GOBIERNO DE MENDOZA

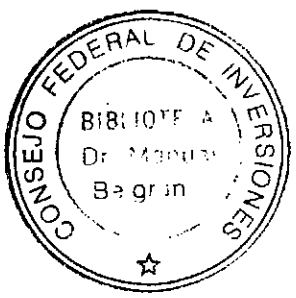
SECRETARÍA ADMINISTRATIVA LEGAL Y TÉCNICA

UNIDAD DE REFORMA DEL ESTADO

---

firma Digital

Primer informe parcial



CONSEJO FEDERAL DE INVERSIONES

CONSULTOR: LIC. PABLO GUILLERMO LIOY

Fecha de impresión 28/09/2004 1:23

ÍNDICE

I. Introducción

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

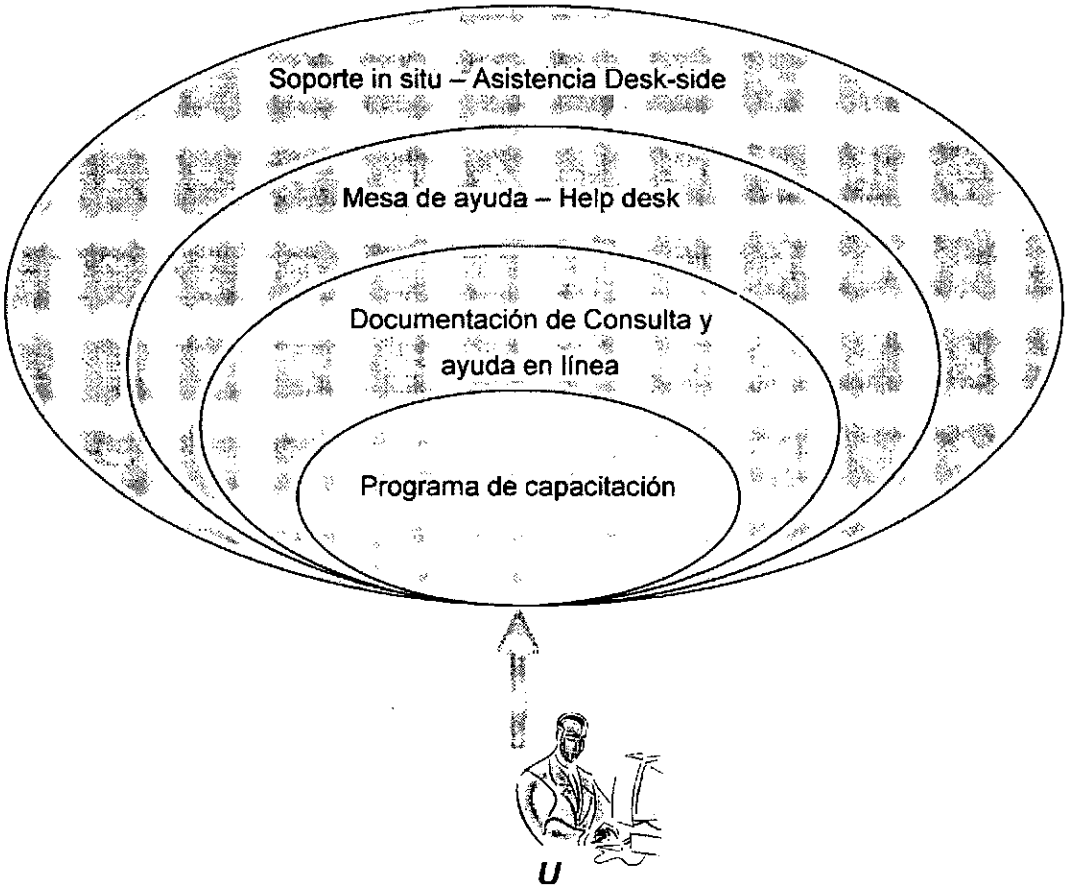
Actividad	Estado
1. ***Extensión de la Experiencia Piloto de Repositorio de Normas Legales con Firma Digital:***	Concluida
• Soporte continuo: se responderá a los requerimientos de soporte de los usuarios y operadores del sistema.	Concluida
•Seguridad y backup: se planificará y desarrollará procedimientos y mecanismos de seguridad preventiva y correctiva a nivel físico y lógico sobre los datos contenidos en el repositorio.	Concluida
•Mantenimiento del ciclo de vida del sistema: se garantizará la dinámica, flexibilidad y escalabilidad del sistema a través de la retroalimentación y actualización permanente.	Concluida
•Carga de datos históricos: se desarrollará y aplicará 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.	Concluida

Primer informe parcial: la culminación de la actividad 1 se presentará a los dos meses de iniciadas las tareas.

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*** [1] 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.

---

[1] *Ver Anexo - Manual de Usuario Digesto Digital*

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 mis-

ma, 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.

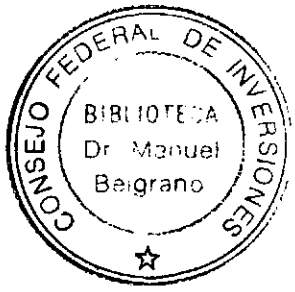
Producir aplicaciones en las cuales el usuario pueda aprovechar el potencial del paradigma de la navegación de sitios *web*, mientras ejecuta transacciones sobre bases de información, es una tarea que requiere de un profundo conocimiento de los requerimientos y un cuidadoso esfuerzo de diseño. Si se 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 mu-

chos 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. desarrollados 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.

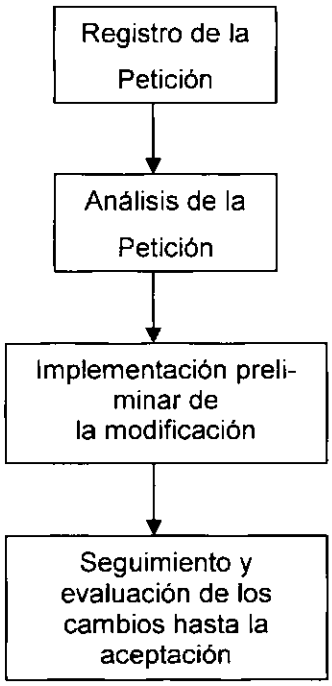
Las tareas de desarrollo que sea necesario realizar son determinadas en función de los componentes del sistema afectados por la modificación. Estas tareas pertenecen a actividades de los procesos Análisis, Diseño, Construcción e Implantación.

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:



Presentamos a continuación una breve descripción de cada actividad y los instrumentos de documentación que se aplican a cada una. Finalmente documentaremos las peticiones de mantenimiento solicitadas hasta el momento y su procesamiento.

Actividad 1: Registro de la Petición

El objetivo de esta actividad es establecer un sistema estándar para documentar peticiones de mantenimiento, con el fin de controlar y canalizar los cambios propuestos por los usuarios, proporcionando una gestión efectiva del mantenimiento.

Es importante asignar responsabilidades para evitar la realización de cambios que beneficien a un usuario o sector de usuarios, pero que produzcan un impacto negativo sobre otros muchos. Se debe recordar, que la proyección es escalar el repositorio a otras áreas del Poder Ejecutivo, en cuyo caso se dará soporte a sectores usuarios con necesidades potencialmente diferentes. Por tanto, es necesario que todas las peticiones de mantenimiento sean presentadas de una forma estándar, que permita su clasificación y facilite la identificación del tipo de mantenimiento requerido.

Una vez que la petición ha sido registrada, que se ha determinado el tipo de mantenimiento y los módulos a los que inicialmente puede afectar, se comprueba su viabilidad.

El instrumento que prevé la *MME* para concretar esta tarea es un *catálogo de peticiones*, el cual servirá de base para abordar, en tareas posteriores, el análisis de la petición, realizar la modificación solicitada y proporcionar datos estadísticos sobre peticiones recibidas o atendidas.

En el caso de que la petición involucre un mantenimiento correctivo, se debe consignar en el catálogo una completa descripción de las circunstancias que llevaron al fallo, adjuntando datos de entrada, mensajes de error, o cualquier otro material de soporte que se considere oportuno. Para peticiones de mejora se debe remitir una especificación de los requisitos a contemplar. En cualquier caso, será imprescindible recoger la identificación, origen y tipo de petición, asignarle una prioridad inicial e incorporar una descripción, lo más precisa posible, que facilite su posterior análisis.

Hoja de Registro Petición de Mantenimiento				
Petición de Mantenimiento N°.:		*Prioridad Preliminar Asignada:*		
Tipo de Mantenimiento:	☐*Correctivo*	☐ *Evolutivo*	☐ *Adaptativo*	☐ *Perfectivo*
Fecha de la petición:		*Sector Usuario / Usuario:*		
Descripción de la petición:				
Documentación y Anexos que se adjuntan:				
Requerimiento registrado por:				

Actividad 2: Análisis de la Petición

En esta actividad se lleva a cabo el diagnóstico y análisis del cambio pedido. Se analiza el alcance de la petición en lo referente a los módulos y capas del repositorio afectadas, valorando hasta que punto pueden ser modificados en función del ciclo de vida del software, las posibilidades de desarrollo técnico y el impacto sobre el sistema en su conjunto.

El enfoque de este estudio varía según el tipo de mantenimiento, teniendo en cuenta que en el caso de un mantenimiento correctivo que implique un error crítico debe abordarse el cambio de forma inmediata sin profundizar en el origen del mismo. No obstante, una vez reanudado el servicio, es imprescindible analizar el problema y determinar cuál es la solución definitiva.

El instrumento previsto para esta tarea es un informe descriptivo del análisis que incluya como mínimo la siguiente información:

- Petición de mantenimiento N°:
- Fecha y responsables del análisis:

- Análisis preliminar e identificaciones de requerimientos
- Identificación de propuestas de solución alternativas
- Estudio de viabilidad e impacto
- Módulos del sistema sobre los que impacta el o los cambios propuestos:
- Resolución final sobre la viabilidad o no de efectuar los cambios.
- Aceptación o rechazo de la petición.
- Curso de acción a seguir, propuesta elegida.
- Asignación de responsables de efectuar el mantenimiento.
- Prioridad asignada al tratamiento de la petición.
- Plazos de ejecución estimados.

Este informe deberá ser adjuntado a la *Hoja de Registro* de la petición.

Actividad 3: Implementación preliminar de la modificación

Una vez finalizado el estudio previo de la petición y aprobada su implementación, se pasa a identificar de forma detallada cada uno de los elementos afectados por el cambio mediante un análisis de impacto. Este análisis tiene como objetivo determinar qué parte del sistema y en que capa se verá afectada; y en qué medida, dejando claramente definido y documentado qué componentes se deben modificar, tanto de software como de hardware si fuera necesario.

Si la modificación lo requiere se deberán realizar en esta etapa los estudios, consultas o investigaciones necesarias sobre tecnologías y herramientas de desarrollo que se deban aplicar al desarrollo.

Contando con los elementos previos, se podrá fijar un plan de acción con el fin de cumplir el plazo máximo de entrega.

Una vez aceptado el plan de acción, se activan los correspondientes procesos de desarrollo para llevar a cabo la implementación de la solución.

Al mismo tiempo, se especifican las pruebas de regresión con el fin de evitar el efecto onda en el sistema, una vez realizados los cambios.

Los instrumentos previstos en la *MME* para documentar esta actividad son:

- *Plan de Acción* previsto para los cambios: se deberán planificar tareas, recursos, tiempos y responsables, indicando puntos de control para el seguimiento del plan.
- *Documentación de análisis, diseño y desarrollo* de los cambios: estos documentos se construirán con las metodologías habituales de documentación de sistema, y deberán integrarse y complementar la documentación original del sistema.
- Especificación del *Plan de Pruebas de Regresión*: en este documento se deberán especificar los casos de prueba en función de las relaciones existentes entre los distintos componentes del software y de la información mantenida en las bases de datos.

Actividad 4: Seguimiento y evaluación de cambios hasta la aceptación

En esta etapa, se realiza el seguimiento de los cambios que se están llevando a cabo en los procesos de desarrollo, de acuerdo a los puntos de control establecidos en el *Plan de Acción*. Durante este seguimiento, se comprueba que sólo se han modificado los elementos que se ven afectados por el cambio y que se han realizado las pruebas correspondientes, especialmente las pruebas de integración y de sistema. Del resultado obtenido se hace una evaluación del cambio para la posterior aprobación.

Una vez finalizado el cambio en desarrollo, se realizan las *Pruebas de Regresión* que fueron especificadas en la actividad anterior, comprobando que ningún módulo o componente no modificado, pero con posibilidades de verse afectado, ha variado su comportamiento habitual. Las pruebas de regresión tratan de eliminar el llamado efecto onda, es decir, que los cambios

provocados por una petición no introduzcan un comportamiento no deseado o errores adicionales en otros componentes no modificados.

Finalmente, se informa si ha habido incidencias con el fin de que se resuelvan del modo más conveniente. En el caso de detectarse problemas, se elabora un informe que recoge las incidencias y se remite a quién proceda para que tome las medidas correctivas que considere oportunas. Una vez que el comportamiento es correcto, se documenta el resultado global de la evaluación de las pruebas que incluye la aprobación por parte del responsable de mantenimiento.

La aprobación final de los cambios se realiza al finalizar las pruebas de regresión, y después de comprobar que todo lo que ha sido modificado o puede verse afectado por el cambio, funciona correctamente.

Naturalmente los instrumentos previstos para documentar esta actividad *MME* son:

- *Documentación de los resultados de las pruebas de integración.*
- *Nota final de aprobación y cierre de la petición.*

Peticiones de Mantenimiento atendidas

Se informa brevemente las peticiones de mantenimiento que se han registrado y atendido a la fecha.

Mantenimientos Correctivos

Las peticiones de mantenimiento correctivas recibidas a la fecha no han revestido criticidad y se han circunscrito exclusivamente a la capa de interfase del sistema. En este sentido se realizaron correcciones sobre:

- La accesibilidad a los campos de formularios: se habilitaron accesos alternativos por selección de mouse y teclas de tabulación.
- Validación de ingreso de valores nulos en campos de formularios.
- Se mejoró y completó la ayuda en línea.

Mantenimiento Evolutivo

A partir de un análisis sobre el procedimiento de firma digital de documentos para el repositorio y de ciertas restricciones de hardware e idioma detectadas, el equipo de desarrollo del Proyecto de firma digital, detectó como necesidad crítica contar con una herramienta propia de firma digital sobre archivos PDF, en lugar de continuar utilizando pluggins para Acrobat. Disponer de un módulo propio de firma de archivos en formato PDF resultaría una evolución significativa para la aplicación, por cuanto podría integrarse el procedimiento de firma en el entorno propio del sistema que gestiona el repositorio, y de esta forma agilizar y mejorar sustantivamente el circuito.

Frente a esta necesidad se registró la petición y se emprendieron las tareas de análisis para encontrar una solución viable.

Luego de investigaciones y consultas preliminares se decidió encarar el desarrollo haciendo uso de dos librerías de desarrollo Java de uso libre y código abierto:

- ***BouncyCastle*** es una librería de clases para desarrollos PKI.
- ***iText*** es una librería de clases para la producción de archivos bajo la especificación PDF 1.3/1.4/1.5

Como documentación de base para la tarea se trabajó con los siguientes papers:

- Especificación estándar PDF 1.3/1.4/1.5 – Adobe System Incorporated. http://partners.adobe.com
- Digital Signatures Appearances (Versión Acrobat 6.0) – Adobe System Incorporated. http://partners.adobe.com

- PDF Public-Key Digital Signatures and Encryption Specification – Adobe System Incorporated. http://partners.adobe.com

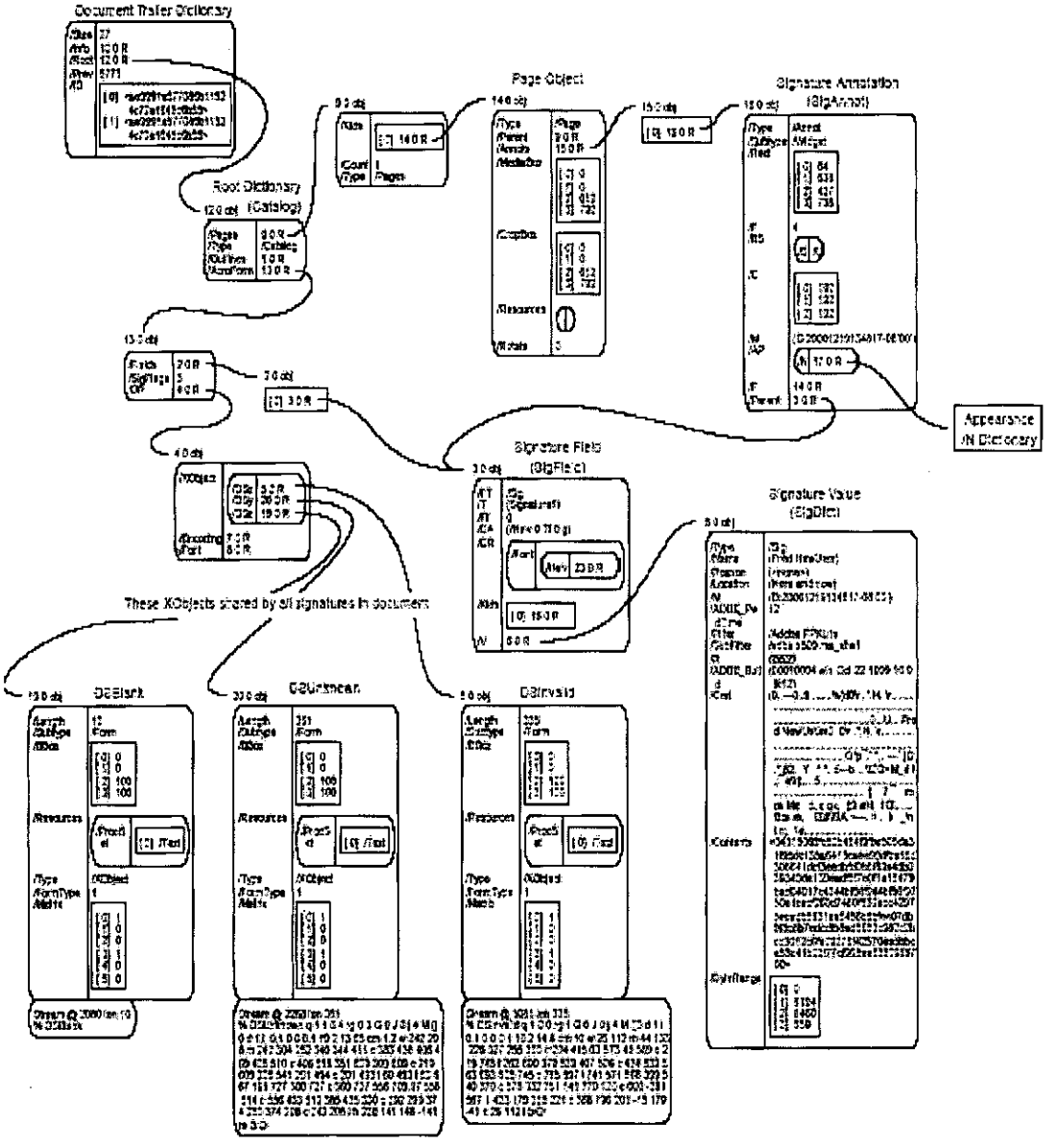
Si bien se definió un Plan de Acción para la tarea, no ha sido posible hacer una planificación ajustada de tiempos de ejecución, dado que el desarrollo es inédito y requiere de una importante cuota de investigación y pruebas.

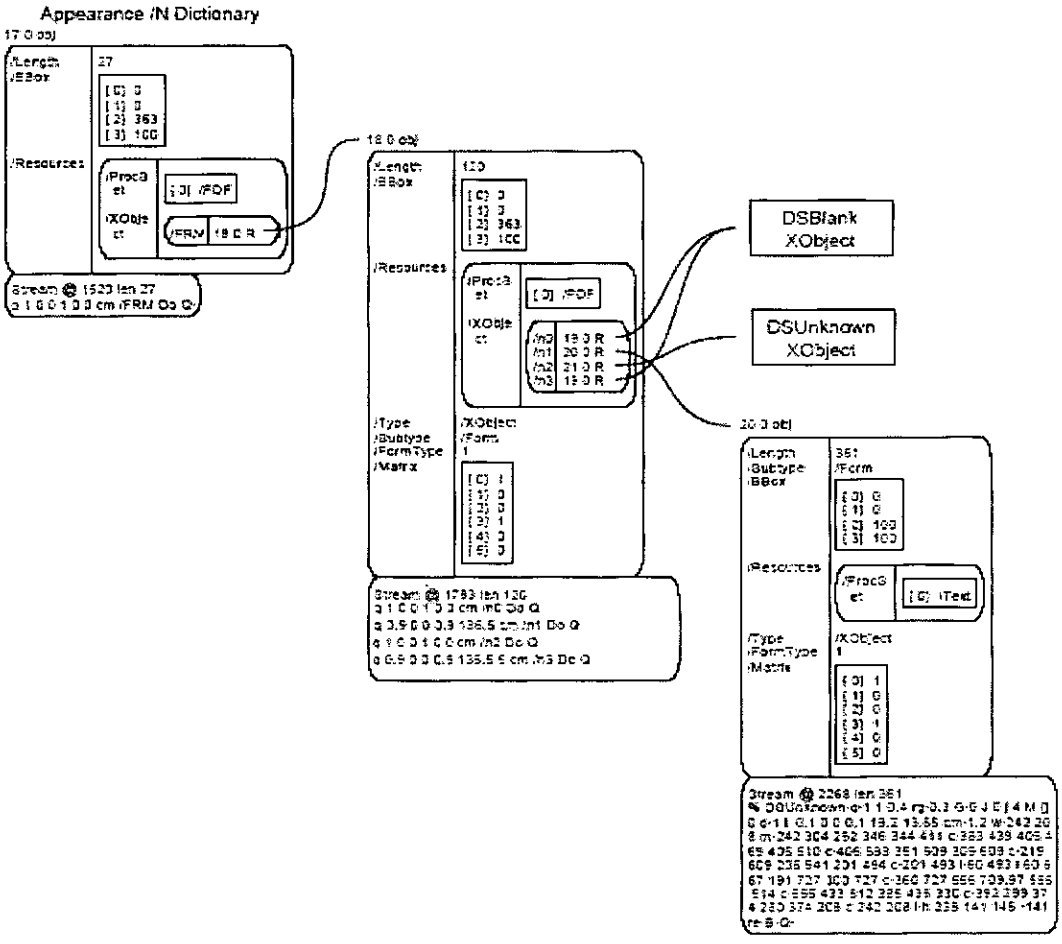
Las tareas realizadas involucraron los siguientes pasos:

- Estudio de archivos PDF firmados digitalmente para identificar el modelo de objetos subyacente, asociados a la firma.
- Análisis de formatos alternativos de representación de firma y certificados digitales en la especificación PDF. Raw y Pkcs#7
- Desarrollo e implementación del modelo.
- Pruebas y ajustes.

El principal desafío para el desarrollo, consistía en lograr una firma ajustada a la especificación PDF 1.5 y encapsulada junta a su cadena de certificación, en un objeto PKCS#7 de forma de garantizar que la misma pueda ser verificada por cualquier browser de archivos PDF, y alternativamente por otras herramientas específicas de validación de firma digital.

Sobre este requerimiento se han realizado importantes avances, contando a la fecha con un prototipo que genera el siguiente modelo de firma sobre un archivo PDF, el cual se ajusta a la especificación estándar PDF 1.4/1.5.

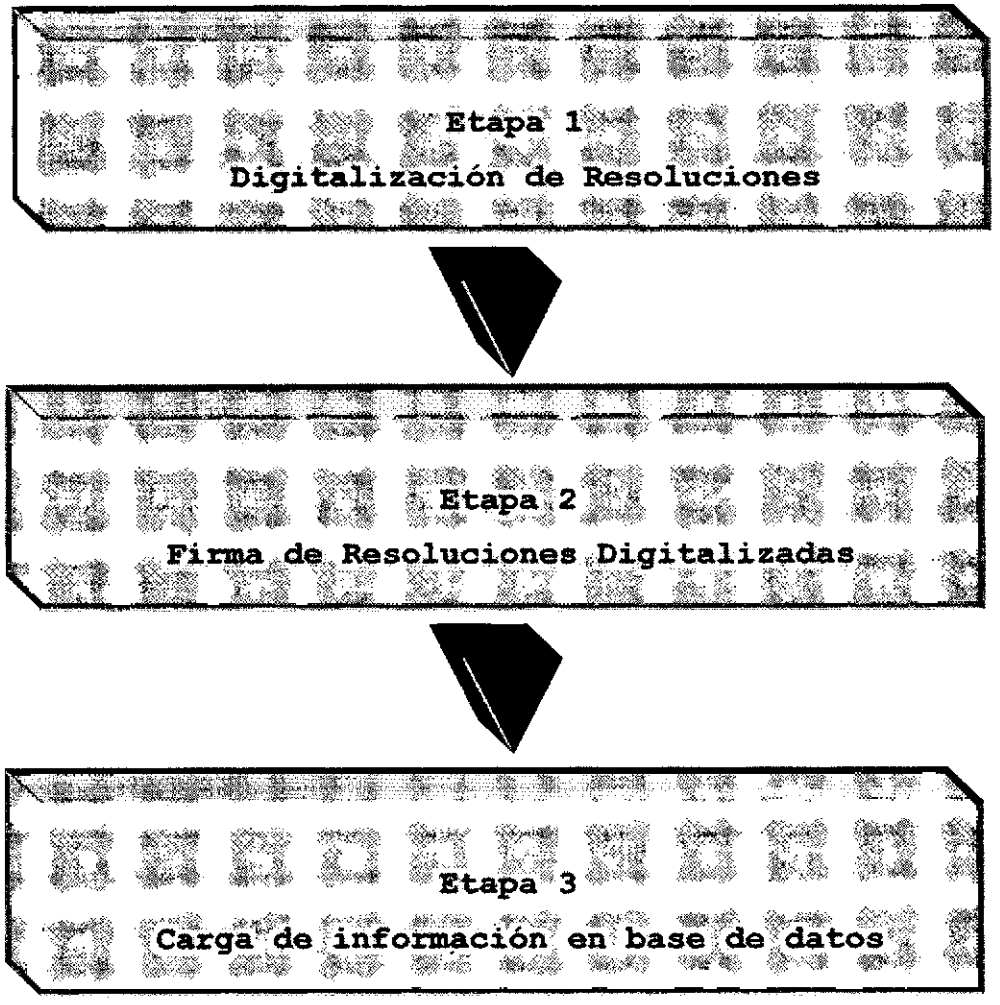

Document Trailer Dictionary
Root Dictionary (Catalog)
Page Object
Signature Annotation (SigAnnot)
Appearance /N Dictionary
Signature Field (SigField)
Signature Value (SigDict)
These XObjects shared by all signatures in document
DctBlank
DctUnknown
DctInvalid



Resta cumplimentar algunos aspectos de compatibilidad con lectores PDF, para poder iniciar la fase de integración del módulo al sistema y emprender de este modo las pruebas de regresión.

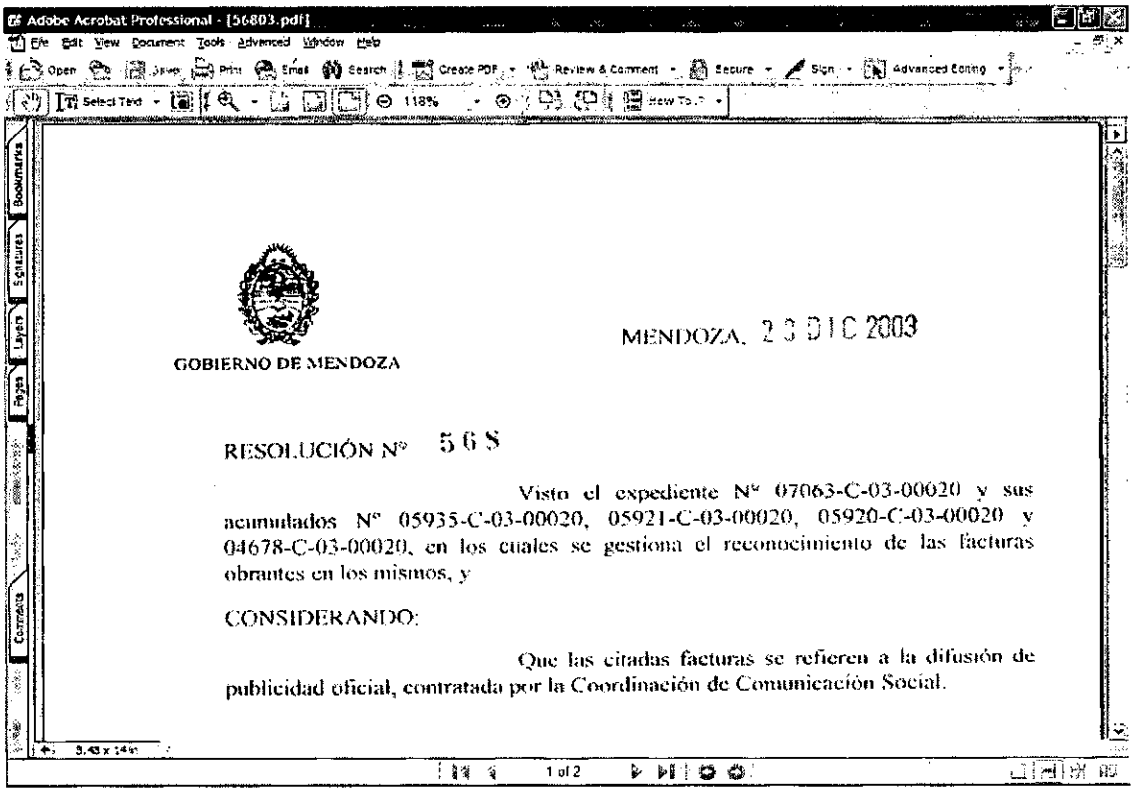
D. Carga de datos históricos:

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.


Adobe Acrobat Professional - [56803.pdf]

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.

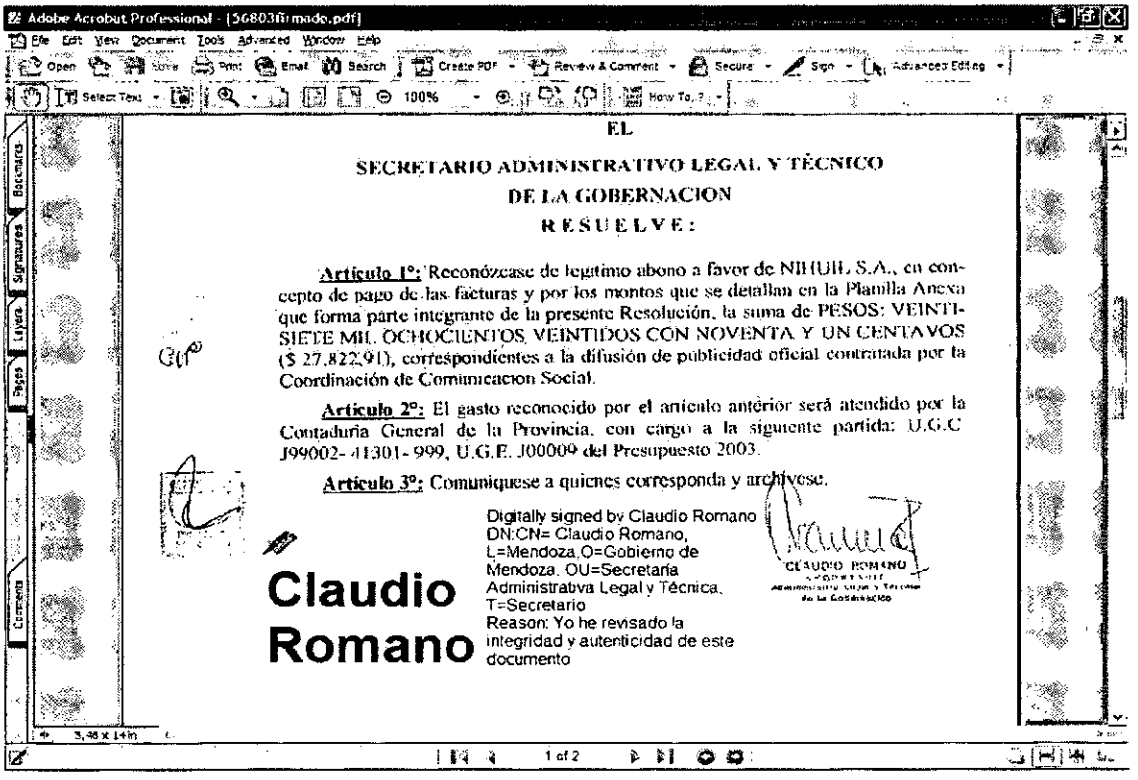
1 of 2

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

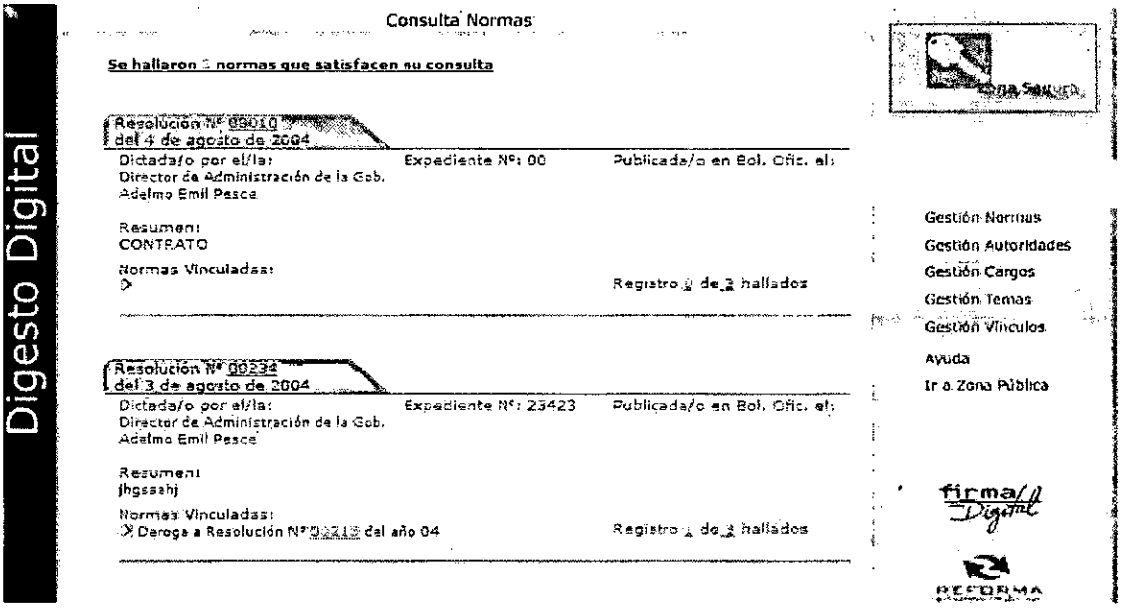
La segunda etapa del proceso incorpora a los documentos digitalizados la propia firma digital de los funcionarios responsables. Esto es, una vez digitalizadas las resoluciones impresas en papel, el archivo digital generado pasa a la firma digital del Director de Administración el Sr. Adelmo Pesce y luego 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.



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. *Anexo - Manual de Usuario Digesto Digital*

Digesto Digital

Secretaría Administrativa Legal y Técnica

MANUAL DEL USUARIO

firma Digital

REFORMA
& MODERNIZACION DEL ESTADO

Gobierno de Mendoza

CFI

El repositorio digital de normas legales con garantía de firma digital, que en adelante llamaremos ***Sistema*** o ***Digesto Digital,*** permite administrar la información referente a resoluciones, normas o decretos producidos en el ámbito de la Administración Pública del Gobierno de Mendoza. Por administración de información se entiende que el sistema informático permite: realizar consultas a una base de datos o índice de normas llegando incluso al documento completo de la norma y sus normas vinculadas, obtener información de resumen y gestionar la correcta registración y actualización de documentos, con el valor agregado de que los mismos tengan la garantía de la firma digital de los funcionarios responsables de su aprobación.

Veremos a continuación en que consisten y cómo desarrollar correctamente cada una de las funciones que el sistema provee. Para ello abordaremos, en los siguientes capítulos, un recorrido por las distintas alternativas de operación y opciones que presenta el sistema.

Cabe señalar, que en el contexto del digesto digital, la idea de repositorio excede el alcance de su denominación, y se acerca a la definición de una biblioteca digital de normas legales. Es decir un *"conjunto de recursos de información en formato digital, insertos en un contexto organizacional que procura la selección, evaluación, registro y sistematización para su disponibilidad y que permite – mediante Tecnologías de información, el acceso local o a distancia por parte de una comunidad de usuarios locales o remotos".*

En este sentido, el sistema presenta las siguientes ventajas cualitativas:

Del Repositorio Digital

- mayor acceso y disponibilidad de la información sin dependencia de barreras temporales, geográficas y espaciales.
- ahorro en costos de papelería y de transferencia

- posibilidades de búsqueda por criterios
- información actualizada
- información centralizada
- información segura y perdurable en el tiempo
- posibilidades de relacionar la información entre sí
- despapelización del Estado
- agilización de los procesos de consulta
- mejoras en la calidad de la información
- liberación de espacios físicos de archivo de papel
- liberación de tiempos en tareas manuales

Del Repositorio Digital con Firma Digital

Esta mejora implica que los textos de las resoluciones no serán firmados en forma hológrafa y luego digitalizados, sino que los mismos responsables de la promulgación suplantarán su firma manuscrita por una Firma Digital en los textos resolutivos que irán directamente al repositorio digital. Con lo cual los textos resolutivos digitalizados tendrán un genuino **valor legal.**

En este sentido Firma Digital proveerá a la información incluida en el repositorio digital de las siguientes garantías:

- ***Integridad:*** los textos de las resoluciones firmados digitalmente por los responsables estarán completos y sin posibilidad de error, ya que la tecnología garantiza la verificación de la integridad de la resolución mediante la aplicación de una función de hash. Cualquier diferencia, pérdida de datos, o modificación de los datos originales será alertada por el sistema.

- ***Autenticidad y autoría:*** se puede contar con la absoluta seguridad sobre el valor de verdad del texto resolutivo ya que, a diferencia de un repositorio común, el texto resolutivo se encontrará firmado digitalmente

por los responsables de su promulgación. Esto es posible gracias a que la verificación de la firma se encuentra disponible para aquellas personas que ingresen a consultar el repositorio, a través de la clave pública del propio firmante.

- ***No repudio:*** debido a las garantías anteriores, la información es digitalmente firmada posee valor legal en el repositorio. Es decir, no se tiene sólo una imagen de una norma en Internet, sino que lo que se tiene es la propia norma digitalizada y firmada digitalmente por los responsables de su promulgación, con lo cual su responsabilidad por lo que firmaron y se encuentra en el repositorio es plena.

De esta forma, los textos resolutivos contenidos en la base de datos, se resguardan mediante métodos de criptografía asimétrica que aseguran la integridad y autoría de las resoluciones y la identidad de las personas que las promulgaron.

2. USUARIOS DEL SISTEMA

El sistema distingue cuatro perfiles de usuario o roles claramente diferenciados:

- ***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. Los 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.

🔔 **Importante:** Este manual está dirigido especialmente a *usuarios-administradores* del sistema, incluyendo aquellos aspectos que interesan a los usuarios-comunes por cuanto los usuarios-administradores deben conocer y probar el uso que los usuarios finales harán del repositorio.

3. ZONA PÚBLICA Y ZONA SEGURA

Los usuarios del repositorio de normas legales deben diferenciar claramente dos espacios de trabajo dentro del sistema, la ***Zona Pública*** y la ***Zona Segura***.

La ***Zona Pública*** como su nombre lo indica, es un espacio abierto a cualquier usuario que tenga acceso a la Intranet Central del Gobierno de Mendoza. Desde allí los usuarios finales podrán consultar las resoluciones, decretos o leyes publicadas en el digesto bajo distintos criterios de búsqueda y organización de la información.

La ***Zona Segura*** es el espacio reservado a los usuarios-administradores para que desde allí puedan cumplir su tarea de carga y actualización de información al sistema. Es segura, por cuanto está protegida con tecnologías de firma digital y certificados digitales garantizando que ninguna persona pueda acceder y manipular los datos del sistema sin estar debidamente identificado y autorizado.

A continuación se explican detalladamente las funciones que el sistema provee en cada una de estas zonas y cómo deben ser utilizadas.

4. ZONA PÚBLICA – CONSULTAS AL REPOSITORIO

La ***Zona Pública*** permite a los *usuarios finales* realizar consultas de normas legales en el digesto según distintos criterios de búsqueda.

El módulo de Consulta consta de dos componentes: consulta básica y consultas avanzadas.

4.1. Consultas Básicas: Este componente permite a los usuarios consultar normas en el repositorio por los siguientes criterios:

a. Número de la norma.
b. Número de expediente vinculado a la norma.
c. Fecha de emisión.
d. Fecha de publicación en el Boletín Oficial.
e. Organización temática.
f. Autoridad que la firma.

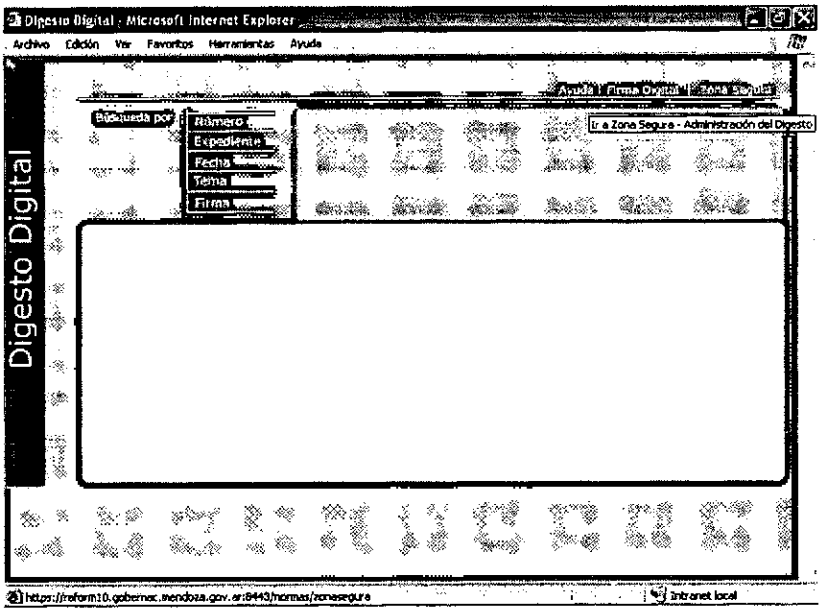


fig. 1 – Criterios de consulta en la zona pública

Ante cualquier consulta realizada se devuelven los datos descriptivos de la o las normas que satisfacen el criterio de búsqueda especificado y se da acceso a los documentos digitales vinculados, tal como lo muestran las siguientes figuras:

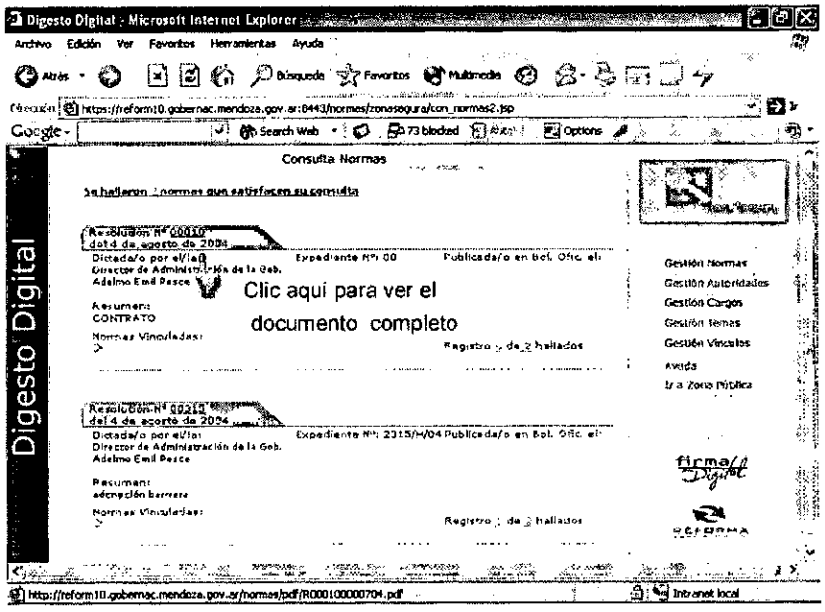


fig.2. Consulta de Resoluciones firmadas por Adelmo Pesce – Fichas de información

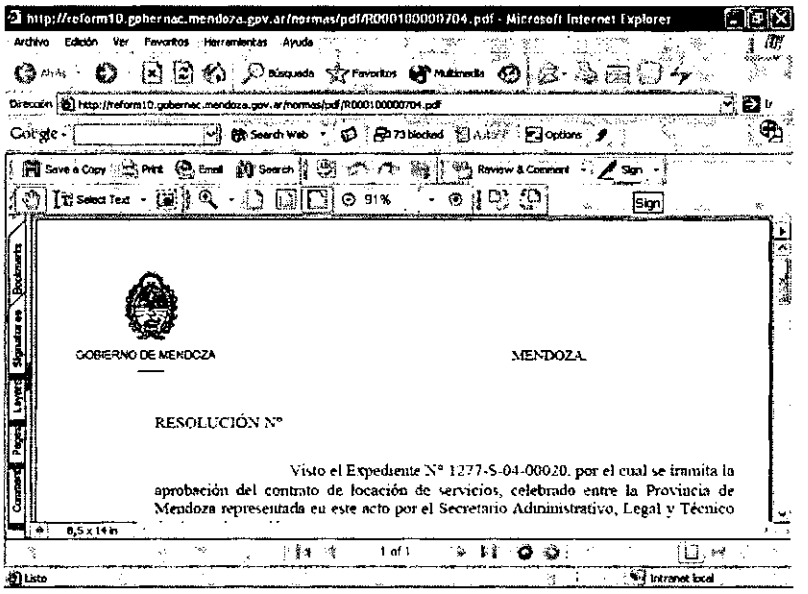


fig. 3. Texto completo de la norma consultada.

Este módulo es de acceso público a cualquier usuario de la Intranet de Gobierno y su uso es totalmente intuitivo.

4.2. Consultas Avanzadas: Este componente permite refinar búsquedas y consultas de documentos ***combinando*** según las necesidades del usuario los siguientes criterios:

a. Número de la norma.
b. Fecha de emisión.
c. Fecha de publicación en el Boletín Oficial.
d. Autoridad que la firma.
e. Cargo o función que la emite.
f. Tema asociado.
g. Descriptores o palabras incluidas en el abstract de la norma.
h. Normas comprendidas en un período determinado.
i. Normas relacionadas a una norma en particular.

De esta manera se pueden imponer filtros compuestos en las consultas a la Base de Datos para ampliar o restringir el conjunto de resultados. Este módulo es de acceso público a cualquier usuario de la Intranet de Gobierno.

5.1. Acceso a la Zona Segura

La Zona Segura, está protegida por tecnología de sitio seguro y sólo tienen acceso a ella los usuarios debidamente identificados y autorizados mediante un Certificado Digital.

A continuación se describen los pasos a seguir en el digesto para acceder a la Zona Segura.

Paso 1: Al hacer clic en el vínculo de acceso a la Zona Segura, el sistema le indicará que está a punto de acceder a un sitio mediante conexión segura SSL y le dará la opción de Aceptar u obtener mayor información. El usuario debe aceptar para continuar con el proceso.

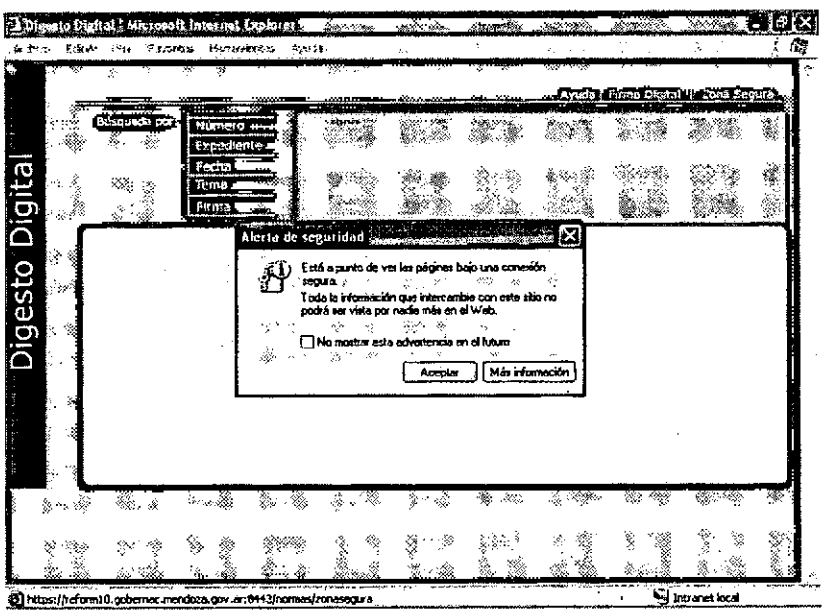


fig. 4. Confirmación de Acceso al Sitio Seguro

Paso 2: El sistema le solicitará que indique el Certificado Digital que va a presentar para autenticarse ante el sitio. En caso de que el usuario, no esté

autorizado para acceder al sitio o que no posea un certificado válido, el sistema devolverá una página de error.

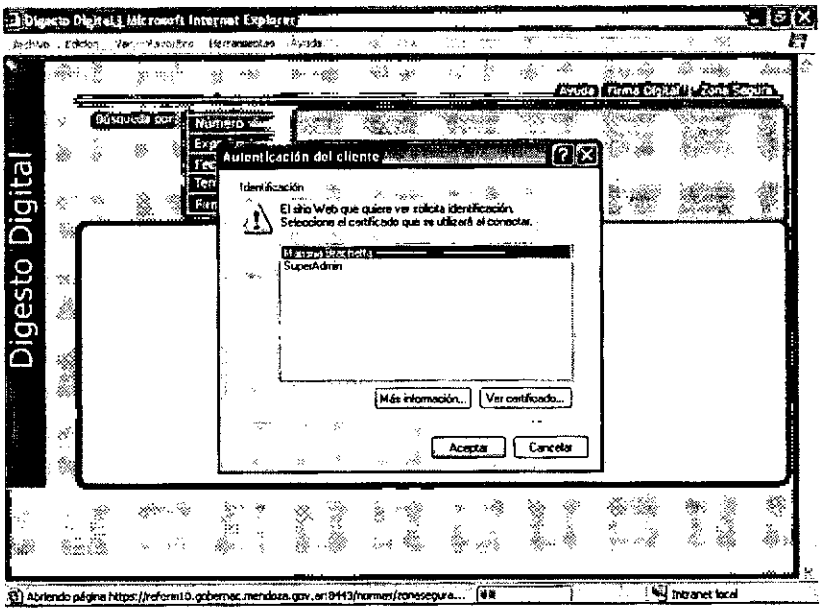


fig. 5. Selección del Certificado Digital

Paso 3: Una vez seleccionado el Certificado a presentar, el sistema le pedirá al usuario que ingrese su clave. Esta clave protege al Certificado de usos indebidos. La clave es fijada por el usuario al momento de instalación de su Certificado y es conocida única y exclusivamente por él.

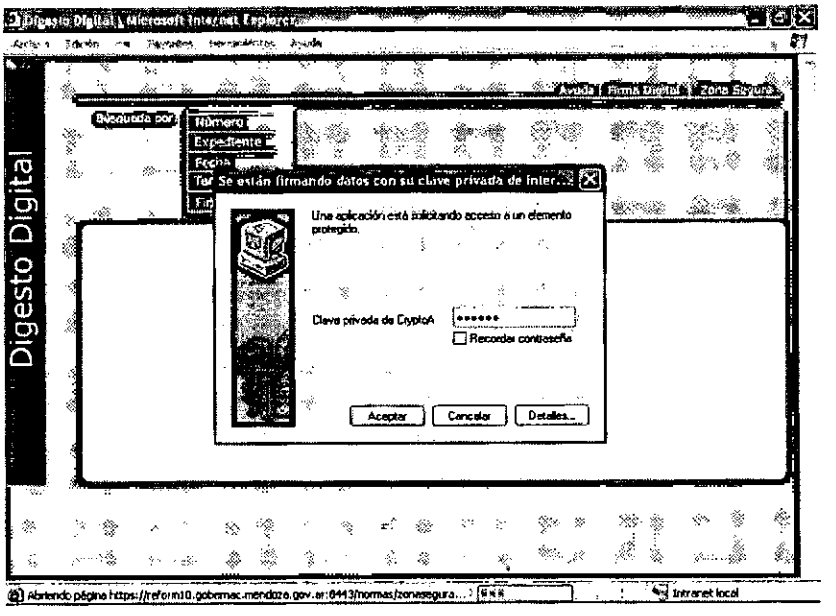


fig. 6. Acceso al Certificado

El usuario podrá opcionalmente ver la información detallada del Certificado Digital presentado.

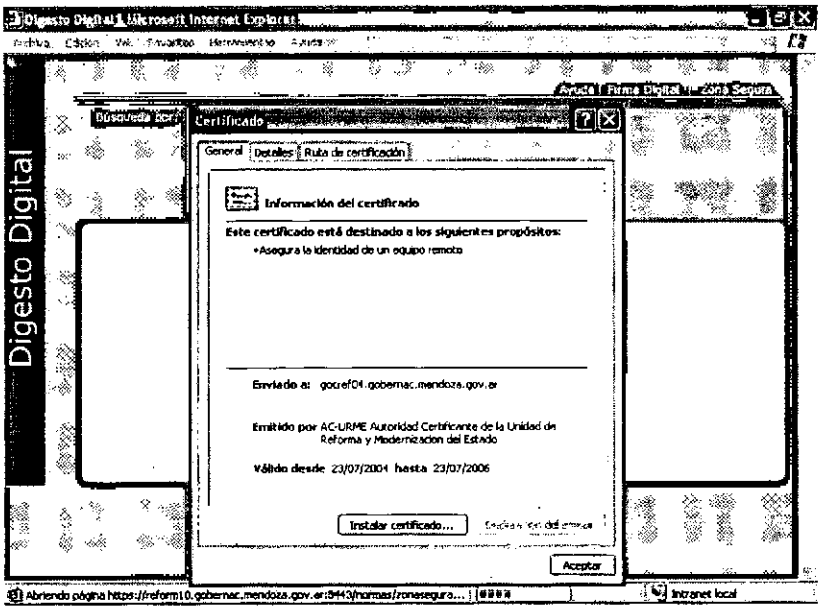


fig. 7. Información del Certificado Presentado

Si la clave que ingresa el usuario es válida, el sistema aceptará el certificado presentado y dará acceso a la Zona Segura.

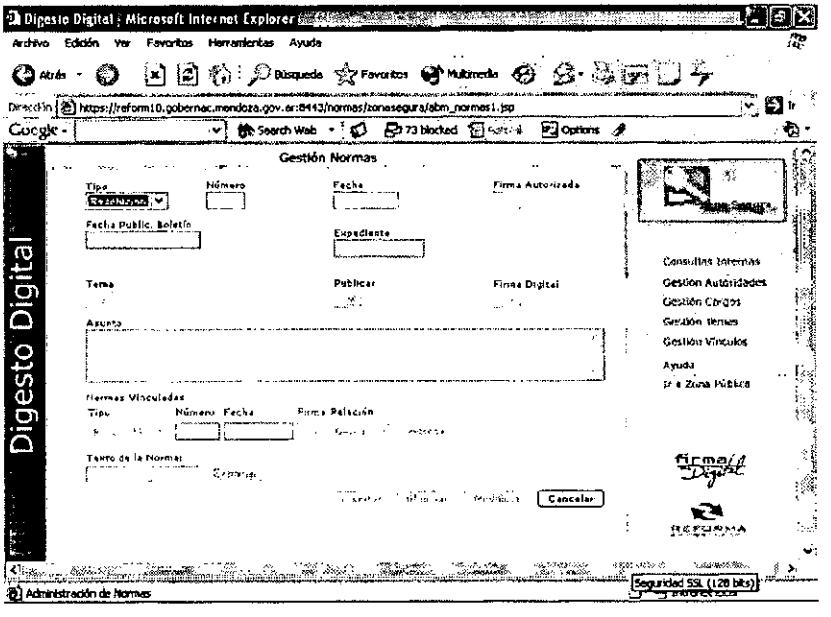


fig. 8. Pantalla principal de la Zona Segura

5.2. Módulo: Consultas Internas

El módulo de Consultas Internas, es la herramienta mediante la cual los *usuario-administradores* pueden consultar la información que han cargado al digesto.

Desde aquí, se podrán hacer consultas avanzadas al Digesto combinando distintos criterios de selección de información, tales como períodos de fecha, organización temática, autoridades firmantes y otros.

En principio, las capacidades y formas de uso de esta herramienta respeta la misma lógica y diseño que las Consultas Avanzadas en la Zona Pública; pero permite el acceso a todo el banco de datos y no sólo al conjunto de normas publicadas en la Zona Pública.

A continuación se describen los pasos que a modo de ejemplo deberían seguirse para concretar una consulta.

Paso 1: El usuario debe introducir los parámetros combinados de consulta en el formulario dispuesto a tal fin. En el siguiente ejemplo se combinan criterios de tipo de norma, número y firma autorizada.

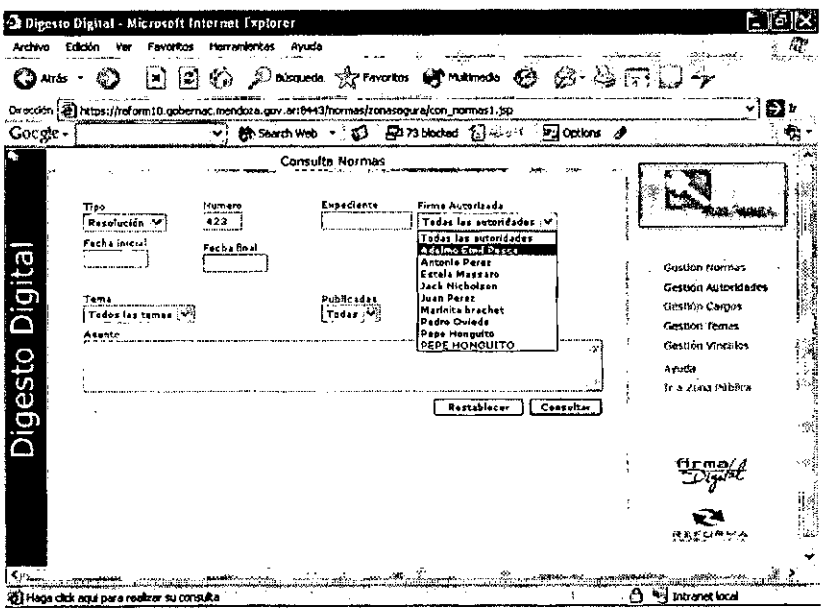


fig. 9. Formulario de Consulta

En caso de que no se encuentren datos que satisfagan los criterios de consulta establecidos, el sistema informará tal situación con el siguiente mensaje de error.

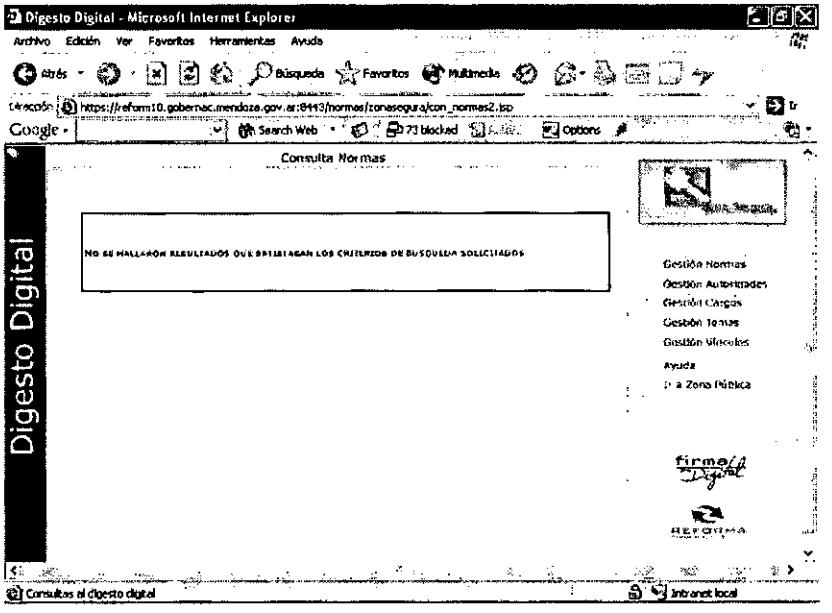


fig. 10. Mensaje de error - consulta fallida

En caso de que se encuentren datos en el repositorio que satisfagan las condiciones solicitadas, el sistema presentará al usuario las fichas de información con los resultados hallados. Una ficha por cada norma encontrada.

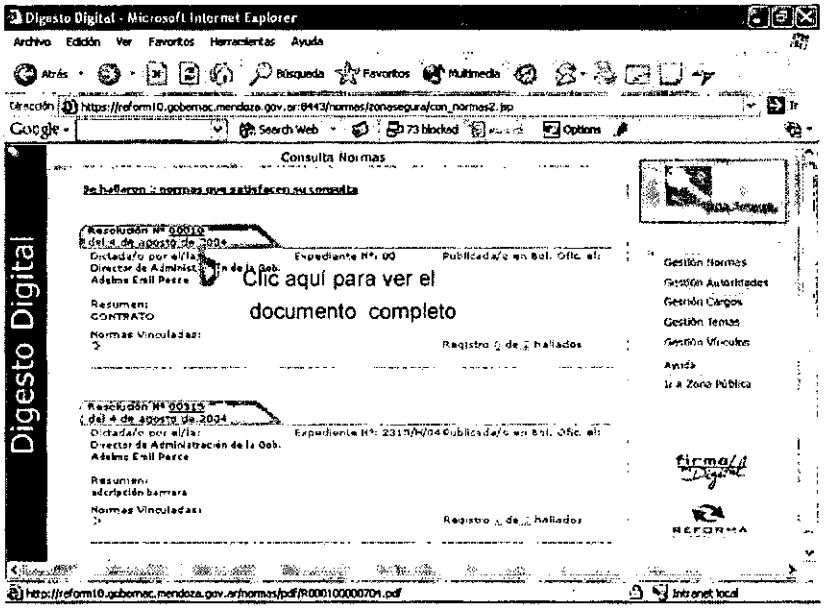


fig. 11. Resultados de la Consulta

Paso 2: Para consultar el documento completo de una norma, el usuario deberá hacer clic sobre el número de norma, en la solapa de la ficha de su interés.

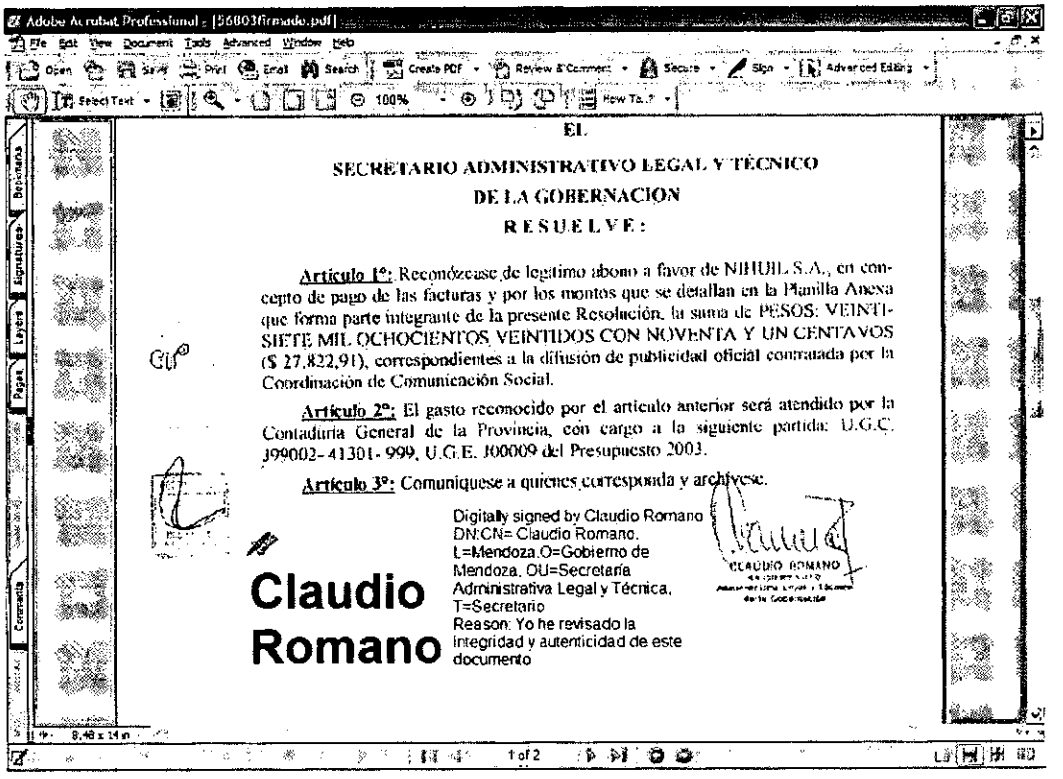


fig. 12. Documento PDF de la Norma, firmado digitalmente

Importante: El documento de la norma se presenta en formato PDF (Formato de Documento Portable de Adobe). Por lo tanto el usuario deberá contar con un lector de documentos PDF, tal como Acrobat Reader para poder ver el archivo. Esta herramienta es gratuita y puede ser descargada e instalada desde el sitio de firma digital http://www.firmadigital.mendoza.gov.ar La verificación de la firma digital, se hace también desde esta herramienta de uso masivo.

5.3. Módulo: Gestión de Datos

Las altas, bajas y modificaciones sobre datos almacenados en el repositorio se realizan a través de ***5 componentes*** interrelacionados que el *usuario-administrador* deberá conocer y manejar.

A continuación veremos los detalles de operación de estos cinco componentes:

5.3.1. Gestión Autoridades

Cada norma almacenada en el repositorio debe estar firmada por una Autoridad Responsable cuyos datos y certificados digitales deben ser correctamente mantenidos y actualizados. Este componente Web implementa las altas, bajas y modificaciones a la tabla que mantiene y controla toda la información vinculada a autoridades.

Para agregar una nueva autoridad

Paso 1: Indique el cargo del funcionario y a continuación seleccione la opción *Nueva Autoridad*. El sistema habilitará automáticamente los campos a ser completados y la opción de *Insertar*.

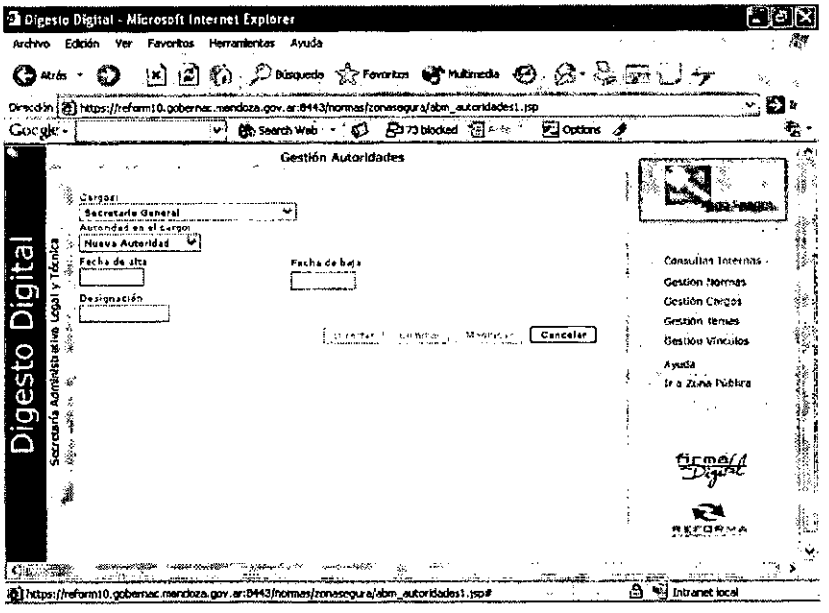


fig. 13. Agregando una nueva autoridad al Digesto

Paso 2: Ingrese Apellido y Nombre de la nueva autoridad, su fecha de designación en el cargo y la fecha de baja prevista. En el campo *Designación*

deberá ingresar el número de resolución o norma mediante la cual se designa al funcionario en el cargo.

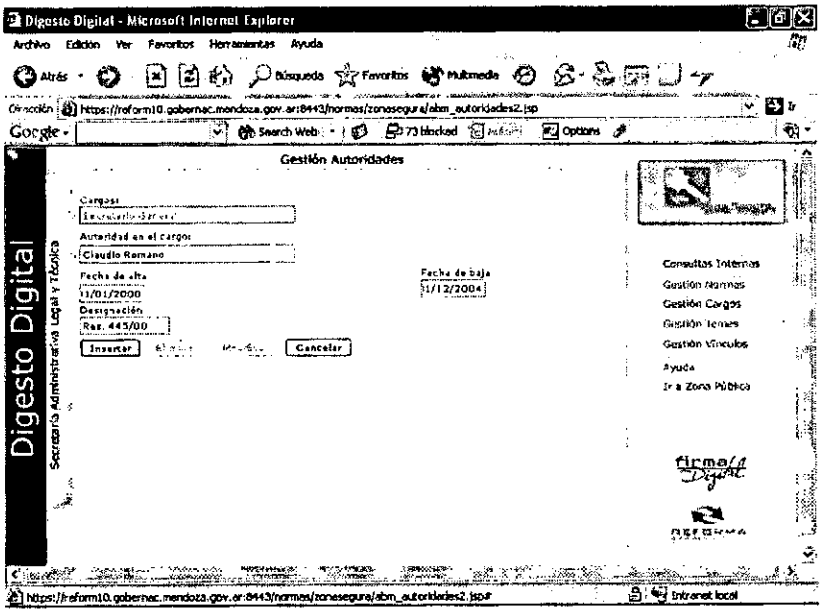
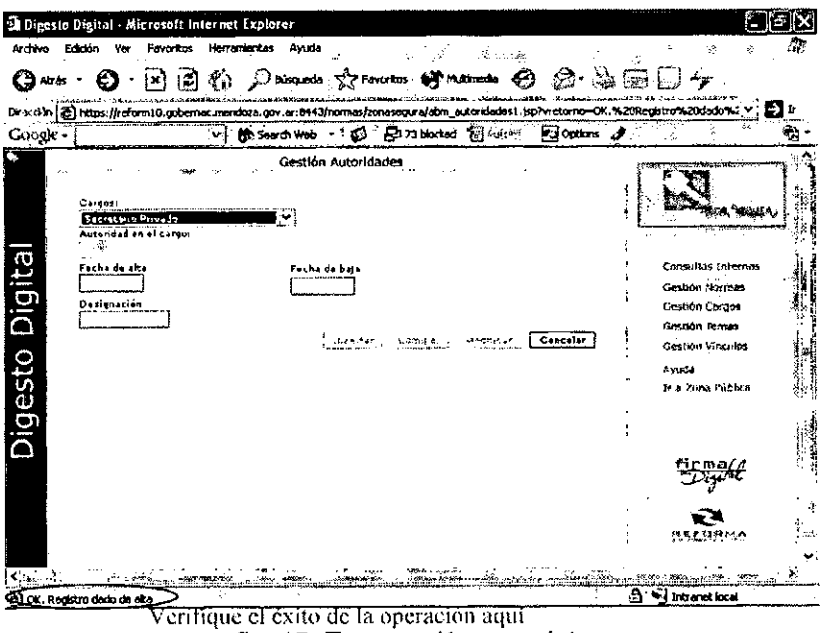


fig. 14. Completando los datos de la Autoridad

Paso 3: Verifique que el alta se halla concretado satisfactoriamente, chequeando la respuesta del sistema en la barra de estado.



Verifique el éxito de la operación aquí

fig. 15. Transacción completa

Importante: En caso de error el sistema informará que no pudo concretar la operación y las causas de la falla para que el usuario pueda corregirlo. Al final del documento, se presentan los casos típicos de error en la operación del sistema.

Para modificar los datos o eliminar una autoridad existente

Paso 1: Indique el cargo del funcionario y el nombre de la autoridad cuyos datos desea modificar o dar de baja. Hecho esto, el sistema habilitará los campos para que sean modificados y las opciones *Eliminar* o *Modificar* según sea el caso.

Paso 2: Modifique los datos deseados y haga clic en *Modificar* para concretar las actualizaciones o haga clic en *Eliminar* para dar de baja a la Autoridad.

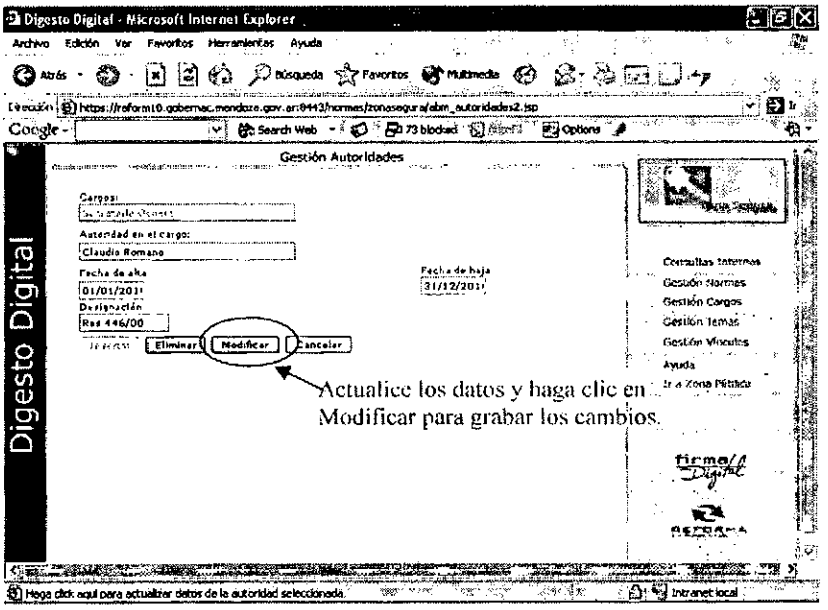


fig. 16. Modificación de datos de Autoridad

En caso de que elija *Eliminar*, el sistema le pedirá que confirme para asegurar que no cometa un error. El sistema validará que no se elimine una Autoridad que ha firmado normas cargadas al Digesto.

Paso 3: Verifique que la transacción se halla concretado satisfactoriamente, chequeando la respuesta del sistema en la barra de estado.

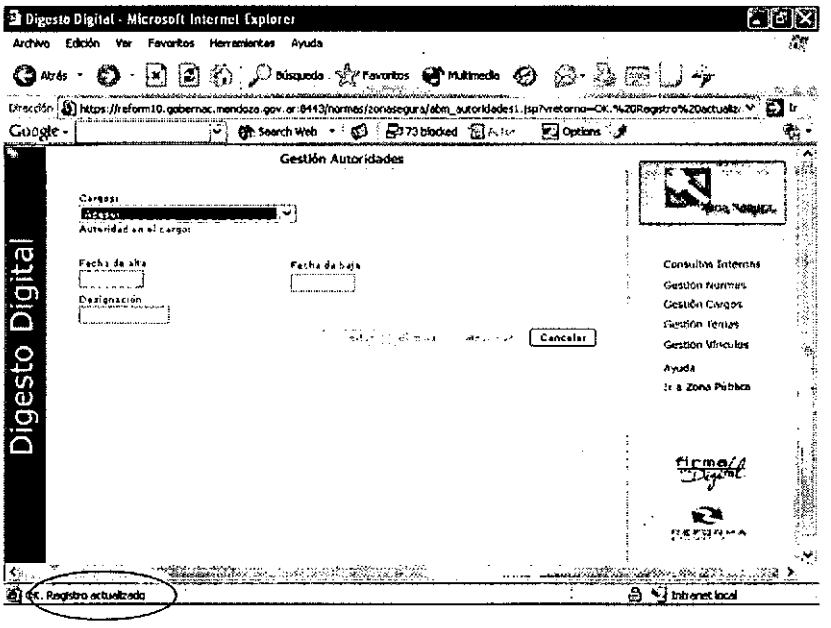


fig. 17. Confirmación de actualización

5.3.2. Gestión Cargos

Cada persona que firma una norma está asociada a un cargo o función en un período determinado. Este componente implementa la administración de la información vinculada a la estructura organizacional y la asignación de personas en cargos.

Para agregar un nuevo cargo

Paso 1: Seleccione la opción *Nuevo Cargo*. El sistema habilitará automáticamente los campos a ser completados y la opción de *Insertar*.

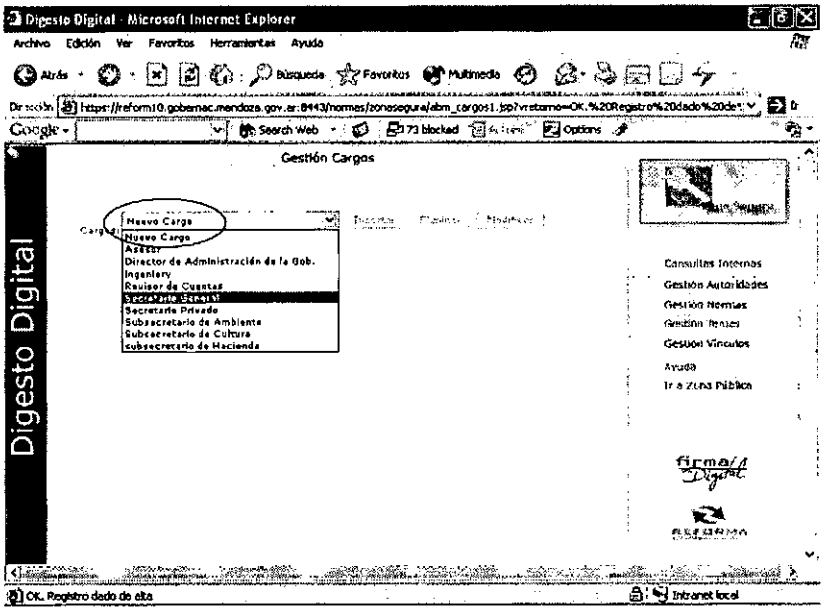


fig. 18. Agregando un nuevo cargo

Paso 2: Ingrese el título del nuevo cargo según como está establecido en la estructura organizacional y haga clic en *Insertar.*

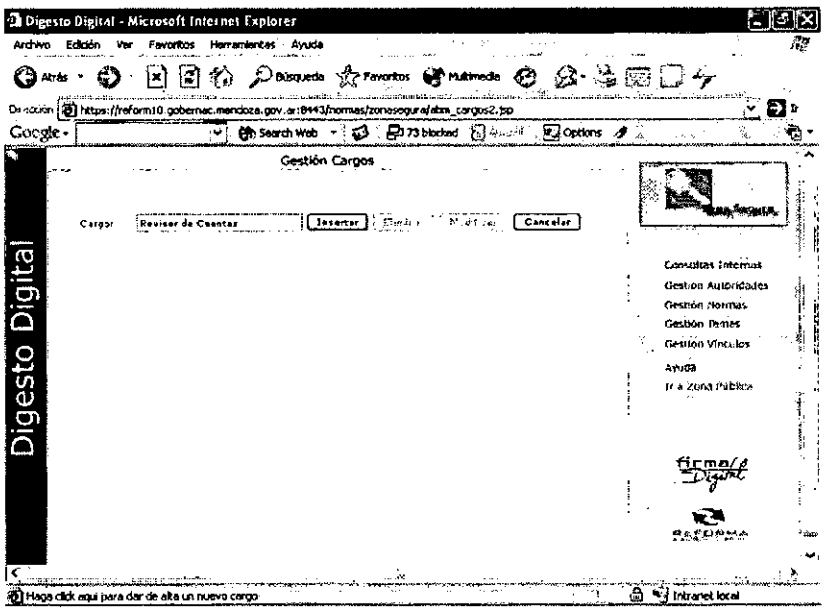


fig. 19. Insertar el cargo

Paso 3: Verifique que el alta se halla concretado satisfactoriamente, chequeando la respuesta del sistema en la barra de estado.

Para modificar los datos o eliminar un cargo existente

Paso 1: Seleccione en la lista de opciones el cargo cuyos datos desea modificar o eliminar. Hecho esto, el sistema habilitará el campo de título del cargo seleccionado para que sea modificado y las opciones *Eliminar* o *Modificar.*

Paso 2: Modifique el título de cargo y haga clic en *Modificar* para concretar la actualización o haga clic en *Eliminar* para dar de baja el cargo.

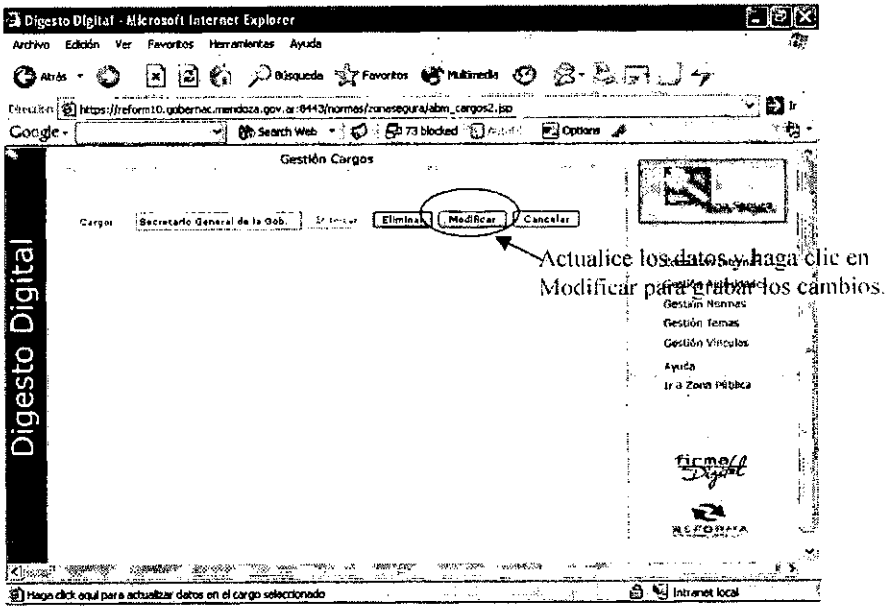


fig. 20. Modificación de cargos

En caso de que elija *Eliminar*, el sistema le pedirá que confirme si está seguro que desea eliminar el cargo seleccionado.

Importante: El sistema validará que no se elimine un cargo asociado a autoridades que han firmado normas cargadas al Digesto.

Paso 3: Verifique que la transacción se halla concretado satisfactoriamente, chequeando la respuesta del sistema en la barra de estado.

5.3.3. Gestión Temas

Como criterio organizador cada norma se asocia a un tema en particular. El componente de altas, bajas y modificaciones de temas permite gestionar la tabla de temas de modo que el repositorio pueda configurarse de acuerdo a necesidades puntuales de clasificación de información en cada implementación.

Para agregar un nuevo tema

Paso 1: Seleccione la opción *Nuevo Tema*. El sistema habilitará automáticamente los campos a ser completados y la opción de *Insertar*.

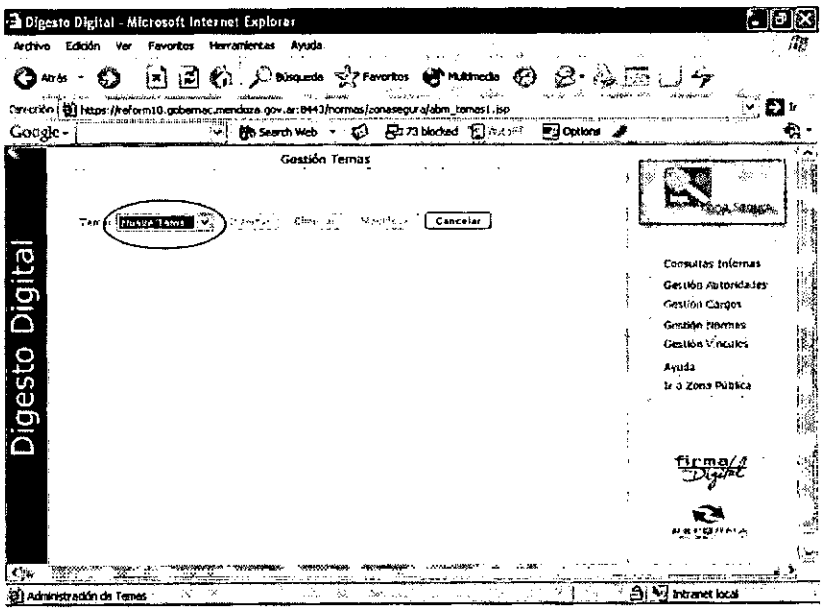


fig. 21. Agregando un nuevo tema

Paso 2: Ingrese el título del nuevo tema de acuerdo a los criterios de organización de la información establecidos y haga clic en *Insertar*.

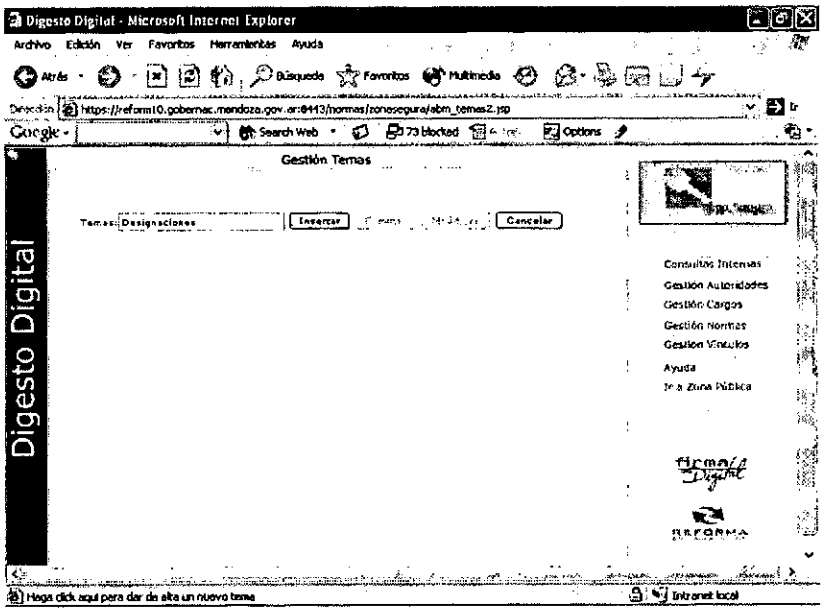


fig. 22. Ingresando el nombre del tema

Paso 3: Verifique que el alta se halla concretado satisfactoriamente, chequeando la respuesta del sistema en la barra de estado.

Para modificar los datos o eliminar un tema existente

Paso 1: Seleccione en la lista de opciones el tema cuyo nombre desea modificar o eliminar. Hecho esto, el sistema habilitará el campo tema para que pueda editarlo y las opciones *Eliminar* o *Modificar.*

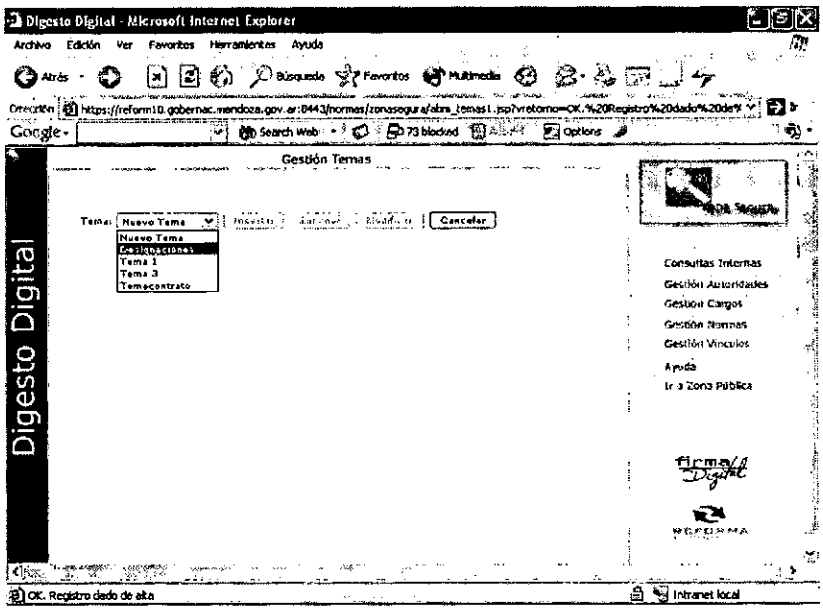


fig. 22. Seleccionando un tema existente

Paso 2: Modifique la descripción del tema y haga clic en *Modificar* para concretar la actualización o haga clic en *Eliminar* para dar de baja al tema seleccionado.

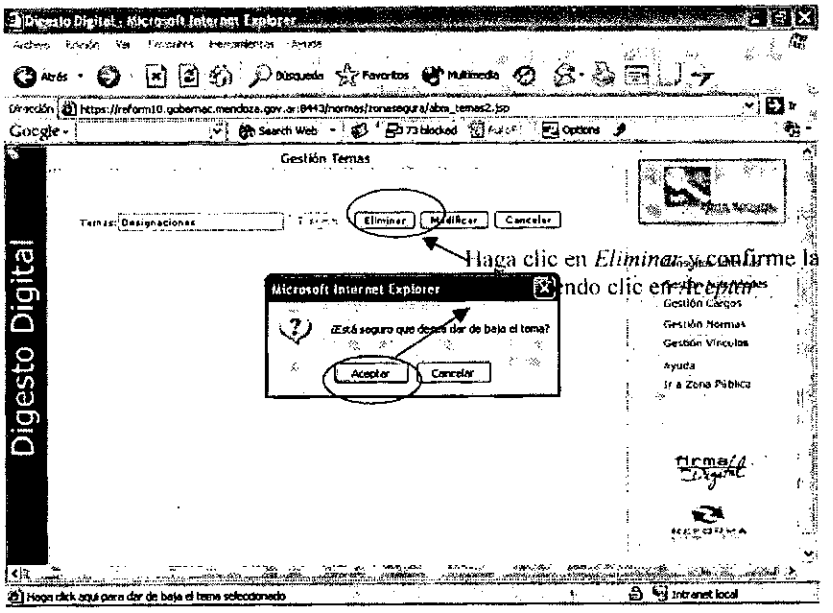


fig. 23. Eliminando un tema

Importante: El sistema validará que no se elimine un tema asociado a normas legales cargadas en el Digesto.

Paso 3: Verifique que la transacción se halla concretado satisfactoriamente, chequeando la respuesta del sistema en la barra de estado.

5.3.4. Gestión Vínculos

Una norma reciente puede relacionarse con otras a través de algún tipo de actualización que la misma impone sobre sus antecedentes. En general los tipos de relación de actualización son: *"modifica"*, *"deroga"*, *"ratifica"* u otras.

Con el objeto de parametrizar los tipos de relación entre normas de modo de garantizar la construcción de un mapa de relación que permita seguir todo el historial de un documento, se mantiene en el sistema una tabla de tipos de vínculos entre normas. Este componente implementa la administración de esta tabla y sus vinculaciones con la tabla de relación entre normas cuyo tratamiento se aborda más adelante.

Para agregar un nuevo tipo de vínculo entre normas

Paso 1: Seleccione la opción *Nueva Relación*. El sistema habilitará automáticamente los campos a ser completados y la opción de *Insertar.*

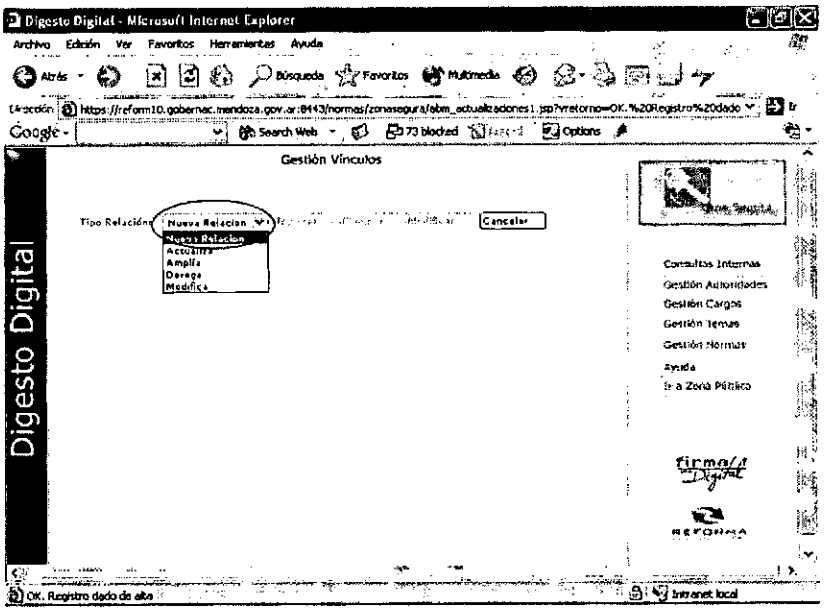


fig. 24. Agregando un nuevo tipo de relación

Paso 2: Tipee la descripción del nuevo vínculo o relación, y haga clic en *Insertar.*

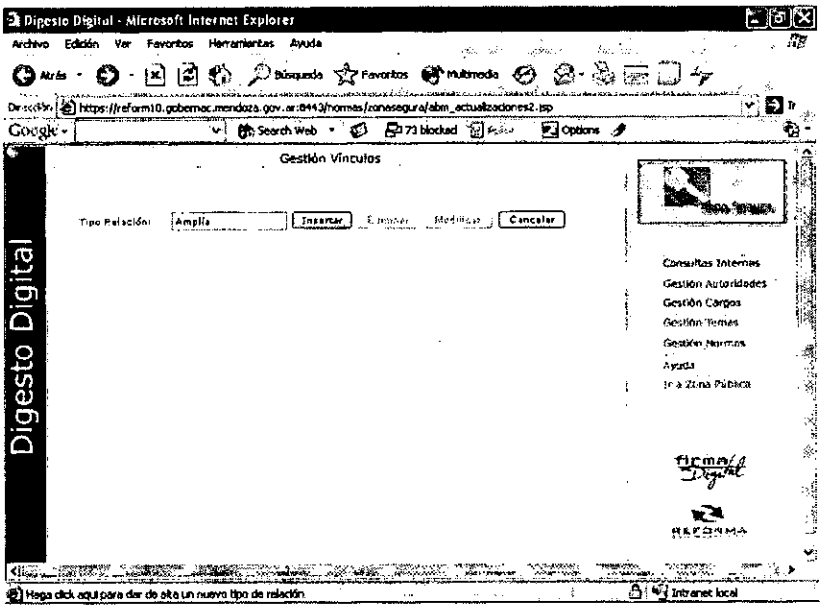


fig. 25. Ingresando el nombre de la relación

Paso 3: Verifique que el alta se halla concretado satisfactoriamente, chequeando la respuesta del sistema en la barra de estado.

🔔 **Importante:** Recuerde que en todo momento, usted dispone de la ayuda en línea; y que el sistema utiliza la barra de estado del navegador para proporcionarle ayudas y guías.

Para modificar los datos o eliminar un tipo de relación o vínculo existente

Paso 1: Seleccione en la lista de opciones el tipo de vínculo cuyo nombre desea modificar o eliminar. Hecho esto, el sistema habilitará el campo *Tipo Relación* para que pueda editarlo y las opciones *Eliminar* o *Modificar.*

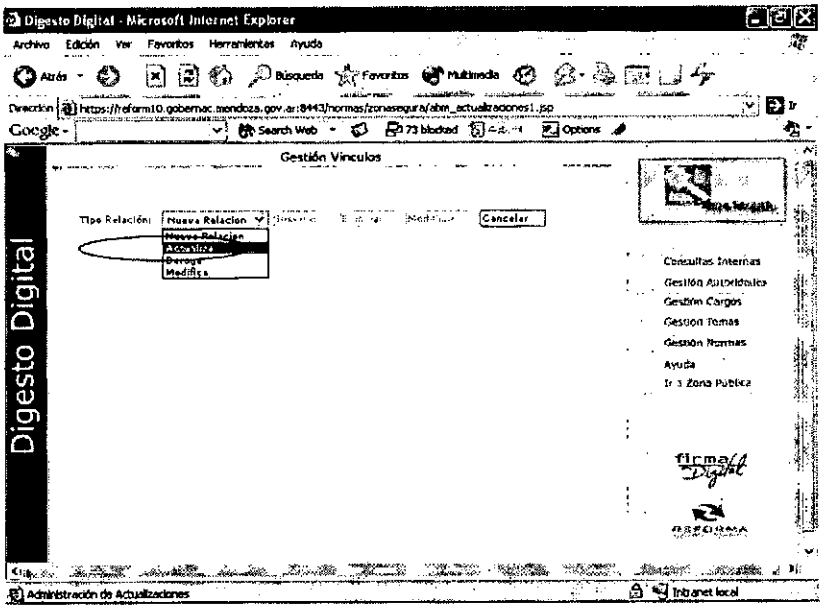


fig. 26. Seleccionando una relación existente

Paso 2: Modifique la descripción del tipo de relación y haga clic en *Modificar* para concretar la actualización o haga clic en *Eliminar* para eliminar el vínculo elegido.

🔔 **Importante:** El sistema validará que no se elimine un tipo de vínculo o relación bajo el cual están asociadas 2 o más normas legales cargadas en el Digesto.

Paso 3: Verifique que la transacción se halla concretado satisfactoriamente, chequeando la respuesta del sistema en la barra de estado.

5.3.5. Gestión de Normas

Este componente gestiona la tabla principal de normas almacenadas en el repositorio. Esta tabla reúne toda la información descriptiva de las normas así como también el documento digital asociado a cada una. A través de este componente, usuarios autorizados pueden cargar nuevas normas al repositorio, modificar datos asociados a una norma o dar de baja algunos documentos, con los debidos controles sobre la información almacenada.

Identificando unívocamente la norma

Para poder administrar los datos referentes a una norma en particular, lo primero que debe hacerse es identificarla unívocamente, de manera que el sistema pueda determinar si la norma existe en su base de datos, o si es una nueva norma a punto de ser ingresada.

Para identificar unívocamente una norma deben completarse los siguientes datos en la pantalla de *Gestión Normas*

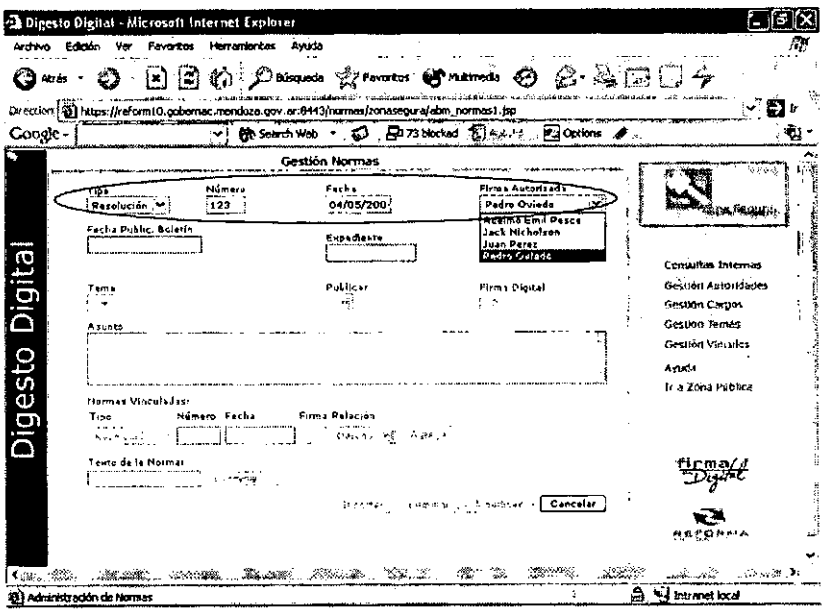


fig. 27. Datos de identificación de una norma

La combinación de *Tipo de norma* + *Número de norma* + *Fecha de emisión de la norma* + *Autoridad que firma la norma*, permite identificar de manera única a una norma en el sistema.

Si la norma existe previamente en el repositorio, el sistema habilitará automáticamente las opciones de *Modificar* o *Eliminar*, para que el usuario pueda realizar cambios en los datos asociados a la norma o dar de baja la norma del sistema respectivamente.

Si la norma no existe previamente en el repositorio, el sistema habilitará automáticamente las opción *Insertar* para cargar los datos y el documento firmado digitalmente al sistema.

🔔 **Importante:** En este punto, es probable que el usuario se pregunte, cómo es posible que el sistema le permita cambiar datos en las normas registradas en el sistema o dar de baja una norma. Frente a esta duda, debe recordar la diferencia entre la *ficha de datos* asociada a la norma y el *documento digital* de la norma propiamente dicho. El documento digital está ***firmado digitalmente*** por una autoridad competente y no podrá ser alterado por nadie. Lo que se administra desde el componente *Gestión Normas* es la *ficha de datos* asociada a la norma, cuyo único fin es organizar la información en el sistema para posibilitar consultas y revisiones posteriores. Por otra parte, debe recordarse que los únicos usuarios que tienen capacidades de alterar o dar de baja datos en el sistema son los *usuarios-administradores*, los cuáles están debidamente identificados y autorizados mediante su Certificado Digital.

Para agregar una nueva norma

Una vez identificada unívocamente la norma, se habilitará el formulario de carga para que complete los datos correspondientes a la ficha de la norma.

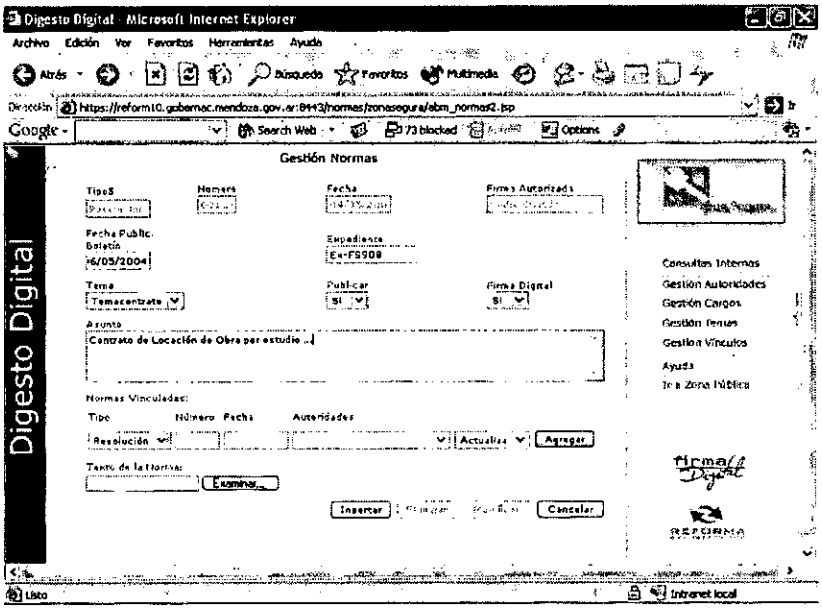


fig. 28. Cargando la ficha de datos de una norma

Es obligatorio completar los campos:

- *Número de Expediente*
- *Tema*
- *Publicar (determina si la norma será visible en la Zona Pública)*
- *Asunto*
- *Texto de la Norma.*

Los campos *Fecha de Publicación en Boletín Oficial* y los aquellos que permiten identificar *Normas Vinculadas*, no son obligatorios y sólo se cargarán cuando correspondan.

En las siguientes figuras se ilustra el agregado de dos resoluciones vinculadas. Para completar esta acción, hay que cargar en el formulario los datos que permiten identificar unívocamente a la norma vinculada y el tipo de relación que las une. El sistema no permitirá vincular normas que no hayan sido previamente cargadas al repositorio, de forma tal de garantizar la consistencia de los datos.

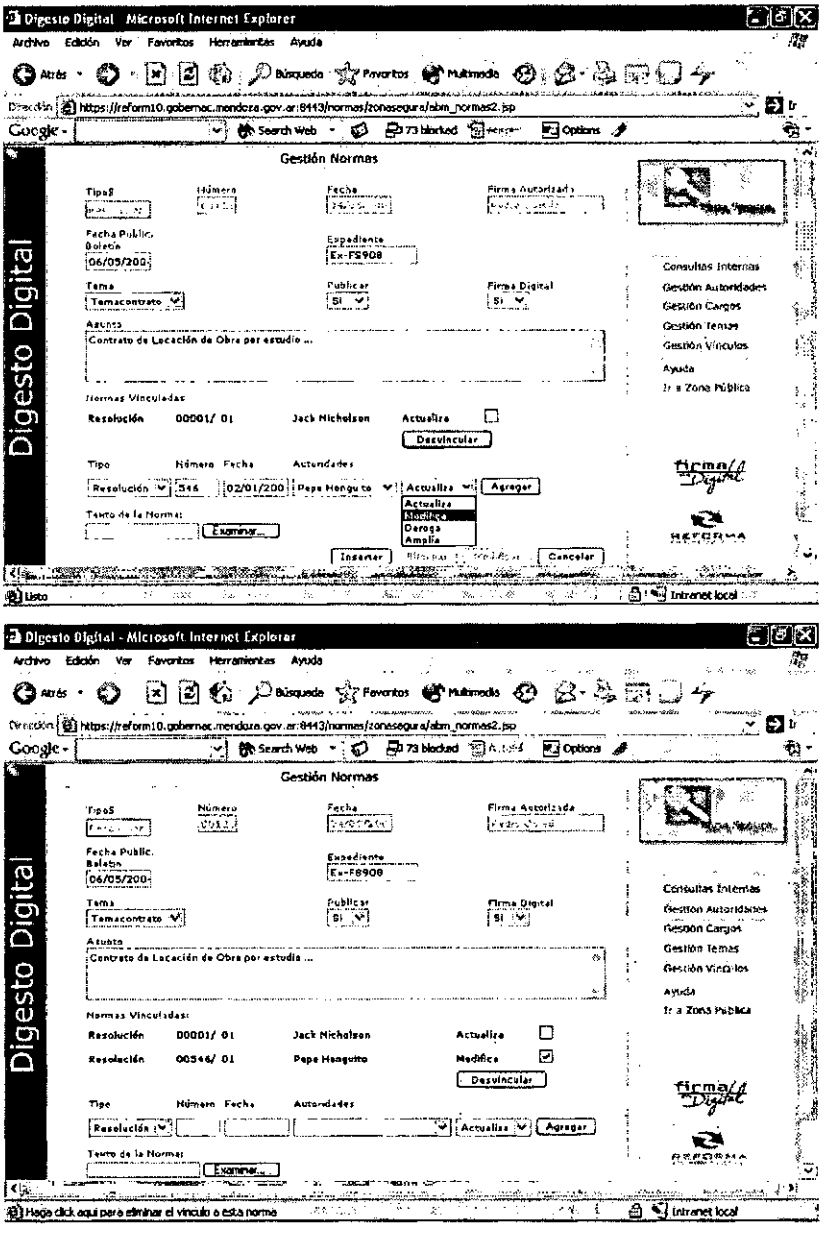


fig. 29. Vinculando normas

Para indicar cuál es el *documento digital* asociado a la *ficha de datos* que debe ser cargado al repositorio, deberá hacer clic en *Examinar* en el campo *Texto de la Norma*. De esta forma se abrirá un cuadro de selección de archivos para que pueda seleccionar el documento PDF correspondiente.

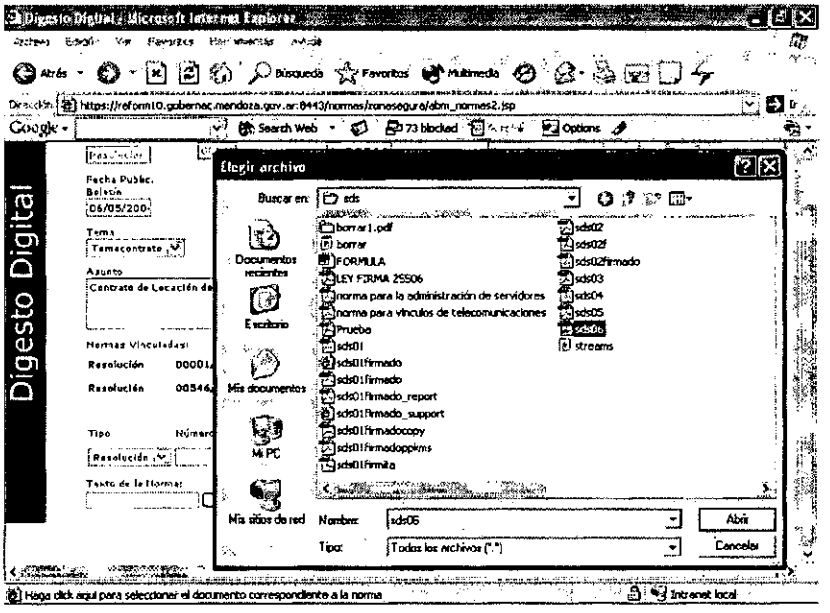


fig. 30. Cargando el documento digital firmado digitalmente

Importante: En la presente versión del sistema el *usuario-administrador* es responsable de verificar la firma digital del documento PDF previo a su carga en el repositorio.

Modificaciones

Una vez identificada la norma a actualizar, se habilitarán los campos con los datos existentes en el sistema para que pueda editarlos y modificarlos.

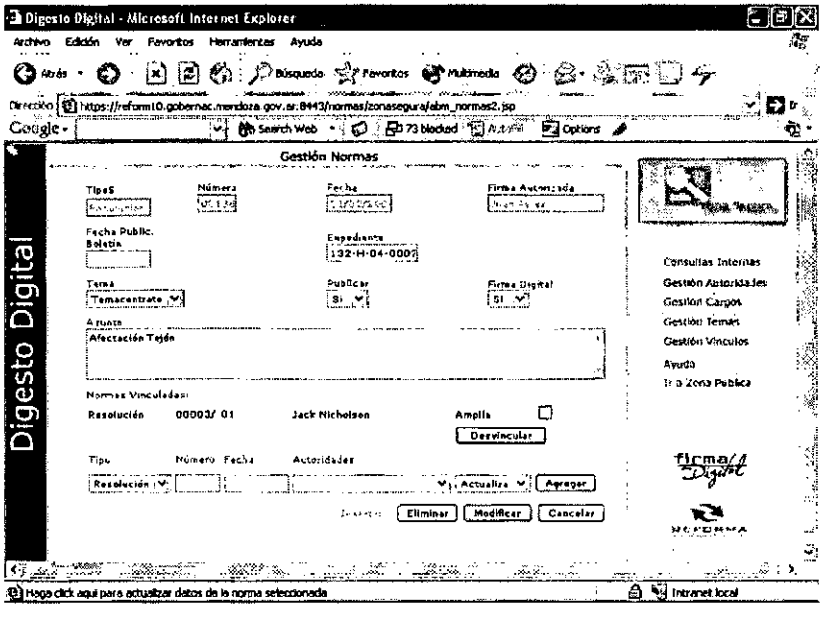


fig. 30. Actualizando datos de la ficha de datos de la norma

🔔 **Importante:** Se permiten actualizaciones sobre cualquier campo de la ficha de datos asociada a la norma, salvo los campos que permiten su identificación unívoca en el sistema. Consistentemente con el concepto de firma digital, tampoco es posible modificar el archivo PDF de la norma.

Baja

Para eliminar una norma del sistema, haga clic en la opción *Eliminar* y confirme la baja.

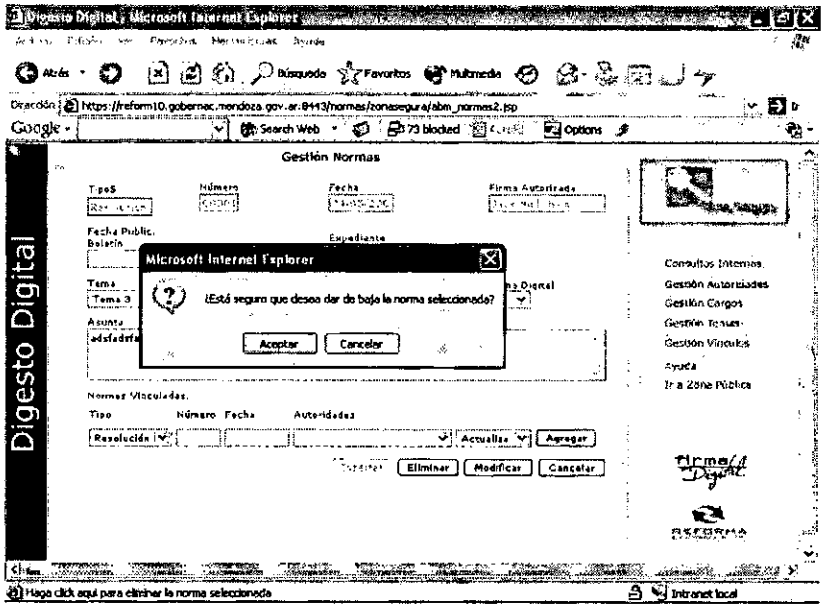


fig. 31. Eliminando una norma del repositorio.

Recuerde ante cualquier operación de alta, baja o modificación que realice sobre el repositorio, verificar el éxito de su transacción mediante el seguimiento de los mensajes que el sistema presenta en la barra de estado.

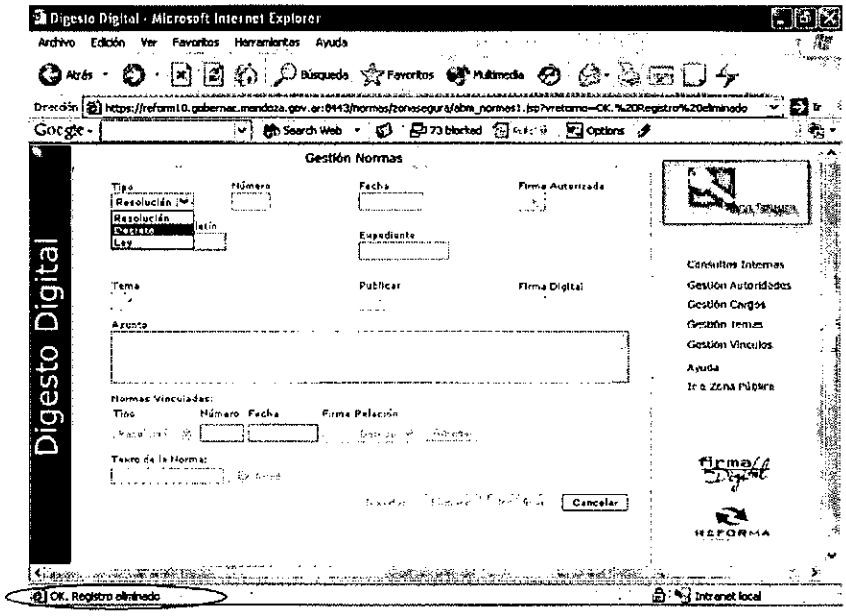


fig. 31. Verificando que se complete la transacción

Se presenta a continuación los mensajes de error, que habitualmente puede presentar el sistema y las acciones a realizar en cada caso.

6.1. Violación de integridad referencial: intento por eliminar una autoridad que ha firmado normas.

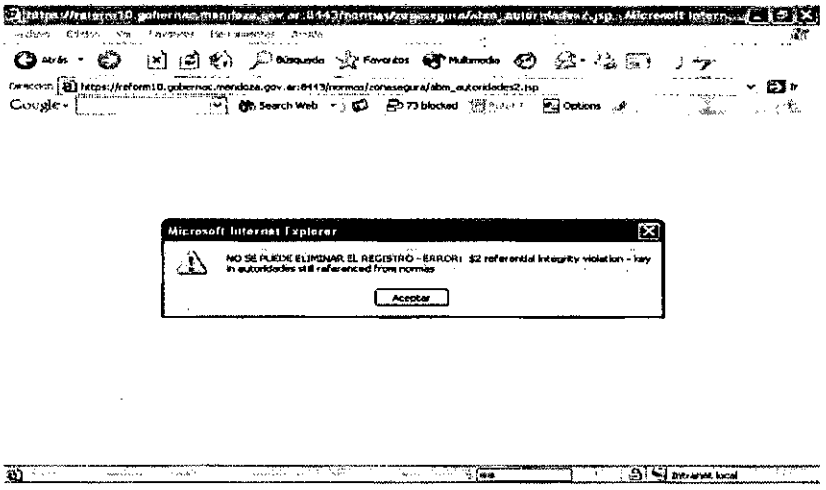


fig. 32. Violación de Integridad Referencial

Solución: Debe eliminar primero las normas vinculadas a esta autoridad.

6.2. Superposición de cargos: Intento de asignar un funcionario a un cargo, que en el período especificado estaba ocupado por otra persona.

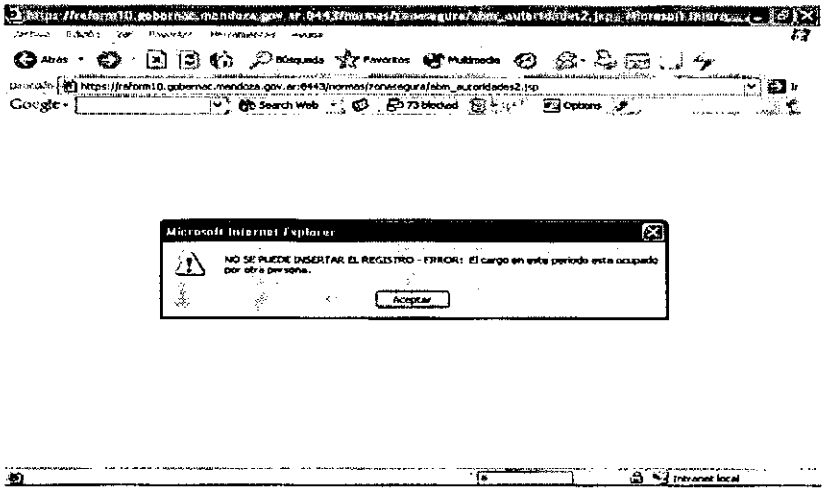


fig. 33. Superposición de cargos

Solución: Verifique los períodos de tiempo en los que los respectivos funcionarios se desempeñaron en el cargo en conflicto.

6.3. Inconsistencia de datos: Intento por dar de baja un dato que mantiene una estrecha vinculación a la *ficha de datos* de una norma.

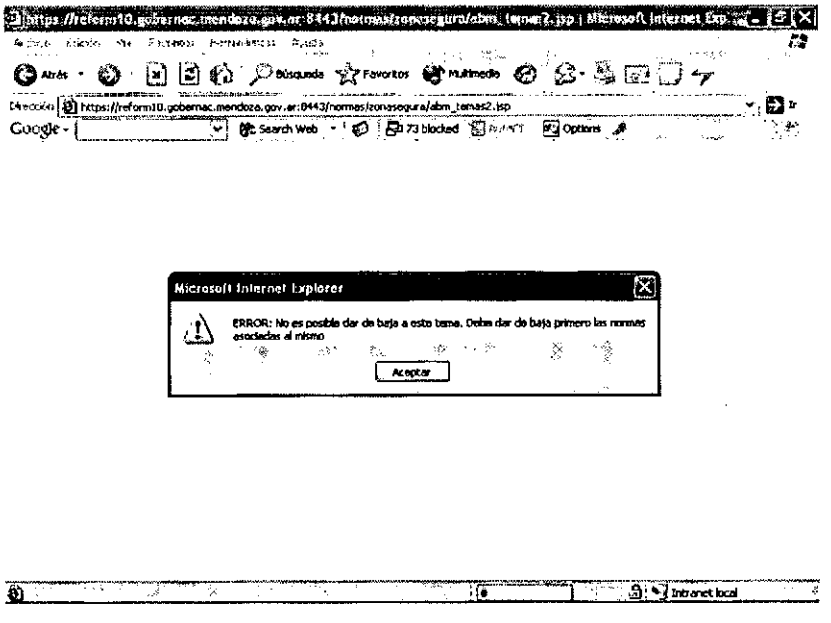


fig. 34. Previsión de inconsistencias

Solución: Revise los datos cargados en las *fichas de datos* asociadas a la información en conflicto.

Es muy importante que el *usuario-administrador* tenga presente que, cualquier transacción que realice sobre los datos del sistema queda debidamente registrada en los archivos de administración del sistema. Este archivo es monitoreado por el *Administrador en TI* y puede ser convenientemente auditado por autoridades competentes cuando así sea requerido.

Cada transacción realizada en el sistema, es debidamente registrada en el archivo de administración o *log*, junto a los datos del usuario, fecha y hora en que la operación fue realizada.
También es posible rastrear intentos de acceso indebido al sistema e intentos por concretar transacciones no permitidas.

Estos elementos contribuyen a la seguridad de la información mantenida en el repositorio y brinda garantías a los *usuarios-administradores* en cuanto a la responsabilidad que les compete en el ejercicio de sus funciones en el sistema.
Por lo expuesto, es fundamental que el *usuario-administrador* mantenga en absoluta reserva su Certificado Digital y la correspondiente clave de acceso.

Unidad de Reforma y Modernización del Estado
Secretaría Administrativa Legal y Técnica
Gobierno de Mendoza

Lic. Pablo Lioy – plioy@mendoza.gov.ar
Ing. Mariana Brachetta –
mbrachetta@mendoza.gov.ar

0261 - 4492021