

Proyecto de Grado

Ingeniería en Computación

*Desarrollo e implementación
de un Sistema de Gestión
de Expediente Electrónico*

Juan López Cabrera
Luis Michelena Scaffo

<u>1</u>	<u>Introducción</u>	<u>4</u>
<u>2</u>	<u>Estudio del problema.</u>	<u>5</u>
2.1	Marco de Trabajo y Conceptos manejados.	5
2.1.1	Marco Regulatorio del Proceso Administrativo Uruguayo.	5
2.1.2	Sistemas de Workflow.	9
2.1.3	Encriptación e Identificación Digital	11
2.1.4	Software Libre y la Administración Pública	17
2.2	Requerimientos del sistema.	22
2.2.1	Requerimientos Funcionales.	23
2.2.2	Requerimientos No Funcionales.	27
<u>3</u>	<u>Descripción del Sistema Base.</u>	<u>30</u>
3.1	Componentes principales de Paflow.	32
3.1.1	Zope	32
3.1.2	PostgreSQL	34
3.2	Productos Zope utilizados por la aplicación base.	35
3.2.1	OpenFlow	35
3.2.2	OpenflowEditor	36
3.2.3	DocumentLibrary	39
3.2.4	Localizer	44
3.3	Descripción Técnica	45
3.3.1	Base de datos	45
3.3.2	El proceso <i>Pratica</i> .	50
<u>4</u>	<u>Descripción de la solución propuesta.</u>	<u>53</u>
4.1	Diseño y Adaptación del sistema a los requerimientos	53
4.1.1	Definición de Workflows de Expedientes.	53
4.1.2	Modificaciones a la base de datos	58
4.1.3	Roles de la aplicación y su función.	61
4.1.4	Esquema de Seguridad en Yará	62
<u>5</u>	<u>Funcionalidades brindadas.</u>	<u>65</u>
5.1	Expedientes	66
5.1.1	Inicio y anulación de expedientes	66
5.1.2	Seguimiento de expedientes	67
5.1.3	Ingreso de Informes	67
5.1.4	Consulta de Expedientes	67
5.1.5	Ingreso de movimientos de expedientes	67
5.1.6	Asignación a responsables	67
5.1.7	Lista de Trabajo.	67
5.1.8	Otros Documentos	68
5.2	Definición de la estructura organizacional.	68
5.3	Definición de Workflows asociados a Expedientes.	68
<u>6</u>	<u>Conclusiones y Pasos Futuros</u>	<u>69</u>
<u>7</u>	<u>Apéndice A – Bibliografía</u>	<u>71</u>
<u>8</u>	<u>Apéndice B: Glosario</u>	<u>73</u>

9 Apéndice C: Presentación De Proyecto De Grado81

1 INTRODUCCIÓN

El presente documento describe el Sistema de Gestión de Expediente Electrónico, al que hemos denominado “**Yarará**”, el cual ha sido realizado en el marco de la presentación, por parte de la Dirección de Informática del Ministerio de Relaciones Exteriores, de una propuesta de realización de este sistema como proyecto de grado para la carrera de Ingeniero en Computación ante la Facultad de Ingeniería de la Universidad de la República.

Desde siempre las grandes oficinas u organizaciones han reunido los documentos asociados con un cierto trámite o acto en legajos que han rotulado con un identificador único, creando así lo que conocemos hoy en día como el expediente tradicional. El mismo constituyó una forma organizada de manejo documental para una era tecnológica que no ofrecía alternativas, basando el éxito de su funcionamiento en las oficinas cuyo único objetivo consistía en poder localizar, en cualquier momento, un determinado expediente.

Los problemas de lentitud, extravíos, robos, deterioros, folios faltantes, imposibilidad de acceso, dificultades de almacenamiento y otros recién fueron encontrando alguna solución en los años '80 cuando se difundieron los primeros programas para seguimiento de expedientes, cuyo cometido esencial era el de llevar registro de la ubicación del expediente físico en todo momento. Pero fue recién hacia finales de los años 90' cuando la baja en los costos de los sistemas de computación así como la difusión de estándares universales y abiertos, particularmente los de Internet, permitieron el desarrollo de Sistemas de Expediente Electrónico en el sentido más amplio del término.

El sistema realizado es un Sistema de Gestión de Expediente Electrónico (SGEE) parametrizable, que trata de responder a las necesidades de administración de los organismos públicos con el objetivo de automatizar y controlar los procesos administrativos existentes como una forma de incrementar su eficacia y eficiencia. Desde un punto de vista técnico, un S.G.E.E. es un Sistema de Workflow centrado en manejo de documentos, donde se tienen requerimientos especiales en cuanto a seguridad.

Este documento se divide en las siguientes partes:

- En el punto 2 se brindan conceptos previos necesarios para comprender la problemática a resolver y su contexto, tanto legal como operativo y tecnológico, así también como los requerimientos que el sistema debía cumplir.
- El punto 3 se describe el software que, por sus funcionalidades y sus características de licencia, fue elegido como la plataforma sobre la cual se construiría el sistema. Esta elección fue el resultado de la comparación de varias herramientas utilizables, las cuales se describen en la Documentación Técnica del sistema por constituir ramas posibles de desarrollo en la vida de este producto. Se describen las funcionalidades que brinda y sus principales componentes.
- En el punto 4 se detallan las modificaciones y agregados realizados al sistema base para cumplir estos requerimientos especificados en el punto 2.
- En el punto 5 se describen, en forma resumida, las principales características de Yarará y sus funcionalidades, las cuales se describen en detalle en su Documentación de usuario
- Finalmente exploramos en el punto 6 los desvíos del sistema a los requerimientos iniciales junto con las características que podrían ser deseables en un futuro para la misma.

2 ESTUDIO DEL PROBLEMA.

En este punto procederemos a reseñar y analizar las restricciones impuestas y los conceptos fundamentales manejados, que serán de utilidad para el lector en los subsiguientes puntos de este informe. Se analizan, en la primera parte, las restricciones legales Uruguayas para este tipo de sistemas, se brinda una introducción a los conceptos fundamentales sobre Encriptación e Identificación Digital y Sistemas de Workflow para finalizar con descripción de lo que es el considerado "Software Libre" y la relevancia que su uso tiene en el ámbito del estado en general y para el tipo de sistema que os ocupa en particular.

En la segunda parte de este punto se detallan los requerimientos del sistema. Para hacerlo, se ha incluido en forma íntegra el documento de requerimientos elaborado entre el equipo de desarrollo y dirección de informática del Ministerio de Relaciones Exteriores en su versión definitiva de fecha 18/07/02.

2.1 Marco de Trabajo y Conceptos manejados.

2.1.1 Marco Regulatorio del Proceso Administrativo Uruguayo.

Antecedentes.

El marco normativo Uruguayo relacionado directamente con este proyecto puede identificarse en los decretos 500/991[13] y 65/998 [19]. El primero contiene normas que regulan el procedimiento administrativo, basado en el expediente "tradicional" (soporte papel), en las instituciones públicas. El segundo es el resultado de la necesidad de reglamentar los art. 694 a 697 de la ley N° 16.736 , tarea que le fue asignada a la Oficina Nacional del Servicio Civil, la cual formó un Grupo de Trabajo multidisciplinario, integrado por profesionales abogados y técnicos en Informática.

El objetivo de dicho Grupo de Trabajo fue lograr que la reglamentación a dictarse fuera una norma "marco", que hiciera posible de forma simple y sencilla, la incorporación de los medios informáticos y telemáticos a la gestión administrativa, adecuándose a las realidades de cada organismo. Los principios fundamentales del decreto son lograr una mayor eficiencia y eficacia en la actuación administrativa. El art. 14 del decreto 65/998 establece a la ONSC como el organismo responsable de determinar los procedimientos y tecnologías a los que se deben ajustar las organizaciones que implementen expedientes electrónicos por lo que su estudio se hace imprescindible para comprender las condicionantes impuestas a un sistema de este tipo.

En lo que sigue de este punto se comentará los conceptos relevantes del decreto 65/998.

Concepto de expediente electrónico.

El art. 2 del Decreto N° 65/998, contiene la definición de expediente electrónico, entendiéndose por tal: *"... La serie ordenada de documentos públicos registrados por vía informática, tendientes a la formación de la voluntad administrativa en un asunto determinado"*. De dicha definición se desprende que el texto aprobado no hace más que recoger el concepto que define el expediente con "soporte papel". Ello es así, por cuanto el espíritu de La reglamentación, ha sido el de introducir la nueva modalidad de gestión administrativa, pero sin que ello suponga el desconocimiento de los principios que han informado la gestión administrativa en su modalidad tradicional.

De esta definición, se desprenden los cuatro elementos del expediente electrónico: a) forma, b) contenido, c) medio o instrumento, y d) fin.

Forma: en primer lugar, se trata de una serie ordenada, esto es, supone una ordenación de documentos, como por ejemplo una petición administrativa, un informe de la Asesoría Letrada, una vista y una resolución del jerarca de un órgano del Estado.

Contenido: en segundo lugar, es una serie ordenada de “documentos públicos”, no de documentos privados. El Código Civil distingue entre instrumentos públicos e instrumentos privados. Según el art. 1 574 del Código Civil, es instrumento público todo aquel que, revestido de un carácter oficial, han sido redactados o extendidos por funcionarios competentes, según las formas requeridas y dentro del límite de sus atribuciones. “Todo instrumento público es un título auténtico, y como tal hace plena fe”. Entonces, podría concluirse que sólo forman parte del expediente electrónico los instrumentos públicos y que una petición presentada, o un recurso administrativo interpuesto por un particular, o una vista evacuada en un procedimiento disciplinario, no constituirían parte del expediente electrónico, porque son instrumentos privados. Cabe, sin embargo, una interpretación diferente. Constituye un expediente electrónico aquella serie ordenada de documentos que se tramitan en la Administración Pública por vía informática, integrado por documentos públicos y documentos privados. La intervención de funcionarios públicos en la tramitación de un expediente en la Administración Pública, le confiere el carácter de documento público a las actuaciones contenidas en el mismo. Así, por ejemplo, ante un escrito presentado por un particular ante una oficina del Estado, el mismo debe ser recibido por un funcionario público, quien debe expedir la constancia correspondiente, extremo que le da el carácter de documento público al documento que originalmente era un instrumento privado.

Medio o instrumento: en tercer lugar, se requiere que la serie ordenada de documentos públicos sean registrados por vía informática, que es lo que califica al expediente electrónico, esto es, el medio o instrumento utilizado que es el informático, por oposición al tradicional expediente de papel.

Fin: en cuarto lugar, nos encontramos con el fin del expediente electrónico, que es la formación de la voluntad administrativa en un asunto determinado, esto es la decisión o la resolución definitiva por parte de la autoridad competente de una repartición de la Administración Pública.

Validez del expediente administrativo electrónico.

El art. 3º del Decreto No. 65/998 le asigna al expediente electrónico la misma validez jurídica y probatoria que al expediente tradicional. Cabe señalar, que el art. 695 de la Ley No. 16.736 de 5 de enero de 1 996, expresa que “*Su validez jurídica y valor probatorio serán idénticos a los de las actuaciones administrativas que se tramiten por medios convencionales*”.

Se agrega que “*La documentación emergente de la transmisión a distancia, por medios electrónicos, entre dependencias oficiales, constituirá, de por sí documentación auténtica y hará plena fe a todos sus efectos en cuanto a la existencia del original transmitido (art. 129 de la Ley No. 16.002 de fecha 25 de noviembre de 1988)*”. Por lo tanto, son válidas las comunicaciones por correo electrónico, fax, o telex. Pero solo en el ámbito de las comunicaciones entre oficinas de la Administración Pública.

Normas sobre procedimiento administrativo electrónico.

El art. 4º del Decreto del Poder Ejecutivo No. 65/998, prescribe que “*Todas las normas sobre procedimiento administrativo serán de aplicación a los expedientes tramitados en forma electrónica, en la medida en que no sean incompatibles con la naturaleza del medio empleado*” Se admite expresamente la presentación de peticiones y recursos administrativos ante la Administración Pública por medio de documentos electrónicos, los que deberán ajustarse a los formatos o parámetros técnicos que oportunamente fije el Poder Ejecutivo. Aquí debemos distinguir dos hipótesis:

- Que la petición o el recurso se presente en un disquete, es decir en un documento electrónico (art. 60)
- Mediante correo electrónico, es decir mediante transferencia electrónica (art. 7º), en cuyo caso la Administración deberá expedir la constancia de su recepción, debiendo contener la fecha, lugar y la firma digital del receptor.

Para ambas hipótesis, el Reglamento prevé la aplicación, en lo pertinente, de las disposiciones contenidas en los arts. 157 a 159 del Decreto No. 500/991, que prevé la presentación de recursos administrativos por telegrama colacionado certificado con aviso de entrega, télex, fax u otro procedimiento similar. Asimismo, se prevé la admisión por parte de la Administración de la presentación de documentos registrados en papel para su utilización en un expediente electrónico (art. 8º), pudiéndose optar entre la digitalización del documento o la formación de una pieza separada. Se establece como meta deseable, la digitalización total de los documentos. En el art. 9º. se autoriza la reproducción y almacenamiento por medios informáticos de los expedientes tradicionales o convencionales; y el art. 1º autoriza, a su vez, la reproducción sobre papel de los expedientes electrónicos, debiendo el funcionario responsable certificar su autenticidad. Tales comunicaciones deberán satisfacer criterios técnicos a definirse, que garanticen los controles de firmas digitales, fecha, hora de recibido, lugar, funcionario receptor, etc., necesarios para su correcta gestión. Dichos controles serán efectuados por las aplicaciones desarrolladas en los Organismos, siguiendo criterios que serán establecidos por la Comisión Nacional de Informática (CONADI), como lo establece el art. 6º.

Sustitución de las firmas autógrafas.

En el Capítulo III del Decreto No. 65/998, se regula lo referente a la firma electrónica y digital, extremo que resulta de capital importancia dado que en el expediente administrativo electrónico se habrá de manifestar la voluntad de la Administración. Se distingue entre la firma electrónica y la firma digital. El art. 18 del Decreto comentado, define a la *firma electrónica* como el resultado de obtener por medio de mecanismos o dispositivos un patrón que se asocie biunívocamente un individuo y a su voluntad de firmar. Esto es lo que comúnmente en informática se conoce como el "password" o contraseña, que es la clave informática que tiene una persona y que solamente ella la puede usar. Se puede pensar, además, en mecanismos mas sofisticados como ser utilización de tarjetas inteligentes o aparatos capaces de identificar a una persona por sus características biométricas. En cambio, la *firma digital*, según el art. 19 del Decreto No. 65/998, es un patrón creado mediante criptografía, debiendo utilizarse sistemas criptográficos "de clave pública" o "asimétricos", o los que determine la evolución de la tecnología.

El art. 22 establece una presunción de autoría del usuario al que se le haya asignado la clave privada correspondiente, respecto de un documento electrónico autenticado mediante firma digital. No obstante la presunción de autenticidad, se admite la prueba en contrario en caso de la falsificación del documento electrónico por la divulgación de la clave por terceros. Se hace referencia especial a la responsabilidad de cada organismo en el manejo de todas las claves, ya sean públicas o privadas, utilizadas para obtener las referidas firmas (art. 20). Respecto al manejo que de la clave o contraseña particular haga el funcionario público actuante en una gestión informatizada, se prevé expresamente que su divulgación constituirá falta grave, lo que permite llegar incluso a su destitución por tal motivo, incluso cuando aquella no llegase a ser utilizada (art. 21).

El inciso segundo del art. 22, consagra como excepción, que la firma del Presidente de la República y de los Ministros de Estado en los decretos y resoluciones del Poder Ejecutivo deben estamparse con la firma en forma ológrafa o autógrafa.

En el art. 23º se detallan los documentos que deberán identificarse mediante una firma digital o electrónica, dado que revisten especial importancia para la Administración. Estos son:

- Los recursos administrativos, así como toda petición que se formule a la Administración.
- Los actos administrativos definitivos.
- Los actos administrativos de certificación o destinados a hacer fe pública.
- Los dictámenes o asesoramientos previos a una resolución definitiva

En el art. 24º se autoriza a que los demás trámites sólo sean identificados por una clave simple (sin encriptación ni firma digital).

Finalmente, en los artículos 25º y 26º, se establecen las penalidades para los casos de adulteración, destrucción y transmisión voluntaria e infiel de documentos.

Coexistencia del documento electrónico y el "soporte papel".

La disposición del art. 8 del decreto reglamenta la etapa de transición resultante de la innovación que se implanta, procurando minimizar el lógico impacto de la nueva normativa.

La referida norma establece que: *"La Administración admitirá La presentación de documentos registrados en papel para su utilización en un expediente electrónico. En tales casos, se podrá optar entre la digitalización de dichos documentos para su incorporación al expediente electrónico o La formación de una pieza separada o una combinación de ambas, fijando como meta deseable La digitalización total de los documentos"*.

De esa manera se trata de contemplar, no solo las distintas realidades existentes a nivel de La Administración Central, sino las posibilidades de aplicación de la nueva herramienta por parte de los usuarios, particulares o administrados, considerando las limitaciones que pudieran plantearse en la etapa inicial. Las aplicaciones de expedientes electrónicos deberán permitir manejar expedientes tradicionales (en papel) junto con los digitales, e incluso en forma mixta. En tal sentido, el art. 8º establece que el funcionario responsable de la digitalización sea "responsable" por la misma, agregando su firma digital (o en su lugar la electrónica) al proceso. En el caso inverso, cuando del expediente electrónico se pasa al papel, el funcionario responsable del proceso deberá hacerse responsable de la autenticidad certificándolo con su firma autógrafa (art. 10º). Estas copias tendrán la misma validez del documento original (art. 17).

En el art. 16 se permite que los documentos digitalizados en su totalidad puedan ser destruidos si se considera conveniente exceptuándose aquellos que se consideren que posean un valor histórico, cultural o de otro tipo para los cuales siguen vigentes las normas existentes para la conservación de documentos.

Racionalización del procedimiento administrativo.

Contenido en el decreto 500/991 e implícito en el decreto analizado, existe la voluntad, expresada en el art. 38, de registrar, por temática de los expedientes, la secuencia de unidades administrativas por las que éste debe pasar para su resolución. En este particular se expresa que:

"El jerarca de cada dependencia o repartición fijará la secuencia de las unidades administrativas que habitualmente deban participar en la sustanciación de cada tipo o clase de expediente por razón de materia, con la que se elaborará la correspondiente hoja de tramitación. Dicha hoja será puesta por la unidad de administración documental como foja inicial del expediente, a continuación de la carátula y antes de toda actuación. La intervención de unidades o órganos de asesoramiento no previstos originalmente en la mencionada hoja; será debidamente justificada por la unidad que la promueva."

A los efectos de optimizar el movimiento de los expedientes, se establece en el art. 11º que los que se encuentren digitalizados no sean desplazados, y los restantes sean dirigidos a archivos transitorios de fácil acceso por los funcionarios involucrados en su estudio.

Sobre los términos y plazos para la sustanciación del proceso, se debe aplicar el Decreto No. 500/991.

En el art. 13 del decreto 65/998 se expresa que la Administración debe poder controlar, mediante el sistema, el cumplimiento de los términos y plazos que rigen para el procedimiento administrativo y, en particular, se menciona que en caso de demoras, el jerarca de la dependencia deberá poder modificar la ruta del expediente (arts. 12 y 13).

2.1.2 Sistemas de Workflow.

Según la definición de la Workflow Management Coalition (WFMC) [25] un workflow es:

“la automatización total o parcial de un proceso de negocio, en el cual documentos, información o tareas son pasadas de un participante a otro, de acuerdo con un conjunto de reglas procedurales”

Para entender esta definición hace falta introducir el concepto de proceso de negocio:

“Conjunto estructurado de tareas, que contribuyen colectivamente a lograr los objetivos de una organización”

Es innecesario reseñar aquí los beneficios, en productividad y calidad que se logran (mas allá de la automatización) formalizando los procesos que se desarrollan dentro de una organización. Tradicionalmente estos procesos, recogidos en “manuales de procedimientos” realizados en lenguaje natural o mediante diagramas de flujo, han estado fuera del ámbito de la automatización. Sin embargo ésta es deseable ya que, mediante la automatización parcial o total de estos, se incrementan los beneficios logrados en su formalización.

Un Sistema de Workflow, según la WfMC es:

“Sistema capaz de definir, administrar y ejecutar Workflows, a través de software que interpreta una representación electrónica del mismo e interactúa con los recursos participantes”

La definición de Sistema de Workflow, publicada en el glosario de la WfMC en 1996, tiene una connotación bastante amplia. Se refiere a todos los procedimientos de trabajo de organizaciones privadas o públicas. La principal pregunta que un Sistema de Workflow debe responder es: *“quien debe hacer que, cuando y como”*. Los procedimientos típicamente están constituidos por actividades elementales como la interacción con una Base de Datos, redacción y firma de documentos, su envío por correo electrónico o una actividad decisional.

Del glosario de la WFMC extraemos otras definiciones importantes para comprender lo que es un Sistema de Workflow

Engine (Motor de Workflow):

“Servicio de Software que brinda el ambiente necesario para la instanciación de un proceso”

Proceso:

“Representación de un proceso comercial de forma que soporte manipulación automática o ejecución por parte de un Sistema de Workflow. El proceso consiste en un conjunto de actividades relacionadas entre sí, con información que indica su inicio y fin, información específica de cada actividad, como ejecutante, aplicación y datos asociados”

Instancia:

“Representación de un proceso incluyendo sus datos asociados. Cada instancia representa un hilo separado de ejecución de un proceso que puede ser controlado independientemente y que posee su propio estado interno e identidad visible externamente, que puede ser usado para manejar la registración o recuperar los datos de control relativos a la ejecución del proceso”

WorkItem (instancia de actividad):

“Representación del trabajo que debe ser realizado en el contexto de una actividad en una instancia de Workflow”

Todos los Sistemas de Workflow son orientados a los procesos. Una definición de proceso es la representación de lo que debe pasar y, usualmente, comprende actividades que a su vez pueden ser sub -procesos.

Los Sistemas de Workflow pueden clasificarse según su uso como [24]:

Workflows de Producción

La meta clave de un Workflow de Producción está en administrar números grandes de tareas similares y en perfeccionar la productividad. Esto se logra automatizando la mayor cantidad de tareas prácticas y persiguiendo una mayor automatización de forma que el único aporte humano que se requiera sea el de administrar excepciones, es decir, el manejo de instancias que caen fuera de límites fijados para el proceso. Los Workflow de Producción pueden administrar procesos complejos, y pueden integrarse estrechamente con sistemas existentes (legados).

Motores Autónomos de Workflow

Un sistema de gestión de workflow autónomo es funcional mas allá del software adicional de aplicación que se puede invocar eventualmente en cada actividad, con excepción del middleware como sistemas de mensajes y sistemas de gestión de base de datos. En un sistema autónomo de Workflow los sistemas de aplicación que son externos al sistema de gestión de workflow se invocan en tiempo de ejecución y los datos relevantes al workflow son pasados entre los participantes del mismo.

Workflow Embebido

Un sistema de gestión de workflow embebido es únicamente funcional si es empleado alrededor (embebido) en otro sistema. La funcionalidad de los sistemas de gestión workflow embebido es mostrada por el sistema de software circundante. El componente de workflow es utilizado por el sistema principal para controlar la sucesión de las funciones de las aplicaciones, para administrar colas y para ayudar con el procesamiento de excepciones.

Administrativos

El aspecto más importante de un sistema administrativo de workflow es la facilidad para definir procesos. Típicamente, hay muchas definiciones que corren concurrentemente y tienden a

involucrar un número grande de empleados. La flexibilidad es más importante que la productividad. Estos sistemas manejan uno o dos órdenes de magnitud inferior en cuanto a número de instancias de proceso por la hora que Sistemas de Workflow de Producción

Colaborativos

Los workflow Colaborativos se enfocan a equipos que trabajaron juntos hacia metas comunes. Los grupos pueden variar desde pequeños, típicamente la realización de un proyecto, a grupos de gente ampliamente dispersa con intereses en comunes. El uso efectivo de workflows Colaborativos como una herramienta de apoyo para los equipos de trabajo se considera en la actualidad como un elemento vital en el éxito de empresas de todo tipo. El uso de Internet y la World Wide Web para apoyar las comunicaciones de los equipos en los emprendimientos es también un factor de éxito crítico en la mayoría de las organizaciones. Las Definiciones de los Procesos no son rígidas y puede modificarse frecuentemente. Los Workflow Colaborativos son llamados a veces Groupware. Por otra parte, hay tipos de Groupware que no son Workflows, por ejemplo, Bulletin Boards o Videoconferencias

AD - HOC

Los sistemas de Workflow Ad-Hoc permiten a los usuarios crear y modificar definiciones de proceso muy rápidamente para permitir que cumplan las condiciones que desean por lo que es posible que se tengan tantas definiciones de procesos como instancias. El Workflow AD - Hoc aumenta al máximo flexibilidad en áreas donde el historial y la seguridad no son los intereses primordiales.

2.1.3 Encriptación e Identificación Digital

En este apartado se resume, en parte lo dicho en las referencias [4 y 19]

2.1.3.1 Nociones Generales

Desde tiempos inmemoriales, el hombre ha necesitado proteger información **reservada** y enviarla por canales inseguros. Quedan en los anales de la historia y de la literatura numerosos ejemplos de casos en que se utilizaron códigos y contraseñas para acceder a dicha información. Valgan como ejemplos el código de transposición utilizado por el Cesar en la antigua Roma para mandar matar a sus enemigos, la clave utilizada en el libro "El señor de los anillos" para acceder a las Cuevas de Moria: "habla amigo y entra" o la maquina Enigma utilizada por los nazi para codificar (o **encriptar**) sus mensajes en la segunda guerra mundial (código que al ser roto por los aliados ayudó grandemente a la victoria aliada). Vale además este último caso para ejemplificar los intentos de romper dichos códigos, para acceder al secreto protegido, costumbre tan antigua como su contraparte.

Así mismo, era necesario verificar, en ausencia del emisor, la veracidad de distintos documentos. Así se utilizaron sellos, para arcilla, en la antigua Babilonia, o en cera, con la impresión del anillo del monarca en la edad media. Y por último la más conocida y utilizada en la actualidad, la **firma autógrafa**.

Con la entrada en forma masiva de la computadora y la red a la vida de las personas comunes y de la sociedad en general, y la explosión de nuevas posibilidades de comunicación e intercambio que esto conllevó, como correo electrónico, video conferencias, etc. estos aspectos adquieren nueva actualidad e hicieron necesario replantearse las normas vigentes para el manejo de documentos.

Estas normas, indefectiblemente, pero sin una indicación explícita, hacían referencia a la propiedad física del papel para incorporar tinta y otras partículas, en forma casi inalterable, registrando de esa forma dibujos y símbolos. Así si bien es posible borrar algo escrito con tinta de un papel, las operaciones corrientes para hacerlo, como las gomas de tinta o el líquido corrector dejan marcas fácilmente detectables.

Dicha inalterabilidad es solo comparable con la de ciertas sustancias que por medio de técnicas basadas en propiedades físicas o químicas pueden ser “marcadas” **y que se pueden modificar una sola vez**. En esta categoría caen por ejemplo **los CD-ROM** o las memorias **ROM** modernos.

- Para mandar información **en forma inalterable** por dichos medios, es necesario trasladar **físicamente** el mismo, lo que hace que el transporte sea lento y de capacidad limitada, especialmente en estos tiempos en que el volumen de información que se mueve es tan grande y las distancias recorridas llegan a ser de magnitud continental o global.
- Para transmitir con mayor velocidad y volumen, es necesario utilizar señales electromagnéticas (electricidad, microondas, o incluso luz) utilizando para eso cables, antenas y satélites. Es decir, el componente físico de la transmisión es la **ruta** y no el **contenedor**. En esas condiciones, se puede interceptar la información en cualquier punto de esa ruta, leerla e incluso modificarla; Todo esto sin el conocimiento del emisor ni del receptor.

En todos los casos, es posible evitar lecturas de la información **solo** si el canal de comunicación está protegido, y el mensaje no se puede abrir. Sin embargo, al utilizar medios electrónicos, no es posible establecer **físicamente** un canal seguro debido a la naturaleza compartida del medio. Así cualquiera que se encuentre en el camino de un paquete en Internet o que se encuentre en el radio de alcance de una emisión de radio o microondas, puede leer la información. Es por eso que se hace necesario el uso de “contenedores” de carácter lógico - matemático. Y es aquí donde reaparecen las comunicaciones “en código”, utilizando **técnicas criptográficas**.

2.1.3.1.1 **LA FIRMA (Escrita, Digital y Electrónica)**

Cuando una trabaja con datos (o documentos) en forma digital, es posible copiar **exactamente** los mismos, con lo que el original es matemáticamente idéntico a la copia, dado que el medio no es físico. Al fin y al cabo un 0 es igual a otro 0. Esto hace que el potencial de fraude sea inmenso. Como ejemplo, es casi trivial, para documentos escaneados, sacarle la firma escaneada de un documento original y anexarla a uno apócrifo, sin posibilidad de detectarlo.

Es por eso que se han desarrollado varias técnicas disponibles actualmente y hay otras en desarrollo, cuyo cometido es el de dotar a la comunicación electrónica con algunas o todas las características de la firma escrita.

Como ejemplos de estos mecanismos, se puede uno referir a lo presentado en el cine: placas donde poner el dedo donde se verifica la huella dactilar, lectores del Iris (mostradas en la película “sentencia previa”) o analizadores de voz (como en la película “Héroes por azar”). Algunos más simples incluyen un panel donde se miden las dimensiones de la mano del interesado. Ejemplos de este tipo se encuentran en uso ya en Uruguay (Facultad de Agronomía o el Palacio

Legislativo, por poner dos ejemplos)

El proceso de “firmar” un documento implica 2 elementos: la voluntad del dueño de la firma para “dibujar” su firma característica y la firma en sí misma. Por otra parte, la firma de una persona cumple varias funciones, dependiendo de la naturaleza del documento firmado: la de establecer la autoría del texto previo (ej.: carta), la adhesión a lo escrito por otro (ej.: reclamo), la de aceptar obligaciones que surgen del texto firmado (ej.: contrato) y el establecimiento certero de que la persona estuvo presente en el lugar y fecha detalladas en el mismo (ej.: asistencia).

Una contraseña empleada para la firma digital difiere de la firma electrónica en cuanto a que la primera es un dato (secuencia de bits) que una vez divulgado permite que cualquiera pueda firmar documentos haciéndose pasar por el titular. En cambio la firma electrónica depende en definitiva de factores biométricos o mecánicos, de muy difícil reproducción por terceros.

2.1.3.2 Criptografía Y Confidencialidad

La ciencia que estudia los procesos de opacado (ocultar la información dentro de sí misma) de la información por medios matemáticos se llama criptografía y se utiliza para evitar que la información sea leída por personas no habilitadas para ello

Con los tiempos se ha ido haciendo más complejos los métodos para poner en clave una información. Así para encriptar algo, se le aplica un algoritmo teniendo como fuentes lo que se quiere proteger y una clave, para generar otro conjunto de datos que carece de sentido si no se tiene para hacer la transformación inversa, siendo, por tanto, apta para transmitirse y se le llama **mensaje encriptado**.

Con respecto a los algoritmos utilizados existen muchos métodos, aunque se pueden hacer algunas clasificaciones:

- El algoritmo empleado puede ser de dominio público o ser secreto del emisor y receptor, aunque la seguridad final del mensaje no depende de este aspecto sino del algoritmo en sí mismo.
- Por la relación entre las claves utilizadas para encriptar y desencriptar respectivamente, si son la misma se habla de un algoritmo criptográfico **simétrico**, si son distintas, se trata de un método **asimétrico o de clave pública** (más adelante explicaremos esto con más detalle).
- Por el tamaño de la clave utilizada: esto determina (junto con el algoritmo en sí) la seguridad del método, cuanto más grande la clave, más difícil resulta romperlo. De hecho en general se mide la seguridad de un método por la cantidad de tiempo que le tomaría a la computadora más rápida existente, hallar la clave.

Es de hacer notar que todos estos métodos son en **TEORÍA**, inseguros, debido que siempre es posible romper una clave teniendo el tiempo suficiente. Es por eso que los métodos cambian continuamente, porque cada vez las computadoras son más rápidas, por lo que el tiempo promedio

para romper un algoritmo dado va decreciendo con el tiempo.

2.1.3.2.1 **Criptografía simétrica**

La criptografía con claves simétricas tiene el inconveniente de que el remitente debe obtener la clave necesaria por un medio más seguro que el utilizado para enviar el mensaje: por ejemplo personalmente. En las comunicaciones modernas es difícil que los interlocutores se conozcan personalmente, por lo que esta opción no es viable. Pero por otra parte, en general son mucho más rápidos que los de clave asimétrica.

Ejemplo: El algoritmo de transposición o del Cesar

Uno de los algoritmos de encriptación simétrica más antiguos (e inseguro).

Utilizado para codificar mensajes textuales: se elige un número X entre 1 y la cantidad de letras del alfabeto: esa será nuestra clave.

*Después, para cada letra del mensaje se la cambia por la letra que está X lugares más adelante en el alfabeto así si $X=5$ y se encuentra con una **A** codificado queda en **F** lo único que se necesita hacer para desencriptarlo, conociendo la clave, es recorrer el texto e ir cambiando cada letra que aparece por la letra que está X lugares antes en el alfabeto.*

Origen	A	B	C	D	E	F	G	H	I	J	K	L	M	N	N	O	P	Q	R	S	T	U	W	X	Y	Z	
Destino	F	G	H	I	J	K	L	M	N	N	O	P	Q	R	S	T	U	W	X	Y	Z		A	B	C	D	E

¿ Cómo se envía la clave si el medio de comunicación no es seguro ? La respuesta está en los algoritmos de encriptación de clave pública. Con ellos no es necesario disponer de un canal seguro.

2.1.3.2.2 **Criptografía asimétrica o de clave pública**

Cada persona (o computadora) dispone de 2 claves (complementarias una de la otra). La primera: clave privada es conocida sólo por él y la utilizará para desencriptar los mensajes recibidos. La segunda: clave pública, es publicada por el propietario para que sea conocida por todos. Esa clave pública es la que deberá emplear cualquier persona que desee enviarle un mensaje encriptado al propietario de ambas claves.

Ambas claves de un mismo usuario están relacionadas matemáticamente, pero es casi imposible calcular la clave privada a partir de la pública, aún conociendo el algoritmo empleado para construir las.

Para encriptar el mensaje, el remitente utiliza la clave pública del destinatario, de tal manera que sólo el destinatario pueda desencriptarlo utilizando su clave privada.

EJEMPLO: El algoritmo de transposición modificado

*En este algoritmo (aun más inseguro que el anterior) de clave pública, las dos etapas (encriptación y desencriptación) son iguales a la de encriptación en el algoritmo del Cesar, pero la clave que se utiliza para desencriptar es $Y+X=0 \pmod{28}$, donde el modulo en base $N \pmod{N}$ es el resto de su división entera por ese número, por ejemplo: $8 \pmod{5}=3$ porque el resto de dividir 8 entre 5 es $3(8=5 * 1 +3)$.*

Así al aplicar ambas etapas, se da toda la vuelta al abecedario y se vuelve a la posición original. Un algoritmo muy similar, en sus bases matemáticas a este, es el de RSA (por las iniciales de sus inventores Rivest, Shamir y Aldeman) que ha demostrado ser de gran seguridad. En forma simplificada, se basa en la aritmética de módulos y en la descomposición en factores primos. Pero en vez de utilizar a la suma modulo N y su neutro el 0, utiliza la multiplicación y su neutro el 1

*Este algoritmo, emplea 2 números D y E que satisfacen la relación: $D * E \pmod{N}=1$ que indica que son inversos en el producto respecto al módulo N)*

Los valores D y E son las claves privada y Pública respectivamente que se emplean en el algoritmo RSA para encriptar texto

El texto T se transforma (encripta) en el texto C con la siguiente ecuación: $C = TE \pmod{N}$

E/ texto C se desencripta obteniendo el texto original T con la ecuación: $T = CD \pmod{N}$.

El uso de la criptografía como técnica para garantizar la confidencialidad no está reglamentada en los decretos que se analizan, y es un aspecto que a nuestro juicio debería analizarse en profundidad ya que puede involucrar consideraciones de Defensa Nacional. Por ejemplo, en Estados Unidos se limita el uso y exportación de software de encriptación de alta Seguridad, aunque en Internet se pueden conseguir los algoritmos de clave pública de uso estándar.

Un ejemplo de tales consideraciones sería el caso de extravío de la clave privada utilizada para encriptar un importante documento legal, comercial o público. En ese caso sería imposible volver a leer dicho documento. Ciertas técnicas de encriptación permiten recrear la clave privada a partir de la pública pero en ese caso: *¿ confiarían los usuarios en ese sistema criptográfico*

sabiendo que se puede calcular su clave privada a partir de la pública ?

Sin embargo, el uso de la criptografía con fines de autenticación de documentos y como firma digital no involucran tales riesgos y es la solución utilizada para las comunicaciones electrónicas.

2.1.3.3 CRIPTOGRAFÍA Y FIRMA DIGITAL

La criptografía puede emplearse también para estampar una firma digital en un documento a ser enviado, así como para verificar si el documento recibido “es copia fiel del original”.

2.1.3.3.1 La función “Resumen” (“Hash function”)

Se puede firmar un texto o una porción del mismo. La porción del mismo que se firma es la que se denomina “mensaje”.

Además del mencionado par de claves (pública/privada) se requiere el uso de una función o algoritmo conocida como “Hash”. Este algoritmo lee el mensaje que se desea firmar, lo procesa y genera una representación comprimida del mensaje. Ese resultado se corresponde de forma prácticamente biunívoca con el texto; de manera tal que si se cambia un sólo carácter del mensaje original, el resultado del resumen es distinto. Puede pensarse en esta función como la “huella digital” de un texto: es información comprimida y representa al texto.

La longitud del resultado del Hash es estándar y generalmente mucho más pequeña que el mensaje original. La finalidad del uso de estas funciones es la de generar un resumen del mensaje para aumentar la eficiencia del software que firma digitalmente, manteniendo una elevadísima correlación con el mensaje original.

EJEMPLO: Suma Módulo N

Se parte el mensaje en pedazos de n bits donde $N=2^n$. Se interpreta esas cadenas como números binarios enteros, se suman y luego se le aplica el módulo N .

2.1.3.3.2 El proceso de firmar (una conexión indivisible)

El usuario selecciona la porción del texto que desea firmar y le aplica la función Hash. Y luego encripta ese valor con su clave privada. Esta firma digital, por tanto es un dato que puede ser descifrado solamente con la clave pública del firmante.

El mensaje se envía y/o almacena junto con la firma digital o bien en forma separada, aunque sólo tiene sentido cuando la firma está enlazada con el mensaje de alguna manera. La firma no tiene utilidad si se separa permanentemente del mensaje.

No debe pensarse en la firma digital como en una digitalización de la firma escrita, sino mas bien **como una conexión lógica e indivisible entre 2 informaciones** (el mensaje y el propietario

de las claves pública y privada). Haciendo una analogía con la firma sobre papel, ningún escribano público aceptaría una firma que ha sido recortada y pegada en un contrato, aún cuando el corte parezca ser igual en ambos trozos.

Quien establece esa **conexión** es el propietario de ambas claves al aplicar la función Hash al mensaje y luego encriptar el resultado con su clave secreta! Por lo expuesto, queda claro que una firma digital es distinta de una firma electrónica.

2.1.3.3 Verificación de la firma digital

Una vez recibido el mensaje, el receptor calcula usando la misma función de Hash que el remitente, un nuevo resultado Hash sobre el mensaje recibido (llamémosle H2).

Luego descripta la firma digital empleando la clave pública del remitente. El resultado debe ser el mismo que se obtuvo con el Hash en el paso previo (H2).

Dado que sólo una clave pública descripta algo encriptado con una clave privada, la verificación de la firma implica:

- 1. el firmante es efectivamente quien dice ser el documento, ya que sólo el conoce su clave privada y por lo tanto sólo el pudo encriptar con su clave privada; y*
- 2. si el Hash aplicado al texto recibido coincide con el de la firma, el texto "es copia fiel del original"*

Como se ve aquí, el proceso de firmar digitalmente no implica restricciones acerca del nivel de seguridad en la encriptación, dado que el mensaje es legible por todos. El uso de la criptografía es sólo en lo que respecta al resultado del Hash para formar la firma digital.

2.1.4 Software Libre y la Administración Pública

Un poco de Historia

En un principio, como las computadoras eran muy caras, no se ponía demasiado atención en los programas, y por eso la gran mayoría de los mismos, era distribuidos libremente entre todos los que quisieran estudiar su código, así por ejemplo todas las universidades podían hacer sus cursos sobre Sistemas Operativos estudiando directamente de los fuentes de UNIX.

Con el tiempo, las empresas empezaron a darse cuenta que la venta de programas podía ser un buen negocio, y fueron cerrando sus programas, haciendo que los usuarios en realidad no fueran propietarios del software que corre en sus máquinas, sino que solo tenían (y tienen) una licencia de uso, sin poder copiar ese programa ni venderle esa licencia a alguien más.

En respuesta a eso, Richard Stallman, un programador de EEUU, creo el proyecto GNU, cuya finalidad es crear desde cero un Sistema operativo completo, compatible con Unix, pero cuyos componentes fueran exclusivamente Software Libre (término del que es creador)

Pero, ¿Qué es software Libre?

El software libre es aquel que trata de brindarle mayores libertades a su usuario, que las brindadas por el Software Propietario. En las palabras de Stallman [15], como se expresa en la FSF:

"Software Libre" se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. De modo más preciso, se refiere a cuatro libertades de los usuarios del software:

- *La libertad de usar el programa, con cualquier propósito (libertad 0).*
- *La libertad de estudiar cómo funciona el programa, y adaptarlo a tus necesidades (libertad 1). El acceso al código fuente es una condición previa para esto.*
- *La libertad de distribuir copias, con lo que puedes ayudar a tu vecino (libertad 2).*
- *La libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie. (libertad 3). El acceso al código fuente es un requisito previo para esto.*

¿Que ventajas presenta el uso del software libre en general?

El hecho que se utilice software libera a los usuarios de los proveedores, pudiendo mejorar ellos mismos el programa que utilizan o pagarle a la persona que ellos elijan, para que lo mejoren por ellos, para adecuarlo al funcionamiento de su organización.

Por otra parte, uno es libre de arreglar las fallas que pudiera tener el programa que utiliza, sin depender para eso del proveedor; esto es particularmente cuando se trata de una falla de seguridad que puede dejar expuesta la información del usuario a otros.

Se puede además instalar con una solo copia instalar el producto en cuantas máquinas quiera, y hacer tantas copias como quiera.

Aspectos puntuales:

- **Sobre seguridad:** En términos más puntuales respecto de la seguridad del software en sí, es bien sabido que el software (propietario o libre) contiene errores de programación o "bugs" (en la jerga informática) en sus líneas de código. Pero también es público y notorio que los bugs en el software libre son menos, y se reparan mucho mas rápidamente, que en el software propietario. No en vano numerosas organismos públicos responsables por la seguridad informática de los sistemas estatales en países desarrollados prescriben el uso de software libre a iguales condiciones de seguridad y eficiencia.
- **Respecto a garantía:** Si bien en el Software Libre los programas se entregan sin garantías, mientras que las garantías del software propietario, en la amplísima mayoría de los casos, están limitadas a la reposición del medio de almacenamiento si este fuera defectuoso, pero en ningún caso se prevén compensaciones por daños directos o indirectos, lucro cesante, etc. Es decir, si como consecuencia de un bug de seguridad en alguno de los productos usados , no oportunamente reparado por el proveedor , un atacante comprometiera sistemas cruciales para el Estado: ¿que garantías, reparaciones y compensaciones proporcionaría la empresa de acuerdo con esas condiciones de licenciamiento? Así, se parte de situaciones similares en ambos

mundos. En la práctica hay sí una garantía, el código que se tiene, es el que se ejecuta.

- **Sobre la propiedad intelectual:** A veces se asocia el Software Libre con actividades que violentan la propiedad intelectual, como las englobadas en el, mal utilizado, termino "piratería" (ya que no hay barcos ni secuestros en esos casos) , sin embargo, el software libre se protege precisamente por medio de la propiedad intelectual. Además, por estar el código disponible, es muy fácil detectar si un proyecto de SL tomó código de otro proyecto, y sin embargo lo opuesto es mucho más fácil (se consigue fácilmente el código) y encima, después, el damnificado no puede auditar el código, porque se entrega el producto ya compilado. Así, en realidad, el SL, más vulnerable a estos problemas.

Las cuestiones de propiedad intelectual están fuera del ámbito de discusión, pues se encuentran amparadas por leyes específicas. El modelo de software libre no implica en modo alguno desconocer estas leyes y de hecho, la amplísima mayoría del software libre está amparado por el copyright. En realidad, la sola inclusión de esta cuestión entre las observaciones más comunes, demuestra el desconocimiento del marco legal en que se desenvuelve el software libre. La incorporación de propiedad intelectual ajena en obras que luego se atribuyen como propias no es una práctica de la que se tenga registro en la comunidad del software libre; si lo es, lamentablemente, en el terreno del software propietario.

- **Costo:** En general se supone que estos productos DEBEN ser gratis, pudiéndose llegar a conclusiones equívocas sobre el monto de los ahorros para el Estado. Si bien son gratis en la mayoría de los casos; esta es una suposición falsa, en principio la gratuidad y la libertad son conceptos ortogonales: hay software propietario y oneroso (por ejemplo, MS Office), software propietario y gratuito (MS Internet Explorer), software libre y oneroso (distribuciones RedHat, SuSE, etc. del sistema GNU/Linux), software libre y gratuito (Apache, OpenOffice, Mozilla), y aun software que se licencia bajo diferentes modalidades (MySQL).

Porqué Software Libre en el Estado?

Es preciso dejar en claro, como lo hace el Dr Edgar Villanueva en [22], que las ventajas prácticas y económicas del Software Libre, son solo una parte del asunto cuando el "usuario" del que se habla es el Estado. Estas ventajas son, en todo caso, un valor agregado marginal, no más que eso. Las razones principales se vinculan a las garantías básicas de un Estado democrático de derecho, como son:

- ***Libre acceso del ciudadano a la información pública.***
- ***Perennidad de los datos públicos.***
- ***Seguridad del Estado y de los ciudadanos.***

Para garantizar el libre acceso de los ciudadanos a la información pública, resulta indispensable que la codificación de los datos no esté ligada a un único proveedor. El uso de formatos estándar y abiertos permite garantizar este libre acceso, logrando si fuera necesario la creación de software libre compatible.

Para garantizar la perennidad de los datos públicos, es indispensable que la utilización y el mantenimiento del software no dependan de la buena voluntad de los proveedores, mucho menos de las condiciones impuestas por éstos, cuando se da una situación monopólica. **Por ello el Estado necesita sistemas cuya evolución pueda ser garantizada gracias a la disponibilidad del código fuente y la posibilidad de modificar ésta.**

Para garantizar la seguridad del Estado o la seguridad nacional, resulta indispensable contar con sistemas desprovistos de elementos que permitan el control a distancia o la transmisión

no deseada de información a terceros. Por lo tanto, se requieren sistemas cuyo código fuente sea libremente accesible al público para permitir su examen por el propio Estado, los ciudadanos, y un gran número de expertos independientes en el mundo. El software Libre aporta mayor seguridad, **pues el conocimiento del código fuente minimiza el problema de programas con código espía**, o malicioso, cuyo número es creciente.

Asimismo, se refuerza la seguridad de los ciudadanos, tanto en su condición de titulares legítimos de la información manejada por el estado, como en su condición de consumidores. En este último caso, no se puede negar, que, en su accionar, el estado muestra pautas, también, de comportamiento a los ciudadanos, además del hecho que si el estado consume Software Libre, permite el surgimiento de una **industria local** de servicios y de una oferta extensa de software libre, desprovisto de potencial **código espía** susceptible de poner en riesgo la vida privada y las libertades individuales de los ciudadanos.

Lo que es necesario comprender, es que el software para ser aceptable para el Estado, no basta con que sea técnicamente suficiente para llevar a cabo una tarea específica, sino que debe dar herramientas, con las cuales el Estado pueda garantizar al ciudadano el procesamiento adecuado de sus datos, velando por su integridad, confidencialidad y accesibilidad a lo largo del tiempo, porque son aspectos muy críticos para su normal desempeño. Y en este aspecto, la licencia del Software es una herramienta fundamental.

Tres aspectos deben tenerse en cuenta al momento de juzgar la implantación de una medida tecnológica en el estado:

- Por su naturaleza misma, cada decisión tomada en el seno del estado, influye en la vida del ciudadano corriente.
- La tecnología de información y comunicaciones tiene un impacto significativo en la calidad de vida de los ciudadanos (sin que por ello sea siempre positivo o de efecto neutro).
- En su funcionamiento, el estado debe velar siempre por ciertos valores básicos, que son fundamentales en cualquier nación democrática.

Además el Software Libre **estimula** la competencia. ¿Por qué esta afirmación? Por un lado, alienta a generar oferta de software con mejores condiciones de usabilidad, y a optimizar trabajos ya establecidos, en un modelo de mejora constante; y en la contra-cara, indirectamente, baja también la barrera para entrar al mercado, permitiendo la creación de nuevos emprendimientos nacionales, en toda una gama de opciones, desde el desarrollar una aplicación desde cero, ayudada por un menor costo de las herramientas de desarrollo (incluyendo lenguajes de programación, entornos integrados de desarrollo, herramientas de gestión de proyecto, etc.) hasta el dar soporte a aplicaciones ya existentes, pasando por casos significativos como la implantación (o adaptación) de un sistema a una realidad específica.

Por otro lado, el aspecto central de la competitividad es la oportunidad de proporcionar al consumidor mejores opciones. Ahora bien, es imposible desconocer que el marketing no juega un papel neutral en las decisiones de compra. Esta influencia queda en buena medida mitigada por el SL, pues la elección dentro del marco propuesto recae en el ***mérito técnico*** del producto y no en el esfuerzo de comercialización del productor; en este sentido, la competitividad se acentúa, pues **el más pequeño productor de software puede competir en un pie de igualdad con la más poderosa de las corporaciones.**

Adicionalmente, incluso al mejorar software libre, ya creado, el estado le brinda al pueblo un servicio, esas modificaciones pueden ser utilizadas en otros lugares para mejorar el desempeño de los mismos.

Porqué un SGEE hecho Software Libre?

Restringiendo un poco lo dicho en el punto anterior y teniendo en cuenta el hecho que está regulada la necesidad de ir pasando a formas electrónicas de manejo de expedientes en toda la administración pública; el hecho de contar con un SGEE hecho sobre software libre, plantea las siguientes ventajas:

1. Bajo costo de instalación inicial (particularmente importante si este proyecto se extiende a otras dependencias del Estado) por conceptos de propiedad intelectual.
2. No exige costos extra en licencias en el cliente, ni en el servidor.
3. Trabaja con interfaces bien definidas, lo que permite que sea posible la inter operación con otros sistemas, que se desarrollen más adelante.
4. Permite que sea más barato la instalación del sistema en más de una dependencia del estado, permitiendo el aprovechamiento del "know how", capacitación y infraestructura. Economizando de esta forma en estos items.
5. Permite realimentación entre los lugares que lo implementen, para lograr el mejoramiento del sistema.
6. Facilita la entrada de otras dependencias a esta tecnología, posibilitando una arquitectura uniforme en todo el estado, reduciendo aún más los costos de implantación, mantenimiento y desarrollo del mismo.
7. Dada la sensibilidad de los datos que se manejan, permite un alto grado de auditoría, aumentando transparencia en el estado; a distintos niveles:
 - **Sobre el código:** Permite verificar la seguridad de los datos.
 - **Sobre el desempeño de la dependencia:** por medio de estadísticas, permite estudiar la eficiencia de Unidades Organizativas y funcionarios.
8. No dependencia de un proveedor (a ningún nivel). De importancia, teniendo en cuenta la necesidad de continuidad en el tiempo de los datos que estos sistemas mantienen.
9. En la Seguridad, permite ir variando con el tiempo proveedores y algoritmos para acompañar el paso del tiempo y los cambios que este traiga.
10. Permite el mantenimiento de la solución a bajo costo, haciendo más fácil la continuidad en el tiempo de la misma.

2.2 Requerimientos del sistema.

Introducción:

El Propósito de este documento es el de servir como base de acuerdo entre el Departamento de Informática del Ministerio de Relaciones Exteriores y el equipo de desarrollo del software demandado, especificando los aspectos relativos a funcionalidad, interfaces externas, performance, atributos y restricciones de diseño en la implementación. Además, funcionará como base de referencia entre los integrantes del equipo de desarrollo al especificar los objetivos a lograr.

Sistema a Construir:

El sistema a realizar es un Sistema de Gestión de Expediente Electrónico (SGEE) parametrizable, que responda a las necesidades de los organismos públicos de administración para automatizar y controlar los procesos administrativos existentes como una forma de incrementar su eficacia y eficiencia. Desde un punto de vista técnico, un S.G.E.E. es un Sistema de Workflow centrado en manejo de documentos, donde se tienen requerimientos especiales en cuanto a seguridad.

Inicialmente el sistema propuesto deberá funcionar en una intranet dentro de la organización donde se instale pero se debe contemplar la posibilidad de la inclusión de un módulo que posibilite interactuar (enviar y recibir expedientes) con un sistema similar instalado en una red remota.

Se debe contemplar la posibilidad de extensión del Sistema para que contemple acceso a la información en base a Web dinámica con el objetivo de:

- Extender el uso del sistema a una organización geográficamente distribuida.
- Proveer acceso a la información a través de la red Internet.

Ambos objetivos implican contemplar la futura inclusión de un módulo que realice las siguientes funciones:

- Definición y manejo de un protocolo adecuado de comunicación
- Encriptado de la información en tránsito
- Control de acceso a la información.

El citado decreto hace la distinción entre “firma electrónica” y “firma digital” entendiéndose por firma electrónica “el resultado de obtener por medio de mecanismos o dispositivos un patrón que asocie biunívocamente a un individuo y su voluntad de firmar”, y por firma digital “un patrón creado mediante criptografía” (artículos 18 y 19, decreto 65/998). El sistema logrará implementar, mediante un sistema de contraseñas, el mecanismo de firma electrónica y, si los plazos para la realización del proyecto lo permiten, se intentará implementar un esquema de firma digital. En todo caso, el diseño del sistema tendrá como objetivo central la inclusión de esta característica.

Usuarios:

Este software tendrá cinco tipos de usuario, con perfiles bien definidos:

Parametrizador.

Es la persona/s encargadas de personalizar el sistema a las necesidades de cierta institución, por las características del mismo, es necesario que tenga una formación en Análisis de Sistemas, ya que es el encargado de plasmar en el Sistema toda la estructura de la institución.

Personal de Mantenimiento:

Son los encargados de mantener la parte del servidor del sistema, es por eso que se trata de un usuario de perfil netamente técnico, encargado de labores de respaldo y replicación de datos, mantenimiento del servidor en el que corre la aplicación, así como mantenimiento de las tablas del sistema. Es por eso que se recomienda conocimientos en administración de servidores y de red. Es posible que se solape con el rol de parametrizador.

Encargados de personal:

Son los encargados de mantener al día la información de cargos del sistema, es por eso una labor netamente administrativa, requiriéndose una formación mínima en ofimática y cierto entrenamiento en el uso de la parte de asignación de cargos del sistema.

Funcionarios en general:

Son los encargados del manejo en sí de los expedientes, por lo tanto además de una preparación en el uso del sistema, es recomendable cierto manejo de herramientas de ofimática, por ejemplo en suites de oficina, como puede ser OpenOffice.org (adecuada al enfoque libre de este proyecto, enmarcada en el fin superior de abaratamiento de costos en la función pública) u otras como Microsoft Office o Lotus Notes.

Público en general:

Son los interesados últimos en los expedientes, dadas sus características heterogéneas, no es posible hacer suposiciones sobre su perfil y, por tanto, es recomendable e incluso necesario que su interacción con el Sistema sea a través de los funcionarios.

2.2.1 Requerimientos Funcionales.

Se pasa a detallar a continuación las funcionalidades que el sistema debe cumplir. Estas se basan en lo especificado en el decreto 65/998. Debiendo contemplar, mediante un diseño adecuado del sistema la incorporación de las características nombradas a continuación.

Esta sección tratará primeramente los requerimientos de administración del sistema necesarios para su parametrización a la realidad de la organización donde funcione, para posteriormente tratar las características deseadas en cuanto a su funcionamiento a nivel de usuario.

Administración del Sistema

Se debe brindar un módulo que se encargue de parametrizar y administrar el sistema, dentro de la organización; para ello será necesario capacitar y responsabilizar a un "administrador de Sistema". Dicha persona necesitará conocimientos básicos de informática. Este subsistema brindará las siguientes funcionalidades al "administrador":

Herramienta de definición de organigrama

Mediante interfaz gráfica se permitirá introducir y modificar el esquema de dependencias de la organización, estableciendo las relaciones jerárquicas dentro de la misma.

Herramienta de Gestión de Cargos

Mediante interfaz gráfica se permitirá la definición, modificación y eliminación de cargos existentes dentro de la organización, estableciendo su posición dentro del organigrama, así como los niveles correspondientes de privilegio en cuanto al acceso a la información.

Herramienta de Gestión de funcionarios

Permitirá, mediante interfaz gráfica, el ingreso y modificación de los datos básicos y cargos de las personas que son asignadas por la organización para el manejo del sistema; luego se las relacionas con las dependencias creadas en el organigrama. Estas personas serán las responsables de realizar las distintas acciones sobre expedientes. Las acciones válidas asociadas a cada persona serán, por tanto, las derivadas del cargo de la misma.

Herramienta de definición de procedimientos administrativos estándar de expedientes (Workflow).

El Workflow del expediente es el conjunto y orden de las dependencias internas a la organización definidas en su organigrama, por donde el expediente debe pasar. En cada punto del recorrido, que llamaremos etapas, se podrán definir entre otros parámetros, la finalidad de esa etapa y el acceso a la información incluida en el expediente hasta ese momento, según los cargos de la dependencia. Esta herramienta permitirá la definición de caminos alternativos, en el caso que la duración de la etapa sobrepase un límite establecido. Se podrán definir, además, alarmas, estableciendo el tiempo, que debe estar el expediente en una cierta dependencia, para que se lance la misma, datos que debe incluir y el destinatario de la misma (por ejemplo: el encargado de la misma, el jefe de esa dependencia o incluso el jefe de la institución).

Estos límites se podrán fijar con distintos alcances, en forma general a todo el sistema, a todas las etapas de un grupo de tipos de expedientes, o a un cierto conjunto de etapas dentro de un tipo de expediente dado.

El orden de los pasajes estará prefijado, el mismo no será taxativo y el usuario, dependiendo de su cargo, podrá realizar envíos a dependencias diferentes a las preestablecidas. El registro de estos desvíos será luego utilizado para comparar con el recorrido previsto para el trámite.

Herramienta de definición de características del expediente.

En la misma se definen elementos morfológicos y de presentación de los datos del expediente, como pueden ser datos que se despliegan en la carátula del mismo, y el formato y distribución de los mismos en la impresión. Estos elementos podrán ser generales a todos los expedientes del sistema o específicos a un cierto tipo de ellos.

Herramienta de gestión de fechas.

El administrador del sistema deberá ser capaz de definir y gestionar las fechas utilizadas por el sistema para reflejar posibles corrimientos de días feriados y demás contingencias por el estilo.

Características funcionales requeridas del Sistema en la parte de Usuario

Inicio de expediente

Un expediente se podrá iniciar en cualquier dependencia interna en la organización, mediante opción en la pantalla de trabajo del operador con el cargo correspondiente para tal acción. El Sistema, después de verificar la validez de la información introducida en la carátula del expediente electrónico que brindará el sistema, otorgará un número identificador correlativo anual único a toda la organización. Posteriormente, se deberá elegir una ruta estándar dada por el sistema, pudiéndose entonces trabajar o dar el pase del expediente.

Opcionalmente, se debe otorgar la funcionalidad de generar un expediente adjuntando la imagen electrónica, mediante el scaneo de página completa, de un documento escrito presentado

por un interesado externo a la organización. El funcionario receptor podrá entonces iniciar un expediente por el procedimiento descrito arriba donde además adjuntará esta imagen.

El diseño del sistema debe prever una futura ampliación del sistema que permita el inicio de un expediente por medio de una petición originada por la recepción de un correo electrónico enviado por un interesado que cumpla los parámetros técnicos que se definan.

Manejo de expedientes

El sistema deberá brindar las siguientes funcionalidades:

- Agregar actuación, si el cargo del operario lo permite.
- Adjuntar documento en formato electrónico. Esto puede requerir su previa digitalización.
- Consultar las actuaciones y documentación adjuntada al expediente. Se debe garantizar la no modificación de esta información.
- Una vez finalizado el trabajo en la dependencia, el jefe de la misma debe poder realizar el pase del expediente a la dependencia que considere adecuada, mas allá del Workflow elegido por defecto asociado al expediente en su inicio.
- El sistema debe mantener en forma automática la información sobre entrada y salida del expediente de la dependencia.
- La impresión parcial o total del mismo.
- Consultas de expedientes.

El sistema debe permitir realizar las siguientes consultas sobre un expediente y su estado:

- Dado un nro. de expediente, saber su estado, en que dependencia se encuentra, tiempo de permanencia en la dependencia actual y tiempo de permanencia en el sistema, fecha de comienzo y fin (en caso de tenerla) del mismo, si está en transito o ya fue terminado.
- Dada una persona, saber sobre que expedientes está actuando (en el caso que sea un funcionario) o cuales son los expedientes en los que es referida (en el caso que sea un usuario).
- Mostrar una lista de expedientes lógicamente relacionados en cuanto al asunto que tratan (búsqueda por tema).
- Mostrar la lista de expedientes que pasaron por una dependencia en un lapso definido de tiempo. Se deberá mostrar una información resumida en este caso.

Unión de Expedientes

El sistema debe brindar la funcionalidad de unir expedientes al operario con el cargo definido para realizar esta acción. Para realizar tal acción, el operario introducirá los números de los expedientes involucrados (del adjuntado y al cual se adjunta) y motivo de la unión manejándose en forma automática la fecha de la unión y la actualización de las carátulas electrónicas involucradas. A partir de ese momento, el sistema debe manejar al expediente sobreviviente de igual manera que a cualquier otro expediente.

Desglose de Expedientes

El sistema debe brindar la funcionalidad de desglosar expedientes previamente unidos al operario con el cargo definido para realizar esta acción. Para realizar tal acción, el operario introducirá el número del expediente con adjuntos y cual de los adjuntos se desglosará y motivo del desglose, manejándose en forma automática la verificación de la fecha de la acción, si los expedientes forman parte de una unión previa y la actualización de las carátulas electrónicas involucradas. El operador especificará un workflow por defecto al expediente que estaba adjuntado. A partir de ese momento, el sistema debe manejar a los expedientes resultantes de la manera usual.

Establecimiento de referencia

Dado un expediente en curso y uno ya resuelto debe ser posible establecer una referencia del primero al último.

Pases de expedientes

Una vez concluida la actuación administrativa en la dependencia, el operario actuante o el jefe de la misma darán el pase del expediente a la dependencia por defecto marcado para el mismo en el primer caso, o a la que se considere conveniente en el segundo. El sistema deberá informar el caso de que un expediente no se encuentre en su workflow predeterminado al momento del pase. Si es así, solo el jefe de la dependencia podrá realizar el movimiento. El sistema debe ser capaz de derivar el expediente de manera automática a la dependencia elegida.

Gestión de Archivo

Un expediente puede ser enviado al archivo solamente cuando existe una resolución firme a su respecto. El archivo de un expediente significa la finalización de su vida administrativa y su baja como expediente "activo" del sistema. A partir de ese momento solo podrá ser objeto de consultas por parte del usuario con el nivel de seguridad adecuado para tal acción. La acción de archivar un expediente puede ser realizada únicamente aquellas dependencias autorizadas a la acción de "Archivar". El operario que realice la acción debe tener a su vez el cargo adecuado.

Seguridad

El sistema deberá chequear de identidad del usuario al inicio de la sesión de trabajo con el sistema, mediante el ingreso de una contraseña personal. Una vez realizado esto el sistema deberá presentar las acciones accesibles a la persona dado su nivel de privilegio.

El sistema debe garantizar, por el uso de medios criptográficos o por el diseño de su arquitectura la confidencialidad de los expedientes en su tránsito en la intranet de la organización, así también como la inalterabilidad de las actuaciones y documentos adjuntados previamente. El sistema debe registrar en forma automática al operario actuante en cada procedimiento administrativo que se sustancie.

Auditoria y control de gestión

El jefe de cada dependencia de la organización debe ser capaz de consultar todo expediente en curso o archivados en su dependencia así también los que lo estén en dependencias subordinadas. El sistema le deberá proveer información sobre

- Las actuaciones y su cantidad realizadas por un funcionario determinado bajo su mando.
- Tiempos de permanencia promedio de expedientes en la dependencia en un lapso dado de tiempo, así como la cantidad de actuaciones realizadas.

- Tiempos promedios de actuación para cada funcionario a su cargo.

2.2.2 Requerimientos No Funcionales

Se detallan en esta área restricciones que debe cumplir el Sistema entregado, pero que, sin embargo, no hacen a las funcionalidades del mismo, incluyendo entre otros aspectos concernientes al uso del sistema, a la portabilidad y licencia del mismo, etc.

Portabilidad.

Se requiere un sistema que sea capaz de correr en plataformas distintas (como puede ser el caso de UNIX o Windows). En caso de depender de otros componentes de software, estos deberán contar con características similares.

Licencia

El sistema entregado deberá contar con una licencia libre y de código abierto. En caso que se dependa de otros componentes de software, estos deberán contar con una licencia similar.

Extensibilidad

Se deberá brindar elementos que permitan una fácil extensión del mismo, junto con documentación al respecto.

Documentación

- La documentación del sistema entregado deberá contar por lo menos de tres partes:
- Manual de Sistema (debiendo incluir ésta lo relativo a la extensibilidad).
- Manual de Administración.
- Manual de Usuario final

Apego a los estándares

Se debe tener en cuenta la reglamentación oficial vigente (decretos 500/991 y 65/998)

SGEE parametrizable

Se exige que el sistema a desarrollar sea adaptable por medio de un mecanismo de parametrización, a organizaciones públicas cuyo funcionamiento administrativo se rija por el decreto 500/91. Para tal fin el sistema brindará herramientas de definición de sus elementos constitutivos (lo cual se trata en la sección 0) que en su conjunto deben lograr este objetivo.

Acceso Multiusuario

El sistema debe correr en una red de área local (LAN), con un pudiendo servir simultáneamente a un mínimo de 50 clientes.

Seguridad

Debe ser posible definir distintos niveles de acceso a la información que maneja el sistema. Además de deberá poder verificar la identidad de las personas actuantes en cada expediente.

Restricciones

Detalle de las Restricciones del Sistema que será construido, una restricción es cualquier decisión que fue impuesta y debe cumplirse, ejemplos son el lenguaje de programación, proceso de software a seguir, herramientas para el desarrollo, metodología para el diseño, componentes rehusados, librerías, clases, etc.

Restricciones de Performance

Cada interacción individual entre el usuario y el sistema de Workflow, en un ambiente de Red de Área Local de 10 Megabits por segundo, con una carga menor o igual a 40 usuarios concurrentes, deben ser resueltas en un lapso de 5 segundos en el 80% de los casos. Nunca deben exceder los 15 segundos, a menos que la conexión de red se encuentre fuera de servicio.

Componentes reusados

Solo se podrán reutilizar componentes que caigan en alguna de las siguientes características:

- Con propiedad del organismo contratante.
- Con propiedad del equipo de desarrollo.
- Con licencia libre.

Restricciones de hardware

El sistema debe ser capaz de cumplir las Restricciones de Performance anteriormente descritas, en máquinas con las siguiente especificaciones:

En el cliente:

Procesador Pentium 150 Mhz.
32 Mb de memoria RAM.

En el servidor:

Procesador Pentium II 300 MHz.
128 Mb de memoria Ram.
4 Gb de disco.

Restricciones en las herramientas de desarrollo

Para el desarrollo del sistema en cuestión se podrán utilizar solamente las herramientas para las que el organismo contratante tiene licencias o en su defecto, las que el equipo de desarrollo considere apropiadas, siempre y cuando tengan licencias libres.

Interfaces

Se detallan a continuación restricciones en las interfaces que debe proveer la aplicación.

Interfaces de Usuario

Las interfaces de usuario deben ser gráficas o de comandos, o una combinación de las mismas.

Interfaces de Software

El sistema debe interactuar con un Sistema manejador de Bases de Datos relacional. Además, el sistema deberá tener una interfaz definida que le permita su comunicación con programas de codificación criptográfica y firma digital.

Interfaces de Comunicación

La comunicación entre el/los servidores y los clientes será hecha utilizando el protocolo de comunicación TCP/IP.

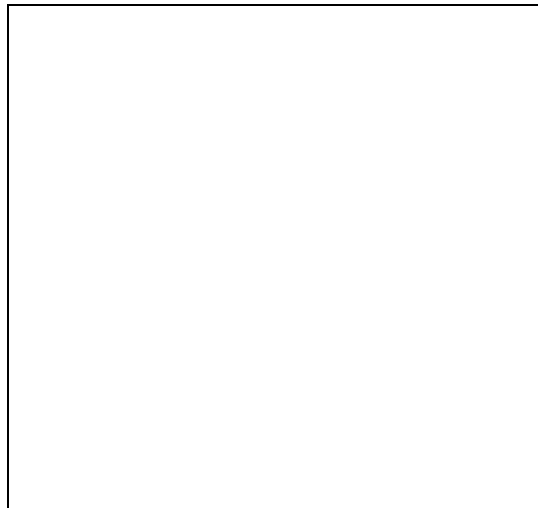
3 DESCRIPCIÓN DEL SISTEMA BASE.

Paflow es un proyecto de software libre patrocinado por CNIPA (Centro Nacional de Informática para la Administración Pública) y la escuela superiora Santa Ana de Pisa, para la experimentación de un núcleo de seguimiento de documentos mínimo y su interoperabilidad con sistemas similares en la Administración Pública Italiana. Está construido enteramente sobre Web e integra, según una arquitectura modular, un motor de workflow (Openflow [18]), un servidor de aplicaciones (Zope [30]), un manejador de documentos y una base de datos relacional (postgreSQL [20]). Ha sido concebido para permitir a la reparticiones de la administración pública el seguimiento de documentos de acuerdo a la normativa DPR 428/98 [2] del gobierno Italiano. La versión con la cual se ha desarrollado Yará parte de la versión correspondiente al 23-03-03 de Paflow [16]. Las restricciones mencionadas anteriormente sobre el lenguaje de programación a utilizar y las prestaciones de servidor de la aplicación fueron relajadas posteriormente de común acuerdo con el cliente del producto.

Descripción de la Arquitectura

Paflow tiene una arquitectura modular en que cada componente logra un conjunto coherente de funciones según un diseño arquitectónico de tres capas:

- Una capa de presentación (interfases de la aplicación Web); una gestión de
- Una capa de manejo lógica de negocio.
- Una capa de investigación, clasificación y almacenamiento de datos.



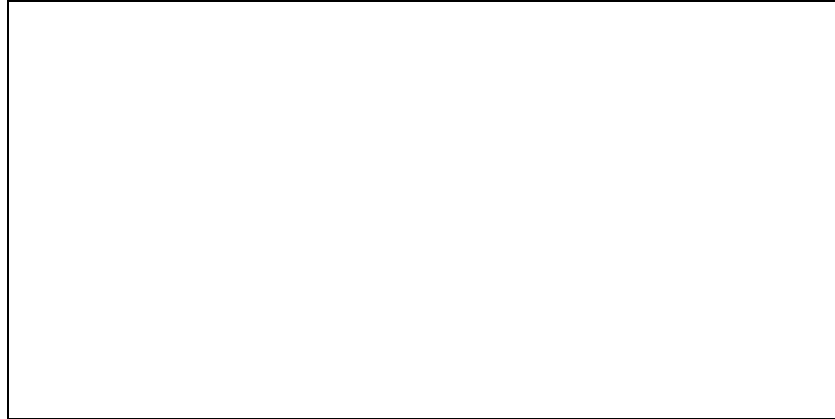
La arquitectura se caracteriza por:

Los módulos se comunican mutuamente mediante interfases estándares (HTTP-CGI, protocolos SMTP-IMAP, SQL).

El corazón Paflow es el servidor de aplicaciones Zope.

Los datos administrados se almacenan sobre una base de datos relacional: PostgreSQL. Paflow puede también configurarse para trabajar con la mayoría de las bases de datos relacionales que soporten SQL99 (Oracle, SQL server vía ODBC, Informix, Sybase, etc.).

La capa de interoperabilidad provee la interfase de conexión de e-mail son provistas por correo Web y un producto de software libre como servidor SMTP-IMAP.



Interacción con el usuario

La interacción con el usuario, el acceso y el uso de Paflow se realizan completamente mediante interfase Web; todas las operaciones que permite el sistema pueden hacerse usando un browser y sobre cualquier plataforma operativa. La interfase ha sido diseñada para ser intuitiva y simple.

Seguridad en el acceso vía Web.

El acceso al sistema puede regularse estableciendo niveles de privilegios y asignándolos a cada usuario o unidades organizativas. La conexión al servidor central puede protegerse usando tecnologías criptográficas y certificados digitales (SSL).

Como se ha dicho anteriormente, Paflow es una aplicación basada en Zope por lo cual saca partido de sus características, en particular de su potente interfaz de administración vía Web.

Funcionalidades.

Las funciones básicas de Paflow permiten la gestión del Registro de Información según el instructivo del AIPA de sobre la gestión de la Información.

El producto permite el registro de la entrada y la salida de documentos en una organización, así como también el registro en un histórico de las diversas versiones de un documento y la cancelación de un registro erróneo. Las operaciones disponibles (creación, modificación, cancelación) son iguales a los que se podría esperar para los registros que se realizan normalmente en papel. Paflow permite el registro automático de mensajes de e-mail. Para la creación de mensajes vía e-mail y su lectura, Paflow integra una sistema de Web mail conectado a un servidor de e-mail con IMAP. **Este módulo no fue encontrado, por lo que no se incluyó en Yará**

Gestión Documentaria

Paflow integra un módulo de gestión documentaria con almacenamiento básico y gestión documentaria que maneja formatos heterogéneos de documentos. Permite la adquisición de imágenes de documentos mediante escáner o archivos. A su vez, los documentos registrados se clasifican en forma jerárquica por temas, permitiéndose además el indexado a texto completo de los mismos. El módulo es capaz indexar, además de archivos de texto, archivos en los principales

formatos: HTML / XML, PDF, Postscript, Microsoft Word(formatos 6.0 / 95,97 & 2000), Excel y Powerpoint.

Interoperabilidad

El módulo de interoperabilidad y gestión de e-mail permite enviar y recibir registros de documentos entre administraciones públicas según las normas de AIPA. Los datos de los registros son transmitidos en formato XML. Además el módulo de interoperabilidad permite el registro automático de los mensajes de salida y entrada trabajado con servidores SMTP e IMAP. Por último, el módulo de interoperabilidad soporta S-MIME V3 (MIME seguro) versión que permite para firmar y codificar los mensajes intercambiados. **Este módulo no fue integrado en Yará, por no tener el código, ni tiempo para implementarlo.**

Workflow de Gestión

Paflow integra el motor de Openflow para administrar automáticamente los procedimientos de asignación de los documentos registrados. El sistema administra directamente los procesos simples de asignación de cada nuevo registro a una persona o a un rol administrativo y permite llevar el registro del estado del documento a cada momento. La definición de roles, el personal y (en general) de la estructura organizativa están constantemente bajo el control del administrador del sistema. Además de las asignaciones simples, es posible explotar las potencialidades de Openflow para definir y administrar procesos administrativos complejos e integrarlos con el sistema de seguimiento de documentos. El proceso implementado en el producto se describe en el punto 3.3.2 de este documento.

3.1 Componentes principales de Paflow

Habiendo brindado una introducción en el punto anterior a la aplicación considerada por el equipo de desarrollo como la mejor opción para la construcción de la aplicación pedida, pasamos a describir los componentes principales de los que hace uso. Comenzamos con el servidor de aplicaciones Zope, el cual constituye la base funcional de Paflow, proseguimos con la Base de Datos que utiliza, PostgreSQL para, posteriormente, describir los productos Zope de los que Paflow hace uso de manera de detallar individualmente la funcionalidad que brindan a Paflow.

3.1.1 Zope

Características Generales

- Se trata de un servidor de aplicaciones para Internet, desarrollado en Python, con amplias facilidades de desarrollo y por el testeado hecho, bastante performante. Página web: <http://www.zope.org/> . Para dar idea de su grado de madurez y seguridad podemos indicar que las siguientes organizaciones hacen uso de esta tecnología :
 - OTAN
 - Viacom
 - SGI (Silicon Graphics) Estados Unidos

(<http://www.zope.org/Resources/ZopePowered>)

Fortalezas

- Extensibilidad: Permite aumentar fácilmente su funcionalidad por medio de Scripts en python (y por ende con Java o C) o perl.

- Uniformidad: Permite tratar de forma unificada varios tipos de objetos, estableciendo de forma conjunta elementos como seguridad y presentación.
- Parametrizabilidad: Por medio de su sistema de templates y su lenguaje DTML, permite establecer plantillas de presentación para todo un sitio o para una cierta parte. Este esquema permite además separar la parte de presentación del sitio, de la parte de mecánica del mismo. Por ejemplo, una plantilla puede ser editada por el programador para darle la mecánica de la misma, y después el diseñador modificarla directamente en un editor común de HTML.
- Organización jerárquica: Este aspecto influye cada parte del sistema. Desde la presentación, la mecánica de la aplicación, la seguridad y el manejo de usuarios. Permite establecer políticas de uso y diseño en forma ordenada. Permite además el delegado de funciones, por ejemplo, ya que se le asigna a cada usuario un cierto conjunto de permisos, en forma selectiva.
- Seguridad: Permite establecer políticas de seguridad, asignando roles a los usuarios, sin existir una diferencia clara entre manejar, implementar o usar una aplicación. De esta forma, permite uniformizar el tema de seguridad, a la vez que deja que el administrador (que es en realidad un usuario como cualquier otro) personalice el esquema a cada aplicación. Además por el esquema jerárquico utilizado permite el delegar poder a distintos niveles. Los usuarios se pueden autenticar de variadas formas, incluyendo entre otras, contra la base de datos del propio Zope, contra la base de usuarios del servidor en que está instalado (Sea UNIX o NT) o contra un servidor LDAP (Que probablemente sea el utilizado en nuestro sistema). Además permite que las conexiones con el servidor sean a través del protocolo SSL.
- InterOperabilidad: Este sistema permite la comunicación de dos formas, a través de plugins hechos en Perl o Python, por ejemplo con bases de datos (Existen por ejemplo servicios de conexión con odbc, MySQL, SQL Server, PostgreSQL, entre otros) o con otras aplicaciones externas a través de XML-RPC. Además el acceso al contenido y la actualización pueden hacerse vía FTP, HTTP o WebDAV.
- Portabilidad: Este Sistema está hecho sobre python y Ansy C, por lo que en cualquier plataforma que cuente con capacidad de procesar ambos lenguajes, es posible correr ZOPE también. Ejemplos MS Windows, Mac OS, Linux.
- Licencia: Cuenta con licencia ZPL.
- Comunidad: Cuenta con una amplia base de usuarios, que brindan soporte y extensiones útiles.
- Accesibilidad: Todo el trabajo de mantenimiento, uso, auditoria, etc. puede hacerse por Internet, desde un browser.
- Escalabilidad: esto se ve en dos frentes, por un lado el esquema jerárquico permite que se deleguen funciones, permitiendo que el sistema sea manejable, incluso a medida que crece. Y en la otra mano, en el caso que se esté teniendo problemas de performance, parte del producto es un utilitario llamado ZEO, que permite distribuir la carga del sistema entre varios servidores.
- Modularidad: En línea es posible encontrar más de 500 productos que permiten aumentar las funcionalidades de un sitio, incluyendo manejo de contenido (wikis, weblogs), búsqueda, conexión a distintas fuentes de datos, etc. Este es el caso del sistema OpenFlow.

- Documentación: Cuenta con información de diseño del Sistema incluyendo características del API (por ejemplo en el ZOPE Book [30] o utilizando el producto ZpythonDoc) , HOWTO's, Código Abierto, El Libro "ZOPE Book", la guía del administrador [29]y del desarrollador [6], etc

Debilidades

- Performance: Aunque en la prueba no se notó (con resultados de respuesta en el orden del segundo, en una máquina Pentium II Celerón (300 MHZ, Windows 98) bastante cargada, el hecho de ser desarrollado en Python podría dar un rendimiento pobre.
- Java: No define un protocolo claro con aplicaciones Java, aunque por lo visto en línea, en trabajos de presentación o mecánica finos, es posible establecer un modelo de comunicación Zope->Jython->Java (en el cliente) o Zope → JPI (Java to Python Interface) → Java (en el servidor)

3.1.2 PostgreSQL

PostgresSql [20] es una de las Bases de Datos más potentes de Software Libre, superior en varios aspectos a algunas RDBMS propietarias, incluyendo un amplio subconjunto del Estándar SQL92. Incluyendo además de las estructuras básicas de SQL:

- Manejo de Permisos a nivel de tabla.
- Restricciones (Constraints)
- Disparadores (triggers)
- Reglas (Rules)
- Integridad Transaccional
- Procedimientos almacenados (Stored Procedures): Además de permitir procedimientos en un dialecto del PL/SQL, permite la creación de scripts de Python y perl, entre otros.
- Tipos no atómicos y blobs: Permiten guardar en la base de datos estructurados y contenido binario en general, por ejemplo aspectos multimedia.

Sin embargo, la simplicidad del esquema relacional también hace muy difícil la implementación de ciertas aplicaciones. Postgres ofrece una potencia adicional sustancial al incorporar los siguientes cuatro conceptos adicionales básicos en una vía en la que los usuarios pueden extender fácilmente el sistema:

- Clases
- Herencia
- Tipos
- Funciones

Estas características colocan a Postgres en la categoría de las Bases de Datos identificadas como *objeto-relacionales*. Nótese que éstas son diferentes de las referidas como *orientadas a objetos*, que en general no son bien aprovechables para soportar lenguajes de Bases de Datos relacionales tradicionales. Postgres tiene algunas características que son propias del mundo de las bases de datos orientadas a objetos. De hecho, algunas Bases de Datos comerciales han incorporado recientemente características en las que Postgres fue pionera.

Cuenta además con abundante documentación (incluyendo libros enteros) sobre su manejo, a nivel de usuario, administrador y desarrollador. Por lo que ésta no es más que una

pequeña introducción. Se incluye sin embargo, en la bibliografía, manuales de manejo a nivel de usuario, administrador y desarrollador

La licencia con la que se distribuye es la BSD, con lo que brinda una gran flexibilidad en lo que se puede hacer con ella.

3.2 Productos Zope utilizados por la aplicación base

Paflow, como toda aplicación Zope, hace uso intensivo de productos existentes para ese entorno. Dado que estos le proporcionan su funcionalidad (y, por lo tanto, gran parte de la funcionalidad de Yará) los describiremos brevemente en esta sección.

3.2.1 OpenFlow

OpenFlow es un sistema de workflow, que cuenta con las herramientas básicas necesarias para este cometido (Motor de workflow con posibilidad de asignar aplicaciones a cada etapa, manejo de usuarios y herramienta de definición). Además es de Código Libre, escrito en Python. Funciona sobre Zope. Página web: <http://www.openflow.it>

Este sistema permite la definición y seguimiento de Workflows, de acuerdo a lo especificado por la WfMC, todo eso manteniendo una interfaz y una mecánica simples. Sin embargo hay aspectos en que se podría haber hecho más uso de algunas funcionalidades del Zope. Por otra parte, por la simplicidad del esquema en que se monta el Sistema, no parece complicado modificar partes del sistema para brindar agregados de mantenibilidad y escalabilidad.

Fortalezas:

- **Tamaño:** Este Sistema, entregado como plug-in del Zope, pesa solo 40 Kb en formato comprimido. Esto se debe a que hace uso intensivo de las posibilidades de Zope.
- **Simpleza:** Se desprende del ítem anterior y del hecho de ser hecho en python.
- **Licencia:** Este producto cuenta con licencia GPL.
- **Accesibilidad:** Siguiendo con el esquema de Zope, puede ser mantenido a través de la Web.
- **Permite la asociación de aplicaciones concretas a determinadas etapas,** lo que podría brindar mayor automatismo.
- **Manejo de Excepciones en los procesos:** Permite manejar de forma ordenado casos en que por alguna razón un proceso llega a un estado inesperado, derivándolos a un administrador para que los encauce nuevamente en el flujo del proceso.
- **Rediseño Dinámico de Procesos:** Permite modificar los procesos incluso durante su ejecución. Esto brinda gran flexibilidad al proceso. Estos dos últimos puntos son, en realidad, complementarios. En efecto, cuando se da una excepción es una muestra que el proceso necesita un rediseño, sin embargo, al hacer un rediseño, se pueden dejar etapas en un estado inconsistente, con lo que se genera una excepción.
- **Portabilidad:** Al ser completamente hecho en Python hereda su portabilidad.
- **Apego a los estándares:** Este proyecto busca seguir en su funcionamiento lo especificado por la WfMC.

Debilidades:

- El Interfaz de definición del workflow es lenta ya que no es posible tener todas las actividades a la vista al momento de definir el workflow, además el sistema de fijado de relaciones es primitivo, debiendo fijar en cada caso las actividades de inicio y de destino en un comboBox, lo que hace tediosa la tarea de diseño. Este aspecto se soluciona utilizando el Producto OpenFlow Editor [3.2.2]
- Estándares: Este proyecto no implementa el estándar XPDL [28].
- Alarmas: Este proyecto no implementa alarmas dentro del sistema.
- Poca documentación.

3.2.2 OpenflowEditor

OpenFlowEditor es un producto Zope que permite visualizar y modificar workflows definidos mediante OpenFlow. Requiere GraphViz 1.9 o superior.

Debido al papel central de GraphViz en OpenFlowEditor comentaremos éste a continuación para posteriormente comentar las funcionalidades del editor.

GraphViz

GraphViz es un conjunto de herramientas de código abierto para la generación automática de visualizaciones de grafos dirigidos y no dirigidos. Ha sido desarrollado por la sección de investigaciones de AT&T y se encuentra disponible para su descarga, así como su documentación en: <http://www.research.att.com/sw/tools/graphviz> .

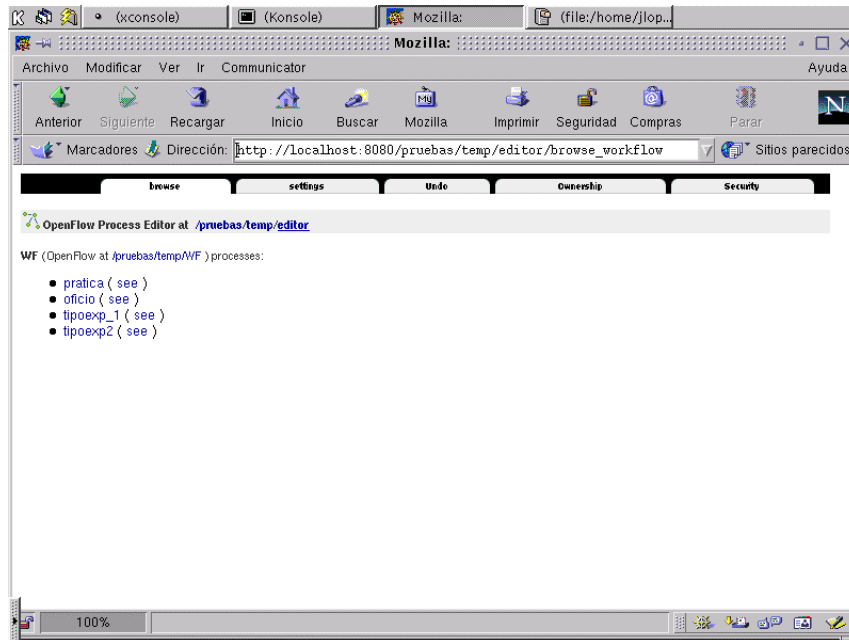
El paquete incluye las herramientas:

- Dot. Es una herramienta de procesamiento por lotes para esquemas de grafos dirigidos. La entrada es una descripción del grafo en el lenguaje descriptivo *dot* y la salida es una versión gráfica del mismo en formato vectorial o de mapa de bits.
- Neato. Es una herramienta de procesamiento por lotes para esquemas de grafos no dirigidos. La entrada es una descripción del grafo en el lenguaje descriptivo *dot* y la salida es una versión gráfica del mismo en formato vectorial o de mapa de bits.
- Twopi. Es una herramienta de procesamiento por lotes para esquemas de grafos circulares no dirigidos. La entrada es una descripción del grafo en el lenguaje descriptivo *dot* y la salida es una versión gráfica del mismo en formato vectorial o de mapa de bits.
- Lefty. un editor de grafos para imágenes técnicas.
- Dotty. Script para grafos dirigidos.
- Lneato. Script para grafos no dirigidos.

Estas herramientas se pueden utilizar individualmente, pero pueden ser extendidas para crear interfaces con bases de datos y sistemas externos.

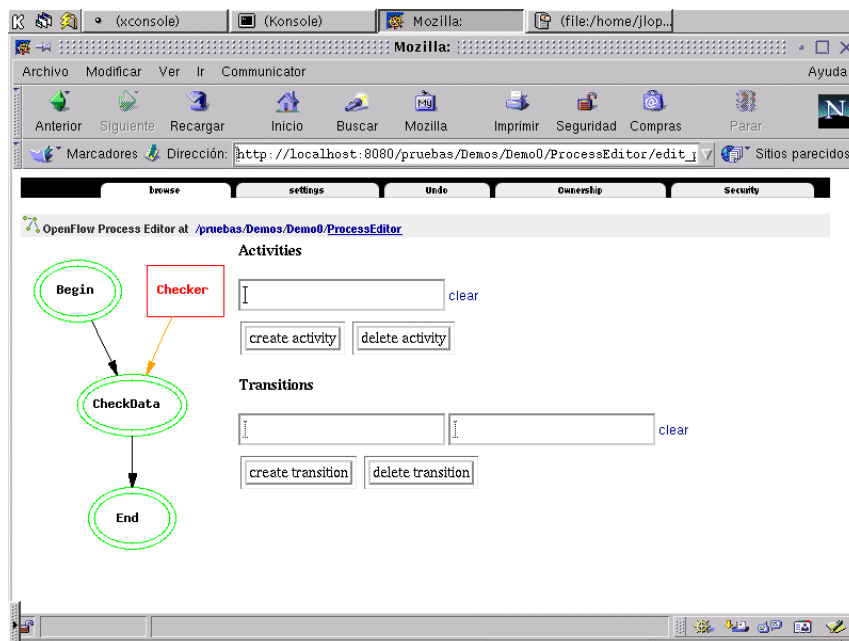
Funcionalidades de OpenFlowEditor

Es posible editar todos los procesos definidos en instancias de OpenFlow que se encuentren en el path de adquisición de la instancia de OpenFlowEditor. La siguiente captura de la internas de gestión de Zope muestra cuatro procesos definidos en la instancia de OpenFlow *WF*



Lista de workflows editables

El usuario puede seleccionar un workflow para editar sus propiedades desde la internas de manejo de la instancia de OpenFlow donde éste reside o puede, haciendo clic en *see*, visualizar el workflow como un grafo dirigido.

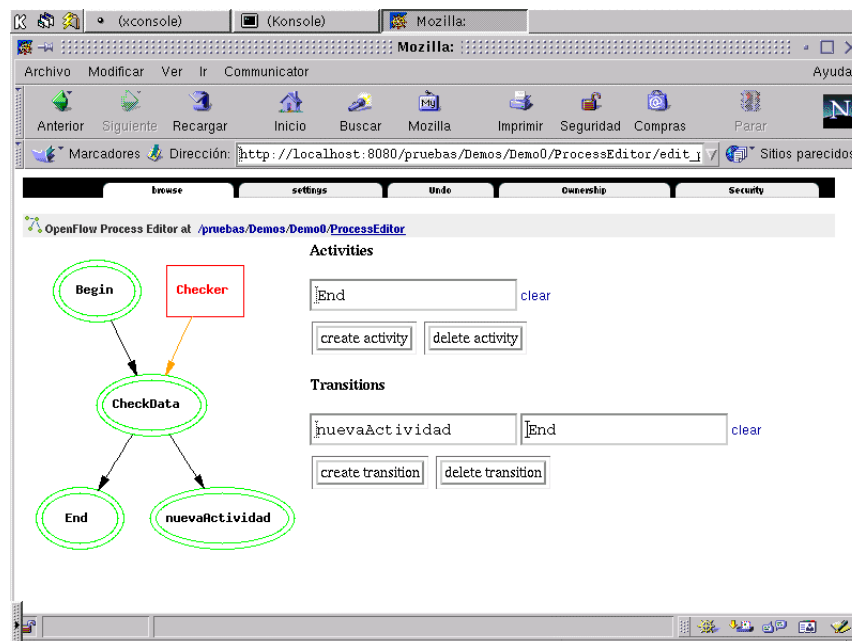


Visualización de un workflow

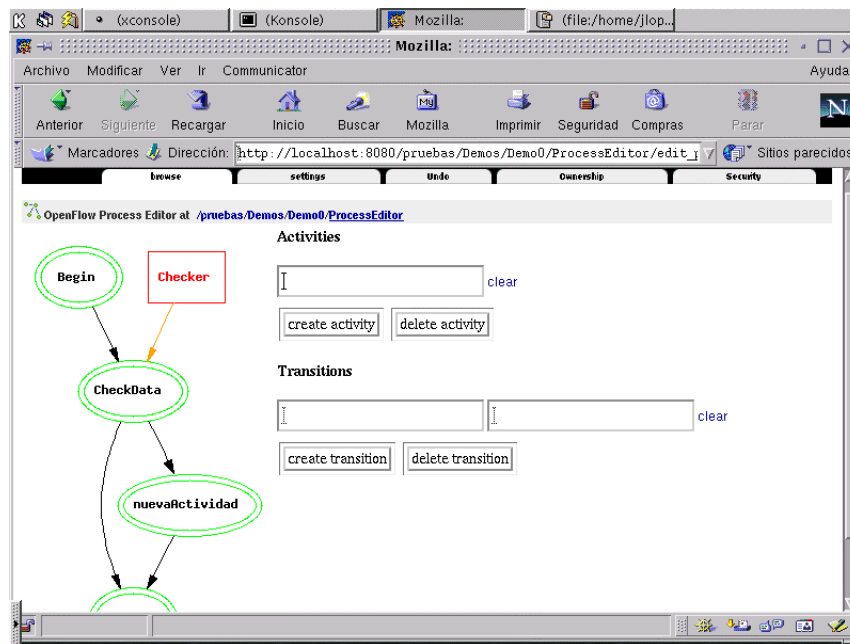
Podemos ver, en forma de elipses, las actividades con que cuenta el workflow (en este caso *Begin*, *CheckData* y *End*) así también como el rol asociado a la actividad *CheckData*; *Checker*. Para generar la visualización automática del workflow en forma de grafo dirigido, OpenFlowEditor hace uso de la herramienta *dot* del paquete *GraphViz*. Para ello, utiliza el API de OpenFlow para generar un archivo temporal con la definición del grafo que representa al workflow en el lenguaje *dot*. Este archivo será la entrada para la herramienta, que generará de forma automática la imagen en formato gif. Por lo anterior, es necesario que el usuario Zope tenga permiso de lectura – escritura en el directorio temporal del sistema (*/tmp* en sistemas tipo UNIX)

OpenFlowEditor soporta, en la actualidad, solamente la definición en forma gráfica de nuevas actividades y transiciones, debiéndose recurrir a la interfaz de manejo de OpenFlow en el ZMI o a su API para la definición de los restantes elementos del workflow (roles, aplicaciones asociadas a las actividades, etc). Las modificaciones realizadas en forma gráfica son incluidas automáticamente en la definición del workflow en la instancia de OpenFlow donde ésta reside haciendo uso del API del motor.

La siguiente captura muestra la inclusión de una nueva actividad y una nueva transición en el workflow de ejemplo



Para definir una nueva transición, el usuario puede seleccionar las actividades de comienzo y fin haciendo clic con el ratón en ellas. La aplicación se encarga de agregar sus nombres en los campos de texto de la transición. Esto se hizo a modo de ejemplo en la captura anterior, donde se pretende crear una nueva transición desde la actividad *nuevaActividad* a *End*. Al crear la transición, la página se carga automáticamente de nuevo reflejando el cambio.



Creación de una nueva transición en el workflow de Ejemplo

3.2.3 DocumentLibrary

DocumentLibrary está diseñado para ser un producto de Zope que permita crear bibliotecas de documentos en la cual se pueda examinar y buscar documentos indexándolos a texto completo.

Almacenamiento de documentos.

Este producto incluye una clase especial de documentos de archivo que permite almacenar e indexar varios formatos de archivo en la biblioteca. Como son objetos de Zope, se pueden asociar también metadatos arbitrarios a los documentos. La instalación por defecto incluye el siguiente conjunto de metadatos, para los documentos almacenados:

- identifier:* URL absoluto del documento.
- title: título especificado por el usuario.
- creator: Autor original
- description: Resumen de documento
- date: Creación o fecha de revisión.
- type: Categoría general.
- format:* el formato de mime de los datos de documento
- source:* el URI del documento original (si existe)
- subject:* títulos de los temas del índice asignados al documento.
- Indica atributos que son incluidos automáticamente.
- Además, están disponibles las siguientes propiedades:
- review_date: Fecha en que el documento fue revisado.
- topics: Lista de id's en Python de índices de temas asignados.
- filename: El nombre del archivo original agregado.

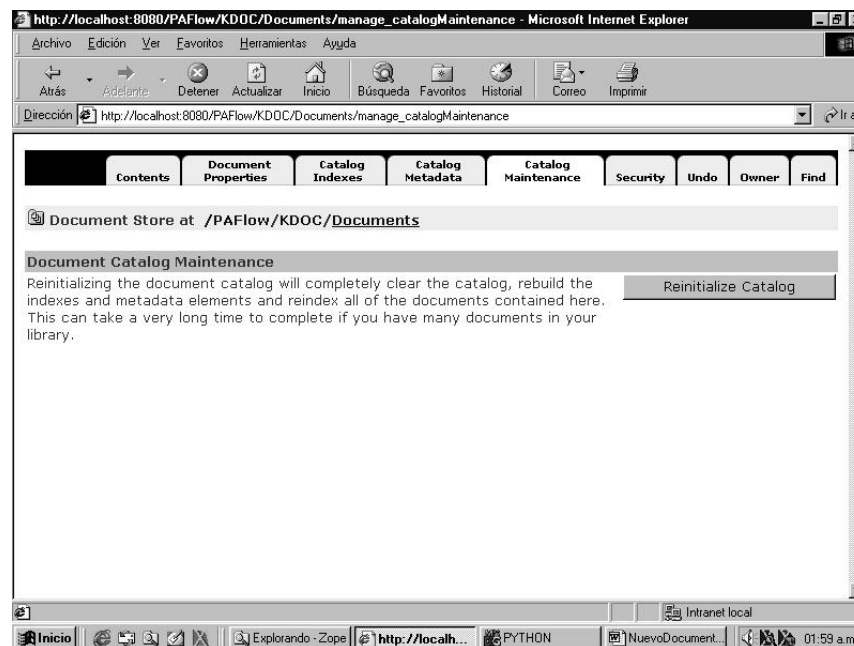
Los documentos almacenados en DocumentLibrary tienen sus hojas de propiedad fijas, las que son manejadas en forma centralizada. Esto permite modificar el esquema de las propiedades de los metadatos para todos los documentos al mismo tiempo.

Los documentos son indexados cuando se incluyen en DocumentLibrary. Actualmente, la indexación a texto completo está soportada para los siguientes formatos de archivo:

- Texto plano.
- HTML / XML.
- PDF.
- Postscript.
- El Microsoft Word (6.0/95, 97 y 2000 formatos)
- Microsoft Excel.
- Microsoft Powerpoint.

Se ha implementado una arquitectura de “plug-in’s” para los convertidores utilizados en la indexación a texto completo, lo que hace que la tarea de añadir soporte para nuevos formatos de archivo sea sencilla.

Desde la interfaz de manejo de Zope se pueden reindexar los documentos existentes en la instancia de DocumentLibrary.



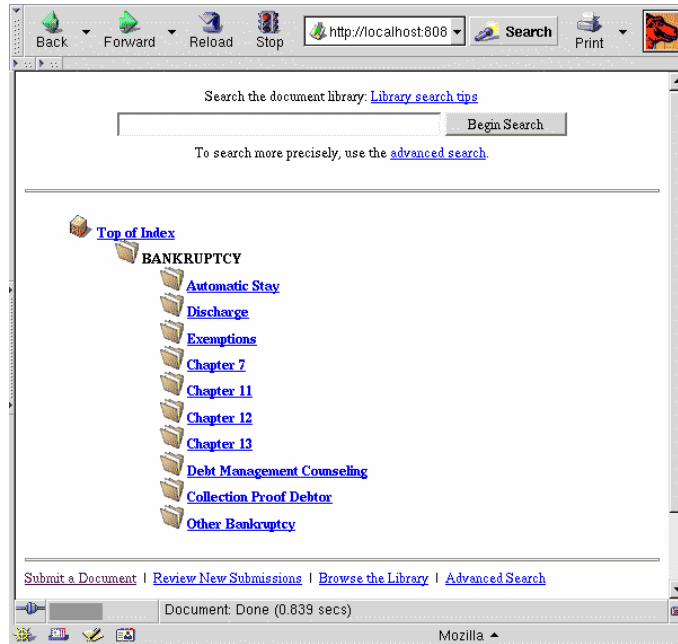
Reinicialización de Catálogo

Índices de temas.

DocumentLibrary soporta un sistema de indexación jerárquico para categorizar documentos. Un documento simple se puede asignar a tantos índice de temas diferentes como se desee.

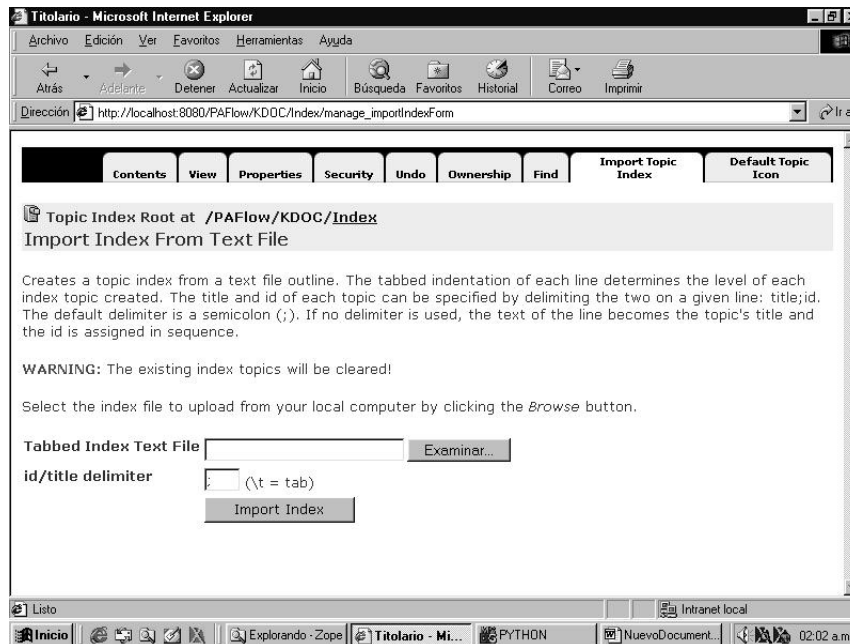
Para mejorar la estética de la interfaz de biblioteca, se puede asignar iconos diferentes a los existentes a los índices de temas desde la interfaz de manejo de Zope (ZMI).

La interfaz de usuario por defecto es un árbol jerárquico en los índices. Esto puede modificarse completamente según las necesidades que se tengan modificando los métodos de DTML en la instancia de DocumentLibrary.



Jerarquía de temas

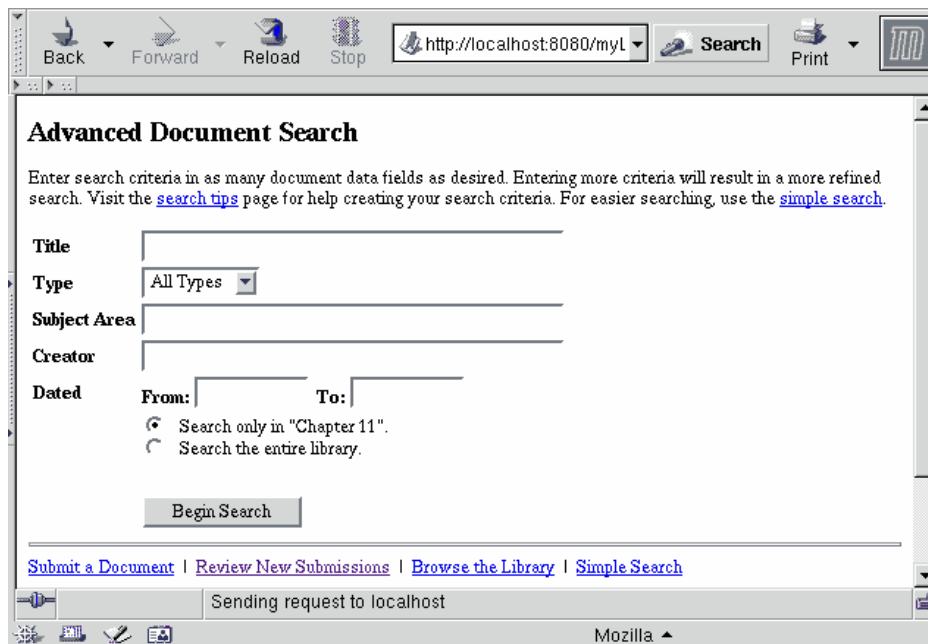
Se puede importar, desde un archivo de texto, una jerarquía entera de índice de temas. El archivo debe contener la jerarquía de temas ordenada por tabulaciones. La distribución incluye un ejemplo de un archivo de este tipo.



Importación del archivo de índices

Búsqueda

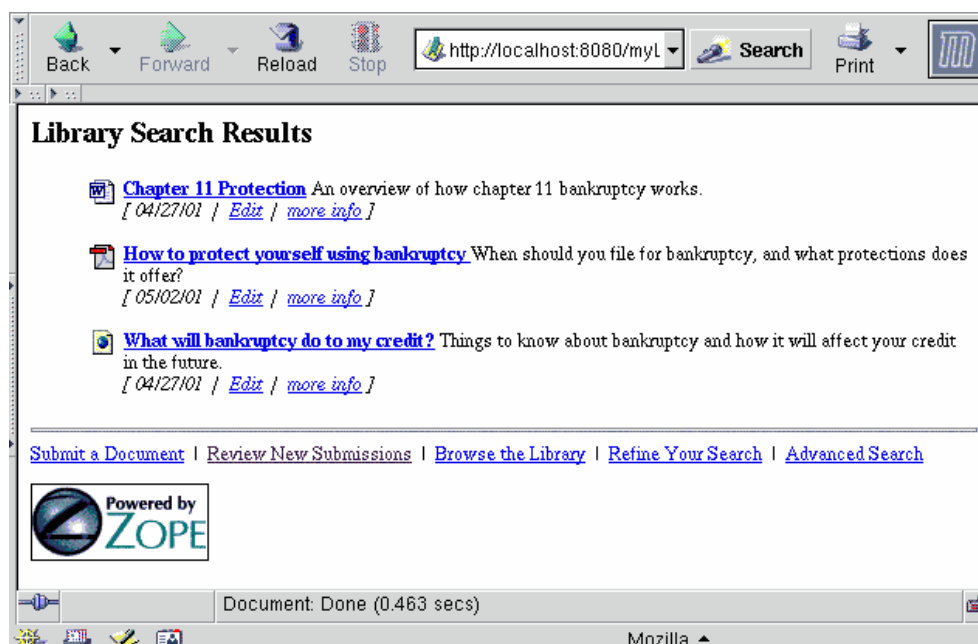
La biblioteca incluye dos interfaces de usuario para las búsquedas: una búsqueda simple donde se buscan documentos por metadatos y texto simultáneamente, y una búsqueda avanzada que permite búsquedas más refinadas.



Búsqueda avanzada

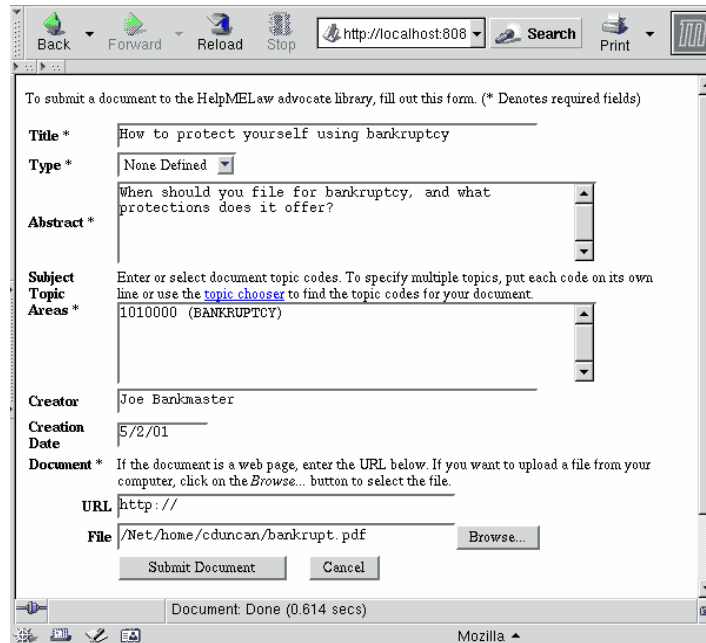
El mecanismo de búsqueda usa Zope Catalog, por lo que se soportan búsqueda booleanas simples ("and", "or", "not" y "near") para contenido textual y metadatos.

Se soporta también, la búsqueda restringida a un índice de tema específico.



Ingreso de documentos y revisión

Los documentos se pueden ingresar a la biblioteca por cualquier usuario al que se halla otorgado los permisos adecuados, incluyendo usuarios anónimos. Los documentos son ingresados cargando un archivo de la computadora del usuario o especificando una URL donde el documento reside. Si se especifica una URL, los datos del archivo se recuperan y almacenan en archivo destino en tiempo de carga.



To submit a document to the HelpMELaw advocate library, fill out this form. (* Denotes required fields)

Title * How to protect yourself using bankruptcy

Type * None Defined

Abstract * When should you file for bankruptcy, and what protections does it offer?

Subject Topic Areas * Enter or select document topic codes. To specify multiple topics, put each code on its own line or use the [topic chooser](#) to find the topic codes for your document.
1010000 (BANKRUPTCY)

Creator Joe Bankmaster

Creation Date 5/2/01

Document * If the document is a web page, enter the URL below. If you want to upload a file from your computer, click on the *Browse...* button to select the file.

URL http://

File /Net/home/cduncan/bankrupt.pdf

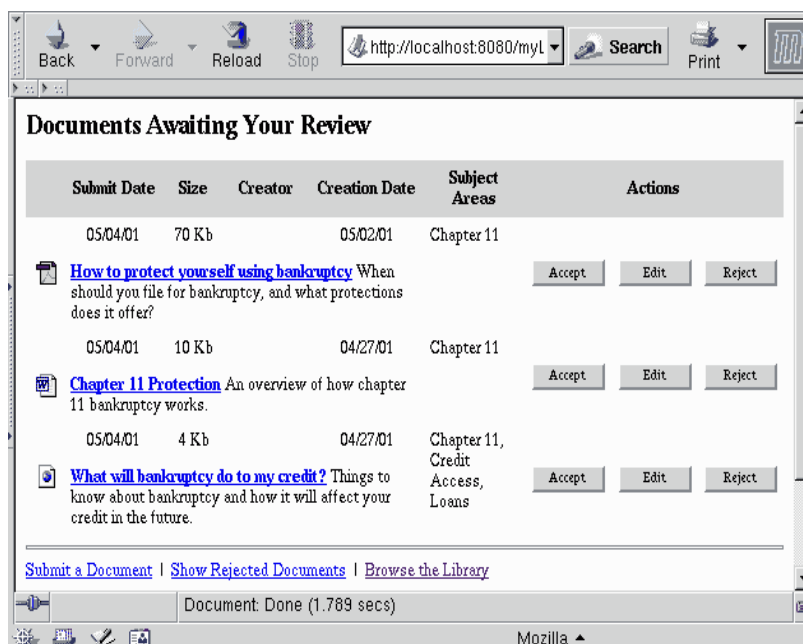
Document: Done (0.614 secs)

Mozilla

Ingreso de Documentos

Para vigilar los ingresos inadecuados, se provee la funcionalidad de revisión para permitir a uno o más revisores aprobar o rechazar ingresos a la librería. Para permitir la delegación de la revisión a varias personas, se puede asignar un índice de tema separado a cada revisor para que revise esos documentos.

Una precaución adicional es la posibilidad de tener una lista de tipos de archivo no permitidos en la biblioteca. Esto se puede adaptar para restringir formatos de archivo inseguros. Por defecto, todos los archivos binarios desconocidos (como ejecutables) no se pueden cargar en la biblioteca. Esto se puede modificar yendo a la pestaña de propiedades de la instancia de Document Library desde el ZMI.



Revisión de Documentos

Compatibilidad

Hasta ahora el producto de DocumentLibrary está enteramente soportado sólo en plataformas UNIX; puede funcionar bajo Windows pero sin la funcionalidad de indexado a texto completo. Sin embargo, debido a su arquitectura modular, sería posible subsanar este problema integrando utilidades que transformen a texto los formatos de archivos soportados que funcionen en la plataforma Windows.

Utilidades adicionales para indexado fulltext

Para el soporte del indexado de texto de documentos MSWord se debe instalar *wvWare*, un utilitario de conversión de código abierto de documentos MSWord. Se puede descargar *WvWare* de: <http://www.wvWare.com/>

El convertidor de PDF requiere *pdftotext* el cual es parte del paquete de código abierto Xpdf. Se puede descargar desde: <http://www.foolabs.com/xpdf/>
Tanto *wvWare* como *pdftotext* deben estar en el path del usuario Zope. Además éste debe tener acceso de escritura a /tmp.

Los convertidores de Excel y Powerpoint requieren el convertidor de código abierto xlHtml disponible en: <http://www.xlhtml.org>

3.2.4 Localizer

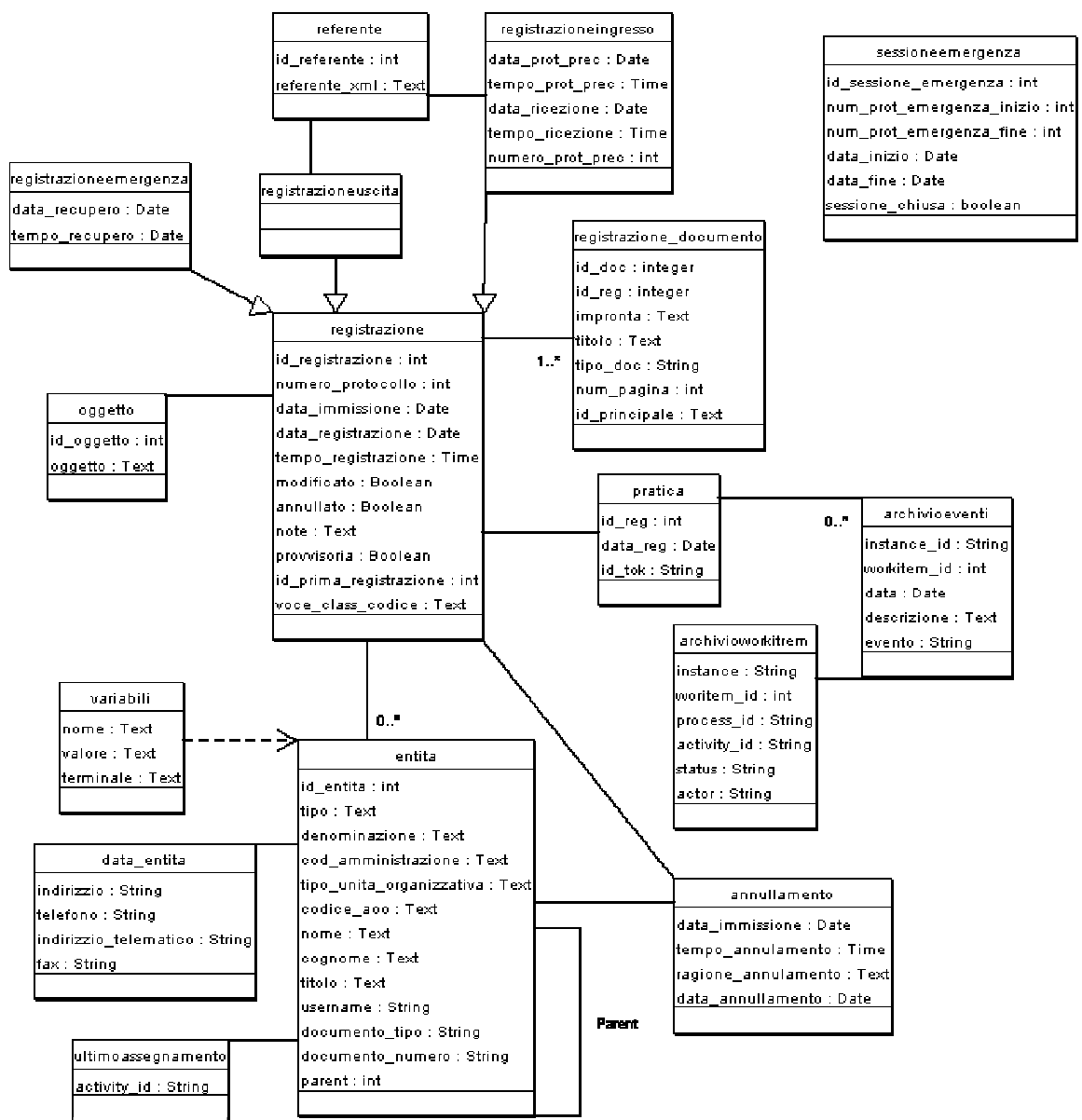
1. Localizer es un producto Zope que permite que una aplicación muestre el mismo mensaje en diferentes idiomas y es utilizado para la internacionalización de aplicaciones.

3.3 Descripción Técnica

Habiendo descrito los componentes del software de base elegido, pasaremos a realizar una descripción de su base de datos y del proceso de workflow implementado en Paflow, como un medio de proveer un marco que permita entender las modificaciones que fueron necesarias realizar a este sistema.

3.3.1 Base de datos

Se muestra en la figura la Base de Datos de Paflow mediante un diagrama UML, para posteriormente comentar la estructura existente.



Los datos administrados por el sistema son representados en el diagrama de clase UML de la figura, en que se evidencian las relaciones que cumplen los datos. Estos están implementados mediante relaciones entre tablas de bases de datos relacionales.

La base de datos de registros es una base de datos relacionales compuesta de diversas tablas, a las cuales se añaden continuamente nuevos registros y nunca cancelaciones, excepto durante una eventual operación especial de "archivo " de registros históricos a causa de la falta de espacio en disco.

Notar que un registro de documentación resulta individualizado completamente por la pareja (data_immissione, numero_protocollo).

Por motivos de espacio, no se incluyen en el diagrama tablas pequeñas que no están relacionadas directamente al núcleo del sistema, con pocos campos. Por ejemplo las reservadas para auto numeración, sin embargo, de todas formas su discusión se encuentra detallada en este documento.

No se representan tampoco, ni se documentan, trazas en el sistema de implementaciones pasadas de la estructura, derivadas por ejemplo, de la actualización del motor de workflow

Se resume a continuación el significado de las diversas clases UML:

Referente

La clase Referente representa entidades remitentes o destinatarios de las comunicaciones de documentos. Los datos se representan, en la clase, directamente en formato XML adhiriendo así a las especificaciones emanadas de AIPA. Esta representación permite una fácil adaptación del software a eventuales modificaciones que estas especificaciones puedan sufrir en futuro, No hay necesidad de modificar la base de datos de registros en la eventualidad de tales modificaciones.

Registro

Un registro es representado mediante la clase abstracta de UML Registrazione, contiene los datos comunes a todos los registros de protocolo:

- Número correlativo único.
- Fecha y hora de registro.
- Un campo booleano, Anulado, que indica la anulación del registro
- Un campo booleano, Modificado, que indica la modificación del registro

Mantiene la información común relativa a los registros en entrada y en salida de documentos, tanto de papel como electrónicos, comprendiendo los anulados, y todas las versiones precedentes de los registros modificados.

El campo data_immissione, para el registro de las modificaciones de un registro, permite la individualización unívoca del registro, conjuntamente al campo numero_protocollo.

El campo provvisoria indica si el usuario tiene que confirmar la efectivización del sellado de los documentos en soporte papel (valor true) o si tal operación ya ha sido efectuada (valor false); solo cuando este campo asume el valor falso el registro es visto también por los demás operadores del sistema; los registros no confirmados dentro un intervalo preestablecido automáticamente se anulan del sistema.

RegistrazioneIngresso

Deriva de Registrazione representa un registro en entrada para el AOH, y mantiene los datos específicos solo al registro:

- Datos relativos a un eventual registro en salida por parte del AOH remitente: número de protocolo, fecha y hora.
- Fecha y hora exacta del recibo de la comunicación en entrada por parte del AOH, en los casos en que halla una coordinación temporal, difiriendo de la ejecución material del registro en entrada, conserven de todos modos una alguna relevancia (ej., en el caso de presentación de un pedido de actuación, en que es fundamental la fecha de llegada de la pregunta, mientras que el registro en entrada puede ser retardado más allá de los límites temporales de presentación del pedido mismo).
- El remitente del registro en entrada, representado con una relación con la clase Referente.
- Memoriza la información suplementaria prevista para el registro de un documento en entrada; data_prot_prec, tempo_prot_prec y numero_prot_prec son respectivamente la fecha, la hora y el número de registro de eventualmente establecidos por un AOH remitente que tiene, a su vez, registrada esa comunicación en salida.
- Data_ricezione y tempo_ricezione son tiempos relativos al recibo físico de la comunicación, en el caso en que ésta no coincida con las de ingreso del registro en el sistema.
- Id_referente individualiza, en la lista Referente, el remitente del registro en examen.

RegistrazioneUscita.

Guarda la información suplementaria prevista para el registro de un documento en salida, actualmente solo el destinatario; deriva de Registrazione, representa un registro en salida para la AOH, y mantiene los datos específicos para un registro particular, o sea los destinatarios de la comunicación de documentos en salida, representados mediante relación 1 - 1 con la clase Referente.

RegistrazioneEmergenza

Mantiene los datos relativos a un registro efectuado en régimen de emergencia e introducido posteriormente en el sistema; memoriza fecha y hora de la operación de "recuperación" del registro, y el operador que lo ha efectuado.

- data_recupero es la fecha en que se recupera el registro en las base de datos.
- id_utente identifica el operador que ha efectuado la Recuperación.

SessioneEmergenza.

Registro de sesiones de emergencia (es decir, sesiones en que el sistema no estuvo disponible), marca lapso de tiempo y números correlativos que cubre. Identifica además al usuario que la registra y si ya está completa.

- id_sessione_emergenza: Clave del registro

- num_prot_emergenza_inizio: Número correlativo en que comienza la sesión de emergencia.
- num_prot_emergenza_fine: Número correlativo en que termina la sesión de emergencia.
- data_inizio: Fecha en que comienza la sesión de emergencia.
- data_fine: Fecha en que termina la sesión de emergencia.
- sessione_chiusa: Campo booleano que expresa si se pueden ingresar nuevos registros en esa sesión.

Entita.

Cada registro de esta tabla mantiene los datos relativos a una entidad o funcionario, donde la entidad es de uno de los tres tipos en los que está conceptualmente basado el sistema y que han sido mencionados anteriormente (administraciones, AOH, unidades organizativas)

Se mantienen los datos de los usuarios que tienen acceso al sistema. Cada individuo resulta identificado por un nombre, un apellido además de todo lo que sea suficiente para la identificación unívoca del usuario en el interior del AOH. Debido a que los usuarios del sistema son usuarios zope se les asocia además un nombre de login. Los privilegios con los que cuentan y sus contraseñas son administradas y mantenidas desde la interfaz de manejo ZMI. Existe la posibilidad, de parte del administrador, de hacer corresponder a un individuo particular "niveles de autenticación" diferentes, al fin de permitir a una misma persona poder acceder al sistema con niveles de privilegio diferentes.

De las entidades, se mantienen los datos necesarios para su individualización mostrados en la figura.

El campo parent proporciona una manera de establecer una jerarquía entre las entidades y usuarios definidos.

Esta tabla no se encuentra normalizada, y presenta el problema que representa cuatro objetos distintos: Persona, Administración, AOH y Unidad Organizativa, sin embargo es funcional y está correctamente integrada en el sistema. Recoge dos conjuntos disjuntos, los de entidades que se encuentran en la administración local (descendientes del registro 0) y los que forman parte del directorio de entidades externas a la misma (descendientes del registro 1), pero que se relacionan con la misma, ya sea solicitando servicios o siendo objeto de solicitudes de servicios.

Oggetto.

Representa los temas de los registros de documentos.

Pratica.

Almacena la asociación de una instancia del proceso "*pratica*" con un registro particular mediante la pareja id_reg, data_reg. La instancia del proceso asocia implícitamente al creador de la instancia y el identificador de la misma mediante la concatenación del nombre de usuario y el identificador.

ArchivoWorkitem.

Por cada actividad en curso se genera un workitem asociado que guarda los datos del estado del proceso para una instancia particular en esa actividad. El objetivo de esta tabla es almacenar los workitems completados para cada actividad del proceso *pratica*.

ArchivoEventi.

El objeto de esta tabla es almacenar todos los eventos de los workitems de una determinada instancia del proceso *pratica* para cada cambio de actor (debido, por ejemplo a una reasignación) y estado del mismo.

Registrazione_Documento.

Almacena la asociación de un determinado documento en la base de datos zope (ZODB) con un número de protocolo particular (mediante *id_reg*). Cuenta, además, con los siguientes campos:

- *Id_doc*: identificador del documento en ZODB.
- *Impronta*: hash asociado al documento, permite garantizar la no modificación del mismo.
- *Titulo*: título del documento.
- *tipo_doc*: tipo del documento (MIME, papel)
- *num_pagina*: número de páginas del documento.
- *id_principal*: identificador del documento principal en ZODB. Toda registración cuenta con un documento principal y un conjunto de documentos asociados.

Datos de Entidad

Estas son cuatro tablas: *telefono*, *fax*, *indirizzo* y *indirizzo_telematicos*, conteniendo datos de localización y comunicación de las entidades, como son el telefono, fax, dirección postal o electrónica, respectivamente. Cada tabla cuenta con 3 partes, el identificador del registro, el identificador de la entidad a la que pertenece y los datos propios del registro.

Variabili

En ésta tabla se guardan variables de sesión, estableciendo nombre de la variable (*nome*) y valor (*valore*), para el usuario (*id_utente*) de una terminal dada (*terminale*).

Annullamento:

Almacena los datos de la anulación de un registro. Se relaciona con el registro que se anula y el usuario que hace la anulación, además tiene los siguientes campos:

- *data annullamento*: Fecha en que sucede la anulación.
- *tempo annullamento*: Hora en se hace la anulación.
- *data immssione*: Fecha en que se ingresa el registro.

- `ragione annullamento`: Razón por la que se anula el registro.

Las siguientes entidades, por su simplicidad, no fueron incluidas en el diagrama presentado más arriba.

Ultimo_assegnamento:

Utilizado en la asignación automática de personas a tareas, registra la última persona que estuvo asignada a una tarea, para ir variando cada vez a quien se le asigna la siguiente.

Log:

Registra la actividad del sistema, cuenta con tres campos:

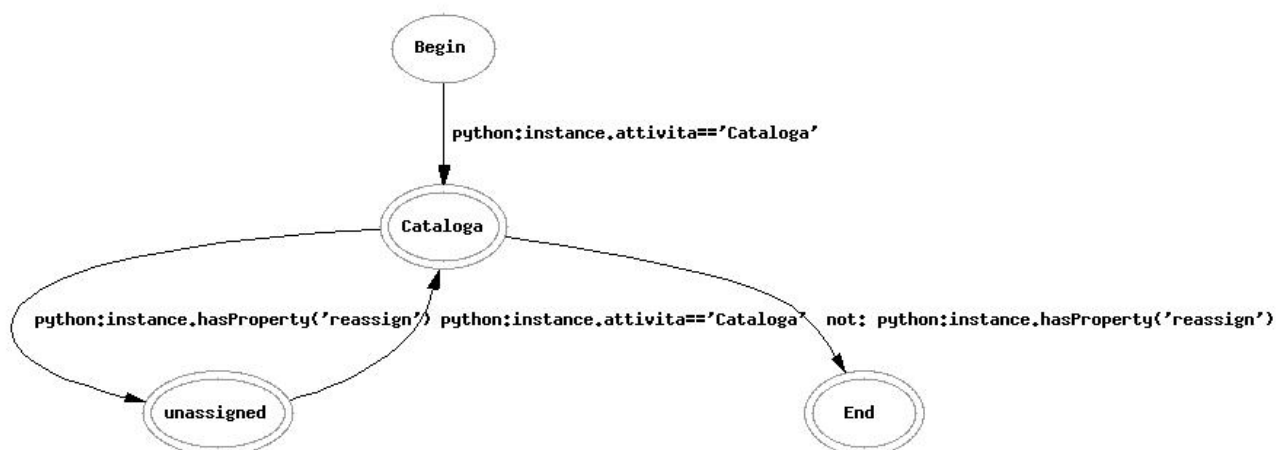
- `timestamp` : Momento en que sucede el hecho
- `Level` : Código de actividad registrada.
- `message` : Mensaje descriptivo asociado.

Número_protocollo:

Ésta tabla registra el próximo número correlativo para asignar, cuenta con el campo :

- `prossimo_numero_protocollo`: Próximo número correlativo disponible.

3.3.2 El proceso *Pratica*.



El proceso "*pratica*" es el único proceso implementado en Paflow. Se crean instancias del mismo al crearse un registro en entrada o en salida. El mismo cuenta con las actividades estándar de comienzo y fin (Begin – End) mas dos actividades "cataloga" y "unassigned". Asociadas a estas actividades se tienen dos aplicaciones; "*assigner*" y "*archiver*", respectivamente. La primera permite la elección de la actividad posterior a "Begin", las cuales están asociadas a un determinado rol interno (mas adelante se aclara este punto), y alternativamente, una segunda actividad en caso de que la primera no sea aceptada por ninguna de las personas con el rol elegido. La segunda,

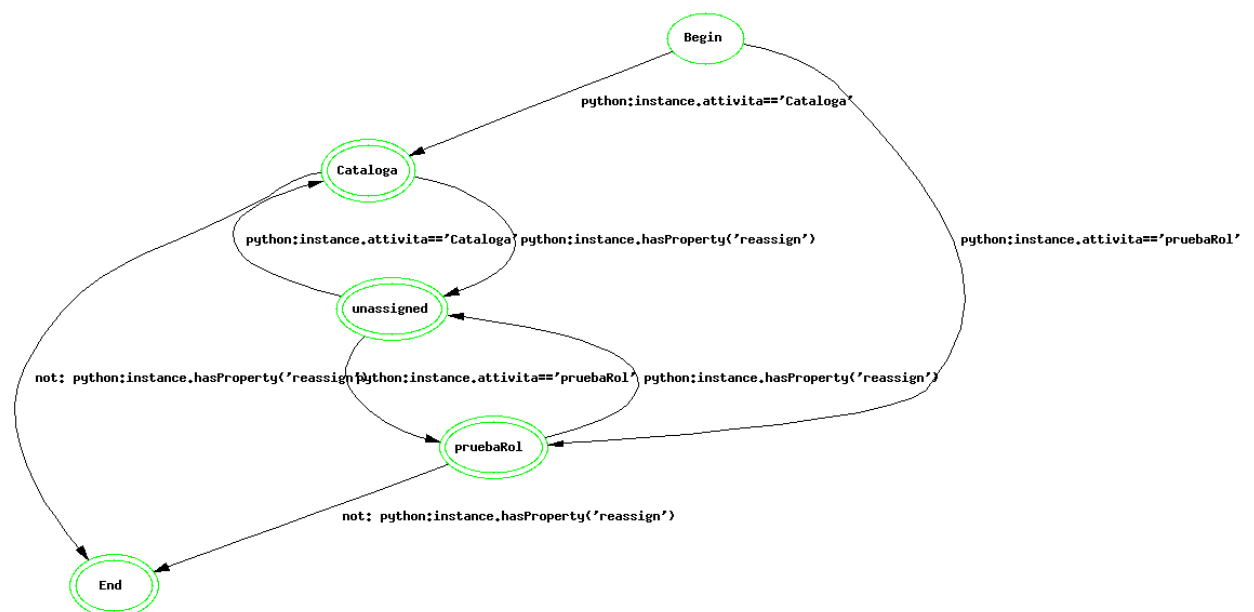
invocada automáticamente en la actividad “End”, guarda los datos relativos a la instancia del proceso en la base de datos del sistema en forma automática.

En la figura se puede ver además, las condiciones en lenguaje Python, las cuales hacen referencia a la existencia de determinada propiedad de la instancia del proceso (la cual se puede agregar o borrar dinámicamente desde una página DTML o ZPT [18]) o al campo actividad del mismo. La semántica del proceso es sencilla. Las instancias del mismo se crean al realizar un registro en entrada o en salida en un Area Organizativa Homogénea (AOH) denominación que es utilizada, por el marco normativo Italiano en que se basa la aplicación, para designar un conjunto de unidades administrativas que poseen una numeración común para sus documentos. La interfaz de usuario de ingreso de registros brinda la posibilidad de manejar documentos en papel teniendo la opción de escanearlos para ingresar su versión electrónica. En caso que no se elija esta opción se genera automáticamente un documento de texto que se adjunta al conjunto de documentos asociados al registro que simplemente deja constancia que ese documento se encuentra en soporte papel. Para asegurar la inalterabilidad de los documentos ingresados se procede a realizar un hash, mediante el algoritmo SHA, a los documentos ingresados.

Las instancias del proceso pasan directamente a la actividad ‘Cataloga’ que es ejecutada por usuarios con el rol ‘Cataloga’ y que son asignadas con política ‘round-robin’, es decir, en forma cíclica entre los poseedores del rol. Estos ‘catalogan’ los documentos asociados al registro vinculando a cada documento un índice dentro del modulo de manejo documental (instancia de [DocumentLibrary](#)).

Usuarios con el rol de administración pueden reasignar, entre los usuarios con el rol apropiado y siguiendo la política round robin, la tarea a realizar.

El sistema cuenta con la posibilidad de definir roles locales a cada administración. Esta funcionalidad se realiza desde el menú Directorio-> Local. Por cada rol que se defina, se crea una actividad del mismo nombre en el proceso *pratica* con transiciones y condiciones que son ejemplificadas en la figura siguiente (se incluyó en el proceso el rol ‘pruebaRol’).



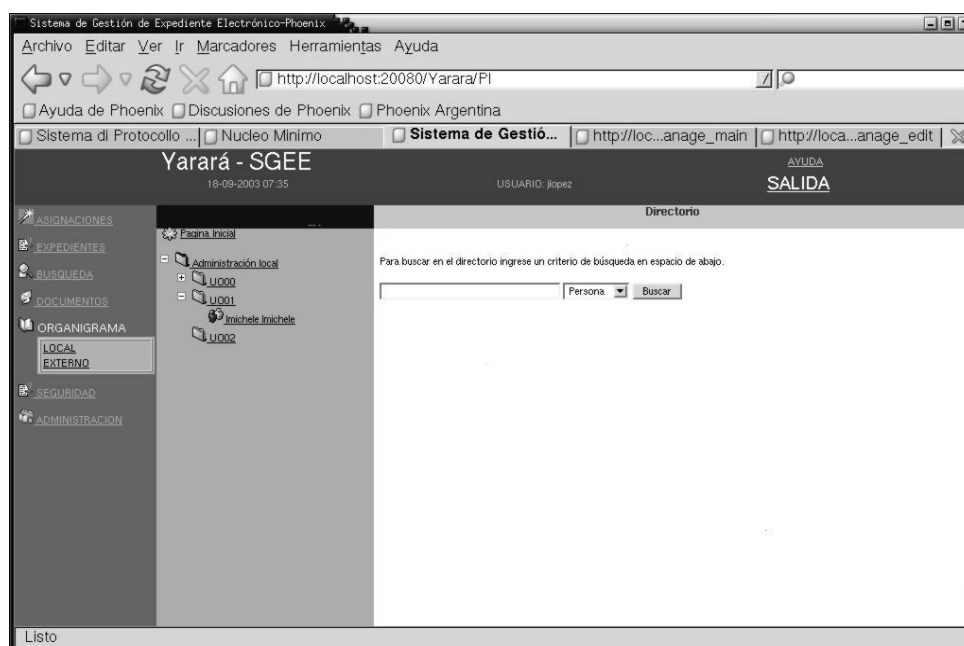
Se asocia la misma aplicación a la actividad creada que la asociada a la actividad 'cataloga', en otras palabras, se cumple la misma actividad que la descrita para *Cataloga*

4 DESCRIPCIÓN DE LA SOLUCIÓN PROPUESTA.

En este punto describiremos como interpretamos y adaptamos el sistema base en el marco de los objetivos de este proyecto, las modificaciones que fueron necesarias a su Base de Datos y al conjunto de roles definidos en la aplicación. Finalmente, describimos la estructura del sistema desarrollada, al que hemos llamado “Yarara” y describimos su esquema de seguridad, incluyendo la implementación de firma electrónica.

4.1 Diseño y Adaptación del sistema a los requerimientos

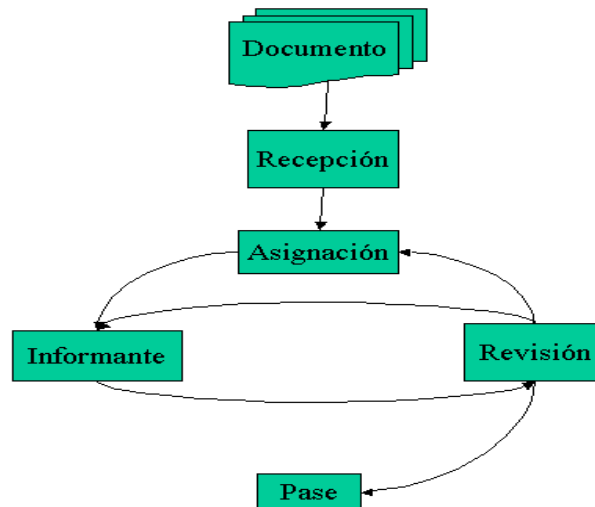
4.1.1 Definición de Workflows de Expedientes.



La figura anterior muestra la definición de unidades organizativas y personas, de manera jerárquica. Paflow, como anteriormente se ha comentado, define el proceso “Pratica”, el cual solo es un proceso de catalogado de los documentos asociados a un registro en entrada o salida, no siendo la intención del sistema original servir para controlar y gestionar los pasos internos de la documentación entre las unidades definidas. En la aplicación desarrollada, se ha reutilizado ese proceso de forma de lograr que represente el proceso administrativo “normal” que se desarrolla en cada oficina pública.

En lo que sigue analizaremos el problema a resolver y mostraremos las modificaciones realizadas a este proceso básico para el cumplimiento de los requerimientos del sistema.

La siguiente figura ilustra las actividades mínimas que realiza toda documentación en las administraciones públicas:



Toda unidad organizativa en la administración pública lleva un registro de los documentos ingresados o que han salido de ella. Es por eso que se ha decidido, cuando se ingresa una Unidad Organizativa, asociarle de manera automática el proceso, cuya descripción y estudio, es el eje de este punto. Básicamente toda oficina recepciona la documentación en un lugar determinado con, usualmente, un funcionario dedicado a su atención. En este lugar, conocido comúnmente como “mesa de entrada” de la unidad (no confundir con el lugar con el lugar donde ingresan o egresan los documentos en la administración, también conocido como mesa de entrada), el funcionario actuante verifica los requisitos formales para la recepción de la documentación. Estos requisitos implican, como mínimo, la integridad documental (no ausencia de fojas), chequear que la última actuación, que debe expresar la intención del jerarca de la oficina que envía el documento que se realice cierta tarea en la oficina receptora, derive la documentación hacia la oficina en cuestión y se encuentre firmada (esto se conoce como un “pase”). Ante un incumplimiento de los requisitos formales el funcionario no acepta la documentación, debiendo esta pasar a la oficina de administración documental de la organización, donde se decidirán las acciones correctivas a tomar. Toda organización pública cuenta con una unidad de este tipo, conocida comúnmente como “Secretaría”. En caso que la documentación cumpla los requisitos formales, el funcionario “da entrada” al mismo. Esto involucra registrar en algún medio (comúnmente papel), los datos relevantes de la documentación (tipo, tema, oficina que lo envió, etc) y su fecha de recepción.

Estos datos constituyen el registro documental de la unidad organizativa. Se genera además, una “constancia de recepción” que certifica que la documentación ha sido aceptada por la oficina actuante y que es utilizada para trazar la documentación en el conjunto de Administración (o sea, determinar que oficina tiene que documentos en su poder). Estas tareas se realizan en la actividad “Recepción” de la figura.

Posteriormente, el trabajo encomendado en el pase se asigna a uno de los funcionarios por el jerarca de la oficina o, eventualmente, por un mando medio. Esto ha sido representado en la figura por la actividad “Asignación”. Seguidamente, el funcionario designado recibe la documentación pudiendo aceptar o no el encargo. Si lo acepta, este genera un nuevo documento, un “informe” (en el caso de expedientes, esto se traduce en la inclusión de una o mas fojas en él) que es sometido a revisión. Si se rechaza, el documento vuelve a ser objeto de una nueva asignación. Estas tareas se realizan en la actividad “Informante” de la figura.

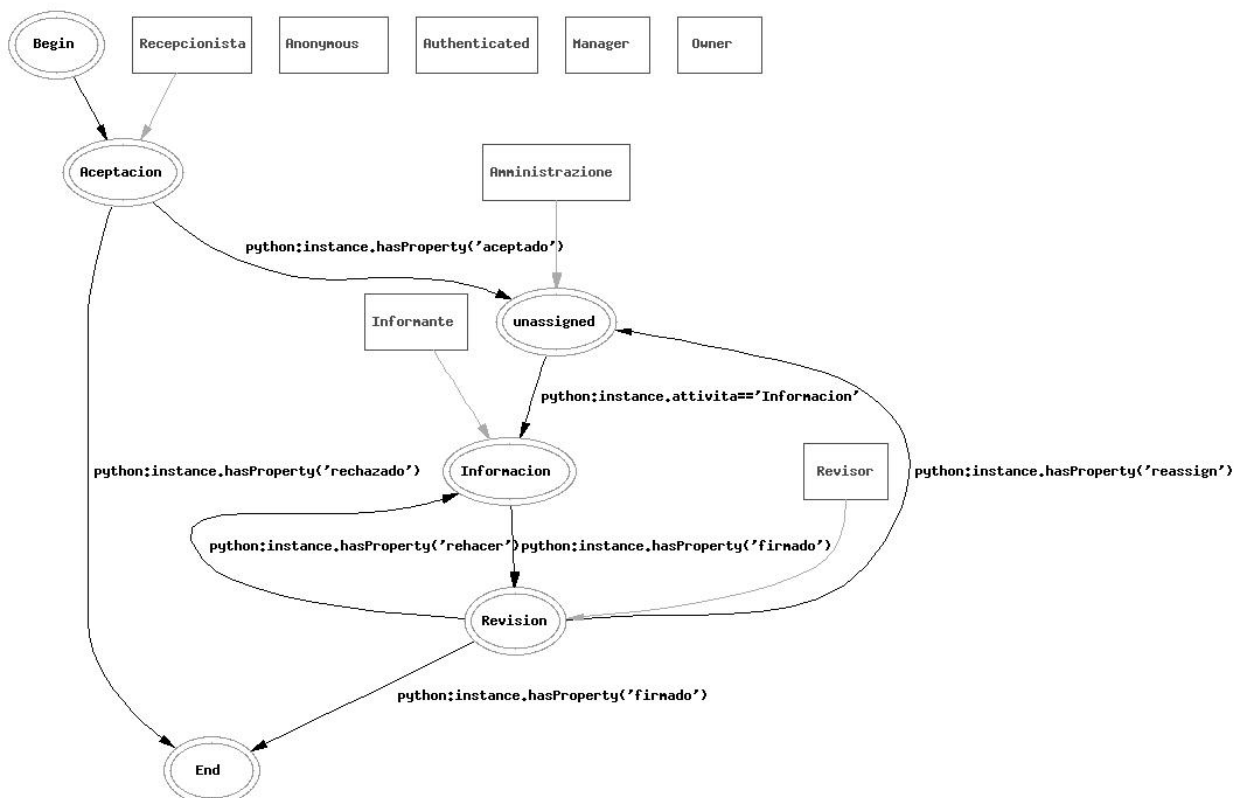
Seguido a la realización del informe, este se somete a la revisión de un funcionario de jerarquía superior. Este puede, según su entender, solicitar al funcionario informante que rehaga el

informe, o que incluya mas información. Puede también considerar necesario la inclusión de un informe por parte de otro funcionario, por lo que puede ser necesario volver a la actividad “asignación” para repetir el proceso. Finalmente puede dar por completa la actuación de la unidad organizativa en el documento, lo que implica generar un “pase” hacia otra oficina con los correspondientes requisitos formales comentados anteriormente para la actividad “Recepción”.

Del análisis anterior, podemos identificar los siguientes actores:

- **Recepcionista**, en actividad “Aceptación”. Es el responsable de chequear los requisitos formales de los documentos para ser aceptados en la unidad administrativa.
- **Asignante**, en actividad “Asignación”. Es el encargado de designar al funcionario que realizará la tarea encomendada a la unidad.
- **Informante**, en actividad “Informante”. Es el funcionario encargado de llevar a cabo la tarea encomendada a la unidad, generando un informe de su actuación.
- **Revisor**, en actividad “Revisión”. Revisa el trabajo realizado por el funcionario encomendado a la tarea que motiva la entrada del documento a la unidad. Decide la eventual salida de la documentación hacia otra unidad organizativa.

Teniendo en cuenta lo anterior, se adaptó el proceso “*pratica*” para representar esta realidad, que llamamos “*proceso genérico*” y que modela las actividades a realizar en cada unidad organizativa de la organización:



Se elimina del proceso la actividad “cataloga” el cual no tiene sentido en la aplicación. Se asocia la aplicación “recepción” a la actividad “Aceptación” la cual simplemente pide al usuario la revisión de los parámetros formales del documento previo a su registro (esto es necesario y no automatizable dada la previsible coexistencia de documentación en papel y electrónica en la operación del sistema). El registro del documento presenta al usuario los datos relevantes del expediente de forma no editable (número, asunto, gestionante, documentos electrónicos y de papel asociados) debiendo este elegir entre aceptarlo o no. En caso de la no aceptación, el sistema deriva automáticamente el expediente a la unidad emisora. Se crea un nuevo rol “Informante” asociándolo a esta actividad.

La actividad “unassigned” y su aplicación permanecen incambiadas, asimilando el rol definido en Paflow; “Amministrazione” al rol requerido por esta actividad.

La actividad “Información” reutiliza la interfaz del proceso “pratica” para la presentación de las asignaciones a los funcionarios, sin embargo la aplicación asociada ha sido modificada para hacer obligatorio la remisión al sistema en forma provisoria de, por lo menos, un documento firmado electrónicamente por el funcionario actuante como condición de cumplimiento de la actividad. Se crea un nuevo rol “Informante” asociándolo a esta actividad.

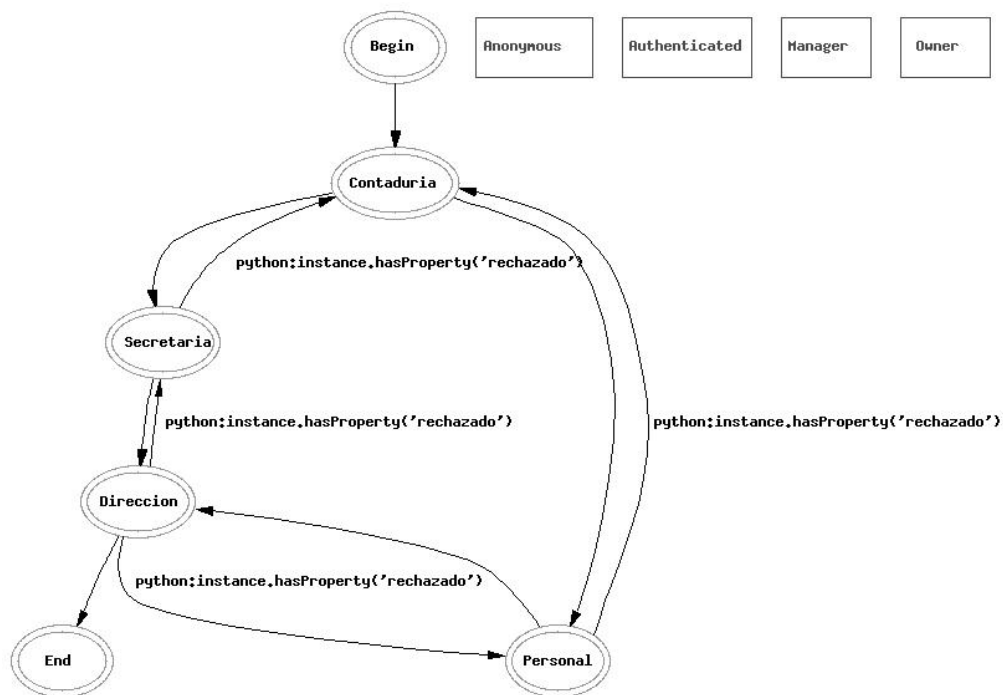
La actividad “Revisión” es quizás, la mas relevante. Posee asociada la aplicación “revisión” la cual una lista de documentos, ingresados en forma temporaria al expediente, para su revisión con las siguientes acciones posibles:

- Reasignar: se rechaza el informe (borrándolo así del sistema) y la instancia pasa a la actividad “unassigned”
- Rehacer: se rechaza el informe, volviendo la instancia al autor del mismo, para su corrección.
- Aceptar y reasignar: se acepta el documento y la instancia pasa a la actividad unassigned para su asignación a otro funcionario para, eventualmente, realizar un nuevo informe.
- Aceptar y Dar pase: Se acepta el documento asociándolo permanentemente a un número de foja, dado automáticamente por el sistema, dentro del expediente. Se pide al funcionario levantar al sistema el “documento de pase” asociado a la oficina a la cual desea enviar el expediente. El destino se elige entre los posibles, dada la definición del workflow que sigue el expediente. El “documento de pase” es un documento electrónico que expresa la voluntad del jerarca de realizar el envío de la documentación a determinada oficina. Se supone conveniente en la implementación del sistema, que estos documentos se encuentren previamente realizados con textos estándar para cada tema y oficina destino según el tipo de expediente que se trate.

Se crea un nuevo rol “Revisor” asociándolo a esta actividad.

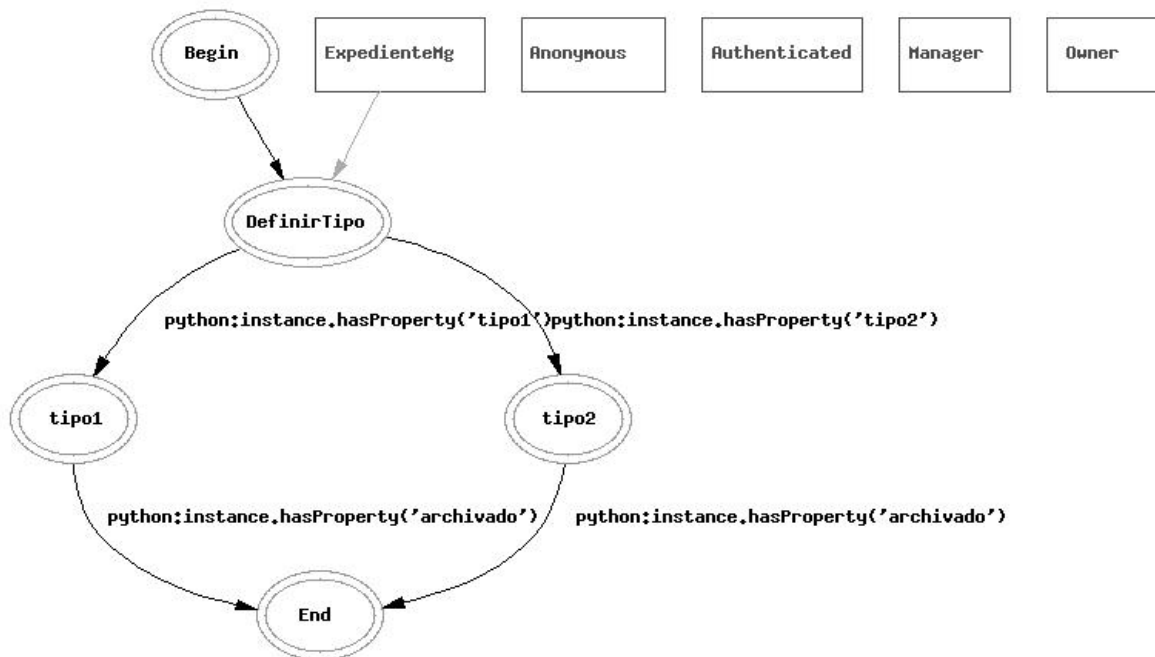
Teniendo este proceso, que llamado “genérico” en la aplicación, se modificó el funcionamiento de la definición de la estructura de la organización de modo que, al ingresar una nueva UO se crea automáticamente un nuevo proceso genérico con el nombre de la misma. De esta manera la definición de procesos según tipos de expedientes se realiza en forma directa. En efecto, para definir un proceso para un determinado tipo de expediente, se procede a crear las actividades de manera usual definiéndolas como “subflows”. Los procesos elegibles como subprocesos son procesos genéricos identificados con la unidad organizativa donde se desarrollan.

Considerando lo anterior, es posible definir, utilizando la interfaz del sistema con OpenflowEditor, procesos para cada tipo de expediente, como el ejemplificado por la siguiente figura:



En él, un hipotético tipo de expediente (llamémosle tipo_prueba) pasa por distintas actividades que se desarrollan en las dependencias del mismo nombre que la actividad. Estas actividades son, a su vez, subprocessos, en un principio idénticos e iguales al “proceso genérico” anteriormente descrito.. Para manejar el caso de no aceptarse un expediente en la unidad se debe incluir lazos con condiciones como las mostradas en la figura anterior.

Finalmente, se reutilizó una vez mas el proceso “pratica” de la siguiente manera:



Este proceso, que llamaremos de “*proceso de vida administrativa*” modela la vida administrativa de un expediente en el ámbito de una organización. Este consiste en la creación del expediente en el sistema, para lo cual se reutiliza la interfaz utilizada para el registro de documentos en entrada, de PAFlow, con el objetivo de generar la “carátula electrónica” del mismo. Se añaden documentos al expediente, escaneando eventualmente los documentos de papel, adjuntando documentos en formato electrónico y ordenándolos numéricamente de manera automática por el sistema. En este momento se crea una instancia del workflow que pasa inmediatamente a la actividad “DefinirTipo”. En esta actividad, dependiendo de la temática del expediente creado, se selecciona una de las actividades “Tipo1” a “TipoN” las cuales deben ser definidas por el parametrizador del sistema como subflows con procesos del tipo ejemplificado anteriormente como “tipo_prueba”. Asociado a la actividad “End” se pide la confirmación explícita de la disposición de archivar el expediente.

4.1.2 Modificaciones a la base de datos

Se determinó que la adecuación del sistema a los requerimientos definidos necesitaba los siguientes cambios estructurales e interpretativos a la Base de Datos del sistema:

Se crean las siguientes entidades:

Expedientes:

Con los atributos
id_expediente integer
id_primer_reg integer
numero_exp integer,
ano integer,
fecha_creacion date,
tiempo_registro date,
estado text,
adjuntado boolean,

Adjuntos:

Con los atributos
id_expediente entero,
id_adjuntado integer,
ano integer,
fecha_adjunto date,
id_funcionario integer,
id_uo integer

desgloces

id_expediente integer,
id_adjuntado integer,
ano integer,
fecha_desgloce date,
id_funcionario integer,
id_uo integer

Registrazione:

Se agregan dos nuevas asociaciones, con las entidades expediente y entita, de forma de asociar los registros generados por cada UO y asociarlos a los respectivos expedientes. En

particular, el registro generado al crear un nuevo expediente en el sistema coincide en los atributos "data_registrazione" y "tempo_registrazione" con los atributos fecha_creacion y tiempo_registro de la entrada correspondiente en la entidad "expediente"

Registrazione_documento:

Ampliamos el campo impronta, que se trataba de un hash para determinar la no modificación del documento al que se hace referencia, para que contenga la firma electrónica del documento, de esta forma mantenemos su sentido original, y además evitamos la posibilidad de rechazo por parte de su autor. Además, se agrega un nuevo campo *firmafuncionario*, de tipo Boolean, que especifica si la firma utilizada corresponde al emisor del documento o al funcionario encargado de autenticarlo.

Se agrega, además, el atributo "num_foja", para generar un ordenamiento entre los documentos del expediente.

Ultimoassegnamento:

En esta tabla debimos incluir el campo *process_id*, ya que pasamos de un esquema en que se tiene un único proceso, a uno en que existen múltiples procesos, pudiendo existir actividades homónimas en procesos distintos.

Pratica.

La tabla *pratica* se asimila a una instancia de la vida de la vida administrativa, asociada a un expediente, independientemente del proceso en que se encuentre el mismo, interpretando el campo *id_reg*, como el identificador del expediente asociado a la instancia dada por *tok_id*.

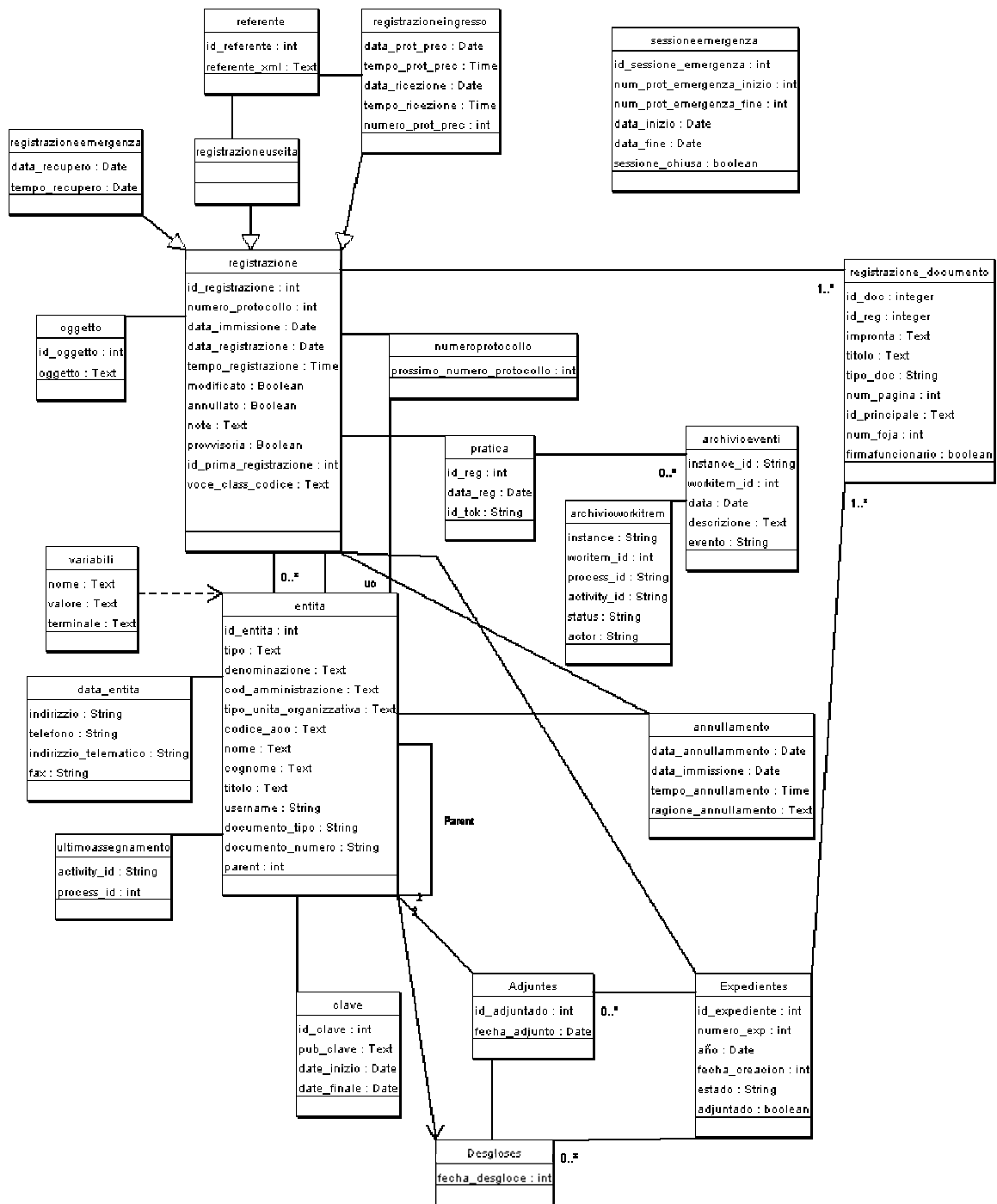
Numero_protocollo:

El número de protocolo pasa, de ser una numeración única para toda la Administración, a representar dos elementos: el número de expediente, en la Administración o el número de registro particular a cada Unidad Organizativa. Para eso se le relaciona con la tabla Entita de forma de interpretar que, si el número de la entidad con la que está relacionado es 1, se representa el número de expediente dentro de la administración local. Si ese no es el caso, se representa el siguiente número correlativo asociado al registro de movimientos de documentos para una dependencia específica. Se agrega además el campo entero *anio*.

Ultimoassegnamento:

Se le agrega el campo *proceso_id*, a los efectos de identificar la actividad, ya que esta entidad en nuestro modelo pasa a ser de tipo débil. Campos: *id_utente*, *activity_id* y *process_id*.

Las modificaciones anteriormente comentadas, llevan a la siguiente estructura para la Base De Datos del Sistema.



Se ha tenido presente, como objetivo de diseño, la reutilización del sistema existente y su adaptación a los requerimientos especificados. En particular se buscó que el uso del sistema permitiera registrar la entrada y salida de documentos en cada unidad organizativa de la administración, de forma de, además de manejar documentos puramente electrónicos, éste brindara un mecanismo de contralor para recepción y envío de documentos en papel .

4.1.3 Roles de la aplicación y su función.

A continuación describimos el conjunto de roles en Yará, la cual consta de algunos roles heredados de la aplicación base aunque con un significado y permisos diferentes a los definidos en Paflow. Esto servirá para describir los actores del sistema y qué pueden realizar con el mismo.

Comenzaremos con los roles ya definidos por Paflow y su significado en la aplicación desarrollada para, posteriormente, describir los roles adicionales creados.

Roles definidos en Paflow.

Nota:

Ya que estos roles son referenciados explícitamente por el código de Paflow en la cual se basa la aplicación desarrollada ("hardcodeados" en la jerga informática), no se han modificado sus nombres.

- Amministrazione: Posee permisos para crear expedientes y definir los rangos de números reservados de expediente para su ingreso en régimen de emergencia (expedientes creados durante un periodo de indisponibilidad del sistema). Actor de la actividad "unassigned" del proceso Genérico. Asigna el trabajo en una unidad organizativa.
- Archivo: Puede acceder al módulo documental del sistema.
- Emergencia: Permiso para iniciar una sesión de emergencia de formación de expedientes.
- Ricerche: Posee el permiso para la buscar registros de movimientos de expedientes y por datos del mismo.

Roles adicionales.

- Diseñador: definición de la estructura interna de la organización (organigrama local). Define UO's y Personas. Define y modifica los workflows de la aplicación (accede a la instancia de OpenflowEditor)
- Recepcionista: es el actor de la actividad "Aceptación". Es el responsable de chequear los requisitos formales de los documentos para ser aceptados en la unidad administrativa.
- ExpedienteMg.: Es el actor de la actividad "DefinirTipo" del workflow "vidaADM"
- Informante: Actor de la actividad "informante" del proceso "Genérico".
- Revisor: Actor de la actividad "revisor" del proceso "Genérico".

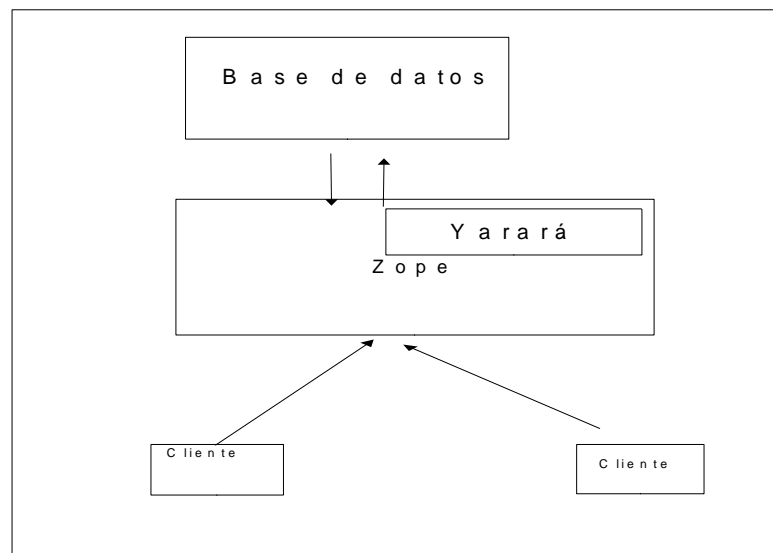
Roles básicos de Zope.

Estos roles son básicos en toda aplicación Zope y no pueden ser modificados.

- Anonymous: Ningún permiso.
- Authenticated: Permiso para cambiar su contraseña, actualizar sus claves de firmado y cambiar su contraseña para proteger el archivo que contiene su clave privada de firma electrónica. Además poseen acceso, desde el menú principal, a su worklist correspondiente según el conjunto de roles del usuario.

Se define en la aplicación un único usuario inicial con los roles “Manager” y “Owner” con nombre de usuario “admin” y password “Yarara”. Como “Manager” este usuario posee todos los permisos sobre todos los objetos de la aplicación.

4.1.4 Esquema de Seguridad en Yarará



El esquema de seguridad, cubre todos los aspectos de intercambio entre las partes del sistema, es decir:

1. La comunicación del navegador del cliente con Zope
2. Acceso desde Zope a Yarará.
3. Interacción de Yarará con el motor de workflow.
4. Comunicación del sistema con la base de datos.
5. Garantía de no modificabilidad de los datos

Como característica general, diremos que los permisos de acceso son manejados en prácticamente todos los casos, por los mecanismos de Zope, por lo que es imperativo un correcto manejo de los permisos sobre éste, muy especialmente los de administración. A los efectos de explicar cada punto, a continuación, lo haremos por separado:

4.1.4.1 Comunicación Navegador – Zope

Este aspecto de la seguridad se asegura utilizando ssl en este paso, de esa forma se garantiza la identidad del servidor y se impiden ataques del tipo „monkey in the middle“ (debiéndose registrar los certificados del servidor en los clientes). Además, imposibilita el uso de “sniffers“ de los datos en tránsito, por ser enviados estos encriptados con un estándar aceptado a nivel internacional (Con una implementación ampliamente utilizada como es la de OpenSSL).

Además, como es lógico, todos los elementos criptográficos debidos al cliente (y sobre todo, al usuario) son realizados localmente en el cliente, sin enviar nunca las claves privadas al servidor. Esto tiene dos consecuencias directas: primero, como ventaja, se gana en seguridad, ya que es mucho más difícil falsear las firmas (incluso para los administradores del sistema) y segundo, como desventaja, exige clientes más potentes, que soporten el ambiente java, utilizado en ciertos aspectos de esta funcionalidad. En el punto 5.2.4.1.1 del Informe Técnico detallamos el applet encargado de la firma digital.

4.1.4.2 Acceso desde Zope a Yará

Una vez que el cliente se ha conectado con Zope, debe autenticarse con el sistema, para eso se utilizan, en esta primera versión del sistema, pares usuario-contraseña (aunque es posible utilizar todos los medios de autenticación soportados por Zope, por ejemplo: LDAP, NIS o certificados); De ésta forma, como ya se explicó en el apartado correspondiente a Zope, se mantiene un manejo capilar de los permisos, asimilando roles de Zope a roles dentro de las Unidades Organizativas, por poner un ejemplo, las personas que cumplen con las tareas de administración, tal como se relatan en los casos de uso, deben tener el rol de Zope "Adminitrazione", sin embargo, en la medida que la parametrización necesite la definición de actividades (y los roles encargados de realizarlas) es posible aumentar el número de actividades y roles. Así, se garantiza la seguridad de acceso a lo almacenado en Zope (incluyendo toda la base documental del sistema) y la lógica correspondiente. De todas formas, se mantiene información en la base de datos que garantiza la integridad del área Documental del Sistema (este aspecto se ampliará en el subpunto 4.1.4.5 de este informe).

4.1.4.3 Interacción de Yará con el motor de workflow (Openflow).

La seguridad en este marco depende, como en el punto anterior, del marco de seguridad brindado por Zope, es decir, a cada actividad se le asignan roles que la pueden cumplir y/o que pueden asignar las instancias de esa actividades a usuarios o roles específicos.

4.1.4.4 Comunicación del sistema con la base de datos

La comunicación con la base de datos es realizada por medio de un usuario único (visible solo a los administradores de zope), lo que aparece como un problema, ya que con un mismo usuario (utilizado indirectamente por todos) es posible modificar todos los datos de la aplicación, por lo que es recomendable una política de respaldos frecuentes. Sin embargo, está política del manejo de permisos para el sistema hace que estos se manejen de forma centralizada, lo que facilita la administración. Por otra parte, se protege este usuario de dos formas, asignando permisos de acceder a los parámetros del objeto de conexión solo a administradores del sistema y restringiendo los permisos de ejecución de los métodos que lo utilizan. .

4.1.4.5 Garantías de no modificación de los datos

Como se hizo notar en el anterior subpunto, los datos que se guardan en la base de datos, son registrados con un único usuario, por lo que se hacen necesarios otros controles sobre la integridad de los mismos. Para esto, se guardan campos de resumen en algunos registros. Actualmente, este método es usado solo en la parte documental del sistema (que consideramos la de mayor importancia), teniendo , como ya se explicitó en el esquema de la base de datos, cada entrada de la tabla de registro de documentos, dos campos de contralor: un campo de timestamp (obtenido por medio de la relación con la tabla *Registrazione*), y uno de firma electrónica (incorporando el "timestamp" antes nombrado, encriptado con la clave del sistema), generada, en forma local al cliente utilizando la librería Cryptix (y el applet desarrollado sobre esta librería para nuestro sistema) con la clave privada del usuario que genera el documento (pudiendo ser la del propio generador del contenido o la del funcionario que certifica la autenticidad del mismo). De momento la firma, es generada utilizando el algoritmo RIPEMD, de 160 bits, como hash y RSA, de 1024 bits, para encriptación (estas claves de encriptación son utilizadas además para este único fin).

NOTA: Este aspecto del esquema de seguridad puede ser mejorado, por ejemplo, utilizando claves de encriptación de mayor largo o cambiando los algoritmos utilizados, pero los elegidos se encuentran entre los considerados más seguros del mercado. Además se podrían

generar varias conexiones distintas a la base de datos, cada una con un perfil de permisos distinto, por ejemplo, usuarios separados para registro del log de eventos, consulta de datos o alta de los mismos, etc. pero sin embargo se decidió que no era esencial (aunque no difícil de lograr) y significaba mayor peso sobre el servidor (ya que se deben mantener 4 o 5 conexiones permanentes distintas, entre Zope y la base de datos) y distracción de recursos en la implementación más necesitados en otros puntos del sistema. Por otra parte, es posible aumentar los tipos de registros que cuentan con campos de resumen, pero nuevamente eso se logra con un mayor gasto de recursos, en la implementación primero y luego en el funcionamiento diario del sistema.

5 FUNCIONALIDADES BRINDADAS.

La aplicación desarrollada posee las siguientes características primordiales.

Diseño de Procesos.

Yarará, mediante la conjunción del motor de Workflow Openflow y su editor OpenflowEditor brinda la posibilidad de diseñar procesos asociados a cada Clase de Expediente y su ruta dentro de la organización. La circulación del expediente en la organización estará gobernada por el proceso diagramado mediante OpenflowEditor. Cada uno de los pasos que recorre el expediente está supervisado por el motor de Workflow.

Registro de Movimientos entre Unidades Organizativas.

La creación y anulación de expedientes, así también como su entrada y salida de las unidades organizacionales que recorre en su substanciación son registradas por Yarará en la Base de Datos del sistema. Se construye así, un conjunto de datos que "cuentan la historia" del expediente registrando sus tiempos de estadía en cada unidad participante en su proceso. Se puede, si se desea, imprimir los datos del registro (de creación, entrada o salida) generados por el sistema de forma de servir como una constancia de la realización del mismo. En cada unidad interviniente se puede aceptar o rechazar (por algún motivo formal) la entrada de un expediente siendo el comportamiento del sistema pedir al usuario los motivos del rechazo y redireccionando el mismo a la unidad que lo envió. Se brinda la posibilidad de que un jefe corrija un informe de un subordinado que considere desacertado o erróneo, sin dejar rastros en el expediente de ello.

Manejo Documental.

Además de la seguridad y el ahorro que el expediente electrónico presenta, la facilidad con que se lleva a cabo la incorporación de documentación nueva al mismo, ya sea de origen físico a través de la digitalización de la misma, o de origen propiamente digital constituye una característica predominante en Yarará.

Se posibilita que los documentos físicos se puedan digitalizar a través del uso de scanners en el momento de su incorporación al expediente electrónico en las unidades que intervienen en su substanciación. A su vez, documentos de diferentes formatos, como ser Texto plano, HTML / XML, PDF, Postscript, Microsoft Word® (en formatos 6.0/95, 97 y 2000), Microsoft Excel®, Microsoft Powerpoint® pueden ser incorporados al expediente e indexados a texto completo. Quien recibe un expediente para su actuación y debe llevar a cabo su estudio, necesitará disponer en su computadora simplemente de un navegador de Internet que soporte cookies, con el plug - in Java y los visores necesarios para el formato que se adopte por los administradores del sistema. Podrá analizar la documentación, e incluir su actuación. En caso de tratarse de expedientes totalmente digitalizados un usuario puede intervenir en la substanciación de un expediente independientemente de su ubicación, ya sea en su casa o desde cualquier lugar del mundo a través de Internet, sin comprometer la seguridad del sistema por eso. La funcionalidad incluye la firma electrónica de documentos y actuaciones con el uso de certificados expedidos por la aplicación, que actúa como Autoridad de Certificación de la organización.

Definición de la estructura de la organización

Yarará gestiona el organigrama de la organización y la seguridad a nivel de autenticación de los usuarios. Para ello utiliza el potente mecanismo de seguridad propio de la aplicación sobre la cual se asienta: Zope. Una vez identificado el miembro de la organización, el sistema le aplica el perfil de seguridad que le corresponde y habilita los permisos adecuados. De tal manera el acceso

al expediente se realiza en forma controlada desde cualquier sistema de computación del organismo.

Seguridad Operacional

El Expediente Electrónico constituye un mecanismo de gestión que incorpora un importante grado de mejora en la seguridad frente al expediente tradicional. El manejo controlado y respaldado del contenido de un expediente electrónico imposibilita el robo de los mismos, la sustracción de folios y la falsificación o alteración de sus partes. Si bien el riesgo de acceso desautorizado a través de los sistemas informáticos se compara con el del usuario que accede en forma desautorizada al expediente físico, el sistema electrónico permite conservar un registro de los accesos, auditar la seguridad, y en definitiva, implantar prácticas de seguridad centralizada, más eficientes y económicas que las determinadas por el expediente tradicional que se distribuye a través de todas las oficinas del organismo.

La firma digital asegura a quien accede un documento que el mismo ha sido firmado por quien el documento declara: si alguien altera el documento, automáticamente la firma digital se invalida.

Seguridad del Almacenamiento

El Expediente Electrónico permite llevar a cabo el almacenamiento de miles o cientos de miles de legajos en pocos metros guardados, mediante el uso de discos ópticos o cintas de computación, obteniendo de esta forma un mecanismo seguro y confiable de conservar los mismos, y recuperando para la organización los centenares de metros cuadrados que se dedican hoy en día a los almacenamientos de expedientes tradicionales. Los riesgos representados por roedores, inundaciones de sótanos, fuegos o la propia imposibilidad de acceso, se ven eliminados o fuertemente restringidos.

5.1 Expedientes

5.1.1 Inicio y anulación de expedientes

El inicio de expedientes puede ser realizado en forma centralizada o descentralizada, según la forma de trabajo del organismo, por aquellas personas que están autorizadas para realizar esta tarea.

Los expedientes se agrupan por "tipo" o "tema" el cual tiene asociado una secuencia de unidades que habitualmente deban participar en la substanciación del mismo y que es definido solo por funcionarios habilitados para esa acción. La definición de los tipos de expediente a tratar, constituye un aporte potencial para la racionalización de los trámites, y es una valiosa oportunidad para unificar criterios y simplificar procedimientos al definir rutas a seguir para cada tema.

El sistema contempla el tratamiento expedientes de origen interno, manejando la numeración en forma automática.

Se requieren además, en el momento del inicio, una serie de datos que permiten identificar al documento: asunto, titular (persona física, jurídica u organismo) que da origen al expediente. A su vez, según el tipo de titular, se completan datos identificatorios. En todos los casos se ingresa la dirección de notificación, teléfono, fax, e-mail. Estos datos son completados en forma automática si el titular ya existe, es decir, si tiene expedientes anteriores, ya que el sistema registra en un "directorio" los datos del iniciador del expediente permitiéndose la búsqueda en el mismo y su actualización.

No se dan bajas físicas de expedientes, de forma de evitar que existan números de expedientes perdidos sin saber el motivo, permitiéndose sí anular documentos que se encuentren en fase de generación, es decir que no hayan tenido movimientos, indicándose en este caso en las observaciones, el motivo de la anulación el documento.

De acuerdo a la situación en que se encuentra el expediente, el sistema le asocia en forma automática un estado: Iniciado, Archivado o Anulado.

El sistema brinda asimismo la posibilidad de imprimir una constancia de inicio de expediente a efectos de entregar al interesado así como constancias de entrada y salida de las unidades intervinientes.

5.1.2 Seguimiento de expedientes

El sistema permite consultar todas las unidades y organismos por los que ha pasado un expediente, así como la fecha de entrada y salida de cada unidad.

5.1.3 Ingreso de Informes

El sistema permite el ingreso de informes permitiendo su indexación a texto completo en diversos formatos; se soportan Texto plano, HTML / XML, PDF, Postscript, Microsoft Word® (en formatos 6.0/95, 97 y 2000), Microsoft Excel®, Microsoft Powerpoint® o la incorporación de documentos escaneados que se agregan al expediente, permitiendo la consulta e impresión de los mismos.

Como paso necesario para el ingreso de informe el sistema solicita al funcionario actuante los datos necesarios para firmar electrónicamente los documentos a incluir en un expediente.

5.1.4 Consulta de Expedientes

El sistema permite la consulta de expedientes por origen, por número, por tema, por unidad actual, por fecha de creación, por titular y / o por palabras, partes de palabras en el texto de los documentos asociados. Se permite también la búsqueda de movimientos de expedientes entre diferente unidades por la fecha del movimiento y por el número de éste, el cual es interno a cada unidad.

5.1.5 Ingreso de movimientos de expedientes

El envío y recepción de expedientes entre unidades se realiza a través del sistema, en forma descentralizada por las unidades que intervienen en el movimiento, quedando registrada automáticamente la fecha en que se produce.

5.1.6 Asignación a responsables

Una vez ingresado el expediente a una unidad, la persona encargada de su ingreso asignará el mismo a un responsable para su tratamiento.

5.1.7 Lista de Trabajo.

El sistema despliega según los permisos que posea el funcionario y la unidad organizacional donde se encuentra definido, dos listas mostrando sus tareas pendientes y sus tareas aceptadas, respectivamente.

5.1.8 Otros Documentos

El sistema permite también el ingreso de otros documentos - oficios, memorándums, etc., permitiendo, para los formatos mencionados anteriormente, su indexación por texto completo.

5.2 Definición de la estructura organizacional.

Yará permite la creación y edición de los diversos elementos de la organización (unidades organizativas y funcionarios) mediante su interfaz a los funcionarios habilitados para esta acción. La creación de una nueva unidad organizativa ocasiona que el sistema asocie de forma automática un proceso básico, denominado "*genérico*" el cual puede ser editado en sus componentes fundamentales (actividades, roles asociados a éstas y transiciones) en forma gráfica mediante el componente integrado OpenflowEditor.

5.3 Definición de Workflows asociados a Expedientes.

El sistema permite, al diseñador del sistema, la creación de workflows para expedientes que, por su temática, requieran un flujo propio dentro de la organización creando, mediante OpenflowEditor y la interfaz propia de Openflow, las actividades del proceso a las cuales se pueden asociar los procesos definidos para las unidades intervinientes como subworkflows. Los workflows de expedientes definidos son mostrados, como paso final en el proceso de creación de un expediente, para que funcionarios con los permisos adecuados puedan determinar el proceso que seguirá el mismo dada su temática.

6 CONCLUSIONES Y PASOS FUTUROS

Podemos concluir que se ha desarrollado una aplicación que cumple los aspectos fundamentales requeridos a este tipo de sistemas por la normativa comentada en el punto [2.1.1.](#) En particular, los dos aspectos claves logrados, es decir, tener la posibilidad de definir procesos que deben llevar expedientes relacionados por su temática (*racionalización administrativa*) y el nivel de seguridad logrado, requisito fundamental debido al carácter legal que poseen los documentos manejados, nos habilitan a creer que se logró implementar una base de software sobre la cual se puede construir una solución que cumpla cabalmente la totalidad de los requerimientos acordados con la parte cliente.

Como pasos futuros identificamos primeramente la implementación de las siguientes características que, por limitaciones de tiempo no se han podido lograr en esta primera versión del sistema, a saber:

- Implementación de un mecanismo de alarmas y manejo automático de plazos para las etapas de los procesos.

Si bien no se encuentra implementado, existe la posibilidad de incluir dentro de la lógica de las aplicaciones asociadas a cada actividad, el seteo de un alarma, por medio del producto Zope **Xcron** (de funcionalidad análoga al demonio cron de ambientes Unix®); y su deshabilitación al final de la actividad, de forma tal, que si no se terminara antes de vencido este plazo, se instruyera al motor de workflow para efectuar la acción correctiva necesaria.

- Implementación de herramienta de definición de días hábiles:

Esta funcionalidad, al no tener implementado el punto anterior, pierde su sentido y es por eso que no se la incluyo.

- Unión y desgloses de expedientes:

A pesar que, al plantear los cambios necesarios en la base de datos original, se tuvo en mente cumplir este requerimiento, los problemas surgidos en la implementación de la firma electrónica y el consecuente retraso que sufrió este proyecto, hicieron que se optara por obviarlo. Sin embargo pensamos que, dado que existe la infraestructura necesaria en la base de datos para registrar estas acciones, su inclusión en el sistema debe ser relativamente sencilla.

Como elementos deseables no incluidos en los requerimientos se cuentan, por ejemplo los siguientes:

- Implementación de ocultamiento de documentos de carácter confidencial.
- Creación de distintos perfiles de acceso a la base de datos, con permisos acordes.
- Implementación de un protocolo de transferencia de Expedientes electrónicos, que permita interoperabilidad entre sistemas semejantes.
- Inclusión de herramientas más amigables de diseño de Interfaz de usuario en la definición de formularios de ingreso de datos. Para facilitar la labor de diseño de procesos.

Conclusiones.

Como conclusión se puede señalar la construcción de un sistema que cumple con los requisitos básicos señalados por la regulación legal vigente, el cual ha sido desarrollado en forma cabal siguiendo la filosofía de software libre, logrando un producto que, se supone, no existía en ese ámbito. Dicho esto debido a que la aplicación base de este sistema (única encontrada) controla la entrada y salida de documentación de en forma global a una organización, pero no los

pasos internos de esa documentación en la misma. Una reseña de las organizaciones que hacen uso de la infraestructura utilizada, Zope, se encuentra en el punto 3.1.1, lo que da idea de su grado de madurez y seguridad. PAFlow, por su parte, se cuenta como uno de los integrantes de ASWAD (Agent-Supported workflow in Public Administration) en <http://www.aswad-project.org>, el cual es un proyecto de software libre, financiado por la Comunidad Europea a través de su programa IST (Information Society Technologies) en su apartado "Essential Technologies and Infrastructure".

El hecho de utilizar (y crear) software libre, permite brindar:

- **Transparencia:** El hecho de tener acceso al código fuente permite auditar y garantizar el mismo.
- **Costo:** La solución no conlleva costo de licenciamiento, ni en si misma, ni en la plataforma necesaria. Además al no atarse a un proveedor, se permite la contratación de servicios de mantenimiento o el mantenimiento interno según sea más conveniente.
- **Seguridad:** Al contar con el código de la aplicación y de las herramientas de criptografía que esta utiliza, y su implementación de los algoritmos de seguridad se permite asegurar, en la medida de los estándares vigentes en cada momento, este aspecto de la aplicación y por tanto de la organización.
- **Independencia Tecnológica:** No se depende de una organización particular, que imponga en forma unilateral la tecnología de una determinada plataforma informática.

7 APÉNDICE A – BIBLIOGRAFÍA

1. CNIPA (EX AIPA) -Linee guida alla realizzazione dei sistemi di protocollo informatico e gestione dei flussi documentali nelle pubbliche amministrazioni (GEDOC 2) (<http://www.cnipa.gov.it>)
2. "Regolamento per la tenuta del protocollo amministrativo con procedura informatica" - (http://www.cnipa.gov.it/site/contentfiles/00120600/120641_dpr428_98.pdf) - 1998
3. All Zope Howto's (www.zope.org/Documentation/How-to)
4. "Criptografía y Seguridad en Computadores"- Manuel J. Lucena López - Universidad de Jaén <http://www.di.ujaen.es/~mlucena>, <http://www.kriptopolis.com> .
5. CPL - Cryptix Public License – (CD de proyecto) - The Cryptix Foundation Limited - 1995
6. DevGuide (<http://www.zope.org/Documentation/Books/ZDG/current>)
7. Documentazione del codice Luigi Palopoli Tommaso Cucinotta. ReTiS Lab - Scuola Superiore S. Anna. 26 aprile 2001. (www.pafLOW.it/Project/DocumentazioneCodice_pdf)
8. Frequently Asked Questions (FAQs) - The Cryptix Foundation Limited(c) - (<http://www.cryptix.org/docs/faq.html> y <http://www.cryptix.org/old/cryptix/FAQ.html>) - 1999
9. Glosario Semántico del UML Versión 1.0 - 13 de Enero de 1997 Copyright © 1997 Rational Software Corporation. De la traducción al Español : Copyright © 1997 Baufest
10. GNU GPL-General Public License (Licencia Pública General) - (CD de proyecto) Free Software Foundation - Richard Stallman – 1991
11. GNU LGPL- Lesser General Public License (Licencia Pública Menos General) - (CD de proyecto) Free Software Foundation - Richard Stallman – 1991
12. JHBCI (TM), OpenSource HBCI Toolkit for Java(TM) (<http://www.jhbcI.de/>) - Uwe Günther - 2003
13. "El Nuevo Procedimiento Administrativo" Secretaría de la Presidencia de la República – ProNaDe (Programa Nacional de Desburocratización) Montevideo, 1991
14. Introducción a XML en Castellano - Alfredo Reino Romero - <http://www.ibium.com/alf/xml.index.asp>
15. La definición de Software Libre - Free Software Foundation - Richard Stallman (<http://www.gnu.org/philosophy/free-sw.es.html>) -2002
16. Manuale dell'utente e dell'amministratore del software PAFLOW 1.0 Luigi Palopoli Tommaso Cucinotta ReTiS Lab - Scuola Superiore S. Anna Versión manual: 1.1 www.pafLOW.it/Project/ManualeUtente_pdf
17. "Núcleo mínimo del sistema de protocolo informático: análisis de los requisitos y proyección de la máxima". Luigi Palopoli - Tommaso Cucinotta ReTiS Lab - Scuola Superiore S. Anna 13 diciembre 2000. www.pafLOW.it/Project/Requisiti_pdf

18. Openflow Tecnical Documentation. www.openflow.it/EN/Documentation/openflowdocs.html
19. "Procedimiento Administrativo Electrónico" - Dr. Ruben Correa Freitas – Compilador. Autores Varios. ONSC - Marzo 1998
20. PostgreSQL 7.1 Documentation -The PostgreSQL Global Development Group (www.postgres.org/docs/7.1/static/postgres.html) - 2001
21. Python Documentation, Release 2.1.3 April 8, 2002 - Guido van Rossum y otros. www.python.org/doc
22. Respuesta a Microsoft - DR. EDGAR DAVID VILLANUEVA NUÑEZ (<http://www.gnu.org.pe/rescon.html>) - 2002
23. Varias licencias y comentarios sobre ellas -Free Software Foundation - Richard Stallman (<http://www.gnu.org/philosophy/license-list.es.html>) - actualizado: 2003
24. Workflow: An Introduction. Rob Allen, Open Image Systems Inc., United Kingdom Chair, WfMC External Relations Committee (http://www.wfmc.org/standards/docs/Workflow_An_Introduction.pdf) - 2001
25. Workflow Management Coalition Terminology & Glossary Document Number WFMC-TC-1011 Document Status - Issue 3.0 (http://www.wfmc.org/standards/docs/TC-1011_term_glossary_v3.pdf) -Feb 99
26. Workflow Management Coalition. The Workflow Reference Model Document Number TC00-1003 Document Status - Issue 1.1 19-Jan-95. Author: David Hollingsworth (<http://www.wfmc.org/standards/docs/tc003v11.pdf>) - 1995
27. Workflow Management Coalition Workflow Standard – Interoperability – (<http://www.wfmc.org/standards/docs/IneropChallPublic.PDF>) - 1999
28. Workflow Process Definition Interface - Workflow Management Coalition – (http://www.wfmc.org/standards/docs/TC-1025_10_xpdl_102502.pdf) - 2002
29. Zope Administrator Guide. Copyright © Digital Creations. www.zope.org/Documentation/Guides/ZAG
30. Zope Book. Amos Latteier and Michel Pelletier. Copyright © 2000 by New Riders Publishing. www.zope.org/Documentation/Books/ZopeBook/current

8 APÉNDICE B: GLOSARIO

- A -

AC: Autoridad de Certificación. En inglés CA (Certificación Authority).

AIPA: Autorità per l'Informatica nella Pubblica Amministrazione. Organización estatal Italiana encargada de dictar normas técnicas normativas para los sistemas informáticos a utilizar en el ámbito de Administraciones Públicas de ese país.

AND-Join: Punto en un workflow donde dos o más actividades, ejecutándose en paralelo, convergen en una única línea de control.

AND-Split: Punto del workflow donde una línea única de ejecución se divide en dos o más líneas de ejecución paralelas, permitiendo que múltiples actividades sean ejecutadas simultáneamente.

AHO: Área Organizativa Homogénea. Conjunto de unidades organizativas de una administración que comparten una metodología única referente al tratamiento de su documentación.

Actividad de Workflow: Descripción de un conjunto de trabajo que conforma un paso lógico en un workflow. Una actividad puede ser manual (no soporta automatización) o una actividad automática. Una actividad de workflow requiere recursos humanos o computacionales para su ejecución; cuando se requiere un recurso humano la actividad se asigna a un Participante de workflow.

Administración de certificados: proceso que incluye, pero no está limitado, a la emisión, verificación, almacenamiento, distribución, publicación y revocación de certificados.

Administración Externa: Organismo externo desde el punto de vista administrativo del organismo del que se trate.

Algoritmo: Transformación matemática que partiendo de un texto plano lo cambia a datos ilegibles cifrados.

Amenaza: Circunstancia o evento que puede causar una denegación de servicio o una destrucción, revelación no autorizada o modificación de datos.

Auditoria: Procedimiento usado para verificar que se están llevando a cabo controles en un sistema de información y que estos son adecuados para los objetivos que se persiguen. Incluye el análisis de las actividades para detectar intrusiones o abusos dentro del sistema informático.

Autenticidad. Característica por la que se garantiza la identidad del usuario que origina un mensaje o transacción, es decir conocer con certeza quién envía algo.

Autenticación: Proceso utilizado para confirmar la identidad y autenticidad de una persona o probar la integridad de información específica.

Autenticación de mensajes: Proceso de autenticación que incluye la identificación de la fuente del mensaje y la verificación de que no ha sido modificado o reemplazado en el tránsito del mismo.

Autoridad Certificadora (AC). Es una tercera parte de confianza que acredita la conexión entre una determinada clave pública y su propietario. La confianza en la AC supone la confianza en los certificados que emite.

Autorización: Las claves y el resto de los elementos de seguridad necesarios, otorgados por la Entidad Pública de Certificación, que identifican al usuario en las transacciones EIT.

- B -

- C -

CRL: Certificate Revocation List. Listas de Certificados revocados. Definido en la norma X.509.

Certificado: Es un documento electrónico en el cual la Autoridad de Certificación (AC) acredita mediante su firma digital que la clave pública pertenece a su propietario. También se denominan Certificados de usuario y de clave pública.

Cifrado: Proceso utilizado para transformar un texto a una forma ininteligible de manera que los datos originales no puedan ser recuperados (cifrado de una vía) o sólo puedan ser recuperados usando un proceso inverso de descifrado (cifrado de dos vías).

Clave de sesión / Clave de cifrado: Clave utilizada en algoritmos simétricos para cifrar y descifrar los mensajes en una única sesión.

Clave Privada: Clave personal que no es conocida por el resto de los usuarios y que es utilizada para crear firmas digitales y, dependiendo del algoritmo, para descifrar mensajes cifrados con la correspondiente clave pública.

Clave Pública: Clave de usuario que es conocida por el resto de los usuarios y que es utilizada para verificar firmas creadas con su correspondiente clave pública. Dependiendo del algoritmo, se usa para cifrar mensajes que pueden ser descifrados con su correspondiente clave privada.

Clave Simétrica: Clave única usada en los algoritmos simétricos tanto para cifrar como para descifrar un mensaje.

Claves de autenticación o de firma: Par de claves (pública y privada) que se utilizan dentro de la infraestructura de clave pública para garantizar la autenticidad de emisor y receptor, así como la integridad de las comunicaciones establecidas.

Claves de soporte de confidencialidad: Par de claves (pública y privada) que se utilizan dentro de la infraestructura de clave pública para intercambiar con seguridad las claves de sesión.

Compromiso: Violación (o sospecha de violación) de una política de seguridad, en la cual puede haber ocurrido una revelación no autorizada de información crítica.

Condición de Transición: Expresión lógica que debe ser evaluada por el Motor de Workflow para decidir la secuencia de ejecución de actividades en un proceso.

Confidencialidad: Característica técnica y administrativa que previene contra la comunicación y divulgación no autorizada de cualquier información referente a las transacciones EIT, ya sea en su inicio, durante su ejecución o conclusión.

Control de acceso: Los elementos e instrumentos de salvaguarda necesarios para garantizar a los usuarios la seguridad de los datos y demás activos del sistema de comunicación y sus aplicaciones EIT.

Criptografía: Ciencia matemática usada para asegurar la confidencialidad y autenticidad de datos mediante el proceso de reemplazarlos por una versión transformada. Esta puede ser reconvertida a la forma original sólo por alguien que posea el algoritmo criptográfico y las claves adecuadas. También es el nombre que se le da a la disciplina que incluye los principios, medios y métodos

para transformar los datos con intención de ocultar la información y prevenir la modificación y los usos no autorizados de la misma.

CSP: Cryptographic Service Provider. Paquete (o conjunto de paquetes) que suministran una implementación concreta de un subjuego de aspectos de criptografía del API de Seguridad del JDK.

- D -

DAP: Directory Access Protocol. Protocolo de acceso al directorio X509.

DES: Data Encryption Standard. Algoritmo de cifrado.

DIB: Directory Information Base.

DSA: Directory System Agent definido en la norma X.509. También es Digital Signature Algorithm del NIST.

DTML: Document Template Markup Language. Lenguaje de scripting del lado del servidor basado en tags propio del servidor Zope.

Desglose de Expedientes: Acto por el cual un expediente unido a otro retoma su vida administrativa autónoma.

Desencriptado: Operación que obtiene un texto original a partir de un texto cifrado.

Disponibilidad: Característica técnica y administrativa que previene contra la denegación no autorizada de acceso a la información.

Dispositivo de creación de firma: Conjunto de datos originales, tales como códigos o claves criptográficas privadas, o dispositivo físico singularmente configurado para la creación de firmas electrónicas por el signatario

Dispositivo de verificación de firma: Conjunto de datos originales, tales como códigos o claves criptográficas públicas, o dispositivo físico singularmente configurado para la verificación de la firma electrónica.

- E -

EDI: Electronic Data Interchange.

EIT: Electrónicas, Informáticas y Telemáticas.

EPC: Entidad Pública de Certificación

Emisión de certificados: Acciones llevadas a cabo por una AC para crear un certificado y comunicárselo al usuario que lo solicitó.

Entidad Emisora: Nombre con el que los navegadores de Microsoft designan a una AC .

Entidad Pública de Certificación Es el organismos público que realiza las funciones de una Autoridad de Certificación, en el ámbito de la administración pública española, directamente o en colaboración con otros órganos administrativos u organismos públicos.

Expediente: Un expediente es una secuencia numerada de documentos que reúne la información de actos administrativos de un determinado asunto.

Expiración de un certificado: Fecha y hora especificadas en un certificado cuando termina el periodo operativo del mismo.

Extensión de un certificado: Campo añadido a un certificado para guardar información adicional.

- F -

FAQ: Frequently Asked Questions

Firma digital: Es un documento electrónico que se genera como resultado de aplicar una función matemática al documento a firmar y posteriormente cifrar el resultado con la clave privada del firmante. Es utilizada por el emisor de un mensaje para identificarse.

Firma electrónica: Véase Firma digital

Firmante de certificados: Nombre con el que los navegadores de Netscape designan a una AC

Función de una sola vía: Función que tan sólo se puede calcular o realizar de una forma , o bien que su inversa es difícil de obtener.

Función de Hash: Función matemática que asocia valores de un dominio extenso a uno de menor rango. Las asociaciones se hacen aparentemente de forma aleatoria. Se utilizan para traducir un mensaje de forma que partiendo del mismo mensaje y función se obtenga siempre el mismo resultado, sea imposible reconstruir el mensaje original a partir del traducido y, además, sea imposible encontrar dos mensajes distintos que den el mismo resultado con la misma función.

- G -

GPL: General Public License.

Gestión de certificados: Administración de certificados.

- H -

HTTPS: Dirección de internet segura.

- I -

IP: Internet Protocol.

ISO / IEC: Organización Internacional de Normalización.

ISO 7816: Norma para la fabricación y utilización de tarjetas inteligentes.

Identificador único de certificado: Valor que identifica unívocamente a un certificado.

Infraestructura de clave pública: Conjunto de mecanismos criptográficos de clave pública basados en la existencia de dos claves (una pública y otra privada) que se utilizan para garantizar la identidad del usuario, la confidencialidad y la integridad de la información transmitida.

Instancia de Workflow: Representación de un proceso incluyendo sus datos asociados. Cada instancia representa un hilo separado de ejecución de un proceso que puede ser controlado independientemente y que posee su propio estado interno e identidad visible externamente, que

puede ser usado para manejar la registraci3n o recuperar los datos de control relativos a la ejecuci3n del proceso.

Integridad: Característica que asegura que el mensaje o comunicaci3n que se recibe llega tal y como se envi3 por el remitente, detectando f3cilmente posibles modificaciones que pudieran haberse producido durante la transmisi3n.

Interoperabilidad: Véase Certificaci3n cruzada

IP: Protocolo Internet. Tecnología que permite el movimiento de informaci3n de una red a otra cuando así se necesita.

- J -

JCE: Java Cryptography Extensi3n. API para encriptaci3n, intercambio de claves, y c3digo de autenticaci3n de mensajes (MCA). Junto con el JCE y los aspectos de criptografía del JDK proporciona un completo API de criptografía independiente de la plataforma. El JCE es una extensi3n incluida a partir de JDK 1.3.

JCA: Java Cryptographic Architecture. Marco de trabajo para acceder y desarrollar funcionalidades de criptografía para la plataforma Java.

JDK: Java Development Kit.

- K -

- L -

LDAP: "Light DAP". Est3ndar derivado del X500 pero no tan completo.

- M -

Mensaje: Representaci3n digital de una informaci3n.

Motor de Workflow: servicio de software que brinda el entorno de ejecuci3n para una instancia de Workflow.

- N -

Navegador: Es un programa realizado para poder buscar, consultar, imprimir, etc. La informaci3n disponible en internet.

No repudio: Mecanismos que proporcionan garantías del origen de un mensaje para proteger al emisor contra la negaci3n de recepci3n por parte del receptor.

- Ñ -

- O -

OR-Join: Punto en un workflow donde dos o m3s actividades convergen en una única actividad com3n como siguiente paso en el workflow

OR-Split: Punto en un workflow donde una l3nea de control toma una decisi3n sobre que alternativa seguir cuando se tienen definidas bifurcaciones.

On-line: Realizar algo de forma inmediata.

Organigrama: estructura jerárquica de unidades de una Organización.

- P -

Partes confiantes: Personas físicas o jurídicas, registradas o no en la AC, que confían en los datos de un certificado o en la firma digital de ese certificado.

Participante de Workflow: Recurso que ejecuta el trabajo representado por un workitem.

Período de validez de un certificado. Periodo que comienza con la emisión del certificado y termina con la fecha de expiración o antes si el certificado es revocado.

Política de seguridad: Documento que recoge todos los requisitos y prácticas de seguridad para asegurar el funcionamiento de la infraestructura de una forma fiable.

Privacidad: Característica que garantiza que nadie salvo el destinatario puede acceder al contenido de un mensaje.

- Q -

- R -

RSA: Rivest, Shamir, Adleman. Algoritmo criptográfico de cifrado de clave asimétrica, utiliza una clave para cifrar y otra para descifrar.

Recuperación de datos: Procedimiento de obtención del mensaje original, a partir de un mensaje cifrado, en situaciones de emergencia.

Registrador: Persona con autoridad para registrar usuarios y revocar certificados en la infraestructura de clave pública de una CA (ver).

Registro de usuarios: Procedimiento por el que se toman los datos personales de un usuario, se confirma su identidad.

Repudio: Negación o intento de negación de haber participado en una comunicación.

Revocación de certificados: Anulación de la validez de un certificado de clave pública antes del fin del periodo de validez.

Rol Organizacional: Grupo de participantes con un grupo particular de atributos.

Rol de Workflow: mecanismo que asocia actividades a los Participantes del Workflow.

- S -

SPI: Service Provider Interfase. Métodos que deben ser implementados para proveedores de servicios de criptografía en la plataforma JCA.

SSL: Secure Socket Layer. Nivel de conexiones seguras. Es un protocolo para cifrar el tráfico de transacciones en una red.

Sistema de Workflow: sistema que define crean y gestiona la ejecución de workflows a través del uso de software, utilizando uno o más motores de workflow, los cuales son capaces de interpretar definiciones de procesos, interactuar con los participantes de workflow.

Subflow o SubWorkflow: Workflow que es iniciado o ejecutado por otro workflow o sub workflow, y que forma parte del workflow llamador.

- T -

TCP / IP: Transfer Control Protocol.

Tarjeta inteligente: Tarjeta que lleva incluido un microprocesador y es utilizada para proporcionar seguridad de la información.

Transición: punto de la ejecución de una instancia de workflow en la cual se completa una actividad y control pasa a otra, la cual comienza.

- U -

UO: Unidad Organizativa. Unidad de ejecución en un organismo público. Es asimilable a lo conocido usualmente como "oficina".

UIT – T: Unión Internacional de Telecomunicaciones. Antes denominada CCITT. Publica normas como la X.509.

UML: Unified Modeling Language: Lenguaje de modelado para especificar, visualizar, construir y documentar elementos de un sistema de Software.

Unión de Expedientes: Acto de unir un expediente a otro de forma que el expediente unido siga el proceso administrativo del segundo.

- V -

Validación de un certificado de usuario: Proceso llevado a cabo por una entidad de confianza o el receptor de un mensaje firmado digitalmente para verificar que el certificado era válido y estaba en el periodo operativo en el momento en el que fue creada la firma.

- W -

WAPI: Workflow APIs y formatos de intercambio. Conjunto de especificaciones que permiten la interoperabilidad entre diferentes componentes de Sistemas de Workflow y aplicaciones.

WWW: World Wide Web.

WYSIWYG: What You See Is What You Get: Programas que presentan a su usuario una interfaz en la que es posible visualizar el resultado final de lo que está haciendo.

WorkItem: representa los datos particulares asociados a una actividad determinada dentro de una instancia de Workflow determinada.

Worklist: lista de workitems asociados a un participante o grupo de participantes particular de un Sistema de Workflow.

WebDAV: estándar que describe como, a través de la extensión del protocolo HTTP 1.1, pueden realizarse acciones de gestión de archivos tales como escribir, copiar, eliminar o modificar.

WFMC: WorkFlow Management Coalition. Organización internacional de vendedores usuarios, analistas y grupos de investigación universitarios cuya misión es promover y desarrollar estándares para el uso de Sistemas de Workflow.

Workflow: la automatización total o parcial de un proceso de negocio, en el cual documentos, información o tareas son pasadas de un participante a otro, de acuerdo con un conjunto de reglas procedurales.

Sistema de Workflow: Sistema capaz de definir, administrar y ejecutar Workflows, a través de software que interpreta una representación electrónica del mismo e interactúa con los recursos participantes

- X -

X509: Norma estándar que define un entorno de autenticación y seguridad. Forma parte de la norma X.500 de UIT -T.

XML: eXtended Markup Language. Es un formato que pensado para servir para independizar el contenido de la presentación del mismo, se crea una estructura a modo de plantilla a la cual se amoldarán el resto de contenidos para crear la página que se mostrará finalmente al usuario. También permite implementar hojas de estilo (XSL).

XPDL: Process Definition Language.

XSL: lenguaje de cascada de estilos para XML.

XSLT: Usado en conjunción con XSL para transformar documentos XML con distintos DTD.

- Y -

- Z -

ZMI: Zope Management Interface. Interfaz Web de manejo y administración del servidor Zope

ZODB: Zope Object Data Base. Base de Datos Orientada a objetos del servidor Zope.

ZPT: Zope Page Templates. Herramienta de generation de páginas web. Hace uso de Template Attribute Language (TAL) para definir atributos que son interpretados por el servidor para generar páginas web dinámicamente. Tiene la ventaja que las etiquetas TAL son ignoradas por los editores WYSIWYG por lo que se puede generar la presentación básica de la página con estas herramientas y modificarlo posteriormente para añadir comportamiento dinámico.

9 APÉNDICE C: PRESENTACIÓN DE PROYECTO DE GRADO

PRESENTACION DE PROYECTO DE GRADO CARRERA INGENIERO EN COMPUTACION - FACULTAD DE INGENIERIA

Identificación del Proyecto

Nombre del Proyecto: Sistema de Gestión de Expediente Electrónico
Año: 2002

Institución en donde se realizara el proyecto: Ministerio de Relaciones Exteriores

Nombre del Responsable del Proyecto por la Institución: Sr. Irio Cerón

Tel: 902 87 93

Fax: 902 87 93

E-mail: irio@mrree.gub.uy

Estudiantes:

Nombre y Apellido	Doc. Identidad	Teléfono	Email
Juan Fernando López Cabrera	3265852-2	4192181	jfl@adinet.com.uy
Luis Pablo Michelena Scaffo	2546708-3	4017370	lmichele@multi.com.uy

Resumen del Proyecto

Como una introducción al tema, se puede decir que desde siempre las grandes oficinas u organizaciones han reunido los documentos asociados con un cierto trámite o acto en legajos, que han rotulado con un identificador único, creando así lo que conocemos hoy en día como el expediente tradicional. El mismo constituyó una forma organizada de manejo documental para una era tecnológica que no ofrecía alternativas, basando el éxito de su funcionamiento en las oficinas cuyo único objetivo consistía en poder localizar, en cualquier momento, un determinado expediente.

Los problemas de extravíos, robos, deterioros, folios faltantes, imposibilidad de acceso, dificultades de almacenamiento y otros; recién fueron encontrando alguna solución en los años '80 cuando se difundieron los primeros programas para seguimiento de expedientes, cuyo cometido esencial era el de llevar registro de la ubicación del expediente físico en todo momento. Pero fue recién hacia finales de los años 90 cuando la baja en los costos de los sistemas de computación, así como la difusión de estándares universales y abiertos - particularmente los de Internet- permitieron el desarrollo de sistemas de Expediente Electrónico en el sentido más amplio del término. En fin, la búsqueda de la Eficiencia Operativa. Permitiendo la completa trazabilidad del trámite y su consulta por parte de los interesados, en forma automática.

Pero si bien actualmente existen sistemas que se encarguen de dicho problema, se busca uno que se ciña a la legislación vigente en el Uruguay, unido a un bajo costo de manejo e implantación.

Es por eso que el Departamento de Informática del Ministerio de Relaciones Exteriores esta interesado en el desarrollo de un Sistema de Expediente Electrónico, con el objetivo de brindar a los funcionarios las mejores herramientas para su gestión diaria, teniendo en cuenta además la política actual del Poder Ejecutivo en reducir los gastos del Estado.

Considerando además que está vigente el decreto 65/998, en el cual se establece la obligatoriedad por parte de las Oficinas Públicas en la adopción de herramientas que permitan manejar los expedientes en forma electrónica, y visto que el sistema desarrollado por la Universidad

de la República (EXPE+), no cumple con los requerimientos propios de un sistema para la Cancillería, se propone:

Realizar como Proyecto de Grado, un Sistema Gestión de Expediente electrónico sobre la base de los requerimientos de la Cancillería pero de tal forma que el mismo pueda ser parametrizado y adaptado a los requerimientos de todas las oficinas del Estado. El mismo podrá ser instalado en forma gratuita para quien lo solicite (Existen en la actualidad otros proyectos desarrollados por Oficinas del Estado pero con costos elevados, NO son gratuitos, por ejemplo este es el caso de UTE).

Descripción del Proyecto

Objetivos

Un sistema de Gestión de Expediente Electrónico parametrizable a los requerimientos de todas las oficinas públicas, que sirva como primer paso hacia el cambio cultural y operativo resultante de la introducción de medios tecnológicos en la gestión del Estado.

Resultados Esperados

Se espera producir un sistema se ajuste a las características más importantes detalladas en el decreto 65/998, logrando una primera aproximación que posibilite el cumplimiento cabal de todos los puntos del referido decreto en futuros desarrollos. Se brindarán las herramientas que permitan la parametrización del sistema a las distintas reparticiones del estado junto con la administración del mismo

Contexto de Trabajo

Los estudiantes trabajarán en estrecho contacto con el Departamento de Informática y las personas que éste considere adecuadas para una completa comprensión del funcionamiento de esta cartera y las características comunes a todas las dependencias del Estado. Se buscará el contacto con la Organización Nacional de Servicio Civil. Esto se llevará a cabo mediante entrevistas y consulta a la documentación. En las etapas finales, se intensificará la concurrencia de los estudiantes a las oficinas de la Cancillería donde podrán crear un entorno de pruebas y una vez aprobada, implantar la solución.

Plan de Trabajo

Cronograma

Mes 1. Relevamiento de requerimientos. Estudio de las funcionalidades, características y posible idoneidad como soluciones al problema planteado, de los Sistemas de Gestión de Expediente Electrónicos existentes en el mercado. Estudio de la reglamentación vigente referida al tema.

Mes 2. Análisis y diseño de Sistema e interfaz.

Meses 3 a 8. Implementación del Sistema. Se elicitará el sistema mediante la presentación de prototipos a finales de los meses 4 y 6.

Meses 6 a 8. Testeo e instalación del Sistema. Elaboración de la documentación de usuario.

Metodología de Trabajo

Para este proyecto se utilizará un modelo de desarrollo incremental con prototipado.

Se definirán una serie de entregables de acuerdo al cronograma planteado. El objetivo de esto es evitar atrasos en el proyecto.

Formación ofrecida al estudiante

Bibliografía específica

Se tendrá como guía los decretos relacionados al tema (65/998 y 500/991)

Recursos Informáticos

Hardware

Dos o más computadoras conectadas en red, una de las cuales deberá ser capaz de ejecutar un DBMS.

Sistema Operativo

Existe flexibilidad en este ítem. Sin embargo se tomarán en cuenta cuestiones como la existencia de licencias de uso del software, dentro de la cancillería y costo global de implantación de la solución.

Lenguajes

Igualmente existe libertad en la elección del lenguaje de desarrollo, siempre y cuando la Cancillería cuente con las licencias adecuadas al caso. Se buscará la mayor portabilidad del código generado.

Herramientas

Otros

Acceso a sistemas similares en uso dentro de la administración pública y a la documentación correspondiente.

Conocimientos previos del estudiante

Exigidos

Redes (curso)

Recomendados

Criptografía, Ingeniería de Software, utilización de herramientas parametrizables y conocimiento de sistemas de WorkFlow.