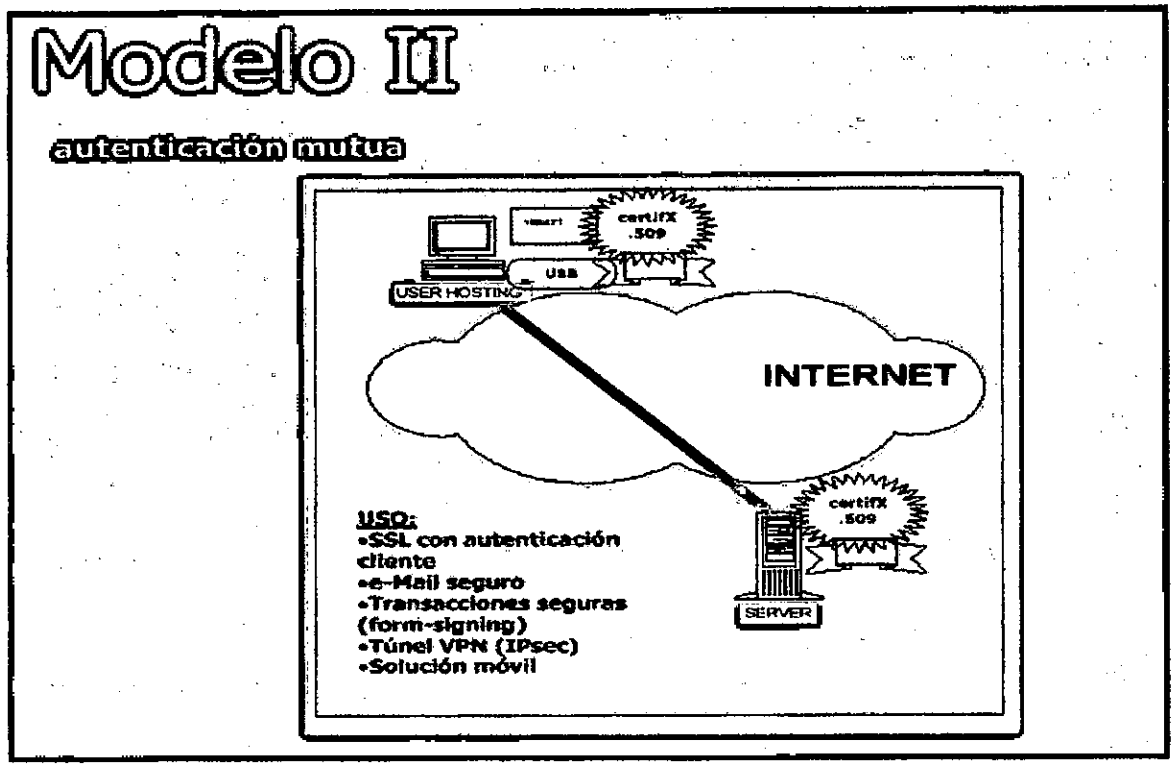
- **Autenticación unívoca del servidor seguro:** el cliente tiene la garantía de estar *hablando* con el servidor al que accede.
- **Privacidad en el intercambio de información:** sólo el cliente y el servidor seguro conocen lo que viaja por la red. Nadie distinto a ellos podrá leer la información que intercambien. Ahora que se ha establecido un canal de transmisión seguro SSL, es posible el intercambio de datos. Cuando el servidor o el cliente desea enviar un mensaje al otro, se genera un digest (utilizando un algoritmo de hash), encriptan el mensaje y el digest y se envía, cada mensaje es verificado utilizando el digest.

"Este modelo es el elegido y será usado para la transmisión de datos confidenciales de los usuarios de la intranet de la Peniten-

ciaría de Mendoza con el objeto de proveer una serie de garantías", a saber:

- ***Identificación unívoca***: Constituye una mejora fundamental al momento de aportarle al usuario la total seguridad de estar ingresando por el sitio oficial de la Penitenciaría y no en una réplica del mismo.
- ***Confidencialidad***: la información que viaje desde el usuario a la Base de Datos no podrá ser interceptada. Constituye una mejora radical en la seguridad en el traspaso de datos mediante herramientas de encriptado de información. Contribuye al aseguramiento de la integridad y veracidad de la información.
- ***Integridad:*** los datos enviados por usuarios llegarán completos y sin posibilidad de error, ya que la tecnología garantiza la verificación de la integridad de los mensajes mediante la aplicación de una función de hash. Cualquier diferencia, pérdida de datos, o modificación de los datos originales enviados será alertada por el sistema.

De esta forma, todos los datos provenientes de los usuarios que realizan altas, modificaciones, bajas o simplemente consultas se resguardan, mediante métodos de encriptación que aseguran la integridad y confidencialidad de la información que viaja por la web.



Modelo II: En el segundo modelo la aplicación de ésta tecnología proporciona:

- **Autenticación mutua entre el servidor seguro y el cliente.** El servidor sabe con total seguridad quien es el cliente que esta al otro lado y el cliente tiene la garantía de estar *hablando* con el servidor al que accede.
- **Privacidad en el intercambio de información.** Sólo el cliente y el servidor seguro conocen lo que viaja por la red. Nadie distinto a ellos podrá leer la información que intercambien. Ahora que se ha establecido un canal de transmisión seguro SSL, es posible el intercambio de datos. Cuando el servidor o el cliente desea enviar un mensaje al otro, se genera un digest (utilizando un algoritmo de hash), encriptan el mensaje y el digest y se envía, cada mensaje es verificado utilizando el digest.

"Este modelo representa una variante interesante para una futura extensión de la implementación de sitio seguro"

D. Desarrollo e implementación:

Instalación de la Plataforma de Desarrollo

La Intranet de la Penitenciaría provincial está montada sobre una Plataforma de Software Microsoft (Windows NT Server 4.0 + SP, IIS 4.0 con extensiones Active Server Page). Esto introduce cambios significativos en relación a los desarrollos de sitio seguro precedentemente implementados sobre plataformas Linux-Apache (Guía de Trámites) y Sun (Zona segura del sitio de resoluciones de la Secretaría Administrativa, Legal y Técnica) respectivamente. Por tal motivo se estimó conveniente instalar un servidor de desarrollo donde realizar la instalación y pruebas preliminares en lugar de operar directamente sobre el web-server en producción, a fin de preservar la integridad y disponibilidad de las aplicaciones que se sirven desde la Intranet Penitenciaria. Una vez que el proceso de instalación y configuración del sitio seguro estuvo debidamente probado y documentado se instrumentaron los cambios necesarios sobre el web-server en producción.

En esta línea de trabajo se instaló una plataforma de desarrollo con la siguiente configuración.

1. Windows XP-Professional SP2

2. Internet Information Server 5.0 con extensiones de servidor para Front Page y el complemento MMC (Microsoft Management Console)

Cabe aclarar que la penitenciaría cuenta con una plataforma basada en Sistema Operativo Microsoft NT Server 4.0 + SP e IIS 4.0. No obstante esto, se sugirió un upgrade a las nuevas versiones de software para mejorar las funciones generales de seguridad y administración del sitio. Por otra par-

te, se evaluó la documentación del software y se observó que la actualización de versiones no ha afectado los esquemas de trabajo con Sockets seguros (SSL) y el uso de certificados de autenticación de sitios. Además el upgrade entre versiones de S.O y web-server es directo.

Configuración del sitio de prueba

Una vez instalado el software de base se procedió a instalar y configurar un sitio web con fines de prueba. En consistencia con el diseño estructural de la Intranet Penitenciaria se configuró un único sitio en el home-directory por defecto de IIS ubicado en el directorio c:\inetpub\wwwroot\ y accesible mediante los IP 192.168.0.1 o http://localhost o http://black4 según la configuración establecida para el protocolo TCP/IP en el servidor de prueba.

Nota: black4 es el nombre del equipo donde está instalado el servidor de desarrollo; por tanto en la plataforma de desarrollo constituye el dominio para el sitio de prueba.

En primera instancia no se configuraron directorios virtuales, puesto que la estructura de sitio de la penitenciaría provincial no hace uso de esta característica y que es recomendable para el uso de Certificados de Servidor configurar un único sitio.

Para administrar el servidor se utilizó la internase de administración de equipos de Windows XP, Microsoft Mangement Console (MMC). Esta herramienta provee un panel de control para la administración de los servicios de Internet Information Server incluyendo configuración de sitios, mapeo de directorios virtuales, definición de documentos por defecto, manejo de errores, administración de usuarios, instalación de servicios y componentes, administración de logs y desarrollo de los esquemas de seguridad incluyendo comunicaciones seguras SSL.

Una vez instalada la plataforma de desarrollo se efectuaron configuraciones alternativas y pruebas para estudiar el manejo de esta herramienta de control y diseñar una configuración de sitio apropiada previo a la implementación de canal seguro SSL.

La instalación de la plataforma de desarrollo implicó la instalación manual de IIS, componentes adicionales y la configuración de sitio. Las configuraciones adecuadas fueron después instrumentadas sobre el servidor en producción con sistema operativo NT Server. Sin embargo, es importante documentar que ante una eventual actualización desde NT 4.0 a Windows XP Professional en el servidor en producción como se ha sugerido, IIS 5.0 se instalará de manera predeterminada adoptándose todas las configuraciones preexistentes por lo que no será necesario en principio ajustar configuraciones.

Emisión/ Instalación de Certificados para el Servidor

Como se ha mencionado previamente, el desarrollo de sitio seguro proporciona seguridad usando una combinación del protocolo SSL (Secure Sockets Layer) y certificados digitales.

Secure Sockets Layer (SSL) es un protocolo desarrollado inicialmente por Netscape Communications Corporation para dar seguridad a la transmisión de datos en Internet. Utilizando la criptografía de clave pública, SSL provee autenticación de servidor y validación de cliente, encripción de datos sobre la capa de transporte, e integridad de los datos en las comunicaciones cliente/servidor.

Para el Sitio Seguro de la Penitenciaría se implementó a través de SSL, cifrado de 128 bits totalmente compatible con los principales navegadores Microsoft y Netscape.

SSL maneja las comunicaciones encriptadas y la mutua autentificación entre navegadores y el servidor seguro. Los certificados SSL proporcionan autentificación para el servidor seguro.

En esta primera fase de desarrollo, se implementó sitio seguro con autenticación de servidor, pero sin validación de cliente. Esta implementación prescinde de la presentación de Certificados Digitales de usuarios en transacciones con el sitio seguro. En el esquema actual, el acceso restringido a la información se garantiza mediante la utilización de la autenticación de Windows integrada, básica o de texto implícita. Esto permite, sólo a los usuarios autorizados, ver todos los archivos y tener acceso a las aplicaciones de páginas Active Server en el servidor Web. También da control completo a los administradores sobre el sitio.

Bajo este esquema de desarrollo, el paso siguiente a la instalación de la plataforma y la configuración del sitio de prueba, consistió en la emisión de un Certificado de Servidor para el servidor de desarrollo.

Al igual que otros web-server IIS da la posibilidad de trabajar con certificados autofirmados o con certificados validados por una Autoridad Certificante. Ante la alternativa de trabajar con certificados autofirmados; se decidió utilizar los certificados que podía emitir la AC-URME (Autoridad Certificante de la Unidad de Reforma y Modernización del Estado), aún en su carácter de prototipo, con dos objetivos.

1. Probar los servicios del software PKI implementado y sus desarrollos complementarios, en una aplicación concreta y con un marco procedimental determinado.

2. Instaurar la necesidad de contar con una Autoridad Certificante a la hora de emprender este tipo de desarrollos. Esto tiende a generar conciencia de que es la Autoridad Certificante quien proporciona garantías concernientes a la identidad de la organización que provee el sitio web.

A continuación se presenta a modo de marco general, el ***procedimiento informático*** que debe desarrollarse para obtener un Certificado Digital firmado por una Autoridad Certificante (AC). Este procedimiento que algunas veces es transparente al usuario, es el que en general proponen la mayoría de la empresas líderes en Certificación Digital y los documentos de trabajo más aceptados en la industria. Así mismo, es totalmente coherente con los requisitos establecidos por la Ley 25.506 y sus normas complementarias.

1. El solicitante o suscriptor crea, haciendo uso de alguna herramienta proveedora de servicios criptográficos, un par de claves encriptadas, pública y privada.

2. Una vez creado el par de claves, el solicitante genera una petición de certificado basada en la clave pública. La sintaxis detallada de esta petición o CSR está descripta por el Estándar PKCS#10 de RSA. La petición contiene información sobre el suscriptor. En el caso de que éste sea un servidor habrá datos referentes al dominio, responsables y hosting del mismo.

3. El solicitante deberá entonces enviar la petición de certificado o CSR, junto con los documentos que prueben su identidad a una AC que resulte confiable para los usos a los que estará determinado el Certificado.

4. La Autoridad Certificante, a través de su Autoridad de Registro posiblemente, cumplimentará los procedimientos establecidos para verificar la identidad del suscriptor.

5. Una vez cumplimentadas las verificaciones pertinentes, la Autoridad Certificante firmará y enviará al suscriptor o responsable del sitio su certificado digital.

6. Luego los suscriptores deberán instalar los Certificados en su browser o en su servidor (en el caso de un certificado SSL) y utilizarlos para manejar transacciones seguras.

Presentado este marco general, documentamos a continuación detalladamente, el procedimiento informático que se siguió para emitir el Certificado SSL para el servidor de desarrollo.

La Interfase de Administración de Servicios de Internet Information Server incluye tres asistentes para administrar la seguridad de un sitio Web seguro. El Asistente para certificados de servidor Web permite administrar las características de Capa de sockets seguros (SSL) y los certificados de servidor. El asistente para CTL permite administrar listas de certificados de confianza (CTL). Las listas de certificados de confianza son listas de entidades emisoras de certificados de confianza para cada sitio Web o directorio virtual. El asistente de permisos permite asignar permisos de acceso NTFS y Web a sitios Web, directorios virtuales y archivos en el servidor.

En este punto, nos interesa documentar en particular el modo de operación del asistente para certificados de servidor Web. Este asistente permite solicitar, instalar y renovar los certificados de servidor a través de una interfaz gráfica. El asistente detecta si ya se ha instalado un certificado de servidor y si va a caducar. Los Certificados a instalar pueden ser emitidos por una Autoridad Certificante según el estándar X509 ya sea por una entidad emisora de certificados en línea, como los Servicios de Certificate Server de Microsoft o la CA de VeriSign, o por un archivo que se ha obtenido previamente en el Administrador de claves (KeyStore en IIS).

Para solicitar y posteriormente instalar el Certificado SSL en el servidor de desarrollo se utilizó este asistente siguiendo los distintos pasos:

1. Mediante el Asistente para la Certificados de Servidor Web de IIS, se generó el par de claves pública y privada y se emitió la Solicitud de Requerimiento de Certificados según lo prescribe la norma RSA PKCS#10. Como resultado de este proceso se obtuvo un archivo de

texto certreq.txt el cual contiene el requerimiento de emisión (CSR - Certificate Request).

Se agregó un usuario a la base de datos del prototipo AC-URME para procesar el requerimiento a nombre de este usuario. Los usuarios creados en la AC-URME permiten identificar a una entidad final o un servidor y gestionar el CVS de los Certificados asociados a esta entidad. A cada usuario en la ACURME se pueden asociar solicitudes y certificados en distintos estados: a la espera de ser aprobado, generado, revocado, etc.

2. Se procesó el requerimiento de emisión de certificado para el usuario black4 agregado, obteniéndose el certificado en formato PEM-Encoded.

3. Una vez obtenido el archivo ***black4.pem*** con el Certificado SSL firmado por la AC-URME, se procedió a instalar el certificado en el web-server. Esta instalación se realiza asociando el par de claves generadas previamente al archivo PEM-Encoded del Certificado mediante un wizard proporcionado por el Asistente para Certificados Web de IIS. Esta combinación de clave y certificado se almacena en un registro del servidor.

Configuración de SSL en IIS

Una vez instalado el certificado SSL en el servidor de desarrollo, se configuró SSL mediante el Administrador de Servicios de Internet del MMC (Microsoft Mangement Console).

IIS permite habilitar características SSL para todo el sitio o para determinados directorios físicos o virtuales mapeados en un sitio. Estos aspec-

tos son configurados desde la hoja de propiedades Directorios en la consola de administración del web-server.

Este modo de operación implica decidir, previo a la puesta en marcha del sitio seguro de la Penitenciaría Provincial, que tipo de contenidos deben ser asegurados mediante el uso de esta tecnología y determinar que directorios reales o virtuales dentro de la estructura de archivos del sitio deben ser protegidos. En particular, IIS requiere que para cada directorio que se desee proteger se configuren adecuadamente los siguientes aspectos.

- ***requerir canal seguro (SSL):*** esta opción debe estar activada para requerir un vínculo de comunicación cifrada (https) para ese directorio en particular.

- ***requerir cifrado de 128 bits:*** el nivel de cifrado también debe configurarse explícitamente para cada directorio a asegurar. En el caso de la Penitenciaría se decidió trabajar en todos los casos con cifrado de 128 bits.

- ***certificados de cliente:*** en primera instancia no se implementará autenticación de clientes para el sitio seguro de la Penitenciaría. Por ello se desactivaron las funciones vinculadas a la solicitud de certificados de cliente para cada directorio a proteger. La opción ***omitir certificados de cliente*** fue desactivada.

E. Prueba del Sistema:

Una vez instalada y configurada la plataforma de desarrollo, se diseño e instrumentó un conjunto de pruebas para evaluar la operatoria completa del Sitio Seguro en función del modelo de comportamiento esperado. En función de los resultados se realizaron los ajustes necesarios en la configuración del webserver y en el formato de los Certificados de prueba emitidos previo a la puesta

F. Puesta en marcha de la implementación

Concretada la etapa de pruebas se realizaron las actividades necesarias para la instalación y puesta en marcha de sitio seguro en el servidor en producción y la capacitación del administrador del web-server.

En un trabajo conjunto con el responsable informático de la Penitenciaría Provincial se fijaron pautas en cuanto a responsabilidades asumidas, procedimientos de trabajo y controles.

La puesta en marcha implicó el desarrollo de las siguientes tareas:

1. Definiciones finales sobre la metodología de implementación y puesta en marcha
2. Identificación de aplicaciones a proteger
3. Asignación de recursos y responsables
4. Capacitación de responsables
5. Emisión del Certificado de Servidor
6. Configuración de sitio seguro en el servidor en producción

Definiciones finales sobre la metodología de implementación

De acuerdo a los resultados positivos de las pruebas realizadas en la plataforma de desarrollo y a las características operativas de la Intranet Penitenciaria se decidió implementar los cambios directamente en el web-server en producción, previendo un resguardo de las configuraciones previas de IIS como previsión de contingencias. No existe en la plataforma tecnológica de la Penitenciaría un esquema de hardware redundante para prevenir caídas de servidores u otro tipo de mecanismos de protección que permitieran proponer un esquema de implementación alternativo.

Identificación de aplicaciones a proteger

En función de los niveles de seguridad definidos para la información, se decidió requerir conexión segura para todas aquellas aplicaciones que sirvieran contenido dinámico en función de bases de datos internas.

Asignación de recursos y responsables

El administrador de la Intranet penitenciaria fue asignado como responsable de la administración del sitio seguro y de la preservación de la clave privada del Certificado de Sitio.

Esta persona se desempeño durante la etapa de implementación, con el soporte permanente del equipo de desarrollo de firma digital y bajo el control del responsable informático de la Penitenciaría Provincial.

La implantación efectiva de sitio seguro no requirió extender la actual infraestructura de conectividad, equipos e insumos con que opera la Intranet Penitenciaria.

Capacitación de responsables

Se capacitó al Administrador del Web-Server en los aspectos técnicos y procedimentales relativos al uso de tecnologías de clave pública, el uso de certificados, el protocolo SSL, el perfil de certificados de servidor y la infraestructura PKI. Se profundizó especialmente en las configuraciones técnicas necesarias en el Administrador de Servicios de Internet Information Server para la implantación de canal seguro SSL.

El adiestramiento requirió cuatro jornadas de 4hs. realizadas en la oficina de Cómputos de la Penitenciaría Provincial.

Emisión e Instalación del Certificado de Servidor

Siguiendo el mismo procedimiento descrito en la fase de desarrollo, se procedió a obtener e instalar el Certificado SSL para el servidor en producción. La siguiente tabla describe el perfil del Certificado de Servidor que actualmente se encuentra operativo en la Intranet Penitenciaria.

Certificados de Servidor / SSL

El Certificado SSL fue emitido por la AC-URME a pedido formal del Responsable Informático de la Penitenciaría Provincial. No obstante se debe considerar que el carácter de prototipo experimental de la AC-URME restringe la validez y credibilidad del Certificado emitido. Por este motivo se ha solicitado formalmente a la ONTI (Oficina Nacional de Tecnologías de la Información) que contemple la posibilidad de adecuar su Autoridad Certificante para emitir Certificados de Autenticación de Equipos a personas jurídicas a través de nuestra Autoridad de Registro.

Configuración de sitio seguro en el servidor en producción

Una vez instalado el certificado SSL en el servidor en producción y determinados los directorios cuyo contenido sería accesible mediante canal seguro, se configuró el uso de SSL en el web-server del Servidor siguiendo, para cada carpeta en el Administrador de Servicios de Internet Information Server, el procedimiento documentado en la fase de desarrollo.

Este procedimiento fue realizado por los técnicos de la unidad en cooperación permanente con el Administrador del web-server de la Intranet Penitenciaria.

G. Evaluación de la experiencia:

Resulta necesario identificar las variables e indicadores más apropiados, y preparar o adaptar los instrumentos que se pueden utilizar para recoger la información, combinando métodos cualitativos y cuantitativos de investigación.

Hemos definido una serie de indicadores que son de gran utilidad a la hora de recoger feedback crítico. Nos servirán para evaluar los resultados de la experiencia piloto de Sitio Seguro en el tiempo y para diseñar las acciones correctivas que, en función de estos, resulten necesarias de implementar.

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 piloto Sitio Seguro (Mediciones realizadas al 07/01/05)	
Indicadores Cualitativos	**Métricas y Resultados**
Satisfacción de los usuarios:	No se han registrado quejas por el sistema
# Quejas y Reclamos	de Sitio Seguro
Indicadores Cuantitativos	**Métricas y Resultados**
Eficiencia:	
% de certificados emitidos correctamente	100 % (1 de servidor)
# de fallas del sistema	0 (No se produjeron fallas)
# de interrupciones del servicio	0 (El servició estuvo disponible 365/7)
Asistencia:	
# de asistencias otorgadas	8 (ocho) Acciones de asistencia técnica
% de asistencias exitosas	100%
Uso del Sistema:	
# de comunicaciones seguras establecidas	3123
Acciones correctivas detectadas	**Acciones correctivas implementadas**
No se han detectado hasta la fecha	Ninguna
Calificación ponderada final	
Implementación exitosa de la experiencia	

V. Participación en el proceso de reglamentación de la Ley

El hecho de que la tecnología de firma digital sea de reciente data, determinada la necesidad de acompañar los cambios legales que propone de una adecuada información sobre sus alcances y utilidades. El equipo de Firma Digital ha desarrollado las siguientes tareas relacionadas con el proceso de reglamentación de la ley 7234 :

- **Reuniones con los miembros de la Asesoría General de la Gobernación:** se mantuvieron reuniones con la citada dependencia, en donde se explicaron detalladamente los alcances y utilidades del proyecto de firma digital y se aclararon las tendencias nacionales y el estado actual de la materia.

- **Reuniones con Tribunal de Cuentas:** se realizaron reuniones participativas para aclarar los alcances de reglas constitucionales locales y las modificaciones al tratamiento de decretos, resoluciones, los modos de realización de trámites y las rendiciones de cuentas con vistas a la "despapelización del Estado".

- Se brindó asesoramiento desde los conocimientos específicos y Know How adquirido en materia de Firma Digital por parte del equipo del proyecto.

En la actualidad el proceso de reglamentación sigue vigente, ya se ha bocetado el articulado básico de la norma y se ha concientizado a las de-

pendencias legales. Sin duda aún queda mucho trabajo por hacer en ésta línea y también es necesario que la Nación termine de expedirse con la normativa relacionada al Licenciamiento. Por ahora, la tendencia adoptada por el equipo de firma digital es la realización de aplicaciones con el sustento legal atorgado por la ley a la firma electrónica que en muchos casos se equipara al de la firma digital y tecnológicamente no posee diferencia alguna.

VI. Investigación de nuevas tecnologías de firma digital

A. SELLADO DE TIEMPO / TIMESTAMPING

1. Introducción

En este apartado se informa sobre los resultados de la investigación y pruebas preliminares realizadas para determinar la factibilidad técnica y operativa de contar con un servicio de Sellado de Tiempo (TimeStamping) sobre las aplicaciones de firma digital desarrolladas.

El cuerpo del informe está dividido en tres bloques. En primer lugar se explica en que consiste el servicio de timestamping, cuál es la finalidad de aplicar un sello de tiempo sobre un documento electrónico, que arquitectura soporta al servicio, que entidades intervienen y cuáles son los estándares tecnológicos aplicables. El segundo bloque fundamenta la necesidad de disponer este servicio sobre las aplicaciones desarrolladas en el contexto del Proyecto de Firma Digital. Finalmente, se resumen las principales conclusiones y sugerencias obtenidas del proceso de investigación y pruebas, las cuáles emiten una recomendación final sobre el camino a seguir para un diseño detallado e implementación real de un proyecto de timestamping.

2. Sellos de Tiempo

Un sello de tiempo es un mecanismo tecnológico mediante el cual, una ***autoridad competente*** puede certificar que una determinada información existe en un ***instante de tiempo*** particular. El sellado de tiempo es una parte esencial del concepto de ***documento electrónico***, ya que permite certificar el momento de su emisión y eventualmente de su firma digital. El ti-

mestamping es el recurso del cuál se vale la tecnología PKI para garantizar la validez de una firma digital en el tiempo, aún después que caduca el certificado de clave pública asociado.

En un servicio de timestamping intervienen tres entidades:

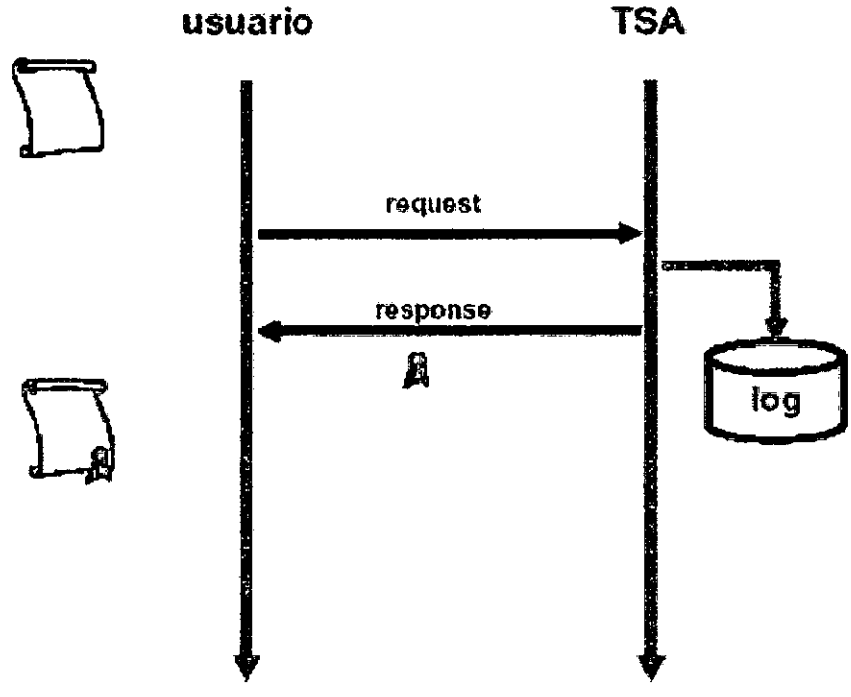
1. ***requester:*** Es la entidad que posee documentos, información o, en general, cualquier tipo de datos electrónicos a los que quiere incluir un sello de tiempo para probar que existían en un determinado instante.
2. ***verifier:*** Es la entidad que quiere comprobar que los datos sellados que ha recibido contienen un sello de tiempo válido. Puede ser la misma entidad que utilizó el servicio de sellado de tiempo, para comprobar que el sello generado es válido y correcto.
3. ***TSA (Time Stamping Authority):*** La Autoridad de Sellado de Tiempo es el proveedor del servicio. Su finalidad es la de comprobar la validez de los datos a sellar, obtener de una fuente o reloj fiable un parámetro de tiempo que indica el instante en el cual los datos se están sellando y generar el sello de tiempo que irá unido a esos datos. De esta forma, la TSA asegura que esos datos existían en una determinada fecha y garantiza que el parámetro de tiempo de ese sello es correcto.

Se describe a continuación el ***proceso de sellado de tiempo***, en el cual interactúan estas tres entidades:

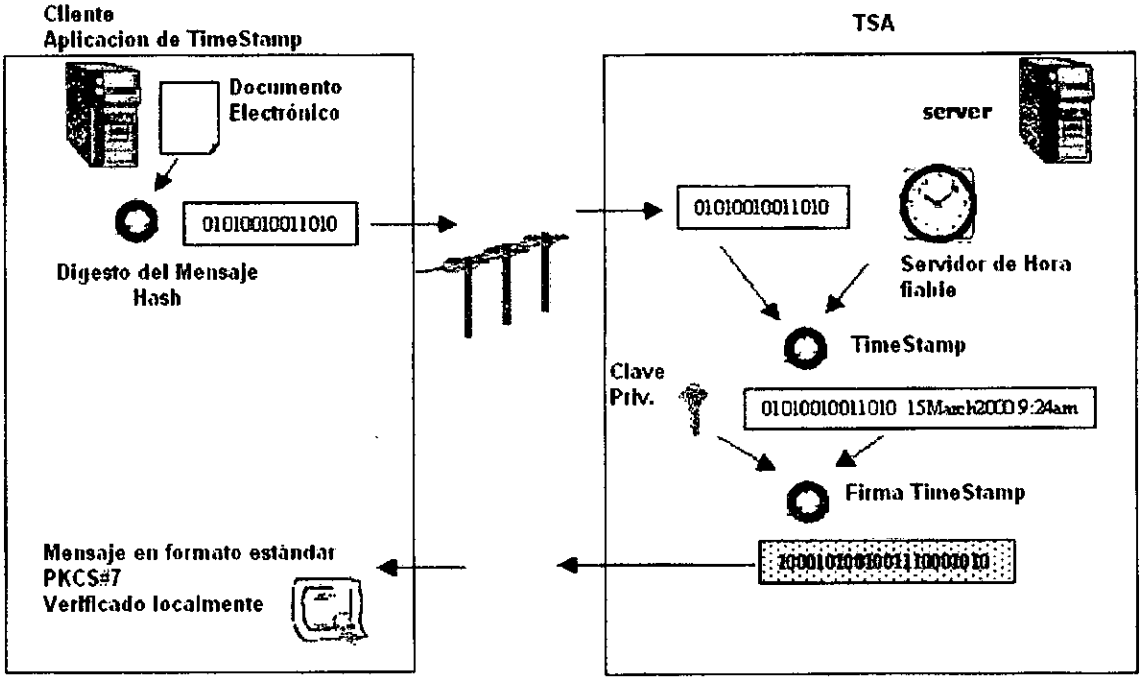
1. El requester que necesita sellar un documento electrónico u otro tipo de datos, genera, haciendo uso de alguna aplicación criptográfica, un hash del documento y construye un mensaje timestamp request que envía a la TSA. Según lo prescribe la RFC 3161 sobre el Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), un timestamp request ***(TimeStampReq)*** incluye los siguientes campos:
   - el hash generado
   - el nombre del algoritmo hash utilizado
   - *nonce*, un número suficientemente grande como para que la probabilidad de volver a generar el mismo sea muy pequeña.

de los cuales, sólo los dos primeros parámetros son obligatorios.

2. La TSA comprueba que el mensaje recibido sea correcto. En caso afirmativo, genera el sello o ***time stamp token***. El sello, según la recomendación, contendrá:
   - el parámetro de tiempo generado o recibido de una fuente fiable
   - el valor hash enviado por el *requester*
   - la información generada para unir criptográficamente el parámetro de tiempo con el hash de los datos
3. La TSA devuelve el sello a la entidad que lo pidió utilizando un mensaje ***time stamp response***
4. El *requester* debe comprobar el contenido del mensaje recibido. Normalmente recibirá el sello o, en caso contrario, un error. Si recibe el sello, comprobará que lo que se ha sellado es lo que se quería sellar y que el parámetro de tiempo incluido es válido, o en su defecto que el *nonce* sea el mismo.



Proceso de Sellado



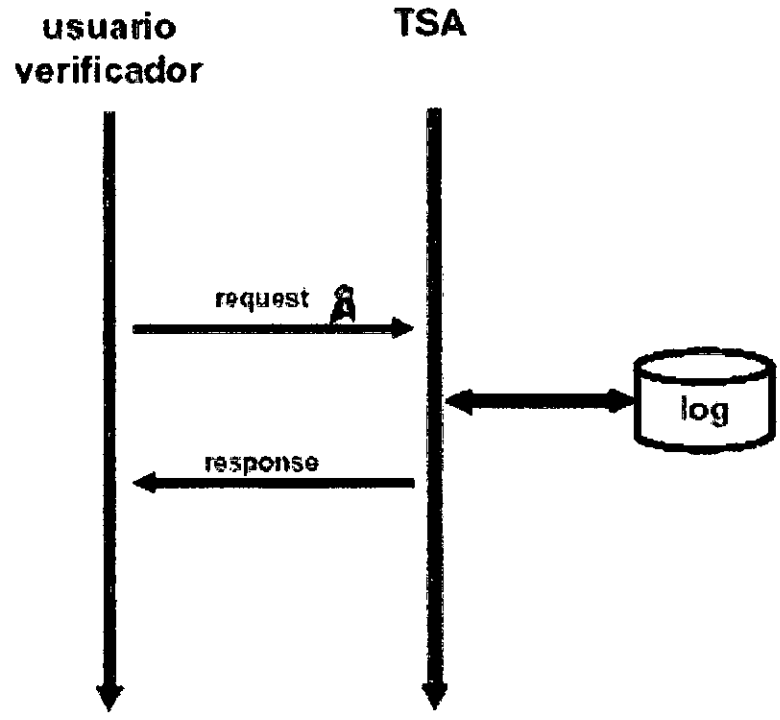
Intercambio de mensajes

Con respecto al proceso de verificación de un sello, no existe un proceso único de verificación. Esto depende del mecanismo que utilice la TSA para producir los sellos. A continuación describimos un modelo habitual en TSAs que utilizan clave privada:

Una entidad, en este caso el *verifier*, posee un documento auténtico (o una copia exacta) y su sello. Para comprobar la autenticidad de ese sello tiene que seguir los siguientes pasos:

1. Este primer paso se realiza lo realiza la entidad verificadora. Se realiza el hash del documento y se comprueba si coincide con el que contiene el sello
2. El segundo paso en verificar si el sello es auténtico. Para ello, el *verifier* envía un mensaje ***validate request*** a la TSA. En este mensaje va incluido el sello
3. La TSA comprueba que el sello enviado no sido falsificado y que fue creado por ella, comparándolo con el que tiene almacenado

4. Por último, la TSA devuelve a la entidad verificadora la confirmación de que el sello es auténtico y que fue creado en el instante de tiempo que indica, o un error si no fuese así.



Proceso de Verificación

Se documentan a continuación los ***aspectos más relevantes*** del servicio de TimeStamping, sobre los que se indagó en la ***investigación preliminar***.

Fuentes de tiempo fiable

Si bien la ISO e IETF únicamente comentan que se debe utilizar una fuente fiable de tiempo, lo que deja mucha libertad a la hora de implementarla; es fundamental que el parámetro de tiempo asociado al sello sea un parámetro internacionalmente válido y sumamente preciso. En general, las TSA obtienen este parámetro de máquinas sincronizadas a través del proto-

colo NTP (Network Time Protocol) con relojes atómicos o una señal GPS, es decir con servidores "stratum 1". [1]

Algunos de los relojes que habitualmente proporcionan parámetros de tiempo son:

- CH swisstime.ethz.ch (129.132.2.21) – Stratum 1 del Integrated Systems Laboratory, Swiss Fed. Inst. Of.
- DE ntp3.fau.de (131.188.3.223) - Stratum 1 de la University Erlangen-Nuernberg, D-91058 Erlangen, FRG
- Hora oficial americana- Observatorio Naval.

A modo de ejemplo se ha podido establecer que la hora oficial americana (la del observatorio naval) tiene una diferencia típica de 1 segundo y una máxima de 3 segundos, sin embargo, la información de los satélites GPS, tiene precisión aproximada de 130 nanosegundos.

Necesidad de una TSA (Time Stamp Authority)

Para garantizar una prueba fehaciente de la existencia de los datos electrónicos en un punto particular en el tiempo, es necesario una TSA que opere como tercera parte confiable.

El IETF da una definición más extensa de por qué es necesaria una TSA en el proceso de sellado de tiempo:

- para utilizar una fuente fiable de tiempos
- para incluir un valor de tiempo fiable en cada sello
- para incluir un entero único para cada nuevo sello

---

[1] Habitualmente, la señal de tiempo se suele generar por un reloj atómico o una señal GPS, medida por un ordenador, estos son los servidores "stratum 1", los relojes "stratum 2" se encuentran generalmente abiertos al público, una compañía podría mantener sus propios servidores de tiempo "stratum 3".

- . para producir un nuevo sello cuando se reciba una petición válida de un requester
- . para incluir en cada sello un identificador que indique la política de seguridad bajo la cuál ha sido creado
- . para sellar únicamente el hash de los datos
- . para verificar que la longitud del hash es conforme al algoritmo de hashing utilizado
- . para que no sean examinados los datos que se están siendo sellados nada más que para comprobar su longitud, tal y como se especificaba en el punto anterior
- . para firmar cada sello usando una clave generada exclusivamente para este propósito. Para ello, debe poseer distintas claves privadas para emplear diferentes políticas de seguridad, diferentes algoritmos, diferentes tamaños de clave privada.
- . para que no se incluya ninguna identificación del requester en el sello

La siguiente tabla aporta datos de ***TSAs de libre acceso con fines de prueba*** que fueron utilizadas en las pruebas preliminares de TimeStamping realizadas sobre la aplicación de Resoluciones con archivos en formato PDF.

hostname:port, IP_address:port or URL	***Protocolo***	***TSA web page***
tsp.test.polito.it:8318	Pure TCP (RFC3161)	http://security.polito.it/test/tsp/
tsa.cryptoapps.com:3318	Pure TCP (RFC3161)	n/a
http://195.223.2.6:8080/	HTTP	http://195.223.2.6

timestamp 195.223.2.6:3318	(POST) TCP-RFC3161	:8080
testtsa.actalis.it:318	Pure TCP (RFC3161)	n/a
http://www.edelweb.fr/cgi-bin/service-tsp https://clepsydre.edelweb.fr/dvcs/service-tsp	HTTP (POST) HTTPS (POST)	http://www.edelweb.fr/tsa.html
tsp.iaik.at:318 tsp.iaik.at:10318 http://tsp.iaik.at/tsp/TspRequest Port: 80 https://tsp.iaik.at/tsp/TspRequest Port: 443	Pure TCP SSL HTTP HTTPS	http://tsp.iaik.at
dse200.ncipher.com:318	Pure TCP (RFC3161) HTTP (POST)	n/a
http://info.szikszi.hu:8080/tsa https://info.szikszi.hu:8443/tsa	HTTP (POST) HTTPS (POST)	http://www.opentsa.org/

Formato de los Mensajes

Todos los mensajes intercambiados entre la TSA y los clientes, están representados en notación ASN.1

Se documenta a continuación las especificaciones de formato propuestas en la RFC3161.

Time Stamp Request

Representación ISO	Representación IETF
TimeStampReq ::= SEQUENCE {	TimeStampReq ::= SEQUENCE {
version Integer { v1(1) },	version INTEGER { v1(1) },
messageImprint MessageImprint,	messageImprint MessageImprint,
reqPolicy PolicyInformation OPTIONAL,	reqPolicy TSAPolicyId OPTIONAL,
nonce Integer OPTIONAL,	nonce INTEGER OPTIONAL,
certReq BOOLEAN DEFAULT FALSE,	certReq BOOLEAN DEFAULT FALSE,
extensions [0] Extensions OPTIONAL	extensions [0] IMPLICIT Extensions OPTIONAL
}	}

El significado de los campos es el siguiente:

- *versión*: número de versión de la sintaxis utilizada
- *messageImprint*: contiene el hash de los datos que se quiere sellar. La longitud del hash tiene que coincidir con la longitud de hash del algoritmo utilizado:

Representación ISO	Representación IETF
MessageImprint ::= SEQUENCE {	MessageImprint ::= SEQUENCE {
hashAlgorithm AlgorithmIdentifier,	hashAlgorithm AlgorithmIdentifier,
hashedMessage OCTET STRING	hashedMessage OCTET STRING
}	}

El algoritmo de hash indicado en *hashAlgorithm* debería ser uno conocido por la TSA. También comprobará que sea suficientemente fuerte. Si la TSA no reconoce el algoritmo usado o piensa que es débil, denegará el servicio al cliente y le mandará un mensaje de error indicando este problema con el algoritmo utilizado

- *reqPolicy*: indica a la TSA la política bajo la cuál quiere que se proporcione el sello
- *nonce*: permite al cliente comprobar el retardo en la respuesta cuando no se dispone de reloj local. La respuesta debe contener este mismo número o se rechazará
- *certReq*: si existe y está activado, la TSA debe proporcionar su certificado de clave pública en el mensaje de respuesta
- *extensions*: es una forma de permitir añadir nuevos campos en el futuro.

Si se incluye algún campo de extensión que la TSA no reconozca, ésta devolverá un mensaje de error de extensión no aceptada. El mensaje *time stamp request* no identifica al cliente, y esta información no es validada por la TSA. En el caso en que la TSA requiera su identidad deberá utilizar un mecanismo alternativo de identificación o autenticación.

Time Stamp Response

Representación ISO		Representación IETF	
TimeStampResp ::=	SEQUENCE {	TimeStampResp ::=	SEQUENCE {
status	PKIStatusInfo,	status	PKIStatusInfo,
timeStampToken	TimeStampToken OPTIONAL	timeStampToken	TimeStampToken OPTIONAL
}		}	

- *status*: tanto ISO como IETF remiten a la RFC 2510 para conocer la definición de la estructura *PKIStatusInfo*:

```
PKIStatusInfo ::= SEQUENCE {
status          PKIStatus,
statusString    PKIFreeText    OPTIONAL,
failInfo        PKIFailureInfo OPTIONAL
}
```

status: Si esta campo está a cero o a uno indica que el sello viene en el mensaje de respuesta. Para cualquier otro valor indica que el sello no viene en el mensaje de respuesta:

```
PKIStatus ::= INTEGER {
    granted   (0),          --a TimeStampToken, as requested, is present.
    grantedWithMods   (1),  --a TimeStampToken, with modifications, is present.
    rejection   (2),
    waiting   (3),
    revocationWarning   (4),   -- this message contains a warning that a revocation is
                               imminent
    revocationNotification (5)  -- notification that a revocation has occurred
}
```

statusString: puede usarse para indicar eventos de error

failInfo: indica las causas por las que no se ha generado el sello de tiempo

```
PKIFailureInfo ::= BIT STRING {
  badAlg            (0),      -- unrecognized or unsupported Algorithm Identifier
  badRequest        (2),      -- transaction not permitted or supported
  badDataFormat (5),          -- the data submitted has the wrong format
  timeNotAvailable (14),      -- the TSA's time source is not available
  unacceptedPolicy (15),      -- the requested TSA policy is not supported by the TSA
  unacceptedExtension (16), -- the requested extension is not supported by the TSA
   addInfoNotAvailable (17)  -- the additional information requested could not be
                                understood or is not available
   systemFailure      (25)   -- the request cannot be handled due to system failure
}
```

- *timeStampToken*: este campo es el que contiene el sello de tiempo generado. Se define como:

Representación ISO	Representación IETF
TimeStampToken ::= ContentInfo	TimeStampToken ::= ContentInfo

ContentInfo es una estructura que encapsula información firmada en una estructura TSTInfo. Está definida en la RFC 2630, y tiene los siguientes campos:

```
TSTInfo ::=  SEQUENCE {
        version                 Integer { v1 (1) },
        policy                  PolicyInformation,
        messageImprint          MessageImprint,
        serialNumber            Integer,
        genTime                 GeneralizedTime,
        accuracy                Accuracy OPTIONAL,
        nonce                   Integer OPTIONAL,
        tsa                     GeneralName OPTIONAL,
        extensions              [0] Extensions OPTIONAL
}
```

version: indica la versión del sello

policy: si se ha generado el sello, será igual al del mensaje de petición

messageImprint: será igual al del mensaje de petición

serialNumber: es un entero asignado por la TSA y debe ser único para cada sello que genere. Por tanto, un sello será

identificado por el nombre de la TSA que lo generó y el número de serie asignado

genTime: es el instante de tiempo en el que se creó el sello. Tanto ISO como el IETF expresan el instante de tiempo referido a la escala *UTC*, para evitar confusiones con las horas locales. El formato debe ser el siguiente:

CC YY MM DD hh mm ss Z

CC representa el siglo (19-99)
YY representa el año (00-99)
MM representa el mes (01 - 12)
DD representa el día (01-31)
hh representa la hora (00-23)

accuracy: en los casos que sea necesario, proporciona una precisión incluso de microsegundos:

```
Accuracy ::= SEQUENCE {
        seconds         [1] Integer OPTIONAL,
        millis          [2] Integer (1..999) OPTIONAL,
        micros          [3] Integer (1..999) OPTIONAL,
}
```

nonce: aparece si lo hace en el mensaje de petición, y tendrá el mismo valor

tsa: sirve para identificar a la TSA

extensions: están definidas en la RFC 2459

Validate Request

En la RFC 3161 del IETF no se contempla el proceso de verificación del sello de tiempo:

Representación ISO

ValidateRequest ::= SEQUENCE {
version INTEGER { v1(0) },
tst TimeStampToken,
requestID [0] OCTET STRING OPTIONAL
}

- *tst*: contiene el sello que se quiere verificar
- *requestID*: identificador que se utiliza para vincular una petición con su respuesta

Validate Reply

Representación ISO

ValidateReply ::= SEQUENCE {
version INTEGER { v1(0) },
status PKIStatusInfo,
tst TimeStampToken,
requestID [0] OCTET STRING OPTIONAL
}

- *status*: es similar al comentado para el mensaje *time stamp response*
- *requestID*: identificador que debe coincidir con el del mensaje *validaterequest* recibido

Mecanismos de producción de sellos de tiempo

La ISO en su normativa, define dos tipos de sellos:

Sellos Independientes

Un sello es independiente si, a la hora de verificar su autenticidad o su validez, la entidad verificadora no tiene que acceder a otro u otros sellos.

Hay tres tipos de TSAs diferentes que proporcionan este tipo de sellos:

- ***TSAs que firman con clave pública:*** en este mecanismo la TSA tiene una clave pública que utiliza para firmar los sellos. La ventaja reside en que si una entidad quiere verificar la autenticidad del sello puede hacerlo a través del servicio que proporciona la PKI sobre la que se apoya esta firma, y de esta forma, en la verificación no tiene por qué participar la TSA. El inconveniente es que este mecanismo requiere una PKI, lo que involucra listas de certificados y de revocaciones en el proceso de verificación.
- ***TSAs que firman con clave privada:*** en este mecanismo la TSA tiene una clave privada que utiliza para firmar los sellos. La ventaja respecto del caso anterior es que no se necesita una PKI, por lo que el mecanismo de producción y verificación de sellos se simplifica. El inconveniente es que se necesita de la TSA tanto para producir como para verificar los sellos. Además, la comunicación se debe hacer a través de un canal seguro para proteger los datos enviados.
- ***TSAs que almacenan evidencias:*** es parecido al caso anterior, pero ahora la TSA no devuelve ningún resultado, sino que almacena el sello como prueba de la existencia del documento sellado. La ventaja es que se reduce el tráfico de información confidencial a través de la red. La autoridad se encarga de generar el sello y almacenarlo. El inconveniente, además de que es necesario la participación de la TSA en el proceso de verificación, está en que ésta debe ser muy fiable ya que,

si se produjese algún problema de seguridad, se pondría en entredicho la validez de los sellos almacenados.

Sellos enlazados

Un sello está enlazado (*linked* token) cuando se le relaciona criptográficamente con otros sellos. De esta forma se aumenta la seguridad del sistema y disminuye el nivel de fiabilidad requerido para una TSA. Se basa en el uso del hashing. El sello enlazado se forma gracias a tres operaciones: agregado, enlazado y publicación que se pueden combinar de diferentes formas. La documentación detallada de este proceso puede consultarse en la RFC 3161.

Tipos de Documentos Electrónicos que soportan TimeStamping y restricciones de tamaño

Según la documentación consultada se puede sellar cualquier tipo de archivo digital tales como:

- documentos ofimáticos .doc, .xls, .mdb
- presentaciones
- e-mails
- archivos de audio .wav, .mp3, etc.
- archivos de video
- correos de audio
- imágenes
- faxes
- transacciones financieras y documentos bancarios
- subastas on-line
- software
- derechos de autor
- bases de datos

En particular, se realizaron pruebas de sellado sobre documentos en formato ***PDF (Portable Document Format)*** en el contexto de la aplicación de Resoluciones de la Secretaría Administrativa, Legal y Técnica

Se comprobó que no existen restricciones sobre el tamaño de los archivos a sellar. La documentación de algunas TSAs comenta que el límite es superior a 264 bits o 4x109 gigabytes, una cantidad unos cuantos millones de veces superior a la capacidad de un ordenador doméstico. Este límite lo impone el algoritmo que utilizan para realizar el hash de los datos. En definitiva, el único inconveniente para una aplicación real de sellado, es el tiempo que tarde en generarse el hash, ya que dependerá del tamaño del documento. Las pruebas realizadas sobre resoluciones en formato .pdf se concretaron en un tiempo de respuesta promedio de 40 segundos, medido desde inicio a fin de la transacción de sellado sobre el documento.

Estándares aplicables

Se informan a continuación las principales normas, estándares y recomendaciones aplicables al tema de TimeStamp que fueron consultadas.

- ***RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP):).*** Este documento se centra en la implementación de una autoridad de sellado de tiempo (TSA), y en los requisitos de seguridad que debe cumplir, además de especificar los diversos mecanismos que pueden ser utilizados para la petición y generación de sellos. En particular este documento describe el formato de los mensajes TimeStampRequest, TimeStampResponse y del TimeStampToken.
- ***ISO/IEC 18014:*** Standard de propósito intenacional que define el servicio de time-stamping, los protocolos aplicables al transporte de mensajes y sellos, y los mecanismos de producción de sellos.
  - ***ISO/IEC 18014-1 Time stamping services - Part 1 - Framework:*** Documento preliminar sobre el servicio en donde se identifica el objetivo de una TSA, se describe el modelo general sobre el cual

se basan los sellos de tiempo y se definen protocolos básicos de comunicación entre las entidades involucradas.

- ***ISO-IEC 18014-1 Part 2 - Mechanisms producing independent tokens***: Este documento define el modelo y los mecanismos para trabajar bajo el esquema de sellos independientes.
- ***ISO/IEC FDIS 18014-3: 2003 Part 3:*** Mechanisms producing linked tokens: Este documento define el modelo y los mecanismos para trabajar bajo el esquema de sellos enlazados.

3. Sellado de Tiempo de una Firma Digital

Se explican a continuación los motivos que justifican un estudio sobre TimeStamping en el contexto del desarrollo de aplicaciones de firma digital.

Uno de los principales usos del servicio de TimeStamping es el sellado de firmas digitales para probar que la firma fue creada antes de un instante particular en el tiempo y, fundamentalmente, que el certificado de clave pública asociado a la firma era válido en el instante de tiempo en que se construyó la firma.

Lo anterior, permite prolongar la validez de una firma digital más allá del período de validez del certificado asociado, que en general no supera los 365 días para personas físicas.

Otorgar perdurabilidad en el tiempo a la validez de una firma digital sobre un documento digital resulta necesario en la ***aplicación de Resoluciones de la Secretaría Administrativa, Legal y Técnica*** y en la aplicación de ***descentralización de la gestión administrativa de la Dirección General de Escuelas***, puesto que es necesario que las aplicaciones de verificación de firma en ambos casos indiquen que la firma es válida aún después de caducados los certificados.

Contando con un sello de tiempo se pueden chequear por ejemplo las CRLs a esa fecha para determinar la validez de los certificados o la política de no repudio asociada a la firma en ese momento.

Según lo especifica la ***RFC 3161*** en su Apéndice B, para aplicar un sello de tiempo a una firma digital debe seguirse la siguiente técnica básica:

1. El requester, genera la firma digital.
2. La firma es presentada, a la Autoridad de Time Stamping (TSA. La TSA retorna entonces el TimeStampToken (TST) sobre la firma.
3. El requester (o invoker) del servicio debe entonces verificar que el TimeStampToken es correcto.

La verificación de una firma con sello de tiempo se realiza siguiendo los siguientes pasos:

1. Se debe recuperar el TimeStampToken y verificar que el mismo esta aplicado a la firma de un firmante en particular.
2. Se debe recuperar el parámetro de tiempo (date/time) indicado por la TSA en el TimeStampToken.
3. Se debe identificar y recuperar el certificado utilizado por el firmante.
4. Se debe comprobar que el parámetro de tiempo indicado por la TSA en el TimeStampToken se encuentre en el período de validez prescripto para el certificado. Esto permite verificar que el certificado no había caducado cuando se generó la firma.
5. Se debe recuperar la información de revocación (CRL), asociada al certificado del día y hora en que se emitió el sello de tiempo, y verificar que el certificado no figure como revocado a esa fecha.

Si todas estas condiciones son satisfactorias entonces la firma podrá ser declarada como válida.

Los pasos descriptos, tanto en el proceso de sellado como de verificación de una firma sellada, son desarrollados por ***aplicaciones*** que resuelven ambos problemas. El estudio realizado implicó la realización de pruebas con aplicaciones de firma y sellado de documentos en formato PDF (Porta-

ble Document Format). En particular se trabajó con aplicaciones trial de las firmas Ascertia e IPSca. También se realizaron pruebas con versiones trial de Adobe Professional 7.0.; y se indagó la factibilidad de desarrollar un plugin propio de sellado para actualizar el desarrollo de firma realizado en instancias anteriores.

Cabe señalar que a partir de la versión 7.0 Acrobat Reader incorpora funciones de verificación de sellos de tiempo sobre firmas digitales, con lo cual el software realiza todos los pasos descriptos anteriormente para declarar válida una firma aún cuando el certificado del firmante haya caducado o haya sido revocado.

En las pruebas se trabajó con las TSAs mencionadas previamente y en todos los escenarios de prueba configurados, la aplicación de un sello de tiempo sobre resoluciones firmadas fue satisfactorio.

4. Conclusiones

Desde el punto de vista técnico el estudio realizado conduce a la conclusión de que el servicio de sellado de tiempo funciona y resuelve el problema planteado (otorgar validez en el tiempo a las firmas digitales de documentos electrónicos).

El problema reside en la imposibilidad de contar con una Autoridad de Sellado de Tiempo (TSA) en el ámbito de la Administración Pública que cumpla con las condiciones operativas y de seguridad requeridas, cuyos propósitos no sean de prueba o comerciales.

La Infraestructura Nacional de Firma Digital aún no ha realizado avances en este sentido. Por otra parte, resulta inviable en relación a los objetivos del Proyecto de Firma Digital pensar en concretar el desarrollo e implementación de una TSA propia para la Provincia de Mendoza.

En este contexto, entendemos que es conveniente esperar a que la Nación avance en el desarrollo de una TSA que brinde el servicio. Para dar prioridad al tema en el orden de discusión nacional se han cursado pedidos a los equipos técnicos de la ONTI (Oficina Nacional de Tecnologías de la

Información) y a la Comisión Asesora de Firma Digital fundametando la demanda.

VII. Identificación de nuevas implementaciones

A través de la realización de sondeos de nuevos ámbitos de implementación de firma digital, la aplicación de nuestra estrategia de identificación de procedimientos, se realizaron reuniones con los principales responsables y usuarios de los procesos identificados y se generaron nuevas ideas de implementaciones y experiencias relacionadas con tecnología de Firma Digital.

Se realizaron reuniones con autoridades y directores de informática de la DGE (Dirección General de Escuelas) y del Registro del Estado Civil y Capacidad de las Personas y se llegó a bocetar una nueva implementación. Se trata de facilitar el proceso de pedito y entrega de Partidas de Nacimiento para su presentación en las Escuelas en los inicios del ciclo lectivo, mediante la aplicación de tecnologías de firma y timbrado digital. Las precisiones y alcances de este proyecto serán detallados oportunamente, por ahora podemos asegurar que el circuito a desarrollar tendrá las siguientes características y fundamentos a la luz de nuestra **Estrategia para la Identificación de Procedimientos Aptos.**

Guías de aplicación

- Transacciones electrónicas: la administración pública provincial puede expandir la prestación de sus servicios y acercarse al ciudadano a través de transacciones electrónicas seguras. Cuando dichas transacciones revisten características particulares de importancia se puede estimular la aplicación de las tecnologías de firma digital para evitar sobrecostos o generar ahorros fomentando la transparencia en el accionar público.

- 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.

Criterios de selección de circuitos administrativos

- Corresponde a Trámites con alta frecuencia de repetición a cargo de la misma oficina, ente o persona.
- Circuito que requieren autenticación de las partes involucradas
- Circuito administrativos que enlazan importantes distancias geográficas
- Circuito basado en gran cantidad de papeleo
- Circuito administrativo de transferencia de información sensible

Criterios de selección de transacciones aptas para ser firmadas digitalmente

- Requiere efectiva autenticación de personas o entes involucrados en la transacción para demostrar "interés legítimo" en la solicitud de una partida.

Criterios de selección de transacciones aptas para ser encriptadas

- Contiene información estrictamente confidencial
- Contiene información que no debe estar disponible públicamente sin filtros previos

Tales pautas fueron el marco conceptual a tener en cuenta a la hora de seleccionar y priorizar este proyecto que ha diferencia de las anteriores implementaciones será creado y definido a priori teniendo en cuenta directamente los potenciales beneficios y ahorros que la aplicación de la tecnología puede producir.